Polynomiálna hierarchia

kuko

3.10.2017

Teória zložitosti II.

Polynomiálna hierarchia

Definícia (PH cez relácie)

R je polynomiálna relácia, ak $\forall(x, y_1, \ldots, y_n) \in R : \sum |y_i| \leq \text{poly}(x)$ *a R je rozhodnuteľná v polynomiálnom čase.*

$$\Sigma_\mathrm{k}^\mathrm{P} = \{L \mid \exists \textit{poly. rel. } R : x \in L \Leftrightarrow \exists y_1 \forall y_2 \cdots Q_k y_k (x, y_1, \ldots, y_n) \in R\}$$

$$\Pi_\mathrm{k}^\mathrm{P} = \{L \mid \exists \textit{poly. rel. } R : x \in L \Leftrightarrow \forall y_1 \exists y_2 \cdots \overline{Q}_k y_k (x, y_1, \ldots, y_n) \in R\}$$

$$\mathrm{PH} = \bigcup_k \Sigma_\mathrm{k}^\mathrm{P} = \bigcup_k \Pi_\mathrm{k}^\mathrm{P}$$

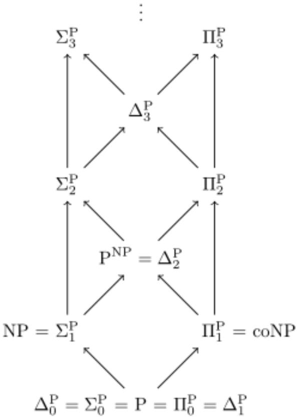
Polynomiálna hierarchia cez orákulá

Definícia (PH cez orákulá)

$$\Sigma_0^{\mathrm{P}} = \Pi_0^{\mathrm{P}} = \mathrm{P} \qquad \Sigma_{k+1}^{\mathrm{P}} = \mathrm{NP}^{\Sigma_k^{\mathrm{P}}} \qquad \Pi_{k+1}^{\mathrm{P}} = \mathrm{coNP}^{\Sigma_k^{\mathrm{P}}} = \mathrm{co}\Sigma_{k+1}^{\mathrm{P}}$$

$$\mathrm{PH} = \bigcup_k \Sigma_k^{\mathrm{P}} = \bigcup_k \Pi_k^{\mathrm{P}}$$

Polynomiálna hierarchia



Obr.: $\mathsf{P} \subseteq \mathsf{NP} \subseteq \Sigma_2^{\mathsf{P}} \subseteq \cdots \subseteq \mathsf{PH} \subseteq \mathsf{PSPACE}$

Kolaps PH

Veta

- *Ak* $\mathrm{P} = \mathrm{NP}$, *tak* $\mathrm{P} = \mathrm{PH}$.
- *Ak* $\Sigma_k^P = \Pi_k^P$, *tak* $\Sigma_k^P = \mathrm{PH}$.

Dôkaz.

- indukciou; nech $\mathrm{P} = \Sigma_i^P = \Pi_i^P$, $L \in \Sigma_{i+1}^P$
- $x \in L \Longleftrightarrow \exists u_1 \forall u_2 \cdots Q u_i : M(x, u_1, \ldots, u_i) = 1$
- nech $L' = \{(x, u_1) \mid \forall u_2 \cdots Q u_i : M(x, u_1, \ldots, u_i) = 1\}$
- $L' \in \Pi_i^P = \mathrm{P}$
- $\Rightarrow x \in L \Longleftrightarrow \exists u_1 : M'(x, u) = 1$, kde M' je NTS pre L'
- $\Rightarrow L \in \mathrm{NP} = \mathrm{P}$
- druhá časť vety sa ukáže podobne

$\square$

Kolaps PH

Veta

- *Ak* $\mathrm{P} = \mathrm{NP}$, *tak* $\mathrm{P} = \mathrm{PH}$.
- *Ak* $\Sigma_k^{\mathrm{P}} = \Pi_k^{\mathrm{P}}$, *tak* $\Sigma_k^{\mathrm{P}} = \mathrm{PH}$.

Dôkaz.

