Sériově paralelní grafy

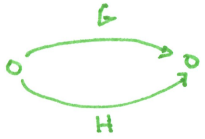
→ původ dle F v negativní normální formě na dle G v CNF.

→ Princip: sestavíme sériově paralelní graf podle indukční struktury F

na začátku: 

nový uzel = nová proměnná y_i $(i = 1, 2, \dots)$

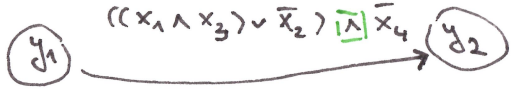
$F = G \wedge H$: transformace grafu na

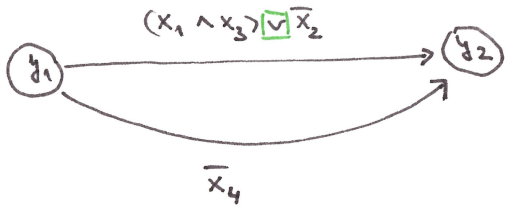


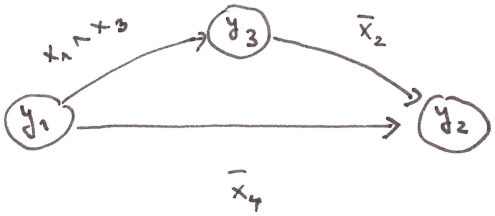
$F = G \vee H$: transformace grafu na

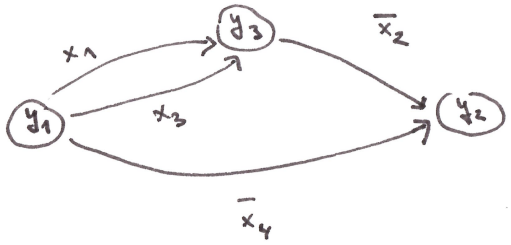
transformujeme dokud nejsou na hranách pouze literály (vzpomeňme, že F byla v negativní normální formě)

Př:









Tvrzení:

a) graf sestavíme v polynomiálním čase vzhledem k velikosti F

b) Pro každé ohodnocení α takové, že $F\alpha = 1$, platí: na každé cestě z y_1 do y_2 existuje aspoň jedna hrana s literálem u tak, že $u\alpha = 1$. Platí i opačná implikace.

Důkaz:

a) i b) Indukcí podle pravidel pro konstrukci grafu.

□

z b) vidíme, že F je ekvivalentní formuli

$$F' = \bigwedge_{\substack{p \text{ je cesta} \\ \text{z } y_1 \text{ do } y_2}} \left(\bigvee_{\substack{u \\ u \text{ je lit} \\ \text{na cestě } p}} u \right)$$

F' může být exponenciálně delší než F, protože může být exp. mnoho cest z y_1 do y_2

Mnohem menší ale pouze sat-ekvivalentní formuli F'' sestavíme

$$F'' = y_1 \wedge \bar{y}_2 \wedge \bigwedge_{(z,z') \text{ jí hrana s labelem } u} (\bar{z} \vee u \vee z')$$

Proč jsou F a F' sat-ekvivalentní?

1) Pro každé α takové, že $F''\alpha = 1$ máme $y_1 = 1$ a $y_2 = 0$ (to plyne z prvních dvou klauzulí v F).

2) každé cestě z y_1 do y_2 odpovídá v F'' sekce klauzulí

~~$(y_1 \wedge (\bar{y}_1 \vee u_1 \vee y_{i_1}) \wedge \ldots$~~

$$(y_1) \wedge (\bar{y}_1 \vee u_1 \vee y_{i_1}) \wedge (\bar{y}_{i_1} \vee u_2 \vee y_{i_2}) \wedge \ldots (\bar{y}_{i_k} \vee u_k \vee y_2) \wedge \bar{y}_2$$

Tato množina klauzulí je za předpokladu $\{y_1 = 1, y_2 = 0\}$ splněna pro ohodnocení, ve kterých je alespoň jeden literál u_j ($j = 1 \ldots k$) pravdivý. (a tedy je-li F'' pravdivá, je pravdivá i F)

Opačným směrem: je-li F pravdivá pro α, pak α splní na každé cestě z y_1 do y_2 alespoň jeden literál a tedy formule je pro α pravdivá.

