TAL

- TŘÍDY SLOŽITOSTI ÚLOH / JAZYKŮ A TO JAK VZHLEDEM K ČASOVÉ SLOŽITOSTI JEJICH ŘEŠENÍ, TAK I PAMĚŤOVÉ SLOŽITOSTI VČETNĚ NEROZHODNUTELNÝCH ÚLOH / JAZYKŮ

- ALGORITMUS
  - POSLOUPNOST VÝPOČETNÍCH KROKŮ PŘEVÁDĚJÍCÍ VSTUP NA VÝSTUP
- INSTANCE PROBLÉMU
  - ZADÁNÍ PARAMETRŮ KTERÁ DANÁ ÚLOHA OBSAHUJE
- ALGORITMUS A ŘEŠÍ ÚLOHU U
  - JESTLIŽE PRO KAŽDÝ VSTUP VRÁTÍ SPRÁVNÉ ŘEŠENÍ
  - MUSÍ SE VŽDY ZASTAVIT
- ANALÝZA ČASOVÉ SLOŽITOSTI
  - NEJHORŠÍ PŘÍPAD
    - $T(n)$
  - PRŮMĚRNÁ SLOŽITOST
    - $T_{AVER}(n)$
    - JAK DLOUHO TRVÁ VYŘÍŠIT INSTANCI VELIKOSTI n A BERE SE V ÚVAHU S JAKOU PRAVDĚPODOBNOSTÍ SE JEDNOTLIVÉ ÚLOHY VYSKYTUJÍ

- ASYMPTOTICKÝ RŮST FUNKCÍ
  - $g(n)$ MUSÍ BÝT NEZÁPORNÁ FCE ($f(n)$ TAKÉ)

"ALESPOŇ TAK"

- O
  - $O(g(n)) = \{f(n) \mid \exists c > 0,\ n_0 \in \mathbb{N}$ TAK ŽE $f(n) \leq c \cdot g(n)\ \forall n \geq n_0\}$
- Ω
  - $\Omega(g(n)) = \{f(n) \mid \exists c > 0,\ n_0 \in \mathbb{N}$ TAK ŽE $f(n) \geq c \cdot g(n)\ \forall n \geq n_0\}$
- Θ
  - $\Theta(g(n)) = \{f(n) \mid \exists c_1 > 0,\ c_2 > 0,\ n_0 \in \mathbb{N}$ TAK ŽE $c_1 \cdot g(n) \leq f(n) \leq c_2 \cdot g(n)\ \forall n \geq n_0\}$

"VÍCE PŘÍ"

- o
  - $o(g(n)) = \{f(n) \mid \forall c > 0\ \exists n_0 \in \mathbb{N}$ TAK ŽE $0 \leq f(n) < c \cdot g(n)\ \forall n > n_0\}$
- ω
  - $\omega(g(n)) = \{f(n) \mid \forall c > 0\ \exists n_0 \in \mathbb{N}$ TAK ŽE $f(n) > c \cdot g(n) \geq 0\ \forall n > n_0\}$

- $f(n) \in o(g(n))$ PRÁVĚ TEHDY KDYŽ $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$

  - PŘEPÍŠEME LIMITU

$$\forall \varepsilon > 0 \ \exists n_0 \in \mathbb{N} \text{ TAK, ŽE } \forall n \geq n_0 \text{ PLATÍ } \left| \frac{f(n)}{g(n)} \right| < \varepsilon$$

  - MŮŽEME PŘEPSAT NA

$$\forall \varepsilon > 0 \ \exists n_0 \in \mathbb{N} \text{ TAK, ŽE } \forall n \geq n_0 \text{ PLATÍ } f(n) < \varepsilon g(n)$$

  - KDYŽ $\varepsilon = 0$ PAK MÁME DEFINICI $f(n) \in o(g(n))$

- $f(n) \in \omega(g(n))$ PRÁVĚ TEHDY KDYŽ $\lim_{n\to\infty} \frac{f(n)}{g(n)} = \infty$

- JESTLIŽE $\lim_{n\to\infty} \frac{f(n)}{g(n)} = a$ PRO $a \in \mathbb{R}$, $a \neq 0$ PAK $f(n) \in \Theta(g(n))$

  - PŘEPÍŠEME LIMITU

$$\forall \varepsilon > 0 \ \exists n_0 \in \mathbb{N} \text{ TAK, ŽE } \forall n \geq n_0 \text{ PLATÍ } \left| \frac{f(n)}{g(n)} - a \right| < \varepsilon$$

  - MŮŽEME PŘEPSAT NA

$$\forall \varepsilon > 0 \ \exists n_0 \in \mathbb{N} \text{ TAK, ŽE } \forall n \geq n_0 \text{ PLATÍ } (a-\varepsilon)g(n) < f(n) < (a+\varepsilon)g(n)$$

  - ZVOLÍME $\varepsilon = \frac{a}{2}$

$$\frac{a}{2} g(n) < f(n) < \frac{3a}{2} g(n) \quad \text{COŽ JE} \quad f(n) \in \Theta(g(n))$$

- PRO O, Θ, Ω PLATÍ TRANSITIVITA A REFLEXIVITA

- $f(n) \in \Theta(g(n))$ IFF $g(n) \in \Theta(f(n))$

- $\log_a(n) \in \Theta(\log_b(n))$ $\forall a > 1$ A $\forall b > 1$

- $\lg n! \in \Theta(n \lg n)$

- GAUSSOVA VĚTA

$$\forall n \geq 1 : \quad n^{\frac{n}{2}} \leq n! \leq \left(\frac{n+1}{2}\right)^n$$

- ZDŮVODNĚNÍ HORNÍHO ODHADU

- PŘEDPOKLAD

$$\frac{a+b}{2} \geq \sqrt{ab}$$

- $(n!)^2 = n(n-1) \dots 2\,1\,1\,2 \dots (n-1)n = \prod_{i=1}^{n} (n-i+1)i$

- $n! = \prod_{i=1}^{n} \sqrt{(n-i+1)i} \leq \prod_{i=1}^{n} \frac{(n-i+1)+i}{2} \leq \prod_{i=1}^{n} \frac{n+1}{2} = \left(\frac{n+1}{2}\right)^n$

- POZNÁMKA ODHAD

$$n \leq (n-i+1)\,i$$

A PROTO

$$n^n \leq (n!)^2$$

$$n^{\frac{n}{2}} \leq n!$$

- REKURZIVNÍ VZTAHY

  - MASTER THEOREM

    - DÁNA $a \geq 1$, $b > 1$, $a, b \in \mathbb{N}$ A NEZÁPORNÁ FCE $f(n)$

    - FCE $T(n)$ JE

      $$T(n) = a\,T\left(\frac{n}{b}\right) + f(n)$$

      KDE $\frac{n}{b}$ JE BUĎ $\lfloor \frac{n}{b} \rfloor$ NEBO $\lceil \frac{n}{b} \rceil$

    - 1. JESTLIŽE $f(n) \in O(n^{\log_b a - \epsilon})$ PRO $\epsilon > 0$, PAK $T(n) \in \Theta(n^{\log_b a})$

    - 2. JESTLIŽE $f(n) \in \Theta(n^{\log_b a})$ PAK $T(n) \in \Theta(n^{\log_b a} \lg n)$

    - 3. JESTLIŽE $f(n) \in \Omega(n^{\log_b a + \epsilon})$ PRO $\epsilon > 0$ A JESTLIŽE $a\,f(\frac{n}{b}) \leq c\,f(n)$ PRO $c < 1$ PRO VŠECHNA POSTATEČNĚ VELKÁ n, PAK $T(n) \in \Theta(f(n))$

  - DAJÍ SE TAKÉ ŘEŠIT POMOCÍ STROMŮ REKURZE

- AMORTIZOVANÁ SLOŽITOST

  - PRŮMĚRNÁ SLOŽITOST NEJHORŠÍHO PŘÍPADU PRO n OPAKOVÁNÍ DANÉ INSTRUKCE

  - PAKLIŽE n OPAKOVÁNÍ VYŽADUJE $O(T(n))$ PAK JEDNO VYŽADUJE $O(T(n))/n$

    - TO JE AMORTIZOVANÁ SLOŽITOST JEDNÉ INSTRUKCE

- možnosti výpočtu
  - agregační
    - zjištění $O(T(n))$ a vydělení n
      - $O(T(n))/n$
  - účetní
    - každá operace má kredit
    - nevyužitý kredit pro operaci lze použít k pro následující operace pro které by jejich kredit nestačil
    - podmínka je že nesmíme jít do zápora
- potenciálová
  - D_i je stav po provedení i-té instrukce
  - máme tedy posloupnost n stavů $D_0, \dots, D_{n-1}$
  - každé D_i je přiřazeno nezáporné číslo
    - potenciál $\phi(D_i)$
  - c_i je skutečná cena přechodu z D_{i-1} do D_i
  - Amortizovaná cena příslušná D_i je definovaná jako

$$\hat{c}_i = c_i + \phi(D_i) - \phi(D_{i-1})$$

  - pak platí

$$\sum_{i=1}^{n} \hat{c}_i = \sum_{i=1}^{n} \left(c_i + \phi(D_i) - \phi(D_{i-1})\right) = \sum_{i=1}^{n} c_i + \phi(D_n) - \phi(D_0)$$

