Zväčšovanie ťažkosti

kuko

6.5.2021

Pokročilá teória zložitosti

Plán

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

Ťažkosť v priemernom prípade

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 $\gamma > 0$).*

Ťažkosť v priemernom prípade

Definícia

Pre $f : \{0,1\}^n \to \{0,1\}$ *a* $\rho \in [0,1]$*:*

$$\mathrm{H}^{\rho}_{\mathrm{avg}}(f) = \max\{S \mid \forall C, \mathrm{SIZE}(C) = S : \Pr_{x \in_R \{0,1\}^n}[C(x) = f(x)] < \rho\}.$$

Pekelne ťažké funkcie z veľmi ťažkých

Yaova XOR lema

- nech

$$f^{\oplus k}(x_1, \ldots, x_k) = \bigoplus_i f(x_i).$$

- ak f je veľmi ťažká $\Longrightarrow$ $f^{\oplus k}$ je pekelne ťažká

Yaova XOR lema

Veta (Yaova XOR lema)

Nech $f : \{0,1\}^n \to \{0,1\}$, *definujme* $f^{\oplus k} : \{0,1\}^{nk} \to \{0,1\}$:

$$f^{\oplus k}(x_1, \ldots, x_k) = \bigoplus_i f(x_i).$$

Potom pre $\varepsilon > 2 \cdot 0.99^k$ *je*

$$\mathrm{H}^{1/2+\varepsilon}_{\mathrm{avg}}(f^{\oplus k}) \geq (\varepsilon^2/400n) \cdot \mathrm{H}^{0.99}_{\mathrm{avg}}(f).$$

Ťažké jadro

Hardcore lema

- Nech f je veľmi ťažká (pri uniformnej distribúcií)
- potom existuje množina/distribúcia H (tzv. ťažké jadro)
- taká, že f je pekelne ťažká na H

Hardcore lema

- distribúcia H na $\{0,1\}^n$ má hustotu δ, ak

$$\forall x \in \{0,1\}^n : \quad \Pr[H = x] \leq \frac{1}{\delta 2^n}$$

- uniformná distribúcia má hustotu 1
- ostatné distribúcie majú hustotu < 1
- uniformná distribúcia na množine veľkosti $\delta 2^n$ je δ-hustá
- mix δ-hustých distr. je δ-hustá distr.

Hardcore lema

Lema (Impagliazzova Hardcore lema)

Existuje 1%-hustá distribúcia H taká, že ak f je veľmi ťažká na U_n, tak f je pekelne ťažká na H.
Presnejšie: pre každý obvod C menší ako $\varepsilon^2/100n \cdot \mathrm{H}_{\mathrm{avg}}^{0.99}(f)$ platí

$$\Pr_{x \in_R H}[C(x) = f(x)] \leq 1/2 + \varepsilon.$$

Yaova XOR lema

Späť k Yaovej XOR leme

Veta (Yaova XOR lema)

$$f^{\oplus k}(x_1, \ldots, x_k) = \bigoplus_i f(x_i).$$

Pre $\varepsilon > 2 \cdot 0.99^k$ *(teda* $k = \Theta(\log 1/\varepsilon)$ *je*

$$\mathrm{H}^{1/2+\varepsilon}_{\mathrm{avg}}(f^{\oplus k}) \geq \underbrace{(\varepsilon^2/400n) \cdot \underbrace{\mathrm{H}^{0.99}_{\mathrm{avg}}(f)}_{S}}_{S'}.$$

Dôkaz Yaovej XOR lemy

Myšlienka dôkazu.

- pre $k = 2$; sporom:
- predpokladajme, že $\exists$ malý obvod počítajúci $f^{\oplus 2}$ s pp. $\geq 1/2 + \varepsilon$ (na uniformnej distribúcií)
- nech H je distribúcia z Hardcore lemy pre f
  - t.j. f sa nedá na H spočítať ani s pp. $1/2 + \varepsilon/2$
- rozložme $U_n = 0.99G + 0.01H$
- z obvodu pre $f^{\oplus 2}$ vyrobíme malý obvod pre f na H

Dôkaz Yaovej XOR lemy

Myšlienka dôkazu.

- pre $k = 2$; sporom:
- predpokladajme, že $\exists$ malý obvod počítajúci $f^{\oplus 2}$ s pp. $\geq 1/2 + \varepsilon$ (na uniformnej distribúcií)
- nech H je distribúcia z Hardcore lemy pre f
  - t.j. f sa nedá na H spočítať ani s pp. $1/2 + \varepsilon/2$
- rozložme $U_n = 0.99G + 0.01H$
- z obvodu pre $f^{\oplus 2}$ vyrobíme malý obvod pre f na H

Dôkaz Yaovej XOR lemy

Myšlienka dôkazu.