- indukciou; nech $\mathrm{P} = \Sigma_i^{\mathrm{P}} = \Pi_i^{\mathrm{P}}$, $L \in \Sigma_{i+1}^{\mathrm{P}}$
- $x \in L \iff \exists u_1 \forall u_2 \cdots Q u_i : M(x, u_1, \dots, u_i) = 1$
- nech $L' = \{(x, u_1) \mid \forall u_2 \cdots Q u_i : M(x, u_1, \dots, u_i) = 1\}$
- $L' \in \Pi_i^{\mathrm{P}} = \mathrm{P}$
- $\Rightarrow x \in L \iff \exists u_1 : M'(x, u) = 1$, kde M' je NTS pre L'
- $\Rightarrow L \in \mathrm{NP} = \mathrm{P}$
- druhá časť vety sa ukáže podobne

□

Kolaps PH

Veta

- *Ak* $\mathrm{P} = \mathrm{NP}$, *tak* $\mathrm{P} = \mathrm{PH}$.
- *Ak* $\Sigma_k^{\mathrm{P}} = \Pi_k^{\mathrm{P}}$, *tak* $\Sigma_k^{\mathrm{P}} = \mathrm{PH}$.

■ **Dôkaz.**

- indukciou; nech $\mathrm{P} = \Sigma_i^{\mathrm{P}} = \Pi_i^{\mathrm{P}}$, $L \in \Sigma_{i+1}^{\mathrm{P}}$
- $x \in L \iff \exists u_1 \forall u_2 \cdots Q u_i : M(x, u_1, \ldots, u_i) = 1$
- nech $L' = \{(x, u_1) \mid \forall u_2 \cdots Q u_i : M(x, u_1, \ldots, u_i) = 1\}$
- $L' \in \Pi_i^{\mathrm{P}} = \mathrm{P}$
- $\Rightarrow x \in L \iff \exists u_1 : M'(x, u) = 1$, kde M' je NTS pre L'
- $\Rightarrow L \in \mathrm{NP} = \mathrm{P}$
- druhá časť vety sa ukáže podobne

□

Kolaps PH

Veta

- *Ak* $\mathrm{P} = \mathrm{NP}$, *tak* $\mathrm{P} = \mathrm{PH}$.
- *Ak* $\Sigma_k^P = \Pi_k^P$, *tak* $\Sigma_k^P = \mathrm{PH}$.

Dôkaz.

- indukciou; nech $\mathrm{P} = \Sigma_i^P = \Pi_i^P$, $L \in \Sigma_{i+1}^P$
- $x \in L \iff \exists u_1 \forall u_2 \cdots Qu_i : M(x, u_1, \ldots, u_i) = 1$
- nech $L' = \{(x, u_1) \mid \forall u_2 \cdots Qu_i : M(x, u_1, \ldots, u_i) = 1\}$
- $L' \in \Pi_i^P = \mathrm{P}$
- $\Rightarrow x \in L \iff \exists u_1 : M'(x, u) = 1$, kde M' je NTS pre L'
- $\Rightarrow L \in \mathrm{NP} = \mathrm{P}$
- druhá časť vety sa ukáže podobne

$\square$

Kolaps PH

Veta

- *Ak* $\mathrm{P} = \mathrm{NP}$, *tak* $\mathrm{P} = \mathrm{PH}$.
- *Ak* $\Sigma_k^{\mathrm{P}} = \Pi_k^{\mathrm{P}}$, *tak* $\Sigma_k^{\mathrm{P}} = \mathrm{PH}$.

■ **Dôkaz.**

- indukciou; nech $\mathrm{P} = \Sigma_i^{\mathrm{P}} = \Pi_i^{\mathrm{P}}$, $L \in \Sigma_{i+1}^{\mathrm{P}}$
- $x \in L \iff \exists u_1 \forall u_2 \cdots Q u_i : M(x, u_1, \ldots, u_i) = 1$
- nech $L' = \{(x, u_1) \mid \forall u_2 \cdots Q u_i : M(x, u_1, \ldots, u_i) = 1\}$
- $L' \in \Pi_i^{\mathrm{P}} = \mathrm{P}$
- $\Rightarrow x \in L \iff \exists u_1 : M'(x, u) = 1$, kde M' je NTS pre L'
- $\Rightarrow L \in \mathrm{NP} = \mathrm{P}$
- druhá časť vety sa ukáže podobne

□

Kolaps PH

Veta

- *Ak* $\mathrm{P} = \mathrm{NP}$, *tak* $\mathrm{P} = \mathrm{PH}$.
- *Ak* $\Sigma_k^P = \Pi_k^P$, *tak* $\Sigma_k^P = \mathrm{PH}$.

Dôkaz.

