

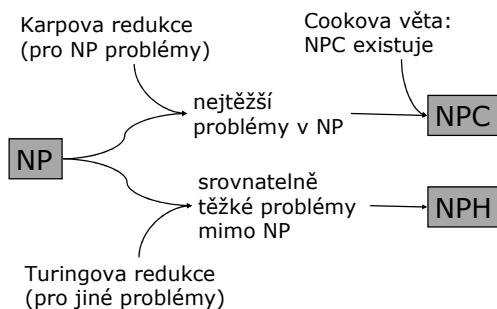
NP-úplné (NPC) a NP-těžké (NPH) problémy

- Karpova redukce
- NP-úplné problémy (NPC)
- Cookova věta
- Turingova redukce
- NP-těžké problémy (NPH)
- problémy mezi P a NPC

Pojmy X-těžký a X-úplný (X-complete a X-hard)

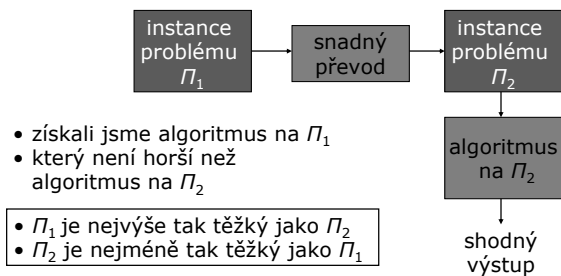
- Problém Π je X-těžký, jestliže se efektivní řešení všech problémů z třídy X dá zredukovat na efektivní řešení problému Π .
- Problém Π je X-úplný, jestliže je X-těžký a sám patří do třídy X.
- efektivní řešení: v polynomiálním čase (jindy např. s omezenou chybou)
- zredukovat: vyřešit pomocí
- za X dosadit: NP, NPO, APX...

NPH a NPC

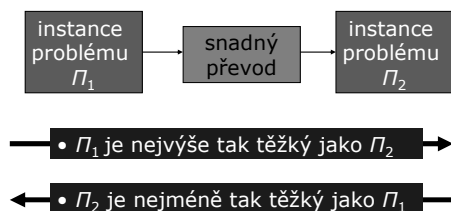


Co jsou nejtěžší problémy v NP?

Co je „lehčí“ a „těžší“ problém?



Který problém je nejtěžší?



Ten, na který jdou převést všechny ostatní.

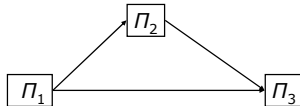
Karpova redukce (polynomiální transformace)

- Definice Karpovy redukce
Rozhodovací problém Π_1 je Karp-redukovatelný na Π_2 ($\Pi_1 \leq \Pi_2$), jestliže existuje polynomiální program pro (deterministický) Turingův stroj, který převede každou instanci I_1 problému Π_1 na instanci I_2 problému Π_2 tak, že výstup obou instancí je shodný.
- Jiné značení: $\leq$

Vlastnosti

- Tranzitivita

$$\Pi_1 \sim \Pi_2 \wedge \Pi_2 \sim \Pi_3 \Rightarrow \Pi_1 \sim \Pi_3$$

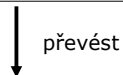


- Třídy polynomiální ekvivalence

$\Pi_1 \sim \Pi_2 \wedge \Pi_2 \sim \Pi_1 \Rightarrow \Pi_1$ a Π_2 jsou polynomiálně ekvivalentní.

Příklad: HC ∞ TSP

Dán graf $G=(V,E)$. Obsahuje tento graf Hamiltonovu kružnici?



Dána množina n měst $C=\{c_1, c_2, \dots, c_n\}$. Pro každá dvě města c_i, c_j je dána vzdálenost $d(c_i, c_j) > 0$. Existuje uzavřená túra, která prochází každým městem právě jednou a má délku nejvýše B ?

Karpova redukce HC ∞ TSP

Algoritmus:

$$V, E \rightarrow C, d(c_i, c_j), B$$

- Nechť každému uzlu v_i odpovídá jiné město c_i .
- Je-li $(v_i, v_j) \in E$, nechť $d(c_i, c_j)=1$ jinak $d(c_i, c_j)=2$
- Nechť $B=|V|$.

