Zložitosť počítania

kuko

12.5.2021

Pokročilá teória zložitosti

Počítacie úlohy

- koľko sledov dĺžky k vedie medzi s a t?
- koľko ciest vedie medzi s a t?
- v koľkých podgrafoch je cesta medzi s a t?
- koľko kostier má daný graf?
- koľko párovaní má daný graf?
- koľko 2-farbení má daný graf?
- koľko riešení má daný 2-SAT?

Počítacie úlohy

- koľko sledov dĺžky k vedie medzi s a t?
- koľko ciest vedie medzi s a t?
- v koľkých podgrafoch je cesta medzi s a t?
- koľko kostier má daný graf?
- koľko párovaní má daný graf?
- koľko 2-farbení má daný graf?
- koľko riešení má daný 2-SAT?

Počítacie úlohy

- koľko sledov dĺžky k vedie medzi s a t?
- koľko ciest vedie medzi s a t?
- v koľkých podgrafoch je cesta medzi s a t?
- koľko kostier má daný graf?
- koľko párovaní má daný graf?
- koľko 2-farbení má daný graf?
- koľko riešení má daný 2-SAT?

Počítacie úlohy

- koľko sledov dĺžky k vedie medzi s a t?
- koľko ciest vedie medzi s a t?
- v koľkých podgrafoch je cesta medzi s a t?
- koľko kostier má daný graf?
- koľko párovaní má daný graf?
- koľko 2-farbení má daný graf?
- koľko riešení má daný 2-SAT?

Počítacie úlohy

- koľko sledov dĺžky k vedie medzi s a t?
- koľko ciest vedie medzi s a t?
- v koľkých podgrafoch je cesta medzi s a t?
- koľko kostier má daný graf?
- koľko párovaní má daný graf?
- koľko 2-farbení má daný graf?
- koľko riešení má daný 2-SAT?

Počítacie úlohy

- koľko sledov dĺžky k vedie medzi s a t?
- koľko ciest vedie medzi s a t?
- v koľkých podgrafoch je cesta medzi s a t?
- koľko kostier má daný graf?
- koľko párovaní má daný graf?
- koľko 2-farbení má daný graf?
- koľko riešení má daný 2-SAT?

Počítacie úlohy

- koľko sledov dĺžky k vedie medzi s a t?
- koľko ciest vedie medzi s a t?
- v koľkých podgrafoch je cesta medzi s a t?
- koľko kostier má daný graf?
- koľko párovaní má daný graf?
- koľko 2-farbení má daný graf?
- koľko riešení má daný 2-SAT?

Počítacie úlohy

- koľko sledov dĺžky k vedie medzi s a t?
- koľko ciest vedie medzi s a t?
- v koľkých podgrafoch je cesta medzi s a t?
- koľko kostier má daný graf?
- koľko párovaní má daný graf?
- koľko 2-farbení má daný graf?
- koľko riešení má daný 2-SAT?

FP, #P

- definujme „počítacie“ triedy funkcií $f : \{0,1\}^* \to \mathbb{N}$ analogické P, NP:

Definícia (FP)

$f \in \mathrm{FP}$, ak f vieme vypočítať v polynomiálnom čase.

Definícia (#P)

$f \in \#\mathrm{P}$, ak f je počet akceptačných výpočtov nejakého polynomálneho NTS.
$\exists$poly TS D, polynóm p: $f(x) = \#\{y \in \{0,1\}^{p(x)} \mid D(x,y) = 1\}$

FP, #P

- definujme „počítacie“ triedy funkcií $f : \{0,1\}^* \to \mathbb{N}$ analogické P, NP:

Definícia (FP)

$f \in \mathrm{FP}$, *ak f vieme vypočítať v polynomiálnom čase.*

Definícia (#P)

$f \in \#\mathrm{P}$, *ak f je počet akceptačných výpočtov nejakého polynomálneho NTS.*
$\exists$*poly TS D, polynóm p:* $f(x) = \#\{y \in \{0,1\}^{p(x)} \mid D(x,y) = 1\}$

FP, #P

- definujme „počítacie“ triedy funkcií $f : \{0,1\}^* \to \mathbb{N}$ analogické P, NP:

Definícia (FP)

$f \in \mathrm{FP}$, ak f vieme vypočítať v polynomiálnom čase.