- indukciou; nech $\mathrm{P} = \Sigma_i^P = \Pi_i^P$, $L \in \Sigma_{i+1}^P$
- $x \in L \iff \exists u_1 \forall u_2 \cdots Qu_i : M(x, u_1, \dots, u_i) = 1$
- nech $L' = \{(x, u_1) \mid \forall u_2 \cdots Qu_i : M(x, u_1, \dots, u_i) = 1\}$
- $L' \in \Pi_i^P = \mathrm{P}$
- $\Rightarrow x \in L \iff \exists u_1 : M'(x, u) = 1$, kde M' je NTS pre L'
- $\Rightarrow L \in \mathrm{NP} = \mathrm{P}$
- druhá časť vety sa ukáže podobne

Kolaps PH

Veta

- *Ak* $\mathrm{P} = \mathrm{NP}$, *tak* $\mathrm{P} = \mathrm{PH}$.
- *Ak* $\Sigma_k^{\mathrm{P}} = \Pi_k^{\mathrm{P}}$, *tak* $\Sigma_k^{\mathrm{P}} = \mathrm{PH}$.

■ **Dôkaz.**

- indukciou; nech $\mathrm{P} = \Sigma_i^{\mathrm{P}} = \Pi_i^{\mathrm{P}}$, $L \in \Sigma_{i+1}^{\mathrm{P}}$
- $x \in L \iff \exists u_1 \forall u_2 \cdots Q u_i : M(x, u_1, \dots, u_i) = 1$
- nech $L' = \{(x, u_1) \mid \forall u_2 \cdots Q u_i : M(x, u_1, \dots, u_i) = 1\}$
- $L' \in \Pi_i^{\mathrm{P}} = \mathrm{P}$
- $\Rightarrow x \in L \iff \exists u_1 : M'(x, u) = 1$, kde M' je NTS pre L'
- $\Rightarrow L \in \mathrm{NP} = \mathrm{P}$
- druhá časť vety sa ukáže podobne

□

Booleovské obvody a PH

Booleovské obvody

Definícia

SIZE$(s(n))$ – *jazyky akceptované triedou Booleovských obvodov s $s(n)$ hradlami (AND/OR/NOT).*
$\mathrm{P/poly} = \bigcup_k \mathrm{SIZE}(n^k)$ – *polynomiálne BO.*

Booleovské obvody

Veta

Uniformné polynomiálne veľké BO akceptujú P.

Veta

Polynomiálne BO akceptujú presne to, čo polynomiálne TS s polynomiálnou radou.

Booleovské obvody

Veta

Uniformné polynomiálne veľké BO akceptujú P.

Veta

Polynomiálne BO akceptujú presne to, čo polynomiálne TS s polynomiálnou radou.

- Hypotéza: NP $\not\subseteq$ P/poly
- NP $\not\subseteq$ P/poly $\Rightarrow$ P $\neq$ NP
- platí to aj obrátene?

Booleovské obvody a PH

- Hypotéza: $\mathrm{NP} \not\subseteq \mathrm{P/poly}$
- $\mathrm{NP} \not\subseteq \mathrm{P/poly} \Rightarrow \mathrm{P} \neq \mathrm{NP}$
- platí to aj obrátene?

Booleovské obvody a PH

- Hypotéza: $\mathrm{NP} \not\subseteq \mathrm{P/poly}$
- $\mathrm{NP} \not\subseteq \mathrm{P/poly} \Rightarrow \mathrm{P} \neq \mathrm{NP}$
- platí to aj obrátene?

Veta (Karp-Lipton)

Ak $\mathrm{NP} \subseteq \mathrm{P}/\mathrm{poly}$, *tak* $\mathrm{PH} = \Sigma_2^{\mathrm{P}}$.

■ **Dôkaz.**

- Nech $\mathrm{SAT} \in \mathrm{P}/\mathrm{poly}$, ukážeme, že $\forall\exists\mathrm{SAT} \in \Sigma_2^{\mathrm{P}}$
- $\forall u : \exists v : \phi(u, v)$?
- uvažujme konkrétne u; $\exists v : \phi(u, v)$? je SAT
- podľa predpokladu existuje obvod C, ktorý pre dané u nájde vhodné v
- t.j. $\forall u : \exists v : \phi(u, v) \iff \exists C : \forall u : \phi(u, C(v))$

□

Karp-Lipton

Veta (Karp-Lipton)

Ak $\mathrm{NP} \subseteq \mathrm{P/poly}$, *tak* $\mathrm{PH} = \Sigma_2^{\mathrm{P}}$.

