Další NP-úplné problémy

Známe SAT, CNF, $3CNF$, k-$KLIKA$

. . . a ještě následující easy NP-úplný problém:

Existence Certifikátu ($CERT$)
Instance: M, x, t, kde M je DTS, x je řetězec, t číslo zakódované jako 1^t
Otázka: Existuje řetězec y s $\|y\| \leq t$, t.ž. M přijme $[x, y]$ v t krocích?

Věta

$CERT$ je NP-úplný.

Důkaz (část I.).

Ukážeme, že $CERT \in \mathrm{NP}$:
Nechť U je univerzální TS, jenž na vstup dostane $[M, x, y]$ a simuluje nad $[x, y]$ práci TS M. Tento stroj bude sloužit jako verifikátor pro $CERT$.

Pokud M přijme v t krocích, U přijme, v opačném případě zamítne.
Dá se ukázat, že bude stačit pouze $\mathcal{O}(t^2)$.

Každopádně stačí polynomiální čas.
$[M, x, t] \in CERT$ p.k. existuje y, pro nějž platí, že $|y| \leq t$ a U přijme $[M, x, 1^t, y]$. □

Důkaz (část II.).

$CERT$ je NP-těžký

Nechť $A \in \mathrm{NP}$, existuje tedy TS M (verifikátor pro A), který pracuje v polynomiálním čase, a polynom $p(n)$, pro které platí, že $x \in A$ p.k. existuje y, $|y| \leq p(|x|)$, t.ž. M přijme $[x, y]$.

Předpokládejme, že čas M je taky omezen $p(n)$.

Definujeme funkci $r : x \mapsto [M, x, p(|x|)]$.

Jistě je možno vyčíslovat ji v polynomiálním čase.

Ukážeme, že jde o redukci.

Pokud $x \in A$, existuje certifikát y délky omezené $p(|x|)$, t.ž. M přijme $[x, y]$.

M zastaví v čase $t = p(|x|)$, protože polynom p omezuje i délku výpočtu M nad $[x, y]$.

Podle definice problému $CERT$ tedy $[M, x, p(|x|)] \in CERT$.

Pokud $[M, x, p(|x|)] \in CERT$, podle definice $CERT$ to znamená, že existuje y, $|y| \leq p(|x|)$, pro nějž $M(x, y)$ přijme $p(|x|)$ krocích, a tedy $x \in A$.

□

NP-úplný problém – Vrcholové pokrytí

Vrcholové pokrytí (VP)
Instance: $[G, k]$, kde $G = (V, E)$ je graf a k je číslo.
Otázka: Tj. $\lvert S\rvert \leq k$ a $(\forall e \in E)[S \cap e \neq \emptyset]$.

Tj.: Existuje množina $S \subseteq V$, která obsahuje nejvýše k vrcholů a z každé hrany obsahuje alepoň jeden koncový vrchol?

Věta

VP *je* NP*-úplný.*

Důkaz (část I.).

$\mathrm{VP} \in \mathrm{NP}$ plyne z toho, že pro danou množinu S dokážeme ověřit v polynomiálním čase, jde-li o vrcholové pokrytí správné velikost.

VP je NP-těžký – ukážeme tak, že ukážeme $3\mathrm{CNF} \leq_{\mathrm{P}} \mathrm{VP}$.

Mějme tedy 3cnf-formuli $\phi = C_1 \wedge \cdots \wedge C_2$ s proměnnými $U = \{u_1, \ldots, u_n\}$. Ukážeme, jak k ní zkonstruovat graf $G = (V, E)$ a číslo k, pro něž bude platit, že v G existuje vrcholové pokrytí velikostí nejvýš k, právě když ϕ je splnitelná. □

Důkaz (část II.).

Pro každou proměnnou $u_i \in U$ definujeme podgraf $T_i = (V_i, E_i)$, kde

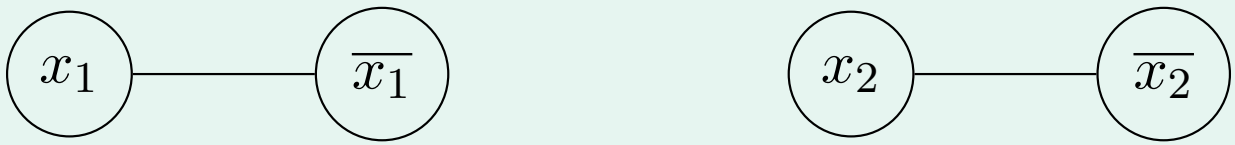
- $V_i = \{u_i, \overline{u_i}\}$
- $E_i = \{\{u_i, \overline{u_i}\}\}$

všimněte si: ve vrcholovém pokrytí musí být alespoň jeden z uzlů u_i a $\overline{u_i}$

□

Příklad

$$\phi = (x_1 \vee x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_2}) \wedge (\overline{x_1} \vee x_2 \vee x_2)$$



Důkaz (část III.)

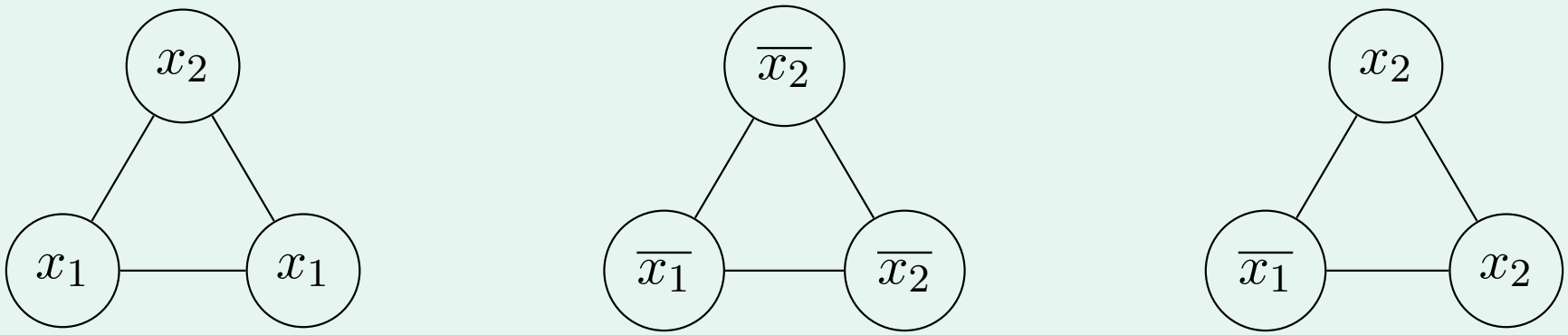
Pro každou klauzuli C_j, $j = 1, \ldots, m$ přidáme úplný podgraf o třech nových vrcholech, tedy trojúhelník $S_j = (V'_j, E'_j)$.

$$V'_j = \{a_1[j], a_2[j], a_3[j]\}$$
$$E'_j = \{\{a_1[j], a_2[j]\}, \{a_1[j], a_3[j]\}, \{a_2[j], a_3[j]\}\}$$

všimněte si: vrcholové pokrytí musí obsahovat alespoň dva vrcholy z V'_j.

