Derandomizácia

kuko

21.4.2021

Pokročilá teória zložitosti

Pravdepodobnostné algoritmy

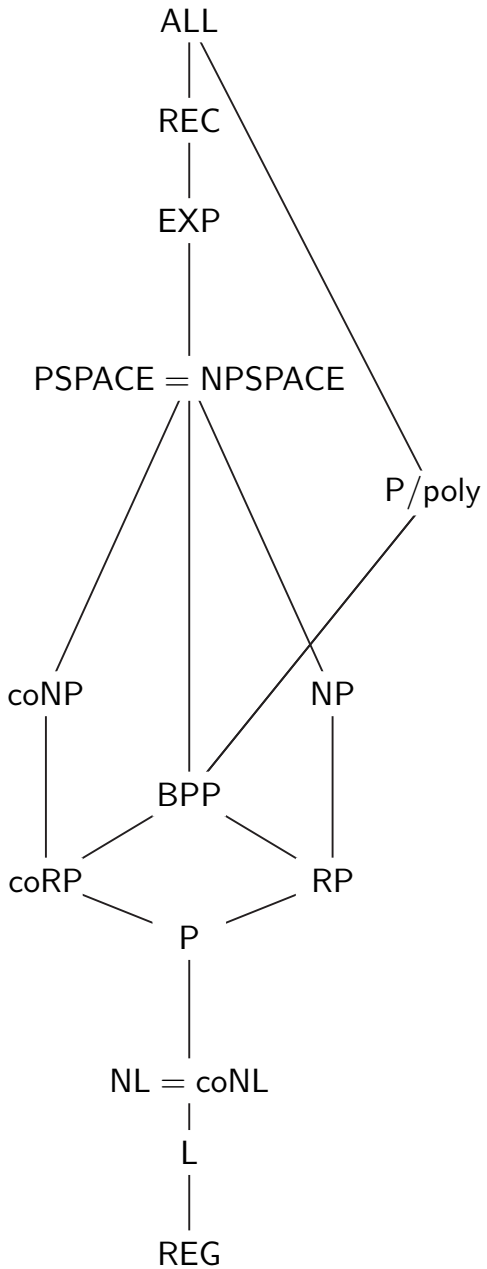
- medián: $1.5n$ vs $> 2n$ porovnaní
- minimálna kostra: $O(m)$ vs $O(m\alpha(n))$
- minimálny rez: $\tilde{O}(n^2)$ vs $O(n^3)$
- test prvočíselnosti: $\tilde{O}(n^2)$ vs $\tilde{O}(n^6)$
- LP: $O(d^2 n + 2^{O(\sqrt{d \log d})})$ vs $O(d^{O(d)} n)$
- 3-SAT: $\tilde{O}(1.308^n)$ vs $\tilde{O}(1.334^n)$
- test rovnosti polynómov: $O(n)$ vs ?

- medián: $1.5n$ vs $> 2n$ porovnaní
- minimálna kostra: $O(m)$ vs $O(m\alpha(n))$
- minimálny rez: $\tilde{O}(n^2)$ vs $O(n^3)$
- test prvočíselnosti: $\tilde{O}(n^2)$ vs $\tilde{O}(n^6)$
- LP: $O(d^2 n + 2^{O(\sqrt{d \log d})})$ vs $O(d^{O(d)} n)$
- 3-SAT: $\tilde{O}(1.308^n)$ vs $\tilde{O}(1.334^n)$
- test rovnosti polynómov: $O(n)$ vs ?

$$(ux+zvy)^2+z(vx-uy)^2 \stackrel{?}{=} (u^2+zv^2)(x^2+zy^2)$$

$$1024x^{10}+(x+\sqrt{3})^{10}+(x-\sqrt{3})^{10}+(\sqrt{3}x+1)^{10}+(\sqrt{3}x-1)^{10}$$

$$\stackrel{?}{=} 1512(x^2+1)^5-1024.$$


ALL
REC
EXP
PSPACE = NPSPACE
P/poly
coNP
NP
BPP
coRP
RP
P
NL = coNL
L
REG

- $P = BPP$?
- $\exists$ dobrý PNG?

- $P = BPP$?
- $\exists$ dobrý PNG?

Definícia

Budeme hovoriť, že funkcia f je

- *ťažká, ak ju obvody veľkosti $S \leq 2^{\gamma n}$ nedokážu spočítať presne (pre nejaké $\gamma > 0$),*
- *veľmi ťažká, ak ju obvody veľkosti $S \leq 2^{\gamma n}$ nedokážu ani len aproximovať na 99% (pre nejaké $\gamma > 0$),*
- *pekelne ťažká, ak ju obvody veľkosti $S \leq 2^{\gamma n}$ nedokážu ani len aproximovať na $1/2 + 1/S$ vstupoch (pre nejaké $\gamma > 0$).*

$$\exists \text{ ťažká funkcia} \Longrightarrow \exists \text{ veľmi ťažká funkcia} \Longrightarrow \exists \text{ pekelne ťažká funkcia}$$
$$\Longrightarrow \exists \text{ dobrý PNG} \Longrightarrow \text{vieme odhadnúť Pr[BPP-alg akceptuje]}$$
$$\Longrightarrow \mathsf{P} = \mathsf{BPP}.$$

Ak $\exists f \in \mathsf{E}$, ktorá potrebuje

$$\text{obvod veľkosti } \left\{ \begin{array}{c} - \\ n^{\omega(1)} \\ 2^{n^{\varepsilon}} \\ 2^{\Omega(n)} \end{array} \right\} \text{ tak } \left\{ \begin{array}{lcc} \mathsf{BPP} & \subseteq & \mathsf{EXP} \\ \mathsf{BPP} & \subseteq & \mathsf{SUBEXP} \\ \mathsf{BPP} & \subseteq & \mathsf{QuasiP} \\ \mathsf{BPP} & = & \mathsf{P} \end{array} \right\}.$$

Pseudonáhodné generátory


TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
NINE NINE NINE NINE NINE NINE
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.
© 2001 United Feature Syndicate, Inc.

batérie štatistických testov:

