

## Kapitola 7

# Trieda NP a NP-úplnosť

O význame triedy  $P$  ako triede prakticky riešiteľných problémov sme už hovorili. Videli sme, že polynomiálny čas je taká vlastnosť problémov, ktorá je nezávislá od výberu výpočtového modelu, pokiaľ sa hýbeme v prvej počítačovej triede. Triedu  $P$  rozhodne môžeme považovať za triedu prakticky riešiteľných úloh. (Neskôr došlo k posunu – za prakticky riešiteľné považujeme aj pravdepodobnostné a aproximačné algoritmy polynomiálnej zložitosti.)

Je veľa takých úloh, pre ktoré nepoznáme deterministické polynomiálne riešenie; všetky známe deterministické algoritmy sú exponenciálnej zložitosti, často založené na preberaní všetkých možností. Mnohé z nich sú však také, že ak poznáme *riešenie*, jeho správnosť vieme overiť v polynomiálnom čase. Tak sme sa inak dostali k triede  $NP$  – sú to problémy, ktorých riešenie vieme overiť v polynomiálnom čase. Riešenie samotného problému možno vyjadriť ako "uhádni a over". Z tohto pohľadu je otázka vzťahu  $P?NP$  vlastne otázkou—čo je ľahšie, nájsť riešenie alebo overiť jeho správnosť?

Nedeterminizmus priniesol do riešenia problémov novú kvalitu. Hoci pochopenie tohto konceptu nie je jednoduché, nedeterministické riešenia—algoritmy—sú často zrozumiteľnejšie, elegantnejšie. Vzhľadom na simulácie z predchádzajúcej časti vieme, že prechod od nedeterminizmu k determinizmu nás môže stať až exponenciálny nárast času. Je to nutné? Sú problémy riešiteľné v nedeterministickom polynomiálnom čase tak ťažké, že sa nedajú riešiť v polynomiálnom deterministickom čase? Otázka vzťahu tried  $P$  a  $NP$  patrí k tým najvýznamnejším. Väčšina informatikov predpokladá, že  $P \neq NP$  a namiesto riešenia vzťahu týchto dvoch tried sa sústreďujeme skôr na to, ako riešiť tie problémy, ktoré sú ťažké.

Kedy hovoríme, že problém je ťažký? Napr. vtedy, ak nepatrí do  $P$ . Dokázať však o konkrétnom probléme, že nepatrí do triedy  $P$ , je nesmierne obtiažne. Uvidíme, že existuje "nástroj", pomocou ktorého pre mnohé problémy pomerne ľahko ukážeme, že sa za predpokladu  $P \neq NP$  v polynomiálnom deterministickom čase riešiť nedajú. Týmto nástrojom sú NP-úplné problémy.

K čomu je to dobré? Ak to nejde deterministicky polynomiálne, treba z niečoho zľaviť—aproximačné, pravdepodobnostné, heuristické riešenia.

### 7.1 Redukcie, NP-úplnosť

Ukážeme, že NP-úplné problémy sú "najťažšie" problémy v triede  $NP$ . Začnime definíciami redukcií, ktoré umožňujú porovnávať obtiažnosť problémov.

*polynomiálna redukcia*  $L \rightsquigarrow L'$  **Definícia 7.1** *Jazyk  $L$  sa nazýva polynomiálne redukovateľný na jazyk  $L'$ , ak existuje polynóm  $p$  a  $p(n)$ -časovo ohraničený DTS  $M$  taký, že  $M$  prepíše každý vstupný reťazec  $w \in \Sigma_L^*$  na reťazec  $w' \in \Sigma_{L'}^*$ , tak, že  $w \in L \Leftrightarrow w' \in L'$ .*

*NP-ťažký, NP-úplný jazyk* **Definícia 7.2** *Jazyk  $L_0$  sa nazýva NP-ťažký, ak  $\forall L \in NP$ :  $L$  je polynomiálne redukovateľný na  $L_0$ . Ak navyše  $L_0 \in NP$  tak je jazyk NP-úplný. Triedu NP-úplných problémov budeme označovať NPÚ.*

O význame NP-úplných problémov hovorí nasledujúca veta, najmä podmienka 2.

### Veta 7.1

1. Ak existuje NP-úplný jazyk  $L$ , ktorý navyše patrí do triedy  $P$ , tak  $P = NP$
2. Ak  $P \neq NP$ , tak trieda NP-úplných problémov patrí do rozdielu  $NP \setminus P$

### Dôkaz:

1. vyplýva z tranzitívnosti relácie polynomiálnej redukovateľnosti a z vlastností skladania polynómov.
2. je dôsledkom 1.

