数理解析研究所講究録
943巻 1996年 35-44

計算の複雑さの平均的な解析について

東京工業大学 情報理工学研究科 計算工学専攻
渡辺 治 (Osamu WATANABE)
watanabe@cs.titech.ac.jp

概要： 計算の複雑さの平均的な解析の理論についての解説．まず，基礎的な枠組を説明し，その後，この分野における重要な話題をいくつか紹介する．重要な未解決問題もあわせて示す．

1. 平均時計算量理論の枠組

与えられた問題（あるいは問題の族）の平均的な計算の難しさを議論するのが，「平均時計算量理論」である．その議論のために，通常の計算の複雑さの理論にはない概念，あるいは記法が少し必要になる．これらをまず準備しておこう．

(1) 入力分布と分布付き問題

簡単に言えば，アルゴリズムの“平均的”な計算時間が「平均時間計算量」で，“平均的に”速いアルゴリズムがあるか否かを議論するのが，「平均時間計算量理論」である．その“平均”とは，入力がある確率分布に従って与えられたときの平均である．したがって，平均時間計算量理論では，普通，問題だけでなく入力分布も決めておかなければ議論にならない（後で，問題だけを議論する方法も述べるが）．

以下では，簡単のため，問題とは $\{0,1\}^*$ 上の言語の認識問題とする．したがって，入力は $\{0,1\}^*$ の要素の文字列となるから，入力分布は $\{0,1\}^*$ 上の分布となる．正確には，次の条件を満たす関数族 $\{\mu_n\}_{n\geq 0}$ を入力分布と呼ぶことにする：

$$\forall n\,[\,\forall x \in \{0,1\}^n\,[\,\mu_n(x) \geq 0\,]\text{ and }\mu_n(\{0,1\}^n) = 1\,].$$
$$(\text{Where } \mu_n(\{0,1\}^n) = \textstyle\sum_{x\in\{0,1\}^n} \mu_n(x).)$$

ただし，以下では $\{\mu_n\}_{n\geq 0}$ を単に μ と略記し，$\mu(x)$ で，$\mu_n(x)$（ただし $n = |x|$）を表すことにする．（補足：Levin が「平均時間計算量理論」の枠組を考えた当初 [Lev86, Gur91] は，純粋に $\{0,1\}^*$ 上の分布（つまり $\mu(\{0,1\}^*) = 1$ となる確率分布 μ）を考えていた．その方が枠組が理論的にきれいにまとまるからだ．しかし，直観的には $\{0,1\}^*$ 上の分布というのは，直観的に理解しづらいので，最近では長さごとに入力分布を考える方式で考える人も多い [Imp95, SW95]．両者の違いはほとんどない [Gur91] ので，本稿では長さごとの入力分布で考えることにする．）

問題 L（ただし問題 L とは $L \subseteq \{0,1\}^*$ の認識問題のこと）と，入力分布 $\mu = \{\mu_n\}_{n\geq 0}$ との組 (L,μ) を分布付き問題 (distributional problem) という．平均時間計算量理論では，原則として，このような分布付き問題の“平均的な”計算の難しさを議論する．

(2) 計算時間の評価の仕方（多項式時間計算可能性）

ある分布付き問題 (L,μ) が与えられ，それに対するアルゴリズム A を考えたとしよう．このアルゴリズムの計算時間をどのように評価すればよいだろうか？まずは，天下り的に定義を述べると，アルゴリズム A の計算時間 time_A が次の式 (AVP) を満たすとき，A は平均的に多項式時間といい，そのようなアルゴリズムが作れる分布付き問題を平均的に多項式時間計算可能という．

$$\text{(AVP)} \qquad \exists c,d>0\ \forall n\geq 0\left[\sum_{x\in\{0,1\}^n}\frac{\mathrm{time}_A(x)^{1/d}}{n}\mu_n(x)\ \leq\ c\right].$$

なお，この定義は time_A に限らなくても，一般に $\{0,1\}^*$ 上で定義される関数 f に対しても使える．つまり，time_A を f に換えて (AVP) が成り立つとき，f は μ-平均で多項式という．