Příklad

$$\phi = (x_1 \vee x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_2}) \wedge (\overline{x_1} \vee x_2 \vee x_2)$$



Důkaz (část IV.)

Podgrafy spojíme mezi sebou hranami, které spojují vrcholy pro literály s jejich výskyty v klauzulí.

Předpokládejme, že pro každé $j = 1, \ldots, m$ je klauzule $C_j = (x_j \vee y_j \vee z_j)$, kde x_j, y_j, z_j jsou literály (pozitivní nebo negativní).

Pak přidáme hrany z S_j do příslušných vrcholů literálů, tedy množinu hran:

$$E''_j = \{\{a_1[j], x_j\}, \{a_2[j], y_j\}, \{a_3[j], z_j\}\}$$

V naší konstrukci nakonec položíme $k = n + 2m$ a $G = (V, E)$, kde

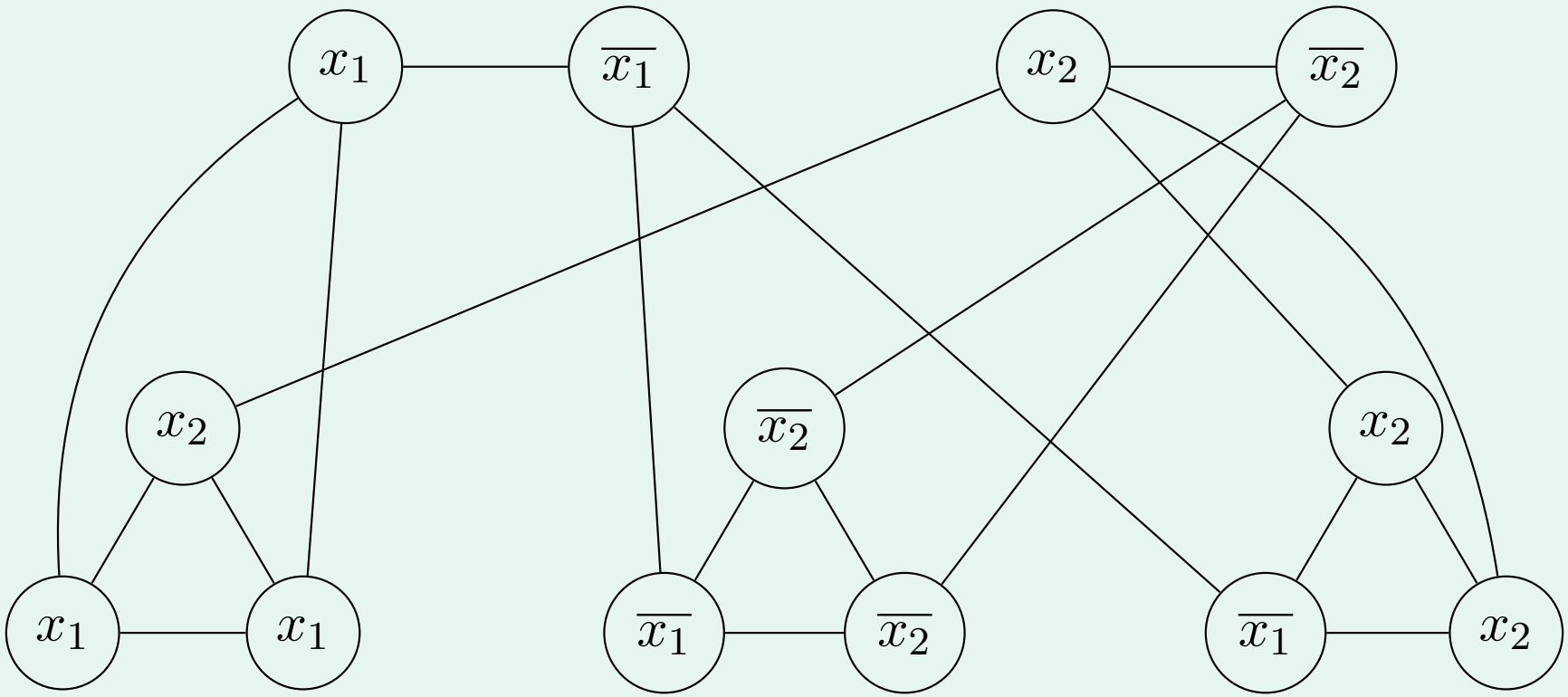
$$V = \left(\bigcup_{1 \le i \le n} V_i\right) \cup \left(\bigcup_{1 \le i \le m} V'_i\right)$$

$$E = \left(\bigcup_{1 \le i \le n} E_i\right) \cup \left(\bigcup_{1 \le i \le m} E'_i\right) \cup \left(\bigcup_{1 \le i \le n} E''_i\right)$$

Z popisu je zjevné, že ji lze zkonstruovat v polynomiálním čase.

Příklad

$$\phi = (x_1 \vee x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_2}) \wedge (\overline{x_1} \vee x_2 \vee x_2)$$



Důkaz (část V.)

Zbývá dokázat, že tato transformace je redukce.
Tj. že

$$\phi \text{ je splnitelná } \Leftrightarrow G \text{ má pokrytí } k \text{ vrcholy.}$$

Idea této části důkazu

Připomínka: Hledání ohodnocení, ve kterém je splnitelná cnf-formule $C_1 \wedge C_2 \wedge \cdots \wedge C_m$ je vlastně nalezení j-tice literálů $\langle l_1, l_2, \ldots, l_m \rangle$, t.ž.

(1) l_i je členem klauzule C_i,

(2) v m-tici se nevyskytuje žádná výroková proměnná jako pozitivní a negativní literál současně.

(1) je v G zajištěno výběrem dvojice uzlů v trojúhelnících: třetí –nevybraný – představuje literál zařazený do m-tice.
(2) je zajištěno provázáním přes dvojice.

