Poznámky z přednášek
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

Algoritmická náhodnost I + II

Peter Černo, 2011
petercerno@gmail.com

Garant: doc. RNDr. Antonín Kučera, CSc.
E-mail: Antonin.Kucera@mff.cuni.cz

Anotace: Předmět je určen pro doktorandské studenty se zájmem o algoritmickou náhodnost. Pojem Kolmogorovské složitosti hraje důležitou roli v teorii informační složitosti. Různé varianty Kolmogorovské složitosti vedou k odlišným pojmům. Alternativní přístup k algoritmické náhodnosti je založen na teorii míry a používá podstatně prostředky teorie rekurze.

Pokročilejší partie algoritmické náhodnosti, kalibrace různých variant. Pojmy "K-triviality", "low for random", jejich ekvivalence a význam. Aplikace v teorii rekurze.

Sylabus:

1. Kolmogorovská složitost (plain, prefix-free).
2. Algoritmická náhodnost prostřednictvím prefix-free Kolmogorovské složitosti.
3. Rekurzivní stromy, Sigma-0-1 a Pi-0-1 třidy.
4. Martin-Löf testy, univerzální Martin-Löf test.
5. Algoritmická náhodnost prostřednictvím Martin-Löf testů.
6. Univerzální tvar.
7. Martingaly.
8. Pojmy "low for random, "K-trivial".
9. Ekvivalence různých pojmů z hlediska algoritmické náhodnosti výpočetně slabých množin.
10. Základní vlastnosti K-triviálních množin.
11. Aplikace v terorii rekurze.
12. Modifikace K-triviálních množin a zobecnění.

Literatura:

1. Ming Li, Paul Vitanyi: An Introduction to Kolmogorov Complexity and Its Applications, Springer, 1997

2. R. Downey, D. Hirschfeldt: Algorithmic randomness and complexity

3. Odifreddi P.: Classical recursion theory. North-Holland, 1989

4. http://www.mcs.vuw.ac.nz/ downey/

This page is intentionally left blank.

14.02.2011 Mo
PETER ČERNO

EXAM: ALGORITMICKÁ NÁHODNOSŤ I

HYPERIMMUNE-FREE DEGREES

$\underset{\sim}{a}$ IS HYPERIMMUNE DEGREE $\iff$
$\exists f \leq_T \underset{\sim}{a}$ NOT DOMINATED BY ANY COMPUTABLE FUNCTION

MILLER & MARTIN: $\underset{\sim}{a} <_T \underset{\sim}{b} \leq_T \underset{\sim}{a}' \Rightarrow$
$\underset{\sim}{b}$ IS HYPERIMMUNE

FOR $\underset{\sim}{a} = \underset{\sim}{\emptyset}$: LET $\emptyset <_T B \leq_T \emptyset'$

$\boxed{wm(n) \overset{def}{:=} \mu s \geq n \, (B_s \upharpoonright_n = B \upharpoonright_n)}$ ... WEAK MODULUS = FIRST TRUE

CLEARLY, $wm \leq_T B$. wm IS NOT COMP. DOMINATED:
IF COMPUTABLE h MAJORIZES $wm \Rightarrow$
B IS COMPUTABLE ↯
TO COMPUTE $B \upharpoonright_m$, SEARCH FOR $n > m$:
$\forall t \in [n, h(n)] : B_t \upharpoonright_m = B_n \upharpoonright_m$.

MILLER & MARTIN: $\exists$ HYPERIMMUNE-FREE DEG. $>_T \underset{\sim}{\emptyset}$.

FORCING WITH COMPUTABLE PERFECT TREES

FUNCTION TREE: $T : 2^{<\omega} \to 2^{<\omega}$:
$T(\sigma 0), T(\sigma 1)$ ARE INCOMPATIBLE EXT. OF $T(\sigma)$.

WE BUILD A SEQUENCE $\{T_i\}_{i \in \omega}$ OF COMP. FUNCTION TREES AND RETURN ANY $A \in \bigcap_i [T_i]$ ...

STAGE 0 : T_0 BE THE IDENTITY MAP

STAGE 2e+1 : WE FORCE NONCOMPUTABILITY

WE ARE GIVEN T_{2e}. LET $i \in \{0,1\}$ S.T.

$T_{2e}(i) \nsubseteq W_e \restriction |T_{2e}(i)|$.

DEFINE $T_{2e+1}(\sigma) := T_{2e}(i\sigma)$.

STAGE 2e+2 : WE FORCE NO COMP. DOMINANCE

WE ARE GIVEN T_{2e+1}. WE WISH EITHER:

(i) $A \in [T_{2e+2}] \Rightarrow \Phi_e^A$ IS NOT TOTAL, OR

(ii) $\exists$ COMPUTABLE f : $\forall A \in [T_{2e+2}]$: $\Phi_e^A \leq f$

1) $\exists n, \sigma$: $\Phi_e^{T_{2e+1}(\tau)}(n)\uparrow \ \forall \tau \succeq \sigma$.

$T_{2e+2}(\nu) := T_{2e+1}(\sigma\nu)$

2) $\neg \exists n, \sigma$: ...

WE BUILD FUNCTION TREE f S.T.:

$\forall \tau \in 2^{<\omega}$: $\Phi_e^{T_{2e+1}(f(\tau))}(|\tau|)\downarrow$

$T_{2e+2}(\tau) := T_{2e+1}(f(\tau))$.

STRONG ARRAY ... A COMPUTABLE COLLECTION OF DISJOINT FINITE SETS $\{F_i\}_{i\in\omega}$

INFINITE SET A IS HYPERIMMUNE $\Leftrightarrow$

$\forall$ STRONG ARRAY $\{F_i\}_{i\in\omega}$ $\exists i$: $F_i \subset \bar{A}$.

C.E. SET A IS HYPERSIMPLE $\Leftrightarrow$ $\bar{A}$ IS HYPERIMMUNE

14.02.2011 Mo
PETER ČERNO

EXAM: ALGORITMICKÁ NÁHODNOST I

MILLER & MARTIN: $\underset{\sim}{a}$ IS HYPERIMMUNE $\Leftrightarrow$ $\underset{\sim}{a}$ CONTAINS A S.T. p_A IS NOT COMP. MAJORIZED.

$\tilde{a}$ IS HYPERIMMUNE $\Leftrightarrow$ CONTAINS A HYPERIM. SET

BASIS THEOREMS

WE CONSIDER ONLY NONEMPTY Π^0_1 CLASSES

KREISEL BASIS THEOREM: EVERY Π^0_1 CLASS HAS A left-C.E. MEMBER.

LOW BASIS THEOREM: EVERY Π^0_1 CLASS HAS A LOW MEMBER.

LET $C = [T]$ WITH T COMPUTABLE.
WE DEFINE $T = T_0 \supseteq T_1 \supseteq \ldots$ RETURN ANY $P \in \bigcap [T_e]$.
SUPPOSE THAT WE HAVE DEFINED T_e. LET:

$$\boxed{U_e := \{ \sigma \mid \Phi_e^\sigma(e)[|\sigma|]\uparrow \}}$$

U_e IS A COMPUTABLE TREE. IF $U_e \cap T_e$ IS INFINITE THEN $T_{e+1} := U_e \cap T_e$. OTHERWISE, $T_{e+1} := T_e$.

HYPERIMMUNE-FREE BASIS THEOREM:
EVERY Π^0_1 CLASS HAS A MEMBER OF HYPERIMMUNE-FREE DEGREE.

