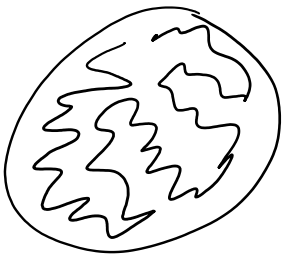
NP

2 November, 2020 21:21

Př: 1) HAM = { ⟨G⟩, G je graf obsahující Hamiltonovskou cestu }



↳ cesta, která navštíví všechny vrcholy a každý právě jednou.

HAM ∈ P ?

Pokud mi někdo ukáže Hamiltonovskou cestu, je snadné ji ověřit.

2) 3COL = { ⟨G⟩, vrcholy G lze obarvit třemi barvami tak, aby sousední vrcholy měli vždy různou barvu }

3COL ∈ P ?

Opět, dané obarvení lze snadno ověřit.

3) LIN = { S ; S je soustava lineárních rovnic, mající řešení }

LIN ∈ P

Dáno řešení, lze snadno ověřit

4) GO = { ⟨B, n⟩ ; B popis pozice na desce GO, n je nejlepší možný příští tah }

GO ∈ P?

Lze ověřit efektivně ověřit?

5) $\overline{HAM}$ Lze efektivně ověřit?

Ověřovatel: polynomiální algoritmus V t.ž.

$\forall x \in L \quad \exists w \in \{0,1\}^* \quad V(x,w) = 1$

$\forall x \notin L \quad \forall w \in \{0,1\}^* \quad V(x,w) = 0.$

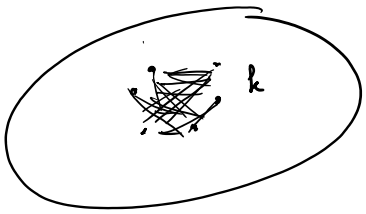
$NP = \{ L \subseteq \{0,1\}^*;$ ∃ ověřovatel pro L a polynom $p(n)$
$\forall x \in L: \exists w \in \{0,1\}^{p(n)}: V(x,w) = 1 \}.$ ($n = |x|$)
$\forall x \notin L \quad \forall w \in \{0,1\}^{p(n)}: V(x,w) = 0$

W... certifikát pro $x \in L$.
(svědek)

- HAM, 3COL, LIN $\in NP$

Otázka: $P = NP$? $1,000,000 Clay Math. Inst.

Př: • CLIQUE $= \{ (G,k);$ G is an undirected graph with a clique of size $k \}$



kterou connected to všechny

CLIQUE $\in NP$

- SUBSET-SUM $= \{ \langle S,t \rangle;$ $S = \{x_1 \dots x_n\}$ & $\exists T \subseteq S$ $\sum_{x \in T} x = t \}$

SUBSET-SUM $\in NP$

- SAT $= \{ \langle \phi \rangle;$ ϕ je splnitelná Booleovská formule $\}$

Booleovská formule: 1) proměnné $x_1, x_2, \dots x_n \in \{0,1\}$ or FALSE TRUE

2) spojky: $\neg, \wedge, \vee$ (negace, AND, OR)

Př: $(x_1 \wedge x_2) \vee (\neg x_1 \vee x_3) \vee (\neg x_7 \wedge \neg x_8)$

- Formule je splnitelná, pokud existuje přiřazení hodnot proměnným $x_1, \dots x_n$ t.ž.

přiřazení hodnot proměnným $x_1, \dots x_n$ t.ž.
formule se vyhodnotí na TRUE.

$SAT \in NP$

Pozorování: $NP \subseteq EXP$ $\qquad EXP = \bigcup_k DTIME(2^{n^k})$

Věta: (Cook-Levinova) $P = NP \Leftrightarrow SAT \in P$.
Dk viz níže.

