

malign measure による a priori measure の 特徴づけについて

東工大・理 小林 孝次郎 (Kojiro Kobayashi)

1 はじめに

アルゴリズム A にサイズ n の入力を与えたときの最悪実行時間を $t_A^{wo}(n)$ とし, アルゴリズム A にサイズ n の入力を確率分布 μ に従って与えたときの平均実行時間を $t_A^{av,\mu}(n)$ とすると, 常に $t_A^{av,\mu}(n) \leq t_A^{wo}(n)$ がなりたち, また多くの場合 $t_A^{wo}(n)$ は, n の関数として $t_A^{av,\mu}(n)$ よりも大きいオーダーの関数になる. Li & Vitányi ([2]) は, 入力の確率分布として “a priori probability” (より正確には “a priori measure”) の名で従来よりよく知られている確率分布 μ を選ぶと, どのようなアルゴリズム A においても平均実行時間 $t_A^{av,\mu}(n)$ と最悪実行時間 $t_A^{wo}(n)$ が同じオーダーの関数になってしまう, つまり

任意のアルゴリズム A に対しある定数 $c(> 0)$ が存在して, 任意の n に対し

$$t_A^{wo}(n) \leq ct_A^{av,\mu}(n),$$

という性質がなりたつことを示した. その後 Miltersen[3] は, 上記の性質を持つ確率分布 μ を “malign probability” (より正確には “malign measure”) と名づけ, その性質を調べた.

以下では我々は, まず malign probability の定義の分析を行い, a priori measure が上のような現象のより本質的な原因と思われる確率分布のある性質を持つことを指摘し, この性質を持つ確率分布を “strongly malign probability” と名づける. 続いて a priori probability と strongly malign probability の関係について考察し, 両者の本質的な違いがどこにあるのかを明らかにすることを試みる.

2 基本概念

$\Sigma = \{0, 1\}$ を 2 つの記号 0, 1 からなる集合, Σ^n を Σ の記号の長さ n のすべての列の集合, Σ^* を集合 $\Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \dots$ とする. Σ^* の要素を語と呼び, 語 x の長さを $|x|$ で表す. measure とは, Σ^* から $\mathbb{R}$ (すべての実数の集合) への関数 μ で, 任意の x に対し $\mu(x) \geq 0$ かつ $\mu(\Sigma^*) < \infty$ であるようなものを意味するものとする ($L \subseteq \Sigma^*$ に対し $\mu(L)$ は $\sum_{x \in L} \mu(x)$ を表す).

f, g が $\mathbb{N}$ から $\mathbb{R}$ (あるいは Σ^* から $\mathbb{R}$) への関数で, ある定数 $c(> 0)$ が存在して任意の n に対し $f(n) \leq cg(n)$ がなりたつとき, $f \lesssim g$ と書く. また $f \lesssim g$ かつ $g \lesssim f$ がなりたつとき $f \approx g$ と書く ($\mathbb{N}$ はすべての自然数の集合).

“アルゴリズム”とは決定性チューリング機械のことであると考え、アルゴリズムはすべて Σ^* のある要素を入力として受取り、(もし止まる場合には) Σ^* のある要素を出力するものと仮定する。アルゴリズム A に入力 x を与えたときの出力 (止まらない場合は “undefined”) を $\phi_A(x)$ で表す。

またアルゴリズム A に入力 x を与えたときの実行時間 (止まらない場合は “undefined”) $\text{time}_A(x)$ としては、Blum が提案した2つの公理 (Blum の公理, [1])

- (1) $\phi_A(x)$ は定義される $\iff \text{time}_A(x)$ は定義される,
- (2) A, x, t に関する述語 “ $\text{time}_A(x) \leq t$ ” は決定可能である,

を満足するような (値が自然数か “undefined” であるような) 任意の関数 $\text{time}_A(x)$ を、アルゴリズムの実行時間の測り方として認めることにする。