WE ARE GIVEN T_e AND WANT TO BUILD T_{e+1}:

(i) $A \in [T_{e+1}] \Rightarrow \Phi_e^A$ IS NOT TOTAL, OR

(ii) $\exists$ COMP. f : $\forall A \in [T_{e+1}] : \Phi_e^A \leq f$.

$$U_e^n := \{\sigma \mid \Phi_e^\sigma(n)[|\sigma|]\uparrow\}$$

IF $\exists n$: $U_e^n \cap T_e$ IS INFINITE THEN $T_{e+1} := U_e^n \cap T_e$

OTHERWISE, $T_{e+1} := T_e$. IN THIS CASE:

... FOR EACH n WE CAN COMPUTE $\ell(n)$:

$\forall \sigma \in T_e \ |\sigma| = \ell(n) : \Phi_e^\sigma(n)\downarrow$ ...

INFINITE SET A IS <u>EFFECTIVELY IMMUNE</u> $\Leftrightarrow$
$\exists$ COMPUTABLE f : $\forall e \ W_e \subseteq A \Rightarrow |W_e| \leq f(e)$.

DEFINE $\varphi(x)\downarrow = y \Leftrightarrow y > 2x$ & $y \in W_x$

$A := \operatorname{rng} \varphi$ IS C.E. & $\bar{A}$ IS EFF. IMMUNE VIA $e \mapsto 2e$.

<u>MARTIN</u>: IF C.E. SET B COMPUTES AN EFF. IMMUNE SET, THEN B IS TURING COMPLETE.

$\Rightarrow$ THE INCOMPLETE C.E. DEGREES DO NOT FORM A BASIS FOR Π_1^0 CLASSES.

IT IS ENOUGH TO FIND A Π_1^0 CLASS ALL OF WHOSE MEMBERS ARE INFINITE SUBSETS OF EFF. IM. $\bar{A}$.

$|A \upharpoonright 2e| \leq e \Rightarrow \bar{A} \cap [2^k-1, 2^{k+1}-2] \neq \emptyset \ \forall k$.

$P := \{B \subseteq \bar{A} \mid \forall k \ B \cap [\ldots, \ldots] \neq \emptyset\}$.

14.02.2011 Mo
PETER ČERNO

EXAM: ALGORITMICKÁ NÁHODNOST I

PA DEGREES

DEGREE $\underset{\sim}{a}$ IS <u>PA DEGREE</u> $\Leftrightarrow$ IT IS A DEGREE OF A COMPLETE EXTENSION OF PEANO ARITHMETIC

<u>SCOTT BASIS THEOREM</u>: IF $\underset{\sim}{a}$ IS A PA DEGREE $\Rightarrow$ THE SETS COMPUTABLE FROM $\underset{\sim}{a}$ FORM A BASIS FOR THE Π^0_1 CLASSES.

LET S BE A COMPLETE EXTENSION OF PA $\in \underset{\sim}{a}$.
LET T BE AN INFINITE COMPUTABLE TREE
WE COMPUTE A PATH $\sigma_0 < \sigma_1 < \dots \in T$ USING S.

<u>SOLOVAY</u>: THE CLASS OF PA DEGREES IS CLOSED UPWARDS.

LET T BE A COMPLETE EXTENSION OF PA COMPUTABLE IN A SET X. USING T, WE WILL BUILD FINITE EXTENSIONS F_σ OF PA S.T. $\bigcup_{\sigma < x} F_\sigma$ IS A COMPLETE EXTENSION OF PA WITH THE SAME DEGREE AS X.

<u>COROLLARY</u>: $\underset{\sim}{a}$ IS A PA DEGREE $\Leftrightarrow$ THE SETS COMPUTABLE FROM $\underset{\sim}{a}$ FORM A BASIS FOR THE Π^0_1 CLASSES.

IN OTHER WORDS: $\underset{\sim}{a}$ IS A PA DEGREE $\Leftrightarrow$ EVERY INFINITE COMPUTABLE BINARY TREE HAS AN $\underset{\sim}{a}$-COMPUTABLE PATH.

SMULLYAN: LET C BE A SEPARATING SET FOR AN EFFECTIVELY INSEPARABLE PAIR OF C.E. SETS A, B. LET X, Y BE DISJOINT C.E. SETS. THEN THERE IS A C-COMPUTABLE SET SEPARATING X AND Y.

USING RECURSION THEOREM DEFINE:

$$W_{\omega_1(n)} = \begin{cases} A \cup \{f(\omega_1(n), \omega_2(n))\} & \text{IF } n \in Y \\ A & \text{OTHERWISE} \end{cases}$$

$$W_{\omega_2(n)} = \begin{cases} B \cup \{f(\omega_1(n), \omega_2(n))\} & \text{IF } n \in X \\ B & \text{OTHERWISE} \end{cases}$$

$$D := \{ n \mid f(\omega_1(n), \omega_2(n)) \in C \}$$

$D \leq_T C$ IS A SEPARATING SET FOR X, Y.

JOCKUSH & SOARE: $\underset{\sim}{a}$ IS A PA DEGRE $\Leftrightarrow$ $\underset{\sim}{a}$ COMPUTES A SEPARATING SET FOR AN EFFECTIVELY INSEPARABLE PAIR.

15.02.2011 TU
PETER ČERNO

EXAM: ALGORITMICKÁ NÁHODNOSŤ I

FIXED-POINT FREE AND DIAGONALLY NONCOMPUTABLE FUNCTIONS

TOTAL f IS <u>FIXED-POINT FREE</u> $\iff W_{f(e)} \neq W_e \ \forall e$

TOTAL g IS <u>DIAGONALLY NONCOMPUTABLE</u> (DNC) $\iff$
$g(e) \neq \Phi_e(e) \ \forall e$.

THEOREM: THE FOLLOWING ARE EQUIVALENT:
(i) SET A COMPUTES A FIXED-POINT FREE FNC.
(ii) SET A COMPUTES A TOTAL h : $\Phi_{h(e)} \neq \Phi_e \ \forall e$.
(iii) SET A COMPUTES A DNC FUNCTION.

<u>(ii) ⇒ (iii)</u> : DEFINE TOTAL COMPUTABLE d:

$$\Phi_{d(u)} = \begin{cases} \Phi_{\Phi_u(u)} & \text{IF } \Phi_u(u)\downarrow \\ \uparrow & \text{OTHERWISE} \end{cases}$$

LET $g := h \circ d$. NOTE $g \leq_T A$. g IS DNC:

IF $g(e) = \Phi_e(e)$, THEN BY (ii)

$$\Phi_{d(e)} \neq \Phi_{h(d(e))} = \Phi_{g(e)} = \Phi_{\Phi_e(e)} = \Phi_{d(e)} \ \lightning$$

<u>(iii) ⇒ (i)</u> :

FIX PARTIAL COMPUTABLE ψ : $W_e \neq \emptyset \Rightarrow \psi(e) \in W_e$.
LET q BE TOTAL COMPUTABLE : $\Phi_{q(e)}(q(e)) = \psi(e)$.
LET $g \leq_T A$ BE DNC.

DEFINE $f \leq_T A$: $W_{f(e)} = \{g(q(e))\}$.

$\Rightarrow$ f IS FIXED-POINT FREE :

IF $W_e = W_{f(e)}$ $\Rightarrow$ $W_e \neq \emptyset$ $\Rightarrow$ $\psi(e) \in W_e$ $\Rightarrow$

$\Rightarrow$ $\psi(e) = g(q(e))$. g IS DNC, SO :

$g(q(e)) \neq \Phi_{q(e)}(q(e)) = \psi(e)$ $\lightning$.

THEOREM : $\underset{\sim}{a}$ IS A PA DEGREE $\Leftrightarrow$ $\underset{\sim}{a}$ COMPUTES A $\{0,1\}$-DNC.