- pre $k = 2$; sporom:
- predpokladajme, že $\exists$ malý obvod počítajúci $f^{\oplus 2}$ s pp. $\geq 1/2 + \varepsilon$ (na uniformnej distribúcií)
- nech H je distribúcia z Hardcore lemy pre f
  - t.j. f sa nedá na H spočítať ani s pp. $1/2 + \varepsilon/2$
- rozložme $U_n = 0.99G + 0.01H$
- z obvodu pre $f^{\oplus 2}$ vyrobíme malý obvod pre f na H

Dôkaz Yaovej XOR lemy

Dôkaz.

- nech H je 1%-hustá distribúcia z Hardcore lemy pre f a $\mathrm{H}_{\mathrm{avg}}^{1/2+\varepsilon/2}$
  - t.j. žiadny obvod veľkosti S' nedokáže vypočítať f s pp. $\geq 1/2+\varepsilon/2$ na H
- definujme „inverznú“ distribúciu G: $\Pr[G=x] = (1/2^n - \delta \Pr[H=x])/(1-\delta)$
  - $U_n = (1-\delta)G + \delta H$
  - $(U_n)^2 = (1-\delta)^2 G^2 + (1-\delta)\delta GH + \delta(1-\delta)HG + \delta^2 H^2$.

Dôkaz Yaovej XOR lemy

Dôkaz.

- nech H je 1%-hustá distribúcia z Hardcore lemy pre f a $\mathrm{H}_{\mathrm{avg}}^{1/2+\varepsilon/2}$
  - t.j. žiadny obvod veľkosti S' nedokáže vypočítať f s pp. $\geq 1/2+\varepsilon/2$ na H
- definujme „inverznú“ distribúciu G: $\Pr[G=x] = (1/2^n - \delta \Pr[H=x])/(1-\delta)$
  - $U_n = (1-\delta)G + \delta H$
  - $(U_n)^2 = (1-\delta)^2 G^2 + (1-\delta)\delta GH + \delta(1-\delta)HG + \delta^2 H^2$.

Dôkaz Yaovej XOR lemy

Dôkaz.

- nech H je 1%-hustá distribúcia z Hardcore lemy pre f a $\mathrm{H}_{\mathrm{avg}}^{1/2+\varepsilon/2}$
  - t.j. žiadny obvod veľkosti S' nedokáže vypočítať f s pp. $\geq 1/2+\varepsilon/2$ na H
- definujme „inverznú“ distribúciu G: $\Pr[G=x] = (1/2^n - \delta \Pr[H=x])/(1-\delta)$
  - $U_n = (1-\delta)G + \delta H$
  - $(U_n)^2 = (1-\delta)^2 G^2 + (1-\delta)\delta GH + \delta(1-\delta)HG + \delta^2 H^2$.

Dôkaz Yaovej XOR lemy

Dôkaz.

- nech H je 1%-hustá distribúcia z Hardcore lemy pre f a $\mathrm{H}_{\mathrm{avg}}^{1/2+\varepsilon/2}$
  - t.j. žiadny obvod veľkosti S' nedokáže vypočítať f s pp. $\geq 1/2+\varepsilon/2$ na H
- definujme „inverznú“ distribúciu G:
  $\Pr[G=x] = (1/2^n - \delta \Pr[H=x])/(1-\delta)$
  - $U_n = (1-\delta)G + \delta H$
  - $(U_n)^2 = (1-\delta)^2 G^2 + (1-\delta)\delta GH + \delta(1-\delta)HG + \delta^2 H^2$.

Dôkaz Yaovej XOR lemy

- pre ľubovoľnú distribúciu $\mathscr{D}$ na $\{0,1\}^{2n}$ označme $P_{\mathscr{D}} = \mathrm{Pr}_{x \in_R \mathscr{D}}[C = f^{\oplus 2}]$
- $1/2 + \varepsilon \leq P_{(U_n)^2} = \underbrace{(1-\delta)^2}_{<\varepsilon/2} \underbrace{P_{G^2}}_{\leq 1} + (1-\delta)\delta P_{GH} + \delta(1-\delta)P_{HG} + \delta^2 P_{H^2}$
- $1/2 + \varepsilon/2 \leq (1-\delta)\delta P_{GH} + \delta(1-\delta)P_{HG} + \delta^2 P_{H^2}$

