Hierarchie

kuko

25.2.2021

Pokročilá teória zložitosti

$$|\mathbb{N}| \prec |2^{\mathbb{N}}|$$

	1	2	3	4	5	6	$\cdots$
S_1	**0**	0	1	0	0	0	$\cdots$
S_2	1	**0**	0	1	1	1	$\cdots$
S_3	0	0	**1**	1	0	0	$\cdots$
S_4	0	1	0	**0**	1	0	$\cdots$
S_5	0	0	0	1	**1**	1	$\cdots$
S_6	0	1	0	1	0	**1**	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
$\bar{D}$	1	1	0	1	0	0	$\cdots$

nevypočítateľný problém:

	w_1	w_2	w_3	w_4	w_5	w_6	$\cdots$
M_1	**0**	0	1	0	0	0	$\cdots$
M_2	1	**0**	0	1	1	1	$\cdots$
M_3	0	0	**1**	1	0	0	$\cdots$
M_4	0	1	0	**0**	1	0	$\cdots$
M_5	0	0	0	1	**1**	1	$\cdots$
M_6	0	1	0	1	0	**1**	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
$\bar{D}$	1	1	0	1	0	0	$\cdots$

Veta (Pamäťová hierarchia)

Nech S je páskovo konštruovateľná a $\log n \leq s(n) = o(S(n))$.
Potom $\mathrm{DSPACE}(s(n)) \subset \mathrm{DSPACE}(S(n))$.
Špeciálne $\mathrm{NL} \subset \mathrm{PSPACE} \subset \mathrm{EXPSPACE}$ *a*
$\mathrm{DSPACE}(n^{\alpha}) \subset \mathrm{DSPACE}(n^{\beta})$ *pre* $0 \leq \alpha < \beta$.

Veta (Pamäťová hierarchia)

Nech S *je páskovo konštruovateľná a* $\log n \leq s(n) = o(S(n))$.
Potom $\mathrm{DSPACE}(s(n)) \subset \mathrm{DSPACE}(S(n))$.
Špeciálne $\mathrm{NL} \subset \mathrm{PSPACE} \subset \mathrm{EXPSPACE}$ *a*
$\mathrm{DSPACE}(n^{\alpha}) \subset \mathrm{DSPACE}(n^{\beta})$ *pre* $0 \leq \alpha < \beta$.

Veta (Časová hierarchia)

Nech T je časovo konštruovateľná funkcia a $n \leq t(n) = o(T(n)/\log t(n))$. Potom $\mathrm{DTIME}(t(n)) \subset \mathrm{DTIME}(T(n))$. *Napríklad* $\mathrm{P} \subset \mathrm{EXP}$.

Veta (Pravdepodobnostná hierarchia)

Nech T je časovo konštruovateľná funkcia a $n \leq t(n) = o(T(n)/\log t(n))$. Potom $\mathrm{BPTIME}(t(n)) \subset \mathrm{BPTIME}(T(n))$. *Napríklad* $\mathrm{BPP} \subset \mathrm{BPEXP}$.

Veta (Nedeterministická pamäťová hierarchia)

Nech $\log n \leq s(n) = o(S(n))$, *kde* S *je páskovo konštruovateľná. Potom* $\mathrm{NSPACE}(s(n)) \subset \mathrm{NSPACE}(S(n))$.

Teda $\mathrm{NL} \subset \mathrm{NSPACE}(n) \subset \mathrm{PSPACE}$. *(Nedeterministický lineárny priestor sú kontextové jazyky.)*

Veta (Nedeterministická pamäťová hierarchia)

Nech $\log n \leq s(n) = o(S(n))$, *kde* S *je páskovo konštruovateľná.*
Potom $\mathrm{NSPACE}(s(n)) \subset \mathrm{NSPACE}(S(n))$.
Teda $\mathrm{NL} \subset \mathrm{NSPACE}(n) \subset \mathrm{PSPACE}$. *(Nedeterministický lineárny priestor sú kontextové jazyky.)*

Veta (Nedeterministická časová hierarchia)

Nech $t(n+1) = o(T(n))$, *kde* t, T *sú ľubovoľné časovo konštruovateľné funkcie. Potom* $\mathrm{NTIME}(t(n)) \subset \mathrm{NTIME}(T(n))$. *Teda napríklad* $\mathrm{NP} \subset \mathrm{NEXP}$.

Veta

Existuje funkcia na n bitoch, ktorá sa nedá vypočítať obvodom veľkosti $s = 2^n/n$ pre dostatočne veľké n.

Dôkaz.

- koľko je funkcií na n bitoch?
- koľko je obvodov veľkosti s?
  - zápis pom. $m = s \times (2\log(n+s)+2) < 2s\log s + O(s)$ bitov
  - $2^m < 2^{2^n}$ už pre $s = 2^n/3n$
  - v skutočnosti je obvodov $\leq 2^m/s!$
  - ušetríme $\log s! = s\log s + O(s)$ bitov
  - pre $s = 2^n/n$ je to $2^n/n(n-\log n) + O(2^n/n) = 2^n[1-\log n/n + O(1/n)] < 2^n$.

□

Veta

Existuje funkcia na n bitoch, ktorá sa nedá vypočítať obvodom veľkosti $s = 2^n/n$ pre dostatočne veľké n.