Důkaz (část VII.)

„$\Leftarrow$“: Mějme G, které má vrcholové pokrytí $W \subseteq V$ velikosti $k = n + 2m$. W musí pokrýt alespoň jeden uzel z každého podgrafu T_i $i = 1, \ldots, n$ a alespoň dva vrcholy z každého trojúhelníku S_j $j = 1, \ldots, m$.

Musí tedy platit $|W| \geq n + 2m$. A protože současně $W \leq n + 2m$, musí ve skutečnosti platit, že W pokrývá právě jeden vrchol z každého T_i a právě dva vrcholy z každého S_i.

Definujeme ohodnocení $t : U \to \{0, 1\}$

$$t(u_i) = \begin{cases} 1 & u_i \in W, \\ 0 & \overline{u}_i \in W. \end{cases}$$

Tedy z každého T_i je ve W jeden vrchol, je v definici $t(u_i)$ vždy splněna právě jedna z podmínek, jde tedy o dobře definované ohodnocení.

Důkaz (část VIII.)

Nechť $C = (x_1 \vee y_j \vee z_j)$ je libovolná klauzule ϕ.

Množina W pokrývá dva vrcholy z trojúhelníku S_j, existuje tedy jeden vrchol, který není pokrytý.

Nechť je to BÚNO $a_1[j]$, protože hrana $\{a_1[j], x_j\}$ musí být pokryta, a tedy $x_j \in W$ a tedy hodnocení přiřadí x_j hodnotu 1.

Tedy

- pokud $x_j = u_i \in W$, platí $t(u_i) = 1$,
- pokud $x_j = \overline{u}_i \in W$, platí $t(u_i) = 0$.

V obou případech je literál x_j splněn ohodnocením t.

Protože to platí pro všechny klauzule, je t splňující ohodnocení ϕ.

Důkaz (část IX.)

„⇒“: Předpokládejme, že ϕ je splněná ohodnocením $t : U \to \{0, 1\}$ a definujme množinu

$$W = \{u_i \mid t(u_i) = 1\} \cup \{\overline{u}_i \mid t(u_i) = 0\}.$$

Množina obsahuje n vrcholů.

Mezi hranami z E''_j vedoucími z každého trojúhelníku S_j musí být alespoň jedna pokrytá nějakým vrcholem z W, neboť t je splňující ohodnocení, které tedy splňuje některý literál z klauzule C_j.

Z každého trojúhelníku stačí tedy vybrat dva vrcholy tak, aby byly pokryty jak hrany z E_j, tak hrany z E''_j. Přidáním těchto vrcholů do W dostaneme vrcholové pokrytí celého grafu velikosti $k = n + 2m$.

Hamiltonovská kružnice v grafu (HAMILTON)

Hamiltonovská kružnice v grafu (HAMILTON)
Instance: $[G, k]$, kde $G = (V, E)$.
Otázka: Existuje v grafu G cyklus vedoucí přes všechny vrcholy?

Věta

HAMILTON *je* NP*-úplný.*

Důkaz (část I.)

$\mathrm{HAMILTON} \in \mathrm{NP}$: zjevné, máme-li k dispozici pořadí vrcholů, snadno v polynomiálním čase ověříme, tvoří-li hamiltonovskou kružnici.

$\mathrm{HAMILTON}$ **je NP-těžký**: ukážeme jako $VP \leq_p \mathrm{HAMILTON}$.

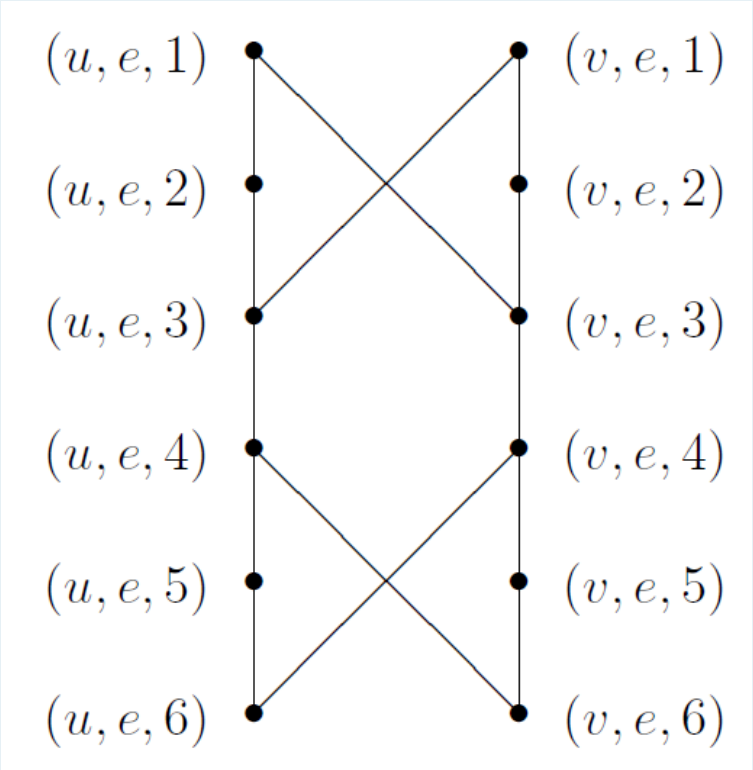
Uvažujme instanci vrcholového pokrytí $[G, k]$.
Zkonstruujeme nový graf $G' = (V', E')$, pro který bude platit, že G' existuje hamiltonovská kružnice p.k. existuje vrcholové pokrytí velikosti k.

Pro každou hranu $e = \{u, v\} \in E$ definujeme podgraf $G'_e = (V'_e, E'_e)$, kde

$$
\begin{aligned}
V'_e &= \{(u, e, i), (v, e, i) \,|\, 1 \leq i \leq 6\} \text{ a} \\
E'_e &= \{\{(u, e, i), (u, e, i+1)\} \,|\, 1 \leq i \leq 5\}\} \\
&\quad \cup \{\{(v, e, i), (v, e, i+1)\} \,|\, 1 \leq i \leq 5\}\} \\
&\quad \cup \{\{(u, e, i), (v, e, 3)\}, \{(u, e, 3), (v, e, 1)\}, \\
&\qquad \{(u, e, 4), (v, e, 6)\}, \{(u, e, 6), (v, e, 4)\}\}\,.
\end{aligned}
$$

Důkaz (část II.)