Dôkaz Yaovej XOR lemy

- súčet koeficientov na pravej strane je < 1 a preto aspoň jedno $P_{\mathscr{D}}$ musí byť viac ako $1/2 + \varepsilon/2$ (primerovací princíp).
- predpokladajme napr., že $P_{HG} \geq 1/2 + \varepsilon/2$, t.j., $\Pr_{x_1 \in_R H, x_2 \in_R G}[C(x_1, x_2) = f(x_1) \oplus f(x_2)] > 1/2 + \varepsilon/2$.
- podľa priemerovacieho princípu musí existovať konkrétne x_2 také, že $\Pr_{x_1 \in_R H}[C(x_1, x_2) \oplus f(x_2) = f(x_1)] > 1/2 + \varepsilon/2$.
- to znamená, že máme obvod D veľkosti S' (počítajúci $x_1 \mapsto C(x_1, x_2) \oplus f(x_2)$ so zadrátovaným $x_2, f(x_2)$), ktorý počíta f na H s pp. $> 1/2 + \varepsilon/2$, čo je spor s hardcorovosťou H.

□

Dôkaz Yaovej XOR lemy

- súčet koeficientov na pravej strane je < 1 a preto aspoň jedno $P_{\mathscr{D}}$ musí byť viac ako $1/2 + \varepsilon/2$ (primerovací princíp).
- predpokladajme napr., že $P_{HG} \geq 1/2 + \varepsilon/2$, t.j., $\Pr_{x_1 \in_R H, x_2 \in_R G}[C(x_1, x_2) = f(x_1) \oplus f(x_2)] > 1/2 + \varepsilon/2$.
- podľa priemerovacieho princípu musí existovať konkrétne x_2 také, že $\Pr_{x_1 \in_R H}[C(x_1, x_2) \oplus f(x_2) = f(x_1)] > 1/2 + \varepsilon/2$.
- to znamená, že máme obvod D veľkosti S' (počítajúci $x_1 \mapsto C(x_1, x_2) \oplus f(x_2)$ so zadrátovaným $x_2, f(x_2)$), ktorý počíta f na H s pp. $> 1/2 + \varepsilon/2$, čo je spor s hardcorovosťou H.

□

Dôkaz Yaovej XOR lemy

- súčet koeficientov na pravej strane je < 1 a preto aspoň jedno $P_{\mathscr{D}}$ musí byť viac ako $1/2 + \varepsilon/2$ (primerovací princíp).
- predpokladajme napr., že $P_{HG} \geq 1/2 + \varepsilon/2$, t.j., $\Pr_{x_1 \in_R H, x_2 \in_R G}[C(x_1, x_2) = f(x_1) \oplus f(x_2)] > 1/2 + \varepsilon/2$.
- podľa priemerovacieho princípu musí existovať konkrétne x_2 také, že $\Pr_{x_1 \in_R H}[C(x_1, x_2) \oplus f(x_2) = f(x_1)] > 1/2 + \varepsilon/2$.
- to znamená, že máme obvod D veľkosti S' (počítajúci $x_1 \mapsto C(x_1, x_2) \oplus f(x_2)$ so zadrátovaným $x_2, f(x_2)$), ktorý počíta f na H s pp. $> 1/2 + \varepsilon/2$, čo je spor s hardcorovosťou H.

