

# Prepis problémov do CNF

## Úvod do matematickej logiky

Robert Lukočka

lukotka@dcs.fmph.uniba.sk

www.dcs.fmph.uniba.sk/~lukotka

M-255

# Informácie o predmete

Predmet pozostáva z troch častí.

- Prednášky (spoločné a AIN)
- Praktické cvičenia (spoločné s AIN)
- Teoretické “cvičenia” (separátne pre INF)

# Teoretické cvičenia

Okrem cvičení ku prednáške, využijeme teoretické cvičenia na doplnenie prednášok o niekoľko tém, ktoré v spoločných prednáškach nie sú

- Prepis formúl pre SAT solvery
- Hilbertovský kalkul (alternatíva ku tablovému kalkulu preberanému na prednáške)
- Veta o kompaktnosti
- Úplnosť prvorádovej logiky s dôkazom
- Lineárne a celočíselné lineárne programovanie
- Branch and bound, Branch and cut.

# Hodnotenie

- Nachádza sa na [stránke predmetu](#)
- Hodnotenie teoretických cvičení bude pozostávať z dvoch domácich úloh
  - Sat solvery (10 bodov)
  - Celočíselné lineárne programovanie / Branch and bound / Branch and cut (10 bodov)

Na úspešné absolvovanie predmetu je nevyhnutné získať z domácich úloh aspoň 6 bodov.

# Problém SAT

Problém splniteľnosti boolovskej formuly

- Vstup: Boolovská formula
- Výstup: Áno ak je formula splniteľná, nie inak
- Príklad:  $A$  je splniteľná formula,  $A \wedge \neg A$  nie.

Napriek tomu, že tento problém je NP-úplný, existujú algoritmy, ktoré si úspešne poradia s pomerne veľkými inštanciami, čo postačuje na riešenie mnohých praktických problémov

# SAT solver

SAT solver je nástroj na riešenie problému SAT.

- Vstup väčšinou požaduje v konjunktívnej normálnej forme (CNF), takýto problém sa nazýva CNF-SAT.
- Logické spojky  $\wedge$ , často nahradíme tým, že uvažujeme množinu disjunkcií, ktoré musia byť splnené súčasne.
- Príklad:

$$A \vee \neg B$$

$$\neg A \vee B$$

$$B$$

Táto množina formúl je splniteľná (formuly sú splnené keď  $B, A$  platia)

- Špeciálny prípad: Prázdna formula je nespniteľná. Prázdna množina formúl je splniteľná.

## Ekvivalentné úpravy

Na prepis do CNF poznáte zatiaľ jeden nástroj - ekvivalentné úpravy. Napr:

- $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$ .
- $(A \leftrightarrow B) \Leftrightarrow (A \vee \neg B) \wedge (\neg A \vee B)$

Problém je, že existujú triedy formúl, ku ktorým každá ekvivalentná CNF má exponenciálnu veľkosť. Potrebujeme teda niečo iné ...

# Ekvisplniteľné formuly

Dve formuly sú ekvisplniteľné, práve vtedy ak sú buď obe splniteľné, alebo obe nespľniteľné

- Každá formula je buď ekvisplniteľná s formulou  $A$ , alebo s formulou  $A \wedge \neg A$  ... už iba vedieť či je formula splniteľná.
- No, ale práve na to chceme použiť SAT solver :) ... Tento fakt nám príliš nepomôže.
- Existujú ekvisplniteľne úpravy, na cvičení budeme pre takéto úpravy používať symbol  $\cong$ .
- Príklad:  $\phi \cong \phi \wedge X$  ak sa  $X$  nenachádza v  $\phi$ .
  - Tieto formuly nie sú ekvivalentné a sú ekvisplniteľné.
  - Táto úprava nám ale príliš nepomôže.
  - Správne pridanie nových premenných však môže byť užitočné.



# Ekvisplniteľné transformácie

Nech  $\phi$  a  $\psi$  sú formuly a  $A$  a  $B$  sú premenné ktoré sa v týchto formulách nenachádzajú.

- $\phi \vee \psi \cong (A \vee B) \wedge (A \rightarrow \phi) \wedge (B \rightarrow \psi)$ .

# Ekvisplniteľné transformácie

Dôkaz: Ak je splniteľná  $\phi \vee \psi$ , potom existuje ohodnotenie premenných také, že

- $\phi \equiv \text{true}$ . Zvoľme  $A \equiv \text{true}$  a  $B \equiv \text{false}$ ,
- $\psi \equiv \text{true}$ . Zvoľme  $A \equiv \text{false}$  a  $B \equiv \text{true}$ .