$\Rightarrow$) $\{0,1\}$-DNC FORM A Π^0_1 CLASS.

$\Leftarrow$) LET A COMPUTE $\{0,1\}$-DNC g.

g SEPARATES $\{e \mid \Phi_e(e) = 0\}$, $\{e \mid \Phi_e(e) = 1\}$.

ARSLANOV'S COMPLETENESS CRITERION

A C.E. SET IS TURING COMPLETE $\Leftrightarrow$ IT COMPUTES A FIXED-POINT FREE FUNCTION.

$\Rightarrow$) $\emptyset'$ COMPUTES A DNC $\Rightarrow$ ... FPF.

$\Leftarrow$) LET A BE A C.E. SET :

A COMPUTES A FPF f ... $\Gamma^A = f$.

ASSUME $\Gamma^A(n)[s]\downarrow$ FOR ALL $n \leq s$.

DEFINE TOTAL COMPUTABLE h :

INITIALLY $W_{h(n)} = \emptyset$.

15.02.2011 Tu
PETER ČERNO

EXAM: ALGORITMICKÁ NÁHODNOST I

IF $n \in \emptyset'[s]$ THEN PUT EVERY $x \in W_{\Gamma^A(h(n))[s]}[s]$ INTO $W_{h(n)}$.

WE CAN COMPUTE $\emptyset'$ FROM A USING h:

IF n ENTERS $\emptyset'$ AT STAGE s:

SUPPOSE $\Gamma^A(h(n))$ HAS SETTLED BY STAGE s

THEN EVERY $x \in W_{\Gamma^A(h(n))}$ IS EVENTUALLY PUT INTO $W_{h(n)}$, WHILE NO OTHER x ENTERS $W_{h(n)}$ $\Rightarrow$ $W_{f(h(n))} = W_{\Gamma^A(h(n))} = W_{h(n)}$ $\lightning$

THUS $\Gamma^A(h(n))$ HAS NOT SETTLED BY STAGE s.

$A \leq_T \emptyset' \Leftrightarrow \exists$ TOTAL COMPUTABLE f:

$$A(n) = \lim_s f(n, s)$$

... SHOENFIELD's LIMIT LEMMA

$$\mathrm{mod}_f(n) := \mu_s \left(\forall t \geq s \; \forall x = 0 \ldots n : f(x,t) = A(x) \right)$$
$$\mathrm{wm}_f(n) := \mu_{s \geq n} \left(\forall x = 0 \ldots n : f(x,s) = A(x) \right)$$

$A \leq_T \mathrm{mod}_f \leq_T \emptyset'$

$A \equiv_T \mathrm{wm}_f$

IF A IS C.E., THEN $A \equiv_T \mathrm{mod}_f$

ARSLANOV'S COMPLETENESS CRITERION II

A C.E. SET IS TURING COMPLETE $\iff$ IT COMPUTES A $\{0,1\}$-DNC FUNCTION.

$\Leftarrow$) LET A BE C.E., $g \leq_T A$ BE $\{0,1\}$-DNC. LET f BE TOTAL COMPUTABLE S.T. $g(n) = \lim_s f(n,s)$, AND $\text{mod}_f \leq_T A$. DEFINE TOTAL COMPUTABLE h:

$$\Phi_{h(n)}(h(n)) = \begin{cases} f(h(n), s) & \text{IF } n \in \emptyset'[s] \\ \uparrow & \text{OTHERWISE} \end{cases}$$

WE CAN COMPUTE $\emptyset'$ FROM mod_f USING h:

IF n ENTERS $\emptyset'$ AT THE STAGE s:

SUPPOSE $f(h(n), s)$ HAS SETTLED BY STAGE s.

THEN $\Phi_{h(n)}(h(n)) = f(h(n), s) = g(h(n)) \neq \Phi_{h(n)}(h(n))$. $\lightning$

THUS $f(h(n), s)$ HAS NOT SETTLED BY STAGE s.

A COINFINITE C.E. SET A IS <u>PROMPTLY SIMPLE</u>

$\iff$ THERE ARE A COMPUTABLE f AND ENUMERATION $\{A_s\}_{s\in\omega}$ S.T. $\forall e$:

$|W_e| = \infty \Rightarrow \exists^\infty x \exists s \, (x \in W_{e,\text{at } s} \wedge x \in A_{f(s)})$

$W_{e,\text{at } s} = W_e[s] \setminus W_e[s-1]$

<u>KUČERA</u>: IF $f \leq_T \emptyset'$ IS FPF ($\{0,1\}$-DNC) $\Rightarrow \exists$ PROMPTLY SIMPLE C.E. SET $B \leq_T f$.

15.02.2011 Tu
PETER ČERNO

EXAM: ALGORITMICKÁ NÁHODNOSŤ I

LET $f \leq_T \emptyset'$ BE FIXED-POINT FREE.

WE BUILD $B \leq_T f$ TO SATISFY:

R_e: $|W_e| = \infty \Rightarrow \exists x \exists s\, (x \in W_{e, \text{at } s} \wedge x \in B_s)$

DURING CONSTRUCTION WE DEF. AUXILIARY COMP. h ...

AT THE STAGE s: FOR EACH $e \leq s$ S.T.

1. R_e IS NOT YET MET,
2. SOME $x > \max\{2e, h(e)\}$ IS IN $W_{e, \text{at } s}$, AND
3. $f_s(h(e)) = f_t(h(e))$ FOR ALL $x \leq t \leq s$

ENUMERATE x INTO B.

USING THE RECURSION THEOREM, LET $W_{h(e)} = W_{f_s(h(e))}$.

B IS C.E.

B IS COFINITE BECAUSE AT MOST ONE x IS PUT INTO B FOR THE SAKE OF EACH R_e AND $x > 2e$

EACH R_e IS MET: SUPPOSE $|W_e| = \infty$

LET u BE S.T. $f_t(h(e)) = f(h(e))$ FOR $\forall t \geq u$.

...

26.09.2011 Mo
PETER ČERNO

ALGORITHMIC RANDOMNESS

KOLMOGOROV COMPLEXITY (PLAIN) OF A STRING σ WITH RESPECT TO $f: 2^{<\omega} \to 2^{<\omega}$:

$$\boxed{C_f(\sigma) = \min\{|\tau| : f(\tau) = \sigma\}}$$

σ IS RANDOM RELATIVE TO f, IF $C_f(\sigma) \geq |\sigma|$

f ... DESCRIPTION SYSTEM

PARTIAL COMP. $U: 2^{<\omega} \to 2^{<\omega}$ ... UNIVERSAL:

FOR EACH PARTIAL COMP. $f: 2^{<\omega} \to 2^{<\omega}$:

THERE IS A STRING ρ_f : $\forall \sigma [U(\rho_f \sigma) = f(\sigma)]$

ρ_f ... CODING STRING, $|\rho_f|$ ... CODING CONST.

$\triangleleft$: $C_U(\sigma) \leq C_f(\sigma) + |\rho_f|$

(PLAIN) KOL. COMPLEXITY: $C(\sigma) \overset{\text{def}}{:=} C_U(\sigma)$

$\triangleleft$: (1) $C(\sigma) \leq |\sigma| + O(1)$

3.1.1 (2) $C(\sigma\sigma) \leq C(\sigma) + O(1)$

(3) $h: 2^{<\omega} \to 2^{<\omega}$ COMP. $\Rightarrow$

$C(h(\sigma)) \leq C(\sigma) + O(1)$

SUPPOSE $C(\sigma) = k$ ... THERE IS A LEAST STAGE s

S.T. $U(\tau)[s]\downarrow = \sigma$ FOR ONE OR MORE τ, $|\tau| = k$

$\sigma_C^* \overset{\text{def.}}{:=}$ LEXICOGRAP. LEAST SUCH τ.