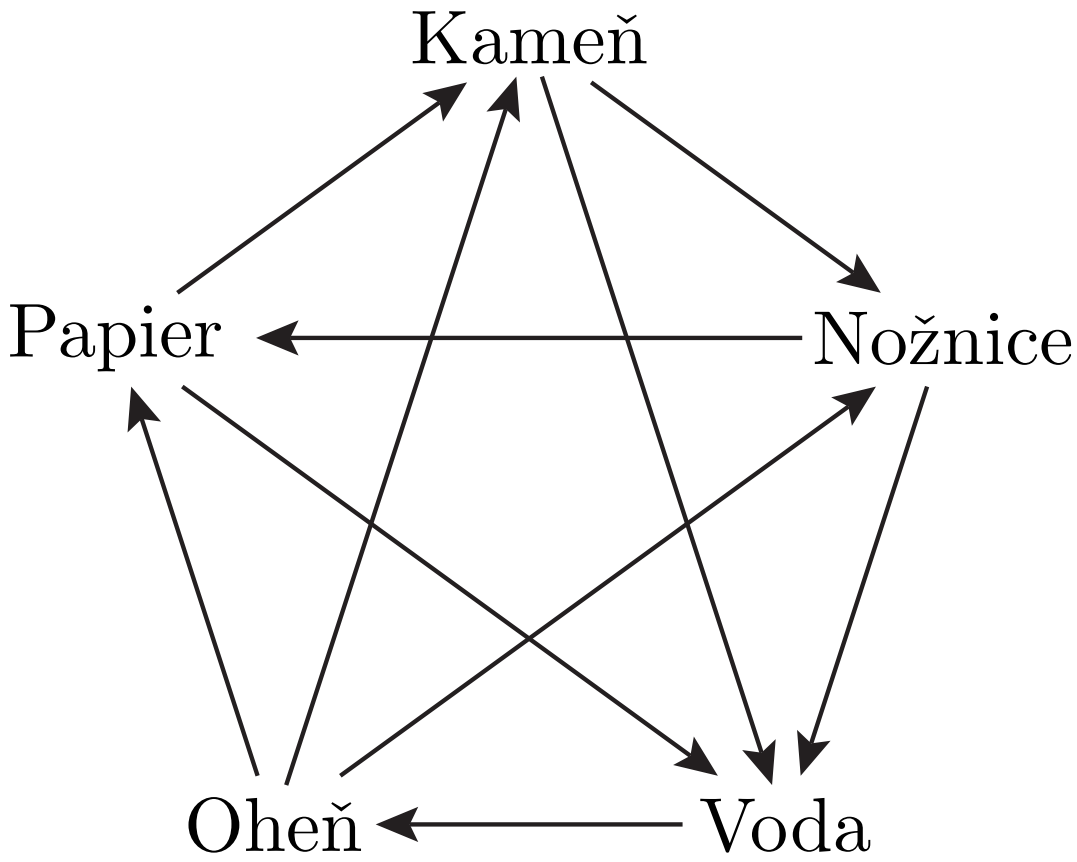
□

Dôkaz Yaovej XOR lemy

- súčet koeficientov na pravej strane je < 1 a preto aspoň jedno $P_{\mathscr{D}}$ musí byť viac ako $1/2 + \varepsilon/2$ (primerovací princíp).
- predpokladajme napr., že $P_{HG} \geq 1/2 + \varepsilon/2$, t.j., $\Pr_{x_1 \in_R H, x_2 \in_R G}[C(x_1, x_2) = f(x_1) \oplus f(x_2)] > 1/2 + \varepsilon/2$.
- podľa priemerovacieho princípu musí existovať konkrétne x_2 také, že $\Pr_{x_1 \in_R H}[C(x_1, x_2) \oplus f(x_2) = f(x_1)] > 1/2 + \varepsilon/2$.
- to znamená, že máme obvod D veľkosti S' (počítajúci $x_1 \mapsto C(x_1, x_2) \oplus f(x_2)$ so zadrátovaným $x_2, f(x_2)$), ktorý počíta f na H s pp. $> 1/2 + \varepsilon/2$, čo je spor s hardcorovosťou H.

□

Malá odbočka do teórie hier



	K	P	N	O	V
K	0	-1	$+1$	-1	$+1$
P	$+1$	0	-1	-1	$+1$
N	-1	$+1$	0	-1	$+1$
O	$+1$	$+1$	$+1$	0	-1
V	-1	-1	-1	$+1$	0

NATIONAL GALLERIES SCOTLAND

The Game of Morra. A Group of Three Italian Sailors, 1765, David Allan

	$(1,2)$	$(1,3)$	$(2,3)$	$(2,4)$
$(1,2)$		$+2$	-3	
$(1,3)$	-2			$+3$
$(2,3)$	$+3$			-4
$(2,4)$		-3	$+4$	

Optimálna stratégia:

- $(1,2)$ s pravdepodobnosťou $4/7 \approx 57\%$
- $(2,4)$ s pravdepodobnosťou $3/7 \approx 43\%$

	$(1,2)$	$(1,3)$	$(2,3)$	$(2,4)$
$(1,2)$		$+2$	-3	
$(1,3)$	-2			$+3$
$(2,3)$	$+3$			-4
$(2,4)$		-3	$+4$	

Optimálna stratégia:

- $(1,2)$ s pravdepodobnosťou $4/7 \approx 57\%$
- $(2,4)$ s pravdepodobnosťou $3/7 \approx 43\%$

- matica **A**
- Alica zvolí riadok i
- Bob zvolí stĺpec j
- A_{ij} je výhra/prehra z pohľadu Alice

- nech $\mathbf{p}, \mathbf{q}$ pravdepodobnostné distribúcie nad riadkami/stĺpcami

$$\begin{aligned}\mathrm{E}[\text{výhra Alice}] &= \sum_{i,j} \underbrace{\Pr[\text{Alica zvolí } i]}_{p_i} \cdot \underbrace{\Pr[\text{Bob zvolí } j]}_{q_j} \cdot A_{ij} \\ &= \sum_{i,j} p_i \cdot A_{ij} \cdot q_j = \mathbf{p}^T \mathbf{A} \mathbf{q}.\end{aligned}$$