Dôkaz.

- koľko je funkcií na n bitoch?
- koľko je obvodov veľkosti s?
  - zápis pom. $m = s \times (2\log(n+s)+2) < 2s\log s + O(s)$ bitov
  - $2^m < 2^{2^n}$ už pre $s = 2^n/3n$
  - v skutočnosti je obvodov $\leq 2^m/s!$
  - ušetríme $\log s! = s\log s + O(s)$ bitov
  - pre $s = 2^n/n$ je to $2^n/n(n-\log n) + O(2^n/n) = 2^n[1-\log n/n + O(1/n)] < 2^n$.

□

Veta

Existuje funkcia na n bitoch, ktorá sa nedá vypočítať obvodom veľkosti $s = 2^n/n$ pre dostatočne veľké n.

Dôkaz.

- koľko je funkcií na n bitoch?
- koľko je obvodov veľkosti s?
  - zápis pom. $m = s \times (2\log(n+s)+2) < 2s\log s + O(s)$ bitov
  - $2^m < 2^{2^n}$ už pre $s = 2^n/3n$
  - v skutočnosti je obvodov $\leq 2^m/s!$
  - ušetríme $\log s! = s\log s + O(s)$ bitov
  - pre $s = 2^n/n$ je to $2^n/n(n-\log n) + O(2^n/n) = 2^n[1-\log n/n + O(1/n)] < 2^n$.

□

Veta

Existuje funkcia na n bitoch, ktorá sa nedá vypočítať obvodom veľkosti $s = 2^n/n$ pre dostatočne veľké n.

Dôkaz.

- koľko je funkcií na n bitoch?
- koľko je obvodov veľkosti s?
  - zápis pom. $m = s \times (2\log(n+s)+2) < 2s\log s + O(s)$ bitov
  - $2^m < 2^{2^n}$ už pre $s = 2^n/3n$
  - v skutočnosti je obvodov $\leq 2^m/s!$
  - ušetríme $\log s! = s\log s + O(s)$ bitov
  - pre $s = 2^n/n$ je to $2^n/n(n - \log n) + O(2^n/n) = 2^n[1 - \log n/n + O(1/n)] < 2^n$.

□

Veta

Existuje funkcia na n bitoch, ktorá sa nedá vypočítať obvodom veľkosti $s = 2^n/n$ pre dostatočne veľké n.

Dôkaz.

- koľko je funkcií na n bitoch?
- koľko je obvodov veľkosti s?
  - zápis pom. $m = s \times (2\log(n+s)+2) < 2s\log s + O(s)$ bitov
  - $2^m < 2^{2^n}$ už pre $s = 2^n/3n$
  - v skutočnosti je obvodov $\leq 2^m/s!$
  - ušetríme $\log s! = s\log s + O(s)$ bitov
  - pre $s = 2^n/n$ je to $2^n/n(n - \log n) + O(2^n/n) = 2^n[1 - \log n/n + O(1/n)] < 2^n$.

□

Veta

Existuje funkcia na n bitoch, ktorá sa nedá vypočítať obvodom veľkosti $s = 2^n/n$ pre dostatočne veľké n.

Dôkaz.

- koľko je funkcií na n bitoch?
- koľko je obvodov veľkosti s?
  - zápis pom. $m = s \times (2\log(n+s)+2) < 2s\log s + O(s)$ bitov
  - $2^m < 2^{2^n}$ už pre $s = 2^n/3n$
  - v skutočnosti je obvodov $\leq 2^m/s!$
  - ušetríme $\log s! = s\log s + O(s)$ bitov
  - pre $s = 2^n/n$ je to $2^n/n(n-\log n) + O(2^n/n) = 2^n[1-\log n/n + O(1/n)] < 2^n$.

□

Veta

Existuje funkcia na n bitoch, ktorá sa nedá vypočítať obvodom veľkosti $s = 2^n/n$ pre dostatočne veľké n.

Dôkaz.

- koľko je funkcií na n bitoch?
- koľko je obvodov veľkosti s?
  - zápis pom. $m = s \times (2\log(n+s)+2) < 2s\log s + O(s)$ bitov
  - $2^m < 2^{2^n}$ už pre $s = 2^n/3n$
  - v skutočnosti je obvodov $\leq 2^m/s!$
  - ušetríme $\log s! = s\log s + O(s)$ bitov
  - pre $s = 2^n/n$ je to $2^n/n(n - \log n) + O(2^n/n) = 2^n[1 - \log n/n + O(1/n)] < 2^n$.

□

Veta

Existuje funkcia na n bitoch, ktorá sa nedá vypočítať obvodom veľkosti $s = 2^n/n$ pre dostatočne veľké n.

Dôkaz.

