■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）

7 章 トピックス

（執筆者：河内亮周）［2010 年 4 月 受領］

■概要■

近年では，計算量理論における数々の重要な結果により様々な新たな分野を開拓されつつある．本章では，計算量理論で近年その重要性が注目されている話題及び切り開かれつつある新たな分野について解説を行う．

【本章の構成】

現代暗号には計算量理論の考え方が大きく影響している．その基礎について（7-1）節で説明を行う．（7-2）節では，近年大きく発展した確率的計算可能証明と呼ばれる対話型証明系の一種について解説する．この計算モデルの結果の非常に重要な応用として，計算困難問題に対する近似不可能性の証明についても触れる．（7-3）節では，乱択計算の限界について，特に乱択計算を決定性計算で模倣するのにどの程度の計算量の差が表れるのかを示す手法について述べる．（7-4）節の DNA コンピュータとは DNA などの生体分子を計算に利用する全く新しい計算モデルであり，その概要について解説する．（7-5）節のパラメータ化計算量では，計算困難問題の入力の大きさ以外のパラメータに着目し，そのパラメータに関してどのように困難性が変わるのか，という問題を議論する．（7-6）節の平均計算量理論は，問題の平均的な難しさを議論するための分野であり，最悪時の計算量を議論する従来の理論と大きく異なっている．その基本について説明を行う．（7-7）節は，ホログラフィック計算と呼ばれるごく最近提唱された全く新しいアルゴリズムの設計指針を紹介する．（7-8）節は「戸田の定理」と今日呼ばれる交代性計算と計数計算の間の重要な関係性について解説する．（7-9）節では，NP 対 P 問題の証明のために取られている「自然な証明」と呼ばれる有力な方法の限界について，近年示された重要な結果について概説する．

■6 群 - 2 編 - 7 章

7-1 暗号基礎理論

（執筆者：小柴健史）[2009 年 1 月 受領]

従来暗号は情報理論的な観点からその安全性を議論をしていたが，計算量理論の考え方を導入することにより応用性の高い柔軟な暗号基礎プロトコルが設計できるようになり現代暗号理論として発展している．特に一方向性関数の概念*は現代暗号理論において重要な役割を果たしており，本節では一方向性関数に帰着される暗号基礎プロトコルについて概観する．

7-1-1 計算モデルと一方向性関数

暗号系の安全性を議論するには，正規ユーザと敵対者の計算モデルを規定する必要がある．計算量理論的な安全性を議論する場合，正規ユーザの計算モデルとして多項式時間チューリング機械を想定し，敵対者のモデルとして確率的多項式時間チューリング機械を想定するのが一般的である．より高い安全性を問題としたい場合には敵対者モデルとして多項式サイズ回路族などの非一様計算モデルを考慮することもある．

関数 $f:\{0,1\}^* \to \{0,1\}^*$ が**一方向性関数**†であるとは (1) 任意の n と任意の $x \in \{0,1\}^n$ について $f(x) \in \{0,1\}^{\ell(n)}$ を計算する多項式時間アルゴリズムが存在し，かつ，(2) どんな確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても‡$\{0,1\}^n$ 上の一様分布 U_n を考えたとき $\mathcal{A}$ の逆計算成功確率 $p_n = \Pr[f(\mathcal{A}(1^n, f(U_n))) = f(U_n)]$ が n に関して無視できるときをいう．ここで，関数 $g(n)$ が n に関して無視できるとは，任意の正多項式 p に対して，ある整数 n_0 が存在し，$n \geq n_0$ となる任意の n で $g(n) \leq 1/p(n)$ を満たす場合である．一方向性関数 f において $\ell(n) = n$ のとき長さ保存であるといい，長さ保存で一対一な場合には一方向性置換という．また，$y \in range(f)$ の逆像の大きさが n ごとに一定であるとき，f を正則一方向性関数という．

7-1-2 一方向性関数から構成される暗号基礎プロトコル

一方向性関数から構成されるもので最も基本的なものの一つが擬似乱数生成器である．まず，分布族の識別困難性について定義する．分布族 X_n と Y_n が識別困難であるとは，任意の確率的多項式時間アルゴリズム $\mathcal{D}$ に対して $|\Pr[\mathcal{D}(X_n) = 1] - \Pr[\mathcal{D}(Y_n) = 1]|$ が n に関して無視できるときをいう．関数 $g:\{0,1\}^* \to \{0,1\}^*$ が，(1) $x \in \{0,1\}^n$ のとき $|g(x)| = \ell(n) > n$ となる ℓ が存在し，g は多項式計算可能で，$g(U_n)$ と $U_{\ell(n)}$ が識別困難であるとき，g を**擬似乱数生成器**であるという．一方向性関数から擬似乱数生成器を構成する上で重要な道具としてハードコア関数がある．長さ正則な関数 h (入力長 n のとき出力長 $\ell_h(n)$) が一方向性関数 f の**ハードコア関数**であるとは $f(U_n)\|h(U_n)$ と $f(U_n)\|U_{\ell_h(n)}$ が識別困難であるときをいう．ここで $u\|v$ は u と v の連接を表す．任意の一方向性関数に対して，長さ $O(\log n)$ ハードコア関数が存在することが知られており[5]，この性質を利用すると，任意の一方向性置換 f を用いて $g(U_n) = f(U_n)\|h(U_n)$ とすることで容易に擬似乱数生成器が構成できる[1, 19]．事実，多く

* 本節で述べる概念の幾つか，例えば，一方向性関数や疑似乱数生成器などは，計算量理論においても同様な概念が存在するが，暗号理論における定義とは異なることに注意する必要がある．

† ここでの定義は入力長 n のとき出力長が n となると限定しているので正確には長さ正則な一方向性関数のものであるが，この条件を課さない一般の一方向性関数から長さ正則な一方向性関数が構成可能である．

‡ $\mathcal{A}$ への入力 1^n は $\ell(n)$ が $O(\log n)$ になるなどの短い場合について $\mathcal{A}$ を不利にしないための便法である．

の具体的な構成例はこの方式に基づいている．また正則一方向性関数からの構成方法[4]や任意の一方向性関数からの構成方法[10]も知られている．任意の一方向性関数からの元々の構成方法は難解であったが，近年の新技術の開発[11, 12, 7]によりその理解が容易になってきている．

擬似乱数生成器，つまり，一方向性関数からビット委託方式が構成できる．ビット委託方式は二者間プロトコルで 2 段階からなる．第 1 段階は委託段階とよばれ第 2 段階は公開段階とよばれる．第 1 段階で委託段階では送信者が選択したビット情報 b をプロトコルを介して暗号化された形となるように受信者に伝達する．この段階で受信者は復号が困難であることが要求され，この性質を秘匿性とよぶ．公開段階では委託段階で委託したビット情報を復号するのに必要な情報をプロトコルを介して伝達し受信者は b を復号する．送信者に悪意があったとして，暗号化情報を受信者に誤って $b \oplus 1$ に復号させるようにさせることができないこともプロトコルに要求され，この性質を束縛性とよぶ．秘匿性と束縛性とを同時に情報理論的な意味で満足させることは不可能であり，一方を情報理論的な意味で他方を計算論的の意味で満足させることが一般的である．擬似乱数生成器から情報理論的束縛性を満足する定数ラウンドのビット委託方式が構成できることが知られている[14]．情報理論的秘匿性を満足するビット委託方式は，まず，一方向性置換からの構成が与えられ[15]，正則一方向性関数から[8]，最後には任意の一方向性関数からの構成が示された[9]．情報理論的秘匿性を満たすビット委託方式は $\Omega(n/\log n)$ のラウンド数下界が示唆されている．ビット委託方式はゼロ知識対話証明のビルディングブロックとしても知られている．情報理論的束縛性を満たすビット委託方式を用いて PSPACE 言語に対する計算論的ゼロ知識対話証明が構成でき，情報理論的秘匿性を満たすビット委託方式を用いて NP 言語に対するゼロ知識対話アーギュメントが構成できる．つまり，一方向性関数*からこれらのゼロ知識対話証明・アーギュメントが構成可能である．

ゼロ知識対話証明は認証技術としても利用できるが，簡易な認証技術として電子署名方式がある．電子署名では署名者と検証者の間のプロトコルであり，署名者のみが持つ秘密鍵 (署名鍵) を用いて文書 m に対する署名 σ を作成し，検証を行いたい者は誰でも公開鍵 (検証鍵) を用いて (m, σ) を作成できるのは唯一秘密鍵を持つ署名者であることを検証し，文書 m の信頼性を保証する．署名の安全性概念は幾つか提案されているが，最も安全とされている概念として適応的選択文書攻撃に対する存在的偽造不可能性がある．任意の文書を偽造対象としたとき，その偽造対象の文書を除き任意に選択した文書の署名文を適応的に得ることができるとしても，対象文書の偽造が困難であるとする概念である．汎用一方向性ハッシュ関数族から安全な電子署名方式が構成できることが示されており[16]，任意の一方向性関数から汎用一方向性ハッシュ関数族が構成できる[18]ことと合わせると，一方向性関数から安全な電子署名が構成できる．

7-1-3 その他の暗号基礎プロトコル

上述したように幾つかの暗号基礎プロトコルは一方向性関数から構成可能であるが，代表的な暗号基礎プロトコルでも一方向性関数からの構成が知られていないものがある．公開鍵暗号および紛失通信方式がその代表例である．単に一方向性関数からの構成が未知であると

* ゼロ知識性の定義において非一様性を考慮するため非一様計算における一方向性関数が必要である．

いうだけでなく，一方向性関数からは構成不可能である傍証が得られている[17]．適応的選択暗号文攻撃に対して頑健性がある公開鍵暗号が最も安全性の高いとされているが，落し戸付き一方向性置換から非対話ゼロ知識証明が構成できそれを利用して構成できる[2]．また，紛失通信方式は多者間セキュア通信の基礎プロトコルであることが知られているが[13]，紛失通信そのものに関しては特殊な落し戸付き一方向性置換からの構成が得られている[6]．また，安全な公開鍵暗号と紛失通信とはお互いに構成不可能であるという傍証も得られている[3]．これらの暗号基礎プロトコルに関しては一層の研究が必要であろう．

