数理解析研究所講究録
第1148巻 2000年 140-145

平均時計算量における 2-tt 還元と many-one 還元の違いについて

名古屋大学 人間情報学研究科　築地 立家 (Tatsuie TSUKIJI)
名古屋大学 人間情報学研究科　相田 慎　(Shin AIDA)

概 要

計算量クラスにおける効率的な還元の概念の代表として，Cook の提唱した Turing 還元 ($\leq^{\mathrm{p}}_{\mathrm{T}}$) と Karp および Levin の提唱した many-one 還元 ($\leq^{\mathrm{p}}_{\mathrm{m}}$) がある．両者の違いについては，例えば，**E** や **NE** の中で $\leq^{\mathrm{p}}_{\mathrm{2d}}$-完全だが $\leq^{\mathrm{p}}_{\mathrm{m}}$-完全ではない言語の構成方法が知られている．また，Ladner, Lynch, Selman は「$\mathbf{P} \neq \mathbf{NP} \iff \leq^{\mathrm{p}}_{\mathrm{m}}$ は $\leq^{\mathrm{p}}_{\mathrm{T}}$ より真に強い還元である」ことを予想した (未解決.) 本稿では，この予想に動機を得て，平均時間計算量における次の命題を証明する ($\leq^{\mathrm{p}}_{\mathrm{m}}, \leq^{\mathrm{p}}_{\mathrm{2d}}$ の定義は Levin に従う.)

$\mathbf{P} \neq \mathbf{NP} \iff$ ある **NP** 言語 A と多項式時間計算可能な分布 μ, ν が存在して，$(A,\mu) \leq^{\mathrm{p}}_{\mathrm{2d}} (A,\nu)$ かつ $(A,\mu) \not\leq_{\mathrm{m}} (A,\nu)$ となる．

1 Introduction

計算量クラスにおける効率的な還元の概念の代表として Cook [Coo71] の導入した Turing 還元 ($\leq^{\mathrm{p}}_{\mathrm{T}}$) と Karp [Kar72] および Levin [Lev73] の提唱した many-one 還元 ($\leq^{\mathrm{p}}_{\mathrm{m}}$) がある．問題 $A, B \subseteq \Sigma^*$ ($\Sigma = \{0,1\}$) について，A が B に Turing 還元可能である ($A \leq^{\mathrm{p}}_{\mathrm{T}} B$) とは，$A$ がオラクル付き多項式時間計算機 $M(B)$ により認識可能なこと ($A = M(B)$) をさす．より強く，質問回数を定数回に限定した還元を で，また 2 回の連言形式に限定した還元を $\leq^{\mathrm{p}}_{\mathrm{2d}}$ で表す．さらに強く，A が B に many-one 還元可能 ($A \leq^{\mathrm{p}}_{\mathrm{m}} B$) であるとは $I \in A$ ($I \in \Sigma^*$) の判定が多項式時間計算可能関数 $f : \Sigma^* \to \Sigma^*$ を介して $f(I) \in B$ の判定と同値になること ($I \in A \iff f(I) \in B$) である．