さて，どうして (AVP) のような条件が出てきたのだろう？直観的には次の (AVP′) の方が自然なような気がする．

$$\text{(AVP}')\qquad \exists c,d>0\ \forall n\geq 0\left[\sum_{x\in\{0,1\}^n}\mathrm{time}_A(x)\mu_n(x)\ \leq\ cn^d\right].$$

実は (AVP′) は不安定な条件なのである．というのも，たとえ time_A が (AVP′) を満たしていても，$(\mathrm{time}_A)^2$ が (AVP′) を満たすとは限らないからだ [Gur91]．平均で多項式時間のアルゴリズムだったのが，たとえば，インプリメントされる機械の都合で 2 乗の遅さになったとしよう．その場合でも，直観的には「平均で多項式時間」であって欲しいのだが，(AVP′) の基準では，多項式時間でなくなる場合も出てきてしまうのである．(ところで，(AVP) $\Longrightarrow$ (AVP′) はつねに成り立つが，逆は一般には成り立たない．つまり (AVP) は (AVP′) より強い条件といえる．)

条件 (AVP) にはまた，直観的な特徴付けもある．Schapire [Sch90] は，(AVP) が次の条件と同値であることを指摘した：

$$\exists p:\text{ polynomial},\ \forall n\geq 0, m\geq 1\ [\ \mu(\{x:\mathrm{time}_A(x)\geq p(n,m)\})\ <\ 1/m\ ].$$

つまり，問題のサイズ n の他にパラメータ m を導入して計算時間を評価し，任意の m に対して，計算時間が $p(n,m)$ 以上になる確率が $1/m$ 以下のとき，「平均的に p 時間」とみなすのである．パラメータが n,m と 2 つになる点が気になるが，なかなか自然な考え方だと思う．また，多項式時間以外の平均時間の評価にも応用できる．実際，Karg と Schuler [SY95] は，この考え方を用いて，「平均的に線形時間」や「平均的に指数関数時間」などの概念を定義し，階層定理を証明している．

(3) 妥当な分布のクラス：P-comp, P-samp

入力分布として，どのような分布関数が妥当だろうか？もちろん，最悪時でも多項式時間に解ける問題は，どんな分布関数と組んでも（平均的に）多項式時間に解ける．また，その逆に，どんな分布関数と組んでも平均的に多項式時間に解けるのならば，実は，最悪時でも多項式時間に解けることが知られている（これに関しては，たとえば [LV92] 参照）．つまり，すべての分布関数を考えると，最悪時の議論と変わらなくなってしまうのである．そこで分布関数の種類を少し制限しよう．

まず話しを簡単にするために，分布関数 μ に対し，次のような条件を追加しておこう：

$$\exists p : \text{polynomial},\ \forall x \in \{0,1\}^* \ [\ \mu(x) \text{ は 2 進小数 } p(|x|) \text{ 桁で表せる }]$$

多項式時間計算可能性を議論する限りには，この条件を仮定しても一般性は失われないので，以下では分布関数 μ は，すべてこの条件を満たすものと仮定する．

Levin [Lev86] は，妥当な分布関数の条件として多項式時間計算可能性を考えた（Levin 自身が本当に“妥当”と思っていたかどうかは疑問）．これは次の条件である．

$$\exists A : \text{poly-time algorithm},\ \forall n \geq 0,\ \forall x \in \{0,1\}^n \ [\ \widehat{\mu}(x) \ = \ A(n,x)\ ].$$

ただし，$\widehat{\mu}$ はいわゆる分布関数．すなわち，集合 $P(x) = \{x' \in \{0,1\}^n : x' \text{ は辞書式順序で } x \text{ より小さい文字列}\}$ を用いて，$\widehat{\mu}(x) = \sum_{x' \in P(x)} \mu(x')$ と定義される関数である．確率密度関数ではなく，分布関数の方が多項式時間で計算可能であるような分布関数を妥当と考えたのだ．このような分布関数のクラスを P-comp と定義する．