■参考文献

1) M. Blum and S. Micali, “How to generate cryptographically strong sequences of pseudo-random bits,” SIAM J. Comput., vol.13, no.4, pp.850-864, 1984.
2) D. Dolev, C. Dwork, and M. Naor, “Nonmalleable cryptography,” SIAM J. Comput., vol.30, no.2, pp.391-437, 2000.
3) Y. Gertner, S. Kannan, T. Malkin, O. Reingold, and M. Viswanathan, “The relationship between public key encryption and oblivious transfer,” in Proc. 41st IEEE Symp. Foundations of Comput. Sci., pp.325-335, 2000.
4) O. Goldreich, H. Krawczyk, and M. Luby, “On the existence of pseudorandom generators,” SIAM J. Comput., vol.22, no.6, pp.1163-1175, 1993.
5) O. Goldreich and L.A. Levin, “A hard-core predicate for all one-way functions,” in Proc. 21st ACM Symp. Theory of Comput., pp.25-32, 1989.
6) I. Haitner, “Implementing oblivious transfer using collection of dense trapdoor permutations,” Lect. Notes. Comput. Sci., vol.2951, pp.394-409, 2004.
7) I. Haitner, D. Harnik, and O. Reingold, “On the power of the randomized iterate,” Lect. Notes Comput. Sci., vol.4117, pp.22-40, 2006.
8) I. Haitner, O. Horvitz, J. Katz, C.-Y. Koo, R. Morselli, and R. Shaltiel, “Reducing complexity assumptions for statistically-hiding commitment,” J. Cryptol., vol.22, no.3, pp.283-310, 2009.
9) I. Haitner, M. Nguyen, S.J. Ong, O. Reingold, and S.P. Vadhan, “Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function,” SIAM J. Comput., vol.39, no.3, pp.1153-1218, 2009.
10) J. Håstad, R. Impagliazzo, L.A. Levin, and M. Luby, “A pseudorandom generator from any one-way function,” SIAM J. Comput., vol.28, no.4, pp.1364-1396, 1999.
11) T. Holenstein, “Key agreement from weak bit agreement,” in Proc. 37th ACM Symp. Theory of Comput., pp.664-673, 2005.
12) T. Holenstein, “Pseudorandom generators from one-way functions: A simple construction for any hardness,” Lect. Notes Comput. Sci., vol.3876, pp.443-461, 2006.
13) J. Kilian, “Founding cryptography on oblivious transfer,” in Proc. 20th ACM Symp. Theory of Comput., pp.20-31, 1988.
14) M. Naor, “Bit commitment using pseudorandomness,” J. Cryptol., vol.4, no.2, pp.151-158, 1991.
15) M. Naor, R. Ostrovsky, R. Venkatesan, and M. Yung, “Perfect zero-knowledge arguments for NP using any one-way permutation,” J. Cryptol., vol.11, no.2, pp.87-108, 1998.
16) M. Naor and M. Yung, “Universal one-way hash functions and their cryptographic applications,” in Proc. 21st Symp. Thoey of Comput., pp.33-43, 1989.
17) O. Reingold, L. Trevisan, and S. Vadhan, “Notions of reducibility between cryptographic primitives,” Lect. Notes Comput. Sci., vol.2951, pp.1-20, 2004.

18) J. Rompel, “One-way functions are necessary and sufficient for secure signatures,” in Proc. 22nd ACM Symp. Theory of Comput., pp.387-394, 1990.
19) A.C. Yao, “Theory and applications of trapdoor functions,” in Proc. 23rd IEEE Symp. Foundations of Comput. Sci., pp.80-91, 1982.

■6 群 - 2 編 - 7 章

7-2 確率的検査可能証明と近似不可能性

（執筆者：玉置　卓）[2008 年 12 月 受領]

本節では確率的検査可能証明（Probabilistically Checkable Proofs: PCP）によるクラス NP の新しい特徴づけと，近似不可能性との関係について述べる．言語 L が NP に属するとは，ある多項式 p と検証者と呼ばれる決定性多項式時間チューリング機械 M が存在して，任意の入力列 $x \in \{0,1\}^*$ に対し，

- $x \in L$ ならば短い（つまり $|y| \le p(|x|)$ の）証拠列 y が存在して $M(x,y)$ が受理
- $x \notin L$ ならば任意の $|y| \le p(|x|)$ なる列 y に対して $M(x,y)$ が拒否

を満たすことであった．

PCP では，多項式時間の検証者が，冗長なかたちで証拠列を表しているオラクルにアクセスする．通常，検証者はこのオラクルビットのうちの数ビットにアクセスするだけであり，それらのビット位置は検証者のコイン投げの結果によって決まる． また，入力列が言語に属するならば（すなわち, 検証者が適切なオラクルにアクセスできるとき），検証者は必ず受理する．これに対し，入力列が言語に属さないならば，どのようなオラクルを使っても，検証者は少なくとも 1/2 の確率で拒否しなければならない．図 7･1 に PCP の概要を示す．

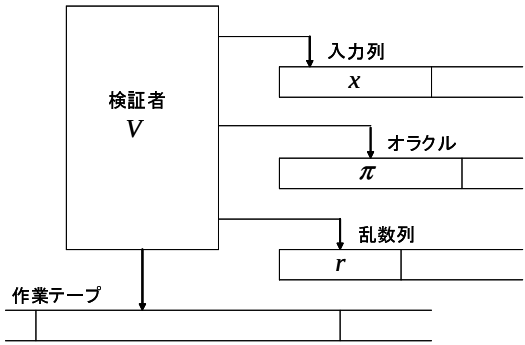

図 7･1　PCP の概要

7-2-1 PCP の定義と能力

言語 L がクラス PCP($r(n), q(n)$) に属するとは，非負整数関数 $r(\cdot), q(\cdot)$，及び検証者と呼ばれる確率的多項式時間オラクル機械 V が存在して，任意の入力列 $x \in \{0,1\}^*$ に対し，

- **完全性**　$x \in L$ ならばあるオラクル π が存在して $V(x,\pi)$ が確率 1 で受理
- **健全性**　$x \notin L$ ならば任意のオラクル π に対して $V(x,\pi)$ が確率 1/2 以上で拒否
- サイズ n の入力に対して，検証者はたかだか $r(n)$ 回のコイン投げとたかだか $q(n)$ のオラクルビットへのアクセスを行う

を満たすことである．

定義より明らかに PCP(0, 0) = P, PCP(poly(n), 0) = coRP, PCP(0, poly(n)) = NP である（coRP は言語に属さない入力に対しては誤りを許す確率多項式時間, poly(n) は n の多項式, つまり $n^{O(1)}$）．更に，PCP($O(\log n)$, poly(n)) ⊆ NP も容易に示される．逆に NP ⊆ PCP($O(\log n)$, $q(n)$) を満たす最小の $q(n)$ はどのような関数か，という問いに驚くべき回答を与えたのが以下の定理である．

定理 (PCP 定理) [1, 2] NP ⊆ PCP($O(\log n)$, $O(1)$).

つまり $q(n)$ を入力列の長さに依存しない定数にまで減らしても NP の言語を認識可能なのである．なお PCP 定理に先立って，対話型証明系の文脈で PCP(poly(n), poly(n)) = NEXP（NEXP は非決定性指数時間）のような結果も示されている．

7-2-2 近似不可能性との関係

3CNF 論理式（各節がたかだか三つのリテラル，つまり変数またはその否定，を含む和積形論理式）が充足可能か判定する問題は 3SAT と呼ばれる NP 完全問題であった．PCP 定理と等価な言明である以下の定理によると，P ≠ NP の仮定のもとで，3SAT は判定が困難であるばかりでなく，近似解を求めることすら不可能であることが示される．

定理 (PCP 定理と等価な言明) ある定数 $\varepsilon > 0$ が存在して, 3CNF 論理式を 3CNF 論理式へ写す多項式時間変換 T で，以下を満たすものが存在する．

- f が充足可能ならば $T(f)$ は充足可能
- f が充足不可能ならば, どんな真偽値割当ても $T(f)$ の節を総数のたかだか $1 - \varepsilon$ の割合でしか充足しない

3CNF 論理式のできるだけ多くの節を充足する真偽値割当て問題を最大 3SAT 問題と呼ぶ．もし，最大 3SAT 問題の任意の例題に対し，最適解の $1 - \varepsilon$ の割合より多くの節を充足する割当てを求める多項式時間アルゴリズムが存在すれば，変換 T と組み合わせることで 3SAT を判定することができる．すなわち P = NP が成り立つので，実際にはそのような近似アルゴリズムは存在しないという強い証拠となっている．

PCP 定理及びより良い性質をもつ PCP の構成により，様々な最適化問題に対する多項式時間近似アルゴリズムの性能限界が証明されている．特に集合被覆問題，彩色数問題，最大クリーク問題，最大 3SAT 問題に対しては，既存の近似アルゴリズムの性能がほぼ最適であることが示されている[3, 4]．

■参考文献

1) S. Arora and S. Safra, “Probabilistic Checking of Proofs: A New Characterization of NP,” J. ACM, vol.45, no.1, pp.70-122, 1998.
2) S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy, “Proof Verification and the Hardness of Approximation Problems,” J. ACM, vol.45, no.3, pp.501-555, 1998.

3) G. Ausiello, P. Crescenzi, G. Gambosi, V. Kann, A. Marchetti-Spaccamela, and M. Protasi, “Complexity and Approximation: Combinatorial Optimization Problems and Their Approximability Properties,” Springer, 1999.
4) V.V. Vazirani, “Approximation Algorithms,” Springer, 2003.

