

Definice: Jazyk L patří do třídy ZPP (zero-error probabilistic polynomial), pokud existuje RTM M takový, že:

- 1) Ještě $w \notin L$, pak M se úspěšně rozhodí o pravděpodobnosti 0.
- 2) Ještě $w \in L$, pak M se úspěšně rozhodí o pravděpodobnosti 1.
- 3) Hlavní hmotnost počtu kroků M v jednom řešení je $p(n)$, kde $p(n)$ je polynom a n je délka vstupního slova.

$\approx M$ nenechá chybu, ale nezáručuje, že bude vždy polynomiální.

Definice: RTM splňující podmínky níže se nazývá stroj typu Las Vegas.

Tvrzení: Ještě L patří do ZPP , pak i I patří do ZPP . (prohodíme koncové a meziprocesy — → všechny RTM nejsou hledacího typu)

Definice: Jazyk L patří do třídy co-RP iff I patří do třídy RP.

Věta: Platí: $PS \subseteq ZPP$, $RP \subseteq NP$, $co\text{-}RP \subseteq co\text{-}NP$

Věta: $ZPP = RP \cap co\text{-}RP$. Když tedy $RP = co\text{-}RP$, tak $ZPP = RP$. důkaz bude příště.

TAL přednáška Důkaz: 1) nejdříve ukážeme, že $RP \cap co\text{-}RP \subseteq ZPP$

7.5.2019

Předpokládejme, že jazyk L leží v obou třídách $RP \cap co\text{-}RP$, existují dva TM typu Monte Carlo: M_1 pro L , a M_2 pro \bar{L} . Označme $p(n)$ den větší s polynomem, které označuje počet kroků M_1 a M_2 . Ještě jiné RTM typu Las Vegas pro jazyk L lze: Pro dané vstupní slovo délky n :

- 1) M nechá pracovat M_1 po dobu $p(n)$ kroků. Ještě M , úspěšně skončí pak i M úspěšně skončí.
- 2) M nechá pracovat M_2 po dobu $p(n)$ kroků. — → — neúspěšně — → — neúspěšně — → —.
- 3) Ještě M měskončíl v 1 nebo 2, pokračuje opět krokem 1.

Dá se ukázat, že M je typu Las Vegas.

2) nyní ukážeme, že $ZPP \subseteq RP \cap co\text{-}RP$.

Předpokládejme, že $L \in ZPP$, tedy k němu existuje RTM typu Las Vegas. Označme $p(n)$ polynom, který učíslaví střední hmotnost počtu kroků RTM M pro vstupní slovo délky n . Vyslovíme RTM M typu Monte Carlo pracující o polynomiálním čase.

M nechá na vstupu w pracovat M_1 , po dobu $2 \cdot p(n)$. Pokud M_1 skončí úspěšně, skončí i M . Pokud skončí neúspěšně nebo neshončí některou zároveň, skončí M neúspěšně.

Dá se ukázat, že M je typu Monte Carlo

Prostore ZPP je rozšířena na doplnky, již i každý jazyk se ZPP ve vídě $co\text{-}RP$.

Věta: Platí: $PS \subseteq ZPP$, $RP \subseteq NP$, $co\text{-}RP \subseteq co\text{-}NP$.

Každý TM je slavně RTM Las Vegas \Leftarrow Pro RTM Monte Carlo sestavíme NTM, který L přijímá.

Definice: Jazyk L je rekurzivní spočívající, označujeme RE, ještě existuje TM M , který přijímá jazyk L .

- Jazyk L je rekurzivní, označujeme R, ještě existuje TM M , který ho rozhoduje

Jazyky, které nejsou rekurzivní, se nazývají nerozhodnutelné nebo algoritmicky neročitelné.

Tvrzení: Ještě je I rekurzivní, pak je i jeho doplnek \bar{I} rekurzivní.

