Dolné odhady pre obvody

kuko

10.10.2017

Teória zložitosti II.

AC

Definícia

AC^0*:*

- *uniformné*
- $\wedge, \vee, \neg$
- $O(1)$ *hĺbka*
- poly$n$ *veľkosť*
- *hradlá* $\wedge$ *a* $\vee$ *majú neobmedzený počet vstupov*

AC hierarchia

Definícia

AC^k:

- *uniformné*
- $\wedge, \vee, \neg$
- $O(\log^k n)$ *hĺbka*
- poly$n$ *veľkosť*
- *hradlá* $\wedge$ *a* $\vee$ *majú neobmedzený počet vstupov*

Definícia

$AC = \bigcup_k AC^k$

AC hierarchia

Definícia

AC^k:

- *uniformné*
- $\wedge$, $\vee$, $\neg$
- $O(\log^k n)$ *hĺbka*
- poly$n$ *veľkosť*
- *hradlá* $\wedge$ *a* $\vee$ *majú neobmedzený počet vstupov*

Definícia

$\mathrm{AC} = \bigcup_k \mathrm{AC}^k$

NC hierarchia

Definícia

NC^k*:*

- *uniformné*
- $\wedge$, $\vee$, $\neg$
- $O(\log^k n)$ *hĺbka*
- poly$n$ *veľkosť*
- *hradlá* $\wedge$ *a* $\vee$ *majú 2 vstupy*

Definícia

$\mathrm{NC} = \bigcup_k \mathrm{NC}^k$

NC hierarchia

Definícia

NC^k*:*

- *uniformné*
- $\wedge$, $\vee$, $\neg$
- $O(\log^k n)$ *hĺbka*
- poly$n$ *veľkosť*
- *hradlá* $\wedge$ *a* $\vee$ *majú 2 vstupy*

Definícia

$\mathrm{NC} = \bigcup_k \mathrm{NC}^k$

NC hierarchia

Veta

$\mathrm{NC}_k \subseteq \mathrm{AC}_k \subseteq \mathrm{NC}_{k+1}$.

Veta

$\mathrm{AC} = \mathrm{NC} =$*jazyky s efektívnymi paralelnými algoritmami (PRAM, poly procesorov, polylog čas).*

Veta

$\mathrm{NL} \subseteq \mathrm{NC} \subseteq \mathrm{P}$

NC hierarchia

Veta

$\mathrm{NC}_k \subseteq \mathrm{AC}_k \subseteq \mathrm{NC}_{k+1}$.

Veta

$\mathrm{AC} = \mathrm{NC} =$*jazyky s efektívnymi paralelnými algoritmami (PRAM, poly procesorov, polylog čas).*

Veta

$\mathrm{NL} \subseteq \mathrm{NC} \subseteq \mathrm{P}$

NC hierarchia

Veta

$\mathrm{NC}_k \subseteq \mathrm{AC}_k \subseteq \mathrm{NC}_{k+1}$.

Veta

$\mathrm{AC} = \mathrm{NC} =$*jazyky s efektívnymi paralelnými algoritmami (PRAM, poly procesorov, polylog čas).*

Veta

$\mathrm{NL} \subseteq \mathrm{NC} \subseteq \mathrm{P}$

Parita

Veta (Furst, Saxe, Sipser)

$\bigoplus \notin \mathsf{AC}^0$.

Parita

Veta (Razborov, Smolensky)

$\bigoplus \notin \mathrm{ACC}^0(3)$.

$\textsc{Mod}_p \notin \mathrm{ACC}^0(q)$ *pre* $p \neq q \in \mathbb{P}$

Dôkaz.

1. obvod $\to$ polynóm, ktorý ho aproximuje
2. parita sa nedá dobre aproximovať polynómom
3. $\Rightarrow$ neexistuje malý obvod $O(1)$ hĺbky

Parita

Veta (Razborov, Smolensky)

$\bigoplus \notin \mathsf{ACC}^0(3)$.

$\textsc{Mod}_p \notin \mathsf{ACC}^0(q)$ *pre* $p \neq q \in \mathbb{P}$

Dôkaz.

1. obvod $\rightarrow$ polynóm, ktorý ho aproximuje
2. parita sa nedá dobre aproximovať polynómom
3. $\Rightarrow$ neexistuje malý obvod $O(1)$ hĺbky

Parita

Veta (Razborov, Smolensky)

$\bigoplus \notin \mathrm{ACC}^0(3)$.
$\mathrm{Mod}_p \notin \mathrm{ACC}^0(q)$ *pre* $p \neq q \in \mathbb{P}$

Dôkaz.

1. obvod $\rightarrow$ polynóm, ktorý ho aproximuje
2. parita sa nedá dobre aproximovať polynómom
3. $\Rightarrow$ neexistuje malý obvod $O(1)$ hĺbky

Parita

Veta (Razborov, Smolensky)

$\bigoplus \notin \mathrm{ACC}^0(3)$.
$\textsc{Mod}_p \notin \mathrm{ACC}^0(q)$ *pre* $p \neq q \in \mathbb{P}$

Dôkaz.

1. obvod $\to$ polynóm, ktorý ho aproximuje
2. parita sa nedá dobre aproximovať polynómom
3. $\Rightarrow$ neexistuje malý obvod $O(1)$ hĺbky

Parita

Veta (Razborov, Smolensky)

$\bigoplus \notin \mathrm{ACC}^0(3)$.
$\textsc{Mod}_p \notin \mathrm{ACC}^0(q)$ *pre* $p \neq q \in \mathbb{P}$

■ **Dôkaz.**

1. obvod $\rightarrow$ polynóm, ktorý ho aproximuje
2. parita sa nedá dobre aproximovať polynómom
3. $\Rightarrow$ neexistuje malý obvod $O(1)$ hĺbky

Parita

Veta (Razborov, Smolensky)

$\bigoplus \notin \mathrm{ACC}^0(3)$.
$\textsc{Mod}_p \notin \mathrm{ACC}^0(q)$ *pre* $p \neq q \in \mathbb{P}$

■ **Dôkaz.**

1. obvod $\to$ polynóm, ktorý ho aproximuje
2. parita sa nedá dobre aproximovať polynómom
3. $\Rightarrow$ neexistuje malý obvod $O(1)$ hĺbky

Parita

Presnejšie:

1. obvod hĺbky d, veľk. $S \longrightarrow$ polynóm stupňa $\sqrt{n}$
   - zhodný na $(1 - S/\Omega(2^{n^\varepsilon}))$-tine vstupov
2. polynóm stupňa $\sqrt{n}$ sa môže zhodovať najviac na $\leq 49/50$ vstupov
3. $\implies S = \Omega(2^{n^\varepsilon})$

Parita

Presnejšie:

1. obvod C hĺbky d, veľk. S $\longrightarrow$ poly $p \in \mathbb{Z}_3[\vec{X}]$ stupňa $(2\ell)^d$
   - $C(x) = p(x)$ na $(1 - S/2^\ell)$-tine vstupov
   - pre $2\ell = n^{1/2d}$:
     - $\deg p = \sqrt{n}$
     - $C(x) = p(x)$ na $(1 - S/2^{n^{1/2d}/2})$-tine vstupov
2. polynóm stupňa $\sqrt{n}$ sa môže zhodovať najviac na $\leq 49/50$ vstupov
3. $\Longrightarrow S > 2^{n^{1/2d}/2}/50 = \Omega(2^{n^\varepsilon})$

Parita

Presnejšie:

1. obvod C hĺbky d, veľk. $S \longrightarrow$ poly $p \in \mathbb{Z}_3[\vec{X}]$ stupňa $(2\ell)^d$
   - $C(x) = p(x)$ na $(1 - S/2^\ell)$-tine vstupov
   - pre $2\ell = n^{1/2d}$:
     - $\deg p = \sqrt{n}$
     - $C(x) = p(x)$ na $(1 - S/2^{n^{1/2d}/2})$-tine vstupov
2. polynóm stupňa $\sqrt{n}$ sa môže zhodovať najviac na $\leq 49/50$ vstupov
3. $\Longrightarrow S > 2^{n^{1/2d}/2}/50 = \Omega(2^{n^\varepsilon})$

Parita

Presnejšie:

1. obvod C hĺbky d, veľk. $S \longrightarrow$ poly $p \in \mathbb{Z}_3[\vec{X}]$ stupňa $(2\ell)^d$
   - $C(x) = p(x)$ na $(1 - S/2^\ell)$-tine vstupov
   - pre $2\ell = n^{1/2d}$:
     - $\deg p = \sqrt{n}$
     - $C(x) = p(x)$ na $(1 - S/2^{n^{1/2d}/2})$-tine vstupov
2. polynóm stupňa $\sqrt{n}$ sa môže zhodovať najviac na $\leq 49/50$ vstupov
3. $\implies S > 2^{n^{1/2d}/2}/50 = \Omega(2^{n^\varepsilon})$

Parita

Presnejšie:

1. obvod C hĺbky d, veľk. $S \longrightarrow$ poly $p \in \mathbb{Z}_3[\vec{X}]$ stupňa $(2\ell)^d$
   - $C(x) = p(x)$ na $(1 - S/2^{\ell})$-tine vstupov
   - pre $2\ell = n^{1/2d}$:
     - $\deg p = \sqrt{n}$
     - $C(x) = p(x)$ na $(1 - S/2^{n^{1/2d}/2})$-tine vstupov
2. polynóm stupňa $\sqrt{n}$ sa môže zhodovať najviac na $\leq 49/50$ vstupov
3. $\Longrightarrow S > 2^{n^{1/2d}/2}/50 = \Omega(2^{n^{\varepsilon}})$

Parita

1. obvod $\longrightarrow$ aproximujúci polynóm
   - vstupné hradlo x_i $\rightarrow$ polynóm X_i
   - $g = \neg f$ $\rightarrow$ polynóm $\tilde{g} = 1 - \tilde{f}$
   - $g = \mathrm{MOD}_3(f_1, \ldots, f_k)$ $\rightarrow$ polynóm $\tilde{g} = (\sum \tilde{f}_i)^2$
   - $g = \bigvee f_i$: naivný spôsob: $\tilde{g} = 1 - \prod(1 - \tilde{f}_i)$ – príliš veľký stupeň

Parita

1. obvod $\longrightarrow$ aproximujúci polynóm
   - vstupné hradlo x_i $\to$ polynóm X_i
   - $g = \neg f$ $\to$ polynóm $\tilde{g} = 1 - \tilde{f}$
   - $g = \mathrm{MOD}_3(f_1, \ldots, f_k)$ $\to$ polynóm $\tilde{g} = (\sum \tilde{f}_i)^2$
   - $g = \bigvee f_i$: naivný spôsob: $\tilde{g} = 1 - \prod(1 - \tilde{f}_i)$ – príliš veľký stupeň

Parita

1. obvod $\longrightarrow$ aproximujúci polynóm
   - vstupné hradlo x_i $\rightarrow$ polynóm X_i
   - $g = \neg f$ $\rightarrow$ polynóm $\tilde{g} = 1 - \tilde{f}$
   - $g = \mathrm{MOD}_3(f_1, \ldots, f_k)$ $\rightarrow$ polynóm $\tilde{g} = (\sum \tilde{f}_i)^2$
   - $g = \bigvee f_i$: naivný spôsob: $\tilde{g} = 1 - \prod(1 - \tilde{f}_i)$ – príliš veľký stupeň

Parita

1. obvod $\longrightarrow$ aproximujúci polynóm
   - vstupné hradlo x_i $\rightarrow$ polynóm X_i
   - $g = \neg f$ $\rightarrow$ polynóm $\tilde{g} = 1 - \tilde{f}$
   - $g = \mathrm{MOD}_3(f_1, \ldots, f_k)$ $\rightarrow$ polynóm $\tilde{g} = (\sum \tilde{f}_i)^2$
   - $g = \bigvee f_i$: naivný spôsob: $\tilde{g} = 1 - \prod(1 - \tilde{f}_i)$ – príliš veľký stupeň

Parita

1. obvod $\longrightarrow$ aproximujúci polynóm
   - vstupné hradlo x_i $\to$ polynóm X_i
   - $g = \neg f$ $\to$ polynóm $\tilde{g} = 1 - \tilde{f}$
   - $g = \mathrm{MOD}_3(f_1, \ldots, f_k)$ $\to$ polynóm $\tilde{g} = (\sum \tilde{f}_i)^2$
   - $g = \bigvee f_i$: naivný spôsob: $\tilde{g} = 1 - \prod(1 - \tilde{f}_i)$ – príliš veľký stupeň