Dôkaz.

- Nech $\textsc{Sat} \in \mathrm{P/poly}$, ukážeme, že $\forall\exists\textsc{Sat} \in \Sigma_2^{\mathrm{P}}$
- $\forall u : \exists v : \phi(u, v)$?
- uvažujme konkrétne u; $\exists v : \phi(u, v)$? je $\textsc{Sat}$
- podľa predpokladu existuje obvod C, ktorý pre dané u nájde vhodné v
- t.j. $\forall u : \exists v : \phi(u, v) \iff \exists C : \forall u : \phi(u, C(v))$

$\square$

Veta (Karp-Lipton)

Ak NP $\subseteq$ P/poly, *tak* PH $= \Sigma_2^P$.

■ **Dôkaz.**

- Nech $\textsc{Sat} \in \mathrm{P/poly}$, ukážeme, že $\forall\exists\textsc{Sat} \in \Sigma_2^P$
- $\forall u : \exists v : \phi(u, v)$?
- uvažujme konkrétne u; $\exists v : \phi(u, v)$? je $\textsc{Sat}$
- podľa predpokladu existuje obvod C, ktorý pre dané u nájde vhodné v
- t.j. $\forall u : \exists v : \phi(u, v) \iff \exists C : \forall u : \phi(u, C(v))$

□

Karp-Lipton

Veta (Karp-Lipton)

Ak $\mathsf{NP} \subseteq \mathsf{P/poly}$, *tak* $\mathsf{PH} = \Sigma_2^{\mathsf{P}}$.

■ **Dôkaz.**

- Nech $\textsc{Sat} \in \mathsf{P/poly}$, ukážeme, že $\forall\exists\textsc{Sat} \in \Sigma_2^{\mathsf{P}}$
- $\forall u : \exists v : \phi(u, v)$?
- uvažujme konkrétne u; $\exists v : \phi(u, v)$? je $\textsc{Sat}$
- podľa predpokladu existuje obvod C, ktorý pre dané u nájde vhodné v
- t.j. $\forall u : \exists v : \phi(u, v) \iff \exists C : \forall u : \phi(u, C(v))$

□

Karp-Lipton

Veta (Karp-Lipton)

Ak NP $\subseteq$ P/poly, *tak* PH $= \Sigma_2^P$.

■ **Dôkaz.**

- Nech $\textsc{Sat} \in \mathrm{P/poly}$, ukážeme, že $\forall\exists\textsc{Sat} \in \Sigma_2^P$
- $\forall u : \exists v : \phi(u, v)$?
- uvažujme konkrétne u; $\exists v : \phi(u, v)$? je $\textsc{Sat}$
- podľa predpokladu existuje obvod C, ktorý pre dané u nájde vhodné v
- t.j. $\forall u : \exists v : \phi(u, v) \iff \exists C : \forall u : \phi(u, C(v))$

□

Veta (Karp-Lipton)

Ak $\mathrm{NP} \subseteq \mathrm{P/poly}$*, tak* $\mathrm{PH} = \Sigma_2^{\mathrm{P}}$.

Dôkaz.

- Nech $\textsc{Sat} \in \mathrm{P/poly}$, ukážeme, že $\forall\exists\textsc{Sat} \in \Sigma_2^{\mathrm{P}}$
- $\forall u : \exists v : \phi(u, v)$?
- uvažujme konkrétne u; $\exists v : \phi(u, v)$? je $\textsc{Sat}$
- podľa predpokladu existuje obvod C, ktorý pre dané u nájde vhodné v
- t.j. $\forall u : \exists v : \phi(u, v) \iff \exists C : \forall u : \phi(u, C(v))$

$\square$

Booleovské obvody

- Hypotéza: NP $\not\subseteq$ P/poly
- NEXP $\not\subseteq$ P/poly, dokonca NEXP $\not\subseteq$ NC^1 (obvody poly veľkosti a log-hĺbky) je otvorený problém
- vieme, že existujú $L \in$ NEXP, ktoré nemajú obvod poly veľkosti a konštantnej hĺbky, ani keď pridáme MOD-hradlá.