■6 群 - 2 編 - 7 章

7-3 脱乱化手法

（執筆者：河内亮周）［2009 年 1 月 受領］

本節では計算量理論における脱乱化手法の主要結果の紹介並びに研究の方向性について概略を解説する．より具体的な内容に関しては解説論文[2, 4, 7]などを参照されたい．

7-3-1 クラス BPP とその脱乱化

脱乱化における最も重要な未解決問題は，クラス BPP とクラス P が等しいか？ という問題である．直観的にはクラス BPP は乱数を使って効率良く受理できる言語のクラスで，$\mathrm{P} \subseteq \mathrm{BPP}$ である．従って，$\mathrm{BPP} = \mathrm{P}$ が成立する場合，ある意味乱択計算が効率的に決定性計算で模倣できると結論づけられる．現段階で，この未解決問題に対して，以下の重要な結果が知られている．

定理 ある論理関数 $f : \{0,1\}^* \to \{0,1\}$ が存在して，$f \in \mathrm{E}$ かつ $f \notin \mathrm{SIZE}(2^{\Omega(n)})$ ならば，$\mathrm{BPP} = \mathrm{P}$ である．

この定理は Babai と Fortnow と Nisan と Wigderson[1], Nisan と Wigderson[10], Impagliazzo[3], Impagliazzo と Wigderson[5]による四つの論文の結果をまとめることで初めて示される．例えば 2^n 時間決定性チューリング機械で計算可能だけれどもサイズ $2^{0.1n}$ の論理回路では計算できない関数が存在すれば BPP の脱乱化が可能となることを示している．

最も一般的な脱乱化手法は擬似乱数生成器の構成である．前述の定理も計算量の高い関数 f から擬似乱数生成器を構成している．擬似乱数生成器はシードと呼ばれる短い乱数列を入力として受け取って非常に長い擬似乱数列を生成する．擬似乱数列は本物の乱数列と見分けがつかないという性質をもっているので，乱択計算で本物の乱数の代わりに擬似乱数を使っても似た計算結果を出すことが期待できる．

定義 関数 $G : \{0,1\}^m \to \{0,1\}^n$ が任意のサイズ $O(n)$ の n 入力論理回路 C に対して $|\Pr_\sigma[C(G(\sigma)) = 1] - \Pr_\rho[C(\rho) = 1]| < 1/n$ であるとき，擬似乱数生成器であると呼ばれる．特に G が $2^{O(m)}$ で決定性計算可能であるとき効率的であると呼ばれる．

任意の n に対して $m = O(\log n)$ となる効率的擬似乱数生成器が存在すれば $\mathrm{BPP} = \mathrm{P}$ となることが知られている．前述の定理では最悪時計算量が高い関数から困難性増幅と呼ばれる手法を用いて平均計算量の高い関数を一度構成し，それから擬似乱数生成器を構成しているが，困難性増幅を経ない直接的構成方法も Umans [12]によって与えられている．

7-3-2 多様化する脱乱化手法

一般に，計算量の高い関数から擬似乱数生成器を構成する手法は計算困難性−乱数性トレードオフと呼ばれており，BPP 以外の多くの乱択計算量クラスに対してもこの手法が取られる．大きなクラスの例として，クラス AM の NP への脱乱化のために Klivans と van Melkebeek は一般化された擬似乱数生成器の構成を与えている[9]．小さなクラスの例としては，無制限ファンイン定数段回路 AC^0 の乱択版 $\mathrm{BP} \cdot \mathrm{AC}^0$ の脱乱化も同様の手法を用いて Viola[14]により示されている．

また近年では，脱乱化に必要な仮定を，論理回路のような非一様計算モデルに対する困難性ではなく，チューリング機械のような一様計算モデルにおける困難性仮定に弱める研究も進んでいる．例えば，Impagliazzo と Wigderson は EXP ≠ BPP の下で BPP のある種の弱い脱乱化が可能であることを示している[6]．

計算困難な関数から脱乱化するだけではなく，その逆の研究も行われている．代表的な結果として，多項式等価検査と呼ばれる BPP に属する問題の脱乱化が可能だとすると NEXP が多項式サイズ論理回路で計算できない，もしくは行列のパーマネントが多項式サイズの算術回路で計算できない，という回路計算量の下界を与えることが Kabanets と Impagliazzo によって示されている[8]．

7-3-3 ほかの概念との関連性

擬似乱数生成器の構成には非常に高度な組合せ論的構造を必要とするが，脱乱化研究の進展上で同時期に発展してきた計算量理論の新しい概念との関係も明らかになった．

例えば Trevisan は擬似乱数生成器の構成方法が一般的に乱数抽出器の構成にもなっていることを示している[11]．最近，その組合せ論的構造を Vadhan が明示的に与え，その構造によって擬似乱数生成器，乱数抽出器，困難性増幅，リスト復号可能符号，エキスパンダグラフ，などの構成の等価性が説明可能，という統一的な理論を与えている．

■参考文献

1) L. Babai, L. Fortnow, N. Nisan, and A. Wigderson, “BPP has subexponential simulation unless EXPTIME has publishable proofs,” Computational Complexity, vol.3, pp.307-318, 1993.
2) A.E.F. Clementi, J.D.P. Rolim, and L. Trevisan, “Recent advances towards proving P=BPP,” Bull. Eur. Association Theoretical Comput. Sci., vol.64 pp.96-103, 1998.
3) R. Impagliazzo, “Hard-core distributions for somewhat hard problems,” in Proceedings of the 36th Annual IEEE Symposium on Foundations of Computer Science, pp.538-545, 1995.
4) R. Impagliazzo, “Hardness as randomness: a survey of universal derandomization,” in Proceedings of the ICM, vol.3, pp. 659-672, 2002, http://arxiv.org/abs/cs.CC/0304040
5) R. Impagliazzo and A. Wigderson, “P=BPP if E requires exponential circuits: Derandomizing the XOR lemma,” in Proceedings of the 29th Annual ACM Symposium on Theory of Computing, pp.220-229, 1997.
6) R. Impagliazzo and A. Wigderson, “Randomness vs. time: de-randomization under a uniform assumption,” in Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science, pp.734-743, 1998.
7) V. Kabanets, “Derandomization: a brief overview,” Bull. EATCS, vol.76, pp.88-103, 2002.
8) V. Kabanets and R. Impagliazzo, “Derandomizing polynomial identity tests means proving circuit lower bounds,” in Proceedings of the 35th Annual ACM Symposium on Theory of Computing, pp.355-364, 2003.
9) A.R. Klivans and D. van Melkebeek, “Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses,” vol.31, no.5, pp.1501-1526, 2002.
10) N. Nisan and A. Wigderson, “Hardness vs randomness,” J. Comput. System Sci., vol.49, pp.149-167, 1994.
11) L. Trevisan, “Extractors and pseudorandom generators,” J. ACM, vol.48, no.4, pp.860-879, 2001.
12) C. Umans, “Pseudo-random generators for all hardnesses,” J. Comput. System Sci., vol.67, no.2, pp.419-440, 2003.

13) S. Vadhan, “The unified theory of pseudorandomness,” SIGACT News, vol.38, no.3, pp.39-54, 2007.
14) E. Viola, “The complexity of constructing pseudorandom generators from hard functions,” Computational Complexity, vol.13, nos.3-4, pp.147-188.

■6 群 - 2 編 - 7 章

7-4 DNA コンピュータ

（執筆者：榊原康文）［2009 年 1 月 受領］

DNA コンピュータとは，生体分子が潜在的にもつ計算能力を発見し，それを利用して目的の計算や機能を実現することを目指す研究である [1, 2]．半導体をデバイスとして用いる現在のシリコンコンピュータに対して，DNA コンピュータは DNA などの生体分子をデバイスとして用いて，分子間相互作用による分子会合や分子認識の原理を使って計算を実行する．情報分子として知られる DNA は，ヌクレオチドが 1 本鎖状に連結した鎖状高分子であり，DNA 配列上の塩基の組み合わせを変えることによりいくらでも多くの情報を表現できる．注意深く設計された配列をもつ DNA 分子が，化学反応により自律的な動作を行うようになり，それらの一連の動作の結果として計算が実行される．

7-4-1 DNA コンピュータの概要

DNA コンピュータにおいて，最も重要な役割を果たすものの一つが，分子が分子を認識する機構である．生体高分子である DNA をデバイスとして用いる DNA コンピュータにおいては，二つの塩基の間のいわゆるワトソン-クリック相補結合と呼ばれる水素結合が分子認識に使われる．DNA 分子の水素結合は，アデニン（A）とチミン（T），シトシン（C）とグアニン（G）の塩基間の相互作用である．更に，DNA の塩基配列を長くするほど A, C, G, T の組み合わせを多く表現できるようになり，認識の種類を必要なだけ増やすことができるようになる．これが DNA コンピュータを構築するうえで最も重要なポイントとなる．十分な長さの注意深く設計された塩基配列をもつ DNA 分子を多く用意することにより，各 DNA は相補的な相手を見つけ出し，水素結合していく．そして DNA の断片が少しずつ結合して集合体となり，最終的に一つの大きな組織体となる（図 7･2 参照）．このように DNA 分子が自律的に会合して集合体を作ることを自己組織化とかセルフアセンブリと呼ぶ．また最終的に形成される集合体の構造は，各 DNA 断片がもつ塩基配列によって決まってくる．すなわち，形成される構造は DNA 分子の塩基配列のなかにプログラムされているわけであり，逆に見れば，塩基配列の設計によって自己組織化をプログラムすることができるわけである．超分子化学では超分子の構造の設計と作成のためにプログラムするのであるが，DNA コンピュータにおいては計算を実行するためにプログラムするのである．

DNA コンピュータでは，次のように計算が実行される．まずはじめに，プログラムを DNA の塩基配列にコード化する．次に多くのプログラムされた DNA の断片とともに次の二つのステップまたはその繰り返しを実行する：(1) 試験管のなかで複数の DNA 分子を自律的に会合させる，(2) DNA 分子を含んだ試験管に対して分子生物学的実験操作を適用する．最後に，作成または抽出された DNA の集合体が目標とする条件を満たすならば計算は成功したことになり終了する．これが DNA コンピュータにおける計算である．出力は，最終的に残った DNA 分子またはその集合体であり，その構造が計算結果を表すことになる．このように DNA コンピュータにおいては，計算を実行するというより，「計算を組み立てる」という方がより適切な表現かもしれない．DNA 分子の自律的会合がどのくらいの計算能力をもつのかについて研究されている [3]．線形な構造の DNA 分子の自律的会合は有限状態オートマトンと同等な計算能力をもち，分岐構造をもつ DNA 分子の自律的会合はプッシュダウンオー

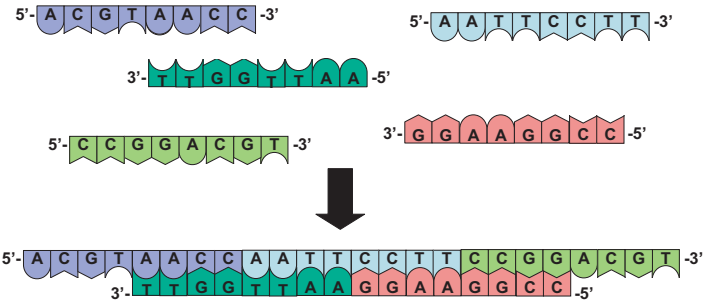

図 7･2　DNA 分子の自己組織化：プログラムされた塩基配列をもつ 5 個の DNA 分子と自律的会合により一つの集合体ができるまで

トマトンと同等な計算能力，DNA タイルと呼ばれる 2 次元の構造をもつ DNA 分子の自律的会合は万能な計算能力をもつことが示されている．このように DNA 分子の自律的会合による計算では，形成される構造の複雑さと計算能力の間に深い関連があることが分かる．