比較的小さな計算量クラスの中で $\leq^{\mathrm{p}}_{\mathrm{T}}$ (あるいは　や $\leq^{\mathrm{p}}_{\mathrm{2d}}$) と $\leq^{\mathrm{p}}_{\mathrm{m}}$ の違いを示唆する多くの研究結果がある ([LLS75, Sel79, KM81, Wat87, LY90, WT92, LM96]). 創始的な仕事として，Ladner, Lynch, Selman [LLS75] らは，2^n 時間で計算できる問題 A について $\overline{A} \leq^{\mathrm{p}}_{\mathrm{m}} A$ を証明した．これは，**E** において $\leq^{\mathrm{p}}_{\mathrm{m}}$ が $\leq^{\mathrm{p}}_{\mathrm{T}}$ より真に強いことを意味する．さらに，Selman [Sel79] は $\mathbf{E} \neq \mathbf{NE}$ ならば $\mathbf{NP} \cup \mathbf{coNP}$ の中で $\leq^{\mathrm{p}}_{\mathrm{m}}$ が $\leq^{\mathrm{p}}_{\mathrm{T}}$ より真に強いことを示した．Ko, Moor [KM81] は **E** の中で -完全だが $\leq^{\mathrm{p}}_{\mathrm{m}}$-完全ではない言語を構成し，Watanabe [Wat87] と Buhurman, Homer, Torenvliet [BHT90] は E や NE の中で $\leq^{\mathrm{p}}_{\mathrm{2d}}$-完全だが $\leq^{\mathrm{p}}_{\mathrm{m}}$-完全 ではない言語を構成した．さらに，Watanabe, Tang [WT92] は **PSPACE** の中で $\leq^{\mathrm{BPP}}_{\mathrm{T}}$-完全と $\leq^{\mathrm{p}}_{\mathrm{m}}$-完全が異なれば $\leq^{\mathrm{p}}_{\mathrm{T}}$-完全と $\leq^{\mathrm{p}}_{\mathrm{m}}$-完全も異なることを示した．Longpré, Young [LY90] は任意の多項式 p について，ある **NP**-完全言語 A, B を構成し，$A \leq^{\mathrm{p}}_{\mathrm{2d}} B$ は $O(n)$ 時間でできるが $A \leq^{\mathrm{p}}_{\mathrm{m}} B$ は $\Omega(p(n))$ 時間以上かかってしまうことを証明した．Lutz, Mayordomo [LM96] は **NP** が p-measure 0 でなければ $\leq^{\mathrm{p}}_{\mathrm{T}}$-完全だが $\leq^{\mathrm{p}}_{\mathrm{m}}$-完全でない **NP** 言語が存在することを証明した．

これらの研究の動機付けのひとつに，Ladner, Lynch, Selman [LLS75] の次の予想 (未解決) がある．

予想 1 ([LLS75]) $\mathbf{P} \neq \mathbf{NP}$ ならば，$A \leq^{\mathrm{p}}_{\mathrm{T}} B$ かつ $A \not\leq^{\mathrm{p}}_{\mathrm{m}} B$ であるような $A, B \in \mathbf{NP}$ が存在する．

小文では，平均時間計算量のクラス Dist(**NP**, **P**-comp) における many-one 還元 $\leq^{\mathrm{p}}_{\mathrm{m}}$ と強い Turing 還元 $\leq^{\mathrm{p}}_{\mathrm{2d}}$ の違いについて考察する．Levin [Lev86] は 平均時間計算量理論を構築するにあたり many-one 還元の概念を次のように導入し，それについての Dist(**NP**, **P**-comp) 完全言語の存在を示した．

定義 1 (Levin[Lev86]) 分布付き問題 (A,μ) と (B,ν) について，(A,μ) が (B,ν) に many-one 還元可能である [Lev86] とは，多項式時間計算可能関数 f と semi-distribution η と多項式 p が存在して，次の条件を満たす時をいい，$(A,\mu) \leq^{\mathrm{p}}_{\mathrm{m}} (B,\nu)$ とかく．

1. 各 x について $x \in A \iff f(x) \in B$ である．

2. 各 y について $\eta(f^{-1}(y)) \leq \nu(y)$ である.
3. 各 x について $\mu(x) \leq p(|x|) \cdot \eta(x)$ である.

分布付き問題間の $\leq^{\mathrm{p}}_{2\mathrm{d}}$ 還元も同様に定義される.

定義 2 (A,μ) が (B,ν) に $\leq^{\mathrm{p}}_{2\mathrm{d}}$ 還元可能であるとは, 多項式時間計算可能な 3 項述語 R, 多項式時間計算可能な関数 f_1, f_2, semi-distributions η_1, η_2 と多項式 p_1, p_2 が存在して, 次の条件を満たす時をいい, $(A,\mu) \leq^{\mathrm{p}}_{2\mathrm{d}} (B,\nu)$ で表す.

