Kalibrace náhodnosti

Antonín Kučera

KTIML, MFF UK

4.12.2012

Matematický pojem náhodnosti je vždy relativní !

Algoritmická náhodnost - náhodnost relativní vzhledem k určité třídě algoritmů a vzhledem k jejich určitému specifickému použití

Filozofický pojem náhodnosti je problém ontologický
(různé varianty Boží existence)

Historicky:

von Mises (1916) - jako pokus o základ teorie pravděpodobnosti

Hlavní přístupy

1. stochastičnost (frekvenční stabilita)
2. chaotičnost (Kolmogorovská složitost)
3. typičnost (teorie míry, martingaly)

Různé varianty v každém přístupu (kalibrace dle jejich síly).

1. Stochastičnost

Stochastičnost posloupnosti nul a jedniček (stochastičnost množiny) znamená vlastnost frekvenční stability nejenom pro tuto posloupnost, ale také pro všechny její podposloupnosti získané pomocí "admissible place selection rules"

Příklad: 010101010.....

(sudá část jsou samé nuly, lichá část samé jedničky)

Tento přístup k náhodnosti je technicky komplikovaný

2. Chaotičnost

Hlavní idea: nestlačitelnost (incompressibility)

"náhodný" ("random") znamená "incompressible"

Dvě hlavní varianty Kolmogorovské složitosti:

- plain Kolmogorov complexity (C)
- prefix-free Kolmogorov complexity (K)

Plain Kolmogorov complexity

(Solomonoff 1960, Kolmogorov 1963-1965, Chaitin 1966)

$C(x) = min\{|y| : y \text{ je popisem (kódem) } x\} \quad (x, y \in 2^{<\omega})$

$C = C_f$ závisí na kódovací (popisovací) funkci f

Pro univerzální Turingův stroj U :
C_U je aditivně optimální pro všechny částečně rekurzivní funkce f
(tzn. efektivně vyčíslitelné funkce f)

Prefix-free Kolmogorov complexity

(Chaitin, Levin)

Vážné námitky k "plain" Kolmogorovské složitosti
napřed lze přečíst řetízek (string) y, zjistit jeho délku (tzn. $|y|$) a potom přečíst znovu a zjistit jeho obsah (y)
to dohromady dává $|y| + log|y|$ bitů

řešení: prefix-free kódování (bezprefixová metoda popisů, kódů)

žádný kód není začátkem jiného kódu
self-delimiting kódování

$K(x) = min\{|y| : y \text{ je popisem (kódem) } x\} \quad (x, y \in 2^{<\omega})$

$K = K_f$ závisí na prefix-free kódovací funkci f
(bezprefixové kódovací metodě f)

Existuje univerzální prefix-free Turingův stroj U (univerzální pro prefix-free Turingovy stroje, prefix-free částečně rekurzivní funkce)

K_U je aditivně optimální pro všechny prefix-free částečně rekurzivní funkce (tzn. efektivně vyčíslitelné funkce, které jsou prefix-free)

Theorem

$K(x) \leq |x| + 2log(|x|) + O(1) = |x| + 2log(|x|) + const.$

Poznámka

Pro oba typy Kolmogorovské složitosti,
plain C i prefix-free K jsou různé varianty:

- omezení výpočtové síly - různé "resource bounded" varianty (například omezení času výpočtu)
- zvětšení výpočtové síly - algoritmy (Turingovy stroje) s orákuly (kódovací metoda s nápovědou orákula)

Náhodnost v polynomiální, aritmetické, hyperaritmetické hierarchii atd.

Příklady: Π^1_1-náhodnost, Δ^1_2, Σ^1_2-náhodnost

Opět: kalibrace náhodnosti podle síly použitých prostředků

Kolmogorovská složitost je definována na konečných řetízcích (konečných posloupnostech nul a jedniček) !

Otázka: jak použít na nekonečné posloupnosti 0 a 1
tzn. na množiny ?