Booleovské obvody

- Hypotéza: NP $\not\subseteq$ P/poly
- NEXP $\not\subseteq$ P/poly, dokonca NEXP $\not\subseteq$ NC^1 (obvody poly veľkosti a log-hĺbky) je otvorený problém
- vieme, že existujú $L \in$ NEXP, ktoré nemajú obvod poly veľkosti a konštantnej hĺbky, ani keď pridáme MOD-hradlá.

Booleovské obvody

- Hypotéza: NP $\not\subseteq$ P/poly
- NEXP $\not\subseteq$ P/poly, dokonca NEXP $\not\subseteq$ NC^1 (obvody poly veľkosti a log-hĺbky) je otvorený problém
- vieme, že existujú $L \in$ NEXP, ktoré nemajú obvod poly veľkosti a konštantnej hĺbky, ani keď pridáme MOD-hradlá.

Booleovské obvody a PH

Veta (Kannan)

$\forall k \exists L \in \Sigma_2^{\mathrm{P}} \cap \Pi_2^{\mathrm{P}} - \mathrm{SIZE}(n^k)$
(Tzn. pre každý polynóm p ∃ jazyk v PH*, ktorý nemá obvod veľkosti* $p(n)$*. Pozor: z toho vôbec nevyplýva, že* $\exists L \in PH - \mathrm{P/poly}$*.)*

■ **Dôkaz.**

- Nech $L \in \mathrm{SIZE}(n^{k+1}) - \mathrm{SIZE}(n^k)$ s lexikograficky najmenším obvodom
- $L \in \Sigma_4^{\mathrm{P}}$
- $\textsc{Sat} \notin \mathrm{SIZE}(n^k) \Rightarrow \textsc{Sat}$ je hľadaný jazyk
- $\textsc{Sat} \in \mathrm{SIZE}(n^k) \Rightarrow \mathrm{NP} \subseteq \mathrm{P/poly} \Rightarrow \mathrm{PH}$ skolabuje [Karp-Lipton] a $L \in \Sigma_4^{\mathrm{P}} = \Sigma_2^{\mathrm{P}} = \Pi_2^{\mathrm{P}}$

□

Booleovské obvody a PH

Veta (Kannan)

$\forall k \exists L \in \Sigma_2^{\mathrm{P}} \cap \Pi_2^{\mathrm{P}} - \mathrm{SIZE}(n^k)$
(Tzn. pre každý polynóm p $\exists$ *jazyk v* PH, *ktorý nemá obvod veľkosti* $p(n)$. *Pozor: z toho vôbec nevyplýva, že* $\exists L \in PH - \mathrm{P/poly}$.*)*

■ **Dôkaz.**

- Nech $L \in \mathrm{SIZE}(n^{k+1}) - \mathrm{SIZE}(n^k)$ s lexikograficky najmenším obvodom
- $L \in \Sigma_4^{\mathrm{P}}$
- $\textsc{Sat} \notin \mathrm{SIZE}(n^k) \Rightarrow \textsc{Sat}$ je hľadaný jazyk
- $\textsc{Sat} \in \mathrm{SIZE}(n^k) \Rightarrow \mathrm{NP} \subseteq \mathrm{P/poly} \Rightarrow$ PH skolabuje [Karp-Lipton] a $L \in \Sigma_4^{\mathrm{P}} = \Sigma_2^{\mathrm{P}} = \Pi_2^{\mathrm{P}}$

□

Booleovské obvody a PH

Veta (Kannan)

$\forall k \exists L \in \Sigma_2^{\mathrm{P}} \cap \Pi_2^{\mathrm{P}} - \mathrm{SIZE}(n^k)$
(Tzn. pre každý polynóm p ∃ jazyk v PH*, ktorý nemá obvod veľkosti* $p(n)$*. Pozor: z toho vôbec nevyplýva, že* $\exists L \in PH - \mathrm{P/poly}$*.)*

Dôkaz.

- Nech $L \in \mathrm{SIZE}(n^{k+1}) - \mathrm{SIZE}(n^k)$ s lexikograficky najmenším obvodom
- $L \in \Sigma_4^{\mathrm{P}}$
- $\textsc{Sat} \notin \mathrm{SIZE}(n^k) \Rightarrow \textsc{Sat}$ je hľadaný jazyk
- $\textsc{Sat} \in \mathrm{SIZE}(n^k) \Rightarrow \mathrm{NP} \subseteq \mathrm{P/poly} \Rightarrow \mathrm{PH}$ skolabuje [Karp-Lipton] a $L \in \Sigma_4^{\mathrm{P}} = \Sigma_2^{\mathrm{P}} = \Pi_2^{\mathrm{P}}$

Booleovské obvody a PH

Veta (Kannan)

$\forall k \exists L \in \Sigma_2^P \cap \Pi_2^P - \mathrm{SIZE}(n^k)$
(Tzn. pre každý polynóm p ∃ jazyk v PH, ktorý nemá obvod veľkosti p(n). Pozor: z toho vôbec nevyplýva, že $\exists L \in PH - \mathrm{P/poly}$.*)*

■ Dôkaz.