Osnova důkazu, že je Karpovou redukcí:

1. HC ∞ TSP má polynomiální složitost
2. výstup je stejný
 - 2.1 $\exists$ kružnice v $G \Rightarrow \exists$ túra v C
 - 2.2 $\exists$ túra v $C \Rightarrow \exists$ kružnice v G

Důkaz HC ∞ TSP

1. HC ∞ TSP má polynomiální složitost ($n=|V|$)

- Konstrukce měst: $O(n)$; vzdálenosti: $O(n^2)$; $B: O(1)$
- $\Rightarrow$ složitost $O(n^2)$;

- 2.1 $\exists$ kružnice v $G \Rightarrow \exists$ túra v C

- $(v_1, v_2, \dots, v_n, v_1)$ Hamiltonova kružnice v G .
- $\Rightarrow (c_1, c_2, \dots, c_n, c_1)$ je túra v C o délce $n \cdot 1$ (každý úsek túry odpovídá hraně)
- $n \leq B$.

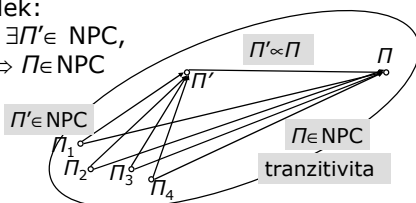
- 2.2 $\exists$ túra v $C \Rightarrow \exists$ kružnice v G

- $(c_1, c_2, \dots, c_n, c_1)$ je túra délky nejvýše B .
- n úseků, délka $B=n$ každý úsek túry má délku 1
- $\Rightarrow$ každý úsek odpovídá hraně
- $(v_1, v_2, \dots, v_n, v_1)$ Hamiltonova kružnice v G . **Q.e.d.**

Třída NP-úplný (NP-Complete, NPC)

- Definice (třída NP-úplný):
- Problém Π je NP-úplný, jestliže
 - $\Pi \in \text{NP}$
 - pro všechny problémy $\Pi' \in \text{NP}$, $\Pi' \leq \Pi$

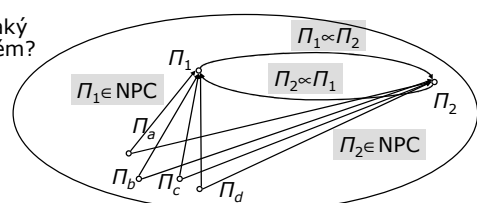
- Důsledek:
 $\Pi \in \text{NP}$, $\exists \Pi' \in \text{NPC}$,
 $\Pi' \leq \Pi \Rightarrow \Pi \in \text{NPC}$



NP-úplný jako třída ekvivalence

- Všechny NPC problémy tvoří třídu ekvivalence
- $\Pi_1, \Pi_2 \in \text{NPC} \Rightarrow \Pi_1 \in \text{NP}, \Pi_2 \in \text{NP}$
- $\Pi_1 \sim \Pi_2$ (protože $\Pi_1 \in \text{NP}, \Pi_2 \in \text{NPC}$)
- $\Pi_2 \sim \Pi_1$ (protože $\Pi_2 \in \text{NP}, \Pi_1 \in \text{NPC}$) **Q.e.d.**

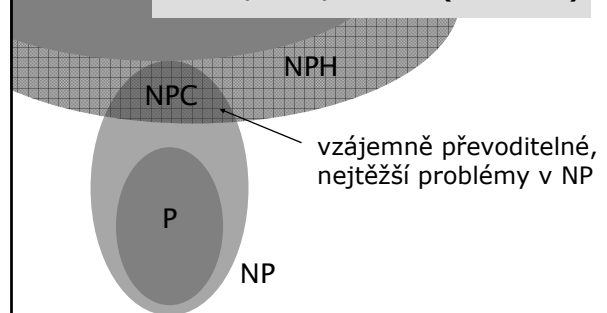
existuje vůbec nějaký NPC problém?