Intuitivní pokus: množina A (nekonečná posloupnost 0 a 1)
je náhodná jestliže každý začátek A délky n
(označován: $A \upharpoonright n$)
nelze popsat kódem kratší délky než n (minus konstanta)
tzn. nestlačitelnost popisů (kódů) začátků A (tzn. $A \upharpoonright n$).

Spravná idea, ale má drobnou vadu !!

Potíže s "plain" Kolmogorovskou složitostí:
obsah y plus informace o jeho délce dávají $|y| + log|y|$ bitů

Theorem (Martin-Löf)

Neexistuje žádná množina A pro kterou $C(A \upharpoonright n) \geq n + const.$ pro všechna n.

Řešení je snadné: bezprefixové kódování !
(bez triků s obsahem a navíc ještě délkou řetízku)

Definice

Množina A je (Chaitin) náhodná jestliže $K(A \upharpoonright n) \geq n + const.$ pro všechna n.

Poznámka

Tato definice vymezuje velmi robustní pojem.
Robustnost je mimo jiné vidět z mnoha ekvivalentních charakterizací (např. pomocí teorie míry) - viz dále.

3. Typičnost

Přístup, který používá pojem míra (je "measure-theoretic")
(Solovay, Schnorr, ..., Demuth, ...)

Fakt: znalost jednoho bitu dané množiny (posloupnosti) znamená, že umíme nalézt třídu míry $1/2$ ve které tato množina leží.
Znalost n bitů vede na třídu míry 2^{-n}

Idea: nepatřit do žádné třídy efektivně míry nula
(to avoid all effectively null classes)
("null" znamená mít Lebesgueovu míru nula)

Různé úrovně pojmu "efektivně" míry nula, což opět vede ke kalibraci náhodnosti.

Definice

Třída množin (posloupností 0 a 1) $\mathcal{A} \subseteq 2^\omega$
je ML-null, (ML=Martin-Löf), tzn. má ML-míru nula,
jestliže existuje efektivně vyčíslitelná posloupnost efektivně otevřených tříd B_n (nazývaných ML-test) taková, že

- $\mu(B_n) < 2^{-n}$, pro všechna n
- $\mathcal{A} \subseteq \bigcap_n B_n$

Množina A je ML-náhodná (nebo také 1-náhodná)
jestliže $\{A\}$ není ML-null.

Theorem (Martin-Löf)

Existuje univerzální (maximální) ML-test $\{U_n\}$.
To znamená, že $\bigcap_n U_n$ *je maximální (největší) třída ML-míry nula a dále, že množina* A *je* 1*-náhodná právě když* $A \notin \bigcap_n U_n$.

Ekvivalence obou přístupů (nestlačitelnost a non míra nula).

Theorem (Schnorr)

Množina A *je* 1*-náhodná (tzn. ML-náhodná) právě když* A *je Chaitin-náhodná.*

Poznámka

To ukazuje robustnost pojmu 1-náhodnosti.

$A \notin \bigcap_n U_n$ právě když $K(A \upharpoonright n) \geq n + const.$ (pro všechna n)

(kde $\{U_n\}$ je univerzální ML-test).

Alternativní přístup k teorii míry je založen na pojmu martingalu. (Ville, 1939).

Poznámka

Neformálně: Martingal odpovídá strategii sázek v kasinu.

Problém: Jak zbohatnout? Jak libovolně zvětšit kapitál?
Lze zbohatnout proti náhodné posloupnosti ?

Definice

Martingal je funkce $F : 2^{<\omega} \to Q^+ \cup \{0\}$ (nebo $R^+ \cup \{0\}$), která splňuje pro každé $\sigma \in 2^{<\omega}$ tzv. průměrující podmínku

$$F(\sigma) = \frac{F(\sigma 0) + F(\sigma 1)}{2}$$

Martingal F :

uspěje na množině A jestliže $\limsup_{n\to\infty} F(A \upharpoonright n) = +\infty$

uspěje na $\mathcal{A} \subseteq 2^\omega$ jestliže uspěje na každé množině $A \in \mathcal{A}$.

$S[F]$ (the success set) je třída množin, na kterých martingal F uspěje.