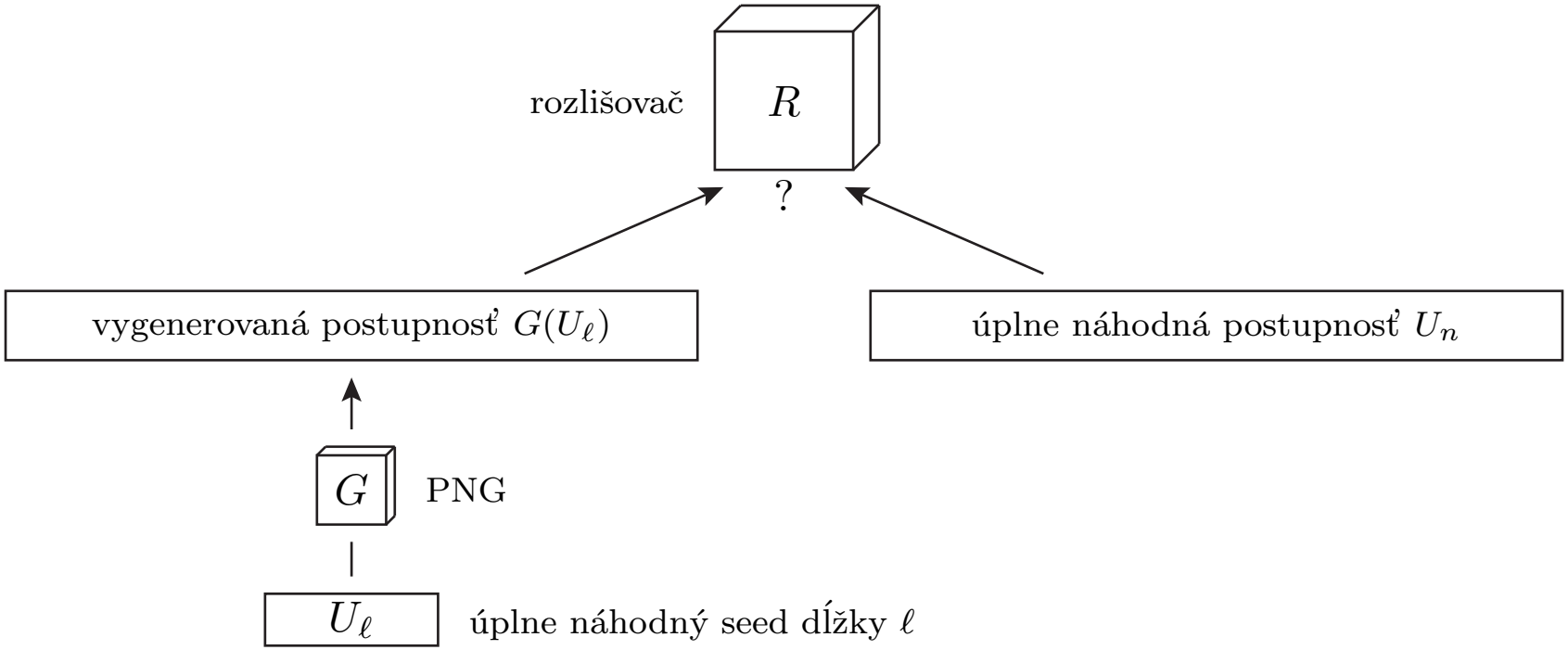
- Diehard
- TestU01
- NIST

- je #núl a jednotiek zhruba rovnaký?
- po blokoch? (podobá sa to na binomické rozdelenie?)
- behov/medzier dĺžky k je zhruba $1/2^k$?

- Gcd test: spustíme Euklidov algoritmus a spočítame
  1. k – počet iterácií
  2. konečnú hodnotu gcd
- z 10M pokusov, očakávame:

k	≤ 3	4	5	6	7	8	9	10	$\cdots$
očak. počet:	5.5	29.5	144.6	590.7	2065	6277	16797	39965	

gcd	1	2	3	4	5	6	7	8	$\cdots$
očak. počet:	6079271	1519817	675474	379954	243171	168869	124067	94989	


rozlišovač
R
?
vygenerovaná postupnosť $G(U_\ell)$
úplne náhodná postupnosť U_n
G
PNG
U_ℓ
úplne náhodný seed dĺžky ℓ

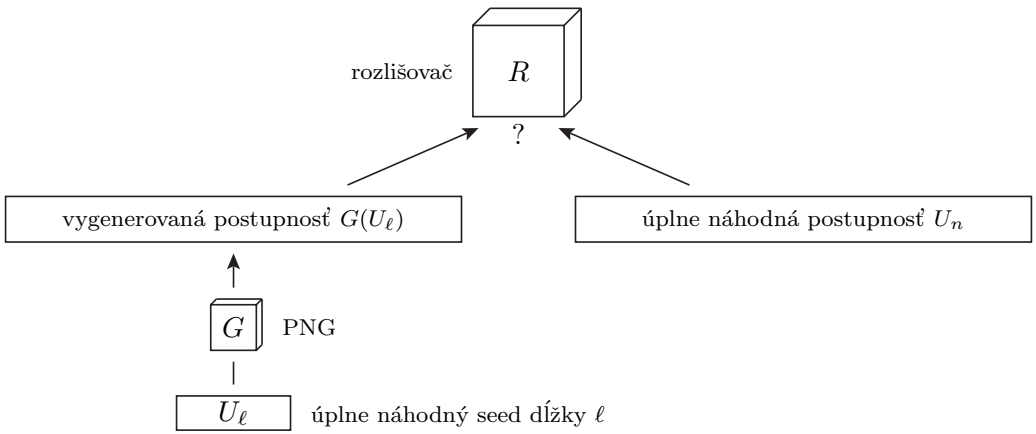
Definícia

R je rozlišovač pre D, ak

$$\left| \Pr_{x \in_R D}[R(x) = 1] - \Pr_{r \in_R U_n}[R(r) = 1] \right| > 1/10,$$

D je S-pseudonáhodná, ak neexistuje rozlišovač veľkosti S. Tzn. $\forall$*obvod C veľkosti S je*

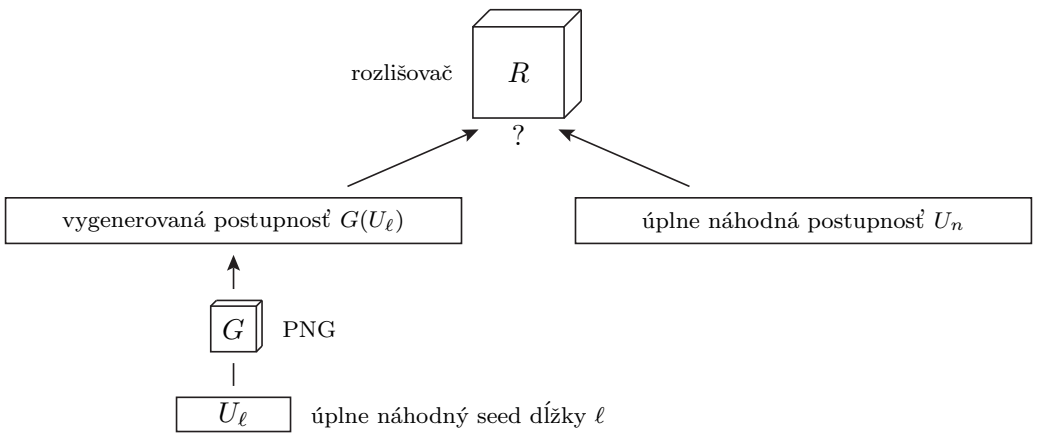
$$\Pr[C(D)] \approx \Pr[C(U_m)] \pm 1/10.$$



Definícia (pseudonáhodný generátor)

$S(\ell)$-pseudonáhodný generátor:

- *funkcia G, v čase $O(2^\ell)$ vyrobí post. dĺžky $S(\ell)$*
- *$G(U_\ell)$ je $S(\ell)^3$-pseudonáhodná distribúcia ($\forall \ell \in \mathbb{N}$)*



- PNG má oveľa viac času ako obvody, ktoré sa ho snažia rozlíšiť

Lema

Ak existuje dobrý PNG, potom vieme derandomizovať.

Lema

Ak existuje $2^{\varepsilon \ell}$*-PNG, potom* $\mathsf{BPP} = \mathsf{P}$.

Dôkaz.

- nech existuje $2^{\varepsilon\ell}$-PNG
- nech $L \in \mathrm{BPP}$
- existuje BPP-algoritmus A
- nahradíme náhodné bity pseudonáhodnými
- keďže G je dobrý PNG, $\forall^\infty x$

$$\Pr[A(x, G(U_\ell))] - \Pr[A(x, U_m)] < 0.1$$

  - v opačnom prípade $r \mapsto A(x, r)$ je obvod, ktorý rozoznáva $G(U_\ell)$ od U_m

- $\Longrightarrow$ stačí A spustiť pre všetky seedy dĺžky $c \log n$ a spočítať väčšinovú odpoveď:

$$\Pr[A(x, G(U_\ell)) = L(x)] \geq 2/3 - 0.1 > 1/2$$

□

Dôkaz.