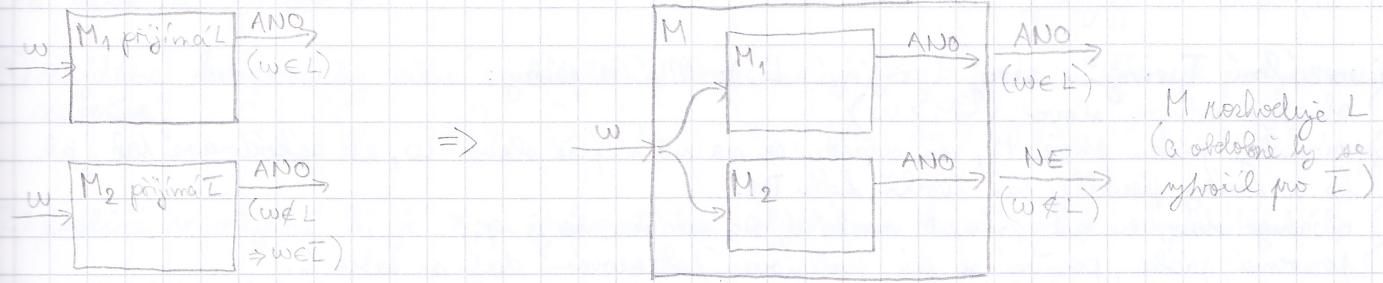
I je rekurzivní, tj. máme TM M , který ho rozhoduje



sestavíme M'
 M' rozhoduje \bar{I}



první tvrzení: Je-li L i \bar{L} rekvereně pročitné, pak jsou i rekverené.



Turingův stroj jako slovo nad abecedou (kód Turingova stroje)

$$\Sigma = \{0, 1\}$$

- slovo q_1 je vstupní, slovo q_2 je koncový následující orální slavu
- páskové symboly jsou $\Gamma = \{X_1, X_2, \dots\}$, kde $X_1 = 0, X_2 = 1, X_3 = B$ a další jsou libovolné páskové symboly.
- pohyby hlavy směrem $D_1 = R, D_2 = L$.

Přechodovou fci $S(q_i, X_j) \rightarrow (q_k, X_l, D_m)$ zapisujeme pomocí znaku 0 a 1: $0^i 1 0^j 1 0^k 1 0^l 1 0^m$, kde jednotky jsou oddělovací a nuly rozdělují indexy stavu, znaku, pohybu hlavy atd.

Kód TM M , nazíváme $\langle M \rangle$, jsou tři jednotky, náslekování všemi přechody v M a ukončení všemi jednotkami. Vše přechody w_i : $\langle M \rangle = M w_1 M w_2 M w_3 \dots w_m M$

Pení jeden TM lze vykortit víc kódů, ale rekonstrukce TM z kódu je jednoznačná.

Binární slova uspořádání do posloupnosti

- slovo $w \in \{0, 1\}^*$ je na místě k , kde k má binární zápis $1k$. (nejprve slova zadáme podle délky, stejně očekáváme seřaditě lexicograficky)

Diagonální jazyk L_d



Na místě i, j v tabulce je 0, když TM s kódem w_i je neplatný, nebo když nepřijímá slovo w_j . Na místě i, j je 1, když TM s kódem w_i přijímá slovo w_j .

Diagonální jazyk je jazyk všech slov, které mají na diagonále mlu, tj samy sebe nepřijímají.

$$L_d = \{\langle M \rangle \mid M \text{ nepřijímá slovo } \langle M \rangle\}$$

Jazyk L_d není R ani RE.

Uta: Neexistuje TM, který by přijímal diagonální jazyk.

Je sporem: Když existoval M_d , že $L_d = L(M_d)$, tak můžeme M_d zaplatit jako nějakého w_d : $\langle M_d \rangle = w_d$. Pak by, že v tabulce neměře na pozici $[w_d, w_d]$ bylo nula ani jednička.

Když $[w_d, w_d] = 0$, pak to znamená, že w_d svoje w_d nepřijímá. Zároveň to znamená, že $w_d \notin L_d$. Pokud by ale $\langle w_d \rangle$ opravdu přijímal L_d , musel by přijmout i w_d .

Když $[w_d, w_d] = 1$, znamená to, že w_d je přijímatelný stejnem $\langle w_d \rangle$. Tím pádem by w_d nemohlo být v L_d , ale to by bylo矛盾, že $[w_d, w_d] = 0$.