$\lhd\!\cdot)$: $C(\sigma, C(\sigma)) = C(\sigma_C^*) \pm O(1)$

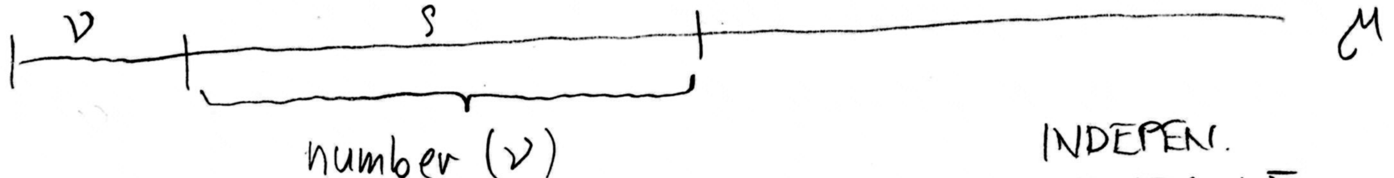
3.1.2

$\lhd\!\cdot)$: $\forall n\ \exists \sigma, |\sigma| = n : C(\sigma) \geq n$

3.1.3

$$\left|\{\sigma \in 2^n : C(\sigma) \geq |\sigma| - k\}\right| > 2^n(1 - 2^{-k})$$

THEOREM 3.1.4. : FIX k. IF μ IS SUFFICIENTLY LONG $\Rightarrow$ $\exists$ INITIAL SEGMENT σ OF μ S.T. $C(\sigma) < |\sigma| - k$.



$\sigma := \nu\rho$ ... $C(\sigma) \leq |\rho| + c$ ← INDEPEN. CONSTANT

IF $|\nu| > c + k \Rightarrow C(\sigma) < |\sigma| - k$. □

FIX d. THERE IS $\mu = \sigma\tau : C(\mu) > C(\sigma) + C(\tau) + d$

LET c: $C(\tau) \leq |\tau| + c$ ← CONSTANT

LET $C(\mu) \geq |\mu|$

$\mu = \sigma\tau$, $C(\sigma) < |\sigma| - k$, WHERE $k = c + d$

$\Rightarrow C(\mu) \geq |\mu| = |\sigma| + |\tau| > C(\sigma) + k + C(\tau) - c$. □

$\lhd\!\cdot)$: $C(\sigma\tau) \leq C(\sigma, \tau) \leq C(\sigma) + C(\tau) + 2 \log C(\sigma) + O(1)$

3.1.5.

26.09.2011 Mo.
PETER ČERNO

ALGORITHMIC RANDOMNESS

$\triangleleft$: $A = \{\sigma \mid C(\sigma) \geq \frac{|\sigma|}{2}\}$ IS IMMUNE.

IF INFINITE C.E. $B \subseteq A$, LET h BE COMP. S.T.:
$h(n) :=$ FIRST STRING σ, $|\sigma| \geq n$ TO ENTER B ... ↯

CONDITIONAL COMPLEXITY

FIX UNIVERSAL ORACLE MACHINE U ...

$$C^A(\sigma) = \min\{|\tau| : U^A(\tau) = \sigma\}.$$

FOR STRINGS:

$$C(\sigma \mid \tau) := \min\{|\mu| : U^{\bar{\tau}}(\mu) = \sigma\}$$

$\bar{\tau}$ ... PREFIX-FREE CODING OF τ

IF $\tau = a_0 \dots a_m$ THEN $\bar{\tau} = a_0 a_0 \dots a_m a_m 01$

... IT IS POSSIBLE TO DEFINE M S.T. $M^{\bar{\sigma}}(\lambda) = \sigma$

SYMMETRY OF INFORMATION

(PLAIN) INFORMATION CONTENT OF τ IN σ:

$$I_C(\sigma : \tau) \overset{\text{def.}}{:=} C(\tau) - C(\tau \mid \sigma)$$

THEOREM: $I_C(\sigma : \tau) = I_C(\tau : \sigma) \pm O(\log C(\sigma, \tau))$

3.3.1.

THEOREM: $C(\sigma, \tau) = C(\tau \mid \sigma) + C(\sigma) \pm O(\log C(\sigma, \tau))$

3.3.2

INFORMATION-THEORETIC CHARACT. OF COMPUT.

IF A IS COMP. $\Rightarrow$ $C(A\restriction_n \mid n) = O(1)$ $\leftarrow$ DEPENDS ON A

THEOREM (LOVELAND): X ... INFIN. COMP. SET

3.4.1 FOR EACH e, THERE ARE ONLY FIN. MANY SETS A S.T. $C(A\restriction_n \mid n) \leq e$ FOR ALL $n \in X$

EACH SUCH A IS COMPUTABLE.

THEOREM (CHAITIN): A IS COMPUTABLE $\Leftrightarrow$

3.4.4. $$C(A\restriction_n) \leq C(n) + O(1) \quad \forall n$$

THERE ARE ONLY $O(2^d)$ MANY A S.T.

$C(A\restriction_n) \leq C(n) + d \quad \forall n$.

SIMILARLY: A IS COMPUTABLE $\Leftrightarrow$

$\exists$ INFIN. COMP. SET X S.T.

$C(A\restriction_n) \leq C(n) + O(1) \quad \forall n \in X$.

PREFIX-FREE MACHINES

$A \subseteq 2^{<\omega}$ IS PREFIX-FREE IF IT IS ANTICHAIN WITH RESP. TO NATURAL PARTIAL ORDERING OF $2^{<\omega}$.

$\sigma \in A$ & $\sigma < \tau \Rightarrow \tau \notin A$.

PREFIX-FREE FUNCTION / MACHINE ...

DOMAIN IS PREFIX-FREE

26.09.2011 Mo
PETER CERNO

ALGORITHMIC RANDOMNESS

PARTIAL COMP. PREFIX-FREE $U: 2^{<\omega} \to 2^{<\omega}$ ... UNIV. :
FOR EACH PARTIAL PREFIX-FREE $f: 2^{<\omega} \to 2^{<\omega}$
$\exists \rho_f : \forall \sigma [U(\rho_f \sigma) \simeq f(\sigma)]$.

... WE FIX UNIVERSAL PREFIX-FREE ORACLE M. $\mathcal{U}$
WE ALSO FIX THE ENUMERATION $\psi_0, \psi_1, \ldots$
OF ALL PARTIAL COMP. PREFIX-FREE FUNCTIONS ...

PREFIX-FREE KOLMOGOROV COMPLEXITY :

$$K(\tau) \overset{def.}{:=} C_{\mathcal{U}}(\tau).$$

$\lhd$: IF $h: 2^{<\omega} \to 2^{<\omega}$ IS COMPUTABLE THEN
3.5.4 $K(h(\sigma)) \leq K(\sigma) + O(1)$

$$K_s(\sigma) \overset{def.}{:=} \min \{ |\tau| : \mathcal{U}(\tau)[s] \downarrow = \sigma \}$$

WE ASSUME THAT $K_s(\sigma)$ IS ALWAYS DEFINED ...
(SINCE $K(\sigma) \leq 2|\sigma| + c$)

$\lhd$ $K_s(\sigma)$ IS COMPUTABLE,
$K_s(\sigma) \geq K_{s+1}(\sigma)$
$K(\sigma) = \lim_s K_s(\sigma)$

THERE IS NO PARTIAL COMP. f WITH
UNBOUNDED RANGE S.T. $f(\sigma) \leq K(\sigma)$
WHENEVER $f(\sigma)\downarrow$.