- Nech $L \in \mathrm{SIZE}(n^{k+1}) - \mathrm{SIZE}(n^k)$ s lexikograficky najmenším obvodom
- $L \in \Sigma_4^P$
- $\textsc{Sat} \notin \mathrm{SIZE}(n^k) \Rightarrow \textsc{Sat}$ je hľadaný jazyk
- $\textsc{Sat} \in \mathrm{SIZE}(n^k) \Rightarrow \mathrm{NP} \subseteq \mathrm{P/poly} \Rightarrow$ PH skolabuje [Karp-Lipton] a $L \in \Sigma_4^P = \Sigma_2^P = \Pi_2^P$

Booleovské obvody a PH

Veta (Kannan)

$\forall k \exists L \in \Sigma_2^{\mathrm{P}} \cap \Pi_2^{\mathrm{P}} - \mathrm{SIZE}(n^k)$
(Tzn. pre každý polynóm p $\exists$ jazyk v PH, *ktorý nemá obvod veľkosti p(n). Pozor: z toho vôbec nevyplýva, že* $\exists L \in PH - \mathrm{P/poly}$.*)*

■ **Dôkaz.**

- Nech $L \in \mathrm{SIZE}(n^{k+1}) - \mathrm{SIZE}(n^k)$ s lexikograficky najmenším obvodom
- $L \in \Sigma_4^{\mathrm{P}}$
- $\textsc{Sat} \notin \mathrm{SIZE}(n^k) \Rightarrow \textsc{Sat}$ je hľadaný jazyk
- $\textsc{Sat} \in \mathrm{SIZE}(n^k) \Rightarrow \mathrm{NP} \subseteq \mathrm{P/poly} \Rightarrow$ PH skolabuje [Karp-Lipton] a $L \in \Sigma_4^{\mathrm{P}} = \Sigma_2^{\mathrm{P}} = \Pi_2^{\mathrm{P}}$

$\square$

Pravdepodobnostné algoritmy a PH

BPP

Definícia

BPP – *jazyky akceptované pravdepodobnostnými TS, takými, že*

- *ak* $x \in L$, *tak* $\Pr_r[M(x) = 1] \geq 2/3$
- *ak* $x \notin L$, *tak* $\Pr_r[M(x) = 1] \leq 1/3$.

Veta

BPP – *jazyky akceptované pravdepodobnostnými TS, takými, že*

- *ak* $x \in L$, *tak* $\Pr_r[M(x,r) = 1] \geq 1 - 1/2^n$
- *ak* $x \notin L$, *tak* $\Pr_r[M(x,r) = 1] \leq 1/2^n$.

BPP

Definícia

BPP – *jazyky akceptované pravdepodobnostnými TS, takými, že*

- *ak* $x \in L$, *tak* $\Pr_r[M(x) = 1] \geq 2/3$
- *ak* $x \notin L$, *tak* $\Pr_r[M(x) = 1] \leq 1/3$.

Veta

BPP – *jazyky akceptované pravdepodobnostnými TS, takými, že*

- *ak* $x \in L$, *tak* $\Pr_r[M(x, r) = 1] \geq 1 - 1/2^n$
- *ak* $x \notin L$, *tak* $\Pr_r[M(x, r) = 1] \leq 1/2^n$.

BPP

- Hypotéza: P $=$ BPP, t.j. algoritmy vieme efektívne „derandomizovať"
- aj BPP $\subseteq$ NP je otvorený problém
- ak existujú „ťažké" funkcie, tak P $=$ BPP

BPP

- Hypotéza: P = BPP, t.j. algoritmy vieme efektívne „derandomizovať“
- aj BPP $\subseteq$ NP je otvorený problém
- ak existujú „ťažké“ funkcie, tak P = BPP

BPP

- Hypotéza: $\mathrm{P} = \mathrm{BPP}$, t.j. algoritmy vieme efektívne „derandomizovať"
- aj $\mathrm{BPP} \subseteq \mathrm{NP}$ je otvorený problém
- ak existujú „ťažké" funkcie, tak $\mathrm{P} = \mathrm{BPP}$

Veta (Sipser-Gács)

$$\mathrm{BPP} \subseteq \Sigma_2^P \cap \Pi_2^P$$

Dôkaz.