Graf G'_e je zobrazen tu:



Jediné vrcholy k nimž v další konstrukci připojíme další hrany budou $(u, e, 1), (u, e, 6), (v, e, 1), (v, e, 6)$, což zaručí, že hamiltonovská kružnice musí vstoupit i vystoupit z podgrafu jedním z těchto 4 vrcholů.

Důkaz (část III.)

Jsou jen 3 způsoby jak pokrýt hranu e v G:

(I) Cesta vstoupí G'_e v $(u, e, 1)$, vystoupí $(u, e, 6)$ a mezitím projde všechny vrcholy (cesta je jednoznačně daná).

(II) Cesta vstoupí G'_e v $(v, e, 1)$, vystoupí $(v, e, 6)$ (symetricky s předchozím případem)

(III) kužnice do podgrafu vstoupí dvakrát, jednou projde „sloupec“ u a jednou projde „sloupec“ v.

všimněte si:

- vzhledem k tomu, že je graf neorentovaný, nezáleží na tom, jestli například v prvním případě vstoupí cesta do G'_e vrcholem $(u, e, 1)$ a vystoupí $(u, e, 6)$, nebo naopak.
- Pokud cesta vstoupí vrcholem $(v, e, 1)$, vystoupí vždy $(v, e, 6)$. Stejně tak pro u.

Důkaz (část IV.)

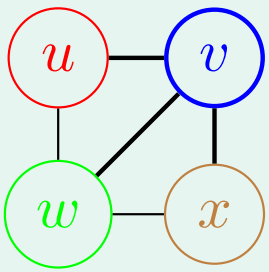
Do množiny vrcholů V' nového grafu G' přidáme ještě k vrcholů $a_1, \ldots, a_k$. Ty použijeme k výběru k vrcholů vrcholového pokrytí.

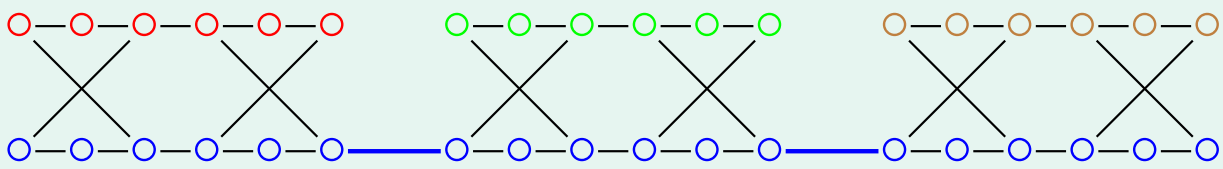
Zbývá popsat, jak spojíme jednotlivé podgrafy G'_e a nově přidané vrcholy a_i Pro každý vrchol $v \in V$ zapojíme jednotlivé grafy G'_e s $v \in e$ za sebe. Přesněji, označme si

- stupeň vrcholu v pomocí $\deg(v)$,
- hrany z G, v nichž se vyskytuje v pomocí $e_{v[1]}, \ldots, e_{v[\deg(v)]}$.

Nyní definujme $E'_v = \big\{\{(v, e_{v[i]}, 6), (v, e_{v[i+1]}, 1)\} \,|\, 1 \leq i < \deg(v)\big\}$.

Příklad



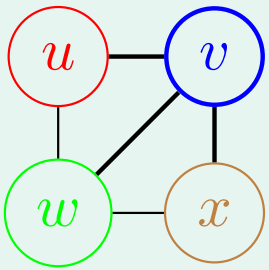


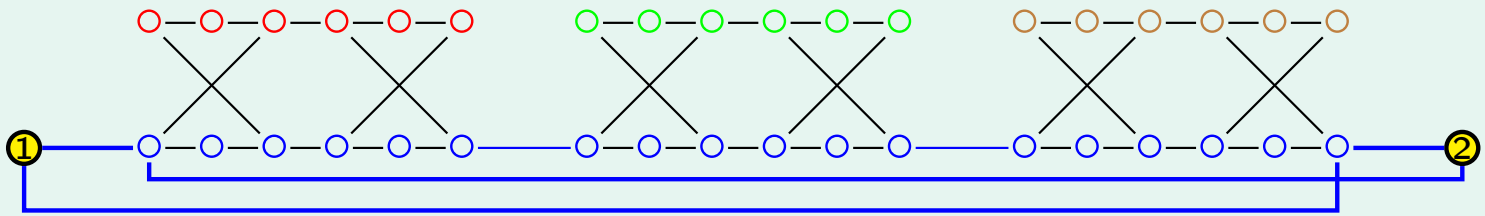
Důkaz (část V.)

Vrcholy na koncích této posloupnosti, tedy $(v, e_{v[1]}, 1)$ a $(v, e_{v[\deg(v)]}, 6)$ připojíme ke všem výběrovým vrcholům $a_1, \ldots, a_k$.

$$E''_v = \left\{ \{a_i, (v, e_{v[1]}, 6)\}, \{a_i, (v, e_{v[\deg(v)]}, 1)\} \mid 1 \leq i \leq k \right\}.$$

Příklad





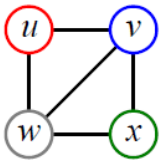
Důkaz (část VI.)