Definícia (#P)

$f \in \#\mathrm{P}$, ak f je počet akceptačných výpočtov nejakého polynomálneho NTS.
$\exists$poly TS D, polynóm p: $f(x) = \#\{y \in \{0,1\}^{p(x)} \mid D(x,y) = 1\}$

FP, #P vs. P, NP

- $\mathrm{FP} \neq \#\mathrm{P}$??
- $\mathrm{FP} = \#\mathrm{P} \implies \mathrm{P} = \mathrm{NP}$
- $\mathrm{FP} = \#\mathrm{P} \impliedby \mathrm{P} = \mathrm{NP}$?? (nevie sa)

FP, #P vs. P, NP

- $\mathrm{FP} \neq \#\mathrm{P}$??
- $\mathrm{FP} = \#\mathrm{P} \implies \mathrm{P} = \mathrm{NP}$
- $\mathrm{FP} = \#\mathrm{P} \impliedby \mathrm{P} = \mathrm{NP}$?? (nevie sa)

FP, #P vs. P, NP

- $\mathrm{FP} \neq \#\mathrm{P}$??
- $\mathrm{FP} = \#\mathrm{P} \Longrightarrow \mathrm{P} = \mathrm{NP}$
- $\mathrm{FP} = \#\mathrm{P} \Longleftarrow \mathrm{P} = \mathrm{NP}$?? (nevie sa)

#P-úplnosť

Definícia (#P-úplnosť)

Funkcia f je #P-úplna, ak je v #P *a* $\#\mathrm{P} \subseteq \mathrm{FP}^f$.

#P-úplne problémy

- koľko sledov dĺžky k vedie medzi s a t?
- koľko kostier má daný graf?
- koľko 2-farbení má daný graf?

$\in$ FP

- koľko ciest vedie medzi s a t?
- v koľkých podgrafoch je cesta medzi s a t?
- koľko párovaní má daný graf?
- koľko riešení má daný 2-SAT?

sú #P-úplné

#P-úplne problémy

- koľko sledov dĺžky k vedie medzi s a t?
- koľko kostier má daný graf?
- koľko 2-farbení má daný graf?

$\in$ FP

- koľko ciest vedie medzi s a t?
- v koľkých podgrafoch je cesta medzi s a t?
- koľko párovaní má daný graf?
- koľko riešení má daný 2-SAT?

sú #P-úplné

#P-úplne problémy

- #Sat je #P-úplný.
- väčšina NP-úplných problémov má #P-úplnú počítaciu verziu
- Funkcia perm na maticiach nad $\mathbb{Z}_2$ je #P-úplná.

Definícia (permanent)

Permanent $n \times n$ matice A definujeme ako

$$\mathrm{perm}(A) = \sum_{\sigma \in S_n} \prod_i A_{i,\sigma(i)}.$$

#P-úplne problémy

- $\#\textsc{Sat}$ je #P-úplný.
- väčšina NP-úplných problémov má #P-úplnú počítaciu verziu
- Funkcia perm na maticiach nad $\mathbb{Z}_2$ je #P-úplná.

Definícia (permanent)

Permanent $n \times n$ matice A definujeme ako

$$\mathrm{perm}(A) = \sum_{\sigma \in S_n} \prod_i A_{i,\sigma(i)}.$$

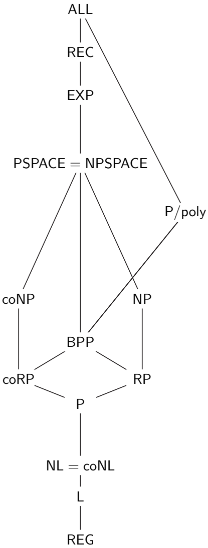
#P-úplne problémy

- #SAT je #P-úplný.
- väčšina NP-úplných problémov má #P-úplnú počítaciu verziu
- Funkcia perm na maticiach nad $\mathbb{Z}_2$ je #P-úplná.

Definícia (permanent)

Permanent $n \times n$ matice A definujeme ako

$$\mathrm{perm}(A) = \sum_{\sigma \in S_n} \prod_i A_{i,\sigma(i)}.$$



- Aký je vzťah PH a #P?

Todova veta

Veta (Toda)

Všetky problémy v PH *vieme vyriešiť pomocou jedinej otázky na* $\#\textsc{Sat}$.

$\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}}$.

Unique SAT

Unique SAT

- SAT môže mať $0 \ldots 2^n$ riešení
- USAT je SAT, pričom máme sľúbené, že ϕ má 0 alebo 1 riešenie
- je USAT „ľahký“?
- je USAT NP-úplný? aspoň pri Turingovskej redukcií?

Unique SAT

- SAT môže mať $0 \dots 2^n$ riešení
- USAT je SAT, pričom máme sľúbené, že ϕ má 0 alebo 1 riešenie
- je USAT „ľahký“?
- je USAT NP-úplný? aspoň pri Turingovskej redukcií?

Unique SAT

- SAT môže mať $0 \dots 2^n$ riešení
- USAT je SAT, pričom máme sľúbené, že ϕ má 0 alebo 1 riešenie
- je USAT „ľahký“?
- je USAT NP-úplný? aspoň pri Turingovskej redukcií?

Unique SAT

- SAT môže mať $0 \dots 2^n$ riešení
- USAT je SAT, pričom máme sľúbené, že ϕ má 0 alebo 1 riešenie
- je USAT „ľahký“?
- je USAT NP-úplný? aspoň pri Turingovskej redukcií?