- ak by A vedela, že B zahrá $\mathbf{q}$, tak

$$\mathrm{E}[\text{výhra pre } i\text{-ty riadok}] = \sum_j \Pr[\text{Bob zvolí } j] \cdot A_{ij} = \mathbf{Aq}.$$

$$\max_{\mathbf{p}} \mathbf{p}^T \mathbf{Aq} = \max_i \mathbf{e}_i^T \mathbf{Aq} \qquad \text{a} \qquad \min_{\mathbf{q}} \mathbf{p}^T \mathbf{Aq} = \min_j \mathbf{p}^T \mathbf{Ae}_j.$$

- ak by A vedela, že B zahrá $\mathbf{q}$, tak

$$\mathrm{E}[\text{výhra pre } i\text{-ty riadok}] = \sum_j \Pr[\text{Bob zvolí } j] \cdot A_{ij} = \mathbf{Aq}.$$

$$\max_{\mathbf{p}} \mathbf{p}^T \mathbf{Aq} = \max_i \mathbf{e}_i^T \mathbf{Aq} \qquad \text{a} \qquad \min_{\mathbf{q}} \mathbf{p}^T \mathbf{Aq} = \min_j \mathbf{p}^T \mathbf{Ae}_j.$$

- pre každé $\mathbf{p}$ spočítame $v_A(\mathbf{p}) = \min_{\mathbf{q}} \mathbf{p}^T \mathbf{A}\mathbf{q}$ – koľko získa, ak Bob zvolí optimálnu stratégiu proti $\mathbf{p}$

nech $v_A = \max_{\mathbf{p}} v_A(\mathbf{p}) = \max_{\mathbf{p}}(\min_{\mathbf{q}} \mathbf{p}^T \mathbf{A}\mathbf{q}) = \max_{\mathbf{p}}(\min_{j} \mathbf{p}^T \mathbf{A}\mathbf{e}_j)$.

- označme $\tilde{\mathbf{p}}$
- podobne Bob: $v_B(\mathbf{q}) = \max_{\mathbf{p}} \mathbf{p}^T \mathbf{A}\mathbf{q}$

nech $v_B = \min_{\mathbf{q}} v_B(\mathbf{q}) = \min_{\mathbf{q}}(\max_{\mathbf{p}} \mathbf{p}^T \mathbf{A}\mathbf{q}) = \min_{\mathbf{q}}(\max_{i} \mathbf{e}_i^T \mathbf{A}\mathbf{q})$.

- označme $\tilde{\mathbf{q}}$

- pre každé $\mathbf{p}$ spočítame $v_A(\mathbf{p}) = \min_{\mathbf{q}} \mathbf{p}^T \mathbf{A}\mathbf{q}$ – koľko získa, ak Bob zvolí optimálnu stratégiu proti $\mathbf{p}$

nech $v_A = \max_{\mathbf{p}} v_A(\mathbf{p}) = \max_{\mathbf{p}}(\min_{\mathbf{q}} \mathbf{p}^T \mathbf{A}\mathbf{q}) = \max_{\mathbf{p}}(\min_{j} \mathbf{p}^T \mathbf{A}\mathbf{e}_j)$.

- označme $\tilde{\mathbf{p}}$
- podobne Bob: $v_B(\mathbf{q}) = \max_{\mathbf{p}} \mathbf{p}^T \mathbf{A}\mathbf{q}$

nech $v_B = \min_{\mathbf{q}} v_B(\mathbf{q}) = \min_{\mathbf{q}}(\max_{\mathbf{p}} \mathbf{p}^T \mathbf{A}\mathbf{q}) = \min_{\mathbf{q}}(\max_{i} \mathbf{e}_i^T \mathbf{A}\mathbf{q})$.

- označme $\tilde{\mathbf{q}}$

- pre každé $\mathbf{p}$ spočítame $v_A(\mathbf{p}) = \min_{\mathbf{q}} \mathbf{p}^T \mathbf{A}\mathbf{q}$ – koľko získa, ak Bob zvolí optimálnu stratégiu proti $\mathbf{p}$

nech $v_A = \max_{\mathbf{p}} v_A(\mathbf{p}) = \max_{\mathbf{p}}(\min_{\mathbf{q}} \mathbf{p}^T \mathbf{A}\mathbf{q}) = \max_{\mathbf{p}}(\min_{j} \mathbf{p}^T \mathbf{A}\mathbf{e}_j)$.

- označme $\tilde{\mathbf{p}}$
- podobne Bob: $v_B(\mathbf{q}) = \max_{\mathbf{p}} \mathbf{p}^T \mathbf{A}\mathbf{q}$

nech $v_B = \min_{\mathbf{q}} v_B(\mathbf{q}) = \min_{\mathbf{q}}(\max_{\mathbf{p}} \mathbf{p}^T \mathbf{A}\mathbf{q}) = \min_{\mathbf{q}}(\max_{i} \mathbf{e}_i^T \mathbf{A}\mathbf{q})$.