- nech existuje $S(\ell)$-PNG
- nech $L \in \mathrm{BPTIME}(S(\ell(n)))$
- existuje algoritmus A bežiaci v čase $cS(\ell(n))$
- nahradíme náhodné bity pseudonáhodnými
- keďže G je dobrý PNG, $\forall^\infty x$

$$\Pr[A(x, G(U_\ell))] - \Pr[A(x, U_m)] < 0.1$$

  - v opačnom prípade $r \mapsto A(x, r)$ je obvod, ktorý rozoznáva $G(U_\ell)$ od U_m
- $\Longrightarrow$ stačí A spustiť pre všetky seedy dĺžky $\ell(n)$ a spočítať väčšinovú odpoveď:

$$\Pr[A(x, G(U_\ell)) = L(x)] \geq 2/3 - 0.1 > 1/2$$

□

Lema

Ak existuje $S(\ell)$-PNG, tak $\forall \ell : \mathbb{N} \to \mathbb{N}$[a] je

$$\mathsf{BPTIME}(S(\ell(n))) \subseteq \mathsf{DTIME}(2^{c\ell(n)})$$

pre nejakú konštantu c.

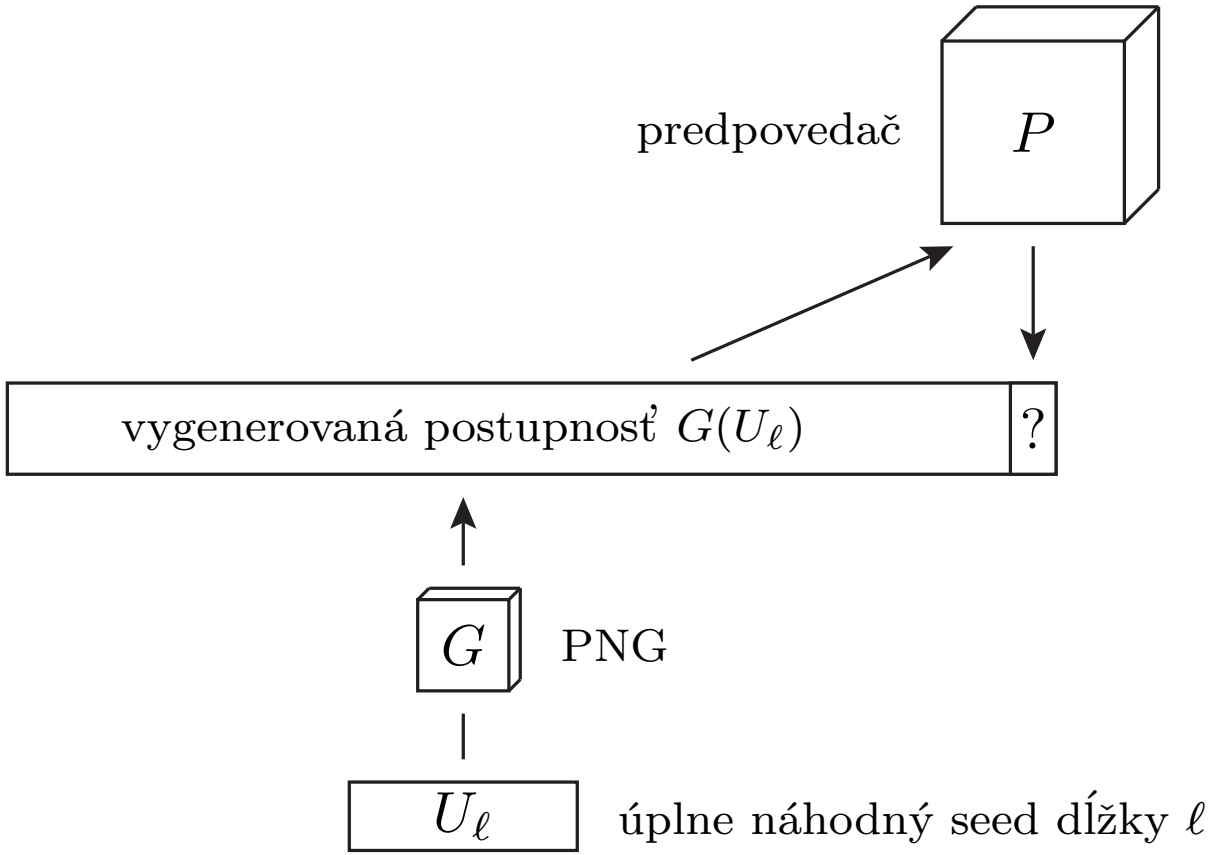
[a] vypočítateľnú v polynomiálnom čase

$\mathrm{BPTIME}(S(\ell(n))) \subseteq \mathrm{DTIME}(2^{c\ell(n)})$

Dôsledok

- $\exists 2^{\varepsilon\ell}$-*PNG* $\Longrightarrow \mathrm{BPP} = \mathrm{P}$
- $\exists 2^{\ell^{\varepsilon}}$-*PNG* $\Longrightarrow \mathrm{BPP} \subseteq \mathrm{QuasiP} = \mathrm{DTIME}(2^{\mathrm{polylog}(n)})$
- $\forall c > 1\ \exists \ell^{c}$-*PNG* $\Longrightarrow \mathrm{BPP} \subseteq \mathrm{SUBEXP} = \bigcap_{\varepsilon>0} \mathrm{DTIME}(2^{n^{\varepsilon}})$

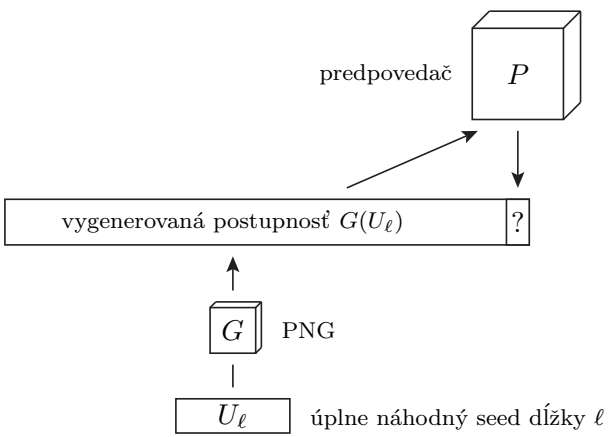
Rozlišovače a predpovedače


predpovedač
P
vygenerovaná postupnosť $G(U_\ell)$
?
G
PNG
U_ℓ
úplne náhodný seed dĺžky ℓ

Definícia

P je predpovedač pre D, ak $\exists i : P$ *dokáže predpovedať i-ty bit z predošlých s výrazne väčšou úspešnosťou ako len náhodné tipovanie:*

$$\Pr_{r \in_R D}[P(r_1, \ldots, r_{i-1}) = r_i] > \frac{1}{2} + \frac{1}{10n}.$$



Veta

Ak $\exists$ rozlišovač R veľkosti S pre $D \Longrightarrow \exists$ predpovedač P veľkosti $2S$.

Dôkaz.

- P na vstupe i, $y_1, \ldots, y_{i-1}$ doplní postupnosť o náhodné $z_i, \ldots, z_m$ a spustí R
- nech $a = R(y_1, \ldots, y_{i-1}, z_i, \ldots, z_m)$.
- ak $a = 1$ (postupnosť vyzerá nenáhodne), odpovie z_i; inak $1 - z_i$

Veta

Ak $\exists$ rozlišovač R veľkosti S pre $D \Longrightarrow \exists$ predpovedač P veľkosti $2S$.

Dôkaz.

- P na vstupe i, $y_1, \ldots, y_{i-1}$ doplní postupnosť o náhodné $z_i, \ldots, z_m$ a spustí R
- nech $a = R(y_1, \ldots, y_{i-1}, z_i, \ldots, z_m)$.
- ak $a = 1$ (postupnosť vyzerá nenáhodne), odpovie z_i; inak $1 - z_i$

Veta

Ak $\exists$ rozlišovač R veľkosti S pre $D \Longrightarrow \exists$ predpovedač P veľkosti $2S$.