実行時間の測り方 $\text{time}_A(x)$ が1つ決められたとき、アルゴリズム A の最悪実行時間 $t_A^{\text{wo}}(n)$ と、measure μ に従って入力を与えたときの平均実行時間 $t_A^{\text{av}, \mu}(n)$ をそれぞれ、 $t_A^{\text{wo}}(n) = \max_{x \in \Sigma^n} \text{time}_A(x)$, $t_A^{\text{av}, \mu}(n) = \sum_{x \in \Sigma^n} (\mu(x)/\mu(\Sigma^n)) \text{time}_A(x)$ によって定義する。

定義 1 measure μ は、次の2つの条件を満足するとき malign (“悪意ある”の意) であるという ([3]):

- (i) 任意の n に対し $\mu(\Sigma^n) > 0$,
- (ii) どのような入力に対しても必ず止まるような任意のアルゴリズム A に対し、 $t_A^{\text{wo}}(n) \leq t_A^{\text{av}, \mu}(n)$ がなりたつ。

3 a priori measure

a priori measure はよく知られている概念であり、いろいろな方法で定義することができる。まず最初に、semicomputable measure の概念を用いる定義を示す。

measure μ は、 $\Sigma^* \times \mathbb{N}$ から $\mathbb{Q}$ への計算可能関数 f で、 $n \leq n'$ なら $f(n) \leq f(n')$ かつ $\lim_{n \rightarrow \infty} f(x, n) = \mu(x)$ であるようなものが存在するとき、semicomputable であるという ($\mathbb{Q}$ はすべての有理数の集合)。semicomputable measure の中には、任意の semicomputable measure μ に対し $\mu \leq \tilde{\mu}$ がなりたつ、という意味で最大のもの $\tilde{\mu}$ が存在することが知られている。このような性質を持つ semicomputable measure $\tilde{\mu}$ を、a priori measure と呼ぶ。a priori measure が存在することはよく知られている。

a priori measure を定義する他の方法は、prefix-free algorithm の概念によるものである。 x, y が Σ^* の元で $yz = x$ なる $z \in \Sigma^*$ が存在するとき、 y は x の prefix であるという。集合

$L \subseteq \Sigma^*$ は, $x \in L$ なら x と異なる x の prefix は決して L に含まれないとき, prefix-free な集合であるという. L が prefix-free な集合なら, $\sum_{x \in L} 2^{-|x|}$ は 1 以下の値になることに注意.

アルゴリズム A は, ϕ_A の定義域, つまり集合 $\{x | \phi_A(x) \text{ は定義される} \}$ が prefix-free であるとき, prefix-free algorithm であるという. prefix-free algorithm の中には, 次のような性質を持つもの A_U が存在することがわかっている: 任意の prefix-free algorithm A に対してある自然数 i が存在し, 任意の $x \in \Sigma^*$ に対し $\phi_{A_U}(0^i 1x) = \phi_A(x)$. このような prefix-free algorithm A_U を, 万能な prefix-free algorithm と呼ぶ. 以下では, このような A_U を 1 つ決めて固定しておく.

$x \in \Sigma^*$ に対し, 自然数 $H(x)$ と実数 $P(x)$ を次のように定義する:

$$H(x) = \min\{|y| \mid y \in \Sigma^*, \phi_{A_U}(y) = x\},$$

$$P(x) = \sum\{2^{-|y|} \mid y \in \Sigma^*, \phi_{A_U}(y) = x\}.$$

第2の式の右辺は, $y \in \Sigma^*$, $\phi_{A_U}(y) = x$ であるようなすべての y に対する $2^{-|y|}$ の総和を意味する.

μ が a priori measure である, という概念を定義する第2の方法は, “ μ は semicomputable でありかつ, $\mu(x) \approx 2^{-H(x)}$ ”, という条件によるものであり, 第3の方法は, “ μ は semicomputable でありかつ, $\mu(x) \approx P(x)$ ”, という条件によるものである. これらのいずれの定義を採用しても, a priori measure の概念として同じものが得られる. 以後ある a priori measure を 1 つ選び, 記号 $\tilde{\mu}$ で表すことにする.