Polynomiální redukce

Def: $A, B \subseteq \{0,1\}^*$ A je polynomiálně redukovatelný na B, pokud $\exists f: \Sigma^* \to \Sigma^*$ t.ž.
f lze spočítat v polynomiálním čase
a $\forall x \in \Sigma^* \quad x \in A \Leftrightarrow f(x) \in B$.

značení: $A \leq_m^P B$

Věta: Pokud $A \leq_m^P B$ a $B \in P$ pak $A \in P$

Př.: CNF tvar formule (konjunktivní normální tvar):

$(x_1 \vee x_2 \vee x_3 \vee \neg x_7) \wedge (\neg x_1 \vee \neg x_3 \vee x_8 \vee x_9) \wedge \dots$

klausule (disjunkce) — konjunkce — literál

- formule má CNF tvar, pokud je to konjunkce disjunkcí (klausulí)
- 3CNF - formule je v 3CNF tvaru, pokud je to konjunkce disjunkcí velikosti ≤ 3.
(každá klausule obsahuje ≤ 3 literály)

$3SAT = \{\langle \phi \rangle;\ \phi$ je splnitelná formule v 3CNF tvaru$\}$

- $3SAT \leq_m^P CLIQUE$

$\psi \xrightarrow{f} (G, t)$

$\psi \in 3SAT \Leftrightarrow G$ má klikovost t

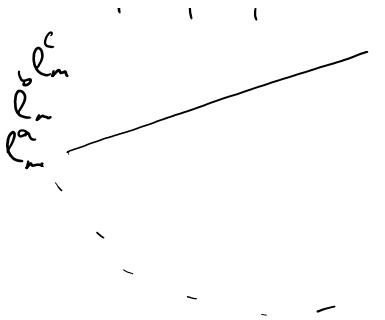
$\psi = (l_1^a \vee l_1^b \vee l_1^c) \wedge (l_2^a \vee l_2^b \vee l_2^c) \wedge (l_3^a \vee l_3^b \vee l_3^c) \dots \wedge (l_m^s \vee l_m^t \vee l_m^u)$

G $\quad l_1^a \quad l_1^b \quad l_1^c$

l_m^c $\qquad l_2^a$

l_2^b

vrcholy jsou



vrcholy jsou literály ze všech klauzulí

spojíme hranou
$\forall$ literály l_i^z a l_j^y
pokud $i \neq j$ a $l_i^z \neq \neg l_j^y$

$t = m$

- ψ má splňující ohodnocení $\Leftrightarrow$ G má kliku velikosti m.

"$\Rightarrow$" zvol pevné splňující ohodnocení. V každé klauzuli zvol jeden literál ohodnocený TRUE.
$\rightarrow$ klika velikosti m.

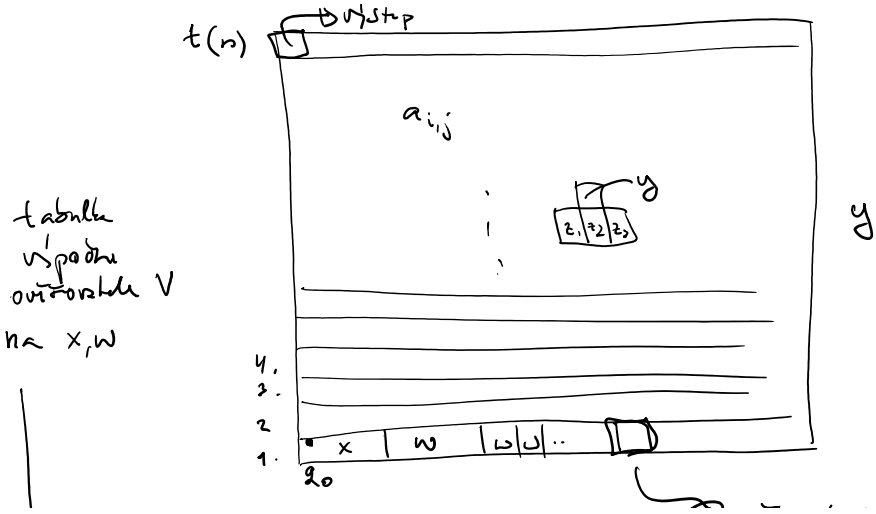
"$\Leftarrow$" zvol splňující ohodnocení, tak, aby literály z klik velikosti m měly hodnotu TRUE.
(zjevně klika vybere z každé klauzule jeden vrch)
$\rightarrow$ splňující ohodnocení splňuje všechny klauzule $\rightarrow$ ψ je splnitelná ■

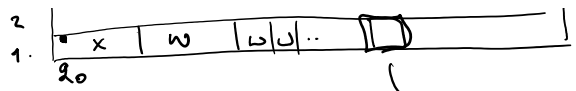
Pokud CLIQUE $\in P \Rightarrow$ 3SAT $\in P$.