THE KC THEOREM

THEOREM (KC) 3.6.1. LET $(d_i, \tau_i)_{i\in\omega}$ BE A COMPUTABLE SEQ. OF PAIRS (REQUESTS) WITH $d_i \in \mathbb{N}$ AND $\tau_i \in 2^{<\omega}$ SUCH THAT $\sum_i 2^{-d_i} \leq 1$. THEN THERE EXISTS A PREFIX-FREE MACHINE M AND STRINGS σ_i OF LENGTH d_i S.T. $M(\sigma_i) = \tau_i$ $\forall i$ AND $\operatorname{dom} M = \{\sigma_i : i \in \omega\}$. MOREOVER, INDEX OF $(d_i, \tau_i)_{i\in\omega}$ $\xrightarrow{\text{EFFECTIVELY}}$ INDEX OF M

FOR EACH $n \geq 0$ DEFINE x^n TO BE:

$$0.x_1^n \ldots x_m^n := 1 - 2^{-d_0} - 2^{-d_1} - \ldots - 2^{-d_n}$$

INVARIANT FOR EACH $n \geq 0$:

FOR EACH k : $x_k^n = 1$ ... STRING μ_k^n, $|\mu_k^n| = k$

$S_n := \{\sigma_i : i \leq n\} \cup \{\mu_k^n : x_k^n = 1\}$

IS PREFIX-FREE

FOR $n = 0$:

$\sigma_0 = 0^{d_0}$ $\qquad 1 - 2^{-d_0} = 0.\overbrace{111\ldots1}^{d_0}$

$\Rightarrow x_k^0 = 1 \iff 1 \leq k \leq d_0$

WE DEFINE $\mu_k^0 = 0^{k-1}1$ FOR $\forall\ 1 \leq k \leq d_0$

26.09.2011 Mo
PETER ČERNO

ALGORITHMIC RANDOMNESS

ASSUME THAT $S_n = \{\sigma_i : i \leq n\} \cup \{\mu_k^n : x_k^n = 1\}$
IS PREFIX-FREE.

CASE 1 : $x^n_{d_{n+1}} = 1$

THEN x^{n+1} IS THE SAME AS x^n, EXCEPT $x^{n+1}_{d_{n+1}} = 0$

LET: $\sigma_{n+1} := \mu^n_{d_{n+1}}$

$\mu_k^{n+1} := \mu_k^n$ FOR ALL $k \neq d_{n+1}$

APPARENTLY $S_{n+1} = S_n$ ... PREFIX-FREE

CASE 2 : $x^n_{d_{n+1}} = 0$

FIND THE LARGEST $j < d_{n+1}$: $x_j^n = 1$

x^{n+1} IS THE SAME AS x^n EXCEPT
FOR POSITIONS $j, \ldots, d_{n+1}$:
$x_j^{n+1} = 0$ AND $x_k^{n+1} = 1$ FOR $j < k \leq d_{n+1}$.

LET: $\sigma_{n+1} := \mu_j^n \, 0^{d_{n+1}-j}$

$\mu_k^{n+1} := \mu_j^n \, 0^{k-j-1} 1$ FOR $j < k \leq d_{n+1}$

$\mu_k^{n+1} := \mu_k^n$ FOR $k < j$ OR $k > d_{n+1}$

S_{n+1} IS THE SAME S_n, EXCEPT μ_j^n IS REPLACED
BY A PAIRWISE INCOMP. SET OF SUPERSTRINGS. $\square$

CORRORLARY : LET $(d_i, \tau_i)_{i\in\omega}$ BE A KC SET.

3.6.2 THEN $K(\tau_i) \leq d_i + O(1)$.

$\lhd$ $\sum_{\sigma\in 2^{<\omega}} 2^{-K(\sigma)} \leq 1$

3.7.1

$\mathcal{U}$ IS PREFIX-FREE $\Rightarrow \sum_{\sigma\in 2^{<\omega}} 2^{-K(\sigma)} < \sum_{\tau\in \mathrm{dom}\,\mathcal{U}} 2^{-|\tau|} \leq 1$. $\square$

$\lhd$ $K(\tau) \leq |\tau| + 2\log|\tau| + O(1)$

$\lhd$ $\forall d\ \exists\sigma :\ K(\sigma) > |\sigma| + \log|\sigma| + d$

IF $K(\sigma) \leq |\sigma| + \log|\sigma| + d\ \ \forall\sigma$, THEN

$$\sum_{\sigma} 2^{-K(\sigma)} \geq \sum_{|\sigma|>0} \frac{2^{-|\sigma|-d}}{n} = \sum_{n>0} 2^n \frac{2^{-n-d}}{n} = \infty . \quad \square$$

$\lhd$ LET $f : 2^{<\omega} \to \mathbb{N} :\ \sum_{\sigma\in 2^{<\omega}} 2^{-f(\sigma)} = \infty$

$\Rightarrow K(\sigma) > |\sigma| + f(\sigma)$ FOR ∞-MANY σ.

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

26.09.2011 M.
PETER ČERNO

ALGORITHMIC RANDOMNESS

COUNTING THEOREM 3.7.6

(i) $\max\{K(\sigma) : |\sigma| = n\} = n + K(n) \pm O(1)$

(ii) $|\{\sigma : |\sigma| = n \ \&\ K(\sigma) \leq n + K(n) - r\}| \leq$

$\leq 2^{n-r+O(1)}$ ⟶ DOES NOT DEPEND ON n, r

DEF. 3.7.7 : INFORMATION CONTENT MEASURE (I.C.M.)
IS A PARTIAL FUNC. $F : 2^{<\omega} \to \mathbb{N}$:

1. $\sum_{F(\sigma)\downarrow} 2^{-F(\sigma)} \leq 1$
2. $\{(\sigma, k) : F(\sigma) \leq k\}$ IS C.E.

WE CAN ENUMERATE I.C.M.s $F_0, F_1, \ldots$

MINIMAL I.C.M.

$$\hat{K}(\sigma) := \min_{F_k(\sigma)\downarrow} \{F_k(\sigma) + k + 1\}$$

FOR ANY I.C.M. F : $\hat{K}(\sigma) \leq F(\sigma) + O(1)$

IN PARTICULAR $\hat{K}(\sigma) \leq K(\sigma) + O(1)$.

⊲ 3.7.8 $\{(k+1, \sigma) : F(\sigma) \leq k\}$ IS KC SET

$\Rightarrow K(\sigma) \leq F(\sigma) + O(1) \quad \forall \sigma \in \mathrm{dom}\, F$.

PROOF OF $K(\sigma) \leq |\sigma| + K(|\sigma|) + O(1)$:

$$\sum_\sigma 2^{-(|\sigma| + K(|\sigma|))} = \sum_n 2^n 2^{-(n+K(n))} = \sum_n 2^{-K(n)} \leq 1$$

$\Rightarrow \sigma \mapsto |\sigma| + K(|\sigma|)$ IS I.C.M.

$\Rightarrow K(\sigma) \leq |\sigma| + K(|\sigma|) + O(1)$. $\square$

PROOF OF COUNTING THEOREM (ii) :

LET $F(n) := \lceil -\log(\sum_{\sigma \in 2^n} 2^{-K(\sigma)}) \rceil$.

THEN $2^{-F(n)} = \Theta(\sum_{\sigma \in 2^n} 2^{-K(\sigma)})$ AND

$$\sum_n 2^{-F(n)} \leq \sum_n \sum_{\sigma \in 2^n} 2^{-K(\sigma)} = \sum_{\sigma \in 2^{<\omega}} 2^{-K(\sigma)} \leq 1,$$

$\{(n,k) : F(n) \leq k\}$ IS C.E. $\Rightarrow$ F IS I.C.M.