Parita

1. obvod $\to$ aproximujúci polynóm
   - $g = \bigvee f_i \implies \exists i : f_i = 1$
   - $\Pr[\sum a_i f_i = 0] \leq 1/2$ pre náhodné a_i
   - vyberieme ℓ náhodných $a^{(1)}, \ldots, a^{(\ell)} \in \mathbb{Z}_3^n$
   - spočítame polynómy $\tilde{h}_k = (\sum_j a_i^{(k)} \tilde{f}_i)^2$
   - zrátame OR týchto ℓ členov naivnou metódou
   - $\forall x \Pr_{\vec{a}}[\tilde{g}(x) \neq C(x)] \leq 1/2^\ell \Rightarrow \exists \vec{a} : \Pr_x[\tilde{g}(x) \neq C(x)] \leq 1/2^\ell$
   - $g = \bigwedge f_i$ – ako $\bigvee$ cez deMorgana

Parita

1. obvod $\to$ aproximujúci polynóm
   - $g = \bigvee f_i \implies \exists i : f_i = 1$
   - $\Pr[\sum a_i f_i = 0] \le 1/2$ pre náhodné a_i
   - vyberieme ℓ náhodných $a^{(1)}, \ldots, a^{(\ell)} \in \mathbb{Z}_3^n$
   - spočítame polynómy $\tilde{h}_k = (\sum_j a_i^{(k)} \tilde{f}_i)^2$
   - zrátame OR týchto ℓ členov naivnou metódou
   - $\forall x \Pr_{\vec{a}}[\tilde{g}(x) \ne C(x)] \le 1/2^\ell \Rightarrow \exists \vec{a} : \Pr_x[\tilde{g}(x) \ne C(x)] \le 1/2^\ell$
   - $g = \bigwedge f_i$ – ako $\bigvee$ cez deMorgana

Parita

1. obvod $\rightarrow$ aproximujúci polynóm
   - $g = \bigvee f_i \implies \exists i : f_i = 1$
   - $\Pr[\sum a_i f_i = 0] \leq 1/2$ pre náhodné a_i
   - vyberieme ℓ náhodných $a^{(1)}, \ldots, a^{(\ell)} \in \mathbb{Z}_3^n$
   - spočítame polynómy $\tilde{h}_k = (\sum_j a_i^{(k)} \tilde{f}_i)^2$
   - zrátame OR týchto ℓ členov naivnou metódou
   - $\forall x \Pr_{\vec{a}}[\tilde{g}(x) \neq C(x)] \leq 1/2^\ell \Rightarrow \exists \vec{a} : \Pr_x[\tilde{g}(x) \neq C(x)] \leq 1/2^\ell$
   - $g = \bigwedge f_i$ – ako $\bigvee$ cez deMorgana

Parita

1. obvod $\rightarrow$ aproximujúci polynóm
   - $g = \bigvee f_i \implies \exists i : f_i = 1$
   - $\Pr[\sum a_i f_i = 0] \leq 1/2$ pre náhodné a_i
   - vyberieme ℓ náhodných $a^{(1)}, \ldots, a^{(\ell)} \in \mathbb{Z}_3^n$
   - spočítame polynómy $\tilde{h}_k = (\sum_j a_i^{(k)} \tilde{f}_i)^2$
   - zrátame OR týchto ℓ členov naivnou metódou
   - $\forall x \Pr_{\vec{a}}[\tilde{g}(x) \neq C(x)] \leq 1/2^\ell \Rightarrow \exists \vec{a} : \Pr_x[\tilde{g}(x) \neq C(x)] \leq 1/2^\ell$
   - $g = \bigwedge f_i$ – ako $\bigvee$ cez deMorgana

Parita

1. obvod $\rightarrow$ aproximujúci polynóm
   - $g = \bigvee f_i \implies \exists i : f_i = 1$
   - $\Pr[\sum a_i f_i = 0] \leq 1/2$ pre náhodné a_i
   - vyberieme ℓ náhodných $a^{(1)}, \ldots, a^{(\ell)} \in \mathbb{Z}_3^n$
   - spočítame polynómy $\tilde{h}_k = (\sum_j a_i^{(k)} \tilde{f}_i)^2$
   - zrátame OR týchto ℓ členov naivnou metódou
   - $\forall x \Pr_{\vec{a}}[\tilde{g}(x) \neq C(x)] \leq 1/2^\ell \Rightarrow \exists \vec{a} : \Pr_x[\tilde{g}(x) \neq C(x)] \leq 1/2^\ell$
   - $g = \bigwedge f_i$ – ako $\bigvee$ cez deMorgana

Parita

1. obvod $\rightarrow$ aproximujúci polynóm
   - $g = \bigvee f_i \implies \exists i : f_i = 1$
   - $\Pr[\sum a_i f_i = 0] \leq 1/2$ pre náhodné a_i
   - vyberieme ℓ náhodných $a^{(1)}, \ldots, a^{(\ell)} \in \mathbb{Z}_3^n$
   - spočítame polynómy $\tilde{h}_k = (\sum_j a_i^{(k)} \tilde{f}_i)^2$
   - zrátame OR týchto ℓ členov naivnou metódou
   - $\forall x \Pr_{\vec{a}}[\tilde{g}(x) \neq C(x)] \leq 1/2^\ell \Rightarrow \exists \vec{a} : \Pr_x[\tilde{g}(x) \neq C(x)] \leq 1/2^\ell$
   - $g = \bigwedge f_i$ – ako $\bigvee$ cez deMorgana

Parita

1. obvod $\to$ aproximujúci polynóm
   - $g = \bigvee f_i \implies \exists i : f_i = 1$
   - $\Pr[\sum a_i f_i = 0] \leq 1/2$ pre náhodné a_i
   - vyberieme ℓ náhodných $a^{(1)}, \ldots, a^{(\ell)} \in \mathbb{Z}_3^n$
   - spočítame polynómy $\tilde{h}_k = (\sum_j a_i^{(k)} \tilde{f}_i)^2$
   - zrátame OR týchto ℓ členov naivnou metódou
   - $\forall x \Pr_{\vec{a}}[\tilde{g}(x) \neq C(x)] \leq 1/2^\ell \Rightarrow \exists \vec{a} : \Pr_x[\tilde{g}(x) \neq C(x)] \leq 1/2^\ell$
   - $g = \bigwedge f_i$ – ako $\bigvee$ cez deMorgana