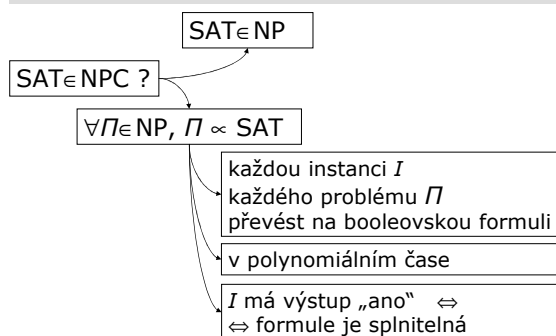
Cookova věta a důsledky

- SAT je NP-úplný
- říká, že NPC není prázdná
- otevírá cestu k důkazům NP-úplnosti převodem
- jsou známy tisíce NPC problémů
- které tvoří třídu ekvivalence
- polynomiální program na jeden $\Rightarrow$
 $\Rightarrow$ polynomiální program na všechny
- nevypadá to, že by $P=NP$...

P, NP, NPC (a NPH)



Osnova důkazu



Důsledky $\Pi \in NP, I \in \Pi_{ANO}$

- Existuje program M pro Turingův stroj, který kontroluje certifikát Y instance I v čase $p(n)$, kde p je polynom a n velikost instance I a skončí ve stavu q_{ANO} .
- Velikost certifikátu je nejvýše $p(n)$.
- Rozsah políček pásky je $-p(n) \dots p(n)+1$.

Konstruovaná formule

- Jestliže $I \in \Pi_{ANO}$, pak formule, která vyjadřuje výrok „proběhl výpočet stroje M , který se zastavil ve stavu q_{ANO} “ má ohodnocení proměnných, při kterém nabývá hodnoty true.
- „Náhrada naprogramovaného počítače kombinačním obvodem“
- Musí obsahovat
 - vlastnosti Turingova stroje
 - program M
 - výsledek „ano“

Celkový stav Turingova stroje

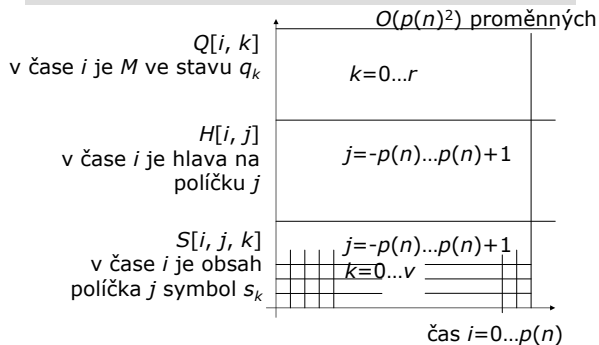
- Stav řídicího automatu
- Obsah všech políček pásky
- Pozice hlavy na pásce

Výpočet Turingova stroje

- Posloupnost celkových stavů v čase $0 \dots t$, kde t je celkový čas výpočtu
- $\rightarrow$ proměnné formule

Proměnné formule

r ...počet stavů; v ...počet symbolů abecedy pásky



Klauzule formule

musí být splněny současně (součin)

počítá to jako Turingův stroj

v každém čase i , řízení je v právě jednom stavu

v každém čase i , hlava je na právě jednom políčku

v každém čase i , každé políčko obsahuje právě jeden symbol

v čase 0, celkový stav je inicializován

výstup je „ano“

v čase $p(n)$, řízení je ve stavu q_{ANO}

program

v každém čase i , celkový stav je výsledkem aplikace přechodové funkce δ na předchozí celkový stav

Ukázky konstrukce některých skupin

v každém čase i , řízení je v právě jednom stavu

$$\neg (Q[i, 0] \cdot Q[i, 1]) = (\neg Q[i, 0] + \neg Q[i, 1])$$

... v nejvýše jednom stavu

... v alespoň jednom stavu

$$(\neg Q[i, j] + \neg Q[i, j'])$$

$i=0 \dots p(n) \quad j=-p(n) \dots p(n)+1$
 $j'=j+1 \dots p(n)+1$

$$(Q[i, 0] + Q[i, 1] + \dots + Q[i, r])$$

$i=0 \dots p(n) \quad k=0 \dots r$

Ukázky konstrukce některých skupin

když hlava není na políčku j , obsah se nezmění

v každém čase i , celkový stav je výsledkem aplikace přechodové funkce δ na předchozí celkový stav