  - podmínka na potenciály: $\phi(D_i) \geq \phi(D_0)$

- ČASOVÁ SLOŽITOST A SPRÁVNOST ALGORITMŮ

  - K OVĚŘENÍ ~~SLOŽITOSTI~~ SPRÁVNOSTI ALGORITMU JSOU TŘEBA OVĚŘIT DVĚ VĚCI

    - ALGORITMUS SE NA KÁŽDÉM VSTUPU ZASTAVÍ

    - ALGORITMUS PO ZASTAVENÍ VYDÁ SPRÁVNÝ VÝSTUP

  - VARIANT

    - K DOKÁZÁNÍ ŽE SE ALGORITMUS ZASTAVÍ

    - ~~H~~ HODNOTA ÚDAJŮ PŘIŘAZENÝCH ČÍSLEM

      - BĚHEM PRÁCE ALGORITMU SE SNIŽUJE

      - A ŽE DOJDE MINIMA A ALGORITMUS SE ZASTAVÍ

  - INVARIANT

    - PODMÍNKA SPRÁVNOSTI ALGORITMU

    - TVRZENÍ, KTERÉ

    - PLATÍ PŘED VYKONÁNÍM PRVNÍHO CYKLU ALGORITMU NEBO PO PRVNÍM VYKONÁNÍ CYKLU

    - PLATÍ-LI PŘED VYKONÁNÍM CYKLU, PAK PLATÍ I PO JEHO VYKONÁNÍ

    - PŘI UKONČENÍ ZARUČUJE SPRÁVNOST ŘEŠENÍ

- TURINGOVY STROJE
  - SKLÁDÁ SE Z
    - ŘÍDÍCÍ JEDNOTKY KTERÁ SE NACHÁZÍ V JEDNOM Z KONEČNÉ MNOHA STAVŮ
    - NEKONEČNÉ PÁSKY ROZDĚLENÉ NA POLE
    - HLAVY KTERÁ ČTE Z PÁSKY A ZAPISUJE NA NÍ
  - NA ZÁKLADĚ SYMBOLU X A STAVU q SE ŘÍDÍCÍ JEDNOTKA TURINGOVA STROJE PŘESUNE DO STAVU p, PŘEPÍŠE OBSAH ČTENÉHO POLE NA Y A POHNE SE DOPRAVA NEBO DOLEVA
  - TURINGŮV STROJ JE SEDMICE
    - $(Q, \Sigma, \Gamma, \delta, p_0, B, F)$
      - Q JE KONEČNÁ MNOŽINA STAVŮ
      - Σ JE KONEČNÁ MNOŽINA VSTUPNÍCH SYMBOLŮ
      - Γ JE MNOŽINA PÁSKOVÝCH SYMBOLŮ ($\Sigma \subset \Gamma$)
      - B JE BLANK ($B \in \Gamma \setminus \Sigma$, "JE PÁSKOVÝ ALE NE VSTUPNÍ SYMBOL")
      - δ JE PŘECHODOVÁ FCE z $(Q \setminus F) \times \Gamma$ DO $Q \times \Gamma \times \{L, R\}$
      - $q_0 \in Q$ JE POČÁTEČNÍ STAV
      - $F \subseteq Q$ JE MNOŽINA KONCOVÝCH STAVŮ
  - SITUACE (KONFIGURACE) TM
    - PLNĚ POPISUJE OBSAH PÁSKY, STAV HLAVY A POZICI HLAVY NA PÁSCE
    - $X_1 X_2 \dots X_{i-1} q X_i X_{i+1} \dots X_n$

- POČÁTEČNÍ KONFIGURACE

$q_0 a_1 \dots a_n$

- KROK TURINGOVA STROJE

- $\delta(q_i, X_j) = (p, Y, R)$

$X_1 X_2 \dots X_{i-1} q X_i X_{i+1} \dots X_k \vdash X_1 X_2 \dots X_{i-1} Y p X_{i+1} \dots X_k$

- $\delta(q_i, X_j) = (p, Y, L)$

$X_1 X_2 \dots X_{i-1} q X_i X_{i+1} \dots X_k \vdash X_1 X_2 \dots p X_{i-1} Y Y_{i+1} \dots X_k$

- JESTLIŽE $\delta(q_i, X_j)$ NENÍ DEFINOVÁNO, TM SE ZASTAVÍ

- VÝPOČET TM

- NAD SLOVEM $w = a_1 a_2 \dots a_k$

- JE POSLOUPNOST KROKŮ

- ZAČÍNÁ V POČÁTEČNÍ KONFIGURACI

$q_0 a_1 a_2 \dots a_n$

- JEDNÁ SE O REFLEXIVNÍ UZÁVĚR A TRANZITIVNÍ UZÁVĚR $\vdash^*$

- PŘÍKLAD SE TM DOSTANE DO JEDNOHO Z KONCOVÝCH STAVŮ $q \in F_i$, ŘÍKÁME ŽE SE TM ZASTAVIL ÚSPĚŠNĚ

- OBSAH PÁSKY JE POTÉ VÝSTUPEM TM NAD VSTUPEM $w = a_1 a_2 \dots a_n$

- JAZYK PŘIJÍMANÝ TM
  - VSTUPNÍ SLOVO $w \in \Sigma^*$ JE PŘIJATO TURINGOVÝM STROJEM M, JESTLIŽE SE TM NA SLOVĚ w ÚSPĚŠNĚ ZASTAVÍ
  - "NA OSTATNÍCH SLOVECH MŮŽE I BĚŽET DONEKONEČNA"
  - MNOŽINA SLOV $w \in \Sigma^*$ KTERÁ TURINGŮV STROJ PŘIJÍMÁ SE NAZÝVÁ JAZYK PŘIJÍMANÝ M
  - ZNAČÍ SE $L(M)$
- FUNKCE REALIZOVANÁ TM
  - DÁNO ZOBRAZENÍ $f: \Sigma^* \to \Sigma^*$
  - M REALIZUJE ZOBRAZENÍ f
  - JESTLIŽE PRO KAŽDÉ $w \in \Sigma^*$ PRO KTERÉ JE $f(w)$ DEFINOVÁNO SE M ÚSPĚŠNĚ ZASTAVÍ S VÝSTUPEM $f(w)$
    - $q_0 w \vdash^* \alpha q_F \beta$ KDE $f(w) = \alpha\beta$
  - PRO w PRO KTERÁ NENÍ $f(w)$ DEFINOVÁNO SE M ZASTAVÍ NEÚSPĚŠNĚ
- ČASOVÁ SLOŽITOST TM
  - $T(n)$,
  - NENÍ DEFINOVANÁ, PAKLIŽE SE PRO NĚJAKÝ VSTUP DÉLKY n TURINGŮV STROJ NEZASTAVÍ
  - MAXIMÁLNÍ POČET KROKŮ PO NICHŽ DOJDE K ZASTAVENÍ TM
    - MAXIMUM SE BERE PŘES VŠECHNY VSTUPY DÉLKY n
- PAMĚŤOVÁ SLOŽITOST TM
  - $S(n)$
  - PAKLIŽE TM POUŽIJE PRO NĚJAKÝ VSTUP DÉLKY n NEKONEČNÉ MNOŽSTVÍ POLÍ NA PÁSCE, PAK NENÍ $S(n)$ DEFINOVÁNO
    - ANI SE NEMŮŽE V TOMTO PŘÍPADĚ ZASTAVIT
  - MAXIMÁLNÍ ROZDÍL POŘADOVÝCH ČÍSEL POLÍ, KTERÁ BYLY BĚHEM VÝPOČTU POUŽITY
    MAXIMUM SE BERE PŘES VŠECHNY VSTUPY DÉLKY n

- JAZYK L JE PŘIJÍMÁN NĚJAKÝM TM, JESTLIŽE EXISTUJE TM M TAKOVÁ, ŽE $L = L(M)$

- TM ROZHODUJE JAZYK L, JESTLIŽE TENTO JAZYK PŘIJÍMÁ A NAVÍC SE NA KAŽDÉM VSTUPU ZASTAVÍ

- ~~ÚSPORA~~

- EXISTUJE VÍCE TYPŮ TM
  - S NEKONEČNOU PÁSKOU NA JEDNA STRANU
  - ULOŽENÍ SE NEPOHNOUT
    - $(Q \setminus F) \times \Gamma$ DO $Q \times \Gamma \times \{R, L, S\}$ (+ STOP)
  - VŠECHNY TYPY JSOU EQUIVALENTNÍ A DÁ SE MEZI NIMI PŘEVÁDĚT

- TURINGŮV STROJ S k-PÁSKAMI
  - ŘÍDÍCÍ JEDNOTKA V JEDNOM Z KONEČNĚ MNOŽINY STAVŮ
  - k-HLAV ČTOUCÍ PÁSEK A ZAPISUJÍCÍ NA NĚ
  - k-NEKONEČNÝCH PÁSEK
  - Q ... MNOŽINA STAVŮ
  - Σ ... MNOŽINA VSTUPNÍCH SYMBOLŮ
  - Γ ... MNOŽINA PÁSKOVÝCH SYMBOLŮ
  - δ ... PŘECHODOVÁ FCE $\delta: (Q \setminus F) \times \Gamma^k \to Q \times \Gamma^k \times \{L, R\}^k$
  - q_0 ... POČÁTEČNÍ STAV
  - B ... BLANK
  - F ... MNOŽINA KONCOVÝCH STAVŮ

- VSTUPNÍ SLOVO JE NA PRVNÍ PÁSCE
- OSTATNÍ PÁSKY MAJÍ VŠUDE B
- ŘÍDÍCÍ JEDNOTKA JE V q_0
- PRVNÍ HLAVA ČTE PRVNÍ SYMBOL VSTUPNÍHO SLOVA

- JAZYK PŘIJÍMANÝ TM S k - PÁSKAMI
  - MNOŽINA VŠECH SLOV w NA KTERÝCH SE TM ÚSPĚŠNĚ ZASTAVÍ

- JAZYK ROZHODOVANÝ TM S k - PÁSKAMI
  - JAZYK KTERÝ JE PŘIJÍMANÝ PLUS TM SE NA VŠECH VSTUPECH ZASTAVÍ

- KE KAŽDÉMU TM S k PÁSKAMI MŮŽEME SESTROJIT TM S JEDNOU PÁSKOU KTERÁ MÁ STEJNÉ CHOVÁNÍ
  - JESTLIŽE k - PÁSKOVÁ TM POTŘEBOVAL K ÚSPĚŠNÉMU ZASTAVENÍ n KROKŮ 1 - PÁSKOVÁ POTŘEBUJE $O(n^2)$ KROKŮ

