集中講義「ランダムネスの理論」2019 年京都大学

記法・定義・定理などをまとめる．

$\omega = \{0, 1, 2, \cdots\}$

$2^{<\omega}$：2 進有限列の集合，2^{ω}：2 進無限列の集合

$f :\subseteq A \to B$：集合 A から集合 B への部分関数，$f : A \to B$：A から B への全域関数

定義 1. 関数 $f :\subseteq 2^{<\omega} \to 2^{<\omega}$ が**計算可能** (computable) であるとは，ある Turing 機械 M が存在して入力文字列 σ をテープに書いて計算を始めたときに，$\sigma \in \mathrm{dom}(f)$ なら M は停止して停止状態のテープには $f(\sigma)$ が書かれていて，$\sigma \notin \mathrm{dom}(f)$ なら M は停止しない，ことをいう．

機械 M と M が計算する関数を同一視する．機械 (machine) とは部分計算可能 (partial computable function) のこと．

$M(\sigma)\downarrow$ で入力 σ で停止することを表し，$M(\sigma)\uparrow$ で入力 σ で停止しないことを表す．

定義 2. 機械 U が**万能** (universal) とは，$(\forall M : \text{machine})(\exists\sigma \in 2^{<\omega})(\forall\tau \in 2^{<\omega})[U(\sigma\tau) \simeq M(\tau)]$

$f(\sigma) \simeq g(\sigma)$ とは，$f(\sigma)\downarrow$ なら $g(\sigma)\downarrow$ で $f(\sigma) = g(\sigma)$，$f(\sigma)\uparrow$ なら $g(\sigma)\uparrow$ である，ことを表す．

定理 3. 万能機械は存在する．

すべての機械を計算可能に並べあげることができる．

すべての全域機械を計算可能に並べあげることはできない．

$A \subseteq \omega$ が**計算可能**とは，$f(n) = \begin{cases} 1 & \text{if } n \in A \\ 0 & \text{if } n \notin A \end{cases}$ が計算可能であること．

$A \subseteq \omega$ が**計算枚挙可能** (c.e.) とは，$(\exists f : \text{部分計算可能関数})[A = \mathrm{dom}(f)]$ となること．

$A = A(0)A(1)A(2)\cdots \in 2^{\omega}$ が**計算可能**とは，$n \mapsto A(n)$ が計算可能であること．

2 進有限列全体を $\lambda, 0, 1, 00, 01, 10, 11, 000, \cdots$ と並べて ω と対応付けることで，ω 上の計算可能性が定義される．

適当な符号化により $\mathbb{Q}$ 上の計算可能性も定義される．

定理 4. $A \subseteq \omega$ が計算可能 $\iff$ A と A^c が *c.e.*

$x \in \mathbb{R}$ が**計算可能**とは，計算可能な有理数列 $\{a_n\}$ が存在して，$(\forall n)[|x - a_n| < 2^{-n}]$ となること．

$x \in \mathbb{R}$ が**左 *c.e.***(left-c.e.) とは，$\{q \in \mathbb{Q} \ : \ q < x\}$ が c.e. であること．

左 c.e. は**下側半計算可能** (lower semicomputable) とも呼ばれる．

関数 $f : 2^{<\omega} \to \mathbb{R}$ が**計算可能**とは，$f(\sigma)$ が一様に計算可能であること．

関数 $f : 2^{<\omega} \to \mathbb{R}$ が**下側半計算可能**とは，$f(\sigma)$ が一様に下側半計算可能であること．

2^{ω} には $[\sigma] = \{X \in 2^{\omega} \ : \ \sigma \prec X\}$ を開基とする位相を入れる．

$U \subseteq 2^{\omega}$ が ***c.e.* 開集合** (c.e. open set) とは，ある計算可能な集合 $S \subseteq 2^{<\omega}$ が存在して，$U = \bigcup_{\sigma\in S}[\sigma]$ と書けること．

関数 $f : 2^{\omega} \to \mathbb{R}$ が**下側半計算可能**とは，入力に対し一様に下から計算可能に近似できること，つまり $\{X \in 2^{\omega} \ : \ f(X) > q\}$ が q に関して一様に c.e. 開集合となること．

μ で $\mu(\sigma) = \mu([\sigma]) = 2^{-|\sigma|}$ から定まる一様測度を表す．

$C_M(\sigma) = \min\{|\tau| \ : \ M(\tau) = \sigma\}$.

U を万能機械として，$C = C_U$.

$C(\sigma) \le |\sigma| + O(1)$.

$A \subset 2^{<\omega}$ が**非接頭** (prefix-free) とは，$(\forall\sigma, \tau \in A)[\sigma \ne \tau \Rightarrow \sigma \not\preceq \tau]$.