□

Z vety vidno, že ak chceme ukázať rovnosť tried  $P = NP$ , stačí pre jediný NP-úplný problém nájsť deterministický polynomiálny algoritmus.

Naopak – ak prijmeme hypotézu, že  $P \neq NP$ , je dôkaz NP-úplnosti dôkazom toho, že problém je z  $NP \setminus P$ . Takto nám pojem NP-úplnosti poskytuje možnosť alternatívneho "dôkazu" toho, že problém nie je prakticky riešiteľný.

Existuje aj iná definícia NP-úplnosti, s ktorou sa stretávame v prípade problémov, ktoré nie sú rozhodovacie.

**Definícia 7.3** *Problém  $L_0$  z  $NP$  je NP-úplný, ak z existencie algoritmu polynomiálnej zložitosti  $T(n)$  riešiaceho  $L_0$  vyplýva existencia algoritmu zložitosti  $p_L(T(n))$  pre každý problém  $L \in NP$ , pričom  $p_L$  je polynóm, ktorý závisí od  $L$ .*

Pri dokazovaní NP-úplnosti robí problém najmä dôkaz toho, že problém je NP-ťažký. Tu využijeme tranzitivitu relácie "byť polynomiálne redukovateľný".

*NP-úplnosť redukciou*

Nech problém  $L_0 \in NP$  je NP-úplný. Potom ho môžeme využiť pri dôkaze NP-úplnosti problému  $L$  nasledovne:

1. ukážeme, že  $L \in NP$
2. ukážeme, že  $L_0$  je polynomiálne transformovateľný na  $L$ ; toto dokazuje polynomiálnu redukovateľnosť ľubovoľného  $L'$  na  $L$  (prečo?)

K použitiu tohto prístupu však potrebujeme nejaký problém, o ktorom už vieme, že je NP-úplný. NP-úplnosť prvého problému musíme dokázať podľa definície.

## 7.2 NP-úplnosť problému splniteľnosti BF

Hlavným výsledkom tejto časti je Cookova veta, ktorá o probléme splniteľnosti boolovskej formuly dokáže, že je NP-úplný.

**Definícia 7.4** Boolovskou formulou (BF) nazveme výrazy

- $x, \neg x$
- ak  $p, q$  sú boolovské formuly, tak aj  $(p \vee q), (p \wedge q), \neg p$  sú boolovské formuly
- iné boolovské formuly nie sú

Nech  $BF$  je Boolovská formula  $n$  premenných  $x_1, \dots, x_n$ ; označujeme  $BF(x_1, \dots, x_n)$ . Hovoríme, že  $BF$  je splniteľná, ak existuje také priradenie hodnôt  $0, 1$  premenným  $x_1, \dots, x_n$ , pri ktorom  $BF$  nadobúda hodnotu  $1$

### Problém splniteľnosti BF

**Vstup:** Boolovská formula  $BF$ , resp. reťazec, ktorý ju kóduje

**Výstup:**  $1$ , ak je formula splniteľná  
 $0$  inak

Podľa potreby a kontextu bude  $SAT$  označovať alebo problém splniteľnosti BF alebo triedu splniteľných BF.

**Veta 7.2 (Cook)** *Problém splniteľnosti BF je NP-úplný*

**Dôkaz:** Príslušnosť problému splniteľnosti do NP ukážeme konštrukciou NTS, ktorý ho rieši.

- nech vstupom je  $BF(x_1, \dots, x_n)$ ; nech  $m$  označuje dĺžku vstupu
- DTS uhádne priradenie hodnôt  $\alpha_1, \dots, \alpha_n$  premenným  $x_1, \dots, x_n$  (prechádzaním po vstupnej páske si na pracovnú pásku zapisuje premenné a im uhádnuté hodnoty; časová zložitosť  $O(m^2)$ )
- dosadí uhádnuté priradenie hodnôt  $\alpha_1, \dots, \alpha_n$  do  $BF$  (prechádzaním po vstupnej páske opisuje na druhú pracovnú pásku BF zo vstupu, pričom namiesto jednotlivých premenných píše hodnoty; časová zložitosť  $O(m^2)$ )
- vyhodnotením  $BF$  s dosadenými hodnotami overí, či  $BF(\alpha_1, \dots, \alpha_n) = 1$ ; časová zložitosť  $O(m^2)$

$L \in NP \Rightarrow L$  je **polynomiálne redukovateľný na SAT** K dôkazu tejto časti treba skonštruovať DTS polynomiálnej zložitosti, ktorý pri vstupe  $w$  v čase polynomiálnom skonštruuje  $BF$  tak, že  $w \in L \Leftrightarrow BF \in SAT$ . Ak pri konštrukcii DTS využijeme len tie vlastnosti/znalosti o jazyku  $L$ , ktoré sú spoločné všetkým jazykom z  $NP$ , bude táto konštrukcia platná pre všetky jazyky z  $NP$ .