7-4-2 細胞オートマトンの実現に向けたアプローチ

今まで見てきた DNA コンピュータの研究では，DNA 分子の自律的会合や自己組織化と，それを制御したり検出する分子生物学の実験操作を用いて計算を実行するのが主な手法であった．しかし，実際の細胞内ではそのほかにも様々な分子（特にタンパク質分子）がより複雑でより高機能なはたらきを行っている．その代表的なものの一つであるタンパク質の合成にかかわる分子とそのメカニズムを利用して，全く新しいそしてより精度の高い DNA コンピュータを実現する研究について紹介する．

リボゾームや転移 RNA，そのほかの合成因子から構成されるタンパク質合成の細胞内メカニズムは，非常に精度が高い機構であり，遺伝コードに従ってメッセンジャー RNA に書かれた配列情報を正確に読み取ってタンパク質を合成していく．一方，遺伝コードを拡張するために，自然界で使用されている 3 塩基コドンを拡張した 4 塩基コドンや 5 塩基コドンなどの拡張コドンの技術が提案されている．そこで，榊原ら [4] は，大腸菌（*E. Coli*）内のタンパク質合成メカニズムを用いて有限オートマトンを計算する方式と実験プロトコルを設計した．この方式は，有限オートマトンという最も基本的な計算モデルを，タンパク質合成メカニズムと拡張コドンを用いて実現し，細胞のなかでその計算を実行する．

実験に用いた有限オートマトンは，2 状態のオートマトンで，入力された文字列中の 1 の個数が偶数倍のときに受理する（すなわち，パリティビットを検出できる）有限オートマトンである．実験の結果，1 の個数が 2, 4, 6 の偶数の場合にはコロニーが青く染まったことが検出され，1, 3, 5 の奇数の場合にはコロニーが染まらなかったことを確認した．このことから，有限オートマトンの計算が正しく実行されたことを確認すると同時に，大腸菌を用いた DNA コンピュータの設計原理が正しかったことを確認できた（図 7･3 参照）．この実験結果は，まだ初等計算機ではあるが世界で初めてバクテリアを用いて計算が実行できたことを証明するものである．

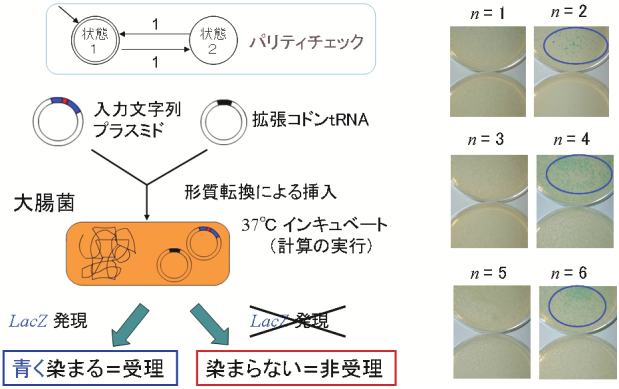

図 7·3　大腸菌を用いたバクテリアコンピュータの実装と実験：（左上）入力された文字列中の 1 の個数が偶数倍のときに受理する 2 状態有限オートマトン．（左下）バクテリアコンピュータによる計算の実行．（右）六つの入力文字列 1, 11, 111, 1111, 11111, 111111 を入力したときの実行結果．上段のプレートは 4 塩基アンチコドン UCCU をもつ tRNA を挿入した場合，下段はその tRNA を挿入しないコントロールを示す．プレート中の円で囲まれた領域は，青色を発現するコロニーを示している．

■参考文献

1) 萩谷昌己, 横森貴 編, “DNA コンピュータ,” 培風館, 2001.
2) Gh. Păun, G. Rozenberg, and A. Salomaa, “DNA Computing,” Springer-Verlag, 1998; (横森貴, 榊原康文, 小林聡 訳, “DNA コンピューティング,” シュプリンガー・フェアラーク東京, 1999)
3) E. Winfree, X. Yang, and N.C. Seeman, “Universal computation via self-assembly of DNA - some theory and experiments,” in DNA Based Computers II (DIMACS series in discrete mathematics and theoretical computer science), vol.44, pp.191-213, 1999.
4) H. Nakagawa, K. Sakamoto, and Y. Sakakibara, “Development of an in vivo computer based on Escherichia coli,” in Proceedings of 11th International Meeting on DNA Based Computers, Lecture Notes in Computer Science 3892, Springer-Verlag, pp.203-212, 2006.

■6 群 - 2 編 - 7 章

7-5 パラメータ化計算量

（執筆者：岡本吉央）[2008 年 12 月 受領]

例えば，クリーク問題を考える．これは無向グラフ G と自然数 k が与えられたときに，G が頂点数 k のクリークを含むか判定する問題である．ただし，G のクリークとは G の頂点部分集合で，その任意の 2 点が隣接しているもののことである．クリーク問題を解くための自明なアルゴリズムは要素数 k の頂点部分集合をすべて見て，それらがクリークであるかどうかを確認するものである．与えられたグラフ G の頂点数が n ならば，要素数 k の頂点部分集合数は $O(n^k)$ となり，このアルゴリズムの時間計算量は $O(n^k k^2)$ である．これは k が定数であっても 1000 ならば $O(n^{1000})$ になり，実用的ではない．しかし，クリーク問題が NP 完全であるという事実に直面すると，計算量の超多項式関数的依存性は避けられないであろう．

それでも，$O(2^k n)$ という時間計算量のアルゴリズムがクリーク問題に対して存在するかもしれない．この計算量も超多項式関数的依存性を持っているので，クリーク問題の NP 完全性とは共生できる．その一方で，k が 1000 であっても 10000 であっても計算量は $O(n)$ である．これは $O(n^k)$ という計算量にない顕著な特徴である．すなわち，$O(2^k n)$ 時間アルゴリズムは $O(n^k)$ 時間アルゴリズムよりも優れていると見なせる．

では，どのような問題が $O(2^k n)$ のような時間計算量のアルゴリズムを持つのだろうか？ あるいは，そのような時間計算量を持たないことを考察するための計算量クラスはどのようなものなのだろうか？ このような問いに答えるための理論が R. Downey と M. Fellows の創始したパラメータ化計算量理論である．本節の内容は主に Flum and Grohe の教科書[1]の数ページを基にしている．

7-5-1 パラメータ化問題と容易な問題

パラメータ化計算量理論では通常の問題にパラメータを付けたパラメータ化問題を考察対象とする．古典的な判定問題はアルファベットを Σ としたとき Σ 上の言語 $Q \subseteq \Sigma^*$ のことである．Σ^* の**パラメータ化** (parameterization) とは多項式時間計算可能関数 $\kappa\colon \Sigma^* \to \mathbb{N}$ のことである．Σ 上の**パラメータ化問題** (parameterized problem) とは，判定問題 $Q \subseteq \Sigma^*$ とパラメータ化 $\kappa\colon \Sigma^* \to \mathbb{N}$ の対 (Q, κ) のことである．パラメータ化問題 (Q, κ) に対して $x \in Q$ は**インスタンス** (instance) と呼ばれ，$\kappa(x)$ は x の**パラメータ** (parameter) と呼ばれる．

パラメータ化問題 (Q, κ) に対する (強一様) **固定パラメータアルゴリズム** ((strongly uniform) fixed-parameter algorithm) とは，Q を解くアルゴリズムで，計算可能関数 $f\colon \mathbb{N} \to \mathbb{N}$ と多項式関数 $p\colon \mathbb{N} \to \mathbb{N}$ を用いて任意のインスタンス x に対する時間計算量が高々 $f(\kappa(x))p(|x|)$ になるもののことである (ただし，$|x|$ は x の長さ)．固定パラメータアルゴリズムを持つパラメータ化問題全体のクラスを FPT（Fixed Parameter Tractable）と呼ぶ．クラス FPT は容易なパラメータ化問題のクラスであると考えられていて，例えば次のような問題 (Q, κ) が FPT に属する．(1：パラメータ化頂点被覆問題) $Q = \{$ 頂点数 k の頂点被覆を持つ無向グラフ (の適当な符号化)$\}$，$\kappa(x) = k$．ただし，グラフの**頂点被覆** (vertex cover) とはその頂点部分集合で，各辺の端点のいずれかを含むもののことである．(2：パラメータ化閉路問題) $Q = \{$ 長さ k の閉路を持つ無向グラフ (の適当な符号化)$\}$，$\kappa(x) = k$．ここで，閉路は同じ頂点を繰り返し含まないものとする．

7-5-2 困難なパラメータ化問題と W 階層

計算量理論の基本概念は計算量クラスと還元である．パラメータ化計算量理論において次の FPT 還元が大きな役割を果たす．アルファベット Σ, Σ' 上のパラメータ化問題 $(Q, \kappa), (Q', \kappa')$ に対して (Q, κ) から (Q', κ') への **FPT 還元** (FPT reduction) とは，次の 3 条件を満たす写像 $R\colon \Sigma^* \to (\Sigma')^*$ のことである．(1) 任意の $x \in \Sigma^*$ に対して，$x \in Q$ と $R(x) \in Q'$ が同値．(2) R は固定パラメータアルゴリズムである．すなわち，ある計算可能関数 f と多項式 p が存在して，任意の $x \in \Sigma^*$ に対する $R(x)$ が $f(\kappa(x))p(|x|)$ 時間で計算可能．(3) 計算可能関数 $g\colon \mathbb{N} \to \mathbb{N}$ が存在して，任意の $x \in \Sigma^*$ に対して $\kappa'(R(x)) \le g(\kappa(x))$ が成立する．次のような基本的な性質が成立することは簡単に分かる．(1) FPT 還元の合成も FPT 還元．(2) (Q, κ) から (Q', κ') への FPT 還元が存在し，$(Q', \kappa') \in$ FPT ならば，$(Q, \kappa) \in$ FPT.