BY MINIMALITY OF K $\exists c$ S.T. $K(n) \leq F(n) + c$

$\Rightarrow 2^{-K(n)} \geq 2^{-F(n)-c} \geq \varepsilon \sum_{\sigma \in 2^n} 2^{-K(\sigma)}$ (FOR $\varepsilon = 2^{-c-1}$)

SUPPOSE THAT THERE ARE MORE THAN $2^{n-r+O(1)}$ STRINGS $\sigma \in 2^n$ S.T. $K(\sigma) \leq n + K(n) - r$, I.E. FOR $S_{n,r} = \{\sigma \in 2^n : K(\sigma) \leq n + K(n) - r\}$ WE HAVE $|S_{n,r}| \geq f(n,r) 2^{n-r}$, f IS UNBOUNDED

THEN $2^{-K(n)} \geq \varepsilon \sum_{\sigma \in 2^n} 2^{-K(\sigma)} \geq \varepsilon \sum_{\sigma \in S_{n,r}} 2^{-K(\sigma)} \geq$

$\geq \varepsilon \cdot f(n,r) 2^{n-r} \cdot 2^{-n-K(n)+r} = \varepsilon f(n,r) 2^{-K(n)}$. $\lightning$ $\square$

<u>CORROLARY</u> : $\exists c : \quad 2^{-K(n)} \geq 2^{-c-1} \sum_{\sigma \in 2^n} 2^{-K(\sigma)} \quad \forall n$.

27.09.2011 Tu
PETER ČERNO

ALGORITHMIC RANDOMNESS

Q: IS THERE A COMPUTABLE UPPER BOUND ON $K(\sigma)$ THAT IS ACHIEVED INFINITELY OFTEN?

THEOREM (SOLOVAY): THERE IS A COMPUTABLE
3.12.1
$g : 2^{<\omega} \to \mathbb{N}$ SUCH THAT:

(i) $K(\sigma) \leq g(\sigma)$ FOR ALL σ, AND

(ii) $K(\sigma) = g(\sigma)$ FOR INFINITELY MANY σ.

PROOF. CONSTRUCT A PREFIX-FREE MACHINE M S.T.:

IF s IS LEAST S.T. $\mathcal{U}(\tau)[s] = n$, THEN $M(\tau)\downarrow = \langle n, s \rangle$.

THERE IS $c \in \mathbb{N}$ S.T. $\exists \mu, |\mu| \leq |\tau| + c : \mathcal{U}(\mu)\downarrow = \langle n, s \rangle$.

DEFINE COMPUTABLE f: $\mathcal{U}(\mu)[f(s)]\downarrow = \langle n, s \rangle$

$\Rightarrow$ IF s IS LEAST S.T. $K(n) = K_s(n)$, THEN

$K_{f(s)}(\langle n, s \rangle) \leq K(n) + c.$ $|\tau|$

DEFINE $\hat{g}(x) := K_{f(s)}(x)$, WHERE $x = \langle n, s \rangle$

CLEARLY $\hat{g}(x) \geq K(x)$ FOR ALL x.

CONSIDER INFINITELY MANY $x = \langle n, s \rangle$ S.T. $K(n) = K_s(n)$,

$\hat{g}(x) = K_{f(s)}(x) \leq K(n) + c \leq K(x) + O(1)$.

$\Rightarrow \exists d \in \mathbb{N}$: $\hat{g}(x) - d = K(x)$ ∞-MANY TIMES

AND $\hat{g}(x) - d < K(x)$ FINITELY MANY T.

DEFINE $g(x) := \hat{g}(x) - d$ AND RESOLVE.

$\square$

$\triangleleft$) 3.12.2 $f : \mathbb{N} \to \mathbb{N}$ COMPUTABLE. FOLLOWING ARE EQ.:

(i) $K(n) \leq f(n) + O(1)$

(ii) $\sum_n 2^{-f(n)} < \infty$

(i) $\Rightarrow$ (ii) TRIVIAL: $\sum_n 2^{-K(n)} \leq 1$

(ii) $\Leftarrow$ (i) FROM MINIMALITY OF K AS I.C.M. $\square$

DEF. 3.12.3 COMPUTABLE $f : \mathbb{N} \to \mathbb{N}$ IS A SOLOVAY FUNCTION, IF

$$\sum_n 2^{-f(n)} < \infty \quad \text{AND} \quad \liminf_n f(n) - K(n) < \infty$$

I.E. $\exists c \in \mathbb{N} : \exists^\infty n : f(n) \leq K(n) + c$.

MEASURES OF RELATIVE RANDOMNESS

K-REDUCIBILITY: $A \leq_K B \Leftrightarrow K(A\restriction_n) \leq K(B\restriction_n) + O(1)$.

SOLOVAY REDUCIBILITY

α IS SOLOVAY REDUCIBLE (S-RED., $\alpha \leq_S \beta$) IF $\exists c$ AND PARTIAL COMP. $f : \mathbb{Q} \to \mathbb{Q}$:

IF $q \in \mathbb{Q}$ AND $q < \beta$, THEN $f(q)\downarrow < \alpha$ AND $\alpha - f(q) < c(\beta - q)$.

$\triangleleft$): LET $q_0 < q_1 < \dots \to \alpha$, $r_0 < r_1 < \dots \to \beta$ BE COMP. SEQUENCES OF RATIONALS

$\alpha \leq_S \beta \Longleftrightarrow \exists c$ AND COMP. g S.T.

$$\alpha - q_{g(n)} < c(\beta - r_n).$$

27.09.2011 Tu
PETER ČERNO

ALGORITHMIC RANDOMNESS

SOLOVAY REDUCIBILITY IMPLIES K-RED. (C-RED.)

LEMMA 9.1.3 $\forall k \in \mathbb{N}\ \exists c_k \in \mathbb{N}$:

$\forall n \in \mathbb{N}\ \forall \sigma, \tau \in 2^n$ IF $|0.\sigma - 0.\tau| < 2^{k-n}$

THEN $C(\sigma) = C(\tau) \pm c_k$, $K(\sigma) = K(\tau) \pm c_k$.

FIX k. FOR $\sigma \in 2^n$ THE SIZE OF

$S = \{\tau \in 2^n : |0.\sigma - 0.\tau| < 2^{k-n}\}$ DEPENDS ONLY ON k

WE CAN DESCRIBE $\tau \in S$ BY GIVING σ AND POSITION

$\Rightarrow C(\tau) \leq C(\sigma) + O(1) \dots$ $\square$

THEOREM 9.1.4: $\alpha \leq_S \beta \Rightarrow \alpha \leq_C \beta$, $\alpha \leq_K \beta$.

LET c AND f PROVE $\alpha \leq_S \beta$ AND $c + 2 < 2^k$.

DEFINE $\beta_n := 0.\beta\restriction_n$, $\alpha_n := 0.\alpha\restriction_n$

$\beta - \beta_n \leq 2^{-n} \Rightarrow \alpha - f(\beta_n) < c2^{-n}$

LET $\tau_n \in 2^n$ S.T. $|0.\tau_n - f(\beta_n)| < 2^{-n}$.

$|\alpha_n - 0.\tau_n| \leq |\alpha - \alpha_n| + |\alpha - f(\beta_n)| + |0.\tau_n - f(\beta_n)| <$

$2^{-n} + c2^{-n} + 2^{-n} = (c+2)2^{-n} < 2^{k-n}$.

$\Rightarrow K(\alpha\restriction_n) \leq K(\tau_n) + O(1)$

τ_n CAN BE OBTAINED FROM $f(\beta_n)$

$\Rightarrow K(\alpha\restriction_n) \leq K(\beta\restriction_n) + O(1)$. $\square$

IF $\alpha \leq_S \beta$ THEN $\alpha \leq_T \beta$.

