数理解析研究所講究録
第876巻 1994年 83-90

一方向関数の相対的な存在に関する考察

坂本 直志
一橋大学 情報処理センター
sakamoto@cc.hit-u.ac.jp

概要

一方向関数として、関数を計算する時は決定性多項式時間で計算可能で、逆関数を計算する時は確率的多項式時間では有限の値しか高い確率で計算できないようなものを考え、このような強い条件を満たす一方向関数の存在を示すようなオラクルを構成した。

逆関数の難しさを単に決定性多項式時間で計算できないことだけ保証するようなオラクルの時間計算量は、入力の長さ n に対して $O(2^{cn})$ であることが知られているが、今回示したオラクルの時間計算量は $O(2^{cn^{\log^* n}})$ である。

1 はじめに

関数 f を計算することは簡単だが、f^{-1} を計算することが難しいような関数を一方向関数という。

計算量理論において、計算が難しいとは f^{-1} を計算することが必ずしも簡単でないことを意味するのだが、直観的な意味では、むしろ「一方向関数」という言葉は f^{-1} が定義されている変域ではほとんどいたるところで計算ができないような関数を意味していると思われる。

本研究では変数と関数の値の長さが変わらないような、文字列に関する関数を対象にし、計算が簡単であるとは、変数の長さに対して決定性の多項式時間で計算できることを意味し、計算が難しいとは、任意の多項式時間の確率的な計算では良い確率で値を求められるのは有限の場合だけであることとした。

つまり本研究で対象にした一方向関数 f とは

1. $|x| = |f(x)|$
2. f は決定性多項式時間計算可能
3. どのような多項式時間確率的アルゴリズム A に対しても $\Pr[A(x) = f^{-1}(x)]$ が十分大きくなるような x は有限個

という条件を満たすものである。

多項式時間周辺の一方向関数の存在は今だ未解決問題であり、$P =?NP$ 問題より難しいことが知られている。本研究ではこのような強い条件を満たす一方向関数の存在を示すようなオラクルを構成した。なお、一方向関数が存在しないようなオラクルとして $PSPACE$ 完全問題をと

ればいいことは既に [BGS75] により示されているので、一方向関数の存在証明は相対化できないような手法でしか証明できない。

2 準備

Σ は文字 0,1 の集合とし $\cdot$ は文字列の連接とする。Σ 上の長さ n の文字列全体の集合を Σ^n とし、$\Sigma^* = \bigcup_{i=0}^{\infty} \Sigma^i$ とする。Σ 上の無限の長さの文字列全体の集合を Σ^∞ とする。文字列の集合 S,T に対し $S \times T = \{s \cdot t \mid s \in S, t \in T\}$ とする。文字列の集合 $A \subseteq \Sigma^*$ に対して集合 $\overline{A} \subseteq \Sigma^\infty$ は $A \times \Sigma^\infty$ を文字列 a に対して $\overline{a}$ は $\{a\} \times \Sigma^\infty$ を表すものとする。$\overline{2^{\Sigma^*}} = \{A \times \Sigma^\infty \mid A \in 2^{\Sigma^*}\}$ とすると、この $(\Sigma^\infty, \overline{2^{\Sigma^*}})$ は可測空間である。このような可測空間に対する確率測度を μ を $(\forall n)(\forall x, y \in \Sigma^n)[\mu(\overline{x}) = \mu(\overline{y})]$ となるように導入する。また、$|a|$ は文字列 a の長さを表す。

$\alpha \in \Sigma^\infty$ に関する述語 $P(\cdot)$ に対して、$A = \{\alpha \in \Sigma^\infty \mid P(\alpha)\}$ が $\overline{2^{\Sigma^*}}$ に含まれる時 $\mu(A)$ は定義されるので、これの値を

$$\Pr_{\alpha \in \Sigma^\infty}[P(\alpha)]$$

で表すこともある。また、文字列の有限集合 $F \subseteq \Sigma^*$ の元に関する述語 $Q(\cdot)$ に対して

$$\Pr_{x \in F}[Q(x)] = \mu(\{\overline{x} \mid x \in F \wedge Q(x)\})$$

と表す。さらに、$x \in F$ と $\alpha \in \Sigma^\infty$ に関する述語 $R(\cdot,\cdot)$ に対して

$$\Pr_{x \in F, \alpha \in \Sigma^\infty}[R(x,\alpha)] = \sum_{x \in F} \mu(\overline{x}) \mu(\{\alpha \in \Sigma^\infty \mid R(x,\alpha)\})$$