Ak  $L \in NP$ , potom existuje NTS  $M$  rozpoznávajúci  $L$ ;  $L = L(M)$ . O NTS  $M$  môžeme bez ujmy na všeobecnosti predpokladať:

- $NTSM$  je jednopáskový
- vstupná abeceda  $\Sigma = \{0, 1\}$
- abeceda symbolov  $\Gamma = \{1, 2, \dots, s\}$ ; pritom predpokladáme, že (napr)  $1$  označuje B (blank)
- množina stavov je  $K = \{1, 2, \dots, q\}$ ; nech  $1$  je počiatkový stav,  $q$  koncový akceptujúci
- časová zložitosť stroja  $M$  je zhora ohraničená polynómom  $p(n)$

O výpočte  $C = C_1, C_2, \dots, C_T$  NTS  $M$  môžeme bez ujmy na všeobecnosti predpokladať, že

- je dĺžky *presne*  $p(n)$
- každá konfigurácia je veľkosti  $p(n)$  - uvažujeme teda aj prípadne "blanky"

Booleovská formula  $BF_w$  vytvorená DTS k vstupnému slovu  $w$  (pri znalosti popisu NTS  $M$ ) bude používať tri skupiny premených. Ak zafixujeme nejaký konkrétny výpočet NTS  $M$   $C = C_1, C_2, \dots, C_{p(n)}$ , možno sa na tieto premenné pozerať ako na predikáty.

$C(i, j, t)$ ,	$1 \leq i \leq p(n), 1 \leq j \leq s,$ $0 \leq t \leq p(n)$	?je pravda, že vo výpočte $C$ je v čase $t$ na $i$ -tom políčku symbol $j$ ?
$S(k, t)$ ,	$1 \leq k \leq q, 0 \leq t \leq p(n)$	?je pravda, že vo výpočte $C$ je v čase $t$ stroj v stave $q$ ?
$H(i, t)$ ,	$1 \leq i \leq p(n), 0 \leq t \leq p(n)$	?je pravda, že vo výpočte $C$ je v čase $t$ hlava na $i$ -tom políčku?

Máme tak  $O(p^2(n))$  premenných, na zápis každej z nich stačí priestor  $O(\log n)$ .

Nech  $Q_0, Q_1, \dots, Q_{p(n)}$  je popis postupnosti konfigurácií. Tento popis je korektným popisom akceptujúceho výpočtu, ak platí nasledujúcich 7 podmienok:

1.  $Q_0$  je počiatočná konfigurácia
2. V každom čase je hlava na práve jednom políčku
3. V každom čase je stroj práve v jednom stave
4. V každom čase je na každom políčku pásky práve jeden symbol
5. Mení sa len to políčko, na ktorom je nastavená hlava
6. Zmena sa deje podľa prechodovej funkcie
7. Posledná konfigurácia je akceptujúca

Teraz popíšeme výslednú formulu  $BF_w$ . Táto vznikne ako logický súčin formúl ABCDEFG. Pri konštrukcii týchto podformulí využijeme predikát

$$U(y_1, y_2, \dots, y_n) = (y_1 \vee y_2 \vee \dots \vee y_n) \cdot \prod_{i \neq j} (\neg y_i \vee \neg y_j)$$

ktorý nadobúda hodnotu 1 práve vtedy, keď *práve jedna* z premenných  $y_1, \dots, y_n$  nadobúda hodnotu 1. Uvedomme si, že zápis  $U(y_1, \dots, y_n)$  je len označenie formuly, ktorá používa  $O(n^2)$  premenných a symbolov.

