

Kolmogorovská zložitost

17.10.2013

Theorem (C nie je rekurzívna...)

Funkcia $C(x)$ **nie je rekurzívna**. Navyše, **neexistuje čiastočne rekurzívna** fcia Φ definovaná na nekonečnej množine, ktorá je na celom svojom definičnom obore s $C(x)$ totožná.

SPORom

- Φ PRF definovaná na nekonečnej množine, A nekonečná rekurzívna podmnožina $D(\Phi)$

- $\Psi(m) = \min\{x : C(x) \geq m, x \in A\}$ je totálna rekurzívna

// $\Phi(x) = C(x)$ na A

- $C(\Psi(m)) \geq m$

- $C(\Psi(m)) \leq C_\Psi(\Psi(m)) + c_\Psi, \quad C_\Psi(\Psi(m)) \leq I(m)$

// $\Psi(m) = x : C(x) \geq m$

$$m \leq C(\Psi(m)) \leq C_\Psi(\Psi(m)) + c_\Psi \leq I(m) + c_\Psi$$



Theorem (C sa dá aproximovať..)

Existuje *totálna rekurzívna fcia* $\Phi(t, x)$ *monotónne klesajúca v* t *taká, že* $\lim_{t \rightarrow \infty} \Phi(t, x) = C(x)$

- $C(x) \leq I(x) + c$
- **každý program** p , $I(p) \leq I(x) + c$ **necháme bežať** t **krokov** a definujeme

$$\Phi(t, x) = \begin{cases} \min\{I(p) : p \text{ zastal a vygeneroval } x\}, & \text{ak existuje} \\ I(x) + c & \text{inak} \end{cases}$$



Pre dané x, t **NEVIEME rozhodnúť, či** $\Phi(t, x) = C(x)$

Def. (limita $\Phi(t, x)$)

Nech $g = g_1, g_2, \dots$ je postupnosť funkcií. Funkcia f je limitou postupnosti g ak $f(x) = \lim_{t \rightarrow \infty} g_t(x)$

Limita je **rekurzívne uniformná**, ak \exists totálna rekurzívna fcia $t(\epsilon)$

$$|f(x) - g_{t(\epsilon)}(x)| \leq \epsilon \quad \forall x$$

$$\Psi = \Psi_1, \Psi_2, \dots \quad \Psi_t(x) = \Phi(t, x)$$

- $C(x)$ JE limitou Ψ
- $C(x)$ NIE JE rekurzívnou limitou Ψ

lebo z problému zastavenia

$$\forall \epsilon, t \text{ existuje nekonečne veľa } x : |C(x) - \Psi_t(x)| > \epsilon$$

vlastnosti C

C je "spojitá" $\exists c : |C(x) - C(x \pm h)| \leq 2l(h) + c$

\Leftrightarrow ak máme program pre x , stačí povedať $\pm h$

C je "logaritmická"

$\Leftrightarrow C(x) \leq l(x) + c$

$\Leftrightarrow \forall k$ je počet x dĺžky n s $C(x) < \log x - k$ nanajvýš 2^{n-k}

"fluktuácia" C

$\forall x \exists x_1, x_2 : |x_i - x| \leq \sqrt{x}$, pričom

1. $C(x_1) \geq I(x)/2 - c$
 2. $C(x_2) \leq I(x)/2 + c$
2. nestlačiteľné $x = x''x'$; $I(x'') = I(x') = n/2 \rightsquigarrow$
 $x_2 = x''0^{n/2}$

$$C(x_2) \leq I(x)/2 + c \sim C(x)/2$$

1. stlačiteľné x ; $C(x) = o(I(x)) \rightsquigarrow$ spodné bity nahradí
 nestlačiteľný $y = y_1 \dots y_{n/2}$
 $x_1 = x''y \quad C(y) \geq I(y) + c = I(x)/2 + c$

Čo vieme o dlhých zložitých behoch...

1 $\forall c \exists d$: neexistuje d po sebe idúcich c -nestlačiteľných čísel

2 $\forall d \exists c$: existuje d po sebe idúcich c -nestlačiteľných čísel

Lemma

$\forall c \exists d$: *neexistuje d po sebe idících c -nestlačitelných čísel*

Majme x c – nestlačitelné $C(x) > l(x) - c$
 uvažujme $x, x + 1, \dots, x + \Delta$, $x + \Delta = i \underbrace{0 \dots 0}_j$:

$$\left. \begin{array}{l} C(x + \Delta) \leq l(i) + l(j) + c \\ l(i) + l(j) + \text{const} < l(x) - c \end{array} \right\} \text{stačí } l(j) + \text{const} < c$$