Př.

$$F'' = y_1 \wedge \bar{y}_2 \wedge (\bar{y}_1 \vee x_1 \vee y_3) \wedge (\bar{y}_1 \vee x_3 \vee y_3) \wedge (\bar{y}_3 \vee \bar{x}_2 \vee y_2) \wedge (\bar{y}_1 \vee \bar{x}_4 \vee y_2)$$

Splnitelnost plynoucí z kombinatorických tvrzení

- **tvrzení:** Pokud množina F (klauzulí) neobsahuje klauzuli s pouze pozitivními (nebo s pouze negativními) literály, pak je F splnitelná.

  Důkaz:

  každá klauzule obsahuje negativní literál, $\Rightarrow F\alpha = 1$ pro $\alpha = \{x_1 = 0, x_2 = 0, \ldots\}$

  (každá klauzule obsahuje pozitivní literál $\Rightarrow F\alpha = 1$ pro $\alpha = \{x_1 = 1, x_2 = 1, \ldots\}$

  ∎

- **tvrzení:** F obsahuje pouze klauzule s nejvýše k literály. Pak pokud jich obsahuje méně než 2^k, tak je splnitelná.

  Důkaz:

  $n = |\mathrm{var}(F)|$, $n \geq k$ (tj. literály se v klauzulích neopakují)

Pro každou klausuli C $(|C| = k)$ existuje 2^{n-k} ohodnocení α $(Var(\alpha) = Var(F))$, která C nesplní (C má k různých proměnných, ze všech 2^k různých ohodnocení těchto proměnných nesplní C pouze jedno.)

Z toho plyne, že existuje nanejvýš $(\text{počet klausulí v } F) \cdot 2^{n-k} < 2^n$ ohodnocení, které nesplní všechny klausule v F.

$m < 2^k$

□

Z předchozího důkazu: C určuje podíl $\frac{1}{2^k}$ ze všech ohodnocení, který nesplní C. Je to $\frac{1}{2^{|C|}}$.

Obecně je to $\frac{1}{2^{|C|}}$.

S použitím v podstatě totožného důkazu tak máme:

Tvrzení: $F = \{C_1, C_2, \dots C_m\}$. Pokud

$$\sum_{j=1}^{m} 2^{-|C_j|} < 1,$$

pak je F splnitelná.

Jak z F z předchozího tvrzení najít ohodnocení, které ji splní?

Předpokládejme, že F neobsahuje klausuli s pozitivním i negativním literálem stejné proměnné (protože takovou klausuli můžeme z F vypustit a na splnitelnosti to nic nemění).

Zafixujme $x \in Var(F)$. Potom definujeme

$$S_x = \sum_{\substack{C \in F \\ x \in C}} \frac{1}{2^{|C|}} \qquad S_{\bar{x}} = \sum_{\substack{C \in F \\ \bar{x} \in C}} \frac{1}{2^{|C|}}$$

$$S = \sum_{\substack{C \in F \\ x, \bar{x} \notin C}} \frac{1}{2^{|C|}}$$

a vidíme, že platí

$$\sum_{C \in F} \frac{1}{2^{|C|}} = S_x + S_{\bar{x}} + S < 1$$

Odtud dostaneme

$$\sum_{C \in F \wedge x=0} \frac{1}{2^{|C|}} = 2 \cdot S_x + S$$

$$\sum_{C \in F \wedge x=1} \frac{1}{2^{|C|}} = 2 \cdot S_{\bar{x}} + S$$

Proč?
Z klausulí obsahujících x tento literál odebereme, jejich velikost se zmenší o 1.
Klausule obsahující $\bar{x}$ z formule zmizí.
Podobně

Obě předchozí sumy nemohou být současně ≥ 1. Můžeme je tohle sečíst a dostaneme

$$2 \cdot S_x + 2 \cdot S_y + 2 \cdot S$$

Pokud by obě sumy byly ≥ 1, tento součet by byl ≥ 2 a tedy

$$S_x + S_{\bar{x}} + S \geq 1,$$

což je spor s naším předpokladem.

Podle toho, která z sum je < 1 ohodnotíme proměnnou x ($2 \cdot S_x + S < 1 \Rightarrow \{x=0\}$ / $2 \cdot S_{\bar{x}} + S < 1 \Rightarrow \{x=1\}$)

a pokračujeme stejným algoritmem s $F\{x=\_\}$.