定理 1 ([2]) a priori measure は malignant である.

この定理の証明については, 文献 [2] を参照されたい. μ をある a priori measure, A を任意のアルゴリズムとし, 長さ n の最悪入力, つまり $\text{time}_A(x)$ を最大にする長さ n の語 x (複数個ある場合には辞書式順序で最初のもの) を $w(n)$ で表すと, 任意の n に対し $\mu(w(n)) \geq c\mu(\Sigma^n)$ がなりたつような定数 $c(> 0)$ が存在する, ということを実質的には証明する.

4 strongly malignant measure

Li & Vitányi により a priori measure はすべて malignant measure であることが示されたが, その逆がなりたないことは容易に示せる. 従ってこの2つの概念は異なるものであり, その間の関係を明らかにすることは興味ある問題である. しかしその前に, malignant measure の概念の定義そのものについて, 考察を行ってみる.

malignant measure の概念の定義は明確ですっきりしているが, よく眺めてみると, 入力サイズの概念の取扱いが不自然であるように思われる.

例としてソーティングについて考えると、サイズが n の場合の入力は、 n 個の自然数 $1, 2, \dots, n$ の 2 進表現をある順序でカンマで区切ってならべたもの（をさらにビット 0, 1 の列によって表したもの）と考えてよいであろう。しかしこれは一般には Σ^n の要素ではない。他の問題のアルゴリズムにおいても、サイズが n の入力と見なされる入力は、必ずしも Σ^n の要素ではない。

上の問題点を考慮して *malign measure* の定義を修正する方法としては色々なものが考えられるが、いずれも得られた定義はかなり複雑なものになる。しかし、Li & Vitányi の “a priori measure は *malign* である” という結果は、*malign measure* の定義を色々な形に修正しても、多くの場合そのままなりたつ。

ところで定理 1 の証明においては、 μ が a priori measure なら、任意の n に対して $\mu(w(n)) / \mu(\Sigma^n) \geq c$ がなりたつような定数 $c (> 0)$ が存在する、ということを証明した。この性質は、任意のアルゴリズム A, B に対し $w(n)$ を $\phi_A(n)$ で、 Σ^n を $\phi_B^{-1}(n) (= \{x \mid \phi_B(x) = n\})$ でおきかえてもそのままなりたつ。つまり a priori measure μ は、“任意のアルゴリズム A, B に対しある定数 $c (> 0)$ が存在して、 $\phi_A(n)$ が定義されるような任意の n に対し $\mu(\phi_A(n)) / \mu(\phi_B^{-1}(n)) \geq c$ がなりたつ” という性質を持つ。

この性質は、measure に関するある本質的で重要な性質であるように思われる。我々はこの性質を持つ measure を *strongly malign measure* と呼ぶことにする。Li & Vitányi の結果は本質的には “a priori measure は *strongly malign* である” ということであり、この *strongly malign* という性質の 1 つのあらわれが（色々と修正した定義によるものも含めた）*malign* という性質である、と考えることもできる。

定義 2 measure μ は、次の 2 つの条件を満足するとき *strongly malign* であるという：

- (i) $\mu(\Sigma^*) > 0$,
- (ii) 任意のアルゴリズム A, B に対しある定数 $c (> 0)$ が存在して、 $\phi_A(n)$ が定義されるような任意の n に対し $\mu(\phi_A(n)) / \mu(\phi_B^{-1}(n)) \geq c$ がなりたつ。

a priori measure が *strongly malign* であるということは、より強いカタチで次節で証明する（定理 4 と系 1）。ここでは *strongly malign* という概念が *malign* という概念より真に強い、ということを示す。

定理 2 *strongly malign measure* は *malign* である。

（証明）*malign measure* の定義の条件 (i) の証明は容易である。条件 (ii) がなりたつことは、アルゴリズム A, B として $\phi_A(n) = w(n)$, $\phi_B^{-1}(n) = \Sigma^n$ がなりたつようなものを選ぶことによって、定理 1 の証明と同様の考え方によって示せる。 （証明終り）

定理 3 strongly malign でない malign measure が存在する.