- nech M je PTS, ktorý na vstupe dĺžky n použije m náhodných bitov
- nech $S_x = \{r \mid M(x,r) = 1\}$
- ak $x \in L$, tak $|S_x| \geq (1 - 2^{-n}) \cdot 2^m$ je veľká
- ak $x \notin L$, tak $|S_x| \leq 2^{m-n}$ je malá
- dokážeme, že ak je S_x veľká, existuje m posunutí, ktoré pokryje celé $\{0,1\}^m$, ale ak je S_x malá, žiadnych m posunutí nepokryje celé $\{0,1\}^m$

BPP a PH

Veta (Sipser-Gács)

$$\mathrm{BPP} \subseteq \Sigma_2^{\mathrm{P}} \cap \Pi_2^{\mathrm{P}}$$

■ **Dôkaz.**

- nech M je PTS, ktorý na vstupe dĺžky n použije m náhodných bitov
- nech $S_x = \{r \mid M(x,r) = 1\}$
- ak $x \in L$, tak $|S_x| \geq (1 - 2^{-n}) \cdot 2^m$ je veľká
- ak $x \notin L$, tak $|S_x| \leq 2^{m-n}$ je malá
- dokážeme, že ak je S_x veľká, existuje m posunutí, ktoré pokryje celé $\{0,1\}^m$, ale ak je S_x malá, žiadnych m posunutí nepokryje celé $\{0,1\}^m$

Veta (Sipser-Gács)

$$\mathrm{BPP} \subseteq \Sigma_2^\mathrm{P} \cap \Pi_2^\mathrm{P}$$

■ **Dôkaz.**

- nech M je PTS, ktorý na vstupe dĺžky n použije m náhodných bitov
- nech $S_x = \{r \mid M(x,r) = 1\}$
- ak $x \in L$, tak $|S_x| \geq (1-2^{-n}) \cdot 2^m$ je veľká
- ak $x \notin L$, tak $|S_x| \leq 2^{m-n}$ je malá
- dokážeme, že ak je S_x veľká, existuje m posunutí, ktoré pokryje celé $\{0,1\}^m$, ale ak je S_x malá, žiadnych m posunutí nepokryje celé $\{0,1\}^m$

Veta (Sipser-Gács)

$$\mathrm{BPP} \subseteq \Sigma_2^{\mathrm{P}} \cap \Pi_2^{\mathrm{P}}$$

Dôkaz.

- nech M je PTS, ktorý na vstupe dĺžky n použije m náhodných bitov
- nech $S_x = \{r \mid M(x,r) = 1\}$
- ak $x \in L$, tak $|S_x| \geq (1 - 2^{-n}) \cdot 2^m$ je veľká
- ak $x \notin L$, tak $|S_x| \leq 2^{m-n}$ je malá
- dokážeme, že ak je S_x veľká, existuje m posunutí, ktoré pokryje celé $\{0,1\}^m$, ale ak je S_x malá, žiadnych m posunutí nepokryje celé $\{0,1\}^m$

BPP a PH

Veta (Sipser-Gács)

$$\mathrm{BPP} \subseteq \Sigma_2^{\mathrm{P}} \cap \Pi_2^{\mathrm{P}}$$

Dôkaz.

- nech M je PTS, ktorý na vstupe dĺžky n použije m náhodných bitov
- nech $S_x = \{r \mid M(x,r) = 1\}$
- ak $x \in L$, tak $|S_x| \geq (1 - 2^{-n}) \cdot 2^m$ je veľká
- ak $x \notin L$, tak $|S_x| \leq 2^{m-n}$ je malá
- dokážeme, že ak je S_x veľká, existuje m posunutí, ktoré pokryje celé $\{0,1\}^m$, ale ak je S_x malá, žiadnych m posunutí nepokryje celé $\{0,1\}^m$