Parita

2. aproximujúci polynóm

- nech $f \in \mathbb{Z}_3[\vec{x}]$, $\deg f = \sqrt{n}$
- nech $G' = \{\vec{x} \mid f(\vec{x}) = \bigoplus(\vec{x})\} \subseteq \{0,1\}^n$;
- $y_i = 1 + x_i \pmod 3$ tá zobrazí $0/1 \mapsto 1/-1$,
  $G' \mapsto G \subseteq \{-1,1\}^n$, $f(\vec{x}) \mapsto g(\vec{y})$
- $f(\vec{x}) = \bigoplus(\vec{x}) \implies g(\vec{y}) = \prod y_i$
- g (stupňa $\sqrt{n}$) $= \prod y_i$ (stupňa n) na celom G
- $\implies G$ musí byť malá

Parita

2. aproximujúci polynóm
   - nech $f \in \mathbb{Z}_3[\vec{x}]$, $\deg f = \sqrt{n}$
   - nech $G' = \{\vec{x} \mid f(\vec{x}) = \bigoplus(\vec{x})\} \subseteq \{0,1\}^n$;
   - $y_i = 1 + x_i \pmod 3$ tá zobrazí $0/1 \mapsto 1/-1$, $G' \mapsto G \subseteq \{-1,1\}^n$, $f(\vec{x}) \mapsto g(\vec{y})$
   - $f(\vec{x}) = \bigoplus(\vec{x}) \implies g(\vec{y}) = \prod y_i$
   - g (stupňa $\sqrt{n}$) $= \prod y_i$ (stupňa n) na celom G
   - $\implies G$ musí byť malá

Parita

2. aproximujúci polynóm
   - nech $f \in \mathbb{Z}_3[\vec{x}]$, $\deg f = \sqrt{n}$
   - nech $G' = \{\vec{x} \mid f(\vec{x}) = \bigoplus(\vec{x})\} \subseteq \{0,1\}^n$;
   - $y_i = 1 + x_i \pmod 3$ tá zobrazí $0/1 \mapsto 1/-1$, $G' \mapsto G \subseteq \{-1,1\}^n$, $f(\vec{x}) \mapsto g(\vec{y})$
   - $f(\vec{x}) = \bigoplus(\vec{x}) \implies g(\vec{y}) = \prod y_i$
   - g (stupňa $\sqrt{n}$) $= \prod y_i$ (stupňa n) na celom G
   - $\implies G$ musí byť malá

Parita

2. aproximujúci polynóm

- nech $f \in \mathbb{Z}_3[\vec{x}]$, $\deg f = \sqrt{n}$
- nech $G' = \{\vec{x} \mid f(\vec{x}) = \bigoplus(\vec{x})\} \subseteq \{0,1\}^n$;
- $y_i = 1 + x_i \pmod 3$ tá zobrazí $0/1 \mapsto 1/-1$,
  $G' \mapsto G \subseteq \{-1,1\}^n$, $f(\vec{x}) \mapsto g(\vec{y})$
- $f(\vec{x}) = \bigoplus(\vec{x}) \implies g(\vec{y}) = \prod y_i$
- g (stupňa $\sqrt{n}$) $= \prod y_i$ (stupňa n) na celom G
- $\implies G$ musí byť malá

Parita

2. aproximujúci polynóm
   - nech $f \in \mathbb{Z}_3[\vec{x}]$, $\deg f = \sqrt{n}$
   - nech $G' = \{\vec{x} \mid f(\vec{x}) = \bigoplus(\vec{x})\} \subseteq \{0,1\}^n$;
   - $y_i = 1 + x_i \pmod 3$ tá zobrazí $0/1 \mapsto 1/-1$, $G' \mapsto G \subseteq \{-1,1\}^n$, $f(\vec{x}) \mapsto g(\vec{y})$
   - $f(\vec{x}) = \bigoplus(\vec{x}) \implies g(\vec{y}) = \prod y_i$
   - g (stupňa $\sqrt{n}$) $= \prod y_i$ (stupňa n) na celom G
   - $\implies G$ musí byť malá

Parita

2. aproximujúci polynóm
   - nech $f \in \mathbb{Z}_3[\vec{x}]$, $\deg f = \sqrt{n}$
   - nech $G' = \{\vec{x} \mid f(\vec{x}) = \bigoplus(\vec{x})\} \subseteq \{0,1\}^n$;
   - $y_i = 1 + x_i \pmod 3$ tá zobrazí $0/1 \mapsto 1/-1$,
     $G' \mapsto G \subseteq \{-1,1\}^n$, $f(\vec{x}) \mapsto g(\vec{y})$
   - $f(\vec{x}) = \bigoplus(\vec{x}) \implies g(\vec{y}) = \prod y_i$
   - g (stupňa $\sqrt{n}$) $= \prod y_i$ (stupňa n) na celom G
   - $\implies G$ musí byť malá

Parita

2. aproximujúci polynóm
   - nech $s : G \to \mathbb{Z}_3$ – takýchto funkcií je $3^{|G|}$
   - ukážeme, že takýchto funkcií je $\leq 3^{(49/50)2^n}$
   - funkcia s sa dá zapísať ako polynóm
     - stupeň každej premennej je ≤ 1
     - ak $\prod_{i \in I} y_i$ je monomiál v s, $|I| > n/2$
     - nahradíme ho $(\prod_{i \in I} y_i)(\prod_{i \notin I} y_i^2) = (\prod_i y_i)(\prod_{i \notin I} y_i) = g(\vec{y}) \prod_{i \notin I} y_i$
     - stupňa $n/2 + \sqrt{n}$
   - $\implies$ všetky fn $G \to \mathbb{Z}_3$ sa dajú vyjadriť ako súčet monomiálov stupňa $n/2 + \sqrt{n}$
   - tých je: $3^{\#\text{monomiálov}} \leq 3^{\sum_{i \leq n/2+\sqrt{n}} \binom{n}{i}} \leq 3^{(49/50)2^n}$

$\square$

Parita

2. aproximujúci polynóm

- nech $s : G \to \mathbb{Z}_3$ – takýchto funkcií je $3^{|G|}$
- ukážeme, že takýchto funkcií je $\leq 3^{(49/50)2^n}$
- funkcia s sa dá zapísať ako polynóm
  - stupeň každej premennej je ≤ 1
  - ak $\prod_{i \in I} y_i$ je monomiál v s, $|I| > n/2$
  - nahradíme ho $(\prod_{i \in I} y_i)(\prod_{i \notin I} y_i^2) = (\prod_i y_i)(\prod_{i \notin I} y_i) = g(\vec{y}) \prod_{i \notin I} y_i$
  - stupňa $n/2 + \sqrt{n}$
- $\implies$ všetky fn $G \to \mathbb{Z}_3$ sa dajú vyjadriť ako súčet monomiálov stupňa $n/2 + \sqrt{n}$
- tých je: $3^{\#\text{monomiálov}} \leq 3^{\sum_{i \leq n/2+\sqrt{n}} \binom{n}{i}} \leq 3^{(49/50)2^n}$