■ **Dôkaz.**

- P na vstupe i, $y_1, \ldots, y_{i-1}$ doplní postupnosť o náhodné $z_i, \ldots, z_m$ a spustí R
- nech $a = R(y_1, \ldots, y_{i-1}, z_i, \ldots, z_m)$.
- ak $a = 1$ (postupnosť vyzerá nenáhodne), odpovie z_i; inak $1 - z_i$

Veta

Ak $\exists$ rozlišovač R veľkosti S pre $D \Longrightarrow \exists$ predpovedač P veľkosti $2S$.

■ **Dôkaz.**

- P na vstupe i, $y_1, \ldots, y_{i-1}$ doplní postupnosť o náhodné $z_i, \ldots, z_m$ a spustí R
- nech $a = R(y_1, \ldots, y_{i-1}, z_i, \ldots, z_m)$.
- ak $a = 1$ (postupnosť vyzerá nenáhodne), odpovie z_i; inak $1 - z_i$

- „hybridný argument“: $n+1$ distribúcií

$$D_0, \ldots, D_n$$

- $D_0 = U_n$, $D_n = D$,
- D_i má prvých i bitov z D a zvyšok sú úplne náhodné bity.
- nech $p_i = \Pr[R(D_i)]$
- $p_n - p_0 = \Pr[R(D)] - \Pr[R(U_n)] \geq \frac{1}{10}$
- $p_n - p_0 = \sum p_i - p_{i-1} \Longrightarrow \exists i : p_i - p_{i-1} \geq \frac{1}{10n}$

- „hybridný argument“: $n+1$ distribúcií

$$D_0, \ldots, D_n$$

- $D_0 = U_n$, $D_n = D$,
- D_i má prvých i bitov z D a zvyšok sú úplne náhodné bity.
- nech $p_i = \Pr[R(D_i)]$
- $p_n - p_0 = \Pr[R(D)] - \Pr[R(U_n)] \geq \frac{1}{10}$
- $p_n - p_0 = \sum p_i - p_{i-1} \Longrightarrow \exists i : p_i - p_{i-1} \geq \frac{1}{10n}$

- „hybridný argument“: $n+1$ distribúcií

$$D_0, \ldots, D_n$$

- $D_0 = U_n$, $D_n = D$,
- D_i má prvých i bitov z D a zvyšok sú úplne náhodné bity.
- nech $p_i = \Pr[R(D_i)]$
- $p_n - p_0 = \Pr[R(D)] - \Pr[R(U_n)] \geq \frac{1}{10}$
- $p_n - p_0 = \sum p_i - p_{i-1} \Longrightarrow \exists i : p_i - p_{i-1} \geq \frac{1}{10n}$

- „hybridný argument“: $n+1$ distribúcií

$$D_0, \ldots, D_n$$

- $D_0 = U_n$, $D_n = D$,
- D_i má prvých i bitov z D a zvyšok sú úplne náhodné bity.
- nech $p_i = \Pr[R(D_i)]$
- $p_n - p_0 = \Pr[R(D)] - \Pr[R(U_n)] \geq \frac{1}{10}$
- $p_n - p_0 = \sum p_i - p_{i-1} \Longrightarrow \exists i : p_i - p_{i-1} \geq \frac{1}{10n}$

- P predpovie i-ty bit správne buď ak $a = 1$ a $y_i = z_i$, alebo ak $a = 0$ a $y_i = 1 - z_i$

	Áno	Nie	spolu
$z_i = y_i$	A	B	$1/2$
$z_i \neq y_i$	C	D	$1/2$
spolu	p_{i-1}	$1 - p_{i-1}$	1

$$\mathrm{A} = \Pr[\text{Áno} \mid z_i = y_i] \cdot \Pr[z_i = y_i] = \Pr[R(D_i)] \cdot \tfrac{1}{2} = \tfrac{1}{2} p_i$$

$$\mathrm{A} + \mathrm{C} = \Pr[\text{Áno}] = \Pr[R(D_i)] = p_{i-1}$$

$$\mathrm{C} + \mathrm{D} = \Pr[z_i \neq y_i] = 1/2$$

$$\mathrm{A} + \mathrm{D} = \mathrm{C} + \mathrm{D} - (\mathrm{A} + \mathrm{C}) + 2 \times \mathrm{A} = \frac{1}{2} + p_i - p_{i-1}. \qquad \square$$

Dôsledok

G je $S(\ell)$-PNG, ak $\nexists$ predpovedač veľkosti $2S(\ell)^3$.

Ako vyrobiť PNG?

Rozcvička 1: predĺženie o 1 bit

$$G(z) = z\, f(z)$$

$$\exists P, |P| \leq 2n^3 : \Pr_{z \in_r \{0,1\}^\ell}[P(z) = f(z)] \geq 1/2 + 1/10n \quad \textit{(predpovedač)}$$

$$\forall C, |C| \leq S : \Pr_{z \in_r \{0,1\}^\ell}[C(z) = f(z)] \leq \frac{1}{2} + 1/S \quad \textit{(pekelne ťažká fn)}$$

Rozcvička 2: predĺženie o 2 bity

$$G(z) = z_1 f(z_1) z_2 f(z_2), \qquad \text{kde } z = z_1 z_2$$

ak $\exists P$:

$$\Pr_{z_1, z_2 \in_R \{0,1\}^{\ell/2}}[P(z_1 f(z_1) z_2) = f(z_2)] > \frac{1}{2} + \frac{1}{10n},$$

$$\exists z_1 \in \{0,1\}^{\ell/2} : \Pr_{z_2 \in_R \{0,1\}^{\ell/2}}[P(z_1 f(z_1) z_2) = f(z_2)] > \frac{1}{2} + \frac{1}{10n},$$

$$P'(x) = P(\underbrace{z_1 f(z_1)}_{\text{zadrátovaná konštanta}} x),$$

$$\Pr_{x \in_R \{0,1\}^{\ell/2}}[P'(x) = f(x)] > \frac{1}{2} + \frac{1}{10n},$$

$$G(z) = z_1\, f(z_1)\, z_2\, f(z_2), \qquad \text{kde } z = z_1 z_2$$

ak $\exists P$:

$$\Pr_{z_1, z_2 \in_R \{0,1\}^{\ell/2}}[P(z_1\, f(z_1)\, z_2) = f(z_2)] > \frac{1}{2} + \frac{1}{10n},$$

$$\exists z_1 \in \{0,1\}^{\ell/2} : \Pr_{z_2 \in_R \{0,1\}^{\ell/2}}[P(z_1\, f(z_1)\, z_2) = f(z_2)] > \frac{1}{2} + \frac{1}{10n},$$

$$P'(x) = P(\underbrace{z_1\, f(z_1)}_{\textit{zadrátovaná konštanta}}\, x),$$

$$\Pr_{x \in_R \{0,1\}^{\ell/2}}[P'(x) = f(x)] > \frac{1}{2} + \frac{1}{10n},$$

$$G(z) = z_1\, f(z_1)\, z_2\, f(z_2), \qquad \text{kde } z = z_1 z_2$$

ak $\exists P$:

$$\Pr_{z_1, z_2 \in_R \{0,1\}^{\ell/2}}[P(z_1\, f(z_1)\, z_2) = f(z_2)] > \frac{1}{2} + \frac{1}{10n},$$

$$\exists z_1 \in \{0,1\}^{\ell/2} : \Pr_{z_2 \in_R \{0,1\}^{\ell/2}}[P(z_1\, f(z_1)\, z_2) = f(z_2)] > \frac{1}{2} + \frac{1}{10n},$$