DEF. HALTING PROBABILITY Ω OF $\mathcal{U}$
3.13.6 IS $\mu([\![\mathrm{dom}\,\mathcal{U}]\!]) = \sum_{\sigma \in \mathrm{dom}\,\mathcal{U}} 2^{-|\sigma|}$

: IF α IS LEFT-C.E. REAL THEN $\alpha \leq_S \Omega$.
9.2.1

LEMMA THE FOLLOWING ARE EQUIVALENT:
5.1.5 + 5.1.11

(i) THE REAL α IS LEFT-C.E.
(ii) $\exists$ COMP. SEQ. OF RATIONALS $q_0 < q_1 < \dots \to \alpha$
(iii) $\exists$ COMP. SEQ. OF RAT. $r_0, r_1, \dots$: $\alpha = \sum_n r_n$.
(iv) $\exists$ PREFIX-FREE M : $\alpha = \mu([\![\mathrm{dom}\, M]\!])$
(v) $\exists$ PREFIX-FREE C.E. $A \subset 2^{<\omega}$: $\alpha = \sum_{\sigma \in A} 2^{-|\sigma|}$
(vi) $\exists$ PREFIX-FREE COMP. —‖—
(vii) $\exists$ Σ^0_1 CLASS C : $\alpha = \mu(C)$
(viii) $\exists$ Π^0_1 CLASS P S.T. α IS THE LEAST ELEM. OF P
(ix) $\exists$ COMP. TREE T S.T. α IS THE LEFTMOST PATH
...

LET α BE A LEFT-C.E. REAL, M BE A PREFIX-FREE S.T. $\alpha = \mu([\![\mathrm{dom}\, M]\!])$, τ BE S.T. $\mathcal{U}(\tau\sigma) = M(\sigma)$. IF WE CAN APPROXIMATE Ω WITHIN $2^{-(|\tau|+n)}$ THEN WE CAN APPROXIMATE α TO WITHIN 2^{-n}.
$\square$

IF $\Omega \leq_S \alpha \overset{9.1.4}{\Rightarrow} \alpha$ IS 1-RANDOM.

SUCH LEFT-C.E. R. α IS CALLED Ω-LIKE

27.09.2011 Tu
PETER ČERNO

ALGORITHMIC RANDOMNESS

KUČERA-SLAMAN THEOREM: IF LEFT-C.E. α IS 1-RANDOM THEN IT IS Ω-LIKE.

LET β BE LEFT-C.E. REAL. WE SHOW $\beta \leq_S \alpha$.
DEFINE ML-TEST U_n:
STAGE s: IF $\alpha_s \in U_n[s]$ ... DO NOTHING
OTHERWISE LET t BE THE LAST PREVIOUS STAGE AT WHICH WE PUT ANYTHING INTO U_n (OR $t=0$)
PUT INTERVAL $(\alpha_s, \alpha_s + 2^{-n}(\beta_s - \beta_t))$ INTO U_n
WE HAVE $\mu(U_n) \leq 2^{-n}\beta$ ... ML-TEST
$\exists n: \alpha \notin U_n$ ... LET $s_0, s_1, \dots$ BE STAGES AT WHICH WE PUT SOMETHING INTO U_n
THEN FOR $i > 0$: $\alpha_{s_{i+1}} - \alpha_{s_i} > 2^{-n}(\beta_{s_i} - \beta_{s_{i-1}})$ ... □

THEOREM 9.4.1: LET f BE A COMP. FUNCTION.
THEN THE FOLLOWING ARE EQUIV.:
(i) f IS A SOLOVAY FUNCTION.
(ii) $\sum_n 2^{-f(n)}$ IS A 1-RANDOM REAL.

CORROLARY: $\exists$ NONDECREASING SOLOVAY FUNCTION

TAKE COMP. SEQ. $\{r_n\}_{n\in\omega}$ $r_n = 2^{-k_n}$, $k_0 < k_1 < \dots$
S.T. $\sum_n r_n$ IS 1-RANDOM.
LET $f(n) = -\log(r_n) = k_n$ ... □

LEMMA 9.15.1: IF $K^X(A\upharpoonright n) \leq K^X(n) + O(1)$ FOR ALL $n \in S$, S IS INFINITE THEN $A \leq_T S \oplus X'$.

LET $T = \{\sigma : \forall \tau \preceq \sigma (|\tau| \in S \Rightarrow K^X(\tau) \leq K^X(|\tau|) + c)\}$

T IS $(S \oplus X')$-COMPUTABLE TREE, $A \in [T]$

BY RELATIV. COUNT. THEOR. T HAS BOUNDED WIDTH

$\Rightarrow$ A IS ISOLATED PATH ... $(S \oplus X')$-COMPUTABLE. □

DEF. 10.3.2 Y IS LOW FOR 1-RANDOMNESS REDUCIBLE TO X (LR-REDUCIBLE TO X)

$Y \leq_{LR} X$ IF FOR ALL Z:

Z IS X-1-RANDOM $\Rightarrow$ Z IS Y-1-RAND.

THEOREM 10.5.1: THE FOLLOWING ARE EQUIVALENT:

(i) $A \leq_{LR} B$

(ii) FOR EVERY $\Sigma_1^{0,A}$ CLASS T^A, $\mu(T^A) < 1$
$\exists$ $\Sigma_1^{0,B}$ CLASS V^B, $\mu(V^B) < 1$, $T^A \subseteq V^B$

(iii) FOR SOME U^A OF UNIVERSAL ML-TEST
$\exists$ $\Sigma_1^{0,B}$ CLASS V^B, $\mu(V^B) < 1$, $U^A \subseteq V^B$.

A IS LOW FOR K REDUCIBLE TO B (LK-RED.)

$A \leq_{LK} B$ IF $K^B(\sigma) \leq K^A(\sigma) + O(1)$

THEOREM 10.5.9: $A \leq_{LR} B \Leftrightarrow A \leq_{LK} B$. ($\Leftarrow$ IS TRIVIAL)

27.09.2011 Tu
PETER ČERNO

ALGORITHMIC RANDOMNESS

K-TRIVIALITY

RECALL CHAITIN'S THEOREM:

A IS COMPUTABLE $\iff C(A\restriction_n) \leq C(n) + O(1)$

THEOREM (CHAITIN): (CORROLARY OF L. 9.15.1)

11.1.1 IF $K(A\restriction_n) \leq K(n) + O(1)$, THEN A IS Δ^0_2.

..

11.1.3 IF $K(A\restriction_n) \leq K(n) + O(1)$ $\forall n \in S$ ... INFINITE

THEN $A \leq_T S \oplus \emptyset'$

FOR EACH c THERE ARE $O(2^c)$ SETS A SUCH THAT $K(A\restriction_n) \leq K(n) + c$ $\forall n$.

DEF.: A IS K-TRIVIAL IF $K(A\restriction_n) \leq K(n) + O(1)$.

11.1.4 ⊲: IF $K(A\restriction_n) \leq K(n) + O(1)$ $\forall n \in S$ INF. COMPUT.

$\Rightarrow$ A IS K-TRIVIAL.