多項式時間計算可能性はやや人工的な感じがする．それに対し，Ben-David らが導入した「多項式時間生成可能性」という条件はかなり自然である．次の条件を満たす分布関数 μ を多項式時間生成可能性という．

$$\exists G : \text{random poly-time algorithm},\ \forall n \geq 0,\ \forall x \in \{0,1\}^n$$
$$[\ \Pr_G\{\, G(n) = x \,\} \ = \ \mu(x)\ ].$$

つまり，その分布関数 μ の示す確率で，入力例を生成することが（多項式時間で）できる場合，μ を妥当な分布関数と考えようというのである．多項式時間生成可能性な入力分布関数のクラスを P-samp という．

多項式時間生成可能性を妥当な入力分布の条件としようという考え方は，かなり自然だと思う．アルゴリズムのデータとして与えられる入力例は，外界で発生するものか，あるいは他のアルゴリズムの出力として得られるもののいずれかと考えてよい．それらの入力例はどのような分布に従っているだろうか？まず，外界で発生するものに対してだが，物理学や経済学などで用いられている様々な分布は，どれも計算可能性という面で考えると単純で，多

項式時間生成可能と仮定しても構わない．一方，アルゴリズムの出力として得られる入力の分布は，もしそのアルゴリズムが“まともな計算時間”（多項式時間）だったら，まさに多項式時間生成可能になっている．そう考えると，入力分布が多項式時間生成可能と仮定してもよいように思う．

さてここまでは，分布付き問題の難しさを議論する枠組を考えてきた．しかし，問題そのものの平均的な難しさを議論する方法もある．もし，与えられた問題が，すべての妥当な入力分布に対して，平均的に多項式時間計算可能な場合，その問題自身を「平均的に多項式時間計算可能」と考えてもよいだろう．Schuler と Yamakami [SY92] は，

$$\begin{aligned} \mathrm{P}_{\text{P-comp}} &= \{L : \forall \mu \in \text{P-comp}\,[(L,\mu) \text{ is average poly-time computable}]\}, \\ \mathrm{P}_{\text{P-samp}} &= \{L : \forall \mu \in \text{P-samp}\,[(L,\mu) \text{ is average poly-time computable}]\} \end{aligned}$$

というクラスを定義した．つまり，$\mathrm{P}_{\text{P-comp}}$ は，すべての P-comp 分布に対し，$\mathrm{P}_{\text{P-samp}}$ は，すべての P-samp 分布に対し，それぞれ平均的に多項式時間計算可能な問題のクラスである．なお，この定義では，(L,μ) を解くアルゴリズムは，各 μ に依存して決めてよい．つまり，入力分布を知った上でアルゴリズムを設計してもよい，という考え方である．

ところで，クラス P-comp と P-samp の関係としては，次の事実が知られている [BCGL92].

定理 1.1.

(1) P-comp $\subseteq$ P-samp.

(2) P-samp $\subseteq$ P-comp unless no average-case one-way function exists.

補注. 平均時一方向関数（averag-case one-way function）については次節を参照.

したがって，$\mathrm{P}_{\text{P-samp}} \subseteq \mathrm{P}_{\text{P-comp}}$ が成り立つ（包含関係が逆転していることに注意！より広い入力分布のクラスを考えた方が，多項式時間計算可能となるチャンスが減るからである）.

まとめ

今までのまとめとして，主要な計算量クラスを定義（再定義）しておこう.