$$P'(x) = P(\underbrace{z_1\, f(z_1)}_{\text{zadrátovaná konštanta}}\, x),$$

$$\Pr_{x \in_R \{0,1\}^{\ell/2}}[P'(x) = f(x)] > \frac{1}{2} + \frac{1}{10n},$$

$$G(z) = z_1\, f(z_1)\, z_2\, f(z_2), \qquad \text{kde } z = z_1 z_2$$

ak $\exists P$:

$$\Pr_{z_1, z_2 \in_R \{0,1\}^{\ell/2}}[P(z_1\, f(z_1)\, z_2) = f(z_2)] > \frac{1}{2} + \frac{1}{10n},$$

$$\exists z_1 \in \{0,1\}^{\ell/2} : \Pr_{z_2 \in_R \{0,1\}^{\ell/2}}[P(z_1\, f(z_1)\, z_2) = f(z_2)] > \frac{1}{2} + \frac{1}{10n},$$

$$P'(x) = P(\underbrace{z_1\, f(z_1)}\, x),$$

zadrátovaná konštanta

$$\Pr_{x \in_R \{0,1\}^{\ell/2}}[P'(x) = f(x)] > \frac{1}{2} + \frac{1}{10n},$$

$$G(z) = z_1\, f(z_1)\, z_2\, f(z_2), \qquad \text{kde } z = z_1 z_2$$

ak $\exists P$:

$$\Pr_{z_1, z_2 \in_R \{0,1\}^{\ell/2}}[P(z_1\, f(z_1)\, z_2) = f(z_2)] > \frac{1}{2} + \frac{1}{10n},$$

$$\exists z_1 \in \{0,1\}^{\ell/2} : \Pr_{z_2 \in_R \{0,1\}^{\ell/2}}[P(z_1\, f(z_1)\, z_2) = f(z_2)] > \frac{1}{2} + \frac{1}{10n},$$

$$P'(x) = P(\underbrace{z_1\, f(z_1)}_{\textit{zadrátovaná konštanta}}\, x),$$

$$\Pr_{x \in_R \{0,1\}^{\ell/2}}[P'(x) = f(x)] > \frac{1}{2} + \frac{1}{10n},$$

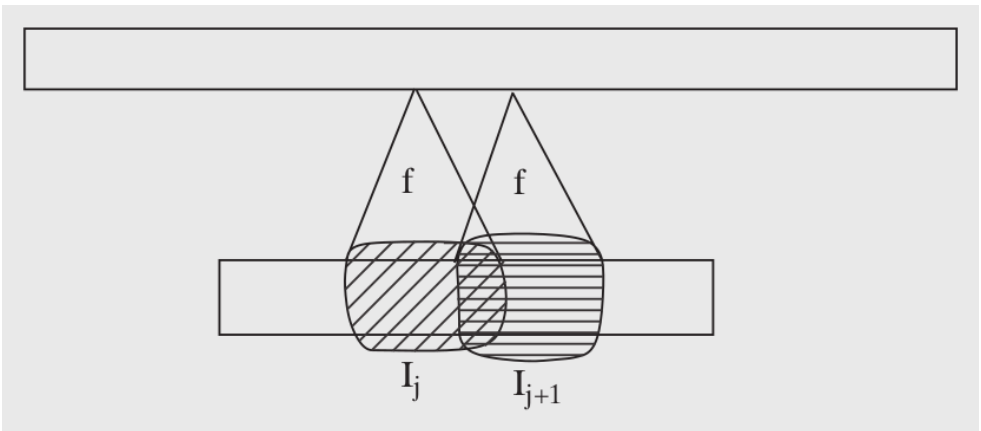
NW generátor

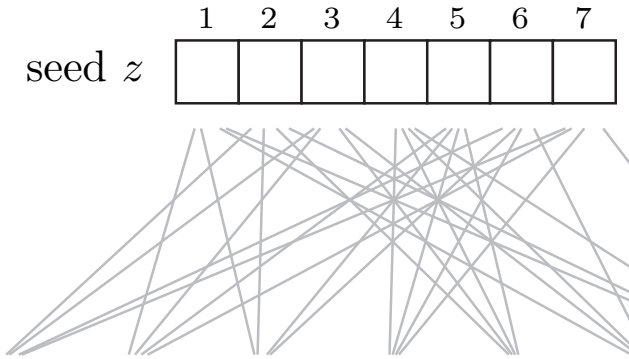
Definícia (Nissan–Wigdersonov generátor)

Nech $f : \{0,1\}^k \to \{0,1\}$ *a* $\mathscr{I} = \{I_1, \ldots, I_n\}$ *je sada* k*-prvkových podmnožín* $\{1, \ldots, \ell\}$.

$$NW^f_{\mathscr{I}}(z) = f(z_{I_1})\, f(z_{I_2}) \cdots f(z_{I_n}),$$

kde z_I *je podreťazec* z *s indexmi z* I.

