Schnorr triviality and a base for uniform Schnorr randomness

証明論と複雑性

2012年9月12日～14日　京都大学数理解析研究所

宮部賢志

京都大学　数理解析研究所

記述量と問い合わせの回数

- 「複雑性とは計算に必要な資源の最小量として導入される各種の量であり，（中略）コルモゴロフ記述量，および問い合わせの回数を含みます。これら各種の複雑性は，互いに関連性をもっています。」（RIMS研究集会「証明論と複雑性」の「目的と範囲」より）

ランダム

	計算可能	その間	ランダム
記述量	定数	その間	多い
問い合わせの回数	定数	その間	多い

話の流れ

- Schnorrランダムネスとその特徴づけ
- Schnorr trivialityとその特徴付け
- 新たな複雑性による特徴付け
- base型による特徴付け

Schnorrランダムネス

Functional

定義

Φ_e を e 番目の oracle Turing machine とする.

$\Phi_e :\subseteq 2^\omega \to 2^\omega$ は Turing functional とも呼ばれる.

Φ_e が total であるとき，truth-table functional と呼ばれる.

use(Φ, A, n) で，$\Phi^A(m)(m \leq n)$ を計算するのに必要な最大の問い合わせを表す.

計算可能

命題

A に関して，以下は同値.

1. A が計算可能.
2. ある Turing machine Φ_e が存在して，すべての n で $A(n) = \Phi_e(n)$.
3. ある Turing functional Φ_e と $B \in 2^\omega$ が存在して，$A = \Phi_e^B$ かつ
$$\mathrm{use}(\Phi_e, B, n) \leq O(1).$$

Schnorrランダム

定理 (Day 201?)

A に関して，以下は同値.

1. A が Schnorr ランダムではない.
2. ある Turing functional Φ_e と $B \in 2^\omega$ および狭義単調増加関数 f が存在して，$A = \Phi_e^B$ かつ

$$\exists^\infty \mathrm{use}(\Phi_e, B, f(n)) \leq f(n) - n$$

Schnorrランダムネス

定義 (Downey and Griffiths)

prefix-free マシン $M :\subseteq 2^* \to 2^*$ の測度を，$\mu([\![\mathrm{dom}(M)]\!])$ により定義する.

定理 (Downey and Griffiths)

A が Schnorr ランダムであることと，すべての計算可能な測度を持つマシン M に対して,

$$K_M(A \upharpoonright n) \geq n - O(1)$$

であることは同値.

決定可能マシン

マシンが決定可能であるとは，その定義域が決定可能であることをいう．$\mathbb{N}$ から $\mathbb{N}$ への非有界非減少関数を order という．

定理 (Bienvenu and Merkle)

A が Schnorr ランダムであることと，すべての決定可能 prefix-free マシン M と計算可能な order$g$ に対し，

$$K_M(A \upharpoonright n) \geq n - g(n) - O(1)$$

であることは同値.

このマシンで Schnorr triviality を特徴付けられるか?

Schnorr triviality

Schnorr triviality

定義 (Schnorr 還元; Downey and Griffiths)
すべての計算可能な測度を持つマシン M に対し，ある計算可能な測度を持つマシン N が存在して，

$$K_N(A \upharpoonright n) \leq K_M(B \upharpoonright n) + O(1)$$

であるとき，$A \leq_{\mathrm{Sch}} B$ と書く．
$A \leq_{\mathrm{Sch}} \emptyset$ のとき，A は Schnorr trivial であるという．

totally i.o. complex

定義 (Hölzl and Merkle)

A が totally i.o. complex であるとは，ある計算可能関数 h が存在して，任意の全域マシン M に対し，無限に多くの n で

$$K_M(A \upharpoonright h(n))) \geq n$$

となることをいう.

定理 (Hölzl and Merkle)

列が totally i.o. complex でないことと，Schnorr trivial であることは同値.

trace

定義

集合の列 $\{T_n\}$ が関数 $f(n)$ の trace であるとは，すべての n に対し，$f(n) \in T_n$ であることをいう．

trace がある計算可能な order h で抑えられるとは，すべての n で $|T_n| \leq h(n)$ となることをいう．

列 A が computably tt-traceable であるとは，ある計算可能な order h が存在して，任意の $f \leq_{\mathrm{tt}} A$ に対し，h で抑えられた f の trace が存在することをいう．

特徴付け

定理 (Franklin and Stephan)

列が computably tt-traceable であることと，Schnorr trivial であることは同値.

問い合わせの回数

定義 (Franklin, Greenberg and Stephan 201?)

$A \leq_{\mathrm{tt}} B$ であるとする．任意の order h に対し，ある functional Φ が存在して，$A = \Phi^B$ かつ

$$\mathrm{use}(\Phi, B, n) \leq h(n)$$

であるとき，$A \leq_{\mathrm{tt(tu)}} B$ と書く．

定理 (Franklin et al.)

A が Schnorr trivial であることと，ある B に対して $A \leq_{\mathrm{tt(tu)}} B$ であることは同値.

複雑性による特徴付け

wdm還元

定義 (宮部)

任意の決定可能 prefix-free マシン M と計算可能な order g に対し，ある決定可能 prefix-free マシン N が存在して，

$$K_N(A \upharpoonright n) \leq K_M(B \upharpoonright n) + g(n) + O(1)$$

であるとき，$A \leq_{\mathrm{wdm}} B$ と書く．

新たな特徴付け

定理 (M.)

A が Schnorr trivial であることと，$A \leq_{\mathrm{wdm}} \emptyset$ であることは同値.

実は，任意の A, B に対し，

$$A \leq_{\mathrm{wdm}} B \iff A \leq_{\mathrm{Sch}} B.$$

Schnorrテストのbase

一様Schnorrランダムネス

定義

マシン M が一様決定可能であるとは，$X \mapsto \mathrm{dom}(M^X)$ が全域計算可能関数になることをいう．

定理

B が A 一様 Schnorr ランダムであることと，すべての一様決定可能 prefix-free マシン M と計算可能な order g に対し，

$$K_{M^A}(B \upharpoonright n) \geq n - g(n) - O(1)$$

であることは同値.

Schnorrテストのbase

定義

A が Schnorr テストに対し base であるとは, 任意の一様決定可能 prefix-free マシン M に対し，ある B が存在して，$A \leq_{\mathrm{tt}} B$ かつ

$$K_{M^A}(B \upharpoonright n) \geq n - g(n) - O(1).$$

定理

A が Schnorr テストの base になることと，Schnorr trivial であることは同値.

Four equivalent notions

Theorem (Nies 2005, Hirschfeldt-Nies-Stephan 2007)
The following are equivalent for a set A:

1. A is low for ML-randomness,
2. A is low for K,
3. A is K-trivial,
4. A is a basis for ML-randomness.

.

Summary

	Schnorr random	uniform Schnorr random
trace	comp. traceable	comp. tt-traceable (FS2010)
low	low for SR	low for unif. SR (FS2010)
low	low for c.m.m.	low for u.m.m. (M2011)
trivial	Schnorr trivial	
trivial	wdm-reducible to 0	
basis		base for unif. SR