定義 1.2.

$$\begin{aligned} \text{AveP} &= \{(L,\mu) : (L,\mu) \text{ is average poly-time computable}\}, \\ \text{P-comp} &= \{\mu : \hat{\mu} \text{ が多項式時間計算可能}\}, \\ \text{P-samp} &= \{\mu : \mu \text{ が多項式時間計算生成可能}\}, \\ \mathrm{P}_{\text{P-comp}} &= \{L : \forall \mu \in \text{P-comp}\,[(L,\mu) \in \text{AveP}]\}, \text{ and} \\ \mathrm{P}_{\text{P-samp}} &= \{L : \forall \mu \in \text{P-samp}\,[(L,\mu) \in \text{AveP}]\}. \end{aligned}$$

2. 平均時計算量理論における主要な話題

前節で枠組を大まかに説明した．ここでは，平均時計算量理論において今までに研究されてきた主要な話題，ならびに関連する未解決問題について述べる．

2.1. NP 問題の多項式時間計算可能性と平均時 NP-完全性

この分野で最も重要なテーマは，やはり，「NP 問題が（すべて）多項式時間計算可能か？」という問題だろう．実は，かなりの NP-完全問題が，ある種の分布の元で平均的に多項式時間に解けることが報告されている（これに関してはここでは省略するが，興味のある方は文献 [Jo84] などを参照するとよいだろう）．しかしだからといって，すべての NP 問題が，すべての妥当な分布の元で（平均的に）多項式時間計算可能かどうかはわからない．むしろ P $\neq$ NP 予想と同様，かなり否定的な考え方が強い．つまり，次のような本質的な問題は未解決である．

Question 1: Prove (or disprove!?) NP $\not\subseteq \mathrm{P}_{\text{P-comp}}$. Similarly, prove NP $\not\subseteq \mathrm{P}_{\text{P-samp}}$.

しかし，“すべての妥当な分布”というのは，どうも考えづらい．最悪時計算量理論では，「NP-完全性」という考え方があり，「この NP 問題さえ解ければ P = NP になってしまう」という問題が定義できた．実は，平均時計算量理論でも，同じようなことがいえる．Levin [Lev86] は，「平均時 NP-完全性」なるものを定義し，最も難しい分布付き NP-問題を示したのである．

まずは基本的な概念や用語などの準備から始めよう．まず分布付き問題の難しさを比較するための手法として，平均時多項式時間還元（$\propto^{\mathrm{P}}_{\mathrm{m}}$-還元）を定義する．これは従来の多項式時間還元（正確には $\leq^{\mathrm{P}}_{\mathrm{m}}$-還元）と同様，1 つ問題のもう 1 つの問題に変換する関数である．ただし，入力分布を考慮に入れる点が大きく違う．

定義 2.1. 関数 h が，分布付き問題 (L_1, μ_1) から (L_2, μ_2) への還元であるための条件は，簡単にいうと以下のようになる（条件 (b) については，たとえば [Gur91] を参照）：

(a) h は L_1 から L_2 への $\leq^{\mathrm{P}}_{\mathrm{m}}$-還元であり，しかも

(b) 入力例 x が h によって y へ変換されたとき，$\mu_2(y)$ が $\mu_1(x)$ に対してそう小さくならない．

これらの条件の重要な点は，次の性質が成り立つことである．

命題 2.2. $(L_1, \mu_1) \propto^{\mathrm{P}}_{\mathrm{m}} (L_2, \mu_2) \wedge (L_2, \mu_2) \in \mathrm{AveP} \Longrightarrow (L_1, \mu_1) \in \mathrm{AveP}$.

この還元を用いて，平均時 NP 完全性 (distributional NP-completeness) は次のように定義できる．

定義 2.3. A distributional problem (L,μ) is *distributional NP-complete* if (a) L is in NP, and (b) for every $L' \in$ NP and $\mu' \in$ P-comp, we have $(L',\mu') \propto_{\mathrm{m}}^{\mathrm{P}} (L,\mu)$.

