Matematická logika

Rostislav Horčík

horcik@math.feld.cvut.cz
horcik@cs.cas.cz
www.cs.cas.cz/~horcik

Splnitelnost množin

Definice

Množina formulí S je splnitelná, pokud existuje pravdivostní ohodnocení u takové, že $u(S) = 1$, tj. $u(\varphi) = 1$ pro všechny $\varphi \in S$.

Věta

Pro množinu formulí S a formuli φ platí

$$S \models \varphi \text{ právě tehdy, když } S \cup \{\neg\varphi\} \text{ není splnitelná.}$$

Klausule

Definice

Literál je buď výroková proměnná (positivní literál) nebo její negace (negativní literál). Literály p a $\neg p$ se nazývají komplementární.
Klausule C je libovolná formule tvaru

$$C = x_1 \vee x_2 \vee \cdots \vee x_n \,,$$

kde x_i jsou literály (navzájem různé).
Pro $n = 0$ definujeme $C = F$ (F značí kontradikci). V tomto případě se C nazývá prázdