ランダムの概念の多数問題

宮部賢志　明治大学理工学部数学科

joint work with Rupert Hölzl

鈴木研・宮部研合同ゼミ@明治大学生田キャンパス

2016年2月18日(金)

テーマ

- 「ランダムの概念の多数問題」
- 「ランダムな列からよりランダムな列は作れるか？」

構成

- 計算論入門
  - 停止問題，Turing次数，多数問題
- ランダムネス入門
  - ML，Schnorr，差ランダムネス
- ランダムの概念の多数問題
  - いろいろなTuring次数，一様計算

計算論入門

自然数の集合

例

1. $\{n \ : \ n$ は偶数 $\}$
2. $\{p \ : \ p$ は素数 $\}$
3. $\{n \ : \$ ある 0 でない自然数に対して $X^n + Y^n = Z^n\}$
4. $\{n \ : \ \sin(n^\circ) \in \mathbb{Q}\}$

自然数が与えられた時に，その自然数がその集合に含まれるかどうか判別する問題を，判定問題という．判定するプログラムが書ける時，その問題は判定可能または計算可能であるという．

計算できない問題

プログラムを適当にコード化することで自然数と対応づけることができる．そこで e 番目のプログラムによる計算可能関数を Φ_e で表す．Φ_e は一般には部分関数である．

$$K = \{e \ : \ \Phi_e(e)\downarrow\}$$

とおくと，K は計算不可能である．

証明

$$K = \{e \ : \ \Phi_e(e) \downarrow\}$$

が計算可能であるとすると，ある指標 n が存在して，

$$\Phi_n(k) = \begin{cases} 0 & (k \notin K) \\ \Phi_k(k) + 1 & (k \in K) \end{cases}$$

しかし，

$$\Phi_n(n) = 0 \Rightarrow n \notin K \Rightarrow \Phi_n(n) \uparrow$$
$$\Phi_n(n) > 0 \Rightarrow \Phi_n(n) = \Phi_n(n) + 1$$

となり，矛盾. .

計算困難さの比較

計算不可能な問題 A, B の困難さを比較する．もし「B を使えば A を計算できる」のであれば，「問題 B は 問題 A よりも難しい」と言え，「問題 A は問題 B に還元される」と言う．

定義

B の情報を使って A を計算できる時，A は B に Turing 還元可能と言い，$A \leq_T B$ で表す．$A \equiv_T B$ を $A \leq_T B$ かつ $B \leq_T A$ で定義すれば，$\equiv_T$ は同値関係となり，2^ω をこの同値関係で割った商は，Turing 次数と呼ばれる．

例えば，$K = \{e \ : \ \Phi_e(e) \downarrow\}$ と $H = \{\langle n, k\rangle \ : \ \Phi_n(k) \downarrow\}$ は Turing 同値である．

証明．$K \leq_T H$ は明らか．

n, k が与えられた時に，すべての入力に対し $\Phi_n(k) \downarrow$ ならば 1 を返しそうでないならば止まらない部分関数は，計算可能でありその指標が存在するが，その指標 $h(n, k)$ を与える関数 h も計算可能である．よって，$h(n, k) \in K$ かどうかを調べればよい．

答えが多数ある問題

$A \subseteq \mathbb{N}$ は次のような性質を持つとしよう.

1. n が合成数の時は $n \notin A$
2. n が素数の時は $n \in A$ でも $n \notin A$ でも良い.

Miller-Rabin 素数判定法はこの問題の解を高速に与えるアルゴリズムとして知られている．解は複数あり得る．このような解の集合を「多数問題」と呼ぶ.

多数問題の困難さを計算可能性の観点から比較しよう．問題 B の解を使って，問題 A の解を計算できる時，問題 A は問題 B に還元されるという．この定式化には 2 種類ある.

定義

$P, Q \subseteq 2^\omega$ に対し，P が Q に Muchnik 還元可能 ($P \leq_w Q$) とは，すべての $f \in Q$ に対し，$g \leq_T f$ となる $g \in P$ が存在すること.

最も簡単な問題は計算可能な解を含む問題で，任意の集合族に対して還元可能.

最も難しい問題は空集合であるが，除いて考えることが多い.

定義

$P, Q \subseteq 2^\omega$ に対し，P が Q に Medvedev 還元可能 ($P \leq_s Q$) とは，Turing functional Φ が存在して，すべての $f \in Q$ に対し，$\Phi^f \in P$ となること.

Muchnik 還元と Medvedev 還元の違いは，一様な計算であるかどうか.

定理 (Simpson 2004)

$$2^\omega <_w \{\text{ML ランダム列}\} <_w \text{PA}$$

ここで，PA はペアノ算術の無矛盾な完全拡大の集合.

ランダムネス入門

統計的検定

統計的検定では，帰無仮説を立て，分布の端 5% に入れば不自然と判定し，そうでなければ自然と判定する．

例えば，100 回コインを投げて，60 回表が出たとする．これは自然だろうか？表と裏が確率 $\frac{1}{2}$ で独立に現れると仮定する．100 回投げて表が出た回数を X とすれば，$Y = \frac{X-50}{\sqrt{100/4}}$ の分布は標準正規分布に近い．標準正規分布の両側 5% 検定は $|Y| > 1.96$ であり，これは $X < 40.2,\ 59.8 < X$ と同値である．よって，60 回表が出るのは不自然である．

統計的仮説検定	ランダムネス
有限列	無限列
独立を仮定する	独立は仮定できない
平均からの乖離を見る	すべての規則を見る
5%	測度0

測度0とは

定理

集合 A は測度 0 を持つ $\iff$ 任意の $\epsilon > 0$ に対してある開集合 O が存在して $A \subseteq O$ かつ $\mu(O) \leq \epsilon$

定義

集合 A は ML-null であるとは，一様 c.e. 開集合の列 $\{U_n\}$ が存在して，すべての n で $A \subseteq U_n$ かつ $\mu(U_n) \leq 2^{-n}$

Cantor空間

2^ω で 2 進無限列の集合を表し，

$$[\sigma] = \{X \in 2^\omega \ : \ \sigma \prec X\}$$

柱状集合 (cylinder set) を開基とする位相を入れた空間を，Cantor 空間と呼ぶ．$\mu(\sigma) = 2^{-|\sigma|}$ により入る測度を fair-coin measure と呼び，以下この測度を入れる．

開集合は開基の和で表せることに注意して，開集合 U が c.e. であるとは，

$$U = \bigcup_{\sigma \in S} [\sigma]$$

となる計算可能な集合 S が存在することと定義する．

MLランダムネス

定義

Martin-Löf 検定 (ML 検定) とは，一様 c.e. 開集合の列 $\{U_n\}$ で，$\mu(U_n) \leq 2^{-n}$ であるものをいう．2 進無限列 $A \in 2^\omega$ が ML 検定 $\{U_n\}$ に合格するとは，$A \notin \bigcap_n U_n$ となることをいう．すべての ML 検定に合格する列を ML ランダムな列という．

基本的性質

定理

ML ランダムな列の集合は測度 1.

証明. ML ランダムでない列の集合は，測度 0 の集合の可算和だから，測度 0.

定理

計算可能な列は ML ランダムではない.

証明. A を計算可能な列として，$U_n = [A \upharpoonright n]$ とすれば，$\{U_n\}$ は ML 検定で，A はこの ML 検定に合格しない.

基本的性質

定理

すべての ML ランダムな列に対して，大数の法則が成立する．

すなわち，A が ML ランダムであれば，

$$\frac{\sum_{k=1}^{n} A(k)}{n} \to \frac{1}{2} \quad (n \to \infty)$$

証明．確率論における大数の法則の証明の計算可能性を確認すればよい．

定義

Schnorr 検定とは，ML 検定 $\{U_n\}$ で $\mu(U_n) = 2^{-n}$ となるものをいう．すべての Schnorr 検定に合格する列を，Schnorr ランダムと呼ぶ.