1. 各 x について $A(x) = R(x, f_1(x), f_2(x))$ である.
2. 各 x, i について $x \in A \iff f_i(x) \in B$ である.
3. 各 y, i について $\eta_i(f_i^{-1}(y)) \leq \nu(y)$ である.
4. 各 x, i について $\mu(x) \leq p_i(|x|) \cdot \eta_i(x)$ である.

本稿では, Dist($\mathbf{NP}$, $\mathbf{P}$-comp) における $\leq^{\mathrm{p}}_{2\mathrm{d}}$ と $\leq^{\mathrm{p}}_{\mathrm{m}}$ の違いを次の形で証明する.

定理 1 $\mathbf{P} \neq \mathbf{NP}$ ならば, ある $A \in \mathbf{NP}$ と多項式時間計算可能な分布 μ, ν が存在して, $(A,\mu) \leq^{\mathrm{p}}_{2\mathrm{d}} (A,\nu)$ かつ $(A,\mu) \not\leq_{\mathrm{m}} (A,\nu)$ となる.

2 準備

文字集合を $\Sigma = \{0,1\}$ とし, 空列を除く長さ有限の文字列の集合を Σ^* とする. Σ^* 上の辞書式順序を σ で表記する ($\sigma(0) = 0, \sigma(1) = 1, \sigma(00) = 2, \sigma(01) = 3, \cdots$.) また, 長さ n の文字列全体の集合 Σ^n 上の辞書式順序を σ_n で表記する ($\sigma(0^n) = 0, \sigma(0^{n-1}1) = 1, \sigma(0^{n-2}10) = 2, \sigma(0^{n-2}11) = 3, \cdots, \sigma(1^n) = 2^{n+1} - 1$.)

平均時間計算量では, 言語と分布 (distribution) の組 (A,μ) を分布付き問題 (distributional problem) と呼び, その計算複雑さを μ のもとで A を認識するのに必要かつ十分な "平均時間" 計算量と定める. 還元の概念もこの平均複雑さを保証する様に導入される. ここでの分布 μ とは Σ^* から実区間 $[0,1]$ への単調増加関数で $\mu(\Sigma^*) = \lim_{\sigma(x)\to\infty} \mu(x) = 1$ を満たすものである ($\mu(\Sigma^*) \leq 1$ のときは semi-distribution とよばれる.) 分布 μ の密度 μ' は $\mu'(0) = \mu(0)$, $\mu'(x) = \mu(x) - \mu(x-1)$ ($x > 0$ のとき) と定義される.

Levin は多項式時間計算可能な分布のクラス ($\mathbf{P}$-samp) を次のように導入した.

定義 3 (Levin [Lev86]) μ が $\mathbf{P}$-sampであるとは, る多項式時間 DTM M が存在して各 x, i について $\left|\mu(x) - M(x, 1^i)\right| \leq 2^{-i}$ となることである.

言語 A が最悪時計算量で困難ならば, 健全な分布 μ 付きの問題 (A,μ) も困難であるべきである. Cai, Selman [CS99] らはの次の定義がこの要請を満足することを示した.

定義 4 ([CS99]) 分布 μ が健全であるとは, ある定数 $s > 0$ が存在して, $\mu(\Sigma^n) = \Omega(1/n^s)$ を満たす時をいう.

本稿においても健全な $\mathbf{P}$-sampを取り扱う. 特に, 各 $x \in \Sigma^n$ について $\mu(x) = \Omega(1/2^n n^s)$ のときに μ は *flat* であるという.

3 定理 1 の証明

必要性は明らかであるから, 十分性 (の対偶) のみを証明する. CNF 式で各節の中のリテラルの個数が 3 個のものを 3-CNF 式, 充足可能な 3-CNF 式を 3-SAT 式と呼ぶ. 3-SAT 式全体の集合 3-SAT は NP 完

全である. 3-CNF 式 F に表れる変数の個数を $n(F)$ と表記する. また $R(F,w)=F(w)$ $(w\in\Sigma^{n(F)})$ とすると

$$\text{3-SAT}=\left\{F:(\exists w)\ 0\le\sigma_{n(F)}(w)<2^{n(F)}\text{ and }R(F,w)=1\right\}$$

である.