M_d nebezpečí vydávat žádoucí slovení, nemůže tedy existovat.

Univerzální jazyk: $L_u = \{\langle M \rangle w \mid w \in L(M)\}$, tj. obsahuje dvojice $\langle M \rangle$ a w , kde M přijímá w .

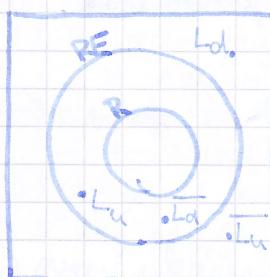
Univerzální Turingův stroj (přijímá L_u); má 4 pásky:

- 1) obsahuje vrchní slovo $\langle M \rangle w$
- 2) simuluje písací stroj M , na sáčku se mu napsí slovo w , ale záklodovane' tak, jak by se maky převdly píti kódůho kódů TM.
- 3) obsahuje stav, ve kterém se M nachází, na sáčku to je q_1 .
- 4) pomocná píska, používá se píti pohybováním/skracováním dat na páse 2.

Pri práci: Najde na páse 1 stav s pásky 3 a symbol se 2. Poče pohybem pásek 2 a posune se na ni, a píše stav na 3. Když se, když na páse 3 je $w=00$, tj. q_2 , → ale je rek. spočet.

Tvzení: Univerzální TM rozchodejí L_u (L_u není rek. spočet).

Dle: Kdyby existoval M_u , který rozchodejí L_u , pak s něj ryboume M_d , který rozchodejí L_d .



Definice: Uloha U se redukuje ($U \leq V$) na úlohu V , jestliže existuje TM A, který pro každou instance I řešení U vytaví instance P řešení V, alesy:

I je AND instance U iff P je AND instance V.

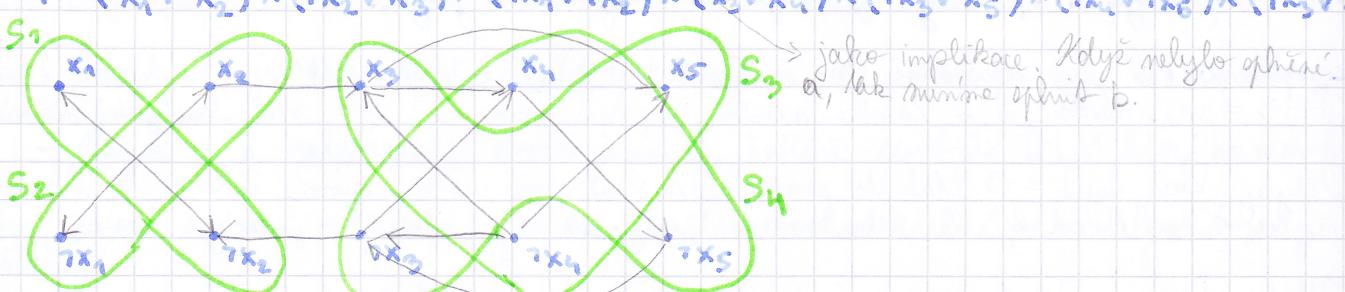
Tvzení: Použáme dve řešoby U, V, tedy $U \leq V$:

- 1) Jestliže V je rozhodnutelná, pak U je rozhodnutelná.
- 2) Jestliže V je nerozhodnutelná, pak U je nerozhodnutelná.
- 3) Jestliže jazyk U není rek. spočet, pak není ani jazyk V.

vižení
9.5.2019 Problem SAT (neplnitelnost CNF) je NP úplný, stejně jako 3-SAT.
Problem 2-SAT je polynomický.

$\Phi = C_1 \wedge C_2 \wedge \dots \wedge C_m$, $C_i = l_1^i \vee l_2^i$, logické proměnné x_1, x_2, \dots, x_n , $|V| = 2^n$
Ustřejme orientovaný graf $G(\Phi)$, kde vrcholy jsou log. proměnné a jejich negace. Pro každou klauzuli $C_j = a \vee b$ vede hranice z $\neg a$ do b a hranice z b do a , celkem $|E| = 2^m$.