$$(\neg S[i, j, l] + H[i, j] + S[i+1, j, l])$$

$i=0 \dots p(n) \quad j=-p(n) \dots p(n)+1 \quad l=0 \dots v$

$$a \Rightarrow b = \neg a + b$$

$$(\neg H[i, j] + \neg Q[i, k] + \neg S[i, j, l] + H[i+1, j+\Delta])$$

$$(\neg H[i, j] + \neg Q[i, k] + \neg S[i, j, l] + Q[i+1, k'])$$

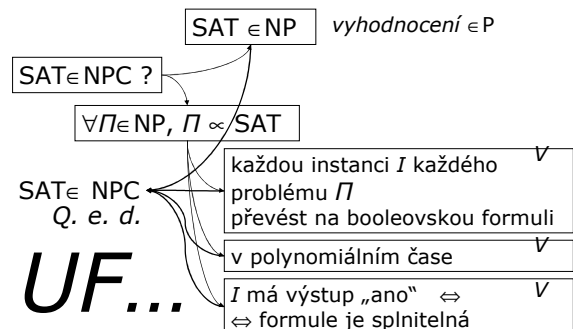
$$(\neg H[i, j] + \neg Q[i, k] + \neg S[i, j, l] + S[i+1, j, l'])$$

$i=0 \dots p(n) \quad j=-p(n) \dots p(n)+1 \quad l=0 \dots v \quad k=0 \dots r$

Polynomiální složitost

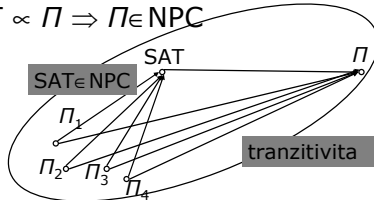
- Ukázat, že velikost výsledné formule F je polynomiální s n – velikostí původní instance
- velikost formule s množinou C klauzulí nad množinou X proměnných: $|X| \cdot |C|$
- $r, v \dots$ konstantní pro daný problém Π
- $|X| = O(p(n)^2) \quad |C| = O(p(n)^2)$
- $|F| = O(p(n)^4)$

Osnova důkazu

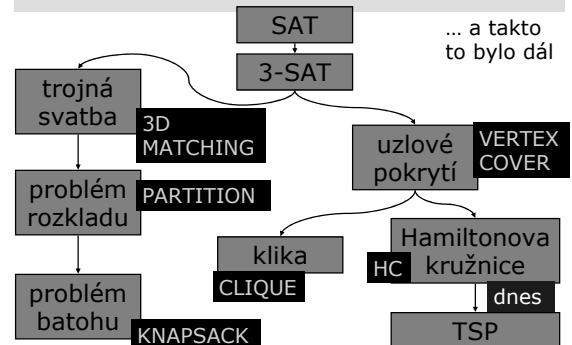


Dokazování NP-úplnosti Π

- Z definice lehce nepraktické, že
- $\Pi' \in \text{NPC}$ je speciálním případem Π
- $\Pi \in \text{NP}, \exists \Pi' \in \text{NPC}, \Pi' \leq \Pi \Rightarrow \Pi \in \text{NPC}$
 $\Pi \in \text{NP}, \text{SAT} \leq \Pi \Rightarrow \Pi \in \text{NPC}$



Na počátku je SAT...



Bestiariu

- **3-SAT:** každá klauzule má právě 3 literály
- **Trojná svatba:**
 - dány disjunktní množiny W, X, Y , $|W|=|X|=|Y|=q$, množina $M \subseteq W \times X \times Y$;
 - existuje $M' \subseteq M$ taková, že $|M'|=q$ a žádné dva prvky M' se neshodují ani v jedné souřadnici?
- **Uzlové pokrytí:**
 - dán graf $G=(V,E)$, celé číslo $K \leq |V|$;
 - existuje $V' \subseteq V$ taková, že $|V'| \leq K$ a $\forall (u,v) \in E, u \in V' \text{ nebo } v \in V'$?