定義 (Franklin - Ng 2011)

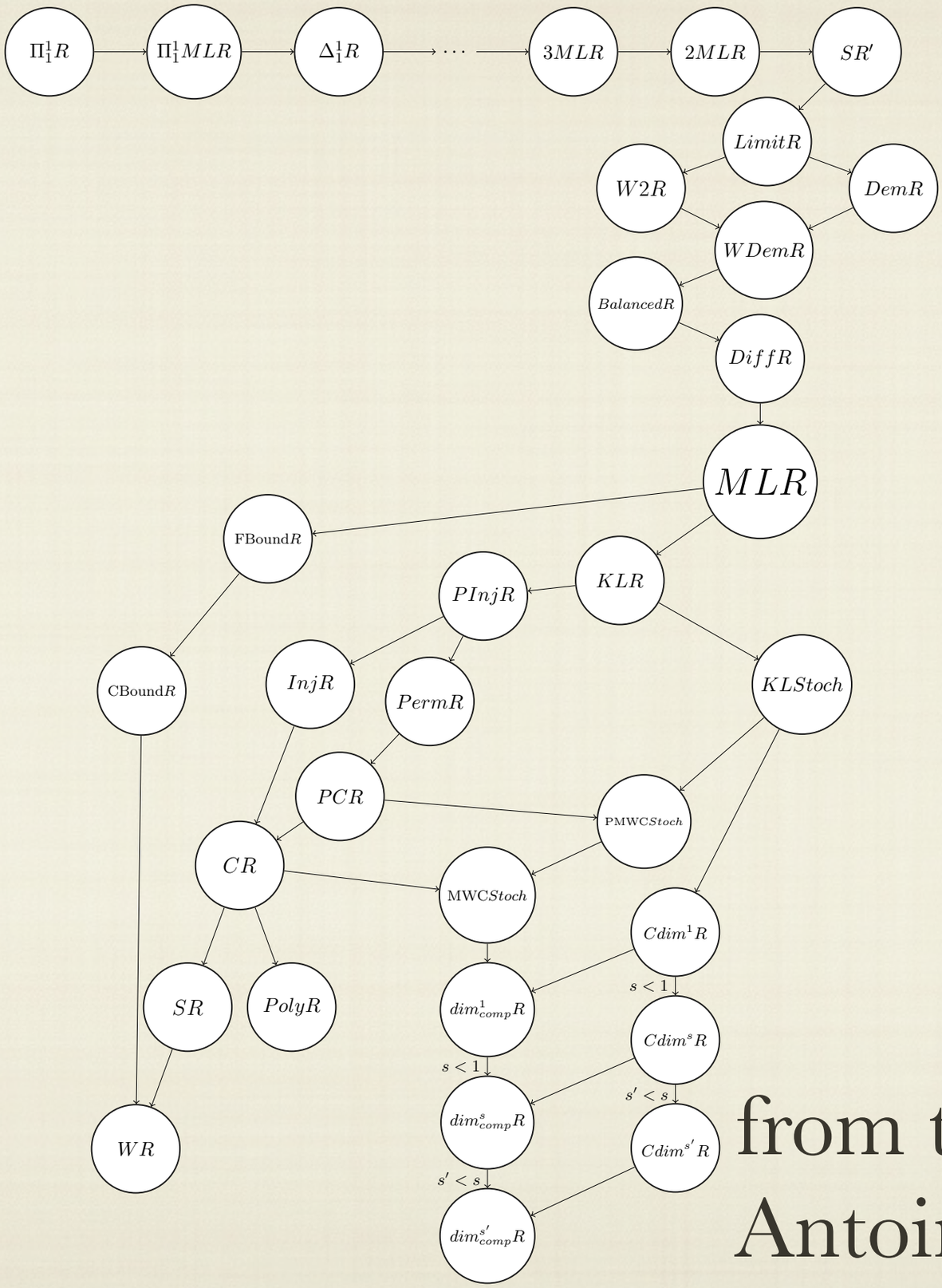
差検定とは，一様な d.c.e. 集合列 $\{V_n\}$ で $\mu(V_n) \leq 2^{-n}$ となるものを言う．すべての差検定に合格する列を，差ランダムと呼ぶ.