### K 1. $Q_0$ je počiatočná konfigurácia

$$A = S(1, 0) \wedge H(1, 0) \wedge \prod_{1 \leq i \leq n} C(i, w_i, 0) \wedge \prod_{n < i \leq p(n)} C(i, 1, 0)$$

**K 2. V každom čase je hlava na práve jednom políčku** Zafixujme čas  $t$ . Potom

$$B_t = U(H(1, t), \dots, H(p(n), t))$$

Keďže podmienka má platiť v každom časovom okamihu,

$$B = \prod_{0 \leq t \leq p(n)} B_t$$

**K 3. V každom čase je stroj práve v jednom stave**

$$C = \prod_{0 \leq t \leq p(n)} U(S(1, t), \dots, S(q, t))$$

**K 4. V každom čase je na každom políčku pásky práve jeden symbol**  
Zafixujme najprv čas  $t$  a políčko  $i$

$$D_{i,t} = U(C(i, 1, t), \dots, C(i, s, t))$$

Podmienka má platiť v každom časovom okamihu a na každom políčku, preto

$$D = \prod_{\substack{1 \leq i \leq p(n) \\ 0 \leq t \leq p(n)}} D_{i,t}$$

**K 5. Mení sa len to políčko, na ktorom je nastavená hlava**

To znamená, že alebo je obsah políčka v dvoch po sebe idúcich časových okamihoch rovnaký, alebo na ňom bola nastavená hlava. Zafixujme najprv čas, políčko aj symbol

$$E_{i,j,t} = (C(i, j, t) \equiv C(i, j, t+1)) \vee H(i, t)$$

Podmienka má platiť v každom čase (pre každé políčko a symbol)

$$E = \prod_{\substack{1 \leq i \leq p(n) \\ 0 \leq t \leq p(n) \\ 1 \leq j \leq s}} E_{i,j,t}$$

**K 6. Zmena sa deje podľa prechodovej funkcie**

Zafixujme čas  $t$ , políčko  $i$ , symbol  $j$  a stav  $k$ . Tieto štyri hodnoty spolu alebo súvisia – v čase  $t$  je stroj v stave  $k$ , hlavu má na políčku  $i$  a na tomto políčku je symbol  $j$  alebo spolu nesúvisia. Nech

$$\delta(j, k) = \{(j_1, k_1, pos_1), \dots, (j_{m(j,k)}, k_{m(j,k)}, pos_{m(j,k)})\}$$

Potom

$$F_{i,j,k,t} = \neg C(i, j, t) \vee \neg S(k, t) \vee \neg H(i, t) \vee \sum_{1 \leq l \leq m(j,k)} C(i, j_l, t+1) \wedge H(i+pos_l, t+1) \wedge S(k_l, t+1)$$

Podmienka platí pre všetky hodnoty  $i, j, k, t$

$$F = \prod_{\substack{1 \leq i \leq p(n) \\ 0 \leq t \leq p(n) \\ 1 \leq j \leq s, 1 \leq k \leq q}} F_{i,j,k,t}$$

**K 7. Posledná konfigurácia je akceptujúca**

Pri platnosti predchádzajúcich podmienok to znamená, že posledný stav má byť akceptujúci

$$G = S(q, p(n))$$

Výstupom *DTS* je teda výsledná formula  $BF_w = A \wedge B \wedge C \wedge D \wedge E \wedge F \wedge G$ . Vzhľadom k tvaru podformúl  $A, B, C, D, E, F, G$  je zrejmé, že časová zložitosť *DTS* je polynomiálna vzhľadom na veľkosť výslednej  $BF_w$ . Sústredíme sa preto len na veľkosť  $BF_w$ .

$$\begin{aligned} A & O(p(n) \log n) \\ B & O(p^3(n) \log n) \\ C & O(q^2 p(n) \log n) \\ D & O(s^2 p(n) \log n) \\ E & O(p^2(n) s \cdot \log n) \\ F & O(p^2(n) s \cdot q \cdot M \cdot \log n), \text{ kde } M = \max\{m(i, j)\} \\ G & O(\log n) \end{aligned}$$

Výsledná veľkosť  $BF_w$  je  $O(p^3(n) \log n)$ . Ešte ostáva ukázať, že  $w \in L \Leftrightarrow BF_w \in SAT$ .

$$w \in L$$

$$\Downarrow$$

$$\exists \text{ akceptujúci výpočet } Q = Q_0, Q_1, \dots, Q_{p(n)}$$

$$\Downarrow$$

priradenie hodnôt premenným  $C(i, j, t), S(k, t), H(i, t)$ , podľa predpisu

$C(i, j, t) = 1 \Leftrightarrow$  je pravda, že vo výpočte  $Q$  je na  $i$ -tom políčku v čase  $t$  symbol  $j$

$S(k, t) = 1 \Leftrightarrow$  je pravda, že vo výpočte  $Q$  je v čase  $t$  stroj v stave  $q$

$H(i, t) = 1 \Leftrightarrow$  je pravda, že vo výpočte  $Q$  je v čase  $t$  hlava na  $i$ -tom políčku

$$\text{zabezpečuje, že } BF_w(C(i, j, t), S(k, t), H(i, t)) = 1$$

□

Keď že vytvorenú formulu  $BF_w$  vieme v polynomiálnom čase previesť na formulu v tvare *KNF*, dostávame nasledujúci dôsledok.