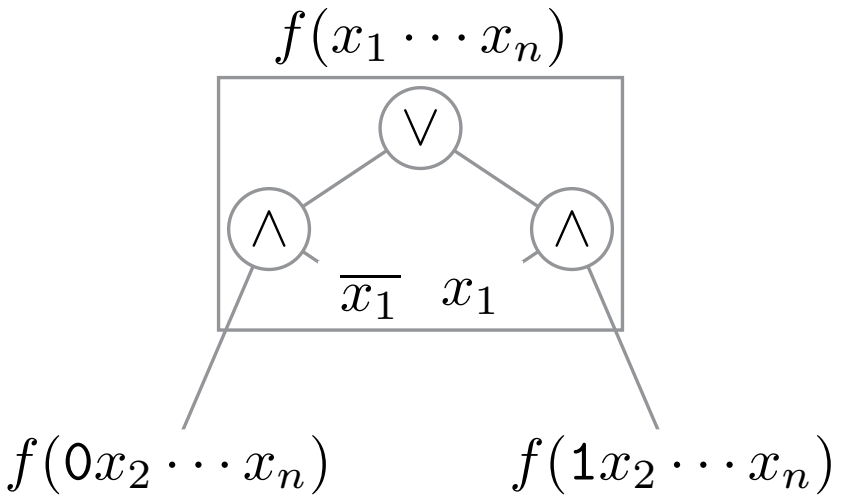
- koľko je funkcií na n bitoch?
- koľko je obvodov veľkosti s?
  - zápis pom. $m = s \times (2\log(n+s)+2) < 2s\log s + O(s)$ bitov
  - $2^m < 2^{2^n}$ už pre $s = 2^n/3n$
  - v skutočnosti je obvodov $\leq 2^m/s!$
  - ušetríme $\log s! = s\log s + O(s)$ bitov
  - pre $s = 2^n/n$ je to $2^n/n(n-\log n) + O(2^n/n) = 2^n[1-\log n/n + O(1/n)] < 2^n$.