- NEDETERMINISTICKÝ TURINGŮV STROJ
  - MŮŽE V JEDNÉ SITUACI PROVÉST NĚKOLIK RŮZNÝCH KROKŮ
  - SEDMICE $(Q, \Sigma, \Gamma, \delta, q_0, B, F)$
    - Q JE KONEČNÁ MNOŽINA STAVŮ
    - Σ JE KONEČNÁ MNOŽINA VSTUPNÍCH SYMBOLŮ
    - Γ JE KONEČNÁ MNOŽINA PÁSKOVÝCH SYMBOLŮ
      - $\Sigma \subset \Gamma$
    - B JE BLANK
      - NENÍ VSTUPNÍ SYMBOL $(B \in \Gamma \setminus \Sigma)$
    - δ JE PŘECHODOVÁ FCE
      - $(Q \setminus F) \times \Gamma$ DO $P_\beta(Q \times \Gamma \times \{L, R\})$
        - KDE $P_\beta(X)$ JE KONEČNÁ PODMNOŽINA MNOŽINY X
    - $q_0 \in Q$ JE POČÁTEČNÍ STAV
    - $F \subseteq Q$ JE MNOŽINA ~~POČÁTEČNÍCH~~ KONCOVÝCH STAVŮ
- KROK JE IDENTICKÝ JAKO V PŘÍPADĚ DETERMINISTICKÉHO TM

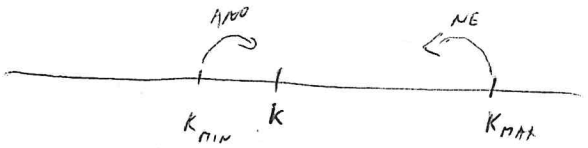
- JAZYK PŘIJÍMANÝ NTM
  - MNOŽINA VŠECH SLOV $w \in \Sigma^*$ PRO KTERÁ
    $q_0 w \vdash^* Y_1 Y_2 \dots Y_i q_F Y_{i+1} \dots Z_m$ PRO NĚJAKÝ KONCOVÝ STAV q_F.
  - "SLOVO w JE PŘIJATO, PAKLIŽE EXISTUJE "PŘIJÍMACÍ VÝPOČET" PO NĚMŽ SE STROJ DOSTANE DO KONCOVÉHO STAVU."
  - PAKLIŽE NTM JAZYK L PŘIJÍMÁ A JEŠTĚ SE NAD KAŽDÝM VSTUPEM ZASTAVÍ, PAK JAZYK L I ROZHODUJE
- JE-LI JAZYK L PŘIJÍMÁN/ROZHODOVÁN NTM, PAK EXISTUJE DETERMINISTICKÝ TM S JEDNOU PÁSKOU KTERÝ L PŘIJÍMÁ/ROZHODUJE.

- POČÍTAČ S LIBOVOLNÝM PŘÍSTUPEM (RAM)
  - COKOLIV CO LZE PŘIJMOUT / REALIZOVAT POMOCÍ TM LZE "SPOČÍTAT" POČÍTAČEM S LIBOVOLNÝM PŘÍSTUPEM. RAM POTŘEBUJE $O(n^2)$, PAKLIŽE TM n
  - SKLÁDÁ SE Z
    - PROGRAMOVÁ JEDNOTKA
      - OBSAHUJE PROGRAMOVÝ REGISTR A VLASTNÍ PROGRAM
        - REGISTR UKAZUJE NA INSTRUKCI CO MÁ BÝT PROVEDENA
    - ARITMETICKÁ JEDNOTKA
      - PROVÁDÍ SČÍTÁNÍ, ODČÍTÁNÍ, NÁSOBENÍ A CELOČÍSELNÉ DĚLENÍ
    - PAMĚŤ
      - ROZDĚLENA NA PAMĚŤOVÉ BUŇKY
      - BUŇKA MŮŽE OBSAHOVAT CELÉ ČÍSLO
      - POŘADOVÉ ČÍSLO BUŇKY JE ADRESA
      - VELIKOST ČÍSEL I POČET BUNĚK JE NEOMEZENÉ
    - VSTUPNÍ JEDNOTKA
      - TVOŘENA VSTUPNÍ PÁSKOU A HLAVOU
      - VSTUPNÍ PÁSKA JE DĚLENA NA POLE
      - HLAVA SNÍMÁ V KAŽDÉM OKAMŽIKU JEDNO POLE
      - PO PŘEČTENÍ SE HLAVA POSUNE O JEDNO POLE VPRAVO
    - VÝSTUPNÍ JEDNOTKA
      - TVOŘENA VÝSTUPNÍ PÁSKOU A HLAVOU
      - VÝSTUPNÍ HLAVA ZAPÍŠE NA PÁSKU A POSUNE SE O POLE DOPRAVA
  - PRO KAŽDÝ PROGRAM P PRO RAM EXISTUJE 5-TI PÁSKOVÝ TM $\$$ TAKOVÝ, ŽE OBA MAJÍ STEJNÉ CHOVÁNÍ

- TŘÍDY SLOŽITOSTI
  - ROZHODOVACÍ ÚLOHY
    - ODPOVĚĎ JE ANO NEBO NE
    - SAT
      - SPLNOVÁNÍ BOOLEOVSKÝCH FORMULÍ
      - JE DÁNA Ψ V CNF
        - ROZHODNĚTE ZDA JE SPLNITELNÁ
          - NEZAJÍMÁ NÁS JEJÍ OHODNOCENÍ
    - ~~TSP~~
      - ~~TRADIČNÍ SAVE SMAN PROBLÉM~~
    - MINIMÁLNÍ KOSTRA
      - DÁN NEORIENTOVANÝ GRAF $G=(V,E)$ A OHODNOCENÍ $c: E \to N$
      - DÁNO ČÍSLO K
      - EXISTUJE ~~KOSTRA~~ MINIMÁLNÍ KOSTRA JEJÍŽ CENA JE NEJVÝŠE K?
    - CESTY
      - ~~DÁN~~ DÁNA MATICE DÉLEK $A=(a(i,j))$
      - DÁN CÍLOVÝ VRCHOL c, VÝCHOZÍ VRCHOL v A ČÍSLO K
      - EXISTUJE CESTA Z v DO c DÉLKY NEJVÝŠE K?
    - TSP
      - EXISTUJE TRASA DÉLKY NEJVÝŠE K?
- VYHODNOCOVACÍ VERZE
  - HLEDÁME CENU OPTIMÁLNÍHO ŘEŠENÍ
    - ALE CO JE TO OPTIMÁLNÍ ŘEŠENÍ NÁS NEZAJÍMÁ
  - MINIMÁLNÍ KOSTRA
    - NAJDĚTE JEJÍ CENU
  - CESTY
    - NAJDĚTE DÉLKU NEJKRATŠÍ CESTY MEZI v A c
  - TSP
    - NAJDĚTE CENU OPTIMÁLNÍ TRASY

- OPTIMALIZAČNÍ VERZE
  - ZAJÍMÁ NÁS OPTIMÁLNÍ ŘEŠENÍ
  - MINIMÁLNÍ KOSTRA
    - NAJDĚTE MINIMÁLNÍ KOSTRU GRAFU
  - CESTY NEJKRATŠÍ
    - NAJDĚTE ~~NEJKRATŠÍ~~ CESTU MEZI r A c
  - TSP
    - NAJDĚTE OPTIMÁLNÍ TRASU

- PAKLIŽE JDE JEDNU VERZE ŘEŠIT POLYNOMIÁLNĚ, PAK JDOU ŘEŠIT POLYNOMIÁLNĚ I OSTATNÍ
  - DŮKAZ NA TSP
    - MÁME ALGORITMUS PRO ROZHODOVACÍ ÚLOHU
      - PŘEVOD NA VYHODNOCOVACÍ ÚLOHU
        - BINÁRNÍM PŮLENÍM HLEDÁME CENU



        - AŽ ZMENŠÍME INTERVAL NA 0, TO JE HODNOTA OPTIMÁLNÍ TRASY
        - POTŘEBOVALI JSME $O(\ln(n))$ VOLÁNÍ PŮVODNÍHO ALG.
      - PŘEVOD NA VYHODNOCOVACÍ ÚLOHU
        - Z MINULÉHO PŘEVODU ZNÁME OPTIMÁLNÍ CENU K
        - POSTUPNĚ KAŽDOU HRANU ZDRAŽÍME A ZAVOLÁME ~~PŮVODNÍ~~ ALGORITMUS PRO ROZHODOVACÍ ÚLOHU A CENU K
          - PAKLIŽE VRÁTÍ ANO
            - HRANA V TSP NELEŽÍ
          - PAKLIŽE VRÁTÍ NE
            - HRANA V TSP LEŽÍ
        - POTŘEBOVALI JSME $O(n^2)$ VOLÁNÍ

- TŘÍDY P A NP
  - INSTANCI LIBOVOLNÉ ROZHODOVACÍ ÚLOHY MŮŽEME ZAKÓDOVAT JAKO SLOVA NAD VHODNOU ABECEDOU
  - ÚLOHA JAKO JAZYK NAD ABECEDOU
    - ROZDĚLÍME INSTANCE ÚLOH NA ANO A NE INSTANCE
    - JAZYK ÚLOHY U (L_U) SE SKLÁDÁ ZE VŠECH ANO INSTANCÍ ÚLOHY U
    - NĚKTERÁ SLOVA NAD DANOU ABECEDOU Σ NEMUSÍ ODPOVÍDAT ŽÁDNÉ INSTANCI DANÉ ÚLOHY
      - TYTO SLOVA CHÁPEME JAKO NE-INSTANCE
      - TUDÍŽ NE INSTANCE TVOŘÍ DOPLNĚK JAZYKA L_w
        - $\Sigma^* \setminus L_w$
  - TŘÍDA P
    - ROZHODOVACÍ ÚLOHA LEŽÍ VE TŘÍDĚ P
    - JESTLIŽE EXISTUJE DETERMINISTICKÝ TURINGŮV STROJ
    - KTERÝ ROZHODNE JAZYK L_U
    - A PRACUJE V POLYNOMIÁLNÍM ČASE
      - $T(n) \in O(P(n))$ KDE P JE NĚJAKÝ POLYNOM
  - TŘÍDA NP
    - ROZHODOVACÍ ÚLOHA LEŽÍ VE TŘÍDĚ NP
    - JESTLIŽE EXISTUJE NEDETERMINISTICKÝ TURINGŮV STROJ
    - KTERÝ ROZHODNE JAZYK L_w
    - A PRACUJE V POLYNOMIÁLNÍM ČASE