**Dôsledok 7.3** *Problém splniteľnosti formuly v tvare KNF je z NP.*

### 7.3 Niektoré NP-úplné problémy

Keď už máme NP-úplný problém, metódou redukcie ukážeme NP-úplnosť aj o niektorých ďalších.

#### Problém 3 splniteľnosti

**Vstup:** formula  $3BF$  v tvare  $3KNF = F_1 \wedge F_2 \wedge \dots \wedge F_q$ ,  $F_i = x_{i1}^{\sigma_{i1}} \vee x_{i2}^{\sigma_{i2}} \vee x_{i3}^{\sigma_{i3}}$

**Výstup:**  $1 \Leftrightarrow 3BF \in SAT$

#### Problém k-kliky

**Vstup:**  $G = (V, E)$ ,  $k \in \mathbb{N}$

**Výstup:**  $1 \Leftrightarrow G$  obsahuje úplný podgraf o  $k$  vrcholoch

**Problém k-pokrytia****Vstup:**  $G = (V, E)$ ,  $k \in \mathbb{N}$ **Výstup:**  $1 \Leftrightarrow$  ak existuje množina vrcholov  $S$ ,  $S \subseteq V$ , mohutnosti  $k$  tak, že  $\forall (u, v) \in E : (u \in S \text{ alebo } v \in S)$ **Problém k-zafarbiteľnosti****Vstup:**  $G = (V, E)$ ,  $k \in \mathbb{N}$ **Výstup:**  $1$  ak množinu vrcholov  $V$  vieme zafarbiť  $k$  farbami tak, že žiadna hrana nemá oba konce rovnakej farby.**Problém HK****Vstup:**  $G = (V, E)$ **Výstup:**  $1 \Leftrightarrow G$  obsahuje hamiltonovskú kružnicu (jednoduchý cyklus prechádzajúci cez každý vrchol grafu)**Veta 7.4** *Problém 3-splniteľnosti je NPÚ.***Dôkaz:** Tvrdenie dokazujeme redukciami z problému splniteľnosti formuly v tvare KNF.**3-Splniteľnosť**  $\in NP$  vlastne netreba dokazovať, pretože všeobecný problém splniteľnosti je z  $NP$ .**Polynomiálna redukcia KNF splniteľnosti na 3 splniteľnosť:** Nech KNF je formula v tvare KNF. Bez ujmy na všeobecnosti môžeme predpokladať, že je to formula tvaru  $(x_1 \vee \dots \vee x_n)$ . Uvažujme formulu

$$3BF = (x_1 \vee x_2 \vee y_1) \wedge (\overline{y_1} \vee x_3 \vee y_2) \wedge \dots \wedge (\overline{y_{i-2}} \vee x_i \vee y_{i-1}) \wedge \dots \wedge (\overline{y_{n-3}} \vee x_{n-1} \vee x_n)$$

kde  $y_j$  sú nové premenné. Túto formulu zrejme na TS vytvoríme v čase polynomiálnom od veľkosti pôvodnej formuly BF.**BF**  $\in SAT$  Nech  $\alpha = (\alpha_1, \dots, \alpha_n)$  je spĺňajúci vektor hodnôt, na ktorom  $BF(\alpha) = 1$ . Potom existuje také  $i$ , že v  $\alpha$  je  $x_i = 1$ . Definujme vektor hodnôt

$$\beta \text{ premenných } y_1, \dots, y_{n-3} \begin{cases} y_j = 1 & \text{pre } j \leq i-2 \\ y_j = 0 & \text{pre } i-2 < j \leq n-3, \end{cases}$$

Potom  $3BF(\alpha, \beta) = 1$ .**3BF**  $\in SAT$  Nech  $\alpha = (\alpha_1, \dots, \alpha_n)$  je vektor hodnôt, na ktorom  $3BF(\alpha) = 1$ .  $3BF \rightarrow BF$  Stačí ukázať, že existuje  $i$  také, že pre  $\alpha = \alpha_1, \dots, \alpha_n$ ,  $i = 1$ . Postupujeme sporom. Nech by  $x_i = 0$  pre každé  $i$ . Keďže  $3BF(\alpha) = 1$ , musí platiť:

$$y_{n-3} = 0 \Rightarrow y_{n-2} = 0 \Rightarrow \dots \Rightarrow y_1 = 0$$

To ale znamená, že  $(x_1 \vee x_2 \vee y_1) = 0$ , čo je spor s predpokladom, že  $3BF(\alpha) = 1$ .