では，どのような分布付き問題が NP 完全になるだろうか？次のような一様分布のもとでの非決定機械の停止性問題 (K,μ_K) が，その代表例である．

$$K = \{\langle i,x,0^t\rangle_{i,n,t} : M_i \text{ accepts } x \in \{0,1\}^n \text{ within } t \text{ steps}\} \text{ and}$$
$$\mu_K(\langle i,x,0^t\rangle_{i,n,t}) = 2^{-n}.$$

ただし $\langle i,x,0^t\rangle_{i,n,t}$ は，i, x, 0^t の組を表しているが，同じ i,n,t に対してつねに同じ長さの文字列になるように工夫したもの（分布関数を長さごとに決めているので，このような制限が必要になってしまう）．

その他の NP-完全問題の例だが，[Gur91, BW92, Wa95] に紹介されている程度でその数は少ない．すべての NP-完全問題は，何らかの分布（しかも P-comp に入る分布）で平均時 NP-完全になることは簡単に示せる（Cook や Karp の証明で出てくる入力例だけに重みを与える分布を考えればよい）．しかし，上の μ_K のようなしごく単純な分布に対して，平均時 NP-完全性を示せた問題は少ない．そこで次のような未解決問題があげられる．

Question 2: Show an example of distributional NP-complete problems for some "simple" distributions. Or prove that, e.g., SAT cannot be distributional NP-complete with "simple" distributions unless some strange thing would happen.

2.2. P-comp 分布 vs. P-samp 分布

平均時 NP-完全性の議論は，そもそも P-comp 分布に対して行なわれている．したがって，たとえば (K,μ_K) が多項式時間計算可能ならば，すべての NP 問題 L，すべての $\mu \in$ P-comp に対して，(L,μ) が多項式時間計算可能となる（つまり NP $\subseteq \mathrm{P}_{\text{P-comp}}$ となる）．しかし，もしかすると，ある NP 問題 L は，ある分布 $\mu \in$ P-samp に対して，多項式時間に計算できないかもしれない．つまり，NP $\subseteq \mathrm{P}_{\text{P-comp}}$ でも，NP $\subseteq \mathrm{P}_{\text{P-samp}}$ とはならないかもしれない（$\mathrm{P}_{\text{P-samp}} \subseteq \mathrm{P}_{\text{P-comp}}$ であったことを思い出して欲しい）．

一方，妥当な入力分布のクラスとしては P-samp の方が自然だ．しかし，P-samp 分布に対しての平均時 NP-完全性の証明は難しい．たとえば (K,μ_K) が，P-samp 分布も含めてすべての分布付き NP 問題に対して，平均時 NP-完全かどうかはわかっていない．しかし，このギャップを埋める次のような定理が，Impagliazzo と Levin により示された [IL90].

定理 2.4. NP $\subseteq \mathrm{P}_{\text{P-comp}} \Longrightarrow$ NP $\subseteq \mathrm{P}_{\text{P-samp}}$.

ただ依然として，次のような疑問は残っている（多少マニア的問題ではあるが）：

Question 3: Prove (or disprove under some reasonable assumption) that (K, μ_K) is distributional NP-complete w.r.t. P-samplable distributions.

2.3. 暗号論的一方向関数との関係

計算量的暗号理論で議論されている一方向関数は，平均時一方向関数 (average-case one-way funciton) などと呼ばれ，平均時 P vs. NP 問題と関係が深い．

簡単にいうと，関数 f が平均時一方向関数であるとは，f 自身は多項式時間で計算可能であるのに，f^{-1} は（平均的に見ても）多項式時間計算不可能な場合をいう（詳しい定義については [Wat94] を参照）．ここで多項式時間計算可能関数 f に対し，その逆元（の 1 つ）を求める問題を INV_f としよう．これも立派な NP 問題である．さて，f が一方向であるということは，この INV_f が $f(\mu_{\mathrm{unif}})$ の確率分布の元で，平均時多項式時間計算可能とならないことと同値である．ところが，$f(\mu_{\mathrm{unif}})$ は，P-samp 分布の一種なので，先ほどの定理 2.4 から，次の関係が示せる．

定理 2.5.

$$\exists \text{ one-way function} \iff \exists f\ [\ (\mathrm{INV}_f, f(\mu_{\mathrm{unif}})) \notin \mathrm{AveP}\ ] \implies \mathrm{NP} \not\subseteq \mathrm{P}_{\text{P-samp}}$$
$$\implies \mathrm{NP} \not\subseteq \mathrm{P}_{\text{P-comp}}.$$

しかし，その逆は重要な未解決問題として残されている．

Question 4: Prove (or disprove under some reasonable assumption) that $\mathrm{NP} \not\subseteq \mathrm{P}_{\text{P-samp}} \implies$ some one-way function exists.