Bestiariu

- **Klika:** („politická klika“)
 - dán graf $G=(V,E)$, celé číslo $K \leq |V|$;
 - existuje úplný podgraf $G'=(V',E')$ grafu G takový, že $|V'| \geq K$?
- **Problém rozkladu:**
 - dána množina $A=\{a_1, \dots, a_n\}$ a funkce $s: A \rightarrow \mathbb{Z}^+$;
 - existuje podmnožina $A' \subseteq A$ taková, že

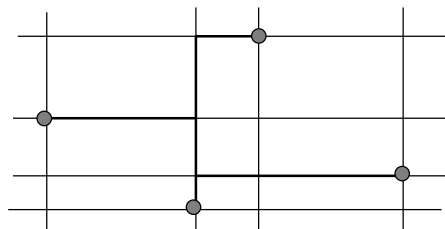
$$\sum_{a \in A'} s(a) = \sum_{a \in A-A'} s(a)$$
 (rozklad na podmnožiny se stejnou cenou)

Bestiariu

- **Steinerův problém:**
 - dán graf $G=(V,E)$
 - dána podmnožina $V' \subseteq V$
 - sestavit minimální souvislý podgraf $H=(W,F)$ takový, že $V' \subseteq W$.
- Mnoho variant na speciálních grafech

Bestiariu

- Steinerův problém v pravoúhlé metrice



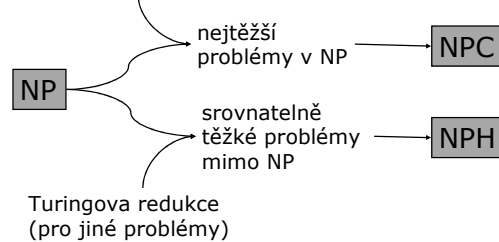
Bestiarium

Problém plánování: (jeden z mnoha)

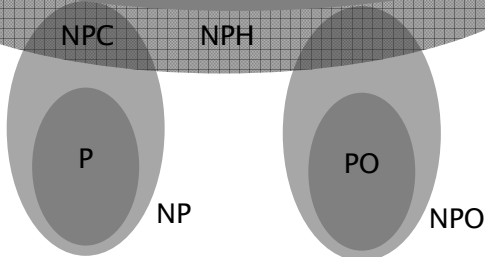
- Dána množina T operací o jednotkové době trvání, dále je dáno částečné uspořádání $<$ na T a maximální doba výpočtu $D \in \mathbb{Z}^+$. Existuje takový plán $\delta: T \rightarrow \{0, 1, \dots, D\}$ že
 - v každém okamžiku z $\{0, 1, \dots, D\}$ je naplánováno nejvýše m operací a
 - je-li $t_i < t_j$ pak $\delta(t_i) < \delta(t_j)$
- Úloha je NP-těžká; je-li však $<$ zobrazitelné množinou stromů, je polynomiální.

NPH a NPC

Karpova redukce
(pro NP problémy)



P, NP, NPC, PO, NPO, NPH



Turingova redukce (Turingova transformace)

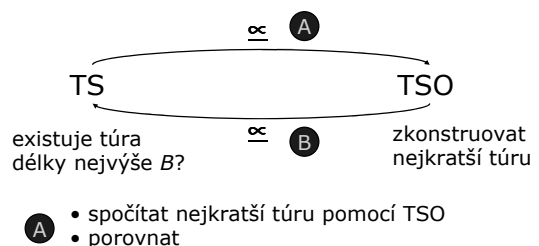
Definice Turingovy redukce

- Rozhodovací problém Π_1 je Turing-redukovatelný na Π_2 ($\Pi_1 \leq_T \Pi_2$), jestliže existuje polynomiální program pro (deterministický) Turingův stroj, který řeší každou instanci I_1 problému Π_1 tak, že používá program M_2 pro problém Π_2 jako podprogram (jehož trvání považujeme za jeden krok).
- Jiné značení: $\leq$ $\leq^T$

Třída NP-těžký (NP-Hard, NPH)

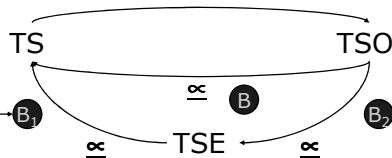
- Definice** (třída NP-těžký):
Problém Π je NP-těžký, jestliže pro všechny problémy $\Pi' \in \text{NP}$, $\Pi' \leq \Pi$
- Karpova redukce je speciálním případem Turingovy redukce (volání podprogramu jednou, přímé použití výsledku)
- $\text{NPC} \subseteq \text{NPH}$