Základní věta (alternativní přístup k teorii míry):

Theorem (Ville, 1939)

Třída $\mathcal{A} \subseteq 2^\omega$ je null (tzn. $\mathcal{A}$ má Lebesgueovu míru nula) právě když existuje martingal, který uspěje na $\mathcal{A}$.

Kalibrace martingalů dle jejich síly (opět) vede na kalibraci pojmu náhodnosti.

Martingaly jsou také velmi důležité při studiu slabších (jemnějších) variant 1-náhodnosti: míra a Hausdorffova dimense v (slabých) třídách složitosti, např. v polynomiální hierarchii (J. Lutz).

Definice

Pro třídu Δ martingalů: množina (posloupnost 0 a 1) A je Δ-náhodná, jestliže žádný Δ-martingal neuspěje na A.

Intuitivně: pomocí Δ strategie nelze proti A zbohatnout.

Příklady:
efektivně vyčíslitelné (computable) martingaly, rekurzivně spočetné martingaly, relativizované martingaly s orákuly (s nápovědou), resource-bounded martingaly (polynomiální čas, ...), ...

Tvrzení

1-náhodnost je ekvivalentní náhodnosti relativně vzhledem ke třídě všech rekurzivně spočetných martingalů

(opět: robustnost pojmu náhodnosti)

POKROČILEJŠÍ ČÁST

VČETNĚ NOVÝCH VÝSLEDKŮ

Definice [Chaitin: Ω-number]

$$\Omega_U = \sum_{U(\sigma)\downarrow} 2^{-|\sigma|} = \mu(dom(U))$$

pro univerzální prefix-free Turingův stroj U.

Ω-number je tzv. halting probablity, tzn. pravděpodobnost, s jakou se univerzální prefix-free Turingův stroj U zastaví na náhodném vstupu.

Theorem (Chaitin)

Ω_U je 1-náhodná (pro libovolný univerzální prefix-free Turingův stroj U).

Problém: a halting probability vs. the halting probability
(analogicky jako: a halting problem vs. the halting problem)

Je dobře známo, že všechny halting problémy jsou stejné až na rekurzivní izomorfii. Zde jsou všechny halting pravděpodobnosti stejné při tzv. Solovay-převeditelnosti (analytický pojem, bez detailů).

Theorem (Chaitin, Calude, Hertling, Khoussainov, Wang, Kučera - Slaman)

Všechny Ω_U jsou "stejné" (Solovay-úplné) a jsou to právě všechna zleva-rekurzivně spočetná (left-c.e.) 1-náhodná realná čísla (pro všechny univerzální prefix-free Turingovy stroje U).

Zajímavý problém: kódování informace do chaosu (do nějaké náhodné množiny) ?
Lze něco do 1-náhodných množin kódovat? Pokud ano, co přesně a do jakých 1-náhodných množin?

Theorem (Kučera-Gács)

Každá množina je T-převeditelná na (zakódovatelná do, vyčíslitelná s pomocí) nějaké 1-náhodné množiny.

Kódovací metoda do 1-náhodných množin je založena na slabší formě "Gödelova fenoménu neúplnosti".
Gödelova metoda je efektivizací paradoxu lháře!

Slavná forma "Gödelova self-referenčního principu":

v aritmetice: já jsem nedokazatelná formule
v náhodnosti: já nemám malou míru.

Vada: toto kódování poskytuje 1-náhodné množiny, které jsou složitější než halting problém (jsou "nad ním"). To není ta pravá náhodnost, za kterou se považují ty množiny, které nejsou nad halting problémem (T-neúplné).

Speciální důležitý případ: které rekurzivně spočetné množiny jsou kódovatelné do T-neúplných 1-náhodných množin?

Slavný dlouho otevřený problém
Letos se po mnoha letech podařilo vyřešit - viz dále.
(Bienvenu, Day, Greenberg, Kučera, Miller, Nies, Turetsky)

Algoritmická slabost

Existuje několik pojmů algoritmické (výpočetní) slabosti ve vztahu k 1-náhodnosti.