- označme $\tilde{\mathbf{q}}$

Veta

Pre každú hru s nulovým súčtom danú maticou $\mathbf{A}$ *platí*

$$\max_{\mathbf{p}}(\min_{\mathbf{q}} \mathbf{p}^T \mathbf{A}\mathbf{q}) = \min_{\mathbf{q}}(\max_{\mathbf{p}} \mathbf{p}^T \mathbf{A}\mathbf{q}).$$

Optimálna stratégia Alice je distribúcia $\tilde{\mathbf{p}}$*, ktorá maximalizuje ľavú stranu a optimálna stratégia Boba je distribúcia* $\tilde{\mathbf{q}}$*, ktorá minimalizuje pravú stranu.*

$$\min X = \max\{m \mid \forall x \in X : m \leq x\}.$$

- $v_A(\mathbf{p}) = \min_j \mathbf{p}^T \mathbf{A} \mathbf{e}_j$ je najväčšie v také, že
$$(\mathbf{p}^T \mathbf{A})_j = \sum_i p_i A_{ij} \geq v \qquad \text{pre každé } j.$$

Alica:

$$\max v,$$
$$\text{za podmienok: } \mathbf{p}^T \mathbf{A} \geq v \cdot \mathbf{1}$$
$$\mathbf{p}^T \mathbf{1} = 1$$
$$\mathbf{p} \geq \mathbf{0}$$

Bob:

$$\min v,$$
$$\text{za podmienok: } \mathbf{A}\mathbf{q} \leq v \cdot \mathbf{1}$$
$$\mathbf{1}^T \mathbf{q} = 1$$
$$\mathbf{q} \geq \mathbf{0}$$

$$\min X = \max\{m \mid \forall x \in X : m \leq x\}.$$

- $v_A(\mathbf{p}) = \min_j \mathbf{p}^T \mathbf{A} \mathbf{e}_j$ je najväčšie v také, že
$$(\mathbf{p}^T \mathbf{A})_j = \sum_i p_i A_{ij} \geq v \qquad \text{pre každé } j.$$

Alica:

$$\max v,$$
$$\text{za podmienok: } \mathbf{p}^T \mathbf{A} \geq v \cdot \mathbf{1}$$
$$\mathbf{p}^T \mathbf{1} = 1$$
$$\mathbf{p} \geq \mathbf{0}$$

Bob:

$$\min v,$$
$$\text{za podmienok: } \mathbf{A}\mathbf{q} \leq v \cdot \mathbf{1}$$
$$\mathbf{1}^T \mathbf{q} = 1$$
$$\mathbf{q} \geq \mathbf{0}$$

$$\min X = \max\{m \mid \forall x \in X : m \leq x\}.$$

- $v_A(\mathbf{p}) = \min_j \mathbf{p}^T \mathbf{A} \mathbf{e}_j$ je najväčšie v také, že
$$(\mathbf{p}^T \mathbf{A})_j = \sum_i p_i A_{ij} \geq v \qquad \text{pre každé } j.$$

Alica:

$$\max v,$$
$$\text{za podmienok: } \mathbf{p}^T \mathbf{A} \geq v \cdot \mathbf{1}$$
$$\mathbf{p}^T \mathbf{1} = 1$$
$$\mathbf{p} \geq \mathbf{0}$$

Bob:

$$\min v,$$
$$\text{za podmienok: } \mathbf{A}\mathbf{q} \leq v \cdot \mathbf{1}$$
$$\mathbf{1}^T \mathbf{q} = 1$$
$$\mathbf{q} \geq \mathbf{0}$$

Hardcore lema

Späť k Hardcore leme:

Lema (Impagliazzova Hardcore lema)

Existuje 1%-hustá distribúcia H taká, že ak f je veľmi ťažká na U_n, tak f je pekelne ťažká na H.
Presnejšie: pre každý obvod C menší ako $\varepsilon^2/100n \cdot \mathrm{H}^{0.99}_{\mathrm{avg}}(f)$ platí

$$\Pr_{x \in_R H}[C(x) = f(x)] \leq 1/2 + \varepsilon.$$

$$\text{ak} \quad f \text{ je veľmi ťažká} \Longrightarrow \exists \text{pekelne ťažké jadro } H,$$

$$\text{ak} \quad \begin{array}{c}\text{každý malý obvod}\\ \text{spočíta } f \text{ na } < 99\%\end{array} \Longrightarrow \exists \text{množina } H \quad \begin{array}{c}\forall \text{malý obvod dokáže vyriešiť}\\ \text{len } < 50+\varepsilon\% \text{ vstupov z } H.\end{array}$$