証明に用いる **NP** 言語は

$$A=\left\{\langle F,y,i\rangle\ :\ (\exists w)\ \sigma_{n(F)}(y)\le\sigma_{n(F)}(w)<\sigma_{n(F)}(y)+2^{\sigma_k(i)}\ \text{ and }\ R(F,w)=1\right\}.$$

である. ここで $w,y\in\{0,1\}^{n(F)}$, $k=\lceil\log_2(n(F))\rceil$ かつ $i\in\{0,1\}^k$ である. また F のビット長は

$$|F|=2\cdot\binom{2(n(F)+1)}{3}\cdot\lceil\log_2(n(F))\rceil$$

である. さらに, 各 $\langle F,y,i\rangle$ について $z\le w<z+2^j$ を満たす各 w は $\forall\, l\ge j+2$ $(w_l=z_l)$ なので

$$\phi(F,y,i)=\left\langle F(x_1,\ldots,x_{j+1},z_{j+2},\ldots,z_{n(F)},y,i\right\rangle$$

とすると $\langle F,y,i\rangle\in A\iff\phi(F,y,i)\in A$ である.

ρ を 3-CNF 上の flat な 多項式時間計算可能分布, α を多項式時間計算可能な超多項式関数として任意に固定する. 証明に用いる $\{\langle F,y,i\rangle:F\in\text{3-CNF},y\in\Sigma^{n(F)},i\in\sigma^k\}$, $k=\lceil\log_2(n(F))\rceil$ 上の分布 (健全な **P**-comp) は ρ,α から以下のように構成する.

$$\mu'(\langle F,y,i\rangle)\ =\ \begin{cases}\rho'(F)\cdot 2^{-n(F)}\cdot\alpha(|F|)^{-i+1} & \text{if } 2\le\sigma_k(i)<n(F),\\ \rho'(F)\cdot 2^{-n(F)}\cdot(1-\sum_{l=2}^{n(F)-1}\alpha(|F|)^{-l+1})\cdot 1/2 & \text{if } \sigma_k(i)=0,\ 1\end{cases}$$

$$\nu'(\langle F,y,i\rangle)\ =\ \begin{cases}\rho'(F)\cdot 2^{-n(F)}\cdot\alpha(|F|)^{-\sigma_k(i)} & \text{if } 1\le\sigma_k(i)<n(F),\\ \rho'(F)\cdot 2^{-n(F)}\cdot(1-\sum_{l=1}^{n(F)-1}\alpha(|F|)^{-l}) & \text{if } \sigma_k(i)=0.\end{cases}$$

補題 1 $(A,\mu)\le^{\mathrm{p}}_{2\mathrm{d}}(A,\nu)$.

(補題の証明) 各 $\langle F,y,i\rangle$ について $(F,y,i)\in A\iff(F,y,2^{i-1})\vee(F,y+2^{i-1},2^{i-1})$ が成り立つ. そこで $f_j(F,y,i)=(F,y+2^{(1-j)(i-1)},2^{i-1})$, $\eta'_j(F,y,i)=\mu'(F,y,i)/2$, $p_j(|\langle F,y,i\rangle|)=2$ $(j=0,\ 1)$ とすると, 定義 2 の条件 (1)(3) は明らかに成り立ち, 条件 (2) は 各 $\langle G,z,j\rangle$ について

$$\begin{aligned}\eta'(f^{-1}(F,z,i-1)\ &=\ \eta'(F,z,i)+\eta'(f^{-1}(F,z-2^{i-1},i))\\ &=\ \eta'(F,z,i)+\eta'(f^{-1}(F,z-2^{i-1},i))\\ &=\ \mu'(F,z,i)/2+\mu'(f^{-1}(F,z-2^{i-1},i))/2\\ &\le\ \nu'(F,y,i-1).\end{aligned}$$

