Hľadanie SMT modelu neskorou kontrolou

(Aplikácia logiky v inteligentných systémoch)

M. Mach

Katedra kybernetiky a umelej inteligencie, FEI, TUKE

október 2020

Princíp neskorej kontroly

- Vyžaduje $\mathcal{T}$-**solver** schopný rozhodnúť o $\mathcal{T}$-splniteľnosti konjunkcie atómov vytvorených podľa teórie $\mathcal{T}$
- **SMT solver** ako kombinácia dvoch solverov

SAT solver

$\updownarrow$

$\mathcal{T}$ solver

- Častou architektúrou SMT solvera je DPLL($\mathcal{T}$) vrátane generovania nových klauzúl $\mathcal{T}$-solverom
- Inkrementálna kontrola

Ukážka neskorej kontroly

$(P \vee Q) \wedge x - 3y \geq 0 \wedge \neg(x + 3y < 6) \wedge (\neg Q \vee y - x \geq 0)$

Splniteľný model (SAT solver)

$I = \{P^I = FALSE, Q^I = TRUE, (x - 3y \geq 0)^I = TRUE, (x + 3y < 6)^I = FALSE, (y - x \geq 0)^I = TRUE\}$

- $x - 3y \geq 0 \wedge x + 3y \geq 6 \wedge y - x \geq 0$ nie je $\mathcal{T}$-splniteľné ($\mathcal{T}$-solver)

Splniteľný model (SAT solver)

$I = \{P^I = TRUE, Q^I = FALSE, (x - 3y \geq 0)^I = TRUE, (x + 3y < 6)^I = FALSE$

- $x - 3y \geq 0 \wedge x + 3y \geq 6$ je $\mathcal{T}$-splniteľné ($\mathcal{T}$-solver)

Fourier-Motzikinova eliminácia premenných

- Pre kontrolu *konjunkcie lineárnych nerovnostných* ohraničení nad *reálnymi* premennými (atómov reálnej lineárnej aritmetiky s nerovnosťami)
- Vstupom je m ohraničení nad n premennými x_i

$$\bigwedge_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} x_j \bowtie b_i$$

$\bowtie$ je operátor nerovnosti $(<, \leq, >, \geq)$, $a_{i,j}$ a b_i sú reálne konštanty

Princíp F-M eliminácie premenných

- Nutná eliminácia rovnostných ohraničení
  - $=$ – vyjadrenie jednej premennej a dosadenie za ňu do ostatných ohraničení
  - $\neq$ – náhrada dvojicou $<$ a $>$ (rozdvojenie postupu)
- Ohraničenie vzhľadom na premennú x_k môže byť
  - neutrálne ohraničenie – premenná v danom ohraničení nevystupuje
  - dolné ohraničenie ($x_k \geq RHS_{i,k}$ alebo $x_k > RHS_{i,k}$)
  - horné ohraničenie ($x_k \leq RHS_{i,k}$ alebo $x_k < RHS_{i,k}$)

$$RHS_{i,k} = \frac{1}{a_{i,k}} \left(b_i - \sum_{j=1}^{k-1} a_{i,j} x_j - \sum_{j=k+1}^{n} a_{i,j} x_j \right)$$

Algoritmus F-M eliminácie premenných

vstup: ohraničenia C nad reálnymi premennými
výstup: TRUE v prípade $\mathcal{T}$-splniteľnosti, FALSE inak

1. $ZP = zoznam\_premennych(C)$
2. **foreach** $V \in ZP$ **do**
3. $\quad HO = horne\_ohranicenia(C,V)$
4. $\quad DO = dolne\_ohranicenia(C,V)$
5. $\quad NO = nove\_ohranicenia(DO,HO)$
6. $\quad C = C \setminus (HO \cup DO) \cup NO$
7. $\quad$ **if** $nesplnitelne(C)$ **then return** FALSE
8. **return** TRUE

Úprava ohraničení pre premennú x_k (1)

- Neutrálne ohraničenia ostávajú nedotknuté.
- Ak premenná má iba dolné ohraničenia, tak ich splnenie je jednoduché – stačí premennej dať dostatočne vysokú hodnotu. Takéto ohraničenia je možné spolu s premennou odstrániť.
- Ak premenná má iba horné ohraničenia, tak ich splnenie je jednoduché – stačí premennej dať dostatočne nízku hodnotu. Takéto ohraničenia je možné spolu s premennou odstrániť.
- Ak premenná má dolné aj horné ohraničenia, tak tieto sa nahradia novými ohraničeniami, v ktorých už daná premenná nevystupuje.

Úprava ohraničení pre premennú x_k (2)

- Ak i-te ohraničenie je dolným ohraničením premennej a j-te ohraničenie je horným ohraničením
  - dolné ohraničenie nemôže byť väčšie ako horné ohraničenie

$$\frac{x_k \geq RHS_{i,k} \qquad x_k \leq RHS_{j,k}}{RHS_{i,k} \leq RHS_{j,k}}$$

    táto podmienka musí byť pridaná k existujúcim ohraničeniam
  - Ak ostrá nerovnosť v jednom z ohraničení, tak aj vo výslednej podmienke
- Párovanie každého dolného ohraničenia s každým horným ohraničením a ich nahradenie novo generovanými podmienkami

Zložitosť F-M eliminácie premenných

- Počet ohraničení môže počas eliminácie narastať
- Najhorší prípad - premenná vystupuje vo všetkých m ohraničeniach ($m/2$ je dolných a $m/2$ je horných)
    - m ohraničení bude nahradených $m^2/4$ ohraničeniami (počet ohraničení rastie kvadraticky)
- Vhodné pre malý počet premenných a ohraničení
    - v solveroch sa nepoužíva
    - vďaka svojej jednoduchosti vhodná pre vytvorenie predstavy o práci $\mathcal{T}$-solvera
- Voľba premenných riadená počtom generovaných ohraničení
    - výber premennej pridávajúcej najmenej ohraničení

Nájdenie modelu F-M elimináciou premenných

- Ak ohraničenia po eliminácii všetkých premenných sú splniteľné, potom konjunkcia pôvodných ohraničení je splniteľná ($\mathcal{T}$-splniteľnosť)
- Nájdenie konkrétnych hodnôt premenných
  - spätný postup cez vykonané iterácie eliminácie premenných
  - v každej iterácii sa priradí hodnota tej premennej, ktorá v nej bola eliminovaná
  - premennej možno priradiť ľubovoľnú hodnotu, spĺňajúcu všetky dolné a horné ohraničenia danej premennej