

## 11 Polynom. redukce a randomizované Turingovy stroje

### 11.1 Řešení příkladu z domácí přípravy.

1. Zkonstruujte polynomiální redukci problému existence hamiltonovské kružnice na problém existence hamiltonovské neorientované cesty.

Fakt, že se jedná o polynomiální redukci pečlivě zdůvodněte.

2. Ukažte, že

Problém nezávislých množin se polynomiálně redukuje na problém SAT.

Polynomiální redukci pečlivě popište a zdůvodněte.

**Výsledek.** Jedna z redukcí je tato:

Je dán prostý neorientovaný graf  $G = (V, E)$  bez smyček. Zkonstruujeme neorientovaný graf  $G' = (V', E')$  takto: Vybereme vrchol  $v \in V$ ; množina vrcholů je  $V' = V \cup \{a, b, c, d\}$  ( $a, b, c, d \notin V$ ). Množina hran je  $E' = E \cup \{\{x, b\} \mid \{x, v\} \in E\} \cup \{\{a, v\}, \{c, a\}, \{b, d\}\}$ .

Pak platí v  $G$  existuje hamiltonovská kružnice právě tehdy, když v  $G'$  existuje hamiltonovská neorientovaná cesta.

**11.2** Zkonstruujte polynomiální redukci problému CNF-SAT na problém nezávislých množin (v prostém neorientovaném grafu bez smyček).

**Výsledek.** Je dán neorientovaný graf  $G = (V, E)$  bez smyček a číslo  $k$ . Ptáme se, zda existuje v  $G$  nezávislá množina o alespoň  $k$  vrcholech.

Zkonstruujeme formuli  $\varphi$  v CNF takto:

Logické proměnné: pro každý vrchol  $v \in V$  zavedeme  $k$  logických proměnných  $x_v^1, \dots, x_v^k$ . Formulemi vyjádříme:

1. Pro každé  $i = 1, \dots, k$  je vybrán přesně jeden vrchol — formule  $\alpha$ .
2. Pro různé  $i, j$ ,  $i, j \in \{1, \dots, k\}$  jsou vybrané vrcholy různé — formule  $\beta$ .
3. Jestliže  $\{u, v\} \in E$ , pak nebyly do nezávislé množiny nebyly vybrány oba vrcholy  $u$  a  $v$  — formule  $\gamma$ .

Add 1)

$$\alpha = \bigwedge_{i=1}^k \left[ \left( \bigvee_{v \in V} x_i^v \right) \wedge \bigwedge_{u \neq v} (\neg x_i^u \vee \neg x_i^v) \right].$$

Add 2)

$$\beta = \bigwedge_{v \in V} \bigwedge_{i \neq j} (\neg x_v^i \vee \neg x_v^j).$$

Add 3)

$$\gamma = \bigwedge_{\{u,v\} \in E} \bigwedge_{i \neq j} (\neg x_u^i \vee \neg x_v^j).$$

Nyní je hledaná formule  $\varphi = \alpha \wedge \beta \wedge \gamma$ .

### 11.3 Problém $k$ -barevnosti, $k \geq 3$

*Vstup:* Prostý neorientovaný graf  $G$ .

*Otázka:* Má graf  $G$  obarvení  $k$  barvami?

Rozhodněte, zda je problém  $k$ -barevnosti  $\mathcal{NP}$  úplný.

**Výsledek.** Problém je  $\mathcal{NP}$  úplný, protože leží v  $\mathcal{NP}$  a polynomiálně se na něj redukuje problém třibarevnosti.

Redukce je např. tato: Vezměme neorientovaný graf  $G = (V, E)$ . Sestrojíme neorientovaný  $G' = (V', E')$ , kde  $V' = V \cup \{x_1, x_2, \dots, x_{k-3}\}$ ,  $x_1, x_2, \dots, x_{k-3} \notin V$ ,  $E' = E \cup \{\{v, x_i\} \mid v \in V, i \in \{1, 2, \dots, k-3\}\} \cup \{\{x_i, x_j\} \mid i \neq j, i, j \in \{1, 2, \dots, k-3\}\}$ .

Nyní  $G$  je třibarevný právě tehdy, když  $G'$  je  $k$ -barevný.

### 11.4 Problém podgrafu

*Vstup:* Jsou dány neorientované grafy  $G$  a  $H$ .

*Otázka:* Obsahuje graf  $G$  podgraf, který je izomorfní grafu  $H$ ?

Rozhodněte, zda je problém podgrafu  $\mathcal{NP}$  úplný.

**Výsledek.** Problém je  $\mathcal{NP}$  úplný, protože leží v  $\mathcal{NP}$  a polynomiálně se na něj redukuje např. problém existence hamiltonovské kružnice (problém hamiltonovské cesty, problém nezávislých množin, problém klik).

**11.5** Navrhněte RTM  $M$ , který se pro dané binární vstupní slovo  $w = a_1 a_2 \dots a_n$ ,  $n > 0$ , chová takto:

- Jestliže na druhé (náhodné) pásce je v prvním poli symbol 0, pak  $M$  zkontroluje, zda se symboly vstupního slova  $w$  na sudých místech shodují s obsahem druhého a dalšího pole náhodné pásky.

Přesněji, označme  $r_i$  obsah  $i$ -tého pole druhé (náhodné) pásky. RTM  $M$  skončí v koncovém stavu právě tehdy, když platí  $a_{2k} = r_{k+1}$  pro všechna  $k$  taková, že  $2k \leq n$ .

- Jestliže na druhé (náhodné) pásce je v prvním poli symbol 1, pak  $M$  zkontroluje, zda se symboly vstupního slova  $w$  na lichých místech shodují s obsahem druhého a dalšího pole náhodné pásky.

Přesněji, RTM  $M$  skončí v koncovém stavu právě tehdy, když platí  $a_{2k+1} = r_{k+2}$  pro všechna  $k$  taková, že  $2k+1 \leq n$ .

1. Pro každé binární slovo  $w$  spočítejte pravděpodobnost, že RTM  $M$  skončí v koncovém stavu.

2. Je pravda, že  $M$  zajišťuje některému jazyku, že leží ve třídě  $\mathcal{RP}$ ? Jestliže ano, pak který jazyk; jestliže ne, uveďte proč.

### Samostaná práce na příští cvičení

**11.6** Navrhněte RTM  $M$ , který se pro dané vstupní slovo  $w = a_1a_2 \dots a_n$ ,  $n > 0$ , nad abecedou  $\{a, b\}$  chová takto:

- Jestliže na druhé (náhodné) pásce je v prvním poli symbol 0, pak  $M$  zkontroluje, zda se jedná o slovo  $w$ , které obsahuje aspoň jedno  $a$  a aspoň jedno  $b$ .
  - Jestliže na druhé (náhodné) pásce je v prvním poli symbol 1, pak  $M$  zkontroluje, zda vstupní slovo  $w$  končí stejným symbolem jako začíná.
1. Pro každé slovo  $w$  spočítejte pravděpodobnost, že RTM  $M$  skončí v koncovém stavu.
  2. Je pravda, že  $M$  zajišťuje některému jazyku, že leží ve třídě  $\mathcal{RP}$ ? Jestliže ano, pak který jazyk; jestliže ne, uveďte proč.