Klausule se příliš nepřekrývají

$C_1, C_2 \ldots$ klausule

$Var(C_1) \cap Var(C_2)$ ..... množina společných proměnných.

Intuice: Pokud je pro mnoho C_i, C_j : $Var(C_i) \cap Var(C_j) = \emptyset$ nalezení ohodnocení, které F splní je snazší.

Theorem (Lokální Lovaszovo Lemma)

$F \ldots$ CNF file, ~~alt ots~~ klausule mají přesně k literálů.

Pokud pro každou klausuli $C \in F$ platí, že existuje méně než

$$\frac{1}{4} \cdot 2^k = 2^{k-2}$$

klausulí $C' \in F$ tak, že $Var(C) \cap Var(C') \neq \emptyset$, pak je F splnitelná.

Důkaz: (uvažujme jenom kostru jádra z důkazu, LLL je důležitá věta, stojí za to ji umět najít a rozhodnout)

Ozn. $F = \{C_1, C_2 \ldots C_m\}$, $Var(F) = \{x_1, x_2 \ldots x_n\}$.

Uvažujme procedury:

```
MAIN(F)
vygenerujeme náhodné ohodnocení α   (Var(α) = Var(F))
pro j = 1 až m
    pokud C_j α == 0
        REPAIR(C_j)
```

```
REPAIR(C)
vygenerujeme náhodné ohodnocení k proměnných v C
a nahradíme jím příslušnou část α
pro j = 1 až m
    pokud Var(C_j) ∩ Var(C) ≠ ∅
        pokud C_j α == 0
            REPAIR(C_j)
```

Musíme ukázat, že procedura REPAIR skončí.

Uvažme s za sebou jdoucích zavolání REPAIR. V nich spotřebujeme $k \cdot s$ náhodných bitů. Na začátku jsme v MAIN spotřebovali n náhodných bitů. Celkem tedy $n + k \cdot s$ náhodných bitů.

Ukážeme, že těchto $n + k \cdot s$ bitů může být (pro velká s) zrekonstruováno z méně než $n + k \cdot s$ bitů (tj. tyto bity lze „zkomprimovat").

To pro nás bude spor:
použijeme výsledek z tzv. kolmogorovovy složitosti: „náhodná" sekvence bitů nejde zkomprimovat (s velkou pravděpodobností)".

Technické podrobnosti: k rekonstrukci si musíme zapamatovat:

- n bitů, které odpovídají obsahovému α po s zavoláních REPAIR
- m bitů, které ukazují, pro které klauzule jsme v MAIN zavolali REPAIR.
- pro každé rekurzivní zavolání REPAIR (C) si zapamatujeme pomocí $\lfloor k - 2 - \varepsilon \rfloor$ $(\varepsilon > 0)$ bitů, pro které klauzule jsme rekurzivní zavolání provedli (viz tvrzení/resp. jeho formulace). tj. celkem $\leq s \cdot (k - 2 - \varepsilon)$.
- pomocí $2s$ bitů si zapamatujeme strom rekurze
  1 ... do hloubky, 0 ... o úroveň výše

$\rightsquigarrow$ 10110110001

Celkem to je $n + m + s \cdot (k - \varepsilon)$ bitů.

Z těchto informací zpětně rekonstruujeme výpočet (např. pomocí stromu rekurze a informací o tom, pro které klauzule jsme REPAIR volali víme argument každého rek. zavolání.)

→ začínáme s α po s zavoláních. Obecně známe α po i zavoláních $(\text{pro } i = s, s-1, \ldots, 0)$

→ vždy, bylo ve výpočtu

$$\alpha \longrightarrow \text{REPAIR}(C) \longrightarrow \alpha'$$

α: po i zavoláních; α': po $i+1$ zavoláních

a známe α', můžeme zpětně α. V α byly nastaveny proměnné z $\text{Var}(C)$ tak, aby $C\alpha = 0$! To lze pouze jedním způsobem.

Takto se postupně dostaneme ke hledaným $n + k \cdot s$ bitům.

Díky: $\Leftarrow$ víme, že skoro pro všechny sekvence náhodných bitů máme

$$n + s \cdot k \leq n + m + s \cdot (k - \varepsilon)$$

a tedy $s \leq m/\varepsilon$.

Tedy pokud je s dostatečně velké, procedura MAIN s velkou pravděpodobností zastaví.