Obmena:

$$\nexists \text{pekelne ťažké jadro} \Longrightarrow \exists \text{malý obvod, ktorý počíta } f \text{ skoro všade,}$$

$$\text{ak } \forall \text{množinu } H \quad \begin{array}{c}\exists \text{malý obvod } C, \text{ ktorý vyrieši}\\ \geq 50+\varepsilon\% \text{ vstupov z } H\end{array} \Longrightarrow \begin{array}{c}\exists \text{malý obvod, ktorý}\\ \text{rieši } f \text{ na } \geq 99\%.\end{array}$$

$$\text{ak} \quad f \text{ je veľmi ťažká} \Longrightarrow \exists \text{pekelne ťažké jadro } H,$$

$$\text{ak} \quad \begin{array}{c}\text{každý malý obvod} \\ \text{spočíta } f \text{ na } < 99\%\end{array} \Longrightarrow \exists \text{množina } H \quad \begin{array}{c}\forall \text{malý obvod dokáže vyriešiť} \\ \text{len } < 50 + \varepsilon\% \text{ vstupov z } H.\end{array}$$

Obmena:

$$\nexists \text{pekelne ťažké jadro} \Longrightarrow \exists \text{malý obvod, ktorý počíta } f \text{ skoro všade,}$$

$$\text{ak } \forall \text{množinu } H \quad \begin{array}{c}\exists \text{malý obvod } C, \text{ ktorý vyrieši} \\ \geq 50 + \varepsilon\% \text{ vstupov z } H\end{array} \Longrightarrow \begin{array}{c}\exists \text{malý obvod, ktorý} \\ \text{rieši } f \text{ na } \geq 99\%.\end{array}$$

$$\text{ak} \quad f \text{ je veľmi ťažká} \Longrightarrow \exists \text{pekelne ťažké jadro } H,$$

$$\text{ak} \quad \begin{array}{c}\text{každý malý obvod} \\ \text{spočíta } f \text{ na } < 99\%\end{array} \Longrightarrow \exists \text{množina } H \quad \begin{array}{l}\forall \text{malý obvod dokáže vyriešiť} \\ \text{len } < 50 + \varepsilon\% \text{ vstupov z } H.\end{array}$$

Obmena:

$$\nexists \text{pekelne ťažké jadro} \Longrightarrow \exists \text{malý obvod, ktorý počíta } f \text{ skoro všade,}$$

$$\text{ak } \forall \text{množinu } H \quad \begin{array}{c}\exists \text{malý obvod } C, \text{ ktorý vyrieši} \\ \geq 50 + \varepsilon\% \text{ vstupov z } H\end{array} \Longrightarrow \begin{array}{c}\exists \text{malý obvod, ktorý} \\ \text{rieši } f \text{ na } \geq 99\%.\end{array}$$

$$\text{ak } \ f \text{ je veľmi ťažká} \Longrightarrow \exists \text{pekelne ťažké jadro } H,$$

$$\text{ak } \begin{array}{c}\text{každý malý obvod}\\ \text{spočíta } f \text{ na } < 99\%\end{array} \Longrightarrow \exists \text{množina } H \begin{array}{l}\forall \text{malý obvod dokáže vyriešiť}\\ \text{len } < 50+\varepsilon\% \text{ vstupov z } H.\end{array}$$

Obmena:

$$\nexists \text{pekelne ťažké jadro} \Longrightarrow \exists \text{malý obvod, ktorý počíta } f \text{ skoro všade,}$$

$$\text{ak } \forall \text{množinu } H \begin{array}{c}\exists \text{malý obvod } C, \text{ ktorý vyrieši}\\ \geq 50+\varepsilon\% \text{ vstupov z } H\end{array} \Longrightarrow \begin{array}{c}\exists \text{malý obvod, ktorý}\\ \text{rieši } f \text{ na } \geq 99\%.\end{array}$$

■ **Dôkaz.**

- uvažujme hru:
  - A zvolí 1%-hustú distribúciu H
  - B zvolí obvod C veľkosti $\leq S'$
  - A zaplatí B sumu $v = \Pr_{x \in_R H}[C(x) = f(x)]$
- z nášho predpokladu B vie vždy vyhrať aspoň $v \geq 1/2 + \varepsilon$

■ **Dôkaz.**

- uvažujme hru:
  - A zvolí 1%-hustú distribúciu H
  - B zvolí obvod C veľkosti $\leq S'$
  - A zaplatí B sumu $v = \Pr_{x \in_R H}[C(x) = f(x)]$
- z nášho predpokladu B vie vždy vyhrať aspoň $v \geq 1/2 + \varepsilon$