□

**Veta 7.5** *Problém k-kliky je NPÚ.*

**Dôkaz:** Tvrdenie dokazujeme redukciovou z problému splniteľnosti formuly v tvare KNF. Časť **problém k-kličky je z NP** prenechávame čitateľovi.

Redukcia spočíva v dvoch krokoch - k vstupnej formule  $F = F_1 \wedge F_2 \wedge \dots \wedge F_q$  zostrojíme v polynomiálnom čase graf  $G = (V, E)$ , o ktorom dokážeme, že obsahuje  $q$ -kličky práve vtedy, keď formula  $F$  je splniteľná.

**Konštrukcia grafu G** Nech  $F = F_1 \wedge F_2 \wedge \dots \wedge F_q, F_i = x_{i1} \vee x_{i2} \vee \dots \vee x_{ik(i)}$ .  $V = \{[i, j] \mid 1 \leq i \leq q, 1 \leq j \leq k(i)\}$ . Prvá zložka ukazuje na  $i$ -tu elementárnu disjunkciu, druhá zložka na literál na  $j$ -tej pozícii.

$E = \{([i, j], [k, l]) \mid i \neq k, x_{ij} \neq \neg x_{kl}\}$  To znamená

$$([i, j], [k, l]) \in E, x_{ij} = x_m^{\sigma_m}, x_{kl} = x_t^{\sigma_t} \quad m = t \Rightarrow \sigma_m = \sigma_t$$

Je zrejmé, že tento popis vieme na DTS vytvoriť v polynomiálnom čase.

$F \longrightarrow G$

**F je splniteľná** Nech formula  $F$  je splniteľná. Potom existuje súbor hodnôt  $\alpha$ ,  $F(\alpha) = 1$ . Nech  $x_{i,mi}$  je ten literál elementárnej disjunkcie  $F_i$ , ktorý sa vyhodnocuje na 1. Tvrdíme, že množina vrcholov  $\{[i, mi], 1 \leq i \leq q\}$  tvorí kličku v grafe  $G$ . K dôkazu stačí overiť, že  $\forall i \neq j$  tvorí dvojica vrcholov  $[i, mi], [j, mj]$  hranu v grafe  $G$ . Nech by existovali také  $i \neq j$ , že  $([i, mi], [j, mj]) \notin E$ . Keďže  $i \neq j$ , znamená to, že  $x_{i,mi} = \neg x_{j,mj}$ . To je ale v spore s faktom, že  $x_{i,mi} = x_{j,mj} = 1$

$G \longrightarrow F$

**G obsahuje q-kličky** Nech  $q$ -kličky tvorí množina vrcholov  $\{[i, mi] \mid 1 \leq i \leq q\}$ . Vytvoríme dve množiny premenných

$$S1 = \{y \mid y = x_{i,mi}, y \text{ je premenná}, 1 \leq i \leq q\}$$

$$S0 = \{y \mid y = \neg x_{i,mi}, y \text{ je premenná}, 1 \leq i \leq q\}$$

Sporom ukážeme, že  $S1 \cap S0 = \emptyset$ . Ak by  $\exists i \neq j$  také, že  $x_{i,mi} = y = \neg x_{j,mj}$ , potom by platilo, že  $([i, mi], [j, mj]) \notin E$ .

Potom pre vektor hodnôt  $\alpha$ , ktorý vznikne tak, že  $y = h$  ak  $y \in Sh$ ,  $h = 0, 1$  platí:  $F(\alpha) = 1$

□

**Cvičenie 7.1** Redukciou z problému  $k$ -kličky dokážte, že problém  $k$ -pokrytia je NPÚ.

**Veta 7.6** Problém  $k$ -zafarbiteľnosti je NPÚ.

**Dôkaz:** Tvrdenie dokazujeme redukciovou z problému 3splniteľnosti. To, že problém  $k$ -zafarbiteľnosti patrí do NP prenechávame čitateľovi.