Ak je splniteľná pravá strana potom existuje ohodnotenie premenných, také, že pravá strana je splnená. To ale znamená, že je splnené aj  $A \vee B$

- Ak je splnené  $A$ , musí byť v tomto ohodnotení splnené aj  $\phi$ , a teda aj  $\phi \vee \psi$ .
- Ak je splnené  $B$ , musí byť v tomto ohodnotení splnené aj  $\psi$ , a teda aj  $\phi \vee \psi$ . □

# Ekvisplniteľné transformácie

Nech  $\phi$  a  $\psi$  sú formuly a  $A$  a  $B$  sú premenné ktoré sa v týchto formulách nenachádzajú.

- $\phi \vee \psi \cong (A \vee B) \wedge (A \rightarrow \phi) \wedge (B \rightarrow \psi)$ .
- $\phi \vee \psi \cong (A \vee B) \wedge (\neg A \vee \phi) \wedge (\neg B \vee \psi)$ .
- Rekurzívne upravíme  $\phi$  a  $\psi$  do CNF a použijeme distributívnosť.
- Počet kláuz = počet kláuz  $\phi$  + počet kláuz  $\psi$  + 1.
- Počet literálov = počet literálov  $\phi$  + počet literálov  $\psi$  + počet kláuz  $\phi$  + počet kláuz  $\psi$  + 4.

Rovnaký postup funguje pre všetky (dokonca aj nebinárne) logické spojky, samozrejme, vtedy môže byť potrebná ekvivalencia namiesto implikácie.

## Špeciálny prípad - DNF $\rightarrow$ CNF

$$(A \wedge B \wedge D) \vee (C \wedge \neg D) \vee (\neg A \wedge \neg B \wedge \neg C)$$

- Riešenie (Klauzy sú namiesto  $\wedge$  oddelené “,” .):

$$X \vee Y \vee Z,$$

$$\neg X \vee A, \neg X \vee B, \neg X \vee D$$

$$\neg Y \vee C, \neg Y \vee \neg D$$

$$\neg Z \vee \neg A, \neg Z \vee \neg B, \neg Z \vee \neg C$$

**Hint z predchádzajúceho slajdu:**

$$\phi \vee \psi \cong (A \vee B) \wedge (\neg A \vee \phi) \wedge (\neg B \vee \psi).$$

# Tseytinova transformácia

Predchádzajúca transformácia má problém v situáciách, keď napr. rozpisujeme spojky  $\leftrightarrow$ , či XOR .

Tseytinova transformácia:

- Pre každú podformulu pridáme novú premennú.
- Musí platiť premenná zodpovedajúca celej formule.
- Okrem toho, musí platiť, že každá nová premenná je ekvivalentná, podformule, kde operandy sú nahradené inými pomocnými premennými.

## Tseytinova transformácia - príklad

$$(A \vee B) \leftrightarrow (C \text{ XOR } (D \wedge E))$$

- $X_1 \leftrightarrow (A \vee B)$
- $X_2 \leftrightarrow (D \wedge E)$
- $X_3 \leftrightarrow (C \text{ XOR } X_2)$
- $X_4 \leftrightarrow (X_1 \leftrightarrow X_3)$
- $X_4$

Veľkosť výstupnej formuly je lineárna od veľkosti vstupnej formuly.

## Tseytinova transformácia - príklad

Bez  $X_4$  (premenná zodpovedajúca koreňu formuly)

- $X_1 \leftrightarrow (A \vee B)$
- $X_2 \leftrightarrow (D \wedge E)$
- $X_3 \leftrightarrow (C \text{ XOR } X_2)$
- $X_1 \leftrightarrow X_3$

Takéto úpravy by ale nemali mať zásadný dopad na trvanie výpočtu.

## Cvičenia

Upravte nasledujúce formuly na equisplniteľné<sup>1</sup>

- $A \vee (C \wedge D) \vee (\neg B \wedge C \wedge D)$ .
- $(A \vee (C \wedge D)) \rightarrow (\neg B \wedge C \wedge D)$ .
- $(A \rightarrow (\neg B \wedge D)) \leftrightarrow (B \vee C \vee D)$
- $(A \rightarrow B) \text{ XOR } (C \wedge D) \text{ XOR } (B \vee C \vee E)$ .

---

<sup>1</sup>Pre zabránenie triviálnym odpovediam, za správne riešenie sa považuje iba taká equisplniteľná formula, že pre každé iné formuly  $\phi$  a  $\psi$ , ktoré neobsahujú vami zavedené nové premenné,  $(\phi \wedge X) \vee \psi \cong (\phi \wedge Y) \vee \psi$ , kde  $X$  je formula zo zadania a  $Y$  je vaše riešenie.



## Cvičenia


Prepíšte nasledujúce problémy ako inštancie CNF-SAT.<sup>2</sup>

- Zistiť či je daný graf 3-zafarbiteľný.
- Zistiť či má daný graf perfektné párovanie vrcholov (toto je síce polynomiálny problém, ale prečo nie...).
- Zistiť, či graf obsahuje tri kompletne podgrafy také, že každá hrana je incidentná s vrcholom jedného z kompletných podgrafov.