Lemma

$\forall d \exists c$: *existuje d po sebe idúcich c -nestlačiteľných čísel*

zoberme **k -nestlačiteľné** x $C(x) > I(x) - k$

zo spojitosti: $\forall |x - y| \leq k : |C(x) - C(y)| \leq 2I(k) + \delta$

$$C(x) - 2I(k) - \delta \leq C(y) \quad \vee \quad C(y) - 2I(k) - \delta \leq C(x)$$

$$I(x) - \underbrace{(k + 2I(k) + \delta)}_c < C(y)$$



Example

$x = x_1 \dots x_n$ - v náhodnom reťazci je počet 0 a 1 "podobný"

$$f_n = \sum_{i=1}^n x_i$$

$g(n, m) = g$, pričom g je najmenšie také, aby # binárnych reťazcov, pre ktoré to platí, bol nanajvyš 2^{n-m}

$$\text{TEST : } V_m = \{x \in \{0, 1\}^n : |2f_n - n| > g(n, m)\}$$

Definition (Efektívny test náhodnosti?)

Nech P je rekurzívne rozdelenie pravdepodobnosti na priestore \mathbb{N} .
 Totálna funkcia $\delta : \mathbb{N} \rightarrow \mathbb{N}$ je **P-test (Martin-Löf)**, ak

- 1 $V = \{(m, x) : \delta(x) \geq m\}$ je rekurzívne vyčísliteľná
- 2 $\sum_x \{P(x | l(x) = n), \delta(x) \geq m\} \leq 2^{-m} \quad \forall n$

\hookrightarrow kritické regióny $V_m = \{x : \delta(x) \geq m\}$ sú vnorené a enumerovateľné

rovnomerné rozdelenie

$$L(x) = 2^{-2l(x)-1}$$

$$L_n(x) = \begin{cases} 2^{-n}, & l(x) = n \\ 0 & \text{inak} \end{cases}$$

2. \rightsquigarrow

$$\sum_{x \in V_m} L_n(x) \leq 2^{-m} \quad \rightsquigarrow \quad d(\{x : l(x) = n, x \in V_m\}) \leq 2^{n-m}$$

Example

$x = 1x_21x_41x_6 \dots$ nie je náhodné vzhľadom k rovnomernému rozdeleniu

$$\delta(x) = \begin{cases} \max\{i : x_1 = x_3 = x_5 = \dots = x_{2i-1} = 1\}, & x_1 \neq 0 \\ 0, & x_1 = 0 \end{cases}$$

δ je TEST:

- 1 δ je rekurzívne vyčísliteľná
- 2 kritický región je malý (2^{-m})

ak $\delta(x) = m, l(x) = n \geq 2m - 1$, tak máme

$$\begin{cases} 2^{m-1} & \text{možností } (2m-1)\text{-dlhého prefixu} \\ 2^{n-(2m-1)} & \text{zvyškov} \end{cases}$$

$$d(\{x : \delta(x) \geq m, l(x) = n\}) = 2^{m-1} \cdot 2^{n-(2m-1)} = 2^{n-m}$$

Definition

univerzálny P-test je test $\delta_0(\cdot|P)$ taký, že ku každému P-testu δ existuje konštanta c_P taká, že $\forall x \delta_0(x|P) \geq \delta(x) - c_P$

binárny reťazec je náhodný vzhľadom k univerzálnemu P-testu, ak je (až na pár výnimiek) náhodný vzhľadom k ľubovoľnému testu

$$\begin{aligned} \delta_0(\cdot|P) \quad U_m &= \{(m, x) : \delta_0(x|P) \geq m\} \\ \delta \quad V_m &= \{(m, x) : \delta(x) \geq m\} \end{aligned}$$

$$V_{m+c} \subseteq U_m$$

Ukážeme, že **univerzálny test existuje**

- 1 P-testy vieme enumerovať
- 2 iteratívna definícia univerzálného P-testu

P-testy vieme enumerovať

zmena enumerácie Φ_1, Φ_2, \dots PRF na enumeráciu $\delta_1, \delta_2, \dots$ P-testov

- $\Phi \rightsquigarrow \Psi$ (indexy vynechané)

Φ, Ψ majú rovnaké obory hodnôt

ak je Ψ_n def $\rightsquigarrow \Psi_1, \dots, \Psi_{n-1}$ tiež def

"dovetail" - postupné simulovanie $\Phi(1), \Phi(2), \dots$

$$\Phi(1)$$

$$\Phi(1) \quad \Phi(2)$$

$$\Phi(1) \quad \Phi(2) \quad \Phi(3)$$

$$\vdots$$

$$\vdots$$

$$\vdots$$

$\Psi(1) = \Phi(i_1)$, kde $\Phi(i_1)$ je prvý výpočet, kt. zostal

...