Unique SAT

Veta (Valiant, Vazirani)

$\mathsf{NP} \subseteq \mathsf{RP}^{\mathrm{USAT}}$

$\mathrm{USAT} \in \mathsf{P} \implies \mathsf{NP} = \mathsf{RP}$

$\mathrm{SAT} \leq_r^P \mathrm{USAT}$

$\exists$ *PPT algoritmus f taký, že*

- $\phi \in \mathrm{SAT} \implies \Pr[f(\phi) \in \mathrm{USAT}] \geq 1/8n$
- $\phi \notin \mathrm{SAT} \implies f(\phi) \notin \mathrm{SAT}$

Veta (Valiant, Vazirani)

$\mathsf{NP} \subseteq \mathsf{RP}^{\mathrm{USAT}}$

$\mathrm{USAT} \in \mathsf{P} \implies \mathsf{NP} = \mathsf{RP}$

$\mathrm{SAT} \leq_r^P \mathrm{USAT}$

$\exists$ *PPT algoritmus f taký, že*

- $\phi \in \mathrm{SAT} \implies \Pr[f(\phi) \in \mathrm{USAT}] \geq 1/8n$
- $\phi \notin \mathrm{SAT} \implies f(\phi) \notin \mathrm{SAT}$

Unique SAT

Veta (Valiant, Vazirani)

$\mathsf{NP} \subseteq \mathsf{RP}^{\mathrm{USAT}}$

$\mathrm{USAT} \in \mathsf{P} \implies \mathsf{NP} = \mathsf{RP}$

$\mathrm{SAT} \leq_r^P \mathrm{USAT}$

$\exists$ *PPT algoritmus f taký, že*

- $\phi \in \mathrm{SAT} \implies \Pr[f(\phi) \in \mathrm{USAT}] \geq 1/8n$
- $\phi \notin \mathrm{SAT} \implies f(\phi) \notin \mathrm{SAT}$

Unique SAT

Veta (Valiant, Vazirani)

$\mathrm{NP} \subseteq \mathrm{RP}^{\mathrm{USAT}}$
$\mathrm{USAT} \in \mathrm{P} \implies \mathrm{NP} = \mathrm{RP}$
$\mathrm{SAT} \leq_r^P \mathrm{USAT}$
$\exists$ *PPT algoritmus f taký, že*

- $\phi \in \mathrm{SAT} \implies \Pr[f(\phi) \in \mathrm{USAT}] \geq 1/8n$
- $\phi \notin \mathrm{SAT} \implies f(\phi) \notin \mathrm{SAT}$

Lema

Lema (Izolačná lema, Valiant, Vazirani)

- $\mathscr{H}_{n,k}$ – *trieda po dvoch nezávislých hašovacích funkcií* $\{0,1\}^n \to \{0,1\}^k$
- $S \subseteq \{0,1\}^n$, $\frac{1}{4} \cdot 2^k \leq |S| \leq \frac{1}{2} \cdot 2^k$
- $\Pr_{h \in_R \mathscr{H}_{n,k}}[\exists! x \in S : h(x) = 0^k] \geq 1/8.$

■ **Dôkaz.**

- nech $p = \Pr_{h \in_R \mathscr{H}_{n,k}}[h(x) = 0^k] = 2^{-k}$
- nech $N =$ počet $x \in S : h(x) = 0^k$
- $E[N] = |S|p \in [\frac{1}{4}, \frac{1}{2}]$
- $\Pr[N = 0] \leq 1 - |S|p + \binom{|S|}{2} p^2$ (princíp inklúzie, exklúzie)
- $\Pr[N \geq 2] \leq \binom{|S|}{2} p^2$ (union bound)
- $\Longrightarrow \Pr[N = 1] \geq |S|p(1 - |S|p) \geq 1/8$

Lema

Lema (Izolačná lema, Valiant, Vazirani)

- $\mathscr{H}_{n,k}$ – *trieda po dvoch nezávislých hašovacích funkcií* $\{0,1\}^n \to \{0,1\}^k$
- $S \subseteq \{0,1\}^n$, $\frac{1}{4} \cdot 2^k \leq |S| \leq \frac{1}{2} \cdot 2^k$
- $\Pr_{h \in_R \mathscr{H}_{n,k}}[\exists! x \in S : h(x) = 0^k] \geq 1/8$.

■ **Dôkaz.**

- nech $p = \Pr_{h \in_R \mathscr{H}_{n,k}}[h(x) = 0^k] = 2^{-k}$
- nech $N =$ počet $x \in S : h(x) = 0^k$
- $E[N] = |S|p \in [\frac{1}{4}, \frac{1}{2}]$
- $\Pr[N = 0] \leq 1 - |S|p + \binom{|S|}{2} p^2$ (princíp inklúzie, exklúzie)
- $\Pr[N \geq 2] \leq \binom{|S|}{2} p^2$ (union bound)
- $\implies \Pr[N = 1] \geq |S|p(1 - |S|p) \geq 1/8$

Lema

Lema (Izolačná lema, Valiant, Vazirani)

- $\mathscr{H}_{n,k}$ – *trieda po dvoch nezávislých hašovacích funkcií* $\{0,1\}^n \to \{0,1\}^k$
- $S \subseteq \{0,1\}^n$, $\frac{1}{4} \cdot 2^k \leq |S| \leq \frac{1}{2} \cdot 2^k$
- $\Pr_{h \in_R \mathscr{H}_{n,k}}[\exists! x \in S : h(x) = 0^k] \geq 1/8$.