なので成り立つ. ■

$(A,\mu)\le^{\mathrm{p}}_{2\mathrm{d}}(A,\nu)$ が証明されたので, 仮定より $(A,\mu)\le^{\mathrm{p}}_{\mathrm{m}}(A,\nu)$ でなければならない. すなわち, 多項式時間計算可能関数 f, semi-distribution η, 多項式 $p>0$ が存在して, 各 $\langle F,y,i\rangle$, $\langle F,z,i-1\rangle$ について

$$\langle F,y,i\rangle\in A\iff f(F,y,i)\in A,$$

$$\eta'(f^{-1}(F,z,i-1))\le\nu'(F,z,i-1),$$

$$\mu'(F,y,i)\le p(F,y,i)^t\eta'(F,y,i)$$

が成り立つ. の量である. 各 $\langle F,y,i\rangle$ について $I_3(\langle F,y,i\rangle)=i$ とすると, 次の補題が成り立つ.

補題 2 各 $\langle F,y,i\rangle$, $i\geq 2$, に対して, $I_3(\phi(F,y,i))>I_3(f(\phi(F,y,i)))$ である.

(補題の証明) $f(\phi(F,y,i))=\langle G,z,j\rangle$ とすると, 仮定より

$$\mu'(\phi(F,y,i)))\leq|\phi(F,y,i)|^t\nu'(G,z,j)$$

すなわち

$$\rho'(F)\cdot 2^{-i+1}\cdot\alpha(|F|)^{-i+1}\leq|\phi(F,y,i)|^t\cdot\rho'(G)\cdot 2^{-n(G)}\cdot\alpha(|G|)^{-j}$$

でなければならないので, ρ は flat かつ α は超多項式なことから $n(G)\leq n(F)-2=i-1$ または $j\leq i-1$ でなければならず, いずれにしても $I_3(\phi(F,y,i))=i>I_3(\phi(G,z,j))$ となる. ■

よって, $g(F,y,i)=\phi(f(F,y,i))$ とすると各 $F\in$ 3-CNF についてある $k(F)\leq n(F)$ が存在して

$$I_3(\phi(F,0,n(F)))>I_3(g(\phi(F,0,n(F)))>\cdots>I_3(g^{(k(F))}(\phi(F,0,n(F)))\in\{0,1\}$$

となり, $F\in$ 3-SAT $\iff$ $I_3(g^{(k(F))}(\phi(F,0,n(F)))\in$ 3-SAT をえて, $I_3(g^{(k(F))}(\phi(F,0,n(F)))\in$ 3-SAT は多項式時間決定可能となる. $F\in$ 3-CNF は任意式であったので 3-SAT $\in$ **NP** が導かれ, **P** = **NP** となる.

Appendix

相田, 築地は 99 年夏の LA [AT99] において次の定理を証明した.

定理 2 1 対 1 の平均時間一方向性関数が存在すれば, どのような多項式時間計算可能分布でも抑えられないようなある多項式時間生成可能分布が存在する.

この証明の系として次の結果もえらた.

系 1 任意の多項式時間生成可能分布がある多項式時間計算可能分布で抑えられたなら, 任意の多項式時間関数 $f:\Sigma^*\to\Sigma^*$ について定数 $d,K>0$ がとれて各 n について

$$\sum_{|x|=n,|f^{-1}f(x)=1|}\frac{1}{2^n}\frac{\mathrm{Time}_M(f(x),1^n)^{1/d}}{n}<K$$

となる.

本付録では, 定理 2 の拡張として, 1 対 1 という仮定をずした次の結果を報告する.

定理 3 平均時間一方向性関数が存在すれば, どのような多項式時間計算可能分布でも抑えられないようなある多項式時間生成可能分布が存在する.

ここで, 平均時間一方向性関数とは次のような関数である.