- NEDETERMINISTICKÝ ALGORITMUS
  - MÁ DVĚ FÁZE
    - ALGORITMUS NÁHODNĚ VYGENERUJE ŘETĚZEC S
      - ODPOVÍDÁ ŘEŠENÍ DANÉ ÚLOHY
    - DETERMINISTICKÝ ALGORITMUS (TM, RAM) NA ZÁKLADĚ VSTUPU A ŘETĚZCE DÁ ODPOVĚĎ ANO NEBO NEVÍM
      - DETERMINISTICKY A POLYNOMIÁLNĚ OVĚŘÍ ŘEŠENÍ
  - NEDETERMINISTICKÝ ALGORITMUS ŘEŠÍ ÚLOHU U JESTLIŽE
    - PRO KAŽDOU ANO INSTANCI U EXISTUJE ŘETĚZEC S, NA JEHOŽ ZÁKLADĚ DÁ ALGORITMUS ODPOVĚĎ ANO
    - A ZÁROVEŇ PRO ŽÁDNOU NE INSTANCI U NEEXISTUJE ŘETĚZEC S NA JEHOŽ ZÁKLADĚ DÁ ALGORITMUS ODPOVĚĎ ANO
  - PRACUJE V ČASE $O(T(n))$ JESTLIŽE PRŮCHOD FÁZÍ 1 I FÁZÍ 2 PRO INSTANCI VELIKOSTI n POTŘEBUJE $O(T(n))$ KROKŮ
  - NEDETERMINISTICKÝ ALGORITMUS SE DÁ POUŽÍT V DEFINICI NP

- TŘÍDA NPC
  - REDUKCE ÚLOH
    - DÁNY DVĚ ROZHODOVACÍ ÚLOHY U A V
    - U SE REDUKUJE NA V
      - PAKLIŽE EXISTUJE ALGORITMUS, KTERÝ PRO KAŽDOU INSTANCI I ÚLOHY U ZKONSTRUUJE INSTANCI I' ÚLOHY V TAK ŽE
        - I JE ANO INSTANCE U IFF I' JE ANO INSTANCE V
      - ZNAČÍME $U \Delta V$
      - "U NENÍ OBTÍŽNĚJŠÍ NEŽ V."
  - POLYNOMIÁLNÍ REDUKCE
    - PAKLIŽE PŘEVODNÍ ALGORITMUS PRACUJE V POLYNOMIÁLNÍM ČASE
    - $U \Delta_P V$

- TRANSITIVITA
  - PAKLIŽE $U \leq_p V$ A $V \leq_p W$, PAK $U \leq_p W$

- NPC ÚLOHY
  - NP-ÚPLNÉ
  - JESTLIŽE
    - 1. U JE V TŘÍDĚ NP
    - 2. KAŽDÁ NP SE POLINOMIÁLNĚ REDUKUJE NA U
  - "TY NEJTĚŽŠÍ MEZI NP ÚLOHAMI"
- JSOU DÁNY DVĚ NP ÚLOHY U A V PRO KTERÉ PLATÍ $U \leq_p V$
  - PAKLIŽE $U \in P$ PAK $V \in P$
  - PAKLIŽE $U \in NPC$ PAK $V \in NPC$
- PAKLIŽE BY NĚKTERÁ NPC ÚLOHA PATŘILA DO P
  - PAK $P = NP$
  - "KAŽDÁ NP ÚLOHA BY BYLA POLYNOMIÁLNĚ ŘEŠITELNÁ"
- COOKOVA VĚTA
  - SAT JE NPC
  - DŮKAZ
    - MYŠLENKA
      - PRVNÍ FÁZE NEDETERMINISTICKÉHO ALGORITMU VYGENERUJE OHODNOCENÍ LOGICKÝCH PROMĚNNÝCH
      - NA ZÁKLADĚ TOHOTO OHODNOCENÍ MŮŽEME MŮŽEME V POLYNOMIÁLNÍM ČASE OVĚŘIT, ZDA JE V TOMTO OHODNOCENÍ FORMULE PRAVDIVÁ NEBO NE

- POPIS PRÁCE TM POMOCÍ FORMULÍ VÝROKOVÉ LOGIKY

  - DÁN TM M S $M, Q, \Sigma, \Gamma, \delta, \varphi_0, A, q_8$.

  - PŘEDPOKLÁDEJME, ŽE M PŘIJÍMÁ SLOVO W A POTŘEBUJE $P(n)$ KROKŮ

  - ZAVEDEME LOGICKÉ PROMĚNNÉ

    - $R_{i,j}$ ... $i = 0, 1 \dots P(n)$
      ... $j = 0, 1 \dots P(n)$

      - HLAVA ČTE V ČASE i j-TÉ POLE PÁSKY

    - S_i^q ... $i = 0, 1 \dots P(n)$
      ... $q \in Q$

      - M JE V ČASE i VE STAVU q

    - $t_{i,j}^A$ ... $i = 0, 1, \dots P(n)$
      ... $j = 1, 2 \dots P(n)$
      ... $A \in \Gamma$
      - V ČASE i JE NA j-TÉM POLI PÁSKY SYMBOL A

- MUSÍME POMOCÍ FORMULÍ VYJÁDŘIT

  - 1. V KAŽDÉM OKAMŽIKU JE TM V PRÁVĚ JEDNOM STAVU

    - V OKAMŽIKU i JE TM V ALESPOŇ JEDNOM STAVU

      $$\bigvee_{q \in Q} S_i^q$$

    - V OKAMŽIKU i NENÍ TM V DVOU(CH) RŮZNÝCH STAVECH

      $$\bigwedge_{q \neq q'} (\neg S_i^q \vee \neg S_i^{q'})$$

    - KONJUNKCE OBOUCH PŘEDCHOZÍCH

      $$\left(\bigvee_{q \in Q} S_i^q\right) \wedge \left(\bigwedge_{q \neq q'} (\neg S_i^q \vee \neg S_i^{q'})\right)$$

- 2. V KAŽDÉM OKAMŽIKU ČTE HLAVA PRÁVĚ JEDNO POLE VSTUPNÍ PÁSKY

  - V OKAMŽIKU i ČTE HLAVA ALESPOŇ JEDNO POLE

$$\bigvee_{1 \le j \le p(n)} h_{i,j}$$

  - V OKAMŽIKU i NEČTE HLAVA TURINGOVA STROJE DVĚ RŮZNÁ POLE

$$\bigwedge_{j \neq k} (\neg h_{i,j} \vee \neg h_{i,k})$$

  - KONJUNKCE

$$\left(\bigvee_{1 \le j \le p(n)} h_{i,j} \right) \wedge \left(\bigwedge_{j \neq k} (\neg h_{i,j} \vee \neg h_{i,k}) \right)$$

- 3. V KAŽDÉM OKAMŽIKU JE NA KAŽDÉM POLI PÁSKY PRÁVĚ JEDEN PÁSKOVÝ SYMBOL

  - V OKAMŽIKU i JE V j-TÉM POLI PÁSKY ALESPOŇ JEDEN PÁSKOVÝ SYMBOL

$$\bigvee_{A \in \Gamma} t^{A}_{i,j}$$

  - V OKAMŽIKU i [illegible], V j-TÉM POLI PÁSKY NEJSOU DVA SYMBOLY

$$\bigwedge_{A \neq A'} (\neg t^{A}_{i,j} \vee \neg t^{A'}_{i,j})$$

  - KONJUNKCE

$$\left(\bigvee_{A \in \Gamma} t^{A}_{i,j} \right) \wedge \left(\bigwedge_{A \neq A'} (\neg t^{A}_{i,j} \vee \neg t^{A'}_{i,j}) \right)$$

– 4. NA ZAČÁTKU PRÁCE JE TM VE STAVU q_0, HLAVA ČTE PRVNÍ POLE PÁSKY A NA PÁSCE JE VSTUPNÍ SLOVO, OSTATNÍ POLE JSOU BLANK

$$S_0^{q_0} \wedge h_{0,1} \wedge t_{0,1}^{a_1} \wedge \dots \wedge t_{0,n}^{a_n} \wedge t_{0,n+1}^{B} \wedge \dots \wedge t_{0,p(n)}^{B}$$

– 5. KROK TURINGOVA STROJE JE DÁN PŘECHODOVOU FCÍ $\delta(q,A) = (p, C, D)$ ($D=1$ JE POSUN VPRAVO, $D=-1$ JE POSUN VLEVO)

$$\bigwedge_i \bigwedge_{A \in \Gamma} \left((S_i^q \wedge h_{i,j} \wedge t_{i,j}^A) \Rightarrow \bigvee (S_{i+1}^p \wedge t_{i+1,j}^C \wedge h_{i+1,j+D}) \right)$$

– 6. V POLÍCH KTERÁ NEČTE HLAVA SE OBSAH PŘESOUVÁ Z i DO $i+1$

$$\bigwedge_i \bigwedge_{A \in \Gamma} \left((\neg h_{i,j} \wedge t_{i,j}^A) \Rightarrow t_{i+1,j}^A \right)$$

– 7. NA KONCI PRÁCE JE TM VE STAVU q_f

$$S_{p(n)}^{q_f}$$

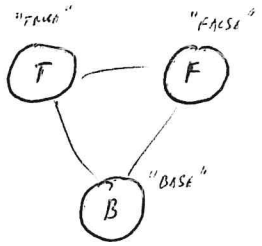
– VÝSLEDNOU FORMULI ZÍSKÁME JAKO KONJUNKCI VŠECH DÍLČÍCH FORMULÍ PRO VŠECHNY ČASOVÉ OKAMŽIKY $i = 0 \dots p(n)$

- 3-CNF SAT
  - DÁNA FORMULE φ V KONJUNKTIVNÍ NORMÁLNÍ FORMĚ
  - KAŽDÁ KLAUZULE MÁ 3 LITERÁLY
  - PAKLIŽE DOKÁŽEME POLYNOMIÁLNĚ ZREDUKOVAT SAT NA 3-CNF SAT, PAK DOKÁŽEME, ŽE 3-CNF SAT JE NP-C
    - PŘEVOD
      - DÁNA FORMULE φ V KONJUNKTIVNÍ NORMÁLNÍ FORMĚ
      - ZKONSTRUUJEME ψ
        - KTERÁ JE V CNF A KAŽDÁ KLAUZULE MÁ MAX. 3 LITERÁLY
        - JE SPLNITELNÁ IFF φ JE SPLNITELNÁ
        - OZNAČÍME $C_1, \dots C_m$ VŠECHNY KLAUZULE V φ
          - PRO KAŽDOU C_i KTERÁ OBSAHUJE VÍCE NEŽ 3 LITERÁLY SESTROJÍME NOVOU FORMULI ψ_C

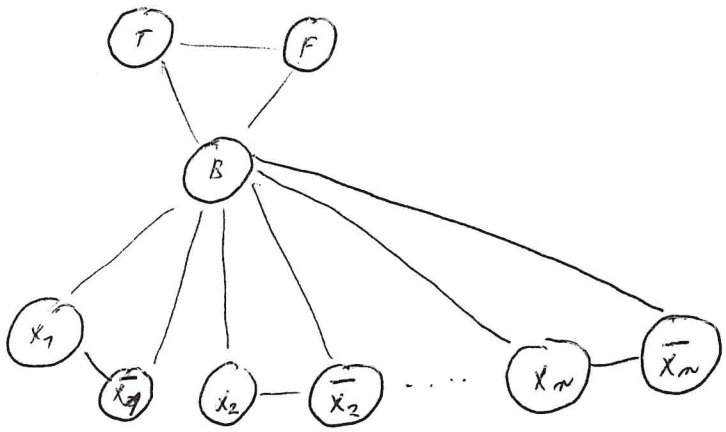
$$\psi_C = (l_1 \vee l_2 \vee x_1) \wedge (\neg x_1 \vee l_3 \vee x_2) \wedge (\neg x_2 \vee l_4 \vee x_3) \wedge \dots \wedge (\neg x_{s-3} \vee l_{s-1} \vee l_s)$$

        - PŘIDÁNÍ NOVÉ x_i
      - VÝSLEDKEM FORMULE 3-CNF POSTUPNÉ KONJUNKCÍ VŠECH $|C_k| \leq 3$ A ψ_C.
      - DŮKAZ POLYNOMIÁLNOSTI PŘEVODU
        - φ MÁ k KLAUZULÍ S MAX s LITERÁLY
          - PAK JSME PŘIDALI MAX $(s-3)k$ NOVÝCH PROMĚNNÝCH
          - PŘIDALI JSME MAX $2(s-3)k$ LITERÁLŮ (KAŽDÁ NOVÁ PROMĚNNÁ SE OBJEVUJE PŘESNĚ DVAKRÁT)
          - TEDY DÉLKA ψ SE PRODLOUŽILA MAX. POLYNOMIÁLNĚ OPROTI φ

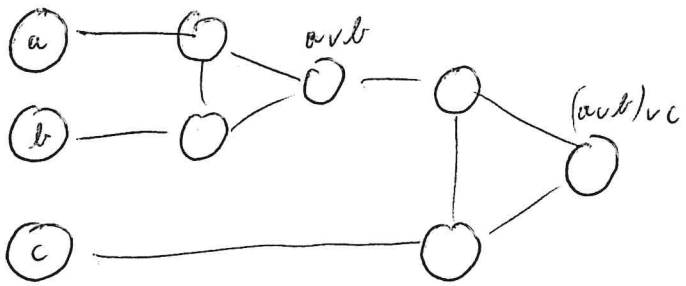
- OBARVENÍ VRCHOLŮ GRAFU (k - BAREVNOST)
  - DÁN GRAF G BEZ SMYČEK A k
  - JE GRAF k BAREVNÝ?
  - 3-CNF SAT $\leq_p$ 3-BAREVNOST
  - DŮKAZ
    - DÁNA FORMULE φ KTERÁ JE 3-CNF
    - MUSÍME SESTROJIT GRAF G TAKOVÝ, ŽE φ JE SPLNITELNÁ TEHDY, KDYŽ JE G 3-BAREVNÝ
    - 1. VYTVOŘENÍ TROJÚHELNÍKU



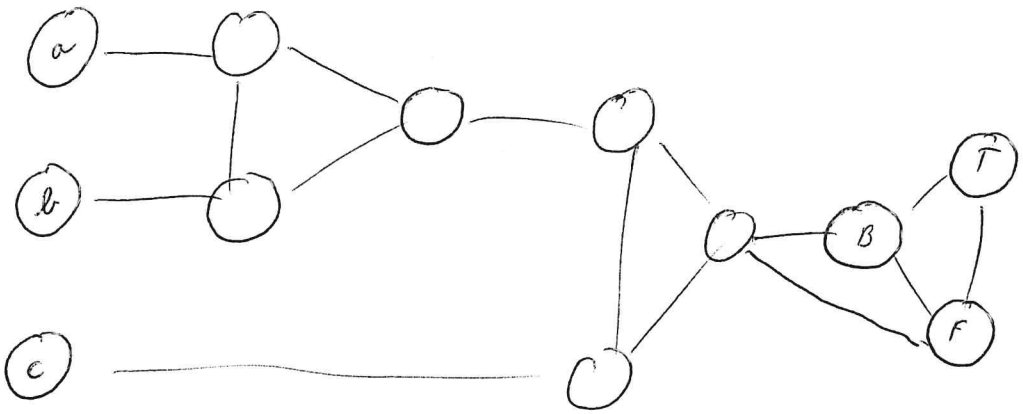
    - 2. NAPOJENÍ KAŽDÉHO LITERÁLU NA B



    - 3. VYTVOŘ OR-GADGET PRO KAŽDÉ C (VYUŽIJ MODY Z MINULÉHO KVÍZU)

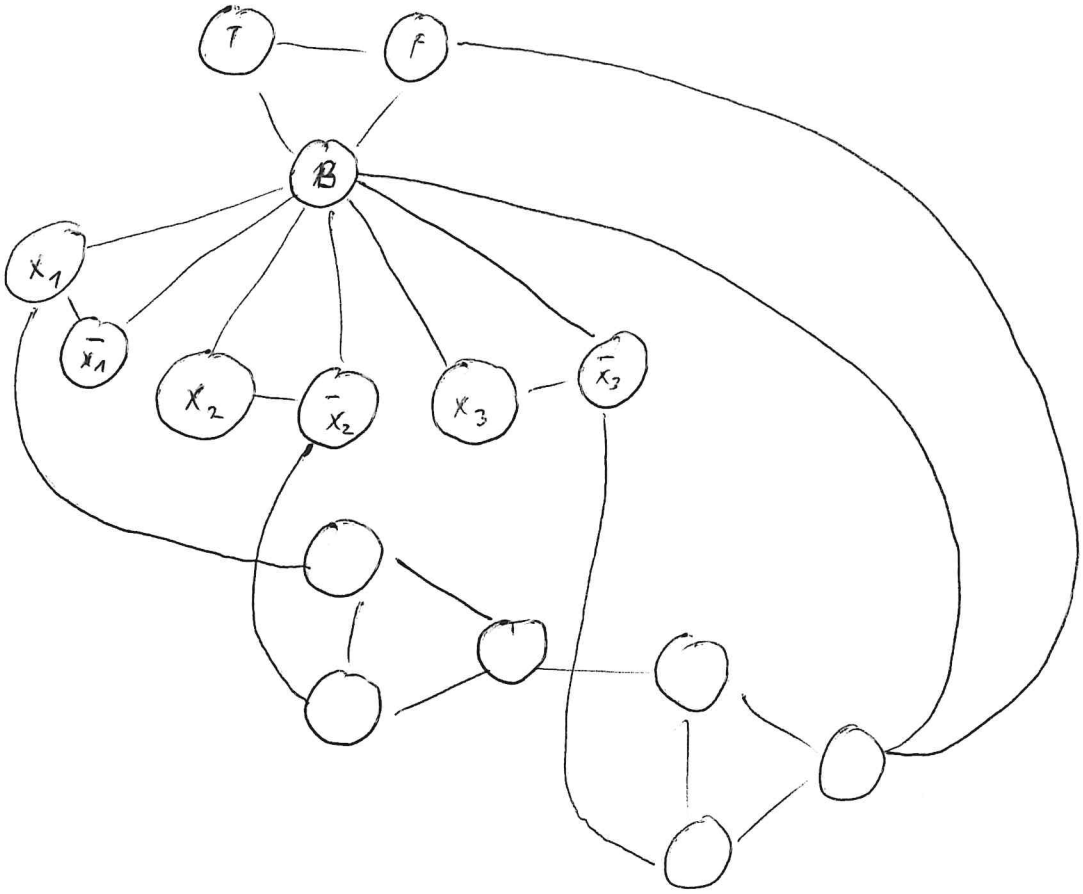


- 4. NÁPOJ OR-GADGETY NA B A F



- UKÁŽKA

$(x_1 \vee \neg x_2 \vee x_3)$



- ILP

- 3-BARVENOST Δ_P ILP

  - DÁN GRAF G

  - ZKONSTRUUJEME INSTANCI ILP KTERÁ MÁ ŘEŠENÍ PRÁVĚ TEHDY KDYŽ G JE 3-BARVITELNÝ

  - POUŽIJEME 0-1 ILP (PROMĚNNÉ NABÝVAJÍ POUZE HODNOT 0 A 1)

  - ZAVEDEME PRO KAŽDÝ VRCHOL TŘI PROMĚNNÉ REPREZENTUJÍCÍ BARVU

    x_v^c, x_v^m, x_v^z

  - VYTVOŘÍME ROVNICE

    - KAŽDÝ VRCHOL MÁ PRÁVĚ JEDNU BARVU

      $x_v^c + x_v^m + x_v^z = 1$

    - PRO KAŽDOU HRANU $e = \{i, j\}$ ZAVEDEME ROVNICE ZAJIŠŤUJÍCÍ STEJNÉ BARVY i A j

      $x_i^c + x_j^c \leq 1$

      $x_i^m + x_j^m \leq 1$

      $x_i^z + x_j^z \leq 1$

  - INSTANCE ILP MÁ $3|V|$ PROMĚNNÝCH A $|V| + 3|E|$ ROVNIC

    TUDÍŽ PŘEVOD JE POLYNOMIÁLNÍ

- PROBLÉM ROZKLADU

  - 3-BARVITELNOST $\leq_p$ PROBLÉM ROZKLADU

  - DÁN GRAF G

  - ZKONSTRUUJEME MNOŽINU X A SYSTÉM JEJÍCH PODMNOŽIN S TAK, ŽE GRAF G JE TŘÍBARVITELNÝ PRÁVĚ TEHDY KDYŽ ZE SYSTÉMU S LZE VYTVOŘIT ROZKLAD MNOŽINY X