□

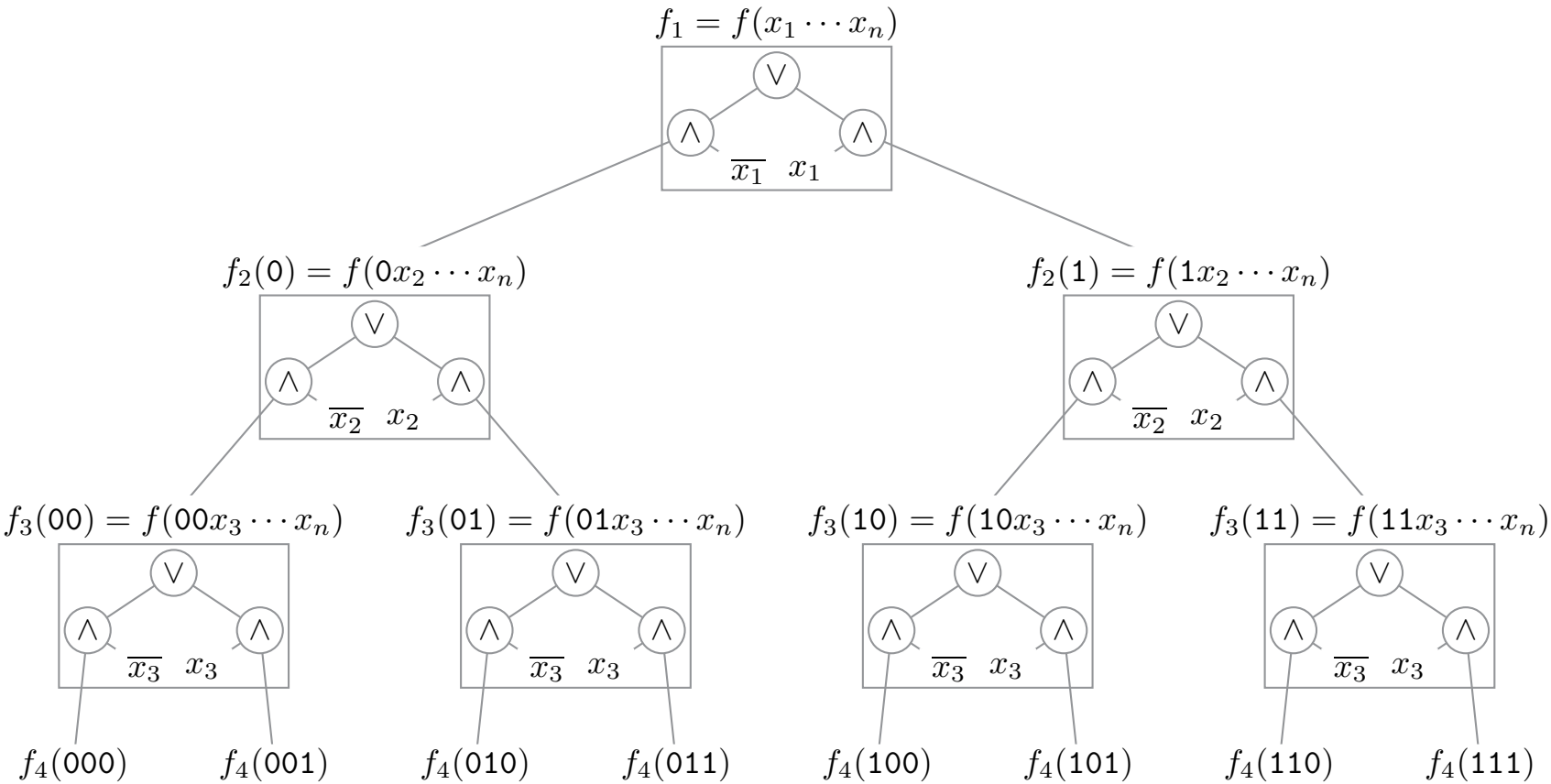
Veta

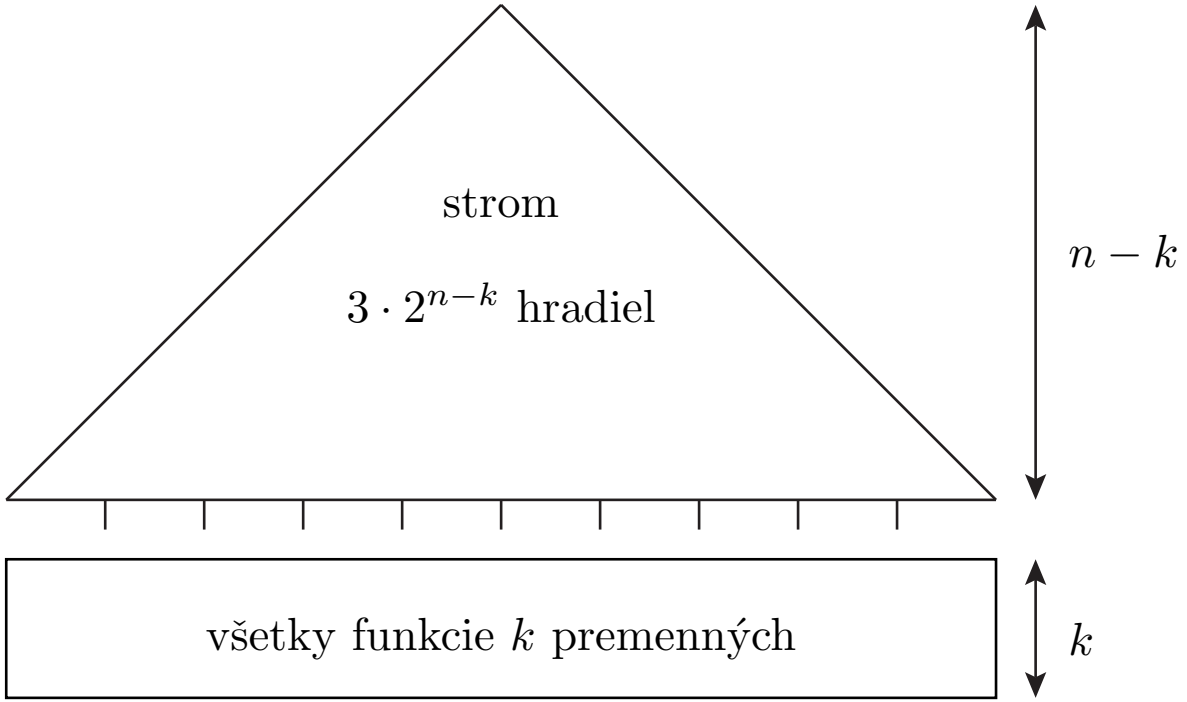
Každá funkcia na n bitoch sa dá vypočítať obvodom veľkosti $O(2^n/n)$, presnejšie $5 \cdot 2^n/n$.

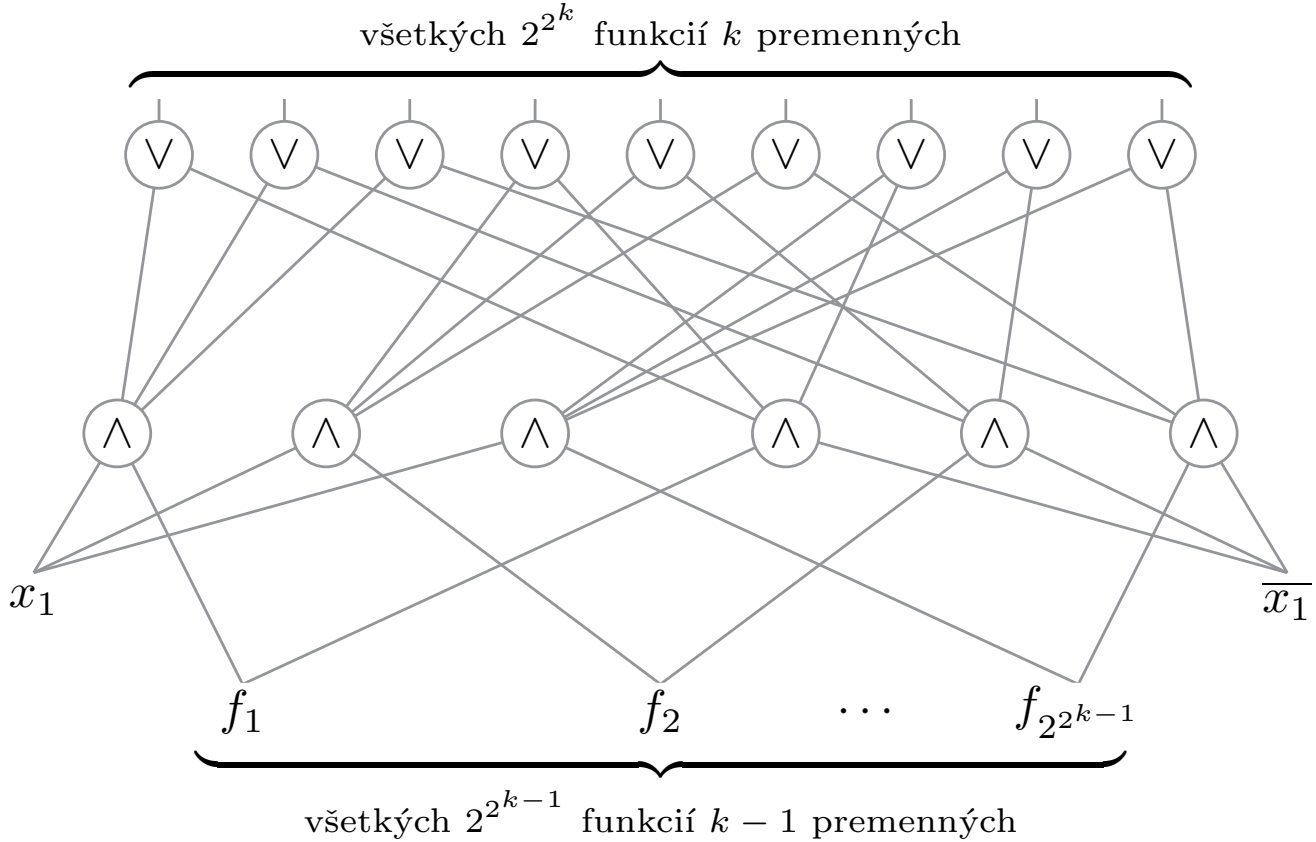
(včera sme ukázali, že existuje obvod veľkosti $O(n2^n)$)