Redukciu spravíme v dvoch krokoch - k danej vstupnej formule  $F = F_1 \wedge \dots \wedge F_t$  nad premennými  $x_1, \dots, x_n$  zostrojíme graf  $G = (V, E)$ , o ktorom ukážeme, že  $F$  je splniteľná práve vtedy keď  $G$  je  $(n+1)$ -zafarbiteľný.

*konštrukcia G*

Graf  $G$  budeme konštruovať tak, aby sme vynútili použitie  $n$  farieb (úplný graf na  $n$  vrcholoch) a aby stačila jedna ďalšia farba práve vtedy, ak je formula splniteľná. Farbenie touto novou farbou bude odpovedať priradeniu hodnoty 0 príslušnej premennej.

$$V = \{x_i, \neg x_i, v_i, 1 \leq i \leq n\} \cup \{F_i, 1 \leq i \leq t\}$$

$$E = \{(v_i, v_j) \mid i \neq j\} \cup \\ \{(v_i, x_j), (v_i, \neg x_j) \mid i \neq j\} \cup \\ \{(x_i, \neg x_i)\} \cup \\ \{(x_i, F_j) \mid x_i \text{ nie je termom } F_j\} \cup \\ \{(\neg x_i, F_j) \mid \neg x_i \text{ nie je termom } F_j\}$$

Všimnime si, že vrcholy  $v_1, \dots, v_n$  tvoria úplný podgraf, preto na ich zafarbenie potrebujeme  $n$  farieb. Nech teda  $v_i$  je zafarbené  $i$ -tou farbou.

Keďže oba vrcholy  $x_i, \neg x_i$  sú spojené s každým  $v_j, j \neq i$ , môžeme pri farbení vrcholov  $x_i, \neg x_i$  používať  $i$ -tu farbu. Navyše je ale každý vrchol  $x_i$  spojený s vrcholom  $\neg x_i$ , preto potrebujeme novú farbu – nazvime ju  $s$ . Takže z dvojice  $x_i, \neg x_i$  je jeden vrchol zafarbený  $i$ -tou farbou a druhý farbou  $s$ . Uvedomme si, že ak chceme graf farbiť minimálnym počtom farieb, je popísané farbenie "jednoznačné".

Ostáva farbenie vrcholov/termov. Čo vieme o  $F_j$ ?  $F_j$  je elementárna disjunkcia troch termov. Ak teda  $n \geq 4$ , pre každé  $j$  existuje  $i(j)$  také, že  $F_j$  je spojený aj s  $x_{i(j)}$  aj s  $\neg x_{i(j)}$ . To vylučuje použitie farby  $s$  na farbenie vrchola  $F_j$ .

Ukážeme, že **pri farbení vrcholov  $F_j$  nepotrebujeme ďalšiu farbu práve vtedy, ak  $F$  je splniteľná formula.**

Nech  $F_j$  obsahuje literál  $y$ , pričom  $\neg y$  je zafarbený farbou  $s$ . Potom  $F_j$  nie je spojený so žiadnym iným vrcholom, ktorý má rovnakú farbu ako  $y$  ( $y$  má  $i$ -tu farbu - rovnako ako  $v_i$ , ktoré je spojené s každým ďalším  $x_r$ , resp.  $\neg x_r$ . Preto žiaden z vrcholov, s ktorými je spojený  $F_j$ , nemôže mať farbu ako  $v_i$ ). V takomto prípade môžeme  $F_j$  zafarbiť rovnakou farbou ako  $y$ . Ak budeme zafarbenie farbou  $s$  považovať za priradenie hodnoty 0 a zafarbenie farbou  $1, 2, \dots, n$  za priradenie hodnoty 1, dostávame

$F_j$  môže byť zafarbené bez použitia ďalšej farby

⇕

∃ priradenie  $(n + 1)$  farieb literálom tak, že  $\forall$  elementárna disjunkcia obsahuje literál  $y$  taký, že  $\neg y$  má priradenú farbu  $s$

⇕

ak možno priradiť hodnoty premenným tak, že  $\forall$  elementárna disjunkcia obsahuje  $y = 1$  ( $\neg y$  má farbu  $s$ ,  $\neg y = 0$ )

⇕

$F$  je splniteľná

□

**Veta 7.7** *Problém HK je NPÚ*

**Dôkaz:** Tvrdenie budeme opäť dokazovať redukciami - tentokrát z problému vrcholového pokrytia. Príslušnosť problému HK do NP nechávame čitateľovi ako cvičenie.