とする。

$\mu(B) \neq 0$ のとき

$$\mu(A|B) = \frac{\mu(A \cap B)}{\mu(B)}$$

とし、$\Pr_{x \in F, \alpha \in \Sigma^\infty}[S(x,\alpha)] \neq 0$ のとき

$$\Pr_{x \in F, \alpha \in \Sigma^\infty}[R(x,\alpha)|S(x,\alpha)] = \frac{\Pr_{x \in F, \alpha \in \Sigma^\infty}[R(x,\alpha) \wedge S(x,\alpha)]}{\Pr_{x \in F, \alpha \in \Sigma^\infty}[S(x,\alpha)]}$$

と定義する。

確率的 Turing 機械とは Σ^* の元と Σ^∞ の元を引数に持つ 2 入力の決定性 Turing 機械のことをいう。但し Σ^∞ の元は片無限のテープの上に記入することにより与えられるとする。Turing 機械が値を出力する時には必ず有限のステップで計算が終ることに注意すると、$\Phi_M(x,y) = \{\alpha \mid M(x,\alpha) = y\}$ に対して $\mu(\Phi_M(x,y))$ は必ず定義され、これを「M が入力 x に対して y を出力する確率」または

$$\Pr_{\alpha \in \Sigma^\infty}[M(x,\alpha) = y]$$

と表す。

[定義 2.1] 入力 x を与えた時、$x \in \mathrm{Dom}(f)$ ならば $p(|x|)$ step 以内に $f(x)$ を出力して停止し、$x \notin \mathrm{Dom}(f)$ ならば停止しないような Turing 機械が存在する部分関数 f のクラスを $\mathbf{DTIMEF}(p(n))$ で表す。$\mathbf{PF} = \bigcup_{i \geq 1} \mathbf{DTIMEF}(n^i + i)$, とおく。

[定義 2.2] 特徴関数 χ_L が $\mathbf{DTIMEF}(p(n))$ に含まれるような集合 L のクラスを $\mathbf{DTIME}(p(n))$ で表す。$\mathbf{P} = \bigcup_{i \geq 1} \mathbf{DTIME}(n^i + i)$, とおく。

オラクル Turing 機械とは通常の Turing 機械に特別なテープ (質問テープと呼ぶ) と特別な状態 (質問状態と呼ぶ) を付加したものである。オラクル Turing 機械は、計算の途中でこの質問テープに文字列を書き込み、質問状態に入ることができる。(この動作を「query する」という) この状態に入ると外部からの入力待ちになり、外部から入力をもらった時点で、その入力により状態を遷移し計算を続行する。

オラクル Turing 機械の計算量は query して入力待ちになっている状態は計測しない。また、外部入力として質問テープに書かれた文字列が、ある集合 A に属すか属さないかを与えると、これは A により相対化された計算になる。集合 A により相対化されたオラクル Turing 機械 M を M^A で表す。また、集合 A により相対化された多項式時間計算可能な関数のクラスを $\mathbf{PF}^A$ のように表す。また相対化に用いた集合 A をオラクルと呼ぶ。

3 一方向関数が存在するオラクル

[定義 3.1] 関数 $f : \Sigma^* \to \Sigma^*$ が *honest* であるとは、ある多項式 p が存在し

$$(\forall x \in \mathrm{Dom}(f))[|x| \leq p(|f(x)|) \leq p(p(|x|))]$$

が成り立つことをいう。

また、関数 $f : \Sigma^* \to \Sigma^*$ が長さ不変であるとは、

$$(\forall x \in \mathrm{Dom}(f))[|x| = |f(x)|]$$

が成り立つことをいう。

[定義 3.2] 関数 $f \in \mathbf{PF}$ が **BPP-最悪時一方向関数**であるとは f が honest かつ $\mathrm{Dom}(f) \in \mathbf{P}$ が無限集合で、任意の多項式時間限定の確率的アルゴリズム M に対して無限個の x が存在し

$$\Pr_{\alpha \in \Sigma^\infty}[M(f(x), \alpha) \in f^{-1}(f(x))] < \frac{8}{9}.$$