$\Psi(j) = \Phi(i_j)$, kde $\Phi(i_j)$ je j -ty výpočet, kt. zostal

- pomocou Ψ definujeme test δ aproximovaním zospodu

pomocou Ψ definujeme test δ aproximovaním zospodu

$\delta[1..\infty]$ - pole aktuálnych hodnôt $\delta(1), \delta(2), \dots$

1 $\delta[x] = 0 \quad \forall x; i \leftarrow 0;$

2 $i \leftarrow i + 1$; vypočítaj $\Psi(i)$, nech $\Psi(i) = (m, x)$;

3 if $\delta(x) \geq m$ then goto 2 else $\delta[x] \leftarrow m$;

4 if $\exists k \in \{1, 2, \dots, m\} \quad \sum \{P(y|I(y) = I(x)) : \delta(y) \geq k\} > 2^{-k}$
 then $\delta[x] \leftarrow 0$; halt
 else goto 2.

- 1 $\delta[x] = 0 \quad \forall x; i \leftarrow 0;$
- 2 $i \leftarrow i + 1;$ vypočítaj $\Psi(i)$, nech $\Psi(i) = (x, m);$
- 3 if $\delta(x) \geq m$ then goto 2 else $\delta[x] \leftarrow m;$
- 4 if $\sum\{P(y|l(y) = l(x)) : \delta(y) \geq k\} > 2^{-k}$ pre nejaké $k = 1, 2, \dots, m$
then $\delta[x] \leftarrow 0;$ halt
else goto 2.

- ak je oborom hodnôt Ψ test \rightsquigarrow neskončíme, ale zospodu ho aproximujeme
- ak Ψ diverguje \rightsquigarrow neskončí a nemení vypočítané (je to enumerovateľná mn.)
- ak oborom hodnôt nie je test \rightsquigarrow podmienka v kroku 4. sa niekedy splní a končíme

Ak zbehneme na $\forall \Phi_1, \Phi_2, \dots$, "dostaneme" P-testy $\delta_1, \delta_2, \dots$

Theorem (univerzálny P-test)

Nech $\delta_1, \delta_2, \dots$ je enumerácia P-testov. Potom

$\delta_0(x|P) = \max\{\delta_y(x) - y : y \geq 1\}$ je univerzálny P-test

- $\delta_0(x|P)$ je totálna
- $V = \{(m, x) : \delta_0(x|P) \geq m\}$ je enumerovateľná
- kritické regióny sú dosť malé

$$\begin{aligned} & \sum_{l(x)=n} \{P(x|l(x) = n) : \delta_0(x|P) \geq m\} \\ & \leq \sum_{y=1}^{\infty} \sum_{l(x)=n} \{P(x|l(x) = n) : \delta_y(x) \geq m + y\} \\ & \leq \sum_{y=1}^{\infty} 2^{-m-y} = 2^{-m} \end{aligned}$$

- δ_0 majorizuje aditívne

Theorem (konkrétny univerzálny test)

$\delta_0(x|L) = I(x) - C(x|I(x)) - 1$ je univerzálny L -test pre rovnomerné rozdelenie L .

že je to test

- $\{(m, x) : \delta_0(x|L) \geq m\}$ je enumerovateľná
- $d(\{x : \delta_0(x|L) \geq m\}) \leq 2^{I(x)-m} - 1$

že je univerzálny

- $\forall \delta \exists c \delta_0(x|L) \geq \delta(x) - c$

že $\delta_0(x|L) = I(x) - C(x|I(x)) - 1$ je univerzálny

$A = \{z : \delta(z) \geq \delta(x)\}$ $x \in A(\text{fix}); \delta = \delta_y$ v štandardnom enumerovaní

- $y, I(x), \delta(x) \rightsquigarrow$ vieme enumerovať prvky z A
- plus j -index x v $A \rightsquigarrow$ máme $x \quad //j \leq I(d(A)) \leq I(x) - \delta(x)$
 $s = 0 \dots 01j, \quad |s| = I(x) - \delta(x)$
- $I(x), I(s) \rightsquigarrow$ vieme $\delta(x)$

$$C(x|I(x)) \leq \underbrace{I(x) - \delta(x)}_{I(s)} + \underbrace{2I(y) + 1}_y \quad c = 2I(y) + 2 \quad \square$$