Redukciu problému spravíme v dvoch krokoch – k vstupnému neorientovanému grafu  $G = (V, E)$  a prirodzenému číslu  $k$  zostrojíme orientovaný graf  $G_D = (V_D, E_D)$ , o ktorom ukážeme, že  $G_D$  má HK práve vtedy, keď  $G$  má vrcholové pokrytie mohutnosti  $k$ .

$V_D = \{a_1, a_2, \dots, a_k\} \cup \{[v, e, b] \mid v \in V, e \in E, b \in \{0, 1\}, v \text{ incidentný s } e\}$  *konštrukcia  $G_D$*

$E_D$  : Ku každému vrcholu  $v_i \in V$  môžeme priradiť usporiadaný zoznam hrán  $f_{i1}, \dots, f_{ip(i)}$  s ním incidentných; pre vrchol  $v_i$  nech  $p(i)$  označuje počet hrán incidentných s  $v_i$ . Potom do  $E_D$  pridávame hrany

$\forall j, i \quad a_j \rightarrow [v_i, e_{i1}, 0], \quad e_{i1} \text{ je prvá na zozname pre } v_i$   
 $\quad \quad \quad [v_i, e_{ip(i)}, 1] \rightarrow a_j, \quad e_{ip(i)} \text{ je posledná na zozname pre } v_i$

Každá hrana  $(v_i, v_j) \in E$  spôsobí vznik podgrafu o 4 vrcholoch

$$\begin{array}{ccc} [v_i, e_{ij}, 0] & \Leftrightarrow & [v_j, e_{ji}, 0] & & A & \Leftrightarrow & B \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ [v_i, e_{ij}, 1] & \Leftrightarrow & [v_j, e_{ji}, 1] & & C & \Leftrightarrow & D \end{array}$$

*pokrytie*  $\longrightarrow$  *HK* Nech  $v_1, \dots, v_k$  tvoria pokrytie v  $G$ . Ukážeme, že v grafe  $G_D$  existuje HK. Uvažujme najprv kružnicu

$$K = \begin{array}{l} a_1, [v_1, f_{11}, 0], [v_1, f_{11}, 1], \dots, [v_1, f_{1p(1)}, 0], [v_1, f_{1p(1)}, 1], \\ a_2, [v_2, f_{21}, 0], \dots, [v_2, f_{2p(2)}, 1], \\ \dots \\ a_k, [v_k, f_{k1}, 0], \dots, [v_k, f_{kp(k)}, 1], a_1 \end{array}$$

Ak ostali nejaké nezaradené vrcholy  $[v_j, e_{ij}, 0], [v_j, e_{ij}, 1]$ , tak vrchol  $v_i$  je z pokrytia (prečo?). Vtedy modifikujeme  $K$  tak, že úsek

$$[v_i, e_{ij}, 0], [v_i, e_{ij}, 1]$$

nahradíme

$$[v_i, e_{ij}, 0], [v_j, e_{ij}, 0], [v_j, e_{ij}, 1], [v_i, e_{ij}, 1]$$

Týmto spôsobom zaradíme všetky doteraz nezaradené vrcholy a na záver bude  $K$  tvoriť HK.

*HK*  $\longrightarrow$  *pokrytie* Nech v  $G_D$  existuje HK  $K$ . Vrcholy  $a_1, \dots, a_k$  rozdeľujú  $K$  na  $k$  úsekov (kvôli jednoduchosti predpokladajme, že  $a_1, \dots, a_k$  je to poradie, v ktorom sa tieto vrcholy vyskytujú na  $K$ ). Vzhľadom k tomu, že ak vojdeme do vrchola  $A$  (obr. vyššie) je prechod štvoricou vrcholov  $A, B, C, D$  v HK možný jedine dvomi spôsobmi -  $ABCD$  alebo  $AD$ , definuje každý úsek medzi  $a_i$  a  $a_{i+1}$  vlastne jeden vrchol z pokrytia; každému takémuto úseku možno priradiť vrchol  $v_t \in V$  taký, že každý vrchol z tohto úseku je tvaru  $[v_t, e_{tj}, 0], [v_t, e_{tj}, 1]$  alebo  $[v_i, e_{tj}, 0], [v_i, e_{tj}, 1]$ . Týmto spôsobom HK  $K$  definuje v grafe  $G$  vrcholové pokrytie mohutnosti najvyšš  $k$ .

□