定理 (Franklin - Ng 2011)

A が差ランダム $\iff$ A が ML ランダムかつ Turing 完全ではない.

Randomness Zoo

Antoine Taveneaux



from the website of
Antoine Taveneaux

ランダムの概念の多数問題

ランダムな列を作る

$$\mathrm{SR} \supset \mathrm{MLR} \supset \mathrm{DiffR}$$

より

$$\mathrm{SR} \leq_s \mathrm{MLR} \leq_s \mathrm{DiffR}$$

が分かる．問題は真に大きいかどうか．言葉を変えれば「ランダムな列からよりランダムな列を作れるか？」だけが問題となる．

定理　SR $<_w$ MLR

証明. MLR $\leq_w$ SR として矛盾を導く．$\mathbf{a}$ を high かつ minimal な Turing 次数とする (Cooper 73)．すべての high 次数には Schnorr ランダムな列が含まれる (Nies-Stephan-Terwijn 2005) ので，それを X とおく．仮定より $Y \leq_T X$ となる ML ランダムな列 Y が存在する．Y は計算可能ではないので，Y の Turing 次数は minimal．しかし，ML ランダムな次数は minimal にはなり得ないので矛盾.

定理　$\mathrm{MLR} \equiv_w \mathrm{DiffR}$

証明. $X = Y \oplus Z \in \mathrm{MLR}$ に対して，$Y \geq_T \emptyset'$ ならば，独立性定理より $Z \in \mathrm{MLR}(Y)$ より Z は 2 ランダムで差ランダム.

定理　$\mathrm{MLR} <_s \mathrm{DiffR}$

証明. $\Phi :\subseteq 2^\omega \to \omega$ を Turing functional で，$X \in \mathrm{MLR}$ なら $\Phi(X) \in \mathrm{MLR}$ となるものとする．ν を Φ による誘導測度とすると，Φ が a.e. 計算可能であることから，ν は計算可能.

ν は絶対連続である．なぜなら，ν が atom X を持てば，$\mu(\Phi^{-1}(\{X\})) > 0$ であることから，ML ランダム列 $Y \in \Phi^{-1}(\{X\})$ が存在して，$X = \phi(Y) \in \mathrm{MLR}$ となる．これは計算可能測度のすべての atom が計算可能であることに矛盾.

定理　MLR $<_s$ DiffR

証明続き．Levin-Kautz の定理より，ν が連続で $\mathbf{a} > 0$ ならば，$\mathbf{a}$ に ML ランダム列が含まれることと $\mathbf{a}$ に ν-ML ランダム列が含まれることは同値である．特に ν-ML ランダム列 $X \in \mathbf{0}'$ が存在する．

ML ランダム性に対する”No-randomness-from-nothing” (Bienvenu-Porter ’12) より，ML ランダム列 Y が存在して $X = \Phi(Y)$．構成より X は差ランダムではない．Φ は任意であったことから，定理が従う．

定理

$$\mathrm{WR} <_w \mathrm{SR} \equiv_w \mathrm{CR} <_w \mathrm{MLR} \equiv_w \mathrm{DiffR} \leq_w \mathrm{W2R} <_w \mathrm{2R}$$

Muchnik 次数の不等号は hyperimmune, high, minimal などの次数を見てやればよい．Medvedev 次数の非一様性に関しては少し複雑な議論が必要.

予想

$$\mathrm{SR} <_s \mathrm{CR}$$

まとめ

- ランダムの概念の階層は自然にMuchnik次数とMedvedev次数に埋め込める
- ランダムの概念と一様計算可能性との関連が示唆される