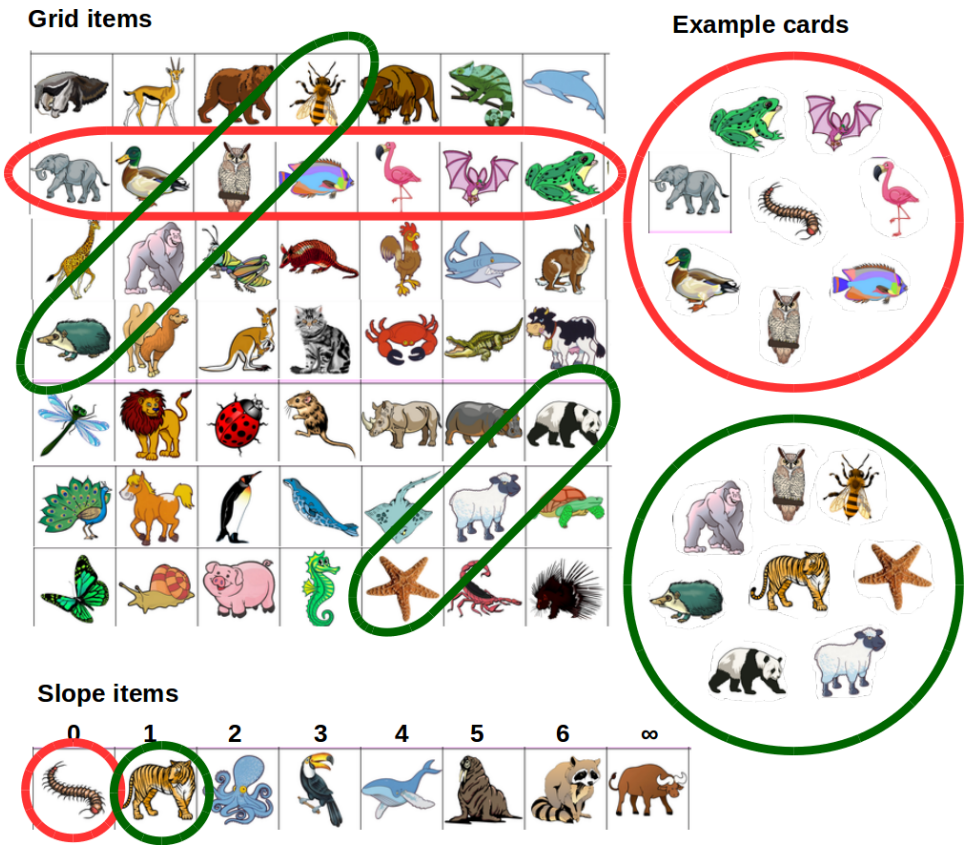




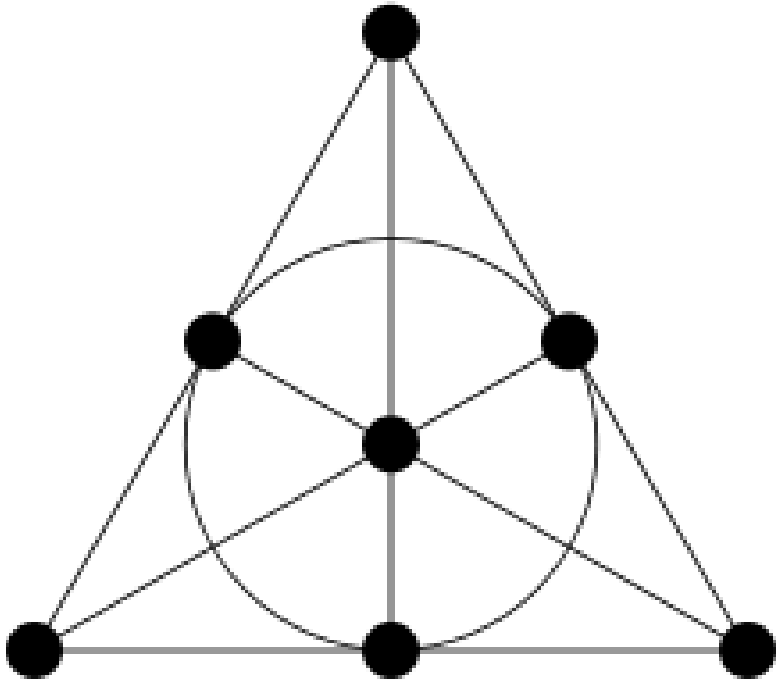
vygenerovaná postupnosť: $f(z_{I_1})\ f(z_{I_2})\ f(z_{I_3})\ f(z_{I_4})\ f(z_{I_5})\ f(z_{I_6})\ f(z_{I_7})$

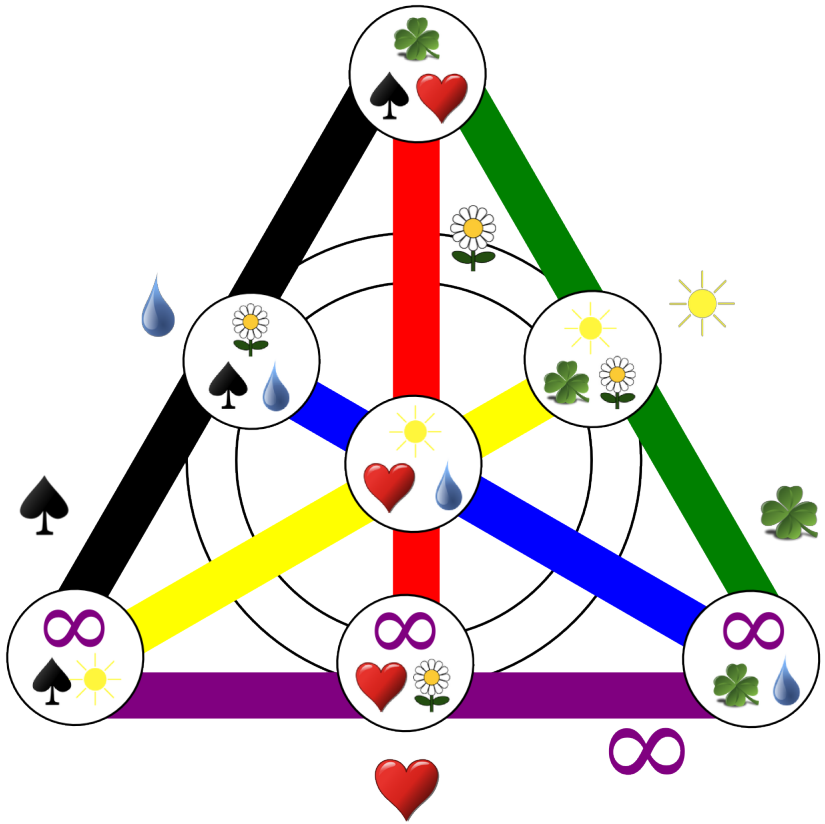
1	2	3	4	5	6	7
	∗	∗			∗	∗
∗		∗		∗		∗
∗	∗			∗	∗	
			∗	∗	∗	∗
	∗	∗	∗	∗		
∗		∗	∗		∗	
∗	∗		∗			∗

Dobble


Grid items
Example cards
Slope items
0
1
2
3
4
5
6
∞

Fanova rovina





Dizajn

Definícia (Kombinatorický dizajn)

Sada množín $\mathscr{I} = \{I_1, \ldots, I_n\}$ *je* (ℓ, k, d)*-dizajn* $(\ell > k > d)$*, ak*

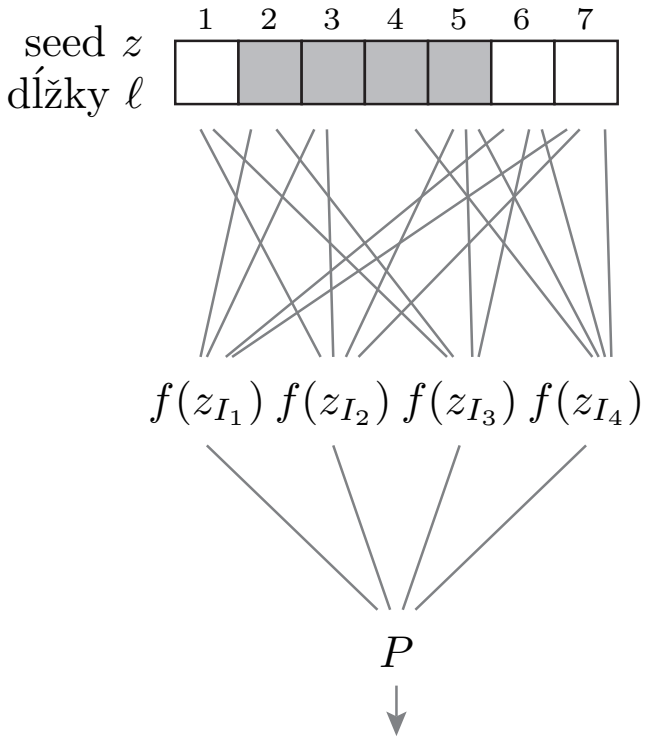
- *podmnožiny* $\{1, \ldots, \ell\}$ *veľkosti* k
- *ľub. dve majú prienik* $\forall j \neq k : |I_j \cap I_k| \leq d$.

- $\mathrm{H}_{\mathrm{avg}}(f) \geq 2^{\gamma k}$
- n – exponenciálny počet množín $2^{d/10} = 2^{\Omega(\ell)}$ – toto zodpovedá dĺžke vygenerovanej postupnosti,
- ℓ – seed dĺžky $c \cdot \log n$, kde $c = (20/\gamma)^2$,
- k – veľkosť množín $\sqrt{c} \cdot \log n$ – toto bude dĺžka vstupu pre f,
- d – veľkosť prieniku $10 \cdot \log n$