定義 5 関数 $f:\Sigma^*\to\Sigma^*$ が**平均時間一方向性関数** (*average-time one-way function*) であるとは, 次の条件を満たすときをいう:

1. f は多項式時間で計算可能である.
2. f^{-1} を確立 1 で計算する (つまり $f(M(f(x),1^n))=f(x)$ が確立 1 で成り立つ) ような任意の乱数発生器付き多項式時間計算機械 M と任意の定数 d,K に対して, 十分大きな 全ての $n\in\mathbf{N}$ の下で,

$$\sum_{|x|=n}\frac{1}{2^n}\frac{\mathrm{Time}_M(f(x),1^n)^{1/d}}{n}>K$$

が成り立つ.

証明中で, 次の hash function を本質的に用いる.

定義 6 ([Yam97]) M を $m \times n$ の 0-1 行列,b を n 次の 0-1 ベクトルとするとき, h を $h(x) = Mx \oplus b$ と定義し, これを *hash function* と呼ぶ. このような h (すなわち M と b) の一様ランダムな分布によって定まる乱数を H_n とかく.

0-1 ベクトル x に対して,$x_{\leftarrow i}$ を x の i-bit prefix とする. h が $x \in X$ を i-識別するとは各 $w \in X - \{x\}$ について

$$h(x)_{\leftarrow i+1} \neq h(w)_{\leftarrow i+1}$$

であることをさす. K_n を $\{0, 1, \ldots, n\}$ 上の一様分布とする.

補題 3 H_n がある $x \in X$ を K_n-識別する確率は $1/4n$ 以上ある.

Proof of 定理 3: 任意の多項式時間生成可能分布がある多項式時間計算可能分布で抑えられたなら, 与えられた多項式時間関数 $f : \Sigma^n \to \Sigma^n$ の逆関数が平均時間の意味で高速に計算されてしまうことを証明する.

まず, f と hash function $h \in \Sigma^{(n+1)^2}$ から多項式時間関数 g を次のように構成する:

$$g(x, i, h) = \langle f(x), h, h(x)_{\leftarrow i} \rangle.$$

このとき, g は $m = |\langle x, h, i \rangle|$ の多項式時間で計算可能である. また, 系 1 より多項式時間機械 $M_{g^{-1}}$ (各 X について $X = M_{g^{-1}}(f(X))$ がなりたつ) と定数 $d, K > 0$ が存在して, 任意の $n > 0$ に対して

$$\sum_{\substack{|X|=m \\ |g^{-1}g(X)|=1}} \mu'_n(g(X)) \frac{\mathrm{Time}_{M_{g^{-1}}}(g(X))^{1/d}}{m} < K \tag{1}$$

である. このとき任意の $X = (x, h, i)$ について $M_{g^{-1}}(X)$ の計算時間は高々 $2^{O(|x|)}$ である.

次に $M_{g^{-1}}$ を様々の g について用意し, それらを $p(n)$ 個はり合わせて f^{-1} を計算するアルゴリズム $M_{f^{-1}}$ (各 x について $x = M_{g^{-1}}(f(x))$ がなりたつ) を次のように構成する ($p(n)$ は適当な多項式).

Step 1. 入力を $y \in f(\Sigma^n)$ とする.

Step 2. $p(n)$ 個の乱数 $h^{(i)} \sim H_n$, $k^{(i)} \sim K_n$ and $r^{(i)} \sim U_n$ $(1 \leq i \leq p(n))$ をランダム独立に生成する.

Step 3. 各 i に対して, $z_i := \langle y, h^{(i)}, r^{(i)}_{\leftarrow k^{(i)}+1} \rangle$ とする.

Step 4. 次の $p(n)$ 個の計算

$$M_{g^{-1}}(z_1), M_{g^{-1}}(z_2), \ldots, M_{g^{-1}}(z_{p(n)})$$

について, この中のある $M_{g^{-1}}(z_i)$ が (成功して) 停止するまで並列に計算する.