Parita

2. aproximujúci polynóm
   - nech $s : G \to \mathbb{Z}_3$ – takýchto funkcií je $3^{|G|}$
   - ukážeme, že takýchto funkcií je $\leq 3^{(49/50)2^n}$
   - funkcia s sa dá zapísať ako polynóm
     - stupeň každej premennej je ≤ 1
     - ak $\prod_{i \in I} y_i$ je monomiál v s, $|I| > n/2$
     - nahradíme ho $(\prod_{i \in I} y_i)(\prod_{i \notin I} y_i^2) = (\prod_i y_i)(\prod_{i \notin I} y_i) = g(\vec{y}) \prod_{i \notin I} y_i$
     - stupňa $n/2 + \sqrt{n}$
   - $\Longrightarrow$ všetky fn $G \to \mathbb{Z}_3$ sa dajú vyjadriť ako súčet monomiálov stupňa $n/2 + \sqrt{n}$
   - tých je: $3^{\#\text{monomiálov}} \leq 3^{\sum_{i \leq n/2 + \sqrt{n}} \binom{n}{i}} \leq 3^{(49/50)2^n}$

□

Parita

2. aproximujúci polynóm
   - nech $s : G \to \mathbb{Z}_3$ – takýchto funkcií je $3^{|G|}$
   - ukážeme, že takýchto funkcií je $\leq 3^{(49/50)2^n}$
   - funkcia s sa dá zapísať ako polynóm
     - stupeň každej premennej je ≤ 1
     - ak $\prod_{i \in I} y_i$ je monomiál v s, $|I| > n/2$
     - nahradíme ho $(\prod_{i \in I} y_i)(\prod_{i \notin I} y_i^2) = (\prod_i y_i)(\prod_{i \notin I} y_i) = g(\vec{y}) \prod_{i \notin I} y_i$
     - stupňa $n/2 + \sqrt{n}$
   - $\Longrightarrow$ všetky fn $G \to \mathbb{Z}_3$ sa dajú vyjadriť ako súčet monomiálov stupňa $n/2 + \sqrt{n}$
   - tých je: $3^{\#\text{monomiálov}} \leq 3^{\sum_{i \leq n/2+\sqrt{n}} \binom{n}{i}} \leq 3^{(49/50)2^n}$

□

Parita

2. aproximujúci polynóm

- nech $s : G \to \mathbb{Z}_3$ – takýchto funkcií je $3^{|G|}$
- ukážeme, že takýchto funkcií je $\leq 3^{(49/50)2^n}$
- funkcia s sa dá zapísať ako polynóm
  - stupeň každej premennej je ≤ 1
  - ak $\prod_{i \in I} y_i$ je monomiál v s, $|I| > n/2$
  - nahradíme ho $(\prod_{i \in I} y_i)(\prod_{i \notin I} y_i^2) = (\prod_i y_i)(\prod_{i \notin I} y_i) = g(\vec{y}) \prod_{i \notin I} y_i$
  - stupňa $n/2 + \sqrt{n}$
- $\implies$ všetky fn $G \to \mathbb{Z}_3$ sa dajú vyjadriť ako súčet monomiálov stupňa $n/2 + \sqrt{n}$
- tých je: $3^{\#\text{monomiálov}} \leq 3^{\sum_{i \leq n/2+\sqrt{n}} \binom{n}{i}} \leq 3^{(49/50)2^n}$

Parita

2. aproximujúci polynóm
   - nech $s : G \to \mathbb{Z}_3$ – takýchto funkcií je $3^{|G|}$
   - ukážeme, že takýchto funkcií je $\leq 3^{(49/50)2^n}$
   - funkcia s sa dá zapísať ako polynóm
     - stupeň každej premennej je ≤ 1
     - ak $\prod_{i \in I} y_i$ je monomiál v s, $|I| > n/2$
     - nahradíme ho $(\prod_{i \in I} y_i)(\prod_{i \notin I} y_i^2) = (\prod_i y_i)(\prod_{i \notin I} y_i) = g(\vec{y}) \prod_{i \notin I} y_i$
     - stupňa $n/2 + \sqrt{n}$
   - $\Longrightarrow$ všetky fn $G \to \mathbb{Z}_3$ sa dajú vyjadriť ako súčet monomiálov stupňa $n/2 + \sqrt{n}$
   - tých je: $3^{\#\text{monomiálov}} \leq 3^{\sum_{i \leq n/2 + \sqrt{n}} \binom{n}{i}} \leq 3^{(49/50)2^n}$

Parita

2. aproximujúci polynóm

- nech $s : G \to \mathbb{Z}_3$ – takýchto funkcií je $3^{|G|}$
- ukážeme, že takýchto funkcií je $\leq 3^{(49/50)2^n}$
- funkcia s sa dá zapísať ako polynóm
  - stupeň každej premennej je ≤ 1
  - ak $\prod_{i \in I} y_i$ je monomiál v s, $|I| > n/2$
  - nahradíme ho $(\prod_{i \in I} y_i)(\prod_{i \notin I} y_i^2) = (\prod_i y_i)(\prod_{i \notin I} y_i) = g(\vec{y}) \prod_{i \notin I} y_i$
  - stupňa $n/2 + \sqrt{n}$
- $\Longrightarrow$ všetky fn $G \to \mathbb{Z}_3$ sa dajú vyjadriť ako súčet monomiálov stupňa $n/2 + \sqrt{n}$
- tých je: $3^{\#\text{monomiálov}} \leq 3^{\sum_{i \leq n/2+\sqrt{n}} \binom{n}{i}} \leq 3^{(49/50)2^n}$