関数 $f \in \mathbf{PF}$ が **BPP-弱無限近似不能一方向関数**であるとは f が honest かつ $\mathrm{Dom}(f) \in \mathbf{P}$ が無限集合で、ある定数 c が存在し、任意の多項式時間限定の確率的アルゴリズム M と有限の場合を除きすべての l に対して

$$\Pr_{x \in \Sigma^l \cap \mathrm{Dom}(f), \alpha \in \Sigma^\infty}[M(f(x), \alpha) \in f^{-1}(f(x))] < 1 - \frac{1}{l^c}.$$

関数 $f \in \mathbf{PF}$ が **BPP**- 強無限近似不能一方向関数であるとは f が honest かつ $\mathrm{Dom}(f) \in \mathbf{P}$ が無限集合で、任意の多項式時間限定の確率的アルゴリズム M とすべての k に対して、有限の場合を除きすべての l に対して

$$\Pr_{x \in \Sigma^l \cap \mathrm{Dom}(f), \alpha \in \Sigma^\infty}[M(f(x), \alpha) \in f^{-1}(f(x))] < \frac{1}{l^k}.$$

ここで、次のような定理が知られている。

[定理 3.3] [Gol89, 渡辺 93, Yao82] **BPP**- 弱無限近似不能一方向関数が存在すれば **BPP**- 強無限近似不能一方向関数が存在する。

これは相対化しても成り立つ。$\mathrm{ex}(0) = 1, \mathrm{ex}(n) = 2^{\mathrm{ex}(n-1)}$ とする。本研究では、関数の定義域を $\bigcup_{i=0}^{\infty} \Sigma^{\mathrm{ex}(i)}$ と制限した時に $\mathbf{BPP}^A$- 弱無限近似不能一方向関数が存在するようなオラクル A を構成する。

[定理 3.4] 関数の定義域が $\bigcup_{i=0}^{\infty} \Sigma^{\mathrm{ex}(i)}$ となるような $\mathbf{BPP}^A$- 弱無限近似不能一方向関数が存在するようなオラクル A が存在する。

(証明) $f_A(x) = \chi_A(x)^{|x|}$ は、$\mathbf{PF}^A$ に属す長さ保存の関数である。この関数に対して定義域を $\bigcup_{i=0}^{\infty} \Sigma^{\mathrm{ex}(i)}$ に制限した場合に、任意の確率的多項式時間限定オラクル Turing 機械では、有限の場合を除き、確率 8/9 より大きい確率で、逆関数の値を求められないように A を定める。

M_i^A は A をオラクルとする確率的オラクル Turing 機械の数え上げとする。

$A_0 = \emptyset$ とし、以下の手続きを $n = 1, 2, \cdots$ と繰り返し、$A = \bigcup_{i=0}^{\infty} A_i$ と定める。

手続き n $N = \mathrm{ex}(n)$ とし、$p(N) = N^n + n$、

$$S_\alpha = \bigcup_{i=1}^{n} \{x \in \Sigma^N \mid M_i^{A_{n-1}}(1^N, \alpha) \text{ を } N^i + i \text{ 時間シミュレートした時に } x \text{ を query または出力した}\}$$

と定義する。

各 Turing 機械は高々 $p(N)$ 回しか query しないので、

$$(\forall \alpha \in \Sigma^\infty)\left[\Pr_{x \in \Sigma^N}[x \in S_\alpha] \leq \frac{np(N)}{2^N}\right]$$

が成り立つ。

$q_D(x) = \mu(\{\alpha \mid x \in S_\alpha\}|D)$ とするとき、

$$\mu(D) \geq \frac{1}{3} + \frac{p(N)}{2^{N/2}} \wedge \Pr_{x \in \Sigma^N}\left[q_D(x) < \frac{1}{2^{N/2}}\right] \geq \frac{1}{3}$$