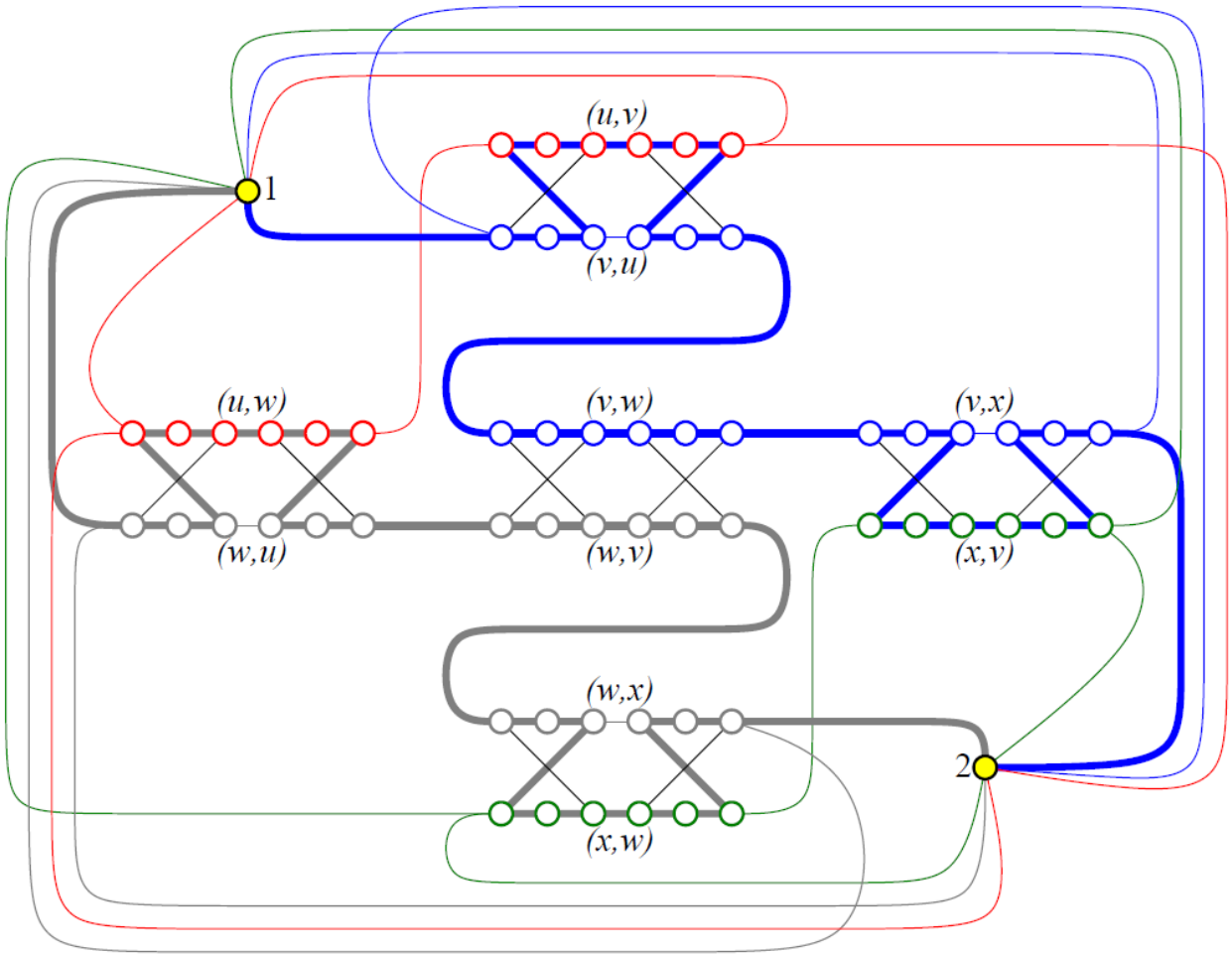
Konstruovaný graf $G' = (V', E')$ vznikne spojením popsaných částí:

$$V' = \{a_1, \ldots, a_k\} \cup \left(\bigcup_{e \in E} V'_e \right)$$

$$E' = \left(\bigcup_{e \in E} E'_e \right) \cup \left(\bigcup_{v \in V} E'_v \right) \cup \left(\bigcup_{v \in V} E''_v \right)$$

Tuto transformaci je zjevně možné provést v polynomiálním čase.


u
v
w
x


(u,v)
1
(v,u)
(u,w)
(v,w)
(v,x)
(w,u)
(w,v)
(x,v)
(w,x)
2
(x,w)

Důkaz (část VII.)

Ukážeme, že jde o redukci:
V G' existuje hamiltonovská kružnice daná pořadím vrcholů $u_1, \ldots, u_n$, kde $n = |V'|$.

Uvažme úsek této kružnice, který začíná a končí v některém z vrcholů $a_1, \ldots, a_k$, přičemž mezi tím žádným z nich neprochází. Nechť tento úsek BÚNO začíná v a_i a končí a_j.

Vrchol následující po a_i v ham. kružnici musí být $(v, e_{v[1]}, 1)$ pro nějaký vrchol $v \in V$.

Vejde-li ham. kružnice vrcholem $(v, e_{v[1]}, 1)$ do $G'_{e_{v[1]}}$, musí z něj vyjít vrcholem $(v, e_{v[1]}, 6)$. Odtud přejde do $(v, e_{v[1]}, 1)$, takto projde všechny grafy G'_e pro hrany e obsahující vrchol v až nakonec přejde z vrcholu $(v, e_{v[\deg(v)]}, 6)$ do a_j.

Důkaz (část VIII)

Definujeme množinu vrcholů

$$S = \{v \,\|\, (\exists i \in \{1, \ldots, k\}) \\ (\exists j \in \{1, \ldots, n\}) \\ [(u_j = a_i) \wedge (u_{(j+1 \bmod k)} = (v, e_{v[1]}, 1)]\}.$$

Tvrdíme, že jde o vrcholové pokrytí v grafu G, přičemž jeho velikost je k.

Nechť $e = \{u, v\}$ je libovolná hrana grafu G, protože $u_1, \ldots, u_n$ určuje pořadí vrcholů na hamiltonovské kružnici, musí projít i podgraf G'_e. Vejde-li do G'_e vrcholem $(u, e, 1)$, pak musí platit, že $u \in S$, podobně pokud vejde vrcholem $(v, e, 1)$, musí platit, že $v \in S$, tedy hrana e je pokryta.

Důkaz (část IX).

Naopak: S je VP velikosti k.
Můžeme uvažovat, že jde o množinu velkou přesně k.
Pokud je menší, doplníme do ní libovolné vrcholy tak, aby její velikost byla k.

Z popisu konstrukce plyne, jak pospojujeme jednotlivé podgrafy odpovídající hranám.

Předp. že $S = \{v_1, \ldots, v_k\} \subseteq V$.
Mezi vrcholy a_i a a_{i+1} (popř. a_1 pokud $i = k$) povedeme cestu mezi podgrafy G'_e pro $e = e_{v_i[1]}, \ldots, e_{v_i[\deg(v_i)]}$ v tomto pořadí.

Graf přitom projdeme způsobem (I) nebo (II). Pokud platí $e \subseteq S$, použijeme způsob (III).

Vzhledem k tomu žč S tvoří vrcholové pokrytí, projdeme takto všechny vrcholy grafu G' a vznikne tedy hamiltonovská kružnice. □

NP-úplný problém – Trojrozměrné párování

Trojrozměrné párování ($3DM$)

Instance: Množina $M \in X \times Y \times Z$, X, Y, Z jsou po dvou disjunktní množiny, z nichž každá obsahuje právě q prvků.