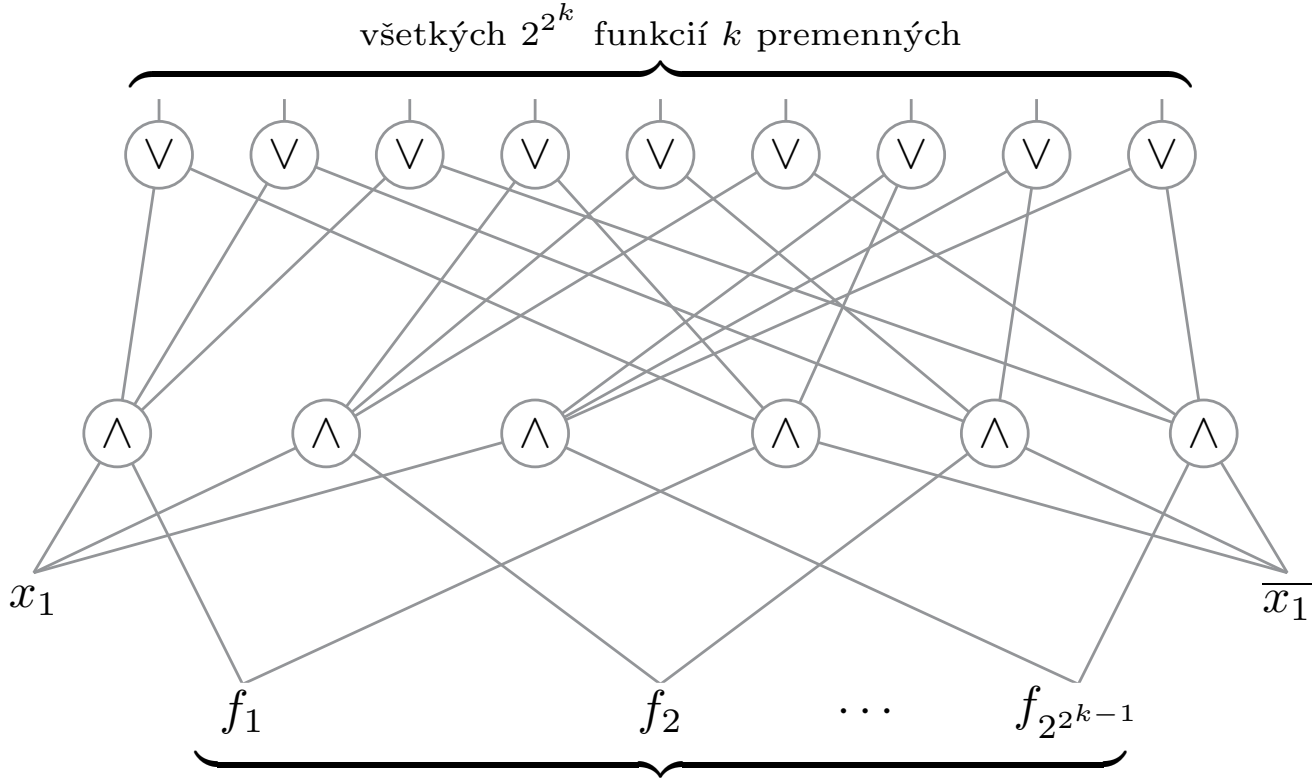
$$f(x_1, \ldots, x_n) = [x_1 \wedge f(1, x_2, \ldots, x_n)] \vee [\overline{x_1} \wedge f(0, x_2, \ldots, x_n)]$$