Definition

Vezmime $\delta_0(x|L) = I(x) - C(x|I(x)) - 1$ ako referenčný univerzálny test vzhľadom k uniformnej distribúcii L . Reťazec nazveme **c-náhodný**, ak $\delta_0(x|L) \leq c$

$$C(x|I(x)) \leq C(x) \leq C(x|I(x)) + 2C(I(x) - C(x|I(x))) + O(1)$$

Definition

Nekonečná postupnosť $\in \{0, 1\}^*$ je **normálna**, ak $\forall k$ je frekvencia výskytu bloku y dĺžky k v limite 2^{-k}

- normálna postupnosť nie je nutne náhodná – Champernow
12345678910111213...
- náhodná postupnosť je normálna

v *konečnom prípade* — každý blok **malej** veľkosti sa v ňom vyskytuje **približne rovnako**

$K()$ - prefixná KZ; nateraz

$$C(x|y) \leq K(x|y) \leq C(x|y) + 2 \log(C(x|y)) + 1$$

Definition

Trieda **deficiency funkcií** $\delta : N \rightarrow N$ takých, že

$$K(n, \delta(n)|n - \delta(n)) \leq c_1$$

- $n - \delta(n)$ vieme rozobrať na $n, \delta(n)$ ale aj $n, \delta(n)$ vieme zakódovať do $n - \delta(n)$
- fixneme c_1 tak, aby vyhovovalo pre bežné deficiency: $\log n, \log \log n, \sqrt{n}, \dots$

Bloky v reťazcoch

Theorem \exists konštanta c taká, že \forall deficiency funkciu δ , $\forall n$ a $x \in \{0, 1\}^n$

$$\text{ak } \mathbf{C(x)} \geq \mathbf{n - \delta(n)} \quad \text{tak} \quad \left| \#_1(x) - \frac{n}{2} \right| \leq \sqrt{\frac{3}{2} \frac{(\delta(n)+c)n}{\log e}}$$

Theorem \exists konštanta c taká, že $\forall n$ a $x \in \{0, 1\}^n$

$$\text{ak } \left| \#_1(x) - \frac{n}{2} \right| \leq 2^{-\delta(n)-c} \sqrt{n} \quad \text{tak} \quad \mathbf{C(x)} \leq \mathbf{n - \delta(n)}$$

Theorem \exists konštanta c taká, že $\forall n$ a $x \in \{0, 1\}^n$

$$\text{ak } \left| \#_1(x) - \frac{n}{2} \right| = j \quad \text{tak} \quad \mathbf{C(x|n)} \leq \mathbf{n - 1/2 \log n + K(j|n) + c}$$

Theorem Nech $l(y) = \ell$, $\ell \leq \log n$. \exists konštanta c tak, že $\forall n \forall x \in \{0, 1\}^n$

$$\text{ak } \mathbf{C(x)} \geq \mathbf{n - \delta(n)} \quad \text{potom} \quad \left| \#_y(x) - pn \right| \leq \sqrt{\alpha pn}$$

$$\text{kde } \alpha = \lceil \mathbf{K(y|n) + \log \ell + \delta(n) + c} \rceil 3\ell / \log e$$

Theorem

∃ konštanta c taká, že \forall deficiency funkciu δ , $\forall n$ a $x \in \{0, 1\}^n$

$$\text{ak } C(x) \geq n - \delta(n) \quad \text{tak} \quad \left| \#_1(x) - \frac{n}{2} \right| \leq \sqrt{\frac{3}{2} \frac{(\delta(n) + c)n}{\log e}}$$

Chernoff $\Pr(|S_n - pn| > m) \leq 2e^{-m^2/3pn}$ // mince $p = 1/2$

■ $A = \{x \in \{0, 1\}^n : |\#_1(x) - n/2| > m\}$, $d(A) \leq 2^{n+1}e^{-2m^2/3n}$

■ zvolíme m tak, aby $\frac{2m^2 \log e}{3n} = \delta(n) + c$

■ **popis** x

- selfdelimiting s $n - \delta(n) \rightsquigarrow \delta(n)$, n c_1

- i je index x v A

$$l(i) \leq \log d(A) \leq (n+1) - (2m^2 \log e)/3n = n+1 - \delta(n) - c$$

$$|0 \dots 0s_i| = n+1 - \delta(n) - c + c_1$$

$$C(x) \leq C_T(x) + c_T \leq n+1 - \delta(n) - c + c_1 + c_T$$

pre $c = c_1 + c_T + 2$ $C(x) < n - \delta(n)$ [Spor]

$$|\#_1(x) - n/2| \leq m \quad \square$$

Theorem

∃ konštanta c taká, že $\forall n$ a $x \in \{0, 1\}^n$

$$\text{ak } \left| \#_1(x) - \frac{n}{2} \right| \leq 2^{-\delta(n)-c} \sqrt{n} \text{ tak } C(x) \leq n - \delta(n)$$