Otázka: Obsahuje M perfektní párování? Neboli, existuje množina $M' \subseteq M$, $|M'| = q$, trojice v níž obsažené jsou po dvou disjunktní?

Věta

$3DM$ je NP-úplný.

Důkaz:
$3DM \in NP$ opět snadné. Plyne to z toho, že pokud máme k dispozici množinu $M' \subseteq M$, dokážeme ověřit v polynomiálním čase, jde-li o párování velikosti q.

$3DM$ je NP-těžký: Ukážeme $CNF \leq_p 3DM$

Nechť $\phi = C_1 \wedge \cdots \wedge C_m$ je cnf-formule s proměnnými $U = \{u_1, \ldots, u_n\}$.

Sestrojíme instanci problému $3DM$, pro kterou bude platit, že v ní existuje perfektní párování, právě když ϕ je splnitelná.

Konstrukci rozdělíme na tři části:

- vytvoříme komponentu, která bude určovat, jakou hodnotu která proměnná dostane.
- vytvoříme komponentu, která bude zajišťovat propojení této hodnoty s klauzulemi, v nichž se tato proměnná vyskytuje.
- doplníme trojice tak, abychom dostali ke splňujícímu ohodnocení skutečně perfektní párování a naopak.

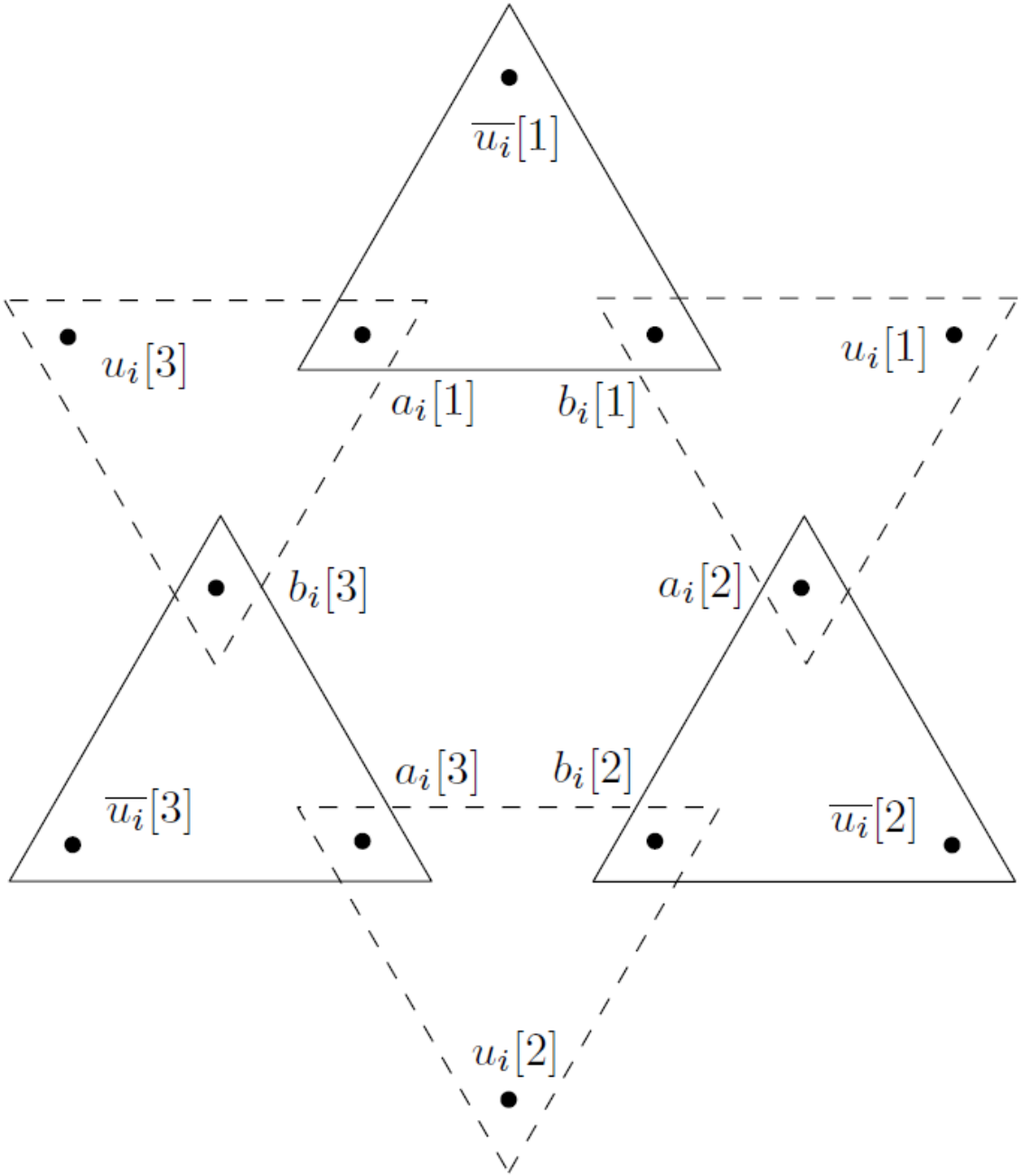
Nechť u_i je libovolná proměnná, za ni přidáme nové vnitřní prvky

- $a_i[1], \ldots, a_i[m]$ do X
- $b_i[1], \ldots, b_i[m]$ do Y

Do Z přidáme prvky $u_i[1], \ldots, u_i[m]$ a $\overline{u}_i[1], \ldots, \overline{u}_i[m]$.

Na těchto prvcích vytvoříme množiny trojic T_i^f a T_i^t takto:

$$T_i^t = \{(a_i[j], b_i[j], \overline{u}_i[j]) \mid 1 \leq j \leq m\}$$
$$T_i^f = \{(a_i[(j+1) \mod m], b_i[j], u_i[j]) \mid 1 \leq j \leq m\}$$
$$T = T_i^t \cup T_i^f$$


$\overline{u_i}[1]$
$u_i[3]$
$u_i[1]$
$a_i[1]$
$b_i[1]$
$b_i[3]$
$a_i[2]$
$a_i[3]$
$b_i[2]$
$\overline{u_i}[3]$
$\overline{u_i}[2]$
$u_i[2]$

Protože žádný z prvků $a_i[j]$ ani $b_i[j]$ se nebude vyskytovat v jiných trojicích, je tímto vynuceno, že perfektní párování musí obsahovat všechny trojice z T_i^t nebo všechny trojice z T_i^f.