- Def: $A \in NP$ je NP-úplný pokud $\forall B \in NP,\ B \leq_m^P A$.

Věta: (Cook-Levinova) SAT je NP-úplný.

Dk: Vezměme si $B \in NP$. Existuje pro něj ověřovací pracující v čase $t(n)$ s certifikátem velikosti $p(n) \leq t(n) - n$. Pro $\forall x \in \Sigma^n$ sestrojíme formuli ψ velikosti $O(t(n))^2 + \dots$ t.ž. $x \in B \Leftrightarrow \psi$ je splnitelná.





políčko obsahuje symbol pásky v daném kroce, indikátor, zda je tam zrovna hlava, a pokud ano, aktuální stav

$t(n)$ čas výpočtu v na vstupech velikosti n

- každé políčko je funkcí f^{konst} tří políček pod ním.
- hodnotu lze zakódovat pomocí C bitů. $C = 1 + \lceil \lg Q \rceil + \lceil \lg \Gamma \rceil$
  → lze sestrojit formuli, která testuje konzistenci vůči $f = f^{konst}$, t.j. je splněna pro zakódování hodnot x_1, x_2, x_3 a y
  $\Leftrightarrow y = f^{konst}(x_1, x_2, x_3)$.

$$\rightarrow \psi = \bigwedge_{i=1}^{t(n)} \bigwedge_{j=1}^{t(n)} \text{“} a_{i,j} = f(a_{i-1,j-1}, a_{i-1,j}, a_{i-1,j+1}) \text{”}$$

↑ přiměřené na okrajích.

$$\wedge \text{“} a_{t(n),1} = 1 \text{”} \wedge \bigwedge_{j=1}^{n} \text{“} x_j = a_{1,j} \text{”}$$

↖ výpočet přijde

ψ je splněná přijímajícím výpočtem V na $\underline{x}$ a vhodné $\underline{w}$

□

Pozorování: $\forall S \subseteq \{0,1\}^* \; \exists \psi(x_1 \dots x_n)$ t.ž.
$\psi(a_1 \dots a_n)$ je TRUE $\Leftrightarrow (a_1 \dots a_n) \in S$.

Věta: Pokud A je NP-úplný, $B \in NP$ a $A \leq_m^P B$, pak B je NP-úplný.

Dk: $\forall A, B, C$ pokud $C \leq_m^P A$ a $A \leq_m^P B$ pak $C \leq_m^P B$. □

Věta: Pokud A je v NP a $B \leq_m^P A$, pak B je v NP.

- Formuli ψ z důkazu Cook-Levinovy věty se dá zapsat jako CNF, stačí aby jednotlivé "malé" podmínky byly zapsány jako CNF (viz Dú.)

→ $CNF\text{-}SAT = \{\langle \varphi \rangle : \varphi$ je Booleovská formule

v CNF tvaru a φ je splnitelná]

CNF-SAT je NP-úplný.

3-SAT = $\{\langle\varphi\rangle ;$ φ je Booleovská fce v 3-CNF tvaru a je splnitelná $\}$

3-CNF: $(x_1 \vee \neg x_2 \vee x_3) \wedge (\ \vee\ \vee\ ) \wedge (\ \vee\ \vee\ ) \dots (\vee\vee)$

každá klauzule je disjunkce nejvýše 3 literálů.

- 3-SAT je NP-úplný

Dk: CNF-SAT $\leq_m^P$ SAT

CNF → 3-CNF

$\varphi \longrightarrow \varphi'$

$\varphi = C_1 \wedge C_2 \wedge C_3 \dots C_m$

klauzule $C_i = l_{i,1} \vee l_{i,2} \vee \dots \vee l_{i,k_i}$

- každý $l_{i,j}$ je buď proměnná nebo její negace
- zavedeme $k_i - 3$ nových proměnných $y_{i,1} \dots y_{i,k_i-3}$ a klauzuli C_i nahradíme konjunkcí klauzulí:

$$(l_{i,1} \vee l_{i,2} \vee y_{i,1}) \wedge (\neg y_{i,1} \vee l_{i,3} \vee y_{i,2}) \wedge$$
$$\wedge (\neg y_{i,2} \vee l_{i,4} \vee y_{i,3}) \dots (\neg y_{i,k_i-3} \vee l_{i,k_i-1} \vee l_{i,k_i})$$

$\longrightarrow \varphi'$ jejíž proměnné jsou původní proměnné φ spolu s pomocnými prom. $y_{i,j}$.

φ je splnitelná $\Leftrightarrow$ φ' je splnitelná

splnitelné ohodnocení $a_1 \dots a_n$ → splnitelné ohodnocení $a_1 \dots a_n$ kde $y_{i,j}$ jsou nastaveny tak, že pokud $l_{i,r}$ je TRUE, pak $y_{i,j}$ = TRUE pro $j < r-1$

a $y_{i,j}$ = FALSE pro $j \leq r-1$

$a_1, \dots a_n$ splňuje ψ ⟵ ohodnocení $a_1 \dots a_n, y_{i,j}$ splňuje ψ'

klauzule C_i se přepíše do ψ'
na $k_i - 2$ klauzulí
za použití $k_i - 3$ pomocných proměnných, tj. mohou
pomocí splnit právě $k_i - 3$ těchto klauzulí;
tzn. alespoň jedna klauzule musí být
splněna pomocí původního literálu
který také splní původní klauzuli C_i. ③

- 3-SAT je NP-úplný a 3-SAT $\leq$ CLIQUE
  $\Rightarrow$ CLIQUE je NP-úplný.

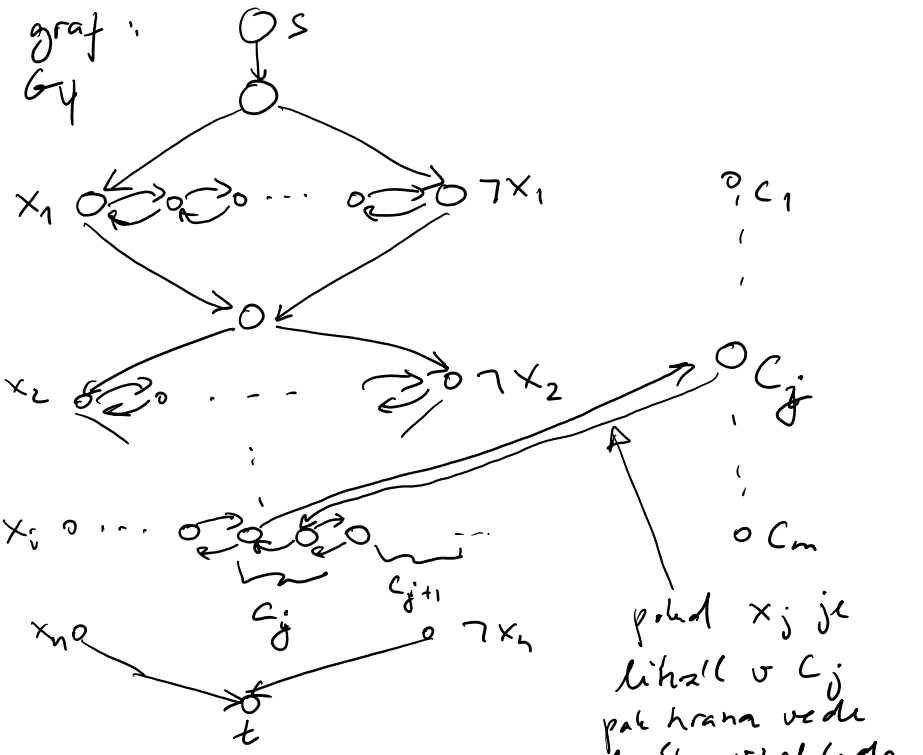
- DHAM = {⟨G⟩, G je orientovaný graf obsahující Hamiltonovskou cestu}

Věta: DHAM je NP-úplný.