暗号論的一方向関数については，いろいろな研究がされており，そこでのテクニックが平均時計算量の解析にも使える場合が多い．たとえば，ハードコア述語の構成法 [Wat94] を用いると，$\mathrm{NP} \not\subseteq \mathrm{P}_{\text{P-comp}}$ の仮定から，どんな多項式時間アルゴリズムも当てずっぽ以上の推定はできないような，大変判定の難しい問題を構成することができる（その応用例が [BFNW93] にある）．

2.4. 最適化問題に対する平均時計算量の解析

もし仮に決定問題が平均時多項式時間判定可能だったとして，関連する解の探索問題や，最適化問題も平均時多項式時間で解けるだろうか？最も一般的な形では，$\mathrm{NP} \subseteq \mathrm{P}_{\text{P-comp}}$ だったとして，それから $\mathrm{SearchP} \subseteq \mathrm{P}_{\text{P-comp}}$ や，$\mathrm{OptP} \subseteq \mathrm{P}_{\text{P-comp}}$ が言えるだろうか？(ただし SearchP, OptP は，それぞれ NP 型探索，NP 型最適化問題のクラス [SW95]) 探索問題や近似問題に対しては，次のような肯定的結果が得られている．

定理 2.6.

(1) [BCGL92] $\mathrm{NP} \subseteq \mathrm{P}_{\text{P-comp}} \Longrightarrow \mathrm{SearchP} \subseteq \mathrm{P}_{\text{P-comp}}$.

(2) [SW95] $\mathrm{NP} \subseteq \mathrm{P}_{\text{P-comp}} \Longrightarrow \mathrm{OptP} \subseteq \mathrm{PTAS}_{\text{P-comp}}$ (i.e., every NP optimization problem has a μ-average-polynomial-time approximation scheme for every P-computable distribution μ).

それに対し，NP 型最適化問題自体の難しさとの関連は，まだよくわかっていない．現在の状況では，次の結果が最善である [SW95].

定理 2.7.

(1) $\mathrm{NP} \subseteq \mathrm{P}_{\mathrm{P}^{\mathrm{NP}}\text{-samp}} \Longrightarrow \mathrm{OptP} \subseteq \mathrm{P}_{\text{P-comp}}$.

(2) $\mathrm{NP} \subseteq \mathrm{P}_{\text{P-comp}} \Longrightarrow \mathrm{NP} \subseteq \mathrm{P}_{\mathrm{P}^{\mathrm{NP}}_{\mathrm{tt}}\text{-samp}}$.

補注. $\mathrm{P}^{\mathrm{NP}}_{\mathrm{tt}}$-samp, P^{NP}-samp は P-samp を拡張したクラス．

Question 5: For which type of NP problems L and distribution μ, can we show that $(L, \mu) \in \mathrm{AveP} \Longrightarrow (\text{Search-}L, \mu) \in \mathrm{AveP}$?

Question 6: $\mathrm{P}^{\mathrm{NP}}_{\mathrm{tt}}$-samp $= \mathrm{P}^{\mathrm{NP}}$-samp ? Or more specifically, $\mathrm{P}_{\mathrm{P}^{\mathrm{NP}}_{\mathrm{tt}}\text{-samp}} = \mathrm{P}_{\mathrm{P}^{\mathrm{NP}}\text{-samp}}$? Or even more specifically, $\mathrm{NP} \subseteq \mathrm{P}_{\mathrm{P}^{\mathrm{NP}}_{\mathrm{tt}}\text{-samp}} \Longrightarrow \mathrm{NP} \subseteq \mathrm{P}_{\mathrm{P}^{\mathrm{NP}}\text{-samp}}$?

2.5. 平均時 vs. 最悪時

平均時と最悪時の解析の関係というのも興味深い．これについては，次のような結果が知られている．

定理 2.8.