- Pokud obsahuje trojice z T_i^t, znamená to, že žádná další nesmí obsahovat $\overline{u}_i$, tedy vynucujeme hodnotu 1 pro u_i.
- Pokud obsahuje trojice z T_i^f, vynucujeme hodnotu 0.

Za klauzuli C_j přidáme

- nový prvek $s_1[j]$ do množiny X,
- nový prvek $s_2[j]$ do množiny Y,

a množinu trojic

$$S_j = \{(s_1[j], s_2[j], u_i[j]) \mid u_i \in C_j\} \cup \{(s_1[j], s_2[j], \overline{u}_i[j]) \mid \overline{u}_i \in C_j\}$$

$$S_j = \{(s_1[j], s_2[j], u_i[j]) \mid u_i \in C_j\} \cup \{(s_1[j], s_2[j], \overline{u}_i[j]) \mid \overline{u}_i \in C_j\}$$

Prvky $s_1[j]$ a $s_2[j]$ se opět nebudou vyskytovat v jiných trojicích, díky tomu v perfektním párování musí být právě jedna trojice z množiny S_j.

Navíc pokud se trojice $(s_1[j], s_2[j], u_i[j])$ vyskytuje v perfektním párování, znamená to, že u $u_i[j]$ se nemůže vyskytovat v jiné trojici a to znamená, že v tomto párování jsou všechny trojice z T_I^t a žádná z T_i^f.

Podobně by to bylo, kdyby v perfektním párování byla trojice s negativním literálem.

Těmito trojicemi jsme ale schopni v párování pokrýt jen $mn + m$ prvků z $2mn$ prvků $u_i[j], \overline{u}_i[j], i = 1, \ldots, n, j = 1, \ldots, m$

- mn jsme pokryli pomocí T_i^t nebo T_i^f pro každé $i = 1, \ldots, n$
- m jsme pokryli pomocí trojic z S_j, $j = 1, \ldots, m$.

Zbývá tedy $2mn - (mn + m) = mn - m = m(n - 1)$ prvků, které nejsme schopni pokrýt (zatím).
Přidáme do

- Do X při dáme $g_1[k]$ pro $k = 1, \ldots, m(n - 1)$.
- Do Y při dáme $g_2[k]$ pro $k = 1, \ldots, m(n - 1)$.

Do M přidáme množinu trojic

$$G = \{(g_1[k], g_2[k], u_i[j]), (g_1[k], g_2[k], \overline{u}_i[j]) \mid 1 \leq k \leq m(n-1), 1 \leq i \leq n, 1 \leq$$

Tím je konstrukce dokončena.

Shrňme si to:

$$
\begin{aligned}
X &= \{a_i[j] \mid 1 \le i \le n, 1 \le j \le m\} \cup \\
&\quad \cup \{s_1[j] \mid 1 \le j \le m\} \\
&\quad \cup \{g_1[j] \mid 1 \le j \le m(n-1)\} \\
Y &= \{a_i[j] \mid 1 \le i \le n, 1 \le j \le m\} \cup \\
&\quad \cup \{s_1[j] \mid 1 \le j \le m\} \\
&\quad \cup \{g_1[j] \mid 1 \le j \le m(n-1)\} \\
Z &= \{u_i[j], \overline{u}_i[j] \mid 1 \le i \le n, 1 \le j \le m\} \\
M &= \left(\bigcup_{i=1}^{n} T_i\right) \cup \left(\bigcup_{i=1}^{n} S_i\right) \cup G
\end{aligned}
$$

Zjevně platí

- $M \subseteq X \times Y \times Z$,
- $|M| = 2mn + 3m + 2m^2n(n-1)$
- $|X| = |Y| = |Z| = 2mn$

Předpokládejme, že v M existuje perfektní párování M', na jehož základě zkonstruujeme ohodnocení t, které bude splňovat formuli ϕ.

Nechť i je libovolný index z $1, \ldots, n$. V M' jsou buď všechny trojice z T_i^t, nebo všechny trojice z T_i^f.

- pokud T_i^t, definujeme $t(u_i) := 1$,
- pokud T_i^f, definujeme $t(u_i) := 0$.

Nechť C_j je libovolná klauzule formule ϕ. Množina M' musí obsahovat právě jednu z trojic z S_j (je to jediná možnost, jak pokrýt $s_1[j]$ a $s_2[j]$ a dvě obsahovat nemůže, by tam byly $s_1[j]$ či $s_2[j]$ duplicitně).

Nechť tato trojice je $(s_1[j], s_2[j], u_i[j])$ pro nějaké $i = 1, \ldots, n$.
Znamená to, že u_i je proměnná vyskytující se jako pozitivní literál v klauzuli C_j. Navíc musí platit, že $u_i[j]$ se nemůže vyskytovat v žádné jiné trojici v M', proto M' obsahuje trojice z T_I^t a nikoli T_I^f a tedy $t(u_i) = 1$, čímž je klauzule C_j splněna.

podobně:
Nechť tato trojice je $(s_1[j], s_2[j], \overline{u}_i[j])$ pro nějaké $i = 1, \ldots, n$.
Znamená to, že u_i je proměnná vyskytující se jako negativní literál v klauzuli C_j. Navíc musí platit, že $\overline{u}_i[j]$ se nemůže vyskytovat v žádné jiné trojici v M', proto M' obsahuje trojice z T_I^f a nikoli T_I^t a tedy $t(u_i) = 0$, čímž je klauzule C_j splněna.

Nechť ϕ je splnitelná, zkonstruujeme perfektní párování následovně.
Nechť $e : U \to \{0, 1\}$ je ohodnocení splňující ϕ a nechť z_j označuje literál, který je v C_j tímto ohodnocením splněn pro $j = 1, \ldots, m$.
Pokud je takových literálů víc, vybereme prostě jeden z nich. Pak položíme:

$$M' = \left(\bigcup_{t(u_i)=1} T_i^t \right) \cup \left(\bigcup_{t(u_i)=0} T_i^f \right) \cup \left(\bigcup_{j=1}^{m} \{(s_1[j], s_2[j], z_j[j])\} \right) \cup G',$$

kde G' je množina vhodně vybraných trojic z G, které doplňují párování o pokrytí zbylých literálů. Není těžké ověřit, že tato definovaná množina M' tvoří perfektní párování M.

Loupežníci ($LOUP$)

Loupežníci ($LOUP$)

Instance: Množina prvků A a s každým prvkem $a \in A$ asociovaná cena (váha, velikost,...) $s(a) \in \mathbb{N}$.