■ Dôkaz.

- nech $p = \Pr_{h \in_R \mathscr{H}_{n,k}}[h(x) = 0^k] = 2^{-k}$
- nech $N =$ počet $x \in S : h(x) = 0^k$
- $E[N] = |S|p \in [\frac{1}{4}, \frac{1}{2}]$
- $\Pr[N = 0] \leq 1 - |S|p + \binom{|S|}{2} p^2$ (princíp inklúzie, exklúzie)
- $\Pr[N \geq 2] \leq \binom{|S|}{2} p^2$ (union bound)
- $\Longrightarrow \Pr[N = 1] \geq |S|p(1 - |S|p) \geq 1/8$

Lema

Lema (Izolačná lema, Valiant, Vazirani)

- $\mathscr{H}_{n,k}$ – *trieda po dvoch nezávislých hašovacích funkcií* $\{0,1\}^n \to \{0,1\}^k$
- $S \subseteq \{0,1\}^n$, $\frac{1}{4} \cdot 2^k \leq |S| \leq \frac{1}{2} \cdot 2^k$
- $\Pr_{h \in_R \mathscr{H}_{n,k}}[\exists! x \in S : h(x) = 0^k] \geq 1/8$.

Dôkaz.

- nech $p = \Pr_{h \in_R \mathscr{H}_{n,k}}[h(x) = 0^k] = 2^{-k}$
- nech $N =$ počet $x \in S : h(x) = 0^k$
- $E[N] = |S|p \in [\frac{1}{4}, \frac{1}{2}]$
- $\Pr[N = 0] \leq 1 - |S|p + \binom{|S|}{2} p^2$ (princíp inklúzie, exklúzie)
- $\Pr[N \geq 2] \leq \binom{|S|}{2} p^2$ (union bound)
- $\implies \Pr[N = 1] \geq |S|p(1 - |S|p) \geq 1/8$

Lema (Izolačná lema, Valiant, Vazirani)

- $\mathscr{H}_{n,k}$ – *trieda po dvoch nezávislých hašovacích funkcií* $\{0,1\}^n \to \{0,1\}^k$
- $S \subseteq \{0,1\}^n$, $\frac{1}{4} \cdot 2^k \leq |S| \leq \frac{1}{2} \cdot 2^k$
- $\Pr_{h \in_R \mathscr{H}_{n,k}}[\exists! x \in S : h(x) = 0^k] \geq 1/8$.

Dôkaz.

- nech $p = \Pr_{h \in_R \mathscr{H}_{n,k}}[h(x) = 0^k] = 2^{-k}$
- nech $N =$ počet $x \in S : h(x) = 0^k$
- $E[N] = |S|p \in [\frac{1}{4}, \frac{1}{2}]$
- $\Pr[N = 0] \leq 1 - |S|p + \binom{|S|}{2} p^2$ (princíp inklúzie, exklúzie)
- $\Pr[N \geq 2] \leq \binom{|S|}{2} p^2$ (union bound)
- $\implies \Pr[N = 1] \geq |S|p(1 - |S|p) \geq 1/8$

Lema (Izolačná lema, Valiant, Vazirani)

- $\mathscr{H}_{n,k}$ – *trieda po dvoch nezávislých hašovacích funkcií* $\{0,1\}^n \to \{0,1\}^k$
- $S \subseteq \{0,1\}^n$, $\frac{1}{4} \cdot 2^k \leq |S| \leq \frac{1}{2} \cdot 2^k$
- $\Pr_{h \in_R \mathscr{H}_{n,k}}[\exists! x \in S : h(x) = 0^k] \geq 1/8$.

■ **Dôkaz.**

- nech $p = \Pr_{h \in_R \mathscr{H}_{n,k}}[h(x) = 0^k] = 2^{-k}$
- nech $N =$ počet $x \in S : h(x) = 0^k$
- $E[N] = |S|p \in [\frac{1}{4}, \frac{1}{2}]$
- $\Pr[N = 0] \leq 1 - |S|p + \binom{|S|}{2} p^2$ (princíp inklúzie, exklúzie)
- $\Pr[N \geq 2] \leq \binom{|S|}{2} p^2$ (union bound)
- $\implies \Pr[N = 1] \geq |S|p(1 - |S|p) \geq 1/8$

Lema

Lema (Izolačná lema, Valiant, Vazirani)

- $\mathscr{H}_{n,k}$ – *trieda po dvoch nezávislých hašovacích funkcií* $\{0,1\}^n \to \{0,1\}^k$
- $S \subseteq \{0,1\}^n$, $\frac{1}{4} \cdot 2^k \leq |S| \leq \frac{1}{2} \cdot 2^k$
- $\Pr_{h \in_R \mathscr{H}_{n,k}}[\exists! x \in S : h(x) = 0^k] \geq 1/8$.