Definice

Množina A je

1. "low" pro 1-náhodnost tzn., jestliže každá 1-náhodná množina je také 1-náhodná relativně vzhledem k A
2. K-triviální jestliže pro všechna n, $K(A \upharpoonright n) \leq K(0^n) + const.$
3. "low" pro K jestliže pro všechny $\sigma \in 2^{<\omega}$, $K(\sigma) \leq K^A(\sigma) + const.$
4. "basis" pro 1-náhodnost, jestliže $A \leq_T Z$ pro nějakou množinu Z takovou, že Z je 1-náhodná relativně k A.

Poznámka

C-triviálnost: $C(A \upharpoonright n) \leq C(0^n) + const.$
Chaitin dokázal, že všechny C-triviální množiny jsou rekurzivní (algoritmicky rozhodnutelné)

Překvapivě toto neplatí pro K-triviálnost.
Existují nerekurzivní K-triviální množiny !

Solovay: komplikovaná konstrukce
Později, několik krátkých a elegantních konstrukcí dokonce rekurzivně spočetných (nerekurzivních) množin, které jsou K-triviální, low pro 1-náhodnost, low pro K, basis pro 1-náhodnost

Všechny dle stejného triku: do what is cheap

Podobnost těchto konstrukcí není náhodná!

Theorem (Nies, Hirschfeldt, Stephan)

Všechny čtyři třídy ($\mathcal{K} = \mathcal{L} = \mathcal{M} = \mathcal{B}$) *jsou stejné.*

Čtyři různé charakterizace stejné třídy !

Nicméně, tyto charakterizace mají různě silný informační obsah.
(Tyto charakterizace nejsou efektivně ekvivalentní!)

Theorem (Hirschfeldt, Nies, Stephan)

Jediné rekurzivně spočetné množiny, které jsou zakódovatelné do T-neúplných 1-náhodných množin jsou K-triviální!

Slavný dlouho otevřený problém:

Jsou všechny K-triviální množiny zakódovatelné do (vyčíslitelné relativně s pomocí) nějaké T-neúplné 1-náhodné množiny ?

Řešení: ANO, ale v obecném případě jenom do velmi mála z nich!