古典的な計算量理論で充足可能性問題 (SAT) が重要な役割を果たしていたように，パラメータ化計算量理論でも SAT が重要な役割を果たす．自然数 k に対して論理関数 ϕ が **k-充足可能** (k-satisfiable) であるとは，k 個の変数が真値を取る真理値割当で φ を充足するものが存在することである．**重み付き充足可能性問題** (weighted SAT: WSAT) とは自然数 k と論理関数 φ が与えられたとき，φ が k-充足可能か決定する問題である．論理関数のクラス Γ に対して pWSAT(Γ) で Q を Γ に属する k-充足可能論理関数 φ (の適当な符号化) のクラスとし，$\kappa(\varphi) = k$ とするパラメータ化問題 (Q, κ) を表す．論理関数のクラスとして自然数 $t \ge 0, d \ge 1$ を用いたクラス $\Gamma_{t,d}$ と $\Delta_{t,d}$ を再帰的に定義する：$\Gamma_{0,d} = \{\lambda_1 \wedge \cdots \wedge \lambda_c \mid c \le d, \lambda_1, \ldots, \lambda_c$はリテラル$\}$, $\Delta_{0,d} = \{\lambda_1 \vee \cdots \vee \lambda_c \mid c \le d, \lambda_1, \ldots, \lambda_c$はリテラル$\}$, $\Gamma_{t+1,d} = \{\bigwedge_{i \in I} \delta_i \mid I$ は有限, $\delta_i \in \Delta_{t,d}\ \forall\, i \in I\}$, $\Delta_{t+1,d} = \{\bigvee_{i \in I} \gamma_i \mid I$ は有限, $\gamma_i \in \Gamma_{t,d}\ \forall\, i \in I\}$．このとき，パラメータ化問題がクラス W[$t$] に属するとは，ある $d \ge 1$ に対する pWSAT($\Gamma_{t,d}$) からその問題への FPT 還元が存在することである．同様に，パラメータ化問題がクラス W[SAT] に属するとは，PROP を論理関数全体の族とするとき pWSAT(PROP) からその問題への FPT 還元が存在することである．パラメータ化問題がクラス W[P] に属するとは，CIRC を論理回路全体の族とするとき pWSAT(CIRC) からその問題への FPT 還元が存在することである．定義より，FPT $\subseteq$ W[1] $\subseteq$ W[2] $\subseteq \cdots \subseteq$ W[SAT] $\subseteq$ W[P] の成立が分かる．この包含関係が等号で成り立つかどうか知られていない．すなわち，W[1] に属する問題で，それに対する固定パラメータアルゴリズムが存在するか分からないものが存在する．例えば任意の W[1] 完全問題はそのようなものである．

W[1] 完全問題や他のクラスに対する困難問題の代表例を挙げる．(1：パラメータ化クリーク問題 (W[1] 完全)) $Q = \{$ 頂点数 k のクリークを持つ無向グラフ (の適当な符号化)$\}$, $\kappa(x) = k$. グラフのクリークは本節冒頭で定義した．(2：パラメータ化支配集合問題 (W[2] 完全)) $Q = \{$ 頂点数 k の支配集合を持つ無向グラフ (の適当な符号化)$\}$, $\kappa(x) = k$. グラフの**支配集合** (dominating set) とは頂点部分集合で，それに属さない頂点の隣接点の一つを必ず含むもののことである．(3：パラメータ化バンド幅問題 (任意の $t \ge 1$ に対して W[t] 困難)) $Q = \{$ バンド幅 k の無向グラフ (の適当な符号化)$\}$, $\kappa(x) = k$. グラフ G の**バンド幅** (bandwidth) とは $\min_f \max_G$ の辺 $\{u,v\}\ |f(u) - f(v)|$ であり，min は G の頂点集合から $\mathbb{N}$ への単射 f すべての上で取る．(4：パラメータ化実行可能線形不等式系問題 (W[P] 完全)) $Q = \{k$ 個の不等式を取り除けば実行可能になる線形不等式系 (の適当な符号化)$\}$, $\kappa(x) = k$.

■参考文献

1) J. Flum and M. Grohe, “Parameterized Complexity Theory,” Springer, Berlin Heidelberg, 2006.

■6 群 - 2 編 - 7 章

7-6 平均計算量

（執筆者：河内亮周）［2008 年 12 月 受領］

本節では計算量理論における平均計算量理論の概略について述べる．より具体的な内容に関しては教科書[1)]などを参照されたい．

7-6-1 なぜ平均計算量か

従来の計算量理論では，解くのに最も時間がかかる最悪時の入力によって問題の難しさを特徴づけていた．その一方で平均計算量理論では問題の難しさを平均的な入力で特徴づけることを目標としている．これには主に二つの動機がある．一つは現代暗号理論への応用であり，もう一つは発見的アルゴリズムに対する問題の難しさの同定である．

現代暗号理論では，素因数分解などの計算困難な問題を利用して暗号プロトコルが構成される．暗号プロトコルの攻撃を行うことも一種の計算問題であり，その問題を暗号が利用している困難問題に帰着することでプロトコルの安全性を保証するためである．従って，暗号プロトコルが利用している問題の最悪計算量は高いが平均計算量が低い場合には，敵対者にとって最悪時には攻撃は難しくなるが，典型的な場合には容易に攻撃可能になってしまうかも知れない．このような暗号プロトコルに用いる問題では平均計算量の高さが重要であることが分かる．

また最悪時では非常に難しいと思われる問題でも典型的な入力は容易に解けることも多い．例えば NP 困難問題は現実世界でも頻繁に現れ，従来の計算量理論では難しい問題だとみなされているが，現実的な状況下の入力に対しては発見的アルゴリズムにより非常に高速に解くことができることがよくある．このような「典型的な入力」に対する計算量の同定はより現実に近い理論の構築に有用だと考えられる．

7-6-2 平均計算量の定義

問題 L の平均的な入力に対する計算量を定式化するためには，入力の分布のアンサンブル $\mathcal{D} = \{D_n\}_{n\in\mathbb{N}}$（ここで D_n は n ビット上の分布）も同時に考える必要がある．この分布付き問題 $(L, \mathcal{D})$ に対して，「平均的に効率良く解ける」ことを厳密に定義したい．あるアルゴリズム A が存在してその問題を分布アンサンブル $\mathcal{D}$ に関する期待多項式時間で解くことができれば，そう定義するのが自然であるように見えるが，この定義には計算モデルの頑健性上の問題がある．

例えば，n ビット入力 $x \in \{0,1\}^n$ に対する A の実行時間を $T(x)$ としたとき，A の模倣を $T^2(x)$ 時間で行う（例えば別の計算モデル上の）アルゴリズム B を考える．当然 A が平均的に効率良く解けるならば B も平均的に効率良く解けるといえるのが自然である．ここで $T(0^n) = 2^n, T(x) = n^2\ (x \neq 0^n)$, つまり一つの要素だけ指数時間で残りは多項式時間であるとすると, A の期待実行時間（T の一様分布に対する期待値）$\mathrm{E}_x[T(x)] = (1-2^{-n})n^2+1$ は n の多項式で抑えられるが, B の期待実行時間（T^2 の一様分布に対する期待値）は $\mathrm{E}_x[T^2(x)] = (1-2^{-n})n^4+2^n$ となるため，指数時間になってしまう．このような問題を避けるため Levin は，時間がかかる入力が現れる確率はそのかかる時間に応じて低くなるべきである，という考え方に基づいて「平均的に効率良く解ける」ことの定式化を行った[3)]．以下の定義は Levin の定義と少

し異なるが等価なものになっている．$(L, \mathcal{D})$ が平均的多項式時間で解けるとは，ある決定性チューリング機械 A とある定数 $\varepsilon > 0$ とある多項式 p が存在して，任意の $t, n > 0$ に対して $\Pr_{x \sim D_n}[T(x) \geq t] \leq p(n)/t^{\varepsilon}$ が成り立つことをいう．平均的多項式時間で解ける問題のクラスを AvgP と呼ぶ．この定義では決定性のアルゴリズムを考えているが，様々な計算モデル（乱択アルゴリズムや論理回路など）に対しても定式化が行われている[1]．

7-6-3 平均計算量での NP 完全性

分布付き問題でも通常の計算量理論と同様に還元の概念を導入することで平均計算量に基づいた NP の完全性が Levin によって定義されている[3]．$(L, \mathcal{D})$ が $(L', \mathcal{D}')$ に平均的多項式時間還元可能であるとは，多項式時間計算可能関数 f が存在して任意の $n \in \mathbb{N}$ と $x \in \mathrm{Supp}(D_n)$ に対して (1) $x \in L$ と $f(x; n) \in L'$ が等価でかつ (2) ある多項式 p と m が存在して任意の $\ell \in \mathbb{N}$ と $y \in \mathrm{Supp}(D'_{m(\ell)})$ に対して $\sum_{x: f(x;\ell)=y} D_\ell(x) \leq p(\ell) D'_{m(\ell)}(y)$ が成立することである．このとき $(L, \mathcal{D}) \leq_{\mathrm{AvgP}} (L', \mathcal{D}')$ と書く．

条件 (1) は通常の多項式時間多対一還元と同じである．条件 (2) は少し複雑だが，直観的には D_n から標本抽出を行い f を計算して y が得られる確率が直接 $D'_m(n)$ から標本抽出して得られる確率よりもあまり大きくないことを意味しており，都合の悪い入力が起こる確率が還元 f によって大きくなり過ぎないことを保証している．

この還元を利用して平均計算量における NP 完全性を定義できる．この際，問題のクラス以外に分布アンサンブルのクラスについても考察する必要がある．ここでは多項式時間計算可能分布アンサンブルというものを考える．$\mathcal{D}$ が多項式時間計算可能分布アンサンブルであるとは $x \in \{0,1\}^n$ と $n \in \mathbb{N}$ が与えられたときに $f_{D_n}(x) = \sum_{y \leq x} D_n(y)$ が多項式時間計算可能であることをいう．そのような分布クラスを $\mathrm{P}_{\mathrm{COMP}}$ と定義する．