Důk.: 3-SAT $\leq_m^P$ DHAM:

ψ formule s proměnnými $x_1 \dots x_n$ a klauzulemi $C_1 \dots C_m$

→ graf:



Hamilt. cesta musí začít v s.

jít do t a přijít do řádku x_i buď zleva nebo zprava a vyhýbat na druhou stranu

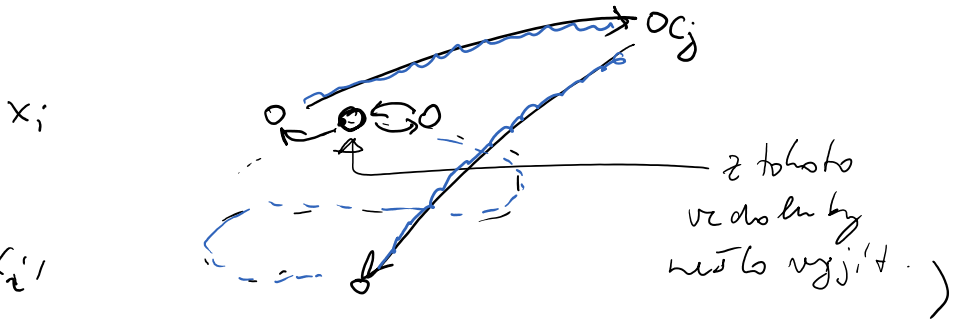
(klec = x_i je TRUE, zprava = "$\neg x_i$ je TRUE")

c_j, jinak do ... vedl z pravého vrcholu.

pokud jsme zleva, můžeme navštívit klauzule C_j, které obsahují literál x_i, pokud jdeme zprava, můžeme navštívit klauzuli C_j obsahující $\neg x_i$.

$\Rightarrow$ pokud ψ je splnitelná, můžeme navštívit všechny vrcholy různých $C_1, \dots C_m \Rightarrow \exists$ Ham. cesta

Pokud $\exists$ Ham cesta v G_ψ, pak odpovídá splňujícímu ohodnocení. (Nutno ověřit, že tato cesta nemůže projít graf způsobem

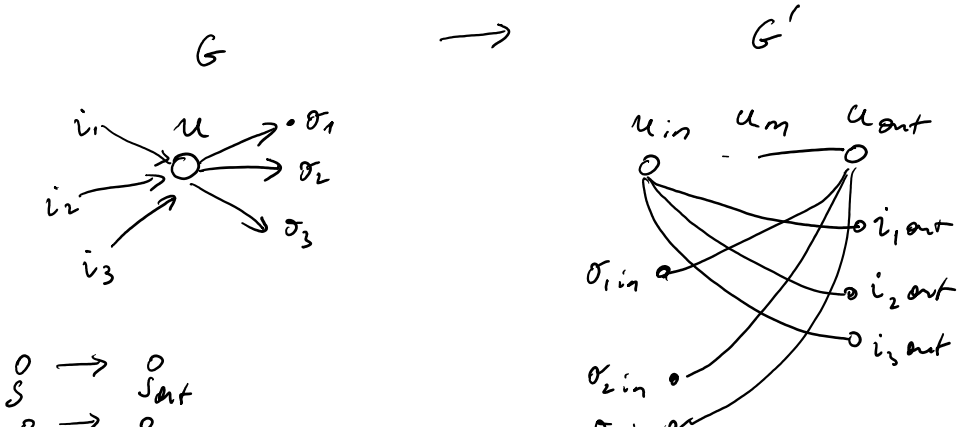


)

- HAM je NP-úplný

  HAM = {⟨G⟩, G je neorientovaný graf obsahující Hamiltonovskou cestu}

Dk: DHAM $\leq_m^P$ HAM



$s \to s_{out}$

$t \to t_{in}$

$u \to u_{in}\ u_m\ u_{out}$

Ham. cesta v G → Ham cesta z s_{out} do t_{in} v G'

z s do t

— // — ⟵ — // —

cesta z s_{out} jde do nějakého u_{in}. Pokud nepokračuje do u_m, nebo u_m již navštívil. (Zůstali bychom v něm)