  - MNOŽINA X:

    - PRO KAŽDÝ VRCHOL $v \in V$ DÁME DO MNOŽINY X PRVKY:

      - v, p_v^c, p_v^m, p_v^z

    - PRO KAŽDOU HRANU $e = \{u, v\}$ DÁME DO MNOŽINY X PRVKY

      - $q_{uv}^c, q_{uv}^m, q_{uv}^z, q_{vu}^c, q_{vu}^m, q_{vu}^z$

    - MNOŽINA MÁ $4|V| + 6|E|$ PRVKŮ

  - SYSTÉM PODMNOŽIN S TVOŘÍ TYTO MNOŽINY

    - PRO KAŽDÝ VRCHOL

      $\{v, p_v^c\}, \{v, p_v^m\}, \{v, p_v^z\}$

    - PRO KAŽDÝ VRCHOL v OZNAČÍME $N(v)$ MNOŽINU VŠECH JEHO SOUSEDŮ. DO S PŘIDÁME MNOŽINY

      $S_v^c = \{p_v^c, q_{vu}^c \mid u \in N(v)\}$

      $S_v^m = \{p_v^m, q_{vu}^m \mid u \in N(v)\}$

      $S_v^z = \{p_v^z, q_{vu}^z \mid u \in N(v)\}$

    - PRO KAŽDOU HRANU $e = \{u, v\}$ PŘIDÁME DO S

      $\{q_{uv}^c, q_{uv}^m\}$ $\{q_{uv}^c, q_{uv}^z\}$ $\{q_{uv}^m, q_{uv}^c\}$ $\{q_{uv}^m, q_{uv}^z\}$

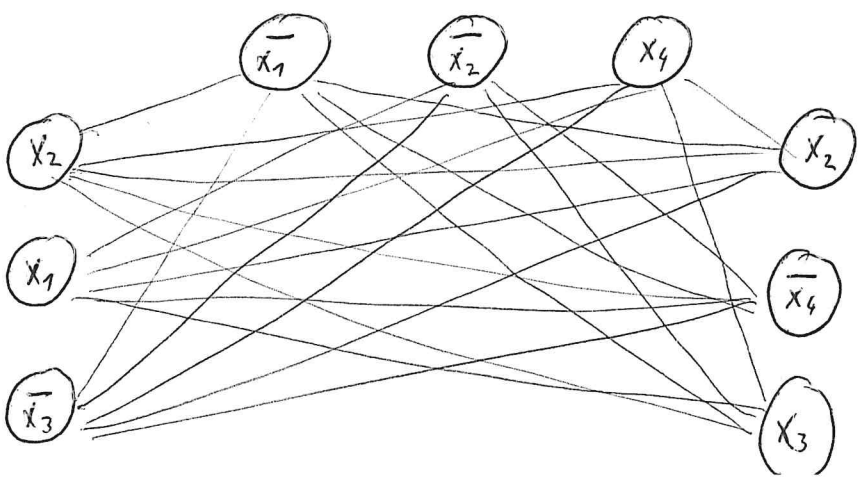
      $\{q_{uv}^z, q_{uv}^c\}$ $\{q_{uv}^z, q_{uv}^m\}$

    - S MÁ $3|V| + 3|V| + 6|E|$ MNOŽIN

- A SE SKLÁDÁ Z ($b(v)$ JE BARVA VRCHOLU v)
  - $\{v, p_v^{b(v)}\}$ $\forall v \in V$
  - $S_v^{b_1}$ A $S_v^{b_2}$ KDE b_1 A b_2 JSOU ZBYLÉ DVĚ BARVY KTERÉ NEPOUŽÍVÁ VRCHOL v
  - $\{q_{uv}^{b(u)}, q_{vu}^{b(v)}\}$ $\forall e = \{u, v\}$
- JESTLIŽE EXISTUJE ROZKLAD $A \subseteq S$ MNOŽINY X, PAK SESTROJÍME OBARVENÍ GRAFU G TAKTO

$$b(v) = b, \; b \in \{c, m, z\} \text{ IFF } \{v, p_v^b\} \in A$$

- PROBLÉM KLIK
  - EXISTUJE V GRAFU KLIKA ALESPOŇ O k VRCHOLECH?
  - 3-CNF SAT $\leq_p$ PROBLÉM KLIK
    - PRO KAŽDOU KLAUZULI VYTVOŘÍME V GRAFU STRANU ~~A PROCEDÍME~~
    - KAŽDÁ STRANA SE SKLÁDÁ Z VRCHOLŮ ODPOVÍDAJÍCÍ LITERÁLŮM ODPOVÍDAJÍCÍ KLAUZULE
    - PROPOJÍME HRANAMI NEKOMPLEMENTÁRNÍ LITERÁLY ZE VŠECH STRAN
      - $(x_2 \vee x_1 \vee \bar{x}_3) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_4) \wedge (x_2 \vee \bar{x}_4 \vee x_3)$



- PAKLIŽE SE V GRAFU NACHÁZÍ KLIKA O
  2 VRCHOLECH, PAK JEDEN VRCHOL V KAŽDÉ
  STAVBĚ MUSÍ BÝT PRAVDIVÝ

- HEURISTIKY
  - PRO VELKÉ NP INSTANCE PROBLÉMŮ
  - POMŮŽE NAJÍT DOSTATEČNĚ DOBRÉ ČI PŘESNÉ ŘEŠENÍ
  - PRACUJE V POLYNOMIÁLNÍM ČASE
  - TAKÉ SE MŮŽEME SETKAT S APROXIMAČNÍ ALGORITMY
  - DEFINICE APROXIMAČNÍHO ALGORITMU
    - UVAŽUJME OPTIMALIZAČNÍ PROBLÉM U
    - POLYNOMIÁLNÍ ALGORITMUS A JE R-APROXIMAČNÍ
    - PAKLIŽE EXISTUJE REÁLNÉ ČÍSLO R TAKOVÉ
    - ŽE ALGORITMUS NAJDE PRO KAŽDOU INSTANCI PROBLÉMU
      ŘEŠENÍ NE HORŠÍ NEŽ R-KRÁT HODNOTA OPTIMÁLNÍHO
      ŘEŠENÍ
  - NE PRO VŠECHNY NP ÚLOHY EXISTUJE R-APROXIMAČNÍ ALGORITMUS
    - TO JE PŘÍKLAD OBECNÉHO TSP
      - PAKLIŽE BYCHOM BYLI TOHO SCHOPNI, PAK BYCHOM POLINOMIÁLNĚ
        DOKÁZALI VYŘEŠIT EXISTENCI HAMILTONOVSKÉ KRUŽNICE V
        POLYNOMIÁLNÍM ČASE A PAK BY P=NP
    - ALE PRO TSP SPLŇUJÍCÍ TROJÚHELNÍKOVOU NEROVNOST

      $$d(i,j) \leq d(i,k) + d(k,j)$$

      EXISTUJE
      - 2-APROX.
        - S KOSTROU
      - CHRISTOPHIDESŮV ALGORITMUS
        - $\frac{3}{2}$-APROX

- TŘÍDA CO-NP
  - JE-LI JAZYK L VE TŘÍDĚ P, PAK JEHO DOPLNĚK $\bar{L}$ JE TAKÉ V TŘÍDĚ P
    - PRO JAZYKY Z TŘÍDY NP TOTO NEUMÍME DOKÁZAT
  - JAZYK PATŘÍ DO TŘÍDY CO-NP, JESTLIŽE JEHO DOPLNĚK PATŘÍ DO TŘÍDY NP
    - PŘÍKLAD
      - USAT
        - DOPLNĚK JAZYKA SAT
        - JAZYK VŠECH NESPLNITELNÝCH ŠAT FORMULÍ A VŠECH SLOV NEODPOVÍDAJÍCÍ BOOLEOVSKÉ FORMULI
      - TAUT
        - JAZYK VŠECH SLOV ODPOVÍDAJÍCÍ TAUTOLOGII VÝROKOVÉ LOGIKY
- NEVÍ SE ZDA NP = CO-NP
- MĚJME L_1 A L_2
  - PLATÍ PRO NĚ $L_1 \Delta_P L_2$
  - PAK TAKÉ PLATÍ $\bar{L}_1 \Delta_P \bar{L}_2$

- TŘÍDA PSPACE A NPSPACE

  - PSPACE

    - JAZYK L PATŘÍ DO PSPACE

    - JESTLIŽE EXISTUJE DETERMINISTICKÝ TURINGŮV STROJ M

    - KTERÝ JAZYK L PŘIJÍMÁ A PRACUJE S POLYNOMIÁLNÍ PAMĚŤOVOU SLOŽITOSTÍ

    - ALE MŮŽE SE ZACYKLIT NA SLOVECH KTERÁ NEPŘIJÍMÁ

    - $P \subseteq PSPACE$

  - NPSPACE

    - JAZYK L PATŘÍ DO NPSPACE

    - JESTLIŽE EXISTUJE NEDETERMINISTICKÝ TURINGŮV STROJ M

    - KTERÝ JAZYK L PŘIJÍMÁ A PRACUJE S POLYNOMIÁLNÍ PAMĚŤOVOU SLOŽITOSTÍ

    - $NP \subseteq NPSPACE$

- JE DÁN NTM\TM M KTERÝ PŘIJÍMÁ JAZYK L S PAMĚŤOVOU SLOŽITOSTÍ $p(n)$.

  - PAK EXISTUJE KONSTANTA C TAKOVÁ, ŽE M PŘIJME SLOVO W DÉLKY n PO NEJVÝŠE $c^{p(n)+1}$ KROCÍCH.