□

Tvrzení (LLL... obecnější verze)

F... fle v CNF. Pokud pro každé $C \in F$ platí

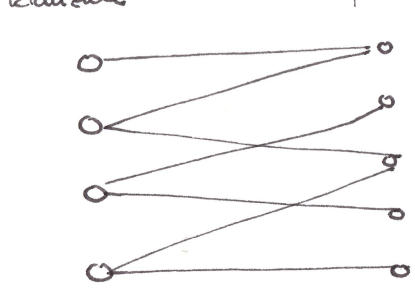
$$\sum_{D \in N(C)} 2^{-|D|} < \frac{1}{4},$$

pak je F splnitelná. Kde $N(C) = \{D \in F \mid Var(D) \cap Var(C) \neq \emptyset\}$.
Ozn.

Počty klausulí vs počty proměnných

Lemma: F... množina klausulí.
Pokud pro každé $G \subseteq F$ platí $|G| \leq |Var(G)|$,
pak je F splnitelná.

Proof: sestavíme bipartitní graf



~~Hrana hrana existuje pokud~~
Hrana (C, x) patří do grafu, pokud $x \in C$ nebo $\bar{x} \in C$.

Podle marriage theorem existuje párování S $|F|$ hranami. Proměnou těchto hran nastavíme tak, aby splnila příslušnou klausuli.

def:
Graf G je bipartitní, pokud lze množinu vrcholů rozdělit na dvě množiny tak, že vrcholy sousedí pouze s vrcholy z opačné množiny.

Př:

je bipartitní

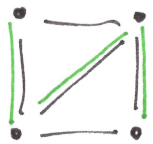
není bipartitní

Množinám z definice říkáme partity.

def:
Párování v grafu G je množina hran tohoto grafu taková, že žádné dvě hrany nesdílí uzel.

Př.

pokrývá



není pokrývající

Párování P pokrývá množinu uzlů A, pokud je každý uzel z A obsažen v některé hraně z P.

věta (Hallova „marriage" theorem).
~~Když~~ bipartitní graf s partitami A, B.
Pokud pro každou $A' \subseteq A$ platí, že $|A'| \leq |N(A')|$,
pak existuje párování, které pokrývá A.

Důkaz:
Vynecháme.

def: F ... množina klausulí
F je ~~nesplnitelná~~ minimálně nesplnitelná pokud
1) je nesplnitelná
2) pro každé $C \in F$ je $F \setminus \{C\}$ splnitelná.

tvrz: Pokud je F minimálně nesplnitelná, pak $|F| > |var(F)|$

(Tarski's Lemma)

Důkaz:

F je nesplnitelná $\rightarrow$ existuje $G \subseteq F$ tak, že $|G| > |var(G)|$. (předchozí věta).

Pokud $G = F$ nemáme co dokazovat.

Předp. že $G \subset F$ je maximální (vzhledem k počtu prvků)

množina splňující naše vlastnost. ↑

Vezměme množinu $F \setminus G$. Pro každou $H \subseteq F \setminus G$ platí

$$|H| < |var(H) \setminus var(G)| < |var(H)|.$$

Kdyby totiž $|H| \geq |var(H) \setminus var(G)|$, pak $|G \cup H| > |var(G \cup H)|$ a G by nebyla max. množina s danou vlastností.

Podle předchozí věty je tedy $F \setminus G$ splnitelná, a navíc pouze pomocí ohodnocení proměnných z množiny $var(F) \setminus var(G)$ (viz).

Ale protože F je minimálně nesplnitelná, je G splnitelná.

Odtud ale plyne, že $(F \setminus G) \cup G$ je splnitelná.

α ↑ bez proměnných z G ; α' ↑ s proměnnými z G

$\Rightarrow \alpha \cup \alpha'$ splní všechny klausule.

To je tedy spor, a musíme mít $F = G$.

Věta:

F ... množina klausulí,
$k \geq 1$,
každá $C \in F$ má nejméně ~~nejvíce~~ k literálů,
Pokud v každé proměnná vystupuje v nejvýše k klausulích, F je splnitelná.

Důkaz:

$G \subseteq F$,
G obsahuje nejméně ~~nejvíce~~ $k \cdot |G|$ výskytů literálů, každá proměnná do tohoto součtu přispěla max k krát.
Tj. $|var(G)| \geq |G|$ a podle marriage theorem (viz lemma na p. 6)
je F splnitelná.

□