Parita

2. aproximujúci polynóm
   - nech $s : G \to \mathbb{Z}_3$ – takýchto funkcií je $3^{|G|}$
   - ukážeme, že takýchto funkcií je $\leq 3^{(49/50)2^n}$
   - funkcia s sa dá zapísať ako polynóm
     - stupeň každej premennej je ≤ 1
     - ak $\prod_{i \in I} y_i$ je monomiál v s, $|I| > n/2$
     - nahradíme ho $(\prod_{i \in I} y_i)(\prod_{i \notin I} y_i^2) = (\prod_i y_i)(\prod_{i \notin I} y_i) = g(\vec{y}) \prod_{i \notin I} y_i$
     - stupňa $n/2 + \sqrt{n}$
   - $\Longrightarrow$ všetky fn $G \to \mathbb{Z}_3$ sa dajú vyjadriť ako súčet monomiálov stupňa $n/2 + \sqrt{n}$
   - tých je: $3^{\#\text{monomiálov}} \leq 3^{\sum_{i \leq n/2+\sqrt{n}} \binom{n}{i}} \leq 3^{(49/50)2^n}$

□

Parita

2. aproximujúci polynóm

- nech $s : G \to \mathbb{Z}_3$ – takýchto funkcií je $3^{|G|}$
- ukážeme, že takýchto funkcií je $\leq 3^{(49/50)2^n}$
- funkcia s sa dá zapísať ako polynóm
  - stupeň každej premennej je ≤ 1
  - ak $\prod_{i\in I} y_i$ je monomiál v s, $|I| > n/2$
  - nahradíme ho $(\prod_{i\in I} y_i)(\prod_{i\notin I} y_i^2) = (\prod_i y_i)(\prod_{i\notin I} y_i) = g(\vec{y})\prod_{i\notin I} y_i$
  - stupňa $n/2 + \sqrt{n}$
- $\Longrightarrow$ všetky fn $G \to \mathbb{Z}_3$ sa dajú vyjadriť ako súčet monomiálov stupňa $n/2 + \sqrt{n}$
- tých je: $3^{\#\text{monomiálov}} \leq 3^{\sum_{i\leq n/2+\sqrt{n}}\binom{n}{i}} \leq 3^{(49/50)2^n}$

$\square$

PH vs. PSPACE

Dôsledok (Furst,Saxe,Sipser)

Existuje orákulum $A \subseteq \{0,1\}^*$, *pre ktoré* $\mathrm{PH}^A \neq \mathrm{PSPACE}^A$.

Dôkaz.

- sporom: $\forall A : \mathrm{PH}^A = \mathrm{PSPACE}^A \implies \bigoplus$ má obvod hĺbky $O(1)$ veľkosti $2^{(\log N)^c}$
- označme $A_n = A \cap \{0,1\}^n$ prvky A dĺžky n
- $L_A = \{0^n \mid |A_n| \bmod 2 = 1\} \subseteq \{0\}^*$
- $\forall A : L_A \in \mathrm{DSPACE}(n)^A$
- ak by $L_A \in \mathrm{PH}^A \implies \exists\Sigma_d$-stroj M s časom n^c
- BUNV nech sa M nepýta A na reťazce dĺžky inej ako $|x|$ (ktoré sú pre odpoveď irelevantné)

Dôsledok (Furst,Saxe,Sipser)

Existuje orákulum $A \subseteq \{0,1\}^*$, *pre ktoré* $\mathrm{PH}^A \neq \mathrm{PSPACE}^A$.

■ **Dôkaz.**

- sporom: $\forall A : \mathrm{PH}^A = \mathrm{PSPACE}^A \implies \bigoplus$ má obvod hĺbky $O(1)$ veľkosti $2^{(\log N)^c}$
- označme $A_n = A \cap \{0,1\}^n$ prvky A dĺžky n
- $L_A = \{0^n \mid |A_n| \bmod 2 = 1\} \subseteq \{0\}^*$
- $\forall A : L_A \in \mathrm{DSPACE}(n)^A$
- ak by $L_A \in \mathrm{PH}^A \implies \exists\Sigma_d$-stroj M s časom n^c
- BUNV nech sa M nepýta A na reťazce dĺžky inej ako $|x|$ (ktoré sú pre odpoveď irelevantné)

PH vs. PSPACE

Dôsledok (Furst,Saxe,Sipser)

Existuje orákulum $A \subseteq \{0,1\}^*$, *pre ktoré* $\mathrm{PH}^A \neq \mathrm{PSPACE}^A$.

Dôkaz.

- sporom: $\forall A : \mathrm{PH}^A = \mathrm{PSPACE}^A \implies \bigoplus$ má obvod hĺbky $O(1)$ veľkosti $2^{(\log N)^c}$
- označme $A_n = A \cap \{0,1\}^n$ prvky A dĺžky n
- $L_A = \{0^n \mid |A_n| \bmod 2 = 1\} \subseteq \{0\}^*$
- $\forall A : L_A \in \mathrm{DSPACE}(n)^A$
- ak by $L_A \in \mathrm{PH}^A \implies \exists\Sigma_d$-stroj M s časom n^c
- BUNV nech sa M nepýta A na reťazce dĺžky inej ako $|x|$ (ktoré sú pre odpoveď irelevantné)

PH vs. PSPACE

Dôsledok (Furst,Saxe,Sipser)

Existuje orákulum $A \subseteq \{0,1\}^*$, *pre ktoré* $\mathrm{PH}^A \neq \mathrm{PSPACE}^A$.

■ **Dôkaz.**

- sporom: $\forall A : \mathrm{PH}^A = \mathrm{PSPACE}^A \implies \bigoplus$ má obvod hĺbky $O(1)$ veľkosti $2^{(\log N)^c}$
- označme $A_n = A \cap \{0,1\}^n$ prvky A dĺžky n
- $L_A = \{0^n \mid |A_n| \bmod 2 = 1\} \subseteq \{0\}^*$
- $\forall A : L_A \in \mathrm{DSPACE}(n)^A$
- ak by $L_A \in \mathrm{PH}^A \implies \exists \Sigma_d$-stroj M s časom n^c
- BUNV nech sa M nepýta A na reťazce dĺžky inej ako $|x|$ (ktoré sú pre odpoveď irelevantné)

PH vs. PSPACE

Dôsledok (Furst,Saxe,Sipser)

Existuje orákulum $A \subseteq \{0,1\}^*$, *pre ktoré* $\mathrm{PH}^A \neq \mathrm{PSPACE}^A$.