■ **Dôkaz.**

- nech $p = \Pr_{h \in_R \mathscr{H}_{n,k}}[h(x) = 0^k] = 2^{-k}$
- nech $N =$ počet $x \in S : h(x) = 0^k$
- $E[N] = |S|p \in [\frac{1}{4}, \frac{1}{2}]$
- $\Pr[N = 0] \leq 1 - |S|p + \binom{|S|}{2} p^2$ (princíp inklúzie, exklúzie)
- $\Pr[N \geq 2] \leq \binom{|S|}{2} p^2$ (union bound)
- $\implies \Pr[N = 1] \geq |S|p(1 - |S|p) \geq 1/8$

□

Unique SAT

■ **Dôkaz.**

- $k \in_R \{2,\ldots,n+1\}$ a $h \in_R \mathscr{H}_{n,k}$
- s pp. $1/n$ bude $2^{k-2} \leq |S| \leq 2^{k-1}$
- a vtedy s pp. $1/8$ existuje jediné x: $h(x) = 0^k$
- nech $\tau(x,y)$ je formula kódujúca „$h(x) = 0^k$“
- výsledok: $\psi \equiv \phi(x) \wedge \tau(x,y)$

□

Unique SAT

■ **Dôkaz.**

- $k \in_R \{2, \ldots, n+1\}$ a $h \in_R \mathscr{H}_{n,k}$
- s pp. $1/n$ bude $2^{k-2} \leq |S| \leq 2^{k-1}$
- a vtedy s pp. $1/8$ existuje jediné x: $h(x) = 0^k$
- nech $\tau(x,y)$ je formula kódujúca „$h(x) = 0^k$“
- výsledok: $\psi \equiv \phi(x) \wedge \tau(x,y)$

□

Unique SAT

■ **Dôkaz.**

- $k \in_R \{2, \ldots, n+1\}$ a $h \in_R \mathscr{H}_{n,k}$
- s pp. $1/n$ bude $2^{k-2} \leq |S| \leq 2^{k-1}$
- a vtedy s pp. $1/8$ existuje jediné x: $h(x) = 0^k$
- nech $\tau(x, y)$ je formula kódujúca „$h(x) = 0^k$"
- výsledok: $\psi \equiv \phi(x) \wedge \tau(x, y)$

□

■ **Dôkaz.**

- $k \in_R \{2, \ldots, n+1\}$ a $h \in_R \mathscr{H}_{n,k}$
- s pp. $1/n$ bude $2^{k-2} \leq |S| \leq 2^{k-1}$
- a vtedy s pp. $1/8$ existuje jediné x: $h(x) = 0^k$
- nech $\tau(x,y)$ je formula kódujúca „$h(x) = 0^k$"
- výsledok: $\psi \equiv \phi(x) \wedge \tau(x,y)$

□

Dôkaz.

- $k \in_R \{2, \dots, n+1\}$ a $h \in_R \mathscr{H}_{n,k}$
- s pp. $1/n$ bude $2^{k-2} \leq |S| \leq 2^{k-1}$
- a vtedy s pp. $1/8$ existuje jediné x: $h(x) = 0^k$
- nech $\tau(x,y)$ je formula kódujúca „$h(x) = 0^k$"
- výsledok: $\psi \equiv \phi(x) \wedge \tau(x,y)$

$\square$

Unique SAT

Veta

$\exists$ *PPT algoritmus f taký, že*

- $\phi \in \textsc{Sat} \implies \Pr[f(\phi) \in \textsc{USat}] \geq 1/8n$
- $\phi \notin \textsc{Sat} \implies f(\phi) \notin \textsc{Sat}$

$\oplus$**P**

Veta

$\exists$ *PPT algoritmus f taký, že*

- $\phi \in \textsc{Sat} \implies \Pr[f(\phi) \in \textsc{USat}] \geq 1/8n$
- $\phi \notin \textsc{Sat} \implies f(\phi) \notin \textsc{Sat}$

Veta

$\exists$ *PPT algoritmus f taký, že*

- $\phi \in \text{SAT} \implies \Pr[f(\phi) \in \oplus\text{SAT}] \geq 1/8n$
- $\phi \notin \text{SAT} \implies f(\phi) \notin \oplus\text{SAT}$