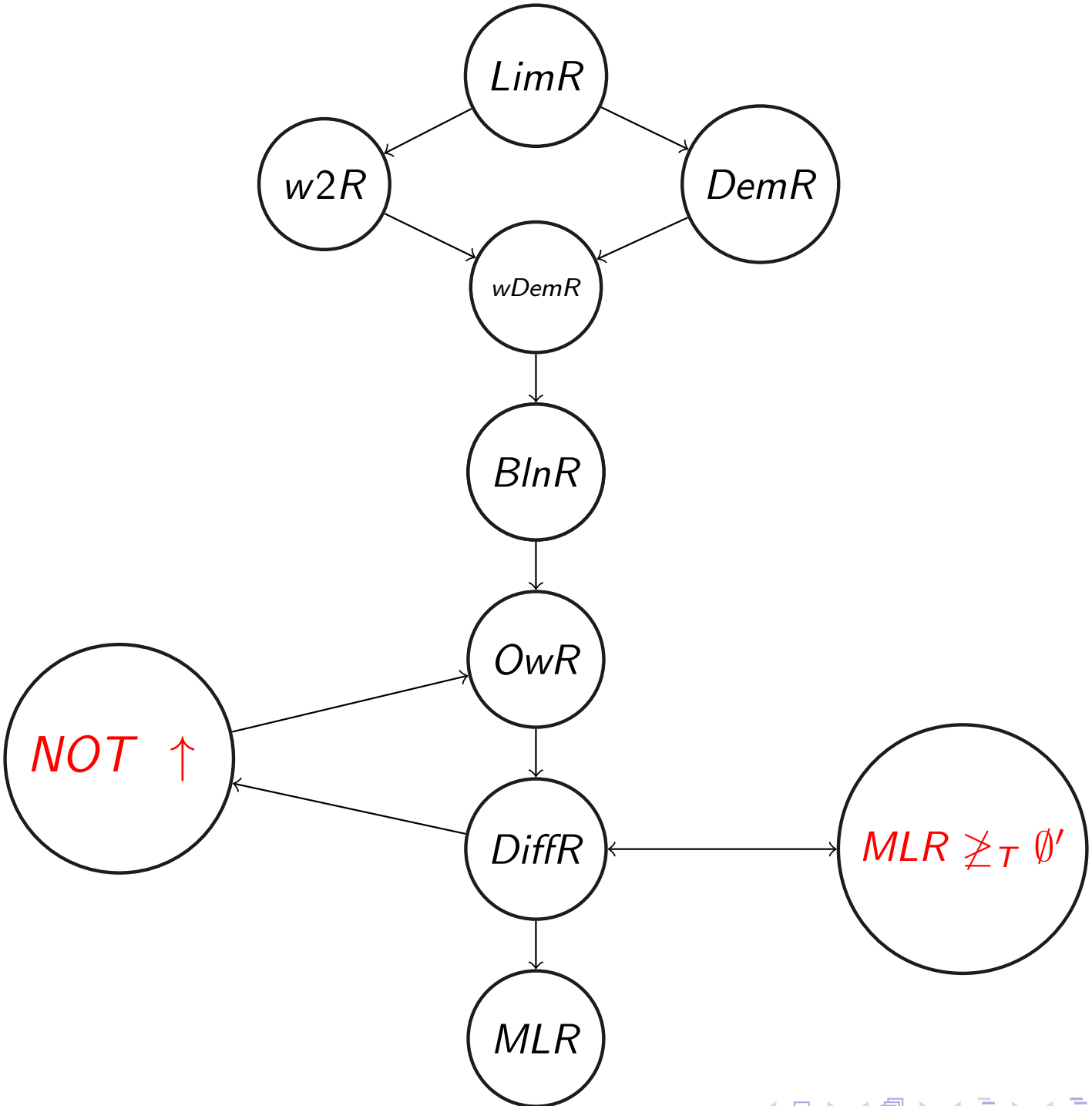
Theorem (Bienvenu, Day, Greenberg, Kučera, Miller, Nies, Turetsky)

K-triviální množiny jsou právě ty množiny, které jsou zakódovatelné do (vyčíslitelné relativně s pomocí) nějaké T-neúplné 1-náhodné množiny.

Poznámka

V obecném případě pouze do takových, které nejsou Oberwolfach náhodné (nově vzniklý pojem).

Poděkování : Research in pairs in Oberwolfach (2012).


LimR
w2R
DemR
wDemR
BlnR
OwR
NOT ↑
DiffR
MLR ≱T ∅′
MLR

Řešení nespočívá v nalezení triku.
Řada dílčích vysledků mnoha lidí dohromady vedla k výsledku překvapivě silnému a matematicky hezkému (s určitou symetrií).

Theorem

- *Každá K-triviální množina je zakódovatelná do (vyčíslitelná relativně s pomocí) libovolné 1-náhodné množiny, která není OW-náhodná,*
- *lépe to obecně nejde (non-OW nelze zeslabit)*
- *existují T-neúplné 1-náhodné množiny, které nejsou OW-náhodné.*

Řešení používá různé efektivní analogy známých vět, např.

- diferencovatelnost funkcí, motto: hezké funkce jsou diferencovatelné "skoro všude",
  kalibrace efektivnosti efektivně vyčíslitelných funkcí a kalibrace pojmu "skoro všude"
- Lebesqueovu větu o hustotě
  měřitelné množiny mají - skoro všude - ve svých bodech hustotu 1

- Přehledový článek:
  Downey, Hirschfeldt, Nies, Stephan : Calibrating randomness
  Bull. Symb. Logic. 12 no 3 (2006) 411-491

- Dvě nové výborné kniky (monografie):

  - Downey, Hirschfeldt : Algorithmic randomness and complexity
    SPRINGER 2010

  - A. Nies: Computability and randomness
    OXFORD UNIVERSITY PRESS 2008

DĚKUJI ZA POZORNOST