分布付き問題 $(L, \mathcal{D})$ が $(\mathrm{NP}, \mathrm{P}_{\mathrm{COMP}})$ 完全であるとは，$L \in \mathrm{NP}$ かつ $\mathcal{D} \in \mathrm{P}_{\mathrm{COMP}}$ であり，$M \in \mathrm{NP}$ かつ $\mathcal{E} \in \mathrm{P}_{\mathrm{COMP}}$ となる任意の分布付き問題 $(M, \mathcal{E})$ に対して $(M, \mathcal{E}) \leq_{\mathrm{AvgP}} (L, \mathcal{D})$ であることをいう．$(\mathrm{NP}, \mathrm{P}_{\mathrm{COMP}})$ 完全問題の例として，限定停止性問題と呼ばれる非決定性チューリング機械が与えられた時間で停止するかを判定する問題にある単純な分布が付いた分布付き問題などがある．もし $(\mathrm{NP}, \mathrm{P}_{\mathrm{COMP}})$ 完全問題が平均的多項式時間で解けるならば任意の $(\mathrm{NP}, \mathrm{P}_{\mathrm{COMP}})$ に属する分布付き問題が平均的多項式時間で解けることを意味する．

より自然な分布アンサンブルのクラスとして多項式時間標本抽出可能分布アンサンブルクラス $\mathrm{P}_{\mathrm{SAMP}}$ がしばしば考えられる．ある分布アンサンブル $\mathcal{D} = \{D_n\}_{n \in \mathbb{N}}$ が $\mathrm{P}_{\mathrm{SAMP}}$ に属するとは，ある多項式時間確率的チューリング機械 S が存在して任意の $n \in \mathbb{N}$ に対して $\Pr[S(1^n) = x] = D_n(x)$ を満たすことである．つまり S は分布 D_n の効率的な標本抽出機となっている．Impagliazzo と Levin の結果[2]より $(\mathrm{NP}, \mathrm{P}_{\mathrm{SAMP}})$ の任意の問題から $(\mathrm{NP}, \mathrm{P}_{\mathrm{COMP}})$ 完全問題へのある種の平均的多項式時間乱択還元が存在することが分かっている．

■参考文献

1) A. Bogdanov and L. Trevisan, “Average-case complexity,” Foundation and Trends in Theoretical Comput. Sci., vol.2, no.1 pp.1-106, 2006.
2) R. Impagliazzo and L.A. Levin, “No better ways to generate hard NP instances than picking uniformly at random,” in Proc. of FOCS, pp.812-821, 1990.
3) L.A. Levin, “Average case complete problems,” SIAM J. Comput., vol.15, no.1, pp.285-286, 1986.

■6 群 - 2 編 - 7 章

7-7 ホログラフィック計算

（執筆者：Jin-Yi Cai［訳：河内亮周］）［2009 年 3 月 受領］

P ≠ NP が成立すると広く考えられているが，この予想はよく研究された幾千もの NP 困難問題のどれにも多項式時間アルゴリズムが見つかっていないことに基づいている．代表的な問題として以下の 3-SAT がある．節 C_j のブール積 $\bigwedge_j C_j$ が与えられたとする．このとき各 C_j は x_i や $\overline{x_{i'}}$ などの三つのリテラルのブール和である．3-SAT はそのブール積の評価値を真にするような真理値の割当て方，つまり充足割当てがあるかどうかを決定する問題である．対応する計数問題つまり 3-SAT に対してすべての充足割当ての数を求める問題は，#P-完全である．更に，数多くのその問題の制限版も NP-完全あるいは#P-完全のままである．そのような問題に対してどんなアルゴリズムも指数関数的な数の可能性を考慮する必要があるため指数時間必要であると考えられている．

しかしながら，指数関数的な数の可能性を確認する必要がありそうというこの考え方では正しい帰結が得られないことがある．ある問題では，一見指数関数的な時間が必要そうに見えるが，実際には巧妙なアルゴリズムがあってその問題を多項式時間で解けることが証明できることもある．一つの例として，問題 PERFECT MATCHING があげられる．この問題は任意のグラフ G が与えられたとき，完全マッチングがあるかどうか，つまり辺の部分集合 M があって各点が M のなかのちょうど一つの辺だけに接続しているかどうかを判定する問題である．もう一つの例は平面グラフの完全マッチングの数を多項式時間で数え上げる Kasteleyn のアルゴリズムである[1]．重み付き平面グラフ $G = (V, E, w)$ に対して，$\mathrm{PerfMatch}(G) = \sum_M \prod_{e \in M} w(e)$ と定義する．この和は G のすべての完全マッチング M 上で取られる．このとき Kasteleyn のアルゴリズムは $\mathrm{PerfMatch}(G)$ を多項式時間で計算できる．L. Valiant はある問題のクラスについて指数関数的な計算速度改良を得るためホログラフィックアルゴリズム（holographic algorithm）の新しい理論を提唱した[2]．これらのアルゴリズムはその操作において Kasteleyn のアルゴリズムを基本構成部品として用いている．

（平面）**マッチゲート（*match gate*）**とは**入力**あるいは**出力**と呼ばれるいくつかの外部頂点をもつ重み付き無向平面グラフである．**生成子マッチゲート**Γ とは組 (G, X) である．ここで $G = (V, E, w)$ であり，$X \subseteq V$ は外部**出力**頂点である．同様に**認識子マッチゲート**は外部**入力**頂点をもつ．Γ がもし偶数個（奇数個）の頂点をもつならば偶マッチゲート（奇マッチゲート）と呼ばれる．組合せ論的対象としては，生成子マッチゲートと認識子マッチゲートには違いがない．それらの違いは**特徴値（*signature*）**テンソルの割当て方に現れてくる．

$\mathbf{b} = [\mathbf{b}_0, \mathbf{b}_1] = \left[\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right]$ を 2 次元ベクトル空間 V をはる標準基底とする．m 出力頂点をもつ生成子 Γ は $\binom{m}{0}$ 型の**反変テンソル**$\mathbf{G} \in V_0^m$ を割り当てられる．この標準基底の下でのテンソルは

$$\sum G^{i_1 i_2 \ldots i_m} \mathbf{b}_{i_1} \otimes \mathbf{b}_{i_2} \otimes \cdots \otimes \mathbf{b}_{i_m}$$

というかたちとなる．ここで

$$G^{i_1 i_2 \ldots i_m} = \mathrm{PerfMatch}(G - Z)$$

であり，Z は特性列 $\chi_Z = i_1 i_2 \dots i_m$ をもつ出力頂点の部分集合である．もし $\boldsymbol{\beta}_j = \sum_i \mathbf{b}_i t^i_j$ が基底変換であれば，$\mathbf{G}$ は反変テンソルとして

$$(G')^{i'_1 i'_2 \dots i'_m} = \sum G^{i_1 i_2 \dots i_m} \tilde{t}^{i'_1}_{i_1} \tilde{t}^{i'_2}_{i_2} \dots \tilde{t}^{i'_m}_{i_m}$$

に変換される．ここで $(\tilde{t}^i_j)$ は (t^i_j) の逆行列である．

同様に，m 入力頂点をもつ認識子 Γ' は $\binom{0}{m}$ 型の**共変テンソル**$\mathbf{R} \in V^0_m$ が割り当てられる．標準（双対）基底 $\mathbf{b}^*$ のもとで，$\mathbf{R}$ は

$$\sum R_{i_1 i_2 \dots i_m} \mathbf{b}^{i_1} \otimes \mathbf{b}^{i_2} \otimes \dots \otimes \mathbf{b}^{i_m}$$

というかたちとなる．ここで

$$R_{i_1 i_2 \dots i_m} = \text{PerfMatch}(G - Z)$$

である．しかしこれは共変テンソルとして

$$(R')_{i'_1 i'_2 \dots i'_m} = \sum R_{i_1 i_2 \dots i_m} t^{i_1}_{i'_1} t^{i_2}_{i'_2} \dots t^{i_m}_{i'_m}$$

に変換される．

マッチグリッド（*match grid*）$\Omega = (A, B, C)$ は重み付き平面グラフであり，互いに素な集合 A, B, C の和集合からなる．$A = (A_1, \dots, A_g)$ は g 個の生成子の集合，$B = (B_1, \dots, B_r)$ は r 個の認識子の集合，$C = (C_1, \dots, C_f)$ は f 本の接続辺の集合である．ここで各辺 C_k は重み 1 をもち，ある A_i とある B_j をつないでおり，すべての構成要素のマッチゲートでの入力・出力頂点は完全マッチングによりつながっている．

$\mathbf{G} = \bigotimes_{i=1}^{g} \mathbf{G}(A_i)$ をすべての生成子特徴値のテンソル積，$\mathbf{R} = \bigotimes_{j=1}^{r} \mathbf{R}(B_j)$ をすべての認識子特徴値のテンソル積とする．このとき Holant (Ω) をある基底 $\boldsymbol{\beta}$ のもとでの二つのテンソル積の縮約と定義する．ここで対応する添え字は f 本の接続辺 C_k に従って合わせられる．

もしこれらのテンソル $\mathbf{G}$ と $\mathbf{R}$ を指数関数的に長いベクトルだとみなすと，Holant (Ω) は単にそれらの内積となる．Valiant の Holant 定理は以下で与えられる．

定理 任意の基底 $\boldsymbol{\beta}$ 上の任意のマッチグリッド Ω に対して，G をその重み付きグラフとしたときに，

$$\text{Holant}\,(\Omega) = \text{PerfMatch}\,(G)$$

が成り立つ．

マッチゲートに基づくホログラフィックアルゴリズムのアイディアは行いたい計算を適切な指数和 Holant (Ω) で表現し，それからその値を PerfMatch (G) として Kasteleyn のアルゴリズムによって計算を行うことにある．その例をここで一つ与えよう．

3-SAT のインスタンス上で充足割当てを数え上げる問題を考えよう．ただしこのインスタンスは制限付きで，各変数 x_i は正リテラルとしてちょうど二つの節 C_j に現れるとする．このインスタンスは 2-3 正則二部グラフとして表現することが可能である．ここで左側の点は

x_i でラベルづけされ，右側の点は C_j でラベルづけされている．更にこのグラフが平面グラフであると仮定する．この制限付き 3-SAT 数え上げ問題も#P-完全であることが知られている．その上，この制限付き版に対して，充足割当て数を 2 で割った余りを求めるだけでも NP-困難である．