Př: $\Phi = (x_1 \vee x_2) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2) \wedge (x_3 \vee x_4) \wedge (\neg x_3 \vee x_5) \wedge (\neg x_4 \vee x_5) \wedge (\neg x_5 \vee x_1)$



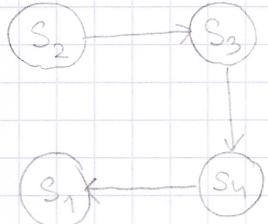
- 1) Existuje-li v grafu orientovaný sled $a \rightarrow b \rightarrow \neg a$, pak existuje i orientovaný sled $\neg b \rightarrow a \rightarrow \neg a$.
- 2) Existuje-li v $G(\Phi)$ cesta $a \rightarrow b$ a $n(a) = 1$, pak $n(b) = 1$, musí $n(b) = 1$.

Ψ je ne splňovaná i f f existuje pravěká x , že v G existují orientované cesty z x do $7x$ nebo z $7x$ do x .

1) najdeme komponenty silné souvislosti, označme je S_1, S_2, \dots . To je polynomické náročné.
 $S = \{ \{x_1, 7x_2\}, \{7x_1, x_2\}, \{x_3, 7x_4, x_5\}, \{7x_3, x_4, 7x_5\} \}$

2) jestliže některá S_i je x a zároveň $7x$, algoritmus končí, Ψ je ne splňovaná.

3) seškrjme bordemaci grafu a udělajme topologicky uspořádání.



uspořádání: T_1, T_2, T_3, T_4
 S_2, S_3, S_4, S_1

4) ochotníme všechny x . Označme T_i komponentu, kde leží x , a T_j komponentu s $7x$.

$$u(x) = 1 \text{ iff } i > j$$

$$u(x) = 0 \text{ iff } j > i$$

V takovém ochotnění bude Ψ pravdivá.

Dk: Když pravidlo platí, tak existuje $c_i = a \vee b$, $u(a \vee b) = 0$, $u(a) = 0$, $u(b) = 0$. Označme $a \in T_{i_1}$, $b \in T_{i_2}$, $\neg a \in T_{i_3}$, $\neg b \in T_{i_4}$ komponenty souvislosti. Dle pravidel ochotnění: $i_1 < i_3$, a zároveň $i_2 < i_4$.
 Protiče $a \vee b \in \Psi$, $G(\Psi)$ má hrany $\neg a \rightarrow b$, $\neg b \rightarrow a$, proto $i_3 \leq i_2$, $i_4 \leq i_1$.
 Z toho $i_1 < i_3 \leq i_2 < i_4 \leq i_1 \Rightarrow i_1 = i_4$, což je spor.

Pr: G je orientovaný graf, chceme ukázat: Hamilton. orient. cyklus \Leftrightarrow Ham. orient. cesta
 Je-li libovolný uzel $v \in G(v)$ a na druhé straně ho uzel v_1 a v_2 . Všichni hrany do v povedou do v_1 , všechny hrany z v povedou do v_2 .



Hamiltonovsky cyklus v G existuje, právě když v G' existuje ham. cesta z v_2 do v_1 .

Pr: Hamiltonovské kroužnice \Leftrightarrow Ham. orientovaná cesta.

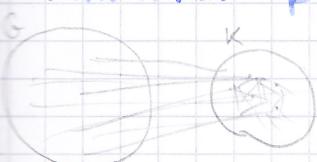
Uzel v rozdělíme na v_1 a v_2 jako předním, ale v_1 a v_2 mají všechny hrany jítce v. V neorientovaném grafu může být jiná ham cesta, která by nezahrnula kroužnicu v G . Proto přidáme uzel v_3 a v_4 spojení mezi v_1, v_2 . V G existuje ham kroužnice, i f f v G' existuje ham cesta z v_3 do v_4 .



\Leftarrow : 3 barevnost \Leftrightarrow 4 barevnost

Do G přidáme uzel v , který má hrany spojen se všemi ostatními uzelmi. Takhý uzel musí mít jednu barvu sam pro sebe.

\Leftarrow : 3 barevnost \Leftrightarrow k-barevnost



Do G přidáme K , když nphyj podgraf o $k-3$ uzelích. Když z uzelů v K pripojíme hrany ke všem uzelům v G .