Veta

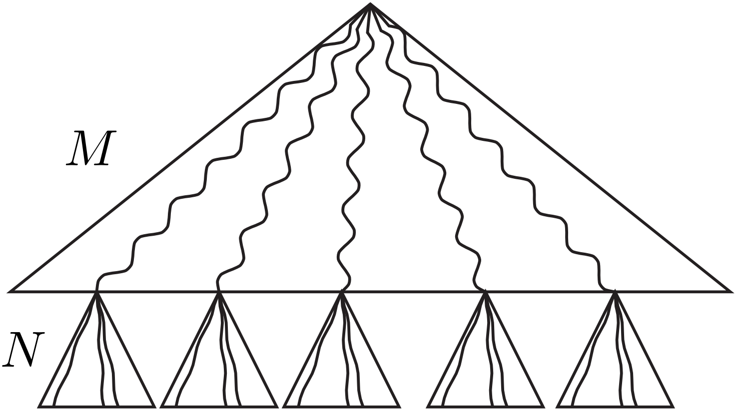
$\exists$ *PPT algoritmus f taký, že*

- $\phi \in \textsc{Sat} \implies \Pr[f(\phi) \in \oplus\textsc{Sat}] \geq 1 - 1/2^m$
- $\phi \notin \textsc{Sat} \implies f(\phi) \notin \oplus\textsc{Sat}$

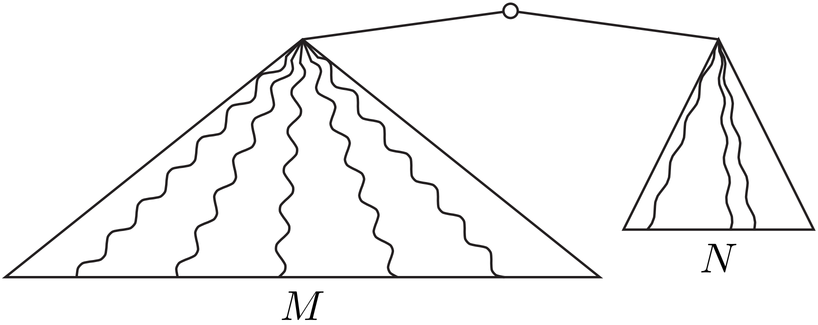
Veta

$\forall k$ $\exists$ PPT algoritmus f taký, že

- $\psi \in \Sigma_k \textsc{Sat} \implies \Pr[f(\psi) \in \oplus\textsc{Sat}] \geq 1 - 1/2^m$
- $\psi \notin \Sigma_k \textsc{Sat} \implies \Pr[f(\psi) \in \oplus\textsc{Sat}] \leq 1/2^m$.



M
N



M
N

$$[\phi \cdot \psi](x,y) \equiv \phi(x) \wedge \psi(y)$$

$$[\phi+\psi](x,y,z) \equiv [z \wedge \phi(x) \wedge \bigwedge_j \neg y_j)] \vee [\neg z \wedge \psi(y) \wedge \bigwedge_i \neg x_i)]$$

$$[\phi + 1](x, z) \equiv z \vee (\neg z \wedge \phi(x))$$

$$\Psi = [(\psi_1 + 1)(\psi_2 + 1) \cdots (\psi_R + 1) + 1]$$

kde $R = 8nm$

$$\Psi \in \oplus\textsc{Sat} \iff \exists i : \psi_i \in \oplus\textsc{Sat}$$

$\rightarrow$ s pp. $1 - (1 - 1/8n)^{8nm} \geq 1 - e^{-m}$

$$\Psi = [(\psi_1 + 1)(\psi_2 + 1) \cdots (\psi_R + 1) + 1]$$

kde $R = 8nm$

$$\Psi \in \oplus\textsc{Sat} \iff \exists i : \psi_i \in \oplus\textsc{Sat}$$

$\rightarrow$ s pp. $1 - (1 - 1/8n)^{8nm} \geq 1 - e^{-m}$

Lema (1)

$\forall k \; \exists \; PPT \; f$:

- $\psi \in \Sigma_k\textsc{Sat} \implies \Pr[f(\psi) \in \oplus\textsc{Sat}] \geq 1 - 1/2^m$
- $\psi \notin \Sigma_k\textsc{Sat} \implies \Pr[f(\psi) \in \oplus\textsc{Sat}] \leq 1/2^m$.

Lema 1

■ **Dôkaz.**

- nech $\phi = \exists x : \psi(x)$, kde ψ je Π_{k-1}-formula
- z IP dostaneme $\psi \mapsto \rho$
  - $\rho(x) \in \oplus\textsc{Sat} \iff \psi(x)$ (s pp. $\geq 1 - 2^{-(m+1)}$)
- použijeme VV-redukciu $K = 16nm$-krát:

$$\Psi = \bigvee_{j=1}^{K} \underbrace{\rho(x) \wedge \tau_j(x,y)}_{\rho'_j} = [(\rho'_1 + 1)(\rho'_2 + 1) \cdots (\rho'_K + 1) + 1].$$

- ak $\exists x : \rho(x)$, tak $\Psi \in \oplus\textsc{Sat}$ s pp. $\geq 1 - 2^{-(m+1)}$, inak $\Psi \notin \oplus\textsc{Sat}$.
- chyba môže nastať pri prevode $\psi \mapsto \rho$ a pri VV-reduckii, obe $\leq 2^{-(m+1)}$

□

Dôkaz.