APPARENTLY: $K(A\restriction_n) \leq K(A\restriction_{h(n)}) + O(1) \leq K(h(n)) + O(1) \leq K(n) + O(1)$. □

THEOREM (ZAMBELLA): THERE IS A

11.1.5 NONCOMPUTABLE K-TRIVIAL C.E. SET.

WE DEFINE NONCOMP. C.E. SET A AND KC SET L

AT STAGE s:

IF WE SEE A SHORTER σ WITH $\mathcal{U}(\sigma)[s]\downarrow = n$

WE ENUMERATE REQUEST $(|\sigma|+1, A_s\upharpoonright_n)$ INTO L

IF THERE IS n AND e $(s > n > 2e)$ S.T. :

$W_{e,s} \cap A_s = \emptyset$, $n > 2e$, $n \in W_{e,s}$, AND

$\sum_{n<j\leq s} 2^{-K_s(j)} \leq 2^{-(e+2)}$, THEN :

WE ENUMERATE n TO A, I.E. $A_{s+1}(n) \neq A_s(n)$

AND THEN FOR EACH j WITH $n < j \leq s$,

FOR THE CURRENTLY SHORTEST $\mathcal{U}$-PROGRAM σ_j FOR j,

WE ALSO ENUMERATE REQUEST $(|\sigma_j|+1, A_{s+1}\upharpoonright_j)$ TO L.

CLEARLY A IS C.E.

SINCE $\lim_m \sum_{j\geq m} 2^{-K(j)} = 0$, IF W_e IS INFINITE,

THEN $A \cap W_e \neq \emptyset$.

SINCE A IS COINFINITE, A IS ALSO <u>NONCOMPUTABLE</u>.

THE WEIGHT OF L IS BOUNDED BY

$\sum_{\sigma\in dom\,\mathcal{U}} 2^{-(|\sigma|+1)} + \sum_e 2^{-(e+2)} \leq \frac{1}{2} + \frac{1}{2} = 1$

$\Rightarrow$ BY KC THEOREM, SINCE $(K(n)+1, A\upharpoonright_n) \in L$

WE HAVE $K(A\upharpoonright_n) \leq K(n) + O(1)$. $\square$

<u>COST FUNCTION</u> $c(n,s) = \sum_{n<j\leq s} 2^{-K_s(j)}$

COST OF ENUMERATING n INTO A AT STAGE s.

<u>VARIATIONS</u> : WE CAN MAKE A PROMPTLY SIMPLE, ...

THE CONSTRUCTION DEPENDS ON ORDERING

OF THE SIMPLICITY REQUIREMENTS ...

27.09.2011 Tu
PETER ČERNO

ALGORITHMIC RANDOMNESS

SOLOVAY FUNCTIONS AND K-TRIVIALITY

RECALL: SOLOVAY FUNCTION IS A COMP. FUNC. S.T. $\sum_n 2^{-f(n)} < \infty$ AND $\exists^\infty n : f(n) \leq K(n) + O(1)$.

$\lhd$: SUPPOSE THAT FOR $\forall$ COMP. f S.T. $\sum_n 2^{-f(n)} < \infty$
11.1.7 $\exists$ COMP. g S.T. $\sum_\sigma 2^{-g(\sigma)} < \infty$ & $g(A\upharpoonright_n) \leq f(n) + O(1)$.
THEN A IS COMPUTABLE.

LET f BE A SOLOVAY FUNCTION.
$\Rightarrow \exists$ COMP. g S.T. $\sum_\sigma 2^{-g(\sigma)} < \infty$ & $g(A\upharpoonright_n) \leq f(n) + c$.
LET d BE S.T. $K(\sigma) \leq g(\sigma) + d$
LET e BE S.T. $\exists^\infty n : f(n) \leq K(n) + e$
FOR ANY SUCH n:

COUNTING T. 3.7.6

$|\{\tau \in 2^n : g(\tau) \leq f(n) + c\}| \leq$
$|\{\tau \in 2^n : K(\tau) \leq K(n) + c + d + e\}| \leq 2^{c+d+e+O(1)}$

Π^0_1 CLASS $\{X \in 2^\omega : \forall n : g(X\upharpoonright_n) \leq f(n) + c\}$
HAS AT MOST $2^{c+d+e+O(1)}$ ELEMENTS $\Rightarrow$ ALL ARE COMP. $\square$

WE CAN USE SOLOVAY FUNCTIONS TO CHARACTERIZE K-TRIVIALITY.

THEOREM 11.1.8: A IS K-TRIVIAL $\Leftrightarrow$ FOR ALL COMP. f S.T. $\sum_n 2^{-f(n)} < \infty$: $K(A\upharpoonright_n) \leq f(n) + O(1)$.

$\Rightarrow$) RECALL L. 3.12.2: FOR ALL COMP. f
$\sum_n 2^{-f(n)} < \infty \Leftrightarrow K(n) \leq f(n) + O(1)$

$\Leftarrow$) LET $\hat{g}$ BE SOLOVAY FUNCTION FROM T. 3.12.1

RECALL: GIVEN n, LET s BE LEAST S.T.: $K_s(n) = K(n)$. THEN $\hat{g}(\langle n,s\rangle) \leq K(n) + O(1)$

LET A BE S.T. $K(A\upharpoonright_n) \leq \hat{g}(n) + O(1)$.
GIVEN n LET s BE LEAST S.T. $K_s(n) = K(n)$
LET $m = \langle n,s\rangle$. SINCE n CAN BE COMP. FROM m:
$K(A\upharpoonright_n) \leq K(A\upharpoonright_m) + O(1) \leq \hat{g}(m) + O(1) \leq K(n) + O(1)$.
$\Rightarrow$ A IS K-TRIVIAL. $\square$

THE FOLLOWING ARE EQUIV. FOR A COMP. g:

(i) g IS A SOLOVAY FUNC.

(ii) A IS K-TRIVIAL $\Leftrightarrow$ $K(A\upharpoonright_n) \leq g(n) + O(1)$.

(WITHOUT PROOF ...)

LET $KT(c) := \{A : \forall n\ K(A\upharpoonright_n) \leq K(n) + c\}$

LET $G(c) = |KT(c)|$. IT CAN BE SHOWN THAT:

THEOREM: $\lim_c G(c)/2^c = 0$, $\sum_c G(c)/2^c < \infty$

THEOREM: $G \not\leq_T \emptyset'$.

27.09.2011 Tu
PETER ČERNO

ALGORITHMIC RANDOMNESS

LOWNESS

IN COMPUTABILITY : A IS LOW IF $A' \equiv_T \emptyset'$

EQUIVALENTLY : A IS LOW IF $\Delta_2^{0,A} = \Delta_2^0$.

GENERALIZATION : A IS LOW FOR $\mathcal{C}$ IF $\mathcal{C}^A = \mathcal{C}$

DEF 11.2.1 : A IS LOW FOR R-RANDOMNESS $\Leftrightarrow$ EVERY R-RANDOM SET IS R-RAND. RELAT. TO A

DEF 11.2.2. : A IS LOW FOR R-TESTS IF EVERY R-TEST RELATIVE TO A IS COVERED BY AN UNRELATIVIZED R-TEST.

A IS LOW FOR MARTIN-LÖF TESTS $\Leftrightarrow$
A IS LOW FOR 1-RANDOMNESS.

DEF 11.2.3 : A IS LOW FOR K $\Leftrightarrow$ $K(\sigma) \leq K^A(\sigma) + O(1)$.

THEOREM : A IS LOW FOR K $\Rightarrow$ A IS K-TRIVIAL.

$K(A\upharpoonright_n) \leq K^A(A\upharpoonright_n) + O(1) \leq K(n) + O(1)$. $\square$

THEOREM : A IS LOW FOR K $\Rightarrow$ A IS LOW FOR 1-RAND.

X IS 1-RANDOM $\Rightarrow$ $K^A(X\upharpoonright_n) \geq K(X\upharpoonright_n) - O(1) \geq n - O(1)$. $\square$

A IS LOW FOR 1-RAND. $\Leftrightarrow$ $A \leq_{LR} \emptyset$

A IS LOW FOR K $\Leftrightarrow$ $A \leq_K \emptyset$? $\square$