機械 M が非接頭とは，$\mathrm{dom}(M)$ が非接頭であること．

M を非接頭機械として，$K_M(\sigma) = \min\{|\tau| \ : \ M(\tau) = \sigma\}$

$K(\sigma) \leq |\sigma| + K(|\sigma|) + O(1)$

定理 5 (Extended Counting Theorem)**.** $R_M(n) = -\log \mu([\{\tau \ : \ |M(\tau)\downarrow| = n\}])$ とすると，

$$|\{\sigma \in 2^n \ : \ K_M(\sigma) \leq n + R_M(n) - r\}| \leq 2^{n-r}$$

万能機械 U に対しては，$R_U(n) = K(n) + O(1)$．

定理 6 (KC 定理)**.** $d_i \in \omega$, $\tau_i \in 2^{<\omega}$, (d_i, τ_i) が計算可能で，$\sum 2^{-d_i} \leq 1$ のとき，*KC* 集合と呼ぶ．$(\exists M$: 非接頭機械$)(\exists \sigma_i \in 2^{d_i})[M(\sigma_i) = \tau_i,\ \mathrm{dom}(M) = \{\sigma_i\}]$

定義 7. $X \in 2^\omega$ が weakly Chaitin random とは，$K(X \upharpoonright n) > n - O(1)$ となること．

定義 8. 一様 c.e. 開集合 $(U_n)_n$ で $(\forall n)[\mu(U_n) \leq 2^{-n}]$ となるものを *Martin-Löf* **検定** (ML-test) と呼ぶ．$X \in 2^\omega$ が ML 検定 $(U_n)_n$ に**合格する** (pass) とは，$X \notin \bigcap_n U_n$ となること．すべての ML 検定に合格する列を ML ランダムな列と呼ぶ．

万能 ML 検定が存在する．

定義 9. 一様 c.e. 開集合の列 $(U_n)_n$ で $\sum \mu(U_n) < \infty$ となるものを *Solovay* **検定**という．

定理 10. *X が ML ランダム $\iff$ 高々有限の n で $X \in U_n$*

定理 11. *$X \in 2^\omega$ が weakly Chaitin random $\iff$ X が ML ランダム*

定義 12. $f : 2^\omega \to [0, \infty]$ が**積分検定** (integral test) とは，f が下側半計算可能で，$\int f d\mu < \infty$ となること．

定理 13. *X が ML ランダム $\iff$ すべての積分検定 f に対し $f(X) < \infty$*

定義 14. $M : 2^{<\omega} \to [0, \infty)$ で $M(\sigma) = \frac{M(\sigma 0) + M(\sigma 1)}{2}$ を満たすものを**マルチンゲール** (martingale) と呼ぶ．

定理 15. *$X \in 2^\omega$ が ML ランダム $\iff$ すべての c.e. マルチンゲール M に対し $\sup_n M(X \upharpoonright n) < \infty$.*

定義 16. ML 検定 $(U_n)_n$ で $\mu(U_n)$ が一様に計算可能なものを *Schnorr* **検定**と呼ぶ．すべての Schnorr 検定に合格する列を *Schnorr* **ランダム**と呼ぶ．

万能 Schnorr 検定は存在しない．

定義 17. Solovay 検定 $(U_n)_n$ で $\sum \mu(U_n)$ が計算可能となるものを *Schnorr-Solovay* **検定**という．

定理 18. *X が Schnorr ランダム $\iff$ 高々有限の n で $X \in U_n$*

定理 19. *$X \in 2^\omega$ が Schnorr ランダム $\iff$ $(\forall h$: 計算可能 order$)$ $(\forall M$: 計算可能マルチンゲール$)$ $[$十分大きな n で $M(X \upharpoonright n) < h(n)]$*

定理 20. *c.e. 開集合 $U \subset 2^\omega$ で，$\mu(U)$ が計算可能，$\mu(U) < 1$ なら，計算可能な列 $X \in 2^\omega$ で $X \notin U$ となるものが存在する．*

定理 21. *Schnorr ランダムで ML ランダムでない列が存在する．*

演習問題

問題 1. $A \in \omega$ が計算可能であることと，A と A^c が c.e. であることは同値である．これを示せ.

問題 2. $f(n) = \min\{C(\sigma) : |\sigma| \geq n\}$ とおく.

(1) $n \to \infty$ のとき $f(n)$ は無限大に発散することを示せ.

(2) 任意の計算可能な非有界単調非減少関数 $g(n)$ に対して，十分大きな n で $g(n) > f(n)$ となることを示せ.

問題 3. 計算可能な列は weakly Chaitin random ではないことを示せ.

問題 4. $x \in [0,1]$ の 2 進展開を $0.X(0)X(1)\cdots$ とする．次を示せ.

(1) x が計算可能であることと，X が計算可能であることは同値である.

(2) x が ML ランダムであることと，X が ML ランダムであることは同値である.

問題 5. M を計算可能な有理数値マルチンゲールとする．λ を空文字とする．すべての n に対して $M(X \upharpoonright n) \leq M(\lambda)$ となるような計算可能な列 $X \in 2^\omega$ が存在することを示せ.

問題 6. T を 2^ω 上のシフト写像とする．X が ML ランダムならば，すべての c.e. 開集合 U で $\mu(U) < 1$ なるものに対して，$(\exists n)T^n(X) \notin U$ である．この事実を使って，同じ条件のもとで $(\exists^\infty n)T^n(X) \notin U$ となることを示せ.