今，各変数 x に対して $G_x = (1,0,0,1)$，そして各節 C に対して $R_C = (0,1,1,1,1,1,1,1)$ と特徴値を割り当てよう．指数和 Holant (Ω) が割当ての数にちょうどなることに注意しよう．このことを見るために，各変数 x に 0-1 の値を与える任意の割当てを考える．その二部グラフでは，変数から節への辺に 0 もしくは 1 のラベルが割当てられる．このときテンソル積 $\bigotimes_x \mathbf{G}_x$ では各要素は 0 もしくは 1 となり，各変数に対して無矛盾なラベルづけと対応するとき，かつそのときに限りその値は 1 となる．これはちょうど真理値割当てに対応する．テンソル積 $\bigotimes_C \mathbf{R}_C$ において，$(0,1,1,1,1,1,1,1)$ が 3 ビット上の OR の真理値表であるように，要素が 1 となるのは各節 C が充足されるときかつそのときに限る．

標準基底のもとで，$G_x = (1,0,0,1)$ は 4 点と 3 辺の路からなる単純なマッチゲートにより実現可能である．その二つの端点は出力頂点であり，各辺は重み 1 をもつ．もしこの路の端点を両方を取り除くかあるいは両方とも取り除かなければ，完全マッチング値 $\mathrm{PerfMatch}(G-Z) = 1$ となり，もし片方の端点だけを取り除くならば，$\mathrm{PerfMatch}(G-Z) = 0$ となることに注意する．もし同様に R_C に対するマッチゲートを見つけることができれば，Kasteleyn のアルゴリズムを用いて#P-完全問題を多項式時間で解くことが可能となる．残念ながら，標準基底のもとで特徴値 $(0,1,1,1,1,1,1,1)$ をもつマッチゲートはない．

しかしながらここで適当な基底変換を選んでもよい．単純な構成により特徴値 $\frac{1}{4}(0,1,1,0,1,0,0,1)$ をもつマッチゲートは存在する．ここで値 0 もしくは 1/4 は $\mathrm{PerfMatch}(G-Z)$ の評価値である．$\boldsymbol{\beta} = \left[\begin{pmatrix}1+\omega\\1-\omega\end{pmatrix},\ \begin{pmatrix}1\\1\end{pmatrix}\right]$ とする．ここで $\omega = e^{2\pi i/3}$ である．$\boldsymbol{\beta}^{\otimes 3}$ で張られるテンソル空間では，OR 特徴値 $(0,1,1,1,1,1,1,1)$ は以下の共変変換のもとで実現される．$(\boldsymbol{\beta}^{-1})^{\otimes 3} = \left(\begin{bmatrix}1+\omega & 1\\ 1-\omega & 1\end{bmatrix}^{-1}\right)^{\otimes 3}$ は

$$\frac{1}{8}\begin{pmatrix}
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1\\
-1+\omega & 1+\omega & 1-\omega & -1-\omega & 1-\omega & -1-\omega & -1+\omega & 1+\omega\\
-1+\omega & 1-\omega & 1+\omega & -1-\omega & 1-\omega & -1+\omega & -1-\omega & 1+\omega\\
-3\omega & -2-\omega & -2-\omega & \omega & 3\omega & 2+\omega & 2+\omega & -\omega\\
-1+\omega & 1-\omega & 1-\omega & -1+\omega & 1+\omega & -1-\omega & -1-\omega & 1+\omega\\
-3\omega & -2-\omega & 3\omega & 2+\omega & -2-\omega & \omega & 2+\omega & -\omega\\
-3\omega & 3\omega & -2-\omega & 2+\omega & -2-\omega & 2+\omega & \omega & -\omega\\
3+6\omega & 3 & 3 & -1-2\omega & 3 & -1-2\omega & -1-2\omega & -1
\end{pmatrix}$$

と等しいので，

$$(0,1,1,1,1,1,1,1)\left(\begin{bmatrix}1+\omega & 1\\ 1-\omega & 1\end{bmatrix}^{-1}\right)^{\otimes 3} = \frac{1}{4}(0,1,1,0,1,0,0,1)$$

となる．したがって

$$(0,1,1,1,1,1,1,1) = \frac{1}{4}(0,1,1,0,1,0,0,1)\boldsymbol{\beta}^{\otimes 3}$$

となる．この方法では $(0,1,1,1,1,1,1,1)$ の各論理値 0 あるいは 1 は $\frac{1}{4}(0,1,1,0,1,0,0,1)$ における完全マッチング値の「重ね合せ」つまり「ホログラフィック混合」として表現される．

特定の問題を多項式時間で解けるようにするため，単一の基底変換のもとで（**R** と **G** に対する）**斉次**実現可能性（simultaneous realizability）が必要となる．Valiant [3]は体 $\mathbf{Z}_7$ 上のこの問題に対してそのような基底が存在することを示した．

このことは充足解の数を 7 で割った余りを多項式時間で求めるという驚くべきアルゴリズムがあることを意味している．

どのような和をホログラフィックアルゴリズムが多項式時間で計算できるのかということは正に**特徴値理論**の研究課題である．対称特徴値のクラスに対する妥当な理論は既に与えられている [4]．また一般の非対称特徴値に向けての進展もいくつかある．

またホログラフィック変換のアイディアは (1) マッチゲートではなく別の多項式時間計算可能な構成部品に基づくホログラフィック計算と，(2) 計算困難性を証明する困難性還元としてのホログラフィック還元手法，という少なくとも二つの方向に更に発展している [5]．

■参考文献

1) P.W. Kasteleyn, “Graph Theory and Crystal Physics,” in Graph Theory and Theoretical Physics, ed. by F. Harary, Academic Press, London, pp.43-110, 1967.
2) L.G. Valiant, “Holographic Algorithms,” SIAM J. Comput., vol.37, no.5, pp.1565-1594, 2008.
3) L.G. Valiant, “Accidental Algorithms,” in Proc. 47th Annual IEEE Symposium on Foundations of Computer Science, pp.509-517, 2006.
4) J.-Y. Cai and P. Lu, “Holographic Algorithms: From Art to Science,” The 39th Annual ACM Symposium on theTheory of Computing, pp.401-410, 2007.
5) J.-Y. Cai, P. Lu, and M. Xia, “Holographic Algorithms by Fibonacci Gates and Holographic Reductions for Hardness,” in Proc. 49th Annual IEEE Symposium on Foundations of Computer Science, pp.644-653, 2008.

■6 群 - 2 編 - 7 章

7-8 計数問題の計算複雑性

（執筆者：戸田誠之助）[2009 年 2 月 受領]

任意に与えられた入力データに対して，事前に決められた条件（以下，「解条件」）を満たす対象（以下，「解」）の個数を求めるような計算問題のことを「**計数問題**」（または，「**数え上げ問題**」）と呼ぶ．例えば，二部グラフが入力データとして与えられたとき，その完全マッチングの個数を求める問題などがその典型である．計算量理論では，計数問題に内在する計算構造を計算量クラス（あるいは，計算モデル）として定式化することを第一の課題とし，ほかの計算量クラスとの相互関係を明らかにすることを第二の課題としている．本節では，これら二つの課題に対する主要な結果を概説する．

上で述べたような計数問題は，入力データを表すビット列（符号語）x と解の候補を表すビット列 y に対して解条件を判定する述語 $A(x,y)$ と適当な多項式 $p(n)$ をもとに，

$$\#_p A(x) = |\{\, y \in \{0,1\}^{p(|x|)} \ :\ A(x,y)\,\}|$$

といったビット列の集合から自然数全体への関数 $\#_p A(x)$ として定式化される．ここで，多項式 $p(n)$ を導入するのは，多くの計数問題における「解」が入力長の多項式程度の長さに符号化し得るという事実を反映している．

述語（解条件）からなる任意の計算量クラス **D** が与えられたとき，**D** に属する任意の述語 $A(x,y)$ と任意の多項式 $p(n)$ をもとに定義される関数 $\#_p A(x)$ すべてからなるクラスを**#·D** で表す．これは前段落で述べたような計数問題からなる計算量クラスを（やや抽象的に）定義している．特に，**D** を **P**（決定性多項式時間）としたときの計算量クラスは**#P** で表され，離散的な多くの計数問題を含んでいることから，計数問題の計算複雑性を分析するための基本的な指標になっている[6]．

計算量理論では，更に，「解の個数」の部分情報を求めるための計算複雑性をも分析している．もっとも典型的には，「解の個数」の偶奇性を判定する問題と，ある（容易に計算される）値と一致するか否かを判定する問題が考察されている．これらの判定問題は**#·D** に属する関数 $\#_p A(x)$ を用いて，それぞれ，

$$\oplus_p A(x) \ \equiv\ \text{“}\#_p A(x) \text{ は奇数”} \qquad \mathrm{EQ}_p^f A(x) \ \equiv\ \text{“}\#_p A(x) = f(x)\text{”}$$

と定義される述語 $\oplus_p A(x)$ と $\mathrm{EQ}_p^f A(x)$ として定式化される．ここで，$f(x)$ は自然数を値とする多項式時間計算可能な任意の関数を表す．このような述語からなる計算量クラスを，それぞれ，$\oplus$**·D** 及び $\mathbf{C}_{=}$**·D** と表す．$\oplus$**·D** は計数問題の計算複雑性を分析するために重要な役割を果たし[3]，$\mathbf{C}_{=}$**·D** は量子計算と密接な関係をもつことが示されたりしている[2]．

計数問題の計算複雑性に関して，非自明な結果を初めて示したのは文献 7) である．その結果は，次の定理の応用として得られる．

定理 1[7] 任意の述語 $A(x,y) \in$**P** と多項式 $p(n)$ に対して，ある述語 $B(x,y,z) \in$ **P** と多項式 $q(n)$ が存在して，次が成り立つ．任意の $x \in \{0,1\}^*$ に対して：

$$\#_p A(x) > 0 \Longrightarrow \Pr\{\, w \in \{0,1\}^{q(|x|)} \ :\ \#_p B_w(x) = 1\,\} \approx 1 \qquad \text{かつ}$$

$$\#_p A(x) = 0 \Longrightarrow \Pr\{\, w \in \{0,1\}^{q(|x|)} \ :\ \#_p B_w(x) = 0\,\} = 1$$

ここで，$\#_p B_w(x)$ は，述語 $B(x,y,z)$ の第 3 引数 z を w に固定した述語 $B_w(x,y)$ をもとに定義された（数え上げの）関数を表す．□