- SAVICHOVA VĚTA

  - PSPACE = NPSPACE

- TUDÍŽ $P \subseteq NP \subseteq (N)PSPACE$

- TESTOVÁNÍ PRVOČÍSELNOSTI

  - L_P
    - JAZYK PRVOČÍSEL
    - $L_P = \{ w \mid w$ JE BINÁRNÍ ZÁPIS PRVOČÍSLA$\}$

  - L_S
    - JAZYK SLOŽENÝCH ČÍSEL
    - $L_S = \{ w \mid w$ JE BINÁRNÍ ZÁPIS SLOŽENÝCH ČÍSEL$\}$

  - $L_S = \overline{L_P}$, $L_P = \overline{L_S}$
    - PROBLÉM JE JEN S JEDNIČKOU
      - MUSÍME JI PŘIDAT DO L_S

  - L_S LEŽÍ V NP
    - JESTLIŽE JE ČÍSLO SLOŽENÉ, PAK MÁ DĚLITELE
    - DĚLITEL SLOUŽÍ JAKO CERTIFIKÁT
      - KDYŽ MÁM HO NĚKDO DÁT, MŮŽEME V POLYNOMIÁLNÍM ČASE OTESTOVAT ZDA JE OPRAVDU DĚLITELEM

  - $L_P \in$ CO-NP

  - L_P JE V NP
    - CERTIFIKÁT JE KOMPLIKOVANĚJŠÍ
      - JDE O GENERÁTOR GRUPY $(\mathbb{Z}_p \setminus \{0\}, \odot, 1)$

- TUDÍŽ L_P A L_S PATŘÍ DO PRŮNIKU NP A CO-NP

- MILLERŮV TEST PRVOČÍSELNOSTI

- VSTUP
  - VELKÉ LICHÉ ČÍSLO n
- VÝSTUP
  - PRVOČÍSLO
  - SLOŽENÉ
- 1. SPOČÍTÁME

  $n-1 = 2^k m$ KDE m JE LICHÉ
- 2. NÁHODNĚ VYBEREME $a \in \{1, 2, \ldots, n-1\}$
- 3. SPOČÍTÁME

  $a^m \bmod n$

  - JESTLIŽE $a^m \equiv 1 \bmod n$
    - PAK STOP A VÝSTUP JE PRVOČÍSLO
- 4. OPAKOVANÝM UMOCŇOVÁNÍM POČÍTÁME

  $a^{2m} \bmod n$, $a^{2^2 m} \bmod n, \ldots, a^{2^k m} \bmod n$
- 5. JESTLIŽE $a^{2^k m} \not\equiv 1 \bmod n$
  - PAK STOP, A VÝSTUP JE SLOŽENÉ
- 6. VEZMEME j TAKOVÉ, ŽE $a^{2^j m} \not\equiv 1 \bmod n$ A $a^{2^{j+1} m} \equiv 1 \bmod n$
  - JESTLIŽE $a^{2^j m} \equiv -1 \bmod n$
    - STOP, JE PRVOČÍSLO
  - JESTLIŽE $a^{2^j m} \not\equiv -1 \bmod n$
    - STOP, JE SLOŽENÉ
- JESTLIŽE DÁ ALGORITMUS VÝSTUP SLOŽENÉ, PAK JE n SLOŽENÉ
- JESTLIŽE DÁ ALGORITMUS VÝSTUP PRVOČÍSLO, PAK JE n PRVOČÍSLO S PRAVDĚPODOBNOSTÍ VĚTŠÍ NEŽ $\frac{1}{2}$

- RANDOMIZOVANÝ TURINGŮV STROJ
  - TM S DVĚMA NEBO VÍCE PÁSKAMI
    - DRUHÁ PÁSKA OBSAHUJE SEKVENCI 0 A 1, OBOJE S PRAVDĚPODOBNOSTÍ $\frac{1}{2}$, NÁHODNĚ VYGENEROVANÉ PRO KAŽDÝ BĚH
    - DRUHÁ PÁSKA SE NEPŘEPISUJE
  - PŘECHODOVÁ FCE

$$\delta(q, X, a) = (p, Y, D_1, D_2) \qquad D_1, D_2 \in \{L, R, S\}$$

  - DÍKY NÁHODNOSTI SEKVENCE MOHOU BÝT DVA PRŮCHODY ALGORITMEM PRO RTM SE STEJNÝM VSTUPEM RŮZNÉ

- TŘÍDA RP
  - JAZYK L PATŘÍ DO RP KDYŽ
  - EXISTUJE RTM TAKOVÝ, ŽE
    - 1. JESTLIŽE $w \notin L$ PAK SE M ZASTAVÍ V q_β S PRAVDĚPODOBNOSTÍ 0
    - 2. JESTLIŽE $w \in L$ PAK SE M ZASTAVÍ V q_β S PRAVDĚPODOBNOSTÍ ALESPOŇ $\frac{1}{2}$
    - 3. EXISTUJE POLYNOM $p(n)$ TAKOVÝ, ŽE KAŽDÝ BĚH M (LIBOVOLNÝ OBSAH DRUHÉ PÁSKY) TRVÁ MAXIMÁLNĚ $p(n)$ KROKŮ, KDE n JE DÉLKA SLOVA.

- MONTE CARLO RTM
  - SPLŇUJE PODMÍNKY 1. A 2.
  - ALE NEMUSÍ BĚŽET V POLINOMIÁLNÍM ČASE

- JE DÁN JAZYK $L \in RP$
  - PAK PRO KAŽDOU KLADNOU KONSTANTU $0 < c < \frac{1}{2}$ JE MOŽNÉ SESTROJIT RTM M S POLYNOMIÁLNÍ SLOŽITOSTÍ TAKOVÝ, ŽE
    - 1. JESTLIŽE $w \notin L$, STROJ M SE ÚSPĚŠNĚ ZASTAVÍ S PRAVDĚPODOBNOSTÍ 0
    - 2. JESTLIŽE $w \in L$, STROJ M SE ÚSPĚŠNĚ ZASTAVÍ S PRAVDĚPODOBNOSTÍ ALESPOŇ $1-c$

- TŘÍDA ZPP
  - JAZYK L PATŘÍ DO ZPP, IFF EXISTUJE RTM M TAKOVÝ, ŽE
    - 1. JESTLIŽE $w \notin L$, PAK SE M ZASTAVÍ ÚSPĚŠNĚ S PRAVDĚPODOBNOSTÍ 0
    - 2. JESTLIŽE $w \in L$, PAK SE M ZASTAVÍ ÚSPĚŠNĚ S PRAVDĚPODOBNOSTÍ 1
    - 3. STŘEDNÍ HODNOTA POČTU KROKŮ M V JEDNOM BĚHU JE $p(n)$, KDE $p(n)$ JE POLYNOM A n JE DÉLKA VSTUPU
    - " M NEDĚLÁ CHYBU, ALE NEZARUČUJE POLYNOMIÁLNÍ POČET KROKŮ PŘI JEDNOM BĚHU "
  - TAKOVÝ RTM SE NAZÝVÁ LAS-VEGAS
  - JESTLIŽE JAZYK L PATŘÍ DO ZPP, PAK I DOPLNĚK $\bar{L}$ PATŘÍ DO ZPP
    - " STAČÍ PRAVÉ KONCOVÉ STAVY OZNAČIT ZA NEKONCOVÉ A NEKONCOVÉ OZNAČIT ZA KONCOVÉ "

- TŘÍDA CO-RP
  - DOPLNĚK TŘÍDY RP
  - CO-RP ∩ RP = ZPP
- P ⊆ ZPP
- RP ⊆ NP
- co-RP ⊆ Co-NP

- NEROZHODNUTELNOST
  - JAZYK L JE REKURSIVNÍ
    - JESTLIŽE EXISTUJE TM KTERÝ ROZHODUJE JAZYK L
    - REKURSIVNÍ JAZYKY SE ZNAČÍ R
  - JAZYK L JE REKURSIVNĚ SPOČETNÝ
    - JESTLIŽE EXISTUJE TM KTERÝ PŘIJÍMÁ JAZYK L
    - "MŮŽE SE ZACYKLIT"
    - REKURSIVNĚ SPOČETNÉ JAZYKY SE ZNAČÍ RS
  - JAZYKŮM CO NEJSOU REKURSIVNÍ ŘÍKÁME
    - ALGORITMICKY NEŘEŠITELNÉ NEBO NEROZHODNUTELNÉ
  - JESTLIŽE JE L REKURSIVNÍ, PAK JE I JEHO DOPLNĚK $\bar{L}$ REKURSIVNÍ
  - JESTLIŽE JE L I $\bar{L}$ REKURSIVNĚ SPOČETNÉ, PAK JE L REKURSIVNÍ
  - PRO JAZYK L MŮŽE NASTAT JEDNA Z MOŽNOSTÍ
    - 1. L I $\bar{L}$ JSOU REKURSIVNÍ
    - 2. JEDEN Z L A $\bar{L}$ JE REKURSIVNĚ SPOČETNÝ A DRUHÝ NENÍ REKURSIVNĚ SPOČETNÝ
    - 3. L I $\bar{L}$ NEJSOU REKURSIVNĚ SPOČETNÉ

- KÓD TURINGOVA STROJE
  - KAŽDÝ TURINGŮV STROJ LZE ZAKÓDOVAT JAKO BINÁRNÍ SLOVO
  - PŘECHOD STROJE M $\delta(q_i, X_j) = (q_k, X_l, D_r)$ ZAKÓDUJEME SLOVEM $w = 0^i 1 0^j 1 0^k 1 0^l 1 0^r$
  - KÓD TURINGOVA STROJE JE
    $\langle M \rangle = 111\, w_1\, 11\, w_2\, 11 \ldots 11\, w_p\, 111$
    - KDE SLOVA $w_1, \ldots, w_p$ ODPOVÍDAJÍ VŠEM PŘECHODŮM M