$f_1 = f(x_1 \cdots x_n)$
$\overline{x_1}$ x_1
$f_2(0) = f(0x_2 \cdots x_n)$
$\overline{x_2}$ x_2
$f_2(1) = f(1x_2 \cdots x_n)$
$\overline{x_2}$ x_2
$f_3(00) = f(00x_3 \cdots x_n)$
$\overline{x_3}$ x_3
$f_3(01) = f(01x_3 \cdots x_n)$
$\overline{x_3}$ x_3
$f_3(10) = f(10x_3 \cdots x_n)$
$\overline{x_3}$ x_3
$f_3(11) = f(11x_3 \cdots x_n)$
$\overline{x_3}$ x_3
$f_4(000)$
$f_4(001)$
$f_4(010)$
$f_4(011)$
$f_4(100)$
$f_4(101)$
$f_4(110)$
$f_4(111)$


strom
$3 \cdot 2^{n-k}$ hradiel
$n - k$
všetky funkcie k premenných
k



$$
\begin{aligned}
A_k &\leq \left(2^{2^{k-1}}\right)^2 + 2 \cdot 2^{2^{k-1}} + A_{k-1} \\
&= 2^{2^k} + \underbrace{3 \cdot 2^{2^{k-1}} + 3 \cdot 2^{2^{k-2}} + 3 \cdot 2^{2^{k-3}} + \cdots + A_1} \\
&< 2^{2^k} + 3k \cdot 2^{2^{k-1}} \\
&= 2^{2^k}\left(1 + 3k/2^{2^{k-1}}\right)
\end{aligned}
$$



$$
\begin{aligned}
A_k &\leq \left(2^{2^{k-1}}\right)^2 + 2 \cdot 2^{2^{k-1}} + A_{k-1} \\
&= 2^{2^k} + \underbrace{3 \cdot 2^{2^{k-1}} + 3 \cdot 2^{2^{k-2}} + 3 \cdot 2^{2^{k-3}} + \cdots + A_1} \\
&< 2^{2^k} + 3k \cdot 2^{2^{k-1}} \\
&= 2^{2^k}(1 + 3k/2^{2^{k-1}})
\end{aligned}
$$

- celkovo: $3 \cdot 2^{n-k} + A_k + n$ hradiel
- pre $k = \log(n - \log n)$ dostaneme

$$S_n = 3 \cdot \frac{2^n}{n - \log n} + \frac{2^n}{n}(1 + o(1)) = (4 + o(1))\frac{2^n}{n}$$

- celkovo: $3 \cdot 2^{n-k} + A_k + n$ hradiel
- pre $k = \log(n - \log n)$ dostaneme

$$S_n = 3 \cdot \frac{2^n}{n - \log n} + \frac{2^n}{n}(1 + o(1)) = (4 + o(1))\frac{2^n}{n}$$

$L(n) =$ veľkosť obvodu pre *najťažšiu* funkciu na n bitoch

$$L(n) \geq \frac{2^n}{n}\left(1 + \frac{\log n - O(1)}{n}\right)$$
$$\leq \frac{2^n}{n}\left(1 + \frac{\log n + \log\log n + O(1)}{n}\right)$$

$L(n, \varepsilon) =$ najmenšie s také, že každá fn. na n bitoch sa dá spočítať obvodom veľkosti s na aspoň $(1/2 + \varepsilon)$-tine vstupov

$$L(n, \varepsilon) = \Theta\left(\frac{2^n \varepsilon^2}{\log(2 + 2^n \varepsilon^2)}\right) + \Theta(n).$$

$L(n) =$ veľkosť obvodu pre *najťažšiu* funkciu na n bitoch

$$L(n) \geq \frac{2^n}{n}\left(1 + \frac{\log n - O(1)}{n}\right)$$
$$\leq \frac{2^n}{n}\left(1 + \frac{\log n + \log\log n + O(1)}{n}\right)$$

$L(n, \varepsilon) =$ najmenšie s také, že každá fn. na n bitoch sa dá spočítať obvodom veľkosti s na aspoň $(1/2 + \varepsilon)$-tine vstupov

$$L(n, \varepsilon) = \Theta\left(\frac{2^n \varepsilon^2}{\log(2 + 2^n \varepsilon^2)}\right) + \Theta(n).$$

Veta (Neuniformná hierarchia)

Pre každé $s : \mathbb{N} \to \mathbb{N}$, $s(n) < 2^n/n$ *je* $\mathsf{SIZE}(s(n)) \subset \mathsf{SIZE}(5s(n))$.

Dôkaz.

- $\forall \ell \exists f : \{0,1\}^\ell \to \{0,1\}$, kt. sa *nedá* vypočítať obvodom veľkosti $2^\ell/\ell$,
- každá fn. sa dá vypočítať obvodom veľkosti $5 \cdot 2^\ell/\ell$
- $g : \{0,1\}^n \to \{0,1\}$ aplikuje f na prvých ℓ vstupov
- $2^\ell/\ell = s(n)$
- potom $g \in \mathsf{SIZE}(5s(n)) - \mathsf{SIZE}(s(n))$.