Veta (Sipser-Gács)

$$\mathrm{BPP} \subseteq \Sigma_2^{\mathrm{P}} \cap \Pi_2^{\mathrm{P}}$$

■ **Dôkaz.**

- nech M je PTS, ktorý na vstupe dĺžky n použije m náhodných bitov
- nech $S_x = \{r \mid M(x,r) = 1\}$
- ak $x \in L$, tak $|S_x| \geq (1 - 2^{-n}) \cdot 2^m$ je veľká
- ak $x \notin L$, tak $|S_x| \leq 2^{m-n}$ je malá
- dokážeme, že ak je S_x veľká, existuje m posunutí, ktoré pokryje celé $\{0,1\}^m$, ale ak je S_x malá, žiadnych m posunutí nepokryje celé $\{0,1\}^m$

BPP a PH

Pokračovanie dôkazu

- ak $|S| \leq 2^{m-n}$ je malá
  - $\Rightarrow m \cdot |S| \leq m2^{m-n} \ll 2^m$
- ak $|S| \geq (1 - 2^{-n}) \cdot 2^m$ je veľká
  - ukážeme, že náhodné posunutia $(S \oplus t_i)$ nepokryjú všetky reťazce s pp. $\leq 100\%$
  - $\Pr_{r,t}[\exists r \notin \bigcup S \oplus t_i]$
  - $\leq 2^m \cdot \Pr_t[r \notin \bigcup S \oplus t_i]$
  - $\leq 2^m \cdot ((2^{-n})^m) \leq 2^{m-mn} < 1$

$\square$

BPP a PH

Pokračovanie dôkazu

- ak $|S| \leq 2^{m-n}$ je malá
  - $\Rightarrow m \cdot |S| \leq m2^{m-n} \ll 2^m$
- ak $|S| \geq (1-2^{-n}) \cdot 2^m$ je veľká
  - ukážeme, že náhodné posunutia $(S \oplus t_i)$ nepokryjú všetky reťazce s pp. $\leq 100\%$
  - $\Pr_{r,t}[\exists r \notin \bigcup S \oplus t_i]$
  - $\leq 2^m \cdot \Pr_t[r \notin \bigcup S \oplus t_i]$
  - $\leq 2^m \cdot ((2^{-n})^m) \leq 2^{m-mn} < 1$

$\square$

BPP a PH

Pokračovanie dôkazu

- ak $|S| \leq 2^{m-n}$ je malá
  - $\Rightarrow m \cdot |S| \leq m2^{m-n} \ll 2^m$
- ak $|S| \geq (1 - 2^{-n}) \cdot 2^m$ je veľká
  - ukážeme, že náhodné posunutia $(S \oplus t_i)$ nepokryjú všetky reťazce s pp. $\leq 100\%$
  - $\Pr_{r,t}[\exists r \notin \bigcup S \oplus t_i]$
  - $\leq 2^m \cdot \Pr_t[r \notin \bigcup S \oplus t_i]$
  - $\leq 2^m \cdot ((2^{-n})^m) \leq 2^{m-mn} < 1$

$\square$

BPP a PH

Pokračovanie dôkazu

- ak $|S| \leq 2^{m-n}$ je malá
  - $\Rightarrow m \cdot |S| \leq m2^{m-n} \ll 2^m$
- ak $|S| \geq (1 - 2^{-n}) \cdot 2^m$ je veľká
  - ukážeme, že náhodné posunutia $(S \oplus t_i)$ nepokryjú všetky reťazce s pp. $\leq 100\%$
  - $\Pr_{r,t}[\exists r \notin \bigcup S \oplus t_i]$
  - $\leq 2^m \cdot \Pr_t[r \notin \bigcup S \oplus t_i]$
  - $\leq 2^m \cdot ((2^{-n})^m) \leq 2^{m-mn} < 1$

$\square$

BPP a PH

Pokračovanie dôkazu

- ak $|S| \leq 2^{m-n}$ je malá
  - $\Rightarrow m \cdot |S| \leq m2^{m-n} \ll 2^m$
- ak $|S| \geq (1-2^{-n}) \cdot 2^m$ je veľká
  - ukážeme, že náhodné posunutia $(S \oplus t_i)$ nepokryjú všetky reťazce s pp. $\leq 100\%$
  - $\Pr_{r,t}[\exists r \notin \bigcup S \oplus t_i]$
  - $\leq 2^m \cdot \Pr_t[r \notin \bigcup S \oplus t_i]$
  - $\leq 2^m \cdot ((2^{-n})^m) \leq 2^{m-mn} < 1$

$\square$