ランダムの程度の助言付き計算
Computation with advice of degree of randomness

宮部賢志
Kenshi Miyabe
京都大学 数理解析研究所
RIMS, Kyoto University *

要約

通常の意味で計算出来ない，もしくは計算が難しい，関数を解析する手段として，次の 2 種類の計算を考えよう．1. ランダム性を計算資源として利用した計算．2. 何らかの離散的な助言を利用した計算．最近，ランダムネスの理論で，この 2 種類の計算と積分計算に深い関係があることが明らかになった．ここでは，その関係の発見に至った経緯を含めて，その解説を行う．

1 はじめに

計算理論 [16] では，計算可能な (computable) 関数を定義する．次に問われるのは「計算不可能な関数がどれくらい計算不可能であるか」である．$\leq_T$ や $\leq_{tt}$ などの 還元可能性 (reducibility) を計算不可能性の測度として使うのが，次数の理論 (degree theory) [5] である．一方，計算複雑性理論 [1] では，多項式時間還元などを使って，計算可能な関数をその計算資源によって分類する．

計算複雑性理論では，乱択アルゴリズム (randomized algorithm) に関連して，計算にランダム性を利用する複雑性クラスも考える．計算の難しさを解析する手段として，通常の還元性とは異なる基準を与えていることに注意しよう．以下ではこのタイプの計算を「ランダム性を計算資源として利用した計算」と呼ぶことにする．

通常，計算の複雑さは入力の長さの関数で判定されるが，複数のパラメータの関数として考えることもある (parameterized complexity)．例えば，最悪計算時間が指数関数となる場合であっても，あるパラメータの値が分かっていれば，その多項式時間で計算できることもある．そのような計算は「離散的な助言を利用した計算」と見ることができる．似た概念が，計算可能性理論や計算論的学習理論など，様々な分野で研究されている．

ところで,「ランダム性を計算資源として利用した計算」において，ランダム性の「何が」計算資源として利用されているのだろうか？ランダムネスの理論において最近,「ランダムの程度を離散的な助言として利用する計算」が注目されるようになった．しかしその発見は計算複雑性理論とはかなり異なった動機に基づくものである．そこで，その発見の経緯を辿りながら，その関係の解説をしたい．

*kmiyabe@kurims.kyoto-u.ac.jp

2　アルゴリズム的ランダムネスと計算可能解析学

ランダムネスの理論 [8, 13, 19] では，ある 2 進無限列がランダムかどうかの定義を与え，その性質を調べる．多くのランダムの概念が提唱されており，弱 2 ランダムネス，Martin-Löf ランダムネス，計算可能ランダムネス，Kurtz ランダムネス などがよく研究されている．ランダムの定義の方法として，テスト，マルチンゲール，複雑性 の 3 つのアプローチがあり，多くのランダムネスではそれらの同値性が示されている．

一方，計算可能解析学 [17, 2, 3, 18] では，実数から実数への計算可能性など，一般の空間上での計算可能性を考える枠組みを提供する．ここ数年，ランダムネスの理論と計算可能解析学の方法を組み合わせて，一般の測度の入った空間でのランダムネスを定義し，測度論や確率論の定理をランダムネスの観点から解析されるようになった．

3　計算可能測度論と Demuth プログラム

3.1　各層計算可能関数の出現

ランダムネスの言葉を使って，確率論の極限定理の精密化を行おう．最も基本的な極限定理は，大数の法則であろう．

命題 1
すべての *Martin-Löf* ランダムな列は大数の法則を満たす．すなわち任意の $A \in 2^\omega$ に対し，A が *Martin-Löf* ランダムならば，

$$\lim_{n\to\infty} \frac{S_n(A)}{n} = \frac{1}{2}.$$

ここで $S_n(A)$ は A の最初の n 桁に含まれる 1 の数を表している．

Martin-Löf ランダムな列は複雑性による特徴付けを持っており，K を prefix-free Kolmogorov 複雑性として，

$$(\exists d)(\forall n) K(A \upharpoonright n) > n - d$$

として特徴付けられる．ここで，$A \upharpoonright n$ は $A \in 2^\omega$ の最初の n 文字を表す．すなわち，この式を満たす列は大数の法則を満たす．まず，

$$d(A) = \sup_n (n - K(A \upharpoonright n))$$

とおこう．この $d(A)$ は，直感的には，A の中に含まれている 非ランダムさ (randomness deficiency, the degree of non-randomness) を表している．Martin-Löf ランダムであることと，この非ランダムさが有限であることが同値である．非ランダムさはテストやマルチンゲール，他の複雑性によっても定義でき，それらは互いに定数以上異なりうる．非ランダムさは厳密な定義ではなく，これらを総称する呼び名である．詳細は例えば [13] の 7.2 節の中の”The degree of nonrandomness in ML-random sets” などを参照せよ．

この d の値と収束速度の関係を論じたのが Davie であった．さらに

$$K^c = \{A \ : \ d(A) \leq c\}$$

とおく．非ランダムさに応じて Martin-Löf ランダムな列の集合を分割しているのである．それに応じて，収束速度が次のように変わるのである．

定理 2 (Davie [6])
ある計算可能な関数 $n(c,\epsilon)$ が存在して，すべての $A \in K^c$ と $n > n(c,\epsilon)$ に対して，

$$\left|\frac{S_n(A)}{n} - \frac{1}{2}\right| < \epsilon.$$

このように，ランダムな列の非ランダムさは，極限定理の収束速度の解析として使われた．この分類した各層ごとには，計算可能に証明が進むことに着目し，それを関数として捉えたのが，Hoyrup と Rojas の功績であった．Davie は複雑性を元にランダムな点を分類したが，以下ではテストを元に分類しよう．μ を Cantor 空間上の一様測度とする．一様に c.e. な開集合の列 $\{U_n\}$ が，すべての n に対して $\mu(U_n) \leq 2^{-n}$ を満たすとき，$\{U_n\}$ を Martin-Löf テスト と呼ぶ．列 $A \in 2^\omega$ が Martin-Löf ランダム であるとは，すべての Martin-Löf テスト $\{U_n\}$ に対し，$A \notin \bigcap_n U_n$ となることを言う．Martin-Löf テスト $\{U_n\}$ が 万能 であるとは，任意の Martin-Löf テスト $\{V_n\}$ に対し，定数 c が存在して，すべての n に対して $V_{n+c} \subseteq U_n$ を満たすことを言う．

定義 3 (Hoyrup-Rojas [9, 10])
減少列の万能テスト $\{U_n\}$ を固定し，$K_n = 2^\omega \setminus U_n$ とおく．関数 $f :\subseteq 2^\omega \to \mathbb{R}$ が 各層計算可能 *(layerwise computable)* であるとは，

$$f|_{K_n}$$

が n に関して一様に計算可能であることを言う．

この時，Davie の結果の K^c が K_c で置き換えられることは少しの計算で分かる．例として，$f(A)$ を $\left|\frac{S_n(A)}{n} - \frac{1}{2}\right| \geq \frac{1}{4}$ を満たす最大の n としよう．A が Martin-Löf ランダムであれば，そのような n が存在するから，$f(A)$ は定義できる．A が Martin-Löf ランダムであるという情報だけでは，最大の n は計算出来ないから，f は計算可能ではない．しかし，Davie の結果から $n(c,1/4)$ 以上ではそのような n が存在しないことが分かるので，f は各層計算可能である．この各層計算可能という概念は重要な概念でかつとても便利であり，さらに複雑な極限定理をランダムネスの言葉で置き換えるのに重要な役割を果たした．

各層計算可能関数は，名前の通り,「定義域を分割して計算可能な関数と見なせる」関数である．同時に，非ランダムさを助言として使う関数と見ることもできる．最初にそのような見方をしたのが誰なのかはハッキリしないが，各層計算可能な関数が引用および解説されるにつれ，そのような見方ができることは研究者の間で理解されていった．各層計算可能関数は，ランダムを計算資源として利用する関数であるが，何を利用しているのかと言うと,「ランダムな列に含まれる非ランダムさ」という離散的な情報を利用しているのである．このような見方はアルゴリズム的ランダムネスならではのものであろう．しかも，$d(A)$ は計算可能ではないが，下側計算可能である．(実は積分可能でもあるので，積分テストである.）よって，各層計算可能関数の計算不可能性は，まさにこの非ランダムさの計算不可能性にあるのである．

3.2 ランダムな点で良い振る舞いをする関数

3.2.1 微分可能性とランダムネス

精密化できる極限定理は大数の法則だけではない．一般に，測度論の定理における

ある性質が，ほとんど至る所（almost everywhere）成り立つ

という形の定理を，

ある性質が，すべての十分ランダムな点で成り立つ

という形に書き換えることができる，と信じられている．

このような試みを始めたのは Demuth で，次の結果が有名である．

定理 4 (Demuth [7])
実数 $x \in [0,1]$ に関して以下は同値．

(i) x は *Martin-Löf* ランダム．

(ii) すべての計算可能な有界変動関数 $f : [0,1] \to \mathbb{R}$ は x で微分可能．

この結果は,「すべての有界変動関数はほとんど至る所微分可能」という事実の実効化（計算可能性を考慮に入れたもの）と見ることができる．面白いのはある意味で逆も成り立ち，ランダムの概念を特徴づけることができることである．この結果はランダムネスの研究者にもごく最近までほとんど知られていなかった．その理由としては様々に考えられるが,

(i) Demuth が構成的数学の文脈で上記の結果を得ており，その記法が独特であったこと,

(ii) ロシア語で書かれていたが，政治的な情勢もあって，西洋との交流がほとんどなかったこと,

などが挙げられる．最近 Nies らによって再発見され，広く知られるようになった．

では，他のランダムの概念ではどうであろうか？まず，Brattka ら [4] らによって，次のような結果が得られた．上記の定理において,「有界変動」を「単調増加」に変えれば計算可能ランダムネスを,「至る所微分可能」に変えれば弱 2 ランダムネスを，特徴付ける．すなわち，各ランダムの概念に適当な計算可能な関数の族が対応している．すべての有界変動関数は 2 つの単調増加関数の差であるにも関わらず，対応するランダムの概念が異なるというのも興味深い．そこで Nies はどの関数族がどのランダムネスに対応するかを研究しようという提案をした．一方，A. Poly は,「計算可能な有界変動関数の微分とはどんな関数族か？」と問うた．計算可能な関数の微分は一般に計算可能にはならないことはよく知られている．振り返ってみると，とても重要な問題であったことが分かる．

3.2.2 L^1 計算可能性

実は Nies らと独立に，Pathak は Lebesgue の微分定理 (Lebesgue differentiation theorem) の計算可能性，特にランダムネスとの関連を調べていた．

定理 5 (Lebesgue [11])
(Lebesgue) 積分可能な関数 $f : [0,1] \to \mathbb{R}$ に対し，ほとんど至る所

$$\lim_{\epsilon \to 0} \frac{\int_{B(x,\epsilon)} f \ d\mu}{\mu(B(x,\epsilon))} = f(x)$$

が成り立つ．ここで，μ は *Lebesgue* 測度，$B(x,\epsilon) = (x-\epsilon, x+\epsilon)$ である．

上記の等式が成り立つ x を Lebesgue 点と呼ぶことにしよう．その深い関連性からこの研究に注目が集まり，最終的に次のような結果が得られた．L^1 ノルム $||\cdot||_1$ を，$||g||_1 = \int |g| d\mu$ で定義する．

定義 6 (Pour-El-Richards [15], Pathak-Rojas-Simpson [14], Miyabe [12])
関数 $f : [0,1] \to \mathbb{R}$ が，L^1 計算可能 であるとは，有理数係数の多項式の計算可能な列 $\{f_n\}$ が存在して，すべての n で，

$$||f - f_n||_1 \leq 2^{-n}$$

となることを言う．更にすべての x で $\lim_n f_n(x) = f(x)$ であるとき，f は 実効的 L^1 計算可能 であると言う．(ただし，ここでの等号は未定義も含める．)

定理 7 (Pathak-Rojas-Simpson [14])
実数 $x \in [0,1]$ に関して以下は同値．

(i) x は *Schnorr* ランダム．

(ii) すべての実効的 L^1 計算可能関数 $f : [0,1] \to \mathbb{R}$ の *Lebesgue* 点である．

Rute も独立に同じ結果を得ている．Pathak らの証明は古典的な結果をなぞったものであるのに対し，Rute の証明はマルチンゲールを使ったランダムネスらしい証明である．ただし，Rute の論文は本原稿執筆時点ではまだ準備中である．

3.2.3 積分テスト

一方，筆者は Nies の講演を聞き，積分テストとの類似性が気にかかった．関数 $t : 2^\omega \to \overline{\mathbb{R}}^+$ が 積分テスト であるとは，積分可能な下側半計算可能関数であることを言う．実数 $x \in [0,1]$ が Martin-Löf ランダムであることと，すべての積分テスト t に対して $t(x) < \infty$ となることは同値である．すぐに分かることだが，積分テスト t に対して，$f(x) = \int_{[0,x]} t \, d\mu$ とおけば，f は有界変動で，$t(x) < \infty$ と f が x で微分可能であることが同値である．ただし，f は一般には計算可能ではない．しかし深い関係があることは明らかで，Schnorr ランダムネスの場合は次のようにまとめられる．

計算可能な積分値を持つすべての下側半計算可能関数 t を，Schnorr ランダムネスに対する積分テスト と呼ぶ．下側半計算可能 (lower semicomputable) 関数とは，直感的には，入力に対して出力を下側から近似できる関数を言う．下側半計算可能関数の積分値は下側半計算可能である．一般に計算可能関数の積分値は下側半計算可能で計算可能とは限らないが，有界な計算可能関数の積分値は計算可能である．

定理 8 (Miyabe [12])
実数 $x \in [0,1]$ に関して以下は同値．

(i) x は *Schnorr* ランダム．

(ii) すべての *Schnorr* ランダムネスに対する積分テスト t に対して，$t(x) < \infty$.

定理を厳密に書くにはいくつかの定義が必要なので省くが，以下の様な関係がある．

> ある関数が L^1 計算可能であることと，2 つの Schnorr ランダムネスに対する積分テストの差になること，は本質的に同じこと．

3.2.4 Schnorr 各層計算可能性

これらの研究の中で，次のような現象が認識されるようになった．

命題 9
f を実効的 L^1 計算可能関数とし，x を *Schnorr* ランダムな点とする．この時，$f(x)$ は x から計算可能である．

この著しい性質は偶然とは思えない．この事実は一体，何を意味しているのだろうか？まず，Hoyrup-Rojas [9] によって，非負の各層下側半計算可能関数が計算可能な積分値を持つなら，実は各層計算可能であることが示されている．ここで，条件を「下側半計算可能関数」に強めれば，「Schnorr ランダムネスに対する積分テストであれば，各層計算可能」であることを意味している．そこで，各層計算可能の Schnorr ランダム版を考えれば，もっと自然な結果が得られるのではないか，という考えが自然に思いつく．実際，次の結果が成り立つのである．

> ある関数が Schnorr 各層計算可能で積分値が計算可能であることと，2 つの Schnorr ランダムネスに対する積分テストの差になること，は本質的に同じこと．

つまり,「L^1 の意味で計算可能に近似可能であること」と,「計算可能な積分値を持ちランダムの程度の助言付きなら計算できること」は，本質的に同じ事なのである．こうして,「ランダムな点での収束速度の計算可能性の研究」と,「ランダムな点で良い振る舞いをする関数の研究」という全く異なる 2 つの研究から,「ランダムの程度の助言付き計算」という概念にたどり着いた．

4 その後の研究

上記のような研究の後，計算可能測度論を Schnorr ランダムネスの観点から再構築しようという試みが，Rute，Hoyrup，筆者などによって行われている．Rute は特に関数の収束についての議論に関心があるのに対し，筆者は可測集合，可測関数など，もっと基本的なところの定義の検討が不十分であると感じて研究を進めている．Hoyrup もいくつか似た結果を独立に得ている．

これまでの議論はランダムネスの理論や計算可能解析の理論の動機から出発したものであった．しかし，この知見は計算複雑性理論における「ランダム性を計算資源として利用した計算」に対して，新たな見方を与えるように思われる．そのためには資源制限ランダムネスの研究をもっと進めることが必要であろう．

Martin-Löf ランダムネスや Schnorr ランダムネスの定義は，そのまま多項式計算時間版を作ることは難しい．しかし，今我々は Schnorr ランダムネスや Kurtz ランダムネスの多くの特徴付けを知っている．通常の定義ではなく，そのような特徴付けの中から，多項式計算時間版を作りやすいものを選んで，多項式計算時間版のそれらのランダムネスを考えることで，資源制限ランダムネスの研究が発展し，計算複雑性理論におけるランダム性の使われ方のより詳細な解析が進むことを願っている．

参 考 文 献

[1] S. Arora and B. Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[2] V. Brattka. Computability over topological structures. In S. B. Cooper and S. S. Goncharov, editors, *Computability and Models*, pages 93–136. Kluwer Academic Publishers, New York, 2003.

[3] V. Brattka, P. Hertling, and K. Weihrauch. A tutorial on computable analysis. *New Computational Paradigms*, pages 425–491, 2008.

[4] V. Brattka, J. S. Miller, and A. Nies. Randomness and differentiability. Submitted.

[5] S. B. Cooper. *Computability theory*. CRC Press, 2004.

[6] G. Davie. The Borel-Cantelli lemmas, probability laws and Kolmogorov complexity. *Annals of Probability*, 29(4):1426–1434, 2001.

[7] O. Demuth. The differentiability of constructive functions of weakly bounded variation on pseudo numbers. *Comment. Math. Univ. Carolin.*, 16(3):583–599, 1975.

[8] R. Downey and D. R. Hirschfeldt. *Algorithmic Randomness and Complexity*. Springer, Berlin, 2010.

[9] M. Hoyrup and C. Rojas. An Application of Martin-Löf Randomness to Effective Probability Theory. In *CiE*, pages 260–269, 2009.

[10] M. Hoyrup and C. Rojas. Applications of Effective Probability Theory to Martin-Löf Randomness. In *ICALP (1)*, pages 549–561, 2009.

[11] H. Lebesgue. *Leçons sur l'Intégration et la recherche des fonctions primitives*. Gauthier-Villars, Paris, 1904.

[12] K. Miyabe. L^1-computability, layerwise computability and Solovay reducibility. Submitted.

[13] A. Nies. *Computability and Randomness*. Oxford University Press, USA, 2009.

[14] N. Pathak, C. Rojas, and S. G. Simpson. Schnorr randomness and the Lebesgue Differentiation Theorem. To appear in Proceedings of the American Mathematical Society.

[15] M. B. Pour-El and J. I. Richards. *Computability in analysis and physics*. Springer, 1989.

[16] M. Sipser. *Introduction to the Theory of Computation*. Course Technology Ptr, second edition edition, 2012.

[17] K. Weihrauch. *Computable Analysis: an introduction*. Springer, Berlin, 2000.

[18] K. Weihrauch and T. Grubba. Elementary Computable Topology. *Journal of Universal Computer Science*, 15(6):1381–1422, 2009.

[19] 宮部賢志. ランダムネスの一般化. 数理解析研究所講究録, 1729:84–94, 2011. 形式体系と計算理論 (Formal systems and computability theory).