□

Veta (Neuniformná hierarchia)

Pre každé $s : \mathbb{N} \to \mathbb{N}$, $s(n) < 2^n/n$ *je* $\mathsf{SIZE}(s(n)) \subset \mathsf{SIZE}(5s(n))$.

Dôkaz.

- $\forall \ell \exists f : \{0,1\}^\ell \to \{0,1\}$, kt. sa *nedá* vypočítať obvodom veľkosti $2^\ell/\ell$,
- každá fn. sa dá vypočítať obvodom veľkosti $5 \cdot 2^\ell/\ell$
- $g : \{0,1\}^n \to \{0,1\}$ aplikuje f na prvých ℓ vstupov
- $2^\ell/\ell = s(n)$
- potom $g \in \mathsf{SIZE}(5s(n)) - \mathsf{SIZE}(s(n))$.

□

Veta (Neuniformná hierarchia)

Pre každé $s : \mathbb{N} \to \mathbb{N}$, $s(n) < 2^n/n$ *je* $\mathsf{SIZE}(s(n)) \subset \mathsf{SIZE}(5s(n))$.

Dôkaz.

- $\forall \ell \exists f : \{0,1\}^\ell \to \{0,1\}$, kt. sa *nedá* vypočítať obvodom veľkosti $2^\ell/\ell$,
- každá fn. sa dá vypočítať obvodom veľkosti $5 \cdot 2^\ell/\ell$
- $g : \{0,1\}^n \to \{0,1\}$ aplikuje f na prvých ℓ vstupov
- $2^\ell/\ell = s(n)$
- potom $g \in \mathsf{SIZE}(5s(n)) - \mathsf{SIZE}(s(n))$.

□

Veta (Neuniformná hierarchia)

Pre každé $s : \mathbb{N} \to \mathbb{N}$, $s(n) < 2^n/n$ *je* $\mathsf{SIZE}(s(n)) \subset \mathsf{SIZE}(5s(n))$.

Dôkaz.

- $\forall \ell \exists f : \{0,1\}^\ell \to \{0,1\}$, kt. sa *nedá* vypočítať obvodom veľkosti $2^\ell/\ell$,
- každá fn. sa dá vypočítať obvodom veľkosti $5 \cdot 2^\ell/\ell$
- $g : \{0,1\}^n \to \{0,1\}$ aplikuje f na prvých ℓ vstupov
- $2^\ell/\ell = s(n)$
- potom $g \in \mathsf{SIZE}(5s(n)) - \mathsf{SIZE}(s(n))$.

□

Veta (Neuniformná hierarchia)

Pre každé $s : \mathbb{N} \to \mathbb{N}$, $s(n) < 2^n/n$ *je* $\mathsf{SIZE}(s(n)) \subset \mathsf{SIZE}(5s(n))$.

Dôkaz.

- $\forall \ell \exists f : \{0,1\}^\ell \to \{0,1\}$, kt. sa *nedá* vypočítať obvodom veľkosti $2^\ell/\ell$,
- každá fn. sa dá vypočítať obvodom veľkosti $5 \cdot 2^\ell/\ell$
- $g : \{0,1\}^n \to \{0,1\}$ aplikuje f na prvých ℓ vstupov
- $2^\ell/\ell = s(n)$
- potom $g \in \mathsf{SIZE}(5s(n)) - \mathsf{SIZE}(s(n))$.

□

Veta (Neuniformná hierarchia)

Pre každé $s : \mathbb{N} \to \mathbb{N}$, $s(n) < 2^n/n$ *je* $\mathsf{SIZE}(s(n)) \subset \mathsf{SIZE}(5s(n))$.

Dôkaz.

- $\forall \ell \exists f : \{0,1\}^\ell \to \{0,1\}$, kt. sa *nedá* vypočítať obvodom veľkosti $2^\ell/\ell$,
- každá fn. sa dá vypočítať obvodom veľkosti $5 \cdot 2^\ell/\ell$
- $g : \{0,1\}^n \to \{0,1\}$ aplikuje f na prvých ℓ vstupov
- $2^\ell/\ell = s(n)$
- potom $g \in \mathsf{SIZE}(5s(n)) - \mathsf{SIZE}(s(n))$.

□

Veta

$\mathrm{BPP} \subset \mathrm{BPEXP}$.

Dôkaz.

- $\mathrm{BPP} \subseteq \mathrm{EXP} \subset \mathrm{EEXP} \subseteq \mathrm{BPEEXP}$
- $\Longrightarrow$ triviálne $\mathrm{BPP} \subset \mathrm{BPEEXP}$
- keby $\mathrm{BPP} = \mathrm{BPEXP} \Rightarrow \mathrm{BPEXP} = \mathrm{BPEEXP}$ (padding, spor)
- (ak $L \in \mathrm{BPTIME}(2^{2^{n^k}})$, vytvorme $L' = \{x\#0^{2^{|x|^k}} \mid x \in L\}$,
- $L' \in \mathrm{BPTIME}(2^n)$
- z predpokladu potom $L' \in \mathrm{BPP}$, takže $L \in \mathrm{BPEXP}$)

□

Veta

$\mathrm{BPP} \subset \mathrm{BPEXP}$.