⇒ pokračuje $u_{in} \to u_m \to u_{out}$ a jde do dalšího u'_{in}, atd. Nakonec skončí v t_{in}. Stejnou cestu lze následovat v G. ☒

- SUBSET-SUM $= \{(\{x_1, x_2, \dots x_k\}, t)$, celá čísla $x_1, \dots x_k, t$ a existuje $S \subseteq \{x_1, \dots x_k\}$, t.ž. $\sum_{x \in S} x = t\}$

Viz: SUBSET-SUM je NP úplný.

Dk: 3-SAT $\le_m^P$ SUBSET-SUM:

$\varphi = l_1 \wedge l_2 \dots \wedge c_m \longrightarrow z_1, \dots z_n, \bar{z}_1, \dots \bar{z}_n, z'_1, \dots z'_m, z^2_1, \dots z^2_m$

VAS $x_1, x_2, \dots, x_n$

deskriptivní zápis

$z_i = \underbrace{00\dots1}_{n}\underbrace{00\dots0}_{m}\ \underbrace{00}_{i}\ \underbrace{1}_{j}\ 00$

literál x_i je v c_j

jinak 0

$\bar{z}_i =$ — // — — // — 100

$\neg x_i$ je v c_j

$z^2_1 = z^1_1 = \underbrace{00\dots0}_{n}\ \underbrace{00\dots0}_{m}\ \underbrace{1}_{j}00\dots0$

$z_1 = t_1 = 00\ldots0$ (n) $\ldots$ (m) $\ldots$ (0)

$t = 11\ldots1333\ldots3$

pokud je ψ splnitelná, splňující ohodnocení
určí zda pro každé i, použít z_i nebo $\overline{z}_i$.
Splnění klauzule se naší hodnotou $\in\{1,2,3\}$, která se doplní
dle potřeby ponorí z_1^2 nebo $\overline{z}_1^2$ na
hodnotu 3 v dané pozici.. ∎

$TAUT = \{\langle\varphi\rangle,\ \varphi$ je Booleovská formule, která
je pravda pro každé ohodnocení
proměnných$\}$

př: $(x_1 \vee \neg x_1) \in TAUT$

- $TAUT \in NP$?
  - $\varphi \in TAUT \iff \neg\varphi \notin SAT$

    $\Rightarrow \overline{TAUT} \le_m^P SAT$ & $SAT \le_m^P \overline{TAUT}$

    $\overline{TAUT} \in NP$ & $\overline{TAUT}$ je NP-úplný
  - $TAUT \in P \Rightarrow P = NP$
  - $TAUT \le_m^P SAT$? [Nikdo neví]

$coNP = \{ L \subseteq \{0,1\}^*;\ \overline{L} \in NP\}$

alternativně: $L \in coNP$ pokud existuje polynomiální
ověřovatel V a polynom $p(n)$ t.ž.

$\forall x \in \{0,1\}^*$ $\quad x \in L \Rightarrow \forall c \in \{0,1\}^{p(|x|)}: V(x,c)=1$

$\quad x \notin L \Rightarrow \exists c \in \{0,1\}^{p(|x|)}: V(x,c)=0$

- $L_V = \{(x,c);\ V(x,c)=1\}$ $\quad L_V \in P$.

  L_V definuje L

- $QBF = \{\langle\varphi\rangle$; φ je kvantifikovaná Bool. formule, která je TRUE $\}$

Př: $\forall x\, \exists y\, (x \vee y) \wedge (\neg x \vee y) \in QBF$

$\forall y\, \exists x\, (x \vee y) \wedge (\neg x \vee y) \in QBF$

$\forall y\, (y) \notin QBF$

formule je Σ_1-formule, pokud jsou všechny proměnné kvantifikovány existenčně, $\exists x_1 \exists x_2 \dots \exists x_n \varphi(x_1 \dots x_n)$