$(\ell \geq 10k^2/d,\ 2d \leq \gamma k)$

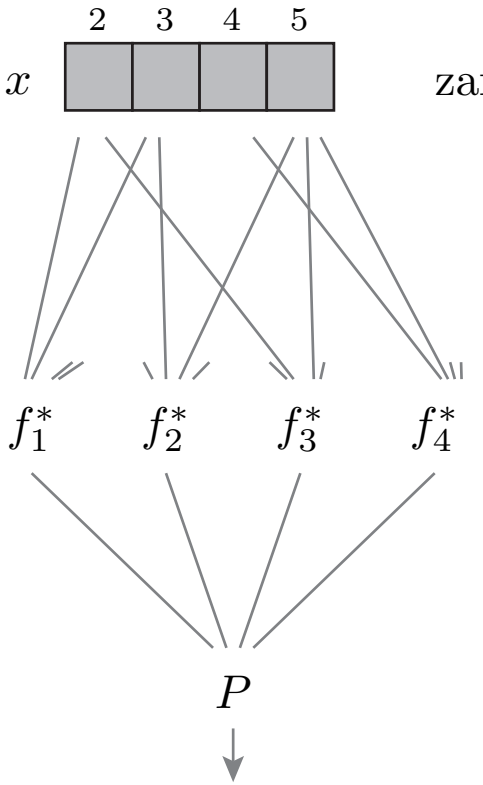
Lema

Nech $\mathscr{I}$ je (ℓ, k, d)-dizajn veľkosti n s parametrami vyššie a $f : \{0,1\}^k \to \{0,1\}$ je pekelne ťažká funkcia. Potom $NW^f_{\mathscr{I}}$ je $2^{\Omega(\ell)}$-PNG.



n podmnožín veľkosti k

vstupy sa prekrývajú
na $\leq d$ pozíciach



zafixujeme zvyšné bity

tieto funkcie závisia
iba od $\leq d$ bitov
takže sa dajú vypočítať
obvodmi veľkosti $\leq 2^{d+1}$

- $\exists$ predpovedač P veľkosti $2n^3 = 2^{3 \cdot d/10+1}$:

$$\Pr_{z \in_R \{0,1\}^\ell}[P(f(z_{l_1}, \ldots, f(z_{l_{i-1}})) = f(z_{l_i})] \geq \frac{1}{2} + \frac{1}{10n}.$$

- nech $f_j(z) = f(z_{l_j})$:

$$\Pr_{z \in_R \{0,1\}^\ell}[P(f_1(z), \ldots, f_{i-1}(z)) = f_i(z)] \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}.$$

- nech $x = z_{l_i}$ bity v l_i, z^* tie zvyšné:

$$\Pr_{x \in_R \{0,1\}^k, z^* \in_R \{0,1\}^{\ell-k}}[P(f_1(x, z^*), \ldots, f_{i-1}(x, z^*)) = f(x)] \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}.$$

- priemerovací argument: $\exists$konkrétne z^*:

$$\Pr_{x \in_R \{0,1\}^k}[P(f_1^*(x), \ldots, f_{i-1}^*(x)) = f(x)] \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}.$$

- $\exists$ predpovedač P veľkosti $2n^3 = 2^{3 \cdot d/10+1}$:

$$\Pr_{z \in_R \{0,1\}^\ell}[P(f(z_{l_1}, \ldots, f(z_{l_{i-1}})) = f(z_{l_i})] \geq \frac{1}{2} + \frac{1}{10n}.$$

- nech $f_j(z) = f(z_{l_j})$:

$$\Pr_{z \in_R \{0,1\}^\ell}[P(f_1(z), \ldots, f_{i-1}(z)) = f_i(z)] \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}.$$

- nech $x = z_{l_i}$ bity v l_i, z^* tie zvyšné:

$$\Pr_{x \in_R \{0,1\}^k, z^* \in_R \{0,1\}^{\ell-k}}[P(f_1(x, z^*), \ldots, f_{i-1}(x, z^*)) = f(x)] \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}.$$

- priemerovací argument: $\exists$konkrétne z^*:

$$\Pr_{x \in_R \{0,1\}^k}[P(f_1^*(x), \ldots, f_{i-1}^*(x)) = f(x)] \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}.$$

- $\exists$ predpovedač P veľkosti $2n^3 = 2^{3 \cdot d/10+1}$:

$$\Pr_{z \in_R \{0,1\}^\ell}[P(f(z_{l_1}, \ldots, f(z_{l_{i-1}})) = f(z_{l_i})] \geq \frac{1}{2} + \frac{1}{10n}.$$

- nech $f_j(z) = f(z_{l_j})$:

$$\Pr_{z \in_R \{0,1\}^\ell}[P(f_1(z), \ldots, f_{i-1}(z)) = f_i(z)] \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}.$$

- nech $x = z_{l_i}$ bity v l_i, z^* tie zvyšné:

$$\Pr_{x \in_R \{0,1\}^k, z^* \in_R \{0,1\}^{\ell-k}}[P(f_1(x, z^*), \ldots, f_{i-1}(x, z^*)) = f(x)] \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}.$$

- priemerovací argument: $\exists$konkrétne z^*:

$$\Pr_{x \in_R \{0,1\}^k}[P(f_1^*(x), \ldots, f_{i-1}^*(x)) = f(x)] \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}.$$

- $\exists$ predpovedač P veľkosti $2n^3 = 2^{3 \cdot d/10+1}$:

$$\Pr_{z \in_R \{0,1\}^\ell}[P(f(z_{I_1}, \ldots, f(z_{I_{i-1}})) = f(z_{I_i})] \geq \frac{1}{2} + \frac{1}{10n}.$$

- nech $f_j(z) = f(z_{I_j})$:

$$\Pr_{z \in_R \{0,1\}^\ell}[P(f_1(z), \ldots, f_{i-1}(z)) = f_i(z)] \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}.$$

- nech $x = z_{I_i}$ bity v I_i, z^* tie zvyšné:

$$\Pr_{x \in_R \{0,1\}^k, z^* \in_R \{0,1\}^{\ell-k}}[P(f_1(x, z^*), \ldots, f_{i-1}(x, z^*)) = f(x)] \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}.$$

- priemerovací argument: $\exists$konkrétne z^*:

$$\Pr_{x \in_R \{0,1\}^k}[P(f_1^*(x), \ldots, f_{i-1}^*(x)) = f(x)] \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}.$$

- každú funkciu d bitov vieme vypočítať obvodom veľkosti 2^{d+1}

$$z \mapsto P(g_1(z), \ldots, g_{i-1}(z))$$

veľkosti $n \cdot 2^{d+1} + 2^{3 \cdot d/10+1} = 2^{1.4d+2} < 2^{2d} \leq 2^{\gamma k}$

- ak by $\exists$ P, vedeli by sme vytvoriť obvod, ktorý počíta f na viac ako

$$\frac{1}{2} + \frac{1}{10n} \geq \frac{1}{2} + \frac{1}{S} \qquad \text{vstupoch.}$$

□

- každú funkciu d bitov vieme vypočítať obvodom veľkosti 2^{d+1}

$$z \mapsto P(g_1(z), \ldots, g_{i-1}(z))$$

veľkosti $n \cdot 2^{d+1} + 2^{3 \cdot d/10+1} = 2^{1.4d+2} < 2^{2d} \leq 2^{\gamma k}$

- ak by $\exists$ P, vedeli by sme vytvoriť obvod, ktorý počíta f na viac ako

$$\frac{1}{2} + \frac{1}{10n} \geq \frac{1}{2} + \frac{1}{S}$$ vstupoch.

□

Zovšeobecnenie lemy

Ak $\mathscr{I}$ *je* (ℓ, k, d)*-dizajn veľkosti* $2^{d/10}$ *a* $f : \{0,1\}^k \to \{0,1\}$ *je pekelne ťažká (*$\mathrm{H}_{\mathrm{avg}}(f) > 2^{2d} = 2^{\gamma k}$*), tak distribúcia* $NW^f_{\mathscr{I}}(U_\ell)$ *je* $\mathrm{H}_{\mathrm{avg}}(f)/10$*-pseudonáhodná.*

Veta (Nissan, Wigderson)

Ak existuje pekelne ťažká funkcia v E, *tak* BPP = P.