Otázka: Lze rozdělit prvky z A na dvě poloviny se stejnou celkovou cenou? Přesněji, existuje množina $A' \in A$ taková, že

$$\sum_{a \in A'} s(a) = \sum_{a \in A \setminus A'} s(a)?$$

Věta

$LOUP$ je NP-úplný.

Důkaz

$LOUP \in NP$ – zase stejné, plyne to z toho, že zadanou množinu A' je snadné ověřit, zda obsahuje prvky poloviční ceny.

$LOUP$ je NP-těžký: Ukážeme $3DM \leq_p LOUP$.

Uvažujme instanci $3DM$, tedy množinu $M \subseteq X \times Y \times Z$, kde $|X| = |Y| = |Z| = q$.

Vytvoříme instanci $LOUP$, tedy množinu A a cenovou funkci $s : A \to \mathbb{N}$, pro něž bude platit, že M má perfektní párování, právě když prvky v A lze rozdělit na dvě části se stejnou cenou.
Předpokládejme, že

$$M = \{m_1, \ldots, m_k\}, X = \{x_1, \ldots x_q, \}Y = \{y_1, \ldots, y_q\}, Z = \{z_1, \ldots, z_q\}.$$

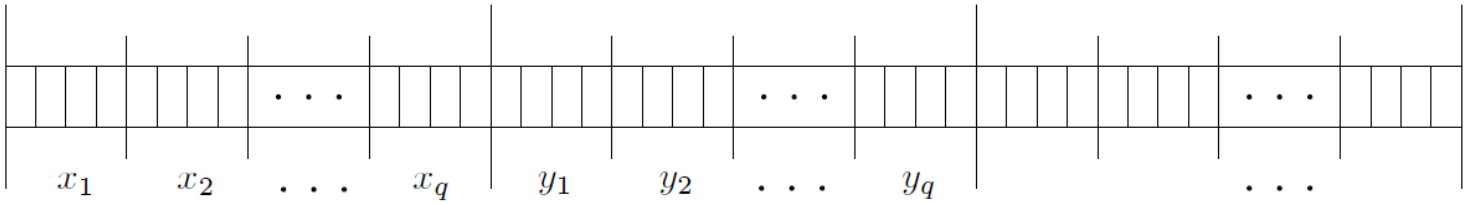
Jednotlivé prvky trojce m_i označme jako $x_{f(i)}, y_{g(i)}, z_{h(i)}$. Tj. funkce f (resp. g, h) vrátí k zadanému indexu i index $f(i)$ (resp. $h(i), g(i)$) prvku trojice m_i, který patří do množiny X (resp. Y, Z).

Postavme $A = \{a_1, \ldots, a_k, b_1, b_2\}$, kde

- $a_1, \ldots, a_k$ odpovídají trojicím $m_1, \ldots, m_k$,
- b_1 a b_2 jsou pomocné vyrovnávací prvky.

Cenu $s(a_1)$ prvku a_i pro $i \in \{1, \ldots, k\}$ popíšeme její binární reprezentací, která bude rozdělena an $3 \cdot q$ zón, z nichž každý má $p = \lceil \log_2(k+1) \rceil$ bitů. Každá z těchto zón bude odpovídat jednomu z elementů $X \cup Y \cup Z$.

Přesněji viz obrázek...



Reprezentace $s(a_i)$ bude záviset jen na prvcích trojice m_i, tedy na $x_{f(i)}$, $y_{g(i)}$, a $z_{h(i)}$. Váha $s(a_i)$ bude mít nastaveny na 1 nejpravější (t.j. nejméně významné) bity v blocích označených těmito třemi prvky, ostatní bity budou nulové:

$$s(a_i) = 2^{p(3q-f(i))} + 2^{p(2q-g(i))} + 2^{p(q-h(i))}.$$

Protože počet bitů, které potřebujeme na reprezentaci je $3pq$ a tedy polynomiální vzhledem k velikosti vstupu.

všimněte si: pokud posčítáme hodoty v kterékoli zóně, nedojde k přetečení, neboť jde o sečtení nejvýše k jedniček.

Položíme

$$B = \sum_{j=0}^{3q-1} 2^{pj},$$

což je číslo, kde v každé zóně nastavíme na 1 nejméně významný bit.
Množina $A' \subseteq \{a_i \mid 1 \leq i \leq k\}$ bude splňovat

$$\sum_{a \in A'} s(a) = B,$$

právě když $M' = \{m_i \mid a_i \in A'\}$ je perfektní párování M.
V tuto chvíli jsme tedy učinili převod problému $3DM$ na problém součtu podmnožiny, kde se ptáme, za existuje výběr prvků s celkovou cenou rovnou zadané hodnotě.
Abychom dostali na poloviny, doplníme dva prvky b_1 a b_2 s cenami:

$$s(b_1) = 2\left(\sum_{i=1}^{k} s(a_i)\right) - B$$

$$s(b_2) = \left(\sum_{i=1}^{k} s(a_i)\right) + B$$

Pokud nyní $A' \subseteq A$ splňuje, že

$$\sum_{a \in A'} s(a) = \sum_{a \in A \setminus A'} s(a),$$

pak se oba součty musí rovnat $2 \sum_{i=1}^{k} s(a_i)$, neboť to je polovina ze součtu všech prvků $\sum_{i=1}^{k} s(a_i) + s(b_1) + s(b_2)$.

Přitom platí, že prvky b_1 a b_2 se nemohou oba vyskytovat na jedné straně, tj. nemohou být oba v A' nebo oba v $A \setminus A'$, protože $s(b_1) + s(b_2) = 3 \sum_{i=1}^{k} s(a_i)$.

bez újmy na obecnosti můžeme předpokládat, že $b_1 \in A'$, $b_2 \in A \setminus A'$.
z toho plyne, že

$$\sum_{a \in A' \setminus \{b_1\}} s(a) = B$$

a prvky v A' bez b_1 tedy určují perfektní párování v M.

Nyní předpokládejme, že $M' \subseteq M$ je pefektní párování. Definujeme
$A' = \{a_i \,|\, m_i \in M'\}$
Musí platit, že $\sum_{a \in A'} s(a) = B$, a tedy
$\sum_{A \in A'} s(a) + s(b_1) = 2 \sum_{i=i}^{k} s(a_i)$,
což znamená, že množina $\{a_i | m_i \in M'\} \cup \{b_1\}$ obsahuje prvky právě poloviční ceny.