■ **Dôkaz.**

- $\mathrm{BPP} \subseteq \mathrm{EXP} \subset \mathrm{EEXP} \subseteq \mathrm{BPEEXP}$
- $\Longrightarrow$ triviálne $\mathrm{BPP} \subset \mathrm{BPEEXP}$
- keby $\mathrm{BPP} = \mathrm{BPEXP} \Rightarrow \mathrm{BPEXP} = \mathrm{BPEEXP}$ (padding, spor)
- (ak $L \in \mathrm{BPTIME}(2^{2^{n^k}})$, vytvorme $L' = \{x\#0^{2^{|x|^k}} \mid x \in L\}$,
- $L' \in \mathrm{BPTIME}(2^n)$
- z predpokladu potom $L' \in \mathrm{BPP}$, takže $L \in \mathrm{BPEXP}$)

□

Veta

BPP $\subset$ BPEXP.

■ **Dôkaz.**

- BPP $\subseteq$ EXP $\subset$ EEXP $\subseteq$ BPEEXP
- $\Longrightarrow$ triviálne BPP $\subset$ BPEEXP
- keby BPP $=$ BPEXP $\Rightarrow$ BPEXP $=$ BPEEXP (padding, spor)
- (ak $L \in \mathrm{BPTIME}(2^{2^{n^k}})$, vytvorme $L' = \{x\#0^{2^{|x|^k}} \mid x \in L\}$,
- $L' \in \mathrm{BPTIME}(2^n)$
- z predpokladu potom $L' \in$ BPP, takže $L \in$ BPEXP)

□

Veta

$\mathrm{BPP} \subset \mathrm{BPEXP}$.

■ **Dôkaz.**

- $\mathrm{BPP} \subseteq \mathrm{EXP} \subset \mathrm{EEXP} \subseteq \mathrm{BPEEXP}$
- $\Longrightarrow$ triviálne $\mathrm{BPP} \subset \mathrm{BPEEXP}$
- keby $\mathrm{BPP} = \mathrm{BPEXP} \Rightarrow \mathrm{BPEXP} = \mathrm{BPEEXP}$ (padding, spor)
- (ak $L \in \mathrm{BPTIME}(2^{2^{n^k}})$, vytvorme $L' = \{x\#0^{2^{|x|^k}} \mid x \in L\}$,
- $L' \in \mathrm{BPTIME}(2^n)$
- z predpokladu potom $L' \in \mathrm{BPP}$, takže $L \in \mathrm{BPEXP}$)

□

Veta

$\mathrm{BPP} \subset \mathrm{BPEXP}$.

Dôkaz.

- $\mathrm{BPP} \subseteq \mathrm{EXP} \subset \mathrm{EEXP} \subseteq \mathrm{BPEEXP}$
- $\Longrightarrow$ triviálne $\mathrm{BPP} \subset \mathrm{BPEEXP}$
- keby $\mathrm{BPP} = \mathrm{BPEXP} \Rightarrow \mathrm{BPEXP} = \mathrm{BPEEXP}$ (padding, spor)
- (ak $L \in \mathrm{BPTIME}(2^{2^{n^k}})$, vytvorme $L' = \{x\#0^{2^{|x|^k}} \mid x \in L\}$,
- $L' \in \mathrm{BPTIME}(2^n)$
- z predpokladu potom $L' \in \mathrm{BPP}$, takže $L \in \mathrm{BPEXP}$)

□

Veta

$\mathrm{BPP} \subset \mathrm{BPEXP}$.

■ **Dôkaz.**

- $\mathrm{BPP} \subseteq \mathrm{EXP} \subset \mathrm{EEXP} \subseteq \mathrm{BPEEXP}$
- $\Longrightarrow$ triviálne $\mathrm{BPP} \subset \mathrm{BPEEXP}$
- keby $\mathrm{BPP} = \mathrm{BPEXP} \Rightarrow \mathrm{BPEXP} = \mathrm{BPEEXP}$ (padding, spor)
- (ak $L \in \mathrm{BPTIME}(2^{2^{n^k}})$, vytvorme $L' = \{x\#0^{2^{|x|^k}} \mid x \in L\}$,
- $L' \in \mathrm{BPTIME}(2^n)$
- z predpokladu potom $L' \in \mathrm{BPP}$, takže $L \in \mathrm{BPEXP}$)

□

Veta

$\mathrm{BPP} \subset \mathrm{BPEXP}$.

■ **Dôkaz.**

- $\mathrm{BPP} \subseteq \mathrm{EXP} \subset \mathrm{EEXP} \subseteq \mathrm{BPEEXP}$
- $\Longrightarrow$ triviálne $\mathrm{BPP} \subset \mathrm{BPEEXP}$
- keby $\mathrm{BPP} = \mathrm{BPEXP} \Rightarrow \mathrm{BPEXP} = \mathrm{BPEEXP}$ (padding, spor)
- (ak $L \in \mathrm{BPTIME}(2^{2^{n^k}})$, vytvorme $L' = \{x\#0^{2^{|x|^k}} \mid x \in L\}$,
- $L' \in \mathrm{BPTIME}(2^n)$
- z predpokladu potom $L' \in \mathrm{BPP}$, takže $L \in \mathrm{BPEXP}$)

□