- **Zvolíme** $m = 2^{-\delta(n)-c} \sqrt{n}$
- $A = \{x \in \{0, 1\}^n : |\#_1(x) - n/2| \leq m\}$
 $d(A) \leq (m+1) \binom{n}{n/2} \leq c_2 \frac{2^n m}{\sqrt{n}}$ Stirling $n! \approx \sqrt{2\pi n} (n/e)^n$
- i je index x v A
 určenie $A : n, m, \delta(n) \rightsquigarrow n - \delta(n), c_1$
 $C_T(x) = \log(d(A)) + c_1 = n - \delta(n) - c_1 + \log c_2$
 $C(x) \leq C_T(x) + c_T \leq n - \delta(n)$

Theorem

Existuje konštanta c taká, že $\forall n$ a $x \in \{0, 1\}^n$

$$\text{ak } \left| \#_1(x) - \frac{n}{2} \right| = j \text{ tak } C(x|n) \leq n - 1/2 \log n + K(j|n) + c$$

- $A = \{x \in \{0, 1\}^n : |\#_1(x) - n/2| = j\}$

- $d(A) \leq 2 \binom{n}{n/2} \leq c_3 \frac{2^n}{\sqrt{n}}$

- i je index x v A
 –enumerácia $A \rightsquigarrow j, n, d(A)$

$$C_T(x|n) \leq \log d(A) + K(j|n) \leq n - 1/2 \log n + \log c_3 + K(j|n)$$

$$C(x|n) \leq C_T(x|n) + c_T \leq n - 1/2 \log n + K(j|n) + c$$

Theorem

Nech $l(y) = \ell$, $\ell \leq \log n$. Existuje konštanta c tak, že $\forall n \forall x \in \{0, 1\}^n$

ak $C(x) \geq n - \delta(n)$ potom $|\#_y(x) - pn| \leq \sqrt{\alpha pn}$

kde $\alpha = [K(y|n) + \log \ell + \delta(n) + c]3\ell / \log e$

Nech dĺžka x , $l(x) = n$, je násobkom dĺžky y , $l(y) = \ell$

$$n = N\ell$$

■ x ako cyklický kruh, ℓ rôznych delení $\#_y(x, i)$ neprekrývajúce sa výskyty

■ $A = \{x \in \{0, 1\}^n : |\#_y(x, i) - pN| > m\}$

■ $d(A) \leq 2^{n+1} e^{-m^2/3pN}$

zvolíme m tak aby $\frac{m^2 \log e}{3pN} = K(\langle y, i \rangle | n) + \delta(n) + c$

■ enumerácia A $i, y, m \rightsquigarrow K(\langle y, i, \delta(n), n \rangle | n - \delta(n)) \leq K(\langle y, i \rangle | n) + c_1$

■ index i prvku x v A

$$\log d(A) \leq \log(2^{n+1} e^{-m^2/3pN}) = n+1 - \frac{m^2 \log e}{3pN} \leq n+1 - K(\langle y, i \rangle | n) - \delta(n) - c$$

$$C(x) \leq C_T(x) + c_T \leq n+1 - \delta(n) - c + c_1 + c_T$$

$$\text{pre } c = c_1 + c_T + 2 \quad C(x) < n - \delta(n)$$

$$|\#_y(x, i) - pN| \leq m$$



$$|\#_y(x, i) - pN| \leq m \quad \frac{m^2 \log e}{3pN} = K(\langle y, i \rangle | n) + \delta(n) + c$$

- $|\#_y(x, i) - pN| \leq \sqrt{\frac{K(\langle y, i \rangle | n) + \delta(n) + c}{\log e} \cdot 3pN}$
- $K(\langle y, i \rangle | n) \leq K(y | n) + K(i | n) + O(1); \quad K(i | n) \leq \log \ell + O(1)$
- $|\#_y(x) - pn| = \sum_{i=0}^{\ell-1} |\#_y(x, i) - pN| \leq \ell \sqrt{\frac{K(y, |n) + \log \ell + \delta(n) + c}{\log e} \cdot 3p \frac{n}{\ell}}$

$$|\#_y(x) - pn| \leq \sqrt{\alpha pn}, \alpha = [K(y|n) + \log \ell + \delta(n) + c]3\ell / \log e \quad \square$$