■ **Dôkaz.**

- sporom: $\forall A : \mathrm{PH}^A = \mathrm{PSPACE}^A \implies \bigoplus$ má obvod hĺbky $O(1)$ veľkosti $2^{(\log N)^c}$
- označme $A_n = A \cap \{0,1\}^n$ prvky A dĺžky n
- $L_A = \{0^n \mid |A_n| \bmod 2 = 1\} \subseteq \{0\}^*$
- $\forall A : L_A \in \mathrm{DSPACE}(n)^A$
- ak by $L_A \in \mathrm{PH}^A \implies \exists \Sigma_d$-stroj M s časom n^c
- BUNV nech sa M nepýta A na reťazce dĺžky inej ako $|x|$ (ktoré sú pre odpoveď irelevantné)

PH vs. PSPACE

Dôsledok (Furst,Saxe,Sipser)

Existuje orákulum $A \subseteq \{0,1\}^*$, *pre ktoré* $\mathrm{PH}^A \neq \mathrm{PSPACE}^A$.

■ **Dôkaz.**

- sporom: $\forall A : \mathrm{PH}^A = \mathrm{PSPACE}^A \implies \bigoplus$ má obvod hĺbky $O(1)$ veľkosti $2^{(\log N)^c}$
- označme $A_n = A \cap \{0,1\}^n$ prvky A dĺžky n
- $L_A = \{0^n \mid |A_n| \bmod 2 = 1\} \subseteq \{0\}^*$
- $\forall A : L_A \in \mathrm{DSPACE}(n)^A$
- ak by $L_A \in \mathrm{PH}^A \implies \exists \Sigma_d$-stroj M s časom n^c
- BUNV nech sa M nepýta A na reťazce dĺžky inej ako $|x|$ (ktoré sú pre odpoveď irelevantné)

Dôsledok (Furst,Saxe,Sipser)

Existuje orákulum $A \subseteq \{0,1\}^*$, *pre ktoré* $\mathrm{PH}^A \neq \mathrm{PSPACE}^A$.

■ **Dôkaz.**

- sporom: $\forall A : \mathrm{PH}^A = \mathrm{PSPACE}^A \implies \bigoplus$ má obvod hĺbky $O(1)$ veľkosti $2^{(\log N)^c}$
- označme $A_n = A \cap \{0,1\}^n$ prvky A dĺžky n
- $L_A = \{0^n \mid |A_n| \bmod 2 = 1\} \subseteq \{0\}^*$
- $\forall A : L_A \in \mathrm{DSPACE}(n)^A$
- ak by $L_A \in \mathrm{PH}^A \implies \exists \Sigma_d$-stroj M s časom n^c
- BUNV nech sa M nepýta A na reťazce dĺžky inej ako $|x|$ (ktoré sú pre odpoveď irelevantné)

PH vs. PSPACE

Pokračovanie dôkazu

- obvod pre $\bigoplus$: vezmime strom výpočtov $M^A(0^n)$ pri všetkých možných orákulách A
- reťazec $\chi_{A_n} \longrightarrow N = 2^n$ vstupov obvodu
- konfigurácie $M \longrightarrow$ hradlá (najviac 2^{n^c})
- počiatočná konfigurácia $\longrightarrow$ výstupné hradlo
- dotaz na orákulum $\longrightarrow$ hradlo čítajúce vstup
- $\exists$-konfigurácia $\alpha \longrightarrow$ OR, vstupy sú $\forall$-konf. β, $\alpha \vdash^* \beta$
- $\forall$-konfigurácia $\longrightarrow$ AND, vstupy sú $\exists$-konf. β, $\alpha \vdash^* \beta$
- M iba d-krát alternuje $\longrightarrow$ obvod má hĺbku d
- veľkosť je $2^{n^c} = 2^{(\log N)^c}$

PH vs. PSPACE

Pokračovanie dôkazu

- obvod pre $\bigoplus$: vezmime strom výpočtov $M^A(0^n)$ pri všetkých možných orákulách A
- reťazec $\chi_{A_n} \longrightarrow N = 2^n$ vstupov obvodu
- konfigurácie $M \longrightarrow$ hradlá (najviac 2^{n^c})
- počiatočná konfigurácia $\longrightarrow$ výstupné hradlo
- dotaz na orákulum $\longrightarrow$ hradlo čítajúce vstup
- $\exists$-konfigurácia $\alpha \longrightarrow$ OR, vstupy sú $\forall$-konf. β, $\alpha \vdash^* \beta$
- $\forall$-konfigurácia $\longrightarrow$ AND, vstupy sú $\exists$-konf. β, $\alpha \vdash^* \beta$
- M iba d-krát alternuje $\longrightarrow$ obvod má hĺbku d
- veľkosť je $2^{n^c} = 2^{(\log N)^c}$

PH vs. PSPACE

Pokračovanie dôkazu

- obvod pre $\bigoplus$: vezmime strom výpočtov $M^A(0^n)$ pri všetkých možných orákulách A
- reťazec $\chi_{A_n} \longrightarrow N = 2^n$ vstupov obvodu
- konfigurácie $M \longrightarrow$ hradlá (najviac 2^{n^c})
- počiatočná konfigurácia $\longrightarrow$ výstupné hradlo
- dotaz na orákulum $\longrightarrow$ hradlo čítajúce vstup
- $\exists$-konfigurácia $\alpha \longrightarrow$ OR, vstupy sú $\forall$-konf. β, $\alpha \vdash^* \beta$
- $\forall$-konfigurácia $\longrightarrow$ AND, vstupy sú $\exists$-konf. β, $\alpha \vdash^* \beta$
- M iba d-krát alternuje $\longrightarrow$ obvod má hĺbku d
- veľkosť je $2^{n^c} = 2^{(\log N)^c}$

Pokračovanie dôkazu

- obvod pre $\bigoplus$: vezmime strom výpočtov $M^A(0^n)$ pri všetkých možných orákulách A
- reťazec $\chi_{A_n} \longrightarrow N = 2^n$ vstupov obvodu
- konfigurácie $M \longrightarrow$ hradlá (najviac 2^{n^c})
- počiatočná konfigurácia $\longrightarrow$ výstupné hradlo
- dotaz na orákulum $\longrightarrow$ hradlo čítajúce vstup
- $\exists$-konfigurácia $\alpha \longrightarrow$ OR, vstupy sú $\forall$-konf. β, $\alpha \vdash^* \beta$
- $\forall$-konfigurácia $\longrightarrow$ AND, vstupy sú $\exists$-konf. β, $\alpha \vdash^* \beta$
- M iba d-krát alternuje $\longrightarrow$ obvod má hĺbku d
- veľkosť je $2^{n^c} = 2^{(\log N)^c}$