- DIAGONÁLNÍ JAZYK L_d
  - JESTLIŽE BINÁRNÍ SLOVO w NEMÁ TVAR KÓDU TURINGOVA STROJE, POVAŽUJEME HO ZA KÓD TURINGOVA STROJE KTERÝ NEPŘIJÍMÁ ŽÁDNÉ SLOVO
    - "NEUDĚLÁ ŽÁDNÝ KROK"
    - $L(M) = \emptyset$
  - L_d SE SKLÁDÁ ZE VŠECH SLOV w TAKOVÝCH, ŽE TM S KÓDEM w NEPŘIJÍMÁ w
  - NEEXISTUJE TM KTERÝ BY PŘIJÍMAL L_d
  - $L_d \neq L(M)$ PRO KAŽDÝ TM M

- UNIVERZÁLNÍ JAZYK
  - L_{UN} JE MNOŽINA SLOV TVARU $\langle M \rangle w$, KDE $\langle M \rangle$ JE KÓD TURINGOVA STROJE A $w \in \{0,1\}^*$ JE BINÁRNÍ SLOVO TAKOVÉ, ŽE $w \in L(M)$

- UNIVERZÁLNÍ TURINGŮV STROJ
  - PŘIJÍMÁ UNIVERZÁLNÍ JAZYK
  - MÁ 4 PÁSKY
    - 1. OBSAHUJE VSTUPNÍ SLOVO $\langle M \rangle w$
    - 2. SIMULUJE PÁSKU TM M
    - 3. OBSAHUJE KÓD STAVU

- UNIVERZÁLNÍ JAZYK L_{UN} JE REKURSIVNĚ SPOČETNÝ
- L_{UN} ALE NENÍ REKURSIVNÍ
  - KDYBY BYL, MUSEL BY SE TM ZASTAVIT
  - TAKOVÝ TM BY ALE BYL SCHOPEN ROZHODNOUT DIAGONÁLNÍ JAZYK

- REDUKCE JAZYKŮ
  - DÁNY DVA JAZYKY $L_1 \subseteq \Sigma^*$ A $L_2 \subseteq \Gamma^*$
  - L_1 SE REDUKUJE NA L_2
    - JESTLIŽE EXISTUJE ALGORITMUS A
    - KTERÝ PRO KAŽDÉ SLOVO $w \in \Sigma^*$ ZKONSTRUUJE SLOVO $A(w) \in \Gamma^*$ TAK, ŽE

      ~~$w \in L_1$ NEPLATÍ $w \in L_2$~~

      $w \in L_1$ IFF $A(w) \in L_2$
    - ZNAČÍME

      $L_1 \triangleleft L_2$

- DÁNY DVĚ ÚLOHY U A V
  - $U \triangleleft V$, PAK PLATÍ
    - JESTLIŽE V JE ROZHODNUTELNÁ, PAK I U JE ROZHODNUTELNÁ
    - JESTLIŽE U JE NEROZHODNUTELNÁ, PAK I V JE NEROZHODNUTELNÁ
    - JESTLIŽE JAZYK U NENÍ REKURSIVNĚ SPOČETNÝ, PAK I JAZYK ÚLOHY V NENÍ REKURSIVNĚ SPOČETNÝ

- JAKÁKOLIV NETRIVIÁLNÍ VLASTNOST REKURZIVNĚ SPOČETNÝCH JAZYKŮ (PŘIJÍMANÝCH TM) JE NEROZHODNUTELNÁ.
  - NETRIVIÁLNÍ VLASTNOSTÍ SE MYSLÍ KAŽDÁ VLASTNOST, KTEROU MÁ ALESPOŇ JEDEN REKURSIVNĚ SPOČETNÝ JAZYK A NEMÁJÍ HO VŠECHNY REKURSIVNĚ SPOČETNÉ JAZYKY.

- DALŠÍ NEROZHODNUTELNÉ PROBLÉMY

  - POSTŮV KORESPONDENČNÍ PROBLÉM

    - DÁNY DVA SEZNAMY SLOV A, B NAD ABECEDOU Σ

      - $A = (w_1, w_2, \ldots, w_k)$, $B = (x_1, x_2, \ldots, x_k)$

    - ŘEKNEME ŽE DVOJICE A, B MÁ ŘEŠENÍ, JESTLIŽE EXISTUJE POSLOUPNOST $i_1, i_2 \ldots i_r$ INDEXŮ TAKOVÁ, ŽE

      $$w_{i_1} w_{i_2} \ldots w_{i_r} = x_{i_1} x_{i_2} \ldots x_{i_r}$$

    - TOTO JE NEROZHODNUTELNÝ PROBLÉM

      - BYL BY ROZHODNUTELNÝ, KDYBYCHOM OMEZILI DÉLKU SEKVENCE

  - TILING PROBLÉM

    - MÁME DÁNY DLAŽDIČKY VELIKOSTI $1\,cm^2$ NĚKOLIKA TYPŮ

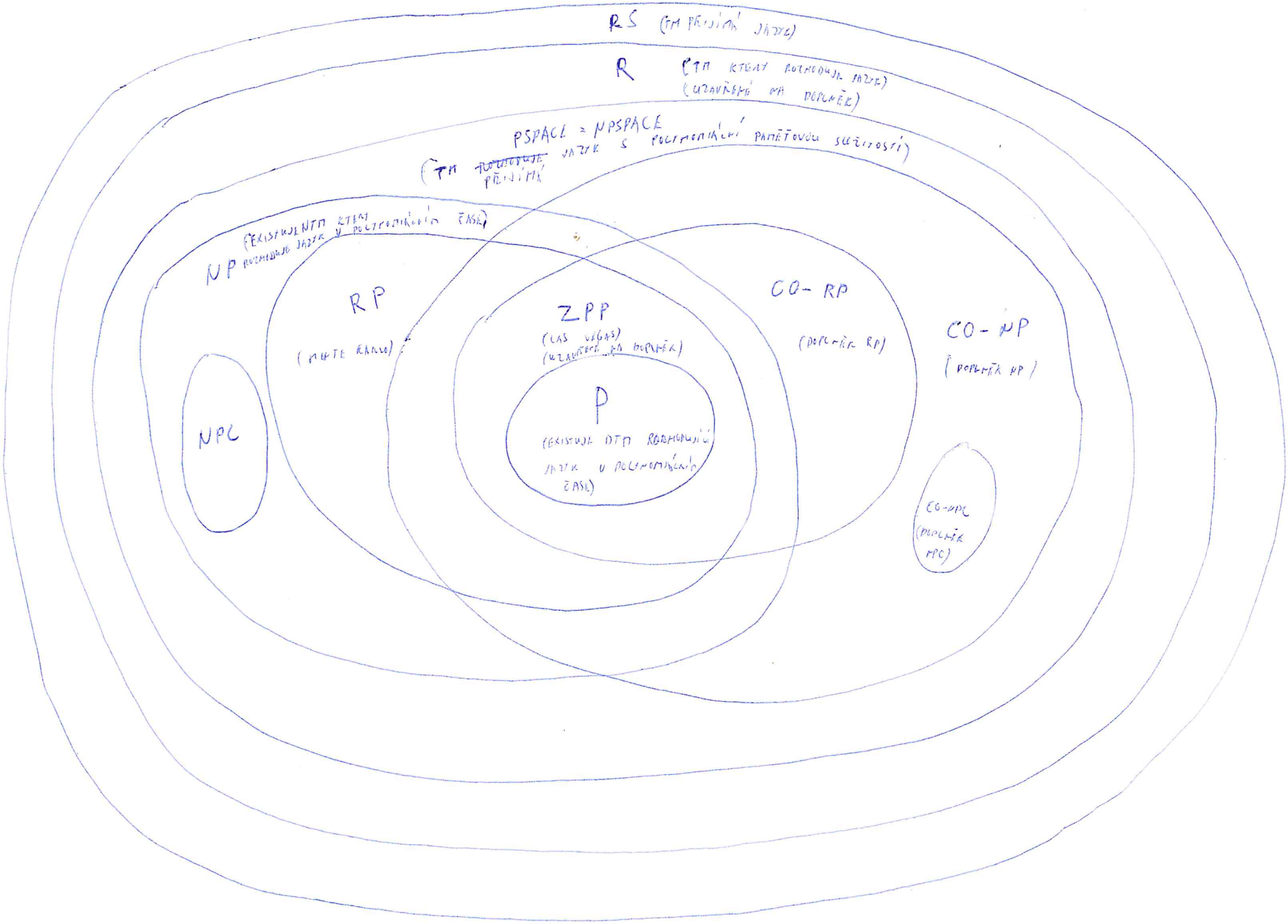
      - KAŽDÁ MÁ JINAK BAREVNĚ OKRAJE

      - MÁME NEOMEZENÝ POČET DLAŽDIČEK KAŽDÉHO TYPU

    - JE MOŽNÉ DLAŽDIČKAMI VYDLÁŽDIT KAŽDOU PLOCHU DANÉHO TYPU TAK, ABY SE DLAŽDIČKY DOTÝKALY HRANAMI STEJNÉ BARVY, ZA PŘEDPOKLADU, ŽE DLAŽDIČKAMI NESMÍME ROTOVAT?

    - JE TO NEROZHODNUTELNÝ PROBLÉM

      - TEDY SPECIÁLNĚ JE NEROZHODNUTELNÉ, ZDA KAŽDOU NEOMEZENOU PLOCHU JDE MOŽNÉ VYDLÁŽDIT PŘEDEM DANOU SADOU DLAŽDIČEK.


RS
(TM PŘIJÍMÁ JAZYK)
R
(TM KTERÝ ROZHODUJE JAZYK)
(UZAVŘENÉ NA DOPLNĚK)
PSPACE = NPSPACE
(TM PŘIJÍMÁ JAZYK S POLYNOMIÁLNÍ PAMĚŤOVOU SLOŽITOSTÍ)
NP
(EXISTUJE NTM KTERÝ ROZHODUJE JAZYK V POLYNOMIÁLNÍM ČASE)
RP
(MUTE RANDOM)
ZPP
(LAS VEGAS)
(UZAVŘENÉ NA DOPLNĚK)
P
(EXISTUJE DTM ROZHODUJÍCÍ JAZYK V POLYNOMIÁLNÍM ČASE)
CO-RP
(DOPLNĚK RP)
CO-NP
(DOPLNĚK NP)
NPC
CO-NPC
(DOPLNĚK NPC)