Hardcore lema

$$\forall H : \exists C : \Pr_{x \in_R H}[C(x) = f(x)] \geq 1/2 + \varepsilon$$

$$\Longrightarrow$$

$$\exists \mathscr{C} : \forall H : \Pr_{C \in_R \mathscr{C}, x \in_R H}[C(x) = f(x)] \geq 1/2 + \varepsilon$$

- pre každú distribúciu existuje slabý žiak $\Longrightarrow$ existuje náhodná distribúcia na žiakoch taká, že ak učiteľ vyberie písomku a ja si zvolím náhodného žiaka, ten odpovie správne s pp. $\geq 1/2 + \varepsilon$

Hardcore lema

- nazvime reťazec x „zlý“, ak $\Pr_{C \in_R \mathscr{C}}[C(x) = f(x)] < 1/2 + \varepsilon$
- zlých reťazcov je len málo, $< 1\%$, inak by sme mohli zvoliť H uniformne na zlých reťazcoch

Hardcore lema

- nazvime reťazec x „zlý“, ak $\Pr_{C \in_R \mathscr{C}}[C(x) = f(x)] < 1/2 + \varepsilon$
- zlých reťazcov je len málo, $< 1\%$, inak by sme mohli zvoliť H uniformne na zlých reťazcoch

Hardcore lema

- Nech $t = 50n/\varepsilon^2$, $C_1, \ldots, C_t \in_R \mathscr{C}$ a nech $C(x)$ je väčšinová odpoveď $C_1, \ldots, C_t$.
- Veľkosť C je $tS' + \text{dačo} < S$
- Z Černofovej nerovnosti vyplýva $\Pr[C(x) \neq f(x)] \ll 1/2^n$ pre všetky dobré x
- podľa union bound $\exists C$ taký, že $C = f$ pre všetky dobré x
- Keďže zlých x je $< 1\%$, C počíta f na 99% a $\mathrm{H}^{0.99}_{\mathrm{avg}}(f) < S$

□

Hardcore lema

- Nech $t = 50n/\varepsilon^2$, $C_1, \ldots, C_t \in_R \mathscr{C}$ a nech $C(x)$ je väčšinová odpoveď $C_1, \ldots, C_t$.
- Veľkosť C je $tS' + \text{dačo} < S$
- Z Černofovej nerovnosti vyplýva $\Pr[C(x) \neq f(x)] \ll 1/2^n$ pre všetky dobré x
- podľa union bound $\exists C$ taký, že $C = f$ pre všetky dobré x
- Keďže zlých x je $< 1\%$, C počíta f na 99% a $\mathrm{H}^{0.99}_{\mathrm{avg}}(f) < S$

Hardcore lema

- Nech $t = 50n/\varepsilon^2$, $C_1, \ldots, C_t \in_R \mathscr{C}$ a nech $C(x)$ je väčšinová odpoveď $C_1, \ldots, C_t$.
- Veľkosť C je $tS' + \text{dačo} < S$
- Z Černofovej nerovnosti vyplýva $\Pr[C(x) \neq f(x)] \ll 1/2^n$ pre všetky dobré x
- podľa union bound $\exists C$ taký, že $C = f$ pre všetky dobré x
- Keďže zlých x je $< 1\%$, C počíta f na 99% a $\mathrm{H}^{0.99}_{\mathrm{avg}}(f) < S$

Hardcore lema

- Nech $t = 50n/\varepsilon^2$, $C_1, \ldots, C_t \in_R \mathscr{C}$ a nech $C(x)$ je väčšinová odpoveď $C_1, \ldots, C_t$.
- Veľkosť C je $tS' + \text{dačo} < S$
- Z Černofovej nerovnosti vyplýva $\Pr[C(x) \neq f(x)] \ll 1/2^n$ pre všetky dobré x
- podľa union bound $\exists C$ taký, že $C = f$ pre všetky dobré x
- Keďže zlých x je $< 1\%$, C počíta f na 99% a $\mathrm{H}^{0.99}_{\mathrm{avg}}(f) < S$

Hardcore lema

- Nech $t = 50n/\varepsilon^2$, $C_1, \ldots, C_t \in_R \mathscr{C}$ a nech $C(x)$ je väčšinová odpoveď $C_1, \ldots, C_t$.
- Veľkosť C je $tS' + \text{dačo} < S$
- Z Černofovej nerovnosti vyplýva $\Pr[C(x) \neq f(x)] \ll 1/2^n$ pre všetky dobré x
- podľa union bound $\exists C$ taký, že $C = f$ pre všetky dobré x
- Keďže zlých x je $< 1\%$, C počíta f na 99% a $\mathrm{H}^{0.99}_{\mathrm{avg}}(f) < S$

□