Pokračovanie dôkazu

- obvod pre $\bigoplus$: vezmime strom výpočtov $M^A(0^n)$ pri všetkých možných orákulách A
- reťazec $\chi_{A_n} \longrightarrow N = 2^n$ vstupov obvodu
- konfigurácie $M \longrightarrow$ hradlá (najviac 2^{n^c})
- počiatočná konfigurácia $\longrightarrow$ výstupné hradlo
- dotaz na orákulum $\longrightarrow$ hradlo čítajúce vstup
- $\exists$-konfigurácia $\alpha \longrightarrow$ OR, vstupy sú $\forall$-konf. β, $\alpha \vdash^* \beta$
- $\forall$-konfigurácia $\longrightarrow$ AND, vstupy sú $\exists$-konf. β, $\alpha \vdash^* \beta$
- M iba d-krát alternuje $\longrightarrow$ obvod má hĺbku d
- veľkosť je $2^{n^c} = 2^{(\log N)^c}$

Pokračovanie dôkazu

- obvod pre $\bigoplus$: vezmime strom výpočtov $M^A(0^n)$ pri všetkých možných orákulách A
- reťazec $\chi_{A_n} \longrightarrow N = 2^n$ vstupov obvodu
- konfigurácie $M \longrightarrow$ hradlá (najviac 2^{n^c})
- počiatočná konfigurácia $\longrightarrow$ výstupné hradlo
- dotaz na orákulum $\longrightarrow$ hradlo čítajúce vstup
- $\exists$-konfigurácia $\alpha \longrightarrow$ OR, vstupy sú $\forall$-konf. β, $\alpha \vdash^* \beta$
- $\forall$-konfigurácia $\longrightarrow$ AND, vstupy sú $\exists$-konf. β, $\alpha \vdash^* \beta$
- M iba d-krát alternuje $\longrightarrow$ obvod má hĺbku d
- veľkosť je $2^{n^c} = 2^{(\log N)^c}$

PH vs. PSPACE

Pokračovanie dôkazu

- obvod pre $\bigoplus$: vezmime strom výpočtov $M^A(0^n)$ pri všetkých možných orákulách A
- reťazec $\chi_{A_n} \longrightarrow N = 2^n$ vstupov obvodu
- konfigurácie $M \longrightarrow$ hradlá (najviac 2^{n^c})
- počiatočná konfigurácia $\longrightarrow$ výstupné hradlo
- dotaz na orákulum $\longrightarrow$ hradlo čítajúce vstup
- $\exists$-konfigurácia $\alpha \longrightarrow$ OR, vstupy sú $\forall$-konf. β, $\alpha \vdash^* \beta$
- $\forall$-konfigurácia $\longrightarrow$ AND, vstupy sú $\exists$-konf. β, $\alpha \vdash^* \beta$
- M iba d-krát alternuje $\longrightarrow$ obvod má hĺbku d
- veľkosť je $2^{n^c} = 2^{(\log N)^c}$

PH vs. PSPACE

Pokračovanie dôkazu

- obvod pre $\bigoplus$: vezmime strom výpočtov $M^A(0^n)$ pri všetkých možných orákulách A
- reťazec $\chi_{A_n} \longrightarrow N = 2^n$ vstupov obvodu
- konfigurácie $M \longrightarrow$ hradlá (najviac 2^{n^c})
- počiatočná konfigurácia $\longrightarrow$ výstupné hradlo
- dotaz na orákulum $\longrightarrow$ hradlo čítajúce vstup
- $\exists$-konfigurácia $\alpha \longrightarrow$ OR, vstupy sú $\forall$-konf. β, $\alpha \vdash^* \beta$
- $\forall$-konfigurácia $\longrightarrow$ AND, vstupy sú $\exists$-konf. β, $\alpha \vdash^* \beta$
- M iba d-krát alternuje $\longrightarrow$ obvod má hĺbku d
- veľkosť je $2^{n^c} = 2^{(\log N)^c}$

PH vs. PSPACE

Pokračovanie dôkazu

- obvod pre $\bigoplus$: vezmime strom výpočtov $M^A(0^n)$ pri všetkých možných orákulách A
- reťazec $\chi_{A_n} \longrightarrow N = 2^n$ vstupov obvodu
- konfigurácie $M \longrightarrow$ hradlá (najviac 2^{n^c})
- počiatočná konfigurácia $\longrightarrow$ výstupné hradlo
- dotaz na orákulum $\longrightarrow$ hradlo čítajúce vstup
- $\exists$-konfigurácia $\alpha \longrightarrow$ OR, vstupy sú $\forall$-konf. β, $\alpha \vdash^* \beta$
- $\forall$-konfigurácia $\longrightarrow$ AND, vstupy sú $\exists$-konf. β, $\alpha \vdash^* \beta$
- M iba d-krát alternuje $\longrightarrow$ obvod má hĺbku d
- veľkosť je $2^{n^c} = 2^{(\log N)^c}$

PH vs. PSPACE

Pokračovanie dôkazu

- $\forall M \exists^\infty A : L(M^A) \neq L_A$
- $\exists A \forall M : L(M^A) \neq L_A$
- diagonalizáciou:
  - v k-tom kroku ideme obabrať M_k
  - vezmime n_k väčšie ako všetky doteraz
  - nech A_k je orákulum, ktoré obabre M_k na vstupe dĺžky n_k
  - $A = \bigcup_k A_k$

$\square$

Pokračovanie dôkazu

- $\forall M \exists^\infty A : L(M^A) \neq L_A$
- $\exists A \forall M : L(M^A) \neq L_A$
- diagonalizáciou:
  - v k-tom kroku ideme obabrať M_k
  - vezmime n_k väčšie ako všetky doteraz
  - nech A_k je orákulum, ktoré obabre M_k na vstupe dĺžky n_k
  - $A = \bigcup_k A_k$

$\square$

Pokračovanie dôkazu

- $\forall M \exists^\infty A : L(M^A) \neq L_A$
- $\exists A \forall M : L(M^A) \neq L_A$
- diagonalizáciou:
  - v k-tom kroku ideme obabrať M_k
  - vezmime n_k väčšie ako všetky doteraz
  - nech A_k je orákulum, ktoré obabre M_k na vstupe dĺžky n_k
  - $A = \bigcup_k A_k$

$\square$