(1) [Gur91] $\mathrm{NP} \subseteq \mathrm{P}_{\text{P-comp}} \Longrightarrow \mathrm{DEXT} = \mathrm{NEXT}$.

(2) [SY92] $\mathrm{NP} \subseteq \mathrm{P}_{\text{E-comp}} \Longrightarrow \mathrm{P} = \mathrm{NP}$.

補注. E-comp は指数関数 (2^{lin}) 時間で計算可能な分布のクラス．

Question 7: Can we show much closer relation, e.g., $\mathrm{NP} \subseteq \mathrm{P}_{\text{P-comp}} \Longrightarrow$ PH collapses ?

2.6. NP 探索問題に対するテスト例題生成手法

ある NP 問題に対して，平均時でうまく動きそうなアルゴリズムを考えたとしよう．そのアルゴリズムをどのようにテストすればよいのだろうか？そのための，テスト例題生成手法の研究も重要である．これについては [Wat94] を参照されたい．

Question 8: Does (Search-SAT, μ_{unif}) have a good test instance generator?

Question 9: For some typical distributional NP problem (with a distribution in P-comp), desigin a good test instance generator.

Question 10: Let μ_{naive} be a distribution given by a certain *naive* test instance generator. Prove (or disprove under some reasonable assumption) that (Search-SAT, μ_{naive}) is not in AveP.

参考文献

[BFNW93] L. Babai, L. Fortnow, N. Nisan, and A. Wigderson, BPP has subexponential time simulations unless EXPTIME has publishable proofs, *Computational Complexity* 3 (1993), 307–318.

[BW92] J. Belanger and J. Wang, Isomorphisms of NP complete problems on random instances, in *Proc. Structures '93* (1993), 65–73.

[BCGL92] S. Ben-David, B. Chor, O. Goldreich, and M. Luby, On the theory of average case complexity, *J. Comput. Syst. Sci.* 44 (1992), 193–219.

[Gur91] Y. Gurevich, Average case completeness, *J. Comput. Syst. Sci.* 42 (1991), 346–398.

[Imp95] R. Impagliazzo, A personal view of average-case complexity, in *Proc. Structures '95* (1995), 134–147.

[IL90] R. Impagliazzo and L. Levin, No better ways to generate hard NP instances than picking uniformly at random, in *Proc. 31st IEEE Sympos. on Foundations of Computer Science* (1990), 812–821.

[Jo84] D.S. Johnson, The NP-Completeness Column: An Ongoing Guide, *J. Algorithms* 5 (1984), 284–299.

[Lev86] L. Levin, Average case complete problems, *SIAM J. Comput.* 15 (1986), 285–286.

[LV92] M. Li and P. Vit'anyi, Worst case complexity is equal to average case complexity under the universal distribution, *Inform. Process. Lett.* 42 (1992), 145–149.

[Sch90] R. Schapire, The emerging theory of average-case complexity, Technical Report MIT/LCS/TM-431, MIT (1990).

[SY95] C. Karg and R. Schuler, Structure in average case complexity, in *Proc. 1st CO-COON*, Lecture Notes in Computer Science ? (1995), ?–?.

[SY92] R. Schuler and T. Yamakami, Structural average case complexity, in *Proc. 12th Foundations of Software Technology and Theoretical Computer Science*, Lecture Notes in Computer Science 652 (1992), 128–139.

[SW95] R. Schuler and O. Watanabe, Towards average-case analysis of NP-optimization problems, in *Proc. Structures '95* (1995), 148–159.

[Wa95] J. Wang, Average-case completeness of a word problem for groups, in *Proc. STOC '95* (1995), to appear.

[Wat94] O. Watanabe, Test instance generation for promised NP search problems, in *Proc. Structures '94*, IEEE, New York, 205–216 (1994).

[Wat94] 渡辺 治, 一方向関数の基礎理論, "離散構造とアルゴリズム III（室田一雄 編）", 近代科学社 (1994), 77–114.