Aj algoritmicky jednoduché veci môžu byť netriviálne.

- Zistiť, či je daný graf les / strom.

---

<sup>2</sup>Pri polynomiálnych problémoch trochu narážame na problém, že čo je to redukcia, ale v tomto prípade si predstavte, že sa jedná o parciálny problém. 

# Cvičenia

- Zistiť, či je daný graf les.

# Cvičenia

- Zistiť, či je daný graf les.

## Možné riešenie

- Hranám priradíme orientáciu (dve premenné na každú hranu).
- Vyžadujeme, aby z každého vrchola vychádzala nanajvýš jedna hrana.
- Ak je v grafe cyklus, orientované hrany tvoria orientovaný cyklus
- Urobíme tranzitívny uzáver a vyžadujeme aby v ňom nebol cyklus dĺžky dva (mať cyklus je nelokálna vlastnosť, vyžaduje si nelokálne riešenie).

## Cvičenia

Premenné - pre každú usporiadanú dvojicu rôznych vrcholov  $(u, v)$  máme premenné  $a_{u,v}$  a  $b_{u,v}$ .

- (1) Pre každú dvojprvkovú množinu vrcholov  $\{u, v\}$ , pridáme klauzu  $\neg b_{u,v} \vee \neg b_{v,u}$ .
- (2) Pre každú dvojprvkovú množinu vrcholov  $\{u, v\}$ , ktoré spája v grafe hrana, pridáme klauzu  $a_{u,v} \vee a_{v,u}$ .
- (3) Pre každý vrchol  $u$ , a každú dvojicu susedných vrcholov  $(v, w)$ , pridáme  $\neg a_{v,u} \vee \neg a_{w,u}$ .
- (4) Pre usporiadanú dvojicu rôznych vrcholov  $(u, v)$ , pridáme klauzu  $\neg a_{u,v} \vee b_{u,v}$ .
- (5) Pre usporiadanú trojicu rôznych vrcholov  $(u, v, w)$ , pridáme klauzu  $\neg b_{u,v} \vee \neg b_{v,w} \vee b_{u,w}$ .

## Cvičenia

*Náčrt dôkazu:* Ak graf je les splníme formuly nasledovne.

- Pre každý komponent vyberieme koreň. Hrany zorientujeme k nemu.
- Toto vytvorí reláciu  $R$  na vrcholoch grafu.
- Urobíme tranzitívny uzáver  $R^+$  tejto relácie.
- Ohodnotíme  $a_{u,v} \equiv \text{true}$ , práve vtedy, keď  $(u, v) \in R$ .
- Ohodnotíme  $b_{u,v} \equiv \text{true}$ , práve vtedy, keď  $(u, v) \in R^+$ .
- Nie je ťažké dokázať, že všetky formuly sú splnené.

## Cvičenia

*Náčrt dôkazu:* Ak graf je nie je les, potom obsahuje kružnicu  $v_1 \dots v_n$ . Pre spor, predpokladajme, že existuje ohodnotenie premenných, ktoré spĺňa všetky formuly.


- Podľa (1), (4), a (2) platí presne jedno z  $a_{v_1, v_n}$  a  $a_{v_n, v_1}$ , BUNV, nech je to  $a_{v_n, v_1}$ .
- Potom, podľa (2) a (3) platí aj  $a_{v_1, v_2}$  a indukciou možno dokázať, že platí  $a_{v_i, v_{i+1}}$ , pre všetky  $1 \leq i \leq n - 1$ .
- Podľa (4), platí  $b_{v_n, v_1}$  a pre všetky  $1 \leq i \leq n - 1$  platí  $b_{v_i, v_{i+1}}$ ,
- Podľa (5), platí  $b_{v_n, v_2}$ , a indukciou možno dokázať, že platí  $b_{v_n, v_{n-1}}$
- Platí  $b_{v_{n-1}, v_n}$  aj  $b_{v_n, v_{n-1}}$ , čo je v spore s (1).

## Úlohy pre vás na vyskúšanie

Prepíšte nasledujúce problémy ako inštancie CNF-SAT.<sup>3</sup>

- Zistiť či je daný graf 3-zafarbiteľný.
- Zistiť či má daný graf perfektné párovanie vrcholov (toto je síce polynomiálny problém, ale prečo nie...).
- Zistiť, či graf obsahuje tri kompletne podgrafy také, že každá hrana je incidentná s vrcholom jedného z kompletných podgrafov.

---

<sup>3</sup>Pri polynomiálnych problémoch trochu narážame na problém, že čo je to redukcia, ale v tomto prípade si predstavte, že sa jedná o parciálny problém. 