Step 5. Step 4 で得られた出力の第 1 成分を出力する.

補題 3 より任意の $f(x)$ について,

$$\Pr\left\{\left|g^{-1}(f(x), H_n, U_{n+1,\leftarrow K_n})\right| \neq 1\right\} > \frac{1}{4n}$$

となる. すなわち, 全ての z_i に対して $\left|g^{-1}(z_i)\right| \neq 1$ となる確率は $(1 - 1/4n)^{p(n)}$ よりも小さい. この事実と式 (1) によって, 確率 TM $M_{f^{-1}}$ の平均計算時間の上限は, 任意の $n > 0$ に対して

$$\sum_{|x|=n} \frac{1}{2^n} \rho'(r; f(x)) \frac{\mathrm{Time}_{M_{f^{-1}}}(f(x), 1^n; r)^{1/d}}{n} < p(n) \cdot K + \left(1 - \frac{1}{4n}\right)^{p(n)} \cdot 2^{O(n)}$$

である. ここで ρ は, このアルゴリズムで出力される $p(n)$ 個の乱数 $h^{(i)}$, $k^{(i)}$ 及び $r^{(i)}$ の分布とする. $p(n) > 4n^2$ であるような p を選べば, f^{-1} は平均多項式時間で計算可能である. □

参考文献

[AT99] 相田 慎, 築地立家, 一方向性関数の平均時間計算量解析, 99 年度の夏の LA シンポジウム, 2,1999.

[BCGL92] S. Ben-David, B. Chor, O. Goldreich and M. Ludy. On the Theory of Average Case Complexity, *Journal of Computer and Systems Science*, 44:193-219, 1992.

[BHT90] H. Buhrman, S. Homer and L. Torenvliest. Completeness for Nondeterministic Completeness Classes, *Mathematical Systems Theory*, 24:179-200, 1991.

[Coo71] S.A. Cook. The complexity of Theorem Proving Procedures. In *the Proceedings of the third ACM symposium on theory of computing*, 151-158, 1971.

[CS99] J. Cai and A. Selman. Fine Separation of Average-Time Complexity Classes. *SIAM Journal on Computing*, 28, 1999.

[Kar72] R.M. Karp. Reducibility among Computational Problems. In R.E. Miller and J.W. Thatcher, eds., *Complexity of Computer Computations* (Plenum, NewYork), 85-104, 1972.

[KM81] K. Koo and D. Moor. Complexity, Approximation and Density. *SIAM Journal on Computing*, 10:787-796, 1981.

[Lev73] L.A. Levin. Universal Sequential Search Problem. *Problems of Information Transmission*, 9:265-266, 1973.

[Lev86] L.A. Levin. Average Case Completeness Classes. *SIAM Journal on Computing*, 15:285-286, 1986.

[LLS75] R. Ladner, N. Lynch and A. Selman. A Comparison of polynomial time reducibilities. *Theoretical Computer Science*, 1:103-123, 1975.

[LM96] J.H. Lutz and E. Mayordomo. Cook versus Karp-Levin: Separating Completeness notions if NP is not small *Theoretical Computer Science*, 164:141-163, 1996.

[LY90] L. Longpré and P. Young. Cook Reducibility is faster than Karp redicibility in NP *Journal of Computer and Systems Science*, 41:389-401, 1990.

[Sel79] A.L. Selman. P-selective Sets, Tally Languages, and the Behavior of Polynomial Time Reductions on NP. *Mathematical Systems Theory*, 13:55-65, 1979.

[Wat87] O. Watanabe. On the Structure of Intractable Complexity Classes. PhD Thesis, Tokyo Institute of Technology, 1987.

[WT92] O. Watanabe and S. Tang. On Polynomial-time Turing and Many-one Completeness in PSPACE *Theoretical Computer Science*, 97:199-215, 1992.

[Yam97] T. Yamakami. Average Case Computational Complexity Theory. *Electronic Colloquium on Computational Complexity*, 1997.