- $\mathrm{H}_{\mathrm{avg}}(f) \geq 2^{\gamma k}$
- n – exponenciálny počet množín $2^{d/10} = 2^{\Omega(\ell)}$ – toto zodpovedá dĺžke vygenerovanej postupnosti,
- ℓ – seed dĺžky $c \cdot \log n$, kde $c = (20/\gamma)^2$,
- k – veľkosť množín $\sqrt{c} \cdot \log n$ – toto bude dĺžka vstupu pre f,
- d – veľkosť prieniku $10 \cdot \log n$

$(\ell \geq 10k^2/d,\ 2d \leq \gamma k)$

Lema

Pre každé $k-1 \geq d \geq 0$ *a* $\ell \geq 2k^2$ *existuje* (ℓ, k, d)*-dizajn veľkosti aspoň* $(\ell/2k)^{d+1}$.

Lema

$\forall \ell \geq 10k^2/d$ *a* $k > d$ *existuje* (ℓ, k, d)*-dizajn veľkosti aspoň* $m = 2^{d/10}$. *Vieme ho vygenerovať v čase* $2^{O(\ell)}$.

Dôkaz.

- greedy, brute-force
- ak máme $\{I_1, \ldots, I_n\}$ pre $n < 2^{d/10}$, vieme vybrať ďalšiu
- vyberme I náhodne, $\forall x \in [\ell]$ vyberieme s pp. $2k/\ell$
- $E[|I|] = 2k$, $E[|I \cap I_j|] = 2k^2/\ell \leq d/5$
- Černof: $\Pr[|I| \leq k] \leq 0.1$ (dokonca exponenciálne malá)
- $\Pr[|I \cap I_j| \geq d] \leq 1/2^{d/10+1}$
- množín je $< 2^{d/10}$, union bound $\Longrightarrow$ pp., že $\exists$množina s veľkým prienikom $\leq \frac{1}{2}$.
- pp., že I nevyhovuje je $\leq 0.6 < 1$

□

Dôkaz.

- greedy, brute-force
- ak máme $\{I_1, \ldots, I_n\}$ pre $n < 2^{d/10}$, vieme vybrať ďalšiu
- vyberme I náhodne, $\forall x \in [\ell]$ vyberieme s pp. $2k/\ell$
- $E[|I|] = 2k$, $E[|I \cap I_j|] = 2k^2/\ell \leq d/5$
- Černof: $\Pr[|I| \leq k] \leq 0.1$ (dokonca exponenciálne malá)
- $\Pr[|I \cap I_j| \geq d] \leq 1/2^{d/10+1}$
- množín je $< 2^{d/10}$, union bound $\Longrightarrow$ pp., že $\exists$množina s veľkým prienikom $\leq \frac{1}{2}$.
- pp., že I nevyhovuje je $\leq 0.6 < 1$

□

Dôkaz.

- greedy, brute-force
- ak máme $\{I_1, \ldots, I_n\}$ pre $n < 2^{d/10}$, vieme vybrať ďalšiu
- vyberme I náhodne, $\forall x \in [\ell]$ vyberieme s pp. $2k/\ell$
- $E[|I|] = 2k$, $E[|I \cap I_j|] = 2k^2/\ell \leq d/5$
- Černof: $\Pr[|I| \leq k] \leq 0.1$ (dokonca exponenciálne malá)
- $\Pr[|I \cap I_j| \geq d] \leq 1/2^{d/10+1}$
- množín je $< 2^{d/10}$, union bound $\Longrightarrow$ pp., že $\exists$množina s veľkým prienikom $\leq \frac{1}{2}$.
- pp., že I nevyhovuje je $\leq 0.6 < 1$

□

Dôkaz.

- greedy, brute-force
- ak máme $\{I_1, \ldots, I_n\}$ pre $n < 2^{d/10}$, vieme vybrať ďalšiu
- vyberme I náhodne, $\forall x \in [\ell]$ vyberieme s pp. $2k/\ell$
- $E[|I|] = 2k$, $E[|I \cap I_j|] = 2k^2/\ell \leq d/5$
- Černof: $\Pr[|I| \leq k] \leq 0.1$ (dokonca exponenciálne malá)
- $\Pr[|I \cap I_j| \geq d] \leq 1/2^{d/10+1}$
- množín je $< 2^{d/10}$, union bound $\Longrightarrow$ pp., že $\exists$množina s veľkým prienikom $\leq \frac{1}{2}$.
- pp., že I nevyhovuje je $\leq 0.6 < 1$

□

Dôkaz.

- greedy, brute-force
- ak máme $\{I_1, \ldots, I_n\}$ pre $n < 2^{d/10}$, vieme vybrať ďalšiu
- vyberme I náhodne, $\forall x \in [\ell]$ vyberieme s pp. $2k/\ell$
- $E[|I|] = 2k$, $E[|I \cap I_j|] = 2k^2/\ell \leq d/5$
- Černof: $\Pr[|I| \leq k] \leq 0.1$ (dokonca exponenciálne malá)
- $\Pr[|I \cap I_j| \geq d] \leq 1/2^{d/10+1}$
- množín je $< 2^{d/10}$, union bound $\Longrightarrow$ pp., že $\exists$množina s veľkým prienikom $\leq \frac{1}{2}$.
- pp., že I nevyhovuje je $\leq 0.6 < 1$

□

Dôkaz.

- greedy, brute-force
- ak máme $\{I_1, \ldots, I_n\}$ pre $n < 2^{d/10}$, vieme vybrať ďalšiu
- vyberme I náhodne, $\forall x \in [\ell]$ vyberieme s pp. $2k/\ell$
- $E[|I|] = 2k$, $E[|I \cap I_j|] = 2k^2/\ell \leq d/5$
- Černof: $\Pr[|I| \leq k] \leq 0.1$ (dokonca exponenciálne malá)
- $\Pr[|I \cap I_j| \geq d] \leq 1/2^{d/10+1}$
- množín je $< 2^{d/10}$, union bound $\Longrightarrow$ pp., že $\exists$množina s veľkým prienikom $\leq \frac{1}{2}$.
- pp., že I nevyhovuje je $\leq 0.6 < 1$

□

■ **Dôkaz.**

- greedy, brute-force
- ak máme $\{I_1, \ldots, I_n\}$ pre $n < 2^{d/10}$, vieme vybrať ďalšiu
- vyberme I náhodne, $\forall x \in [\ell]$ vyberieme s pp. $2k/\ell$
- $E[|I|] = 2k$, $E[|I \cap I_j|] = 2k^2/\ell \leq d/5$
- Černof: $\Pr[|I| \leq k] \leq 0.1$ (dokonca exponenciálne malá)
- $\Pr[|I \cap I_j| \geq d] \leq 1/2^{d/10+1}$
- množín je $< 2^{d/10}$, union bound $\Longrightarrow$ pp., že $\exists$množina s veľkým prienikom $\leq \frac{1}{2}$.
- pp., že I nevyhovuje je $\leq 0.6 < 1$

□

■ **Dôkaz.**

- greedy, brute-force
- ak máme $\{I_1, \ldots, I_n\}$ pre $n < 2^{d/10}$, vieme vybrať ďalšiu
- vyberme I náhodne, $\forall x \in [\ell]$ vyberieme s pp. $2k/\ell$
- $E[|I|] = 2k$, $E[|I \cap I_j|] = 2k^2/\ell \leq d/5$
- Černof: $\Pr[|I| \leq k] \leq 0.1$ (dokonca exponenciálne malá)
- $\Pr[|I \cap I_j| \geq d] \leq 1/2^{d/10+1}$
- množín je $< 2^{d/10}$, union bound $\Longrightarrow$ pp., že $\exists$množina s veľkým prienikom $\leq \frac{1}{2}$.
- pp., že I nevyhovuje je $\leq 0.6 < 1$

□