Σ_1-SAT $= \{\langle\varphi\rangle$; φ je Σ_1-fle, která je pravdivá $\}$

Σ_1-SAT $\equiv$ SAT

Σ_k-Fle $\exists x_1^1 \exists x_2^1 \dots x_n^1 \forall x_1^2 \dots x_n^2 \exists x_1^3 \dots x_n^3 \forall x_1^4 \dots \varphi(x_1^1 \dots x_n^1, \dots x_n^k)$

k bloků kvantifikátorů

Σ_1 začínáme $\exists$

Π_k-Fle — // — ale začínáme $\forall$

Π_1-SAT $\equiv$ TAUT

- TAUT je coNP-úplný

↳ $\in$ coNP & $\forall B \in$ coNP . $B \leq_m^P$ TAUT

Dk: $\overline{B} \in NP \Rightarrow \overline{B} \leq_m^P SAT \Rightarrow \overline{B} \leq_m^P \overline{TAUT}$

$\Rightarrow B \leq_m^P$ TAUT.

□

Σ_k-SAT $= \{\langle\varphi\rangle$; φ je pravdivá Σ_k-fle $\}$

Π_k-SAT $= \{\langle\varphi\rangle$; φ je pravdivá Π_k-fle $\}$

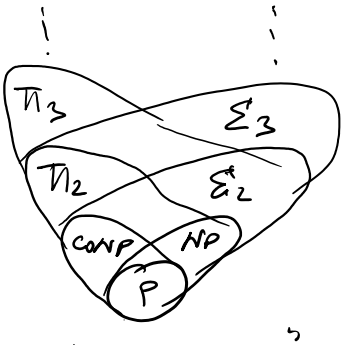
třídy jazyků $\Sigma_k = \{ L \subseteq \{0,1\}^* ;\ L \leq_m^P \Sigma_k\text{-SAT} \}$

$\Pi_k = \{ L \subseteq \{0,1\}^* ;\ L \leq_m^P \Pi_k\text{-SAT} \}$

- Σ_k-SAT je Σ_k-úplný, podobně pro Π_k-SAT

- $k \geq 1$; $\Sigma_k \subseteq \Sigma_{k+1}$

  $\Pi_k \subseteq \Sigma_{k+1}$



$PH = \bigcup_k \Sigma_k$

PH... "polynomiální hierarchie"

- $\mathcal{C}$ ... třída jazyků

  A je $\mathcal{C}$-úplný pokud $A \in \mathcal{C}$ a $\forall B \in \mathcal{C}, B \leq_m^P A$.

Př: 1) Σ_2-SAT je Σ_2-úplný

2) REDUNDANT = $\{\langle \varphi, k \rangle ;$ φ je Bool. fce v DNF takové, že některé je možné odebrat k "termů" a dostaneme ekvivalentní formuli$\}$

DNF $(\neg x_1 \wedge x_2 \wedge x_3) \vee (x_7 \wedge x_8 \ldots) \vee \ldots$

term, literál

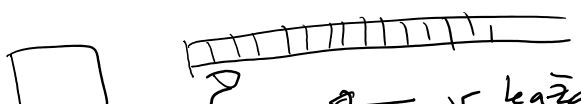
Disjunkce termů

REDUNDANT je Σ_2-úplný

3) 2-COL-AVOID = $\{\langle G, F \rangle ;$ lze obarvit G dvěma barvami, že neobsahuje F jako jednobarevný podgraf$\}$ ... Σ_2-úplný.

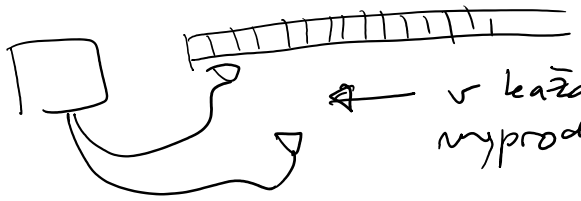
- nedeterministický a pravděpodobnostní výpočty

pásk. TS



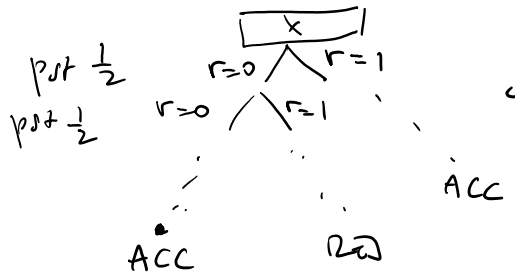
... v každém kroce

pstní TS



TS M s náhodným bitem (pravděpodobnostní TS)