- nech $\phi = \exists x : \psi(x)$, kde ψ je Π_{k-1}-formula
- z IP dostaneme $\psi \mapsto \rho$
  - $\rho(x) \in \oplus\textsc{Sat} \iff \psi(x)$ (s pp. $\geq 1 - 2^{-(m+1)}$)
- použijeme VV-redukciu $K = 16nm$-krát:

$$\Psi = \bigvee_{j=1}^{K} \underbrace{\rho(x) \wedge \tau_j(x,y)}_{\rho'_j} = [(\rho'_1 + 1)(\rho'_2 + 1) \cdots (\rho'_K + 1) + 1].$$

- ak $\exists x : \rho(x)$, tak $\Psi \in \oplus\textsc{Sat}$ s pp. $\geq 1 - 2^{-(m+1)}$, inak $\Psi \notin \oplus\textsc{Sat}$.
- chyba môže nastať pri prevode $\psi \mapsto \rho$ a pri VV-reduckii, obe $\leq 2^{-(m+1)}$

□

■ **Dôkaz.**

- nech $\phi = \exists x : \psi(x)$, kde ψ je Π_{k-1}-formula
- z IP dostaneme $\psi \mapsto \rho$
  - $\rho(x) \in \oplus\text{SAT} \iff \psi(x)$ (s pp. $\geq 1 - 2^{-(m+1)}$)
- použijeme VV-redukciu $K = 16nm$-krát:

$$\Psi = \bigvee_{j=1}^{K} \underbrace{\rho(x) \wedge \tau_j(x,y)}_{\rho'_j} = [(\rho'_1 + 1)(\rho'_2 + 1) \cdots (\rho'_K + 1) + 1].$$

- ak $\exists x : \rho(x)$, tak $\Psi \in \oplus\text{SAT}$ s pp. $\geq 1 - 2^{-(m+1)}$, inak $\Psi \notin \oplus\text{SAT}$.
- chyba môže nastať pri prevode $\psi \mapsto \rho$ a pri VV-reduckii, obe $\leq 2^{-(m+1)}$

□

Lema 1

■ **Dôkaz.**

- nech $\phi = \exists x : \psi(x)$, kde ψ je Π_{k-1}-formula
- z IP dostaneme $\psi \mapsto \rho$
  - $\rho(x) \in \oplus\mathrm{SAT} \iff \psi(x)$ (s pp. $\geq 1 - 2^{-(m+1)}$)
- použijeme VV-redukciu $K = 16nm$-krát:

$$\Psi = \bigvee_{j=1}^{K} \underbrace{\rho(x) \wedge \tau_j(x,y)}_{\rho'_j} = [(\rho'_1 + 1)(\rho'_2 + 1)\cdots(\rho'_K + 1) + 1].$$

- ak $\exists x : \rho(x)$, tak $\Psi \in \oplus\mathrm{SAT}$ s pp. $\geq 1 - 2^{-(m+1)}$, inak $\Psi \notin \oplus\mathrm{SAT}$.
- chyba môže nastať pri prevode $\psi \mapsto \rho$ a pri VV-reduckii, obe $\leq 2^{-(m+1)}$

□

Dôkaz.

- nech $\phi = \exists x : \psi(x)$, kde ψ je Π_{k-1}-formula
- z IP dostaneme $\psi \mapsto \rho$
  - $\rho(x) \in \oplus\textsc{Sat} \iff \psi(x)$ (s pp. $\geq 1 - 2^{-(m+1)}$)
- použijeme VV-redukciu $K = 16nm$-krát:

$$\Psi = \bigvee_{j=1}^{K} \underbrace{\rho(x) \wedge \tau_j(x,y)}_{\rho'_j} = [(\rho'_1 + 1)(\rho'_2 + 1)\cdots(\rho'_K + 1) + 1].$$

- ak $\exists x : \rho(x)$, tak $\Psi \in \oplus\textsc{Sat}$ s pp. $\geq 1 - 2^{-(m+1)}$, inak $\Psi \notin \oplus\textsc{Sat}$.
- chyba môže nastať pri prevode $\psi \mapsto \rho$ a pri VV-reduckii, obe $\leq 2^{-(m+1)}$

$\square$

Lema 1

$$\mathsf{PH} \subseteq \mathsf{BPP}^{\oplus\mathsf{P}[1]}$$

Todova veta

Veta (Toda)

$\mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}}$.

- $\mathrm{NP} \subseteq \mathrm{RP}^{\mathrm{USAT}}$.
- $\mathrm{PH} \subseteq \mathrm{BPP}^{\oplus\mathrm{P}}$.
- $\mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}}$.

Todova veta

Veta (Toda)

$\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}}$.