この定理は，関数 $\#_p B_w(x)$ が w に関して高い確率で 1 以下の値を取ること（注：低い確率で 1 より大きな値を取ることがあり得る）と同時に，“$\#_p A(x) > 0$ か否か” の判定が “$\#_p B_w(x) = 1$ か否か” の判定に高い確率で多項式時間還元可能であることを示している．“$\#_p A(x) > 0$ か否か” を判定する問題すべてからなるクラスが **NP** の別定義になっていることに注意すると，この定理から次の結果が直ちに得られる．

系 2[7] **NP** に属する任意の判定問題は，$\oplus\cdot$**P**（や $\mathbf{C}_{=}\cdot$**P**）に属するある判定問題に高い確率で多項式時間還元可能である． □

これは，ある種の計数問題（例えば，文献 6) で示されている計数問題）に関して，その解の個数の偶奇性を判定することでさえ **NP**-完全問題と同等かそれ以上の計算複雑性を有することを述べている．

定理 1 は，更に，次のように強めるられる．以下，**PH** は多項式時間階層を表す．

定理 3[4] 任意の関数 $\#_p A(x) \in \#\cdot$**PH** に対して，ある述語 $B(x, y, z) \in$ **P** と多項式 $q(n)$ と多項式時間計算可能関数 $f(x)$ が存在して，次が成り立つ．任意の $x \in \{0,1\}^*$ に対して：

$$\Pr\{\, w \in \{0,1\}^{q(|x|)} \;:\; \#_p A(x) = \#_p B_w(x) - f(x) \,\} \approx 1 \qquad \square$$

この定理は，**PH** を解条件のクラスとする（数え上げの）関数が**#P**（正確には，**GapP**[1]）に属する関数に高い確率で多項式時間還元可能であることを示している．これより，系 2 を強めた次の結果が直ちに得られる．

系 4[3, 4] **PH** に属する任意の判定問題は，$\oplus\cdot$**P**（や $\mathbf{C}_{=}\cdot$**P**）に属するある判定問題に高い確率で多項式時間還元可能である． □

この結果に，modular application と呼ばれる $\oplus\cdot$**D** の特異な性質[3]を加味し，解の個数に含まれる全情報を利用することによって，確率的な還元可能性を決定性の還元可能性に置き換えることができる．

定理 5[5] **#·PH** に属する任意の関数は，**#P** に属するある関数に（決定性）多項式時間還元可能である． □

■参考文献

1) S. Fenner, L. Fortnow, and S. Kurtz, “Gap-definable counting classes,” J. Comput. System Sci., vol.48, no.1, pp.116-148, 1994.
2) J.S. Kuwabara, et. al., “$\mathrm{NQP_C}$ = co-$\mathrm{C_{=}P}$,” Information Processing Lett., pp.63-69, vol.7, no.2, 1999.
3) S. Toda, “PP is as hard as the polynomial-time hierarchy,” SIAM J. Comput., vol.20, no.5, pp.865-877, 1991.
4) S. Toda and M. Ogiwara, “Counting classes are at least as hard as the polynomial-time hierarchy,” SIAM J. Comput., vol.21, no.2, pp.316-328, 1992.
5) S. Toda and O. Watanabe, “Polynomial Time 1-Turing Reductions from #PH to #P,” Theoretical Comput. Sci., vol.100, no.1, pp.205-221, 1992.
6) L.G. Valiant, “The complexity of enumeration and reliability problems,” SIAM J. Comput., vol.8, no.3, pp.410-421, 1979.
7) L.G. Valiant and V.V. Vazirani, “NP is as easy as detecting unique solutions,” Theoretical Comput. Sci., vol.47, no.1, pp.85-93, 1986.

■6 群 - 2 編 - 7 章

7-9 自然な証明

（執筆者：天野一幸）［2009 年 1 月 受領］

理論計算機科学における最大の未解決問題である P 対 NP 問題に対する様々な挑戦のうち，有望であると考えられているものの一つが回路計算量を通じたアプローチである．本編 6 章 6-1 で見てきたように，適当な NP 問題に対して，その回路計算量が多項式を超えることが証明できれば，それは直ちに $P \neq NP$ を意味する．80 年代中盤に相次いで得られた，定数段数回路に対するパリティ関数の指数関数下界や，単調論理回路に対するクリーク関数の指数関数下界といった結果〔本編 6 章 6-1 参照〕は，このアプローチの有望さを信じさせるに十分であった．ところが，その後進展のスピードは緩まり，現在においても，上の二つの結果は回路計算量の下界に対する最も主要な結果であり続けている．回路のタイプに制約を設けない場合には，既知の最良の下界は線形でしかない．このようななか，我々が現在もつ証明手法が，P≠NP を証明するには弱すぎるのではないかとの疑念を抱くのは自然の流れといえよう．

現在，回路計算量に対する強い下界を証明することの困難さを最も良く説明していると考えられているのが，Razborov と Rudich によって 90 年代中盤に示された自然な証明（Natural Proof）の概念である[1)]．この業績により両者は，理論計算機科学分野の最高峰の賞の一つであるゲーデル賞を 2007 年に受賞した．本節では，この自然な証明の概念について説明する．

7-9-1 回路計算量の下界証明手法と自然な証明

自然な証明の概念を理解するには，回路計算量の下界の証明の一般的なスタイルを知っておく必要がある．ある論理関数 f が，ある計算量クラス Λ に属さないことの証明は，通常次の 3 ステップからなる: (i) 論理関数に対する，ある性質 C を導入する．(ii) 性質 C をもついかなる論理関数も，所望の計算量クラス Λ には属さないことを証明する．この条件を満たす性質 C は**クラス Λ に対して有用である**と呼ばれる．(iii) 下界を示したい論理関数 f が性質 C を確かに満たしていることを示す．

上で触れたパリティ関数に対する下界の証明を例にとり説明する．ここではターゲットとする計算量クラス Λ は，AND 素子，OR 素子，NOT 素子からなる多項式サイズの定数深さ回路で計算可能な論理関数のクラスとなる．また，性質 C_{AC} は「入力変数のうち，ある適当な個数（例えば $n^{0.1}$ 個）を残して，残りすべてに 0 または 1 を代入する．このとき，どのような代入に対しても，関数の値が定数 0 または 1 に定まらない」と定義される．パリティ関数がこの性質を満たすことは明らかである．有用性を示す二つ目のステップが通常最も難しいが，例えばこの例では，交代補題（Switching Lemma）と呼ばれる組合せ論的手法を巧妙に用いて証明される．一般に，下界の証明は，ターゲットとする計算量クラスに対して有用な，組合せ論的性質の発見が肝となる．

このように証明中で導入される性質が，以下の二つの条件を満たすとき，特にこれを**自然**な性質と呼ぶ．(a) 構成的：論理関数の真理値表（入力変数の個数を n とすると 2^n の長さをもつことに注意）を入力として与えられると，その関数が性質 C を満足するか否かを，真理値表の長さの多項式で表される時間内に判定できる．(b) 広い：n 変数論理関数全体 2^{2^n} 個に対する，性質 C を満足するものの割合が $2^{-O(n)}$ 以上である．例えば，上であげた性質 C_{AC} が，自然な性質であることを示すことは難しくない．

Razborov らは，パリティ関数に関する下界証明手法のみならず，それまでに提案された多くの下界の証明のほとんどすべてが，上の枠組みに従っている，すなわち，有用で，かつ，自然な性質に基づく議論によって行われていることを明らかにし，これを**自然な証明**と名付けた．そのうえで，（強くその存在が予想されている）擬似乱数生成器が存在するならば，回路計算量の超多項式下界を示し得る自然な証明は存在しないことを証明したのである．ここで，擬似乱数生成器とは，直感的には，真にランダムなビット列を入力とし，それより長く，かつ，十分ランダムに見えるビット列を出力するものである．より正確には，長さ n のビット列 x を入力とし，n の多項式時間で $2n$ ビットの列を出力する関数 G_n で，いかなるサイズ 2^{n^ϵ} 以下のサイズの論理回路 D に対しても $D(G_n(x)) = 1$ となる確率と，$D(y) = 1$ となる確率の差が $1/2^{n^\epsilon}$ 以下であることをいう．ここで，ϵ は 0 でない任意の正数を表し，x, y はそれぞれ真にランダムな n ビット，及び $2n$ ビットの列を表す．このような擬似乱数生成器は，現在の暗号システムなどの構成の核をなすものであり，また，例えば，素因数分解が難しいなどの広く信じられている仮定から，容易に構成することができる．

すなわち，彼らの結果は次の一文でまとめられる．

「素因数分解が困難であるとの予想を受け入れるならば，回路計算量に対して我々が現在知っている証明手法の大多数とその自然な拡張をすべてカバーする “自然な証明”によって，P ≠ NP を証明できる可能性は皆無である」

7-9-2 新たな証明手法の開発へ向けて

回路計算量に携わってきた研究者には，自然な証明の概念の発表によって，ある種の失望感に襲われたものも多かったと聞く．しかし，この結果を，新たに開発すべき手法への手がかりを与えるものと捉える向きもある．すなわち，素因数分解が困難であるとの予想を受け入れるならば，とるべき道は，(i) 非構成的な証明を用いる，(ii) ある程度狭い範囲の関数にのみ適用可能な証明を用いる，のどちらかである．

例えば，後者について最近，Chow[2]により，Razborov らの定義のうち広さに関する条件を若干狭める—$2^{-O(n)}$ から $2^{-Q(n)}$，$Q(n) = \exp\exp((\log\log n)^c)$（c はある適当な定数）へ変更する— だけで，自然な証明による障壁は解消されることが示され注目されている．このなかでは，擬似乱数生成器の存在の仮定のもと，（Chow の意味で）有用，かつ，自然な性質が，自然な証明の概念をいわば逆手にとった巧妙な証明により具体的に与えられている．選別器（Discriminator）と名づけられたこの性質を用いた超多項式下界の証明には，少なくとも，Razborov らの自然な証明の結果から来る障壁は全く存在しない．

しかし，もちろんこの結果も，具体的な証明手法の開発へとすぐにつながるほど強いものではない．当面の間は，このような，自然な証明の結果が示唆するところを考慮に入れつつ，新たな手法を模索する動きが続いていくことになりそうである．

■参考文献

1) A.A. Razborov and S. Rudich, “Natural Proofs,” J. Comput. Syst. Sci., vol.55, no.1, pp.24-35, 1997.
2) T.Y. Chow, “Almost-Natural Proofs,” Proc. of the 49th Symp. on Foundation of Computer Science (FOCS 2008), pp.86-91, 2008