(証明) μ を a priori measure とし, μ' を $\mu'(x) = \mu(x)/|x|$ で定義した measure とする. 定理 1 により μ は malign であり, $|x| = n$ なら $\mu'(x)/\mu'(\Sigma^n) = \mu(x)/\mu(\Sigma^n)$ がなりたつから, μ' も malign である. $\lim_{n \rightarrow \infty} \mu'(\phi_A(n)) / \mu'(\phi_B^{-1}(n)) = 0$ がなりたつようなアルゴリズム A, B の存在は容易に示せるので, μ' は strongly malign ではない. (証明終り)

5 a priori measure と strongly malign measure の関係

本節では, a priori measure と strongly malign measure の関係について調べる. 次の定理は, a priori measure の概念を strongly malign measure の定義によく似た形の条件によって特徴づける.

定理 4 measure μ に関する次の 2 つの条件は同値である.

- (1) μ は a priori measure である.
- (2) μ は次の 3 つの条件を満足する.
 - (i) μ は semicomputable である.
 - (ii) $\mu(\Sigma^*) > 0$.
 - (iii) ある定数 $c(> 0)$ が存在して, 任意のアルゴリズム A, B と $\phi_A(n)$ が定義されるような任意の n に対し, $\mu(\phi_A(n)) / \mu(\phi_B^{-1}(n)) \geq c \tilde{\mu}(A) \tilde{\mu}(B)$ がなりたつ.

(証明) $\Rightarrow$ 方向. μ を a priori measure とする. 条件 (i), (ii) の証明は容易である. 条件 (iii) の証明のアイディアは極めて簡単で, 以下のように述べることができる. A の最短の記述, B の最短の記述, $\phi_B^{-1}(n)$ に含まれる任意の語の任意の記述, の 3 つから $\phi_A(n)$ を求めることができる. 従って,

$$\begin{aligned}
 \mu(\phi_A(n)) &\approx \text{無限のビット列を選んだとき, それが } \phi_A(n) \text{ のある記述ではじまる確率} \\
 &\geq 2^{-H(A)} 2^{-H(B)} \cdot (\text{無限ビット列を選んだとき, それが } \phi_B^{-1}(n) \text{ に含まれる} \\
 &\quad \text{ある語のある記述ではじまる確率}) \\
 &= 2^{-H(A)} 2^{-H(B)} P(\phi_B^{-1}(n)) \\
 &\approx \tilde{\mu}(A) \tilde{\mu}(B) \mu(\phi_B^{-1}(n)).
 \end{aligned}$$

$\Leftarrow$ 方向. μ が条件 (i) ~ (iii) を満足するものとする. Σ^* の任意の要素 x_0 を選び, 固定して考える. B を $\phi_B^{-1}(0) = \Sigma^*$ がなりたつようなアルゴリズムとする. 任意の n に対し $\phi_A(n) =$

x_0 がなりたつようなアルゴリズム A が存在する. このような A は x_0 によって決まるので, そのことを明らかにするためにこのような A を A_{x_0} と記すことにする. A_{x_0} は x_0 から決まるから $H(A_{x_0}) \leq H(x_0) + c_1$ がなりたつような定数 c_1 がある. 従って $\tilde{\mu}(A_{x_0}) \geq c_2 \tilde{\mu}(x_0)$ がなりたつような定数 $c_2 (> 0)$ がある. 従って, $\mu(x_0) = \mu(\phi_{A_{x_0}}(0)) \geq c \tilde{\mu}(A_{x_0}) \tilde{\mu}(B) \mu(\phi_B^{-1}(0)) \geq cc_2 \tilde{\mu}(x_0) \tilde{\mu}(B) \mu(\Sigma^*)$ がなりたつ. 従って, $c_3 = cc_2 \tilde{\mu}(B) \mu(\Sigma^*) (> 0)$ とおくと, 結局すべての x_0 に対して $\mu(x_0) \geq c_3 \tilde{\mu}(x_0)$ がなりたつ. また μ は semicomputable である. 従って μ は a priori measure である. (証明終り)

系 1 a priori measure は strongly malign である.

a priori measure の 1 つの特徴づけを与える定理 4 と strongly malign measure の定義 (定義 2) を比較すると, この 2 つの概念の本質的相違は 2 つあることがわかる.