Otázka: Pro daný vstup x, jaká je pravděpodobnost, že M přijme x? $\quad p_M(x) \in [0,1]$



strom výpočtu

$L \in NP \iff \exists$ pravděpodobnostní TS M pracující v poly čase t.ž.

$$\forall x \in \{0,1\}^* \quad \begin{array}{ll} x \in L & \Rightarrow \; p_M(x) > 0 \\ x \notin L & \Rightarrow \; p_M(x) = 0 \end{array}$$

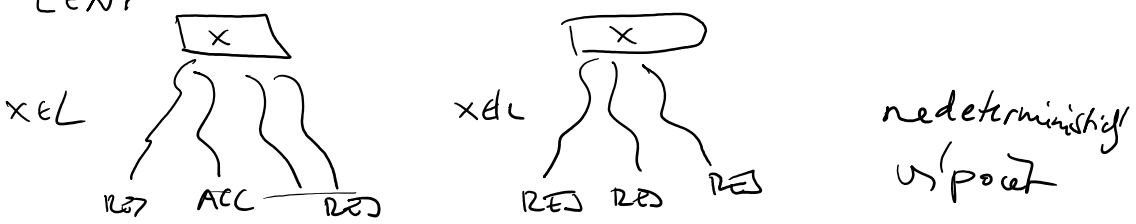
- Def: BPP

$L \in BPP \iff \exists$ pstní TS pracující v poly čase t.ž.

$$\forall x \in \{0,1\}^* \quad \begin{array}{ll} x \in L & \Rightarrow \; p_M(x) \geq 2/3 \\ x \notin L & \Rightarrow \; p_M(x) \leq 1/3 \end{array}$$

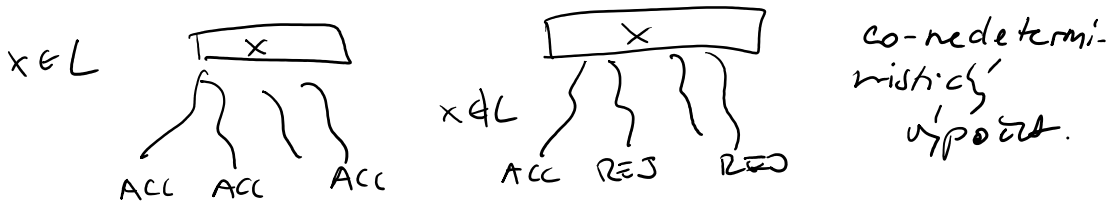
"chyba M na x"

$L \in NP$



nedeterministický výpočet

$L \in coNP$



co-nedeterministický výpočet.

- stejný TS, ale liší se interpretací podmínky přijetí

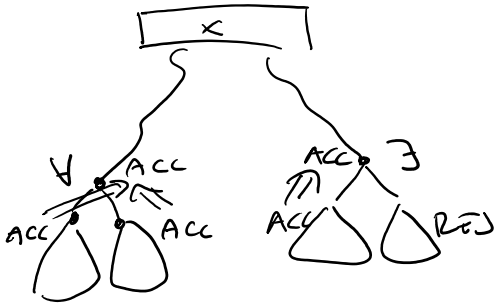
NP → polynomial-time
↳ non-deterministic

BPP → probabilistic → poly-time
↳ bounded error

P → polynomial time

- alternující výpočty – každý stav TS je buď → pravděpodobnostního
označený jako ∃ nebo jako ∀

pro vstup x se přijetí definuje indukcí odspodu stromu výpočtu:



stav ∀ přijímá, pokud oba podstromy výpočtu přijímají
stav ∃ přijímá, pokud alespoň jeden podvýpočet přijímá.

- QBF lze rozpoznávat alternujícími TS pracujícími v poly čase.