Rozhodovací (TS) a optimalizační (TSO) verze TSP



Turingova redukce

- $TSE \in NP$
- $TS \in NPC$
- $TSE \leq TS$
- $TSE \leq TS$



TSE: Dána množina n měst $C = \{c_1, c_2, \dots, c_n\}$. Pro každá dvě města c_i, c_j je dána vzdálenost $d(c_i, c_j)$. Dále dána mez B a cesta θ procházející K městy. Dá se θ prodloužit na túru délky nejvýše B ?

TSE: Dána množina n měst $C = \{c_1, c_2, \dots, c_n\}$, vzdálenost $d(c_i, c_j)$. Dále mez B a cesta θ procházející K městy. Dá se θ prodloužit na túru délky $\leq B$?

$TSO \leq TSE$

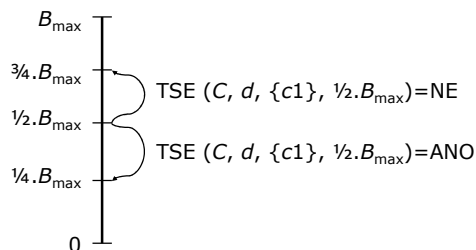
B_2

- Víme, že $B_{\min} = n$, $B_{\max} = n \cdot \max \{d(c_i, c_j)\}$
- Velikost instance měříme $N = n + \log_2 B_{\max}$
- Necht' existuje program TSE (C, d, θ, B). Jak pomocí něj vyřeším TSO?
- 1. Určím B^* pomocí $\log_2 B_{\max}$ volání TSE ($C, d, \{c_1\}, B$).
- 2. Určím další město k c_1 pomocí TSE ($C, d, \{c_1, c_j\}, B^*$).
- 3. Opakuji, až určím celou kružnici

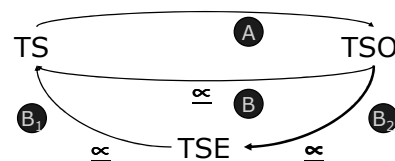
$$O(\log_2 B_{\max}) + O(n^2) = O(N^2)$$

K předchozímu důkazu

1. Určím B^* pomocí $\log_2 B_{\max}$ volání TSE ($C, d, \{c_1\}, B$).

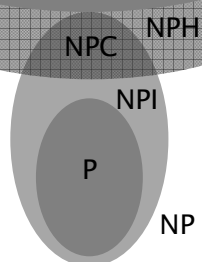


TS a TSO



TS a TSO jsou Turing-ekvivalentní a tedy stejně těžké.

NP-intermediate (NPI)



- NPI: problémy, které nemohou mít polynomiální algoritmus ani na ně nikdy nemůže být převeden SAT, pokud $P \neq NP$
- NP-P-NPC: problémy, pro které ani neumíme nalézt polynomiální algoritmus, ani na ně převést SAT.

Např. izomorfismus grafů, do r. 2004 také test prvočíselnosti

NPI není prázdná

- Důsledek obecnější věty (Ladner 1975):
- Necht' Π je NP-úplný problém a I množina jeho instancí. Pak existuje podmnožina I' jeho instancí, rozpoznatelná polynomiálním algoritmem taková, že problém Π' vzniklý omezením Π na I' není ani NPC, ani P.
- Příklad: musí existovat množina grafů, pro kterou HC není ani NPC, ani P.
- Zatím nalezeny jen zcela „nepřirozené“ případy

Kandidát NPI: isomorfismus grafů

- Dány grafy $G=(V,E)$ a $H=(W,F)$.
- Existuje prosté zobrazení $f: V \rightarrow W$ takové, že pro každé $u,v \in V$ platí $(u,v) \in E$ právě tehdy, když $(f(u),f(v)) \in F$?
- Pokud by tento problém byl NPC, polynomiální hierarchie by zkolabovala (minulá přednáška)

Otevřené verze problémů: problém plánování