第 1 の相違は, a priori measure が必ず semicomputable であるのに対し, strongly malign measure は必ずしも semicomputable でなくてもよいことである.

第 2 の相違は, n を動かしたときの値 $\mu(\phi_A(n))/\mu(\phi_B^{-1}(n))$ の振る舞いに関するものである. a priori measure においても strongly malign measure においても, この値は A, B のみによって決まるある正の定数 $c_{A,B}$ より小さくなることはない. しかしながら, strongly malign measure においてはこの値 $c_{A,B}$ は単に “存在する” だけであるが, a priori measure においてはこの値 $c_{A,B}$ は, A, B の a priori measure の値 $\tilde{\mu}(A), \tilde{\mu}(B)$ と A, B に無関係なある定数 $c (> 0)$ によって, $c_{A,B} = c \tilde{\mu}(A) \tilde{\mu}(B)$ と表せるのである.

定理 5 に示すように, semicomputable でない strongly malign measure が存在するので, このことだけから a priori measure でない strongly malign measure が存在することがわかる. そこで興味ある問題は, measure を semicomputable なものに限定したときに, a priori measure のクラスと strongly malign measure のクラスが一致するか, つまり, μ が semicomputable であるとき,

$$\forall A, B \exists c(> 0) \forall n [\phi_A(n) \text{ が定義される} \implies \mu(\phi_A(n))/\mu(\phi_B^{-1}(n)) \geq c]$$

なら必ず

$$\exists c(> 0) \forall A, B \forall n [\phi_A(n) \text{ が定義される} \implies \mu(\phi_A(n))/\mu(\phi_B^{-1}(n)) \geq c \tilde{\mu}(A) \tilde{\mu}(B)]$$

がなりたつか, という問題であるが, これは未解決である.

定理 5 semicomputable でない strongly malign measure が存在する.

定理 4 と定義 2 にでてくる値 $\mu(\phi_A(n)) / \mu(\phi_B^{-1}(n))$ に含まれる n は, もともとの malign measure の概念に含まれていた “入力サイズ” の概念に対応している. しかし次の 2 つの定理が示すように, “ n ” を含まないもっとすっきりした形で a priori measure と strongly malign measure の概念を特徴付けることも可能である.

定理 6 measure μ に関する次の 2 つの条件は同値である.

- (1) μ は a priori measure である.
- (2) μ は次の 3 つの条件を満足する.
 - (i) μ は semicomputable である.
 - (ii) $\mu(\Sigma^*) > 0$.
 - (iii) ある定数 $c (> 0)$ が存在して, 任意のアルゴリズム A と任意の x に対し $\mu(x) / \mu(\phi_A^{-1}(x)) \geq c \tilde{\mu}(A)$ がなりたつ.

定理 7 measure μ に関する次の 2 つの条件は同値である.

- (1) μ は strongly malign measure である.
- (2) μ は次の 2 つの条件を満足する.
 - (i) $\mu(\Sigma^*) > 0$.
 - (ii) 任意のアルゴリズム A に対してある定数 $c (> 0)$ が存在して, 任意の x に対して $\mu(x) / \mu(\phi_A^{-1}(x)) \geq c$ がなりたつ.

参考文献

- [1] M. Blum, *A machine-independent theory of the complexity of recursive functions*, J. ACM 14 (1967), 322-336.
- [2] M. Li and P.M.B. Vitányi, *A theory of learning simple concepts under simple distributions and average case complexity for the universal distribution*, in Proc. of the 30th FOCS (1989), 34-39.
- [3] P. B. Miltersen, *The complexity of malign ensembles*, in Proc. of the 6th SICT (1991), 164-171.