## Binárny zápis

Počet premenných možno znížiť použitím binárneho zápisu.  
 Uvažujme nasledujúci problém:

- Problém: Zistiť či je daný graf  $2^n$ -zafarbiteľný.

Pre každý vrchol  $v$  budeme mať premenné  $a_{v,i}$ , pre  $1 \leq i \leq n$ .

- Pre susedné vrcholy  $u, v$ . Pridáme formulu:

$$\neg \bigwedge_i (a_{u,i} \leftrightarrow a_{v,i}).$$

- Našťastie, už vieme ako takúto formulu prepísať do CNF ...

Mimochodom, nie je dôležité, aby počet farieb bola mocnina dvojky  
 - napíšte formulu, ktorá overí či premenné reprezentujúce číslo  $v$   
 dvojkovej sústave reprezentuje číslo  $< k$ , kde  $2^{n-1} < k \leq 2^n$ .



# Hamiltonovská kružnica

Ukážeme si viacero možných zápisov problému Hamiltonovskej kružnice (Vstup: graf, výstup: má kružnicu prechádzajúci všetkými vrcholmi).

Postup pomocou zoradenia vrcholov:

- Každému vrcholu priradíme premenné (a formuly) určujúce jeho poradie v kružnici.
- Žiadne dva vrcholy nemôžu mať rovnaké poradie.
- Ak sú dva vrcholy susedné v tomto poradí musia byť susedné aj v grafe

Poradie premennej: Môžeme mať signalizačné premenné, unárnu sústavu, binárnu sústavu.

# Hamiltonovská kružnica

Pomocou orientovaného grafu s výstupným stupňom 1 (podobne ako príklad so stromom).

- Zvolíme jeden vrchol a rozdelíme ho na dva. Do jednej kópie budú hrany vchádzať a z druhej vychádzať (hrany pôjdu do / z tých istých vrcholov ako v pôvodnom grafe). Ostatné hrany považujeme za dve orientované hrany, každá iným smerom. Tieto vrcholy budeme volať počiatočný a koncový.
- Z každého vrchola bude vychádzať práve jedna hrana, okrem vrchola do ktorého hrany iba vchádzajú.
- Do koncového vrchola vchádza nejaká hrana.

# Hamiltonovská kružnica

Ak splníme takéto formuly, existuje cesta spájajúca počiatočný a koncový vrchol. Nemusí však obsahovať všetky vrcholy.

- Funguje idea tranzitívneho uzáveru z príklade o stromu, ale urobíme niečo lepšie - budeme počítat'.
- Počiatočný vrchol bude mať číslo 0, koncový  $n$ .
- Ak bola vybrana orientovana hrana z  $a$  do  $b$  a vrchol  $b$  ma cislo  $n$ , potom vrchol  $a$  musi mat cislo  $n - 1$ .

V tomto prípade je výhodné mať  $|V(G)|$  premenných pre každý vrchol, poradie je indikované najvyššou true premennou (nemusíme preto pridávať formuly zabezpečujúce pekné vlastnosti premenných).

# Počítanie

Mnohé problémy pre svoj prepis na logické formuly vyžadujú “počítanie”.

Existuje množina  $n/4$  vrcholov v grafe  $G$  takých, že každý vrchol je v množine, alebo je susedom vrchola v množine?

Môžeme vrcholy v množine zoradiť, ale to nie je príliš efektívne riešenie. Lepšie je “spočítať” koľko vrcholov je v množine.

# Počítanie

Na počítanie použijeme premenné, ktoré reprezentujú čísla v dvojkovej sústave. Počítať možno dvoma spôsobmi

- Za sebou  $((x_1 + x_2) + x_3) + x_4$ 
  - Často stačí v logických formulách “implementovať” pripočítanie 0 alebo 1.
  - Celkovo však treba  $n \log n$  počítacích premenných, lebo dostávame veľké medzivýsledky
- Paralelne  $((x_1 + x_2) + (x_3 + x_4))$ 
  - Treba v logických formulách “implementovať” sčítačku
  - Lineárne veľa premenných, keďže medzivýsledky sú menšie.

# Symetrie v riešení

Symetrie v riešeniach môžu byť pre SAT solver problémom.

- Ak zisťujeme existenciu hamiltonovskej kružnice tak, že vrcholom návame poradie, chceme
  - Zvoliť prvý vrchol na pevno.
  - Okrem toho môže pomôcť: rozbitie symetrie druhý vrchol vs posledný vrchol.
- Exisuje množina  $n/4$  vrcholov v grafe  $G$  takých ...
  - Pradie vrcholov vo vybranej množine zodpovedá zvolenému poradiu vrcholov v grafe-

# References I



Wikipedia - Conversion into CNF