- $\mathsf{NP} \subseteq \mathsf{RP}^{\mathrm{USAT}}$.
- $\mathsf{PH} \subseteq \mathsf{BPP}^{\oplus\mathsf{P}}$.
- $\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}}$.

Lema

Existuje polynóm $p(x) \in \mathbb{Z}[x]$ *taký, že*

- *ak* $n \equiv 0 \pmod{m}$, *tak* $p(n) \equiv 0 \pmod{m^2}$ *a*
- *ak* $n+1 \equiv 0 \pmod{m}$, *tak* $p(n)+1 \equiv 0 \pmod{m^2}$.

Dôkaz. $p(x) = 3x^4 + 4x^3$

Lema

Existuje polynóm $p(x) \in \mathbb{Z}[x]$ *taký, že*

- *ak* $n \equiv 0 \pmod{m}$, *tak* $p(n) \equiv 0 \pmod{m^2}$ *a*
- *ak* $n + 1 \equiv 0 \pmod{m}$, *tak* $p(n) + 1 \equiv 0 \pmod{m^2}$.

■ **Dôkaz.** $p(x) = 3x^4 + 4x^3$

Ak $n = m \cdot k$, tak

$$p(n) = m^2 \times (3m^2k^4 + 4mk^3)$$

Ak $n = m \cdot k - 1$, tak

$$\begin{aligned} p(n) &= 3(m^4k^4 - 4m^3k^3 + 6m^2k^2 - 4mk + 1) \\ &\quad + 4(m^3k^3 - 3m^2k^2 + 3mk - 1) \\ &= m^2 \times (3m^2k^4 - 8mk^3 + 6k^2) - 1 \end{aligned}$$

$\square$

Lema

$\exists$ *deterministická poly-time transformácia, ktorá ku každej formule* Ψ *vyrobí* Λ, *pričom*

- $\Psi \in \oplus\text{SAT} \implies \#\Psi \equiv -1 \pmod 2 \implies \#\Lambda \equiv -1 \pmod{2^\ell}$, *ale*
- $\Psi \notin \oplus\text{SAT} \implies \#\Psi \equiv 0 \pmod 2 \implies \#\Lambda \equiv 0 \pmod{2^\ell}$.

Dôkaz. $\Psi_0 = \Psi$, $\Psi_{i+1} = [4\Psi_i^3 + 3\Psi_i^4]$ a $\Lambda = \Psi_{\lceil \log \ell \rceil}$. $\square$

Lema

$\exists$ *deterministická poly-time transformácia, ktorá ku každej formule* Ψ *vyrobí* Λ*, pričom*

- $\Psi \in \oplus\textsc{Sat} \implies \#\Psi \equiv -1 \pmod 2 \implies \#\Lambda \equiv -1 \pmod{2^\ell}$, *ale*
- $\Psi \notin \oplus\textsc{Sat} \implies \#\Psi \equiv 0 \pmod 2 \implies \#\Lambda \equiv 0 \pmod{2^\ell}$.

■ **Dôkaz.** $\Psi_0 = \Psi$, $\Psi_{i+1} = [4\Psi_i^3 + 3\Psi_i^4]$ a $\Lambda = \Psi_{\lceil \log \ell \rceil}$. □

Veta (Toda)

$\mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}}$.

■ **Dôkaz.**

- NTS $M(\phi)$:
  - nedeterministicky zvolí postupnosť r dĺžky R
  - spustí redukciu f_r z Lemy 1 $(m = 2)$,
  - dostane formulu Ψ_r
  - zväčší modulus $\longrightarrow \Lambda_r$
  - nedeterministicky zvolí riešenie x
  - overí, či je $\Lambda_r(x)$ a podľa toho akceptuje.
- koľko akceptačných výpočtov má $M(\phi)$?

- $\phi \implies$ pre aspoň $3/4$ r-iek $\Psi_r \oplus \textsc{Sat} \implies \#\Lambda_r \equiv -1 \pmod{2^\ell}$ $\implies \#M(\phi) \in [-2^R, -\frac{3}{4}2^R]$
- $\neg\phi \implies$ pre najviac $1/4$ r-iek $\Psi_r \oplus \textsc{Sat} \implies \#\Lambda_r \equiv -1 \pmod{2^\ell} \implies \#M(\phi) \in [-\frac{1}{4}2^R, 0]$

$\square$

- $\phi \implies$ pre aspoň $3/4$ r-iek $\Psi_r \oplus \textsc{Sat} \implies \#\Lambda_r \equiv -1 \pmod{2^\ell}$ $\implies \#M(\phi) \in [-2^R, -\frac{3}{4}2^R]$
- $\neg\phi \implies$ pre najviac $1/4$ r-iek $\Psi_r \oplus \textsc{Sat} \implies \#\Lambda_r \equiv -1 \pmod{2^\ell} \implies \#M(\phi) \in [-\frac{1}{4}2^R, 0]$

$\square$