を満たす D が存在したとする。

その時 $E = \{x \in \Sigma^N \mid q_D(x) < \frac{1}{2^{N/2}}\}$ とし、

$$S'_\alpha = \bigcup_{i=1}^{n} \{x \in \Sigma^N \mid M_i^{A_{n-1} \cup E}(1^N, \alpha) \text{ を } N^i + i \text{ 時間シミュレートした時に } x \text{ を query または出力した}\}$$

とする時 $\mu(\{\alpha \mid S'_\alpha \cap E \neq \emptyset\})$ の値を求める。

$\alpha \in D$ の場合、$M_i^{A_{n-1} \cup E}$ の計算で E に query し $M_i^{A_{n-1}}$ と計算が変わる確率は、1 つの計算の中で query する回数が高々 $p(N)$ 回なので、

$$\mu(\{\alpha \mid S'_\alpha \cap E \neq \emptyset\} | D) \leq 1 - \left(1 - \frac{1}{2^{N/2}}\right)^{p(N)}$$

よって、

$$\begin{aligned}
&\mu(\{\alpha \mid S'_\alpha \cap E \neq \emptyset\}) \\
&= \mu(D)\mu(\{\alpha \mid S'_\alpha \cap E \neq \emptyset\} | D) + (\mu(\Sigma^\infty - D))\mu(\{\alpha \mid S'_\alpha \cap E \neq \emptyset\} | \Sigma^\infty - D) \\
&\leq \left(\frac{1}{3} + \frac{p(N)}{2^{N/2}}\right)\left(1 - \left(1 - \frac{1}{2^{N/2}}\right)^{p(N)}\right) + \left(\frac{2}{3} - \frac{p(N)}{2^{N/2}}\right) \cdot 1 \\
&\leq \left(\frac{1}{3} + \frac{p(N)}{2^{N/2}}\right)\left(1 - \left(1 - \frac{p(N)}{2^{N/2}}\right)\right) + \frac{2}{3} - \frac{p(N)}{2^{N/2}} \\
&\leq \left(\frac{1}{3} + \frac{p(N)}{2^{N/2}}\right)\frac{p(N)}{2^{N/2}} + \frac{2}{3} - \frac{p(N)}{2^{N/2}} \\
&\leq \frac{2}{3}
\end{aligned}$$

よって、$A_n = A_{n-1} \cup E$ とするとき、$M_i^{A_n}(1^N, \alpha)$ は E の要素を出力しないと $f_{A_n}^{-1}(1^N)$ の値を出力したことにならないので、

$$\Pr_{\alpha \in \Sigma^\infty}[M_i^{A_n}(1^N, \alpha) \in f_{A_n}^{-1}(1^N)] \leq \mu(\{\alpha \mid S'_\alpha \cap E \neq \emptyset\})$$

が成り立ち、

$$\Pr_{x \in \Sigma^N}[f_{A_n}(x) = 0^N] \leq \Pr_{x \in \Sigma^N}[x \notin E] \leq \frac{2}{3} - \frac{p(N)}{2^{N/2}} \leq \frac{2}{3}$$

より、

$$\begin{aligned}
&\Pr_{x \in \Sigma^N, \alpha \in \Sigma^\infty}[M_i^{A_n}(f_{A_n}(x), \alpha) \in f_{A_n}^{-1}(f_{A_n}(x))] \\
&= \Pr_{\alpha \in \Sigma^\infty}[M_i^{A_n}(0^N, \alpha) \in f_{A_n}^{-1}(0^N)] \cdot \Pr_{x \in \Sigma^N}[f_{A_n}(x) = 0^N] \\
&\quad + \Pr_{\alpha \in \Sigma^\infty}[M_i^{A_n}(1^N, \alpha) \in f_{A_n}^{-1}(1^N)] \cdot \Pr_{x \in \Sigma^N}[f_{A_n}(x) = 1^N] \\
&\leq 1 \times \frac{2}{3} + \frac{2}{3} \times \frac{1}{3} \\
&= \frac{8}{9}.
\end{aligned}$$

さて、

$$(\forall \alpha \in \Sigma^\infty)\left[\Pr_{x \in \Sigma^N}[x \in S_\alpha] \leq \frac{np(N)}{2^N}\right]$$

のとき

$$\mu(D) \geq \frac{1}{3} + \frac{p(N)}{2^{N/2}} \wedge \Pr_{x \in \Sigma^N}\left[q_D(x) < \frac{1}{2^{N/2}}\right] \geq \frac{1}{3}$$

を満たす D が存在することを示す。

$$(\forall D)\left[\mu(D) \geq \frac{1}{3} + \frac{p(N)}{2^{N/2}} \Rightarrow \Pr_{x \in \Sigma^N}\left[q_D(x) < \frac{1}{2^{N/2}}\right] < \frac{1}{3}\right]$$

を仮定して矛盾を導く。このとき

$$(\forall D)\left[\mu(D) \geq \frac{1}{3} + \frac{p(N)}{2^{N/2}} \Rightarrow \Pr_{x \in \Sigma^N}\left[q_D(x) \geq \frac{1}{2^{N/2}}\right] \geq \frac{2}{3}\right]$$

が成り立つ。

$$(\forall D)\left[\mu(D) \geq \frac{1}{3} + \frac{p(N)}{2^{N/2}} \Rightarrow \Pr_{x \in \Sigma^N}\left[\mu(\{\alpha \in \Sigma^\infty \mid x \in S_\alpha\}|D) \geq \frac{1}{2^{N/2}}\right] \geq \frac{2}{3}\right]$$

に対し $D = \Sigma^\infty$ とすると

$$\Pr_{x \in \Sigma^N}\left[\mu(\{\alpha \in \Sigma^\infty \mid x \in S_\alpha\}) \geq \frac{1}{2^{N/2}}\right] \geq \frac{2}{3}$$

が成り立つ。

$X = \{x \in \Sigma^N \mid \mu(\{\alpha \in \Sigma^\infty \mid x \in S_\alpha\}) \geq \frac{1}{2^{N/2}}\}$ と置くと

$$\begin{aligned}
&\Pr_{x \in \Sigma^N, \alpha \in \Sigma^\infty}[x \in S_\alpha] \\
&= \Pr_{x \in \Sigma^N, \alpha \in \Sigma^\infty}[x \in S_\alpha | x \in X] \cdot \Pr_{x \in \Sigma^N}[x \in X] + \Pr_{x \in \Sigma^N, \alpha \in \Sigma^\infty}[x \in S_\alpha | x \notin X] \cdot \Pr_{x \in \Sigma^N}[x \notin X] \\
&\geq \frac{1}{2^{N/2}} \cdot \frac{2}{3}
\end{aligned}$$

しかし、

$$(\forall \alpha)\left[\Pr_{x \in \Sigma^N}[x \in S_\alpha] \leq \frac{np(N)}{2^N}\right]$$

より

$$\Pr_{x \in \Sigma^N, \alpha \in \Sigma^\infty}[x \in S_\alpha] \leq \frac{np(N)}{2^N}$$

が成り立つので、矛盾である。

このように構成した $A = \bigcup_{i=0}^{\infty} A_i$ は定理の条件を満たす。

まず、ある確率的多項式時間オラクル Turing 機械 M_n と $L = \mathrm{ex}(l)$ $(l \geq n)$ に対して、入力が $0^L, 1^L$ のとき、A_{l+1} 以降の各元の長さは少なくとも 2^L 以上の長さであるので、$M_n^A(0^L)$ などの計算は $M_n^{A_l}(0^L)$ と同じになる。よって、その計算は手続き l で考慮されていることから、

$$\Pr_{x \in \Sigma^L \cap \mathrm{Dom}(f), \alpha \in \Sigma^\infty}[M(f(x), \alpha) \in f^{-1}(f(x))] < \frac{8}{9}$$

が成り立つ。

よって、十分大きい L に対して $\frac{8}{9} < 1 - \frac{1}{L^c}$ となるので、ある定数 c が存在し、任意の確率的多項式時間オラクル Turing 機械 M_n に対して、有限の場合を除いてすべての L に対して

$$\Pr_{x \in \Sigma^L \cap \mathrm{Dom}(f), \alpha \in \Sigma^\infty}[M(f(x), \alpha) \in f^{-1}(f(x))] < 1 - \frac{1}{L^c}$$

が成り立つ。

さて、この構成した A の時間的複雑さを調べる。

まず S_α 全体の構成については、実は、各シミュレーションでは Turing 機械を高々 $p(N)$ 時間しか実行しないので、S_α の種類も高々 $2^{p(N)}$ 個しかない。また、Turing 機械のシミュレーションにおいて無限列 α を与える必要はなく、高々 $p(N)$ ビットだけ与えれば良い。よって、S_α をすべて求めるのに必要な時間は $O(p(N)2^{p(N)})$ である。

また、E を求める手続きであるが、x に対してすべての $y \in \Sigma^{p(N)}$ に対し $q_{\overline{y}}(x)$ を求めるのに必要な時間は、すべての $\alpha \in \overline{y}$ に対し S_α は等しいので、$2^{p(N)}$ 種類の各 S_α に対して x が含まれているかどうかを調べればいいので、$O(p(N)2^{p(N)})$ 時間で求まる。すべての $x \in \Sigma^N$ に対してこれを行なっても $O(2^N p(N)2^{p(N)})$ 時間である。実は D として適当に $\mu(D) = \frac{1}{2}$ ととっても $q_D(x) \geq \frac{1}{2^{N/2}}$ となるような x は $np(N)2^{N/2-1}$ 個しかないので、$np(N)2^{N/2-1} + 2^N/3 < 2^N$ ならば高々 $np(N)2^{N/2-1} + 2^N/3$ 個の x に対して $q_D(x)$ を計算すれば E は求まる。よって E を求めるには $O((np(N)2^{N/2-1} + 2^N/3)2^{N/2}p(N)2^{p(N)})$ 時間かかる。

よって step n にかかる時間は、$p(N)$ はどのような N の多項式よりもオーダーが大きいので、ある c に対し $O(2^{cP(N)})$ となり、ex の逆関数を $\log^*$ とすると $n = \log^* N$ となることと、step n では A の長さ N の文字列に対して要素を定めていることから、A の時間的複雑さは入力の長さ n に対して $O(2^{cn^{\log^* n}})$ となる。 □

4 まとめ

本研究ではより条件の強い一方向関数の存在を示すオラクルを構成したが、今後は暗号理論的に重要な関数など、存在の示されていない関数に対してオラクルを構成し、オラクルの時間的複雑さなどからそれらの関数の存在証明の複雑さを比較していこうと考えている。

また、今回は技術的な問題から定義域を制限した関数を対象にしたが、そのような制限の必要ないような証明法も興味の対象である。

なお、本研究に関して東京工業大学工学部の渡辺治助教授から適切な助言をいただいたことに感謝する。

参考文献

[BDG88] J. L. Balcázar, J. Díaz, and J. Gabarró. *STRUCTURAL COMPLEXITY I.* Springer-Verlag Berlin Heidelberg, 1988.

[BDG90] J. L. Balcázar, J. Díaz, and J. Gabarró. *STRUCTURAL COMPLEXITY II*, chapter 6 Bi-Immunity and Complexity Cores. Springer-Verlag Berlin Heidelberg, 1990.

[BGS75] T. Baker, J. Gill, and R. Solovay. Relativizations of the $P =?NP$ question. *SIAM J. Compt.*, Vol. 4, pp. 431–442, 1975.

[BS85] J. L. Balcázar and U. Schöning. Bi-immune sets for complexity classes. *Math. Syst. Theory*, Vol. 18, pp. 1–10, 1985.

[Gol89] O. Goldreich. Foundations of cryptography. Class Notes, 1989.

[HLY86] J. Hartmanis, M. Li, and Y. Yesha. Containment, separation, complete sets, and immunity of complexity classes. *Automata, Languages, and Programming, Lecture Notes in Computer Science*, Vol. 226, pp. 136–145, 1986.

[Huy86] D. T. Huynh. Some observations about the randomness of hard problems. *SIAM J. Comput.*, Vol. 15, No. 4, pp. 1101–1105, 1986.

[Yao82] A. C. Yao. Theory and applications of trapdoor functions. In *Proceedings of the 23rd IEEE Annual Symposium on Foundations of Computer Science*, pp. 80–91, 1982.

[渡辺 93] 渡辺治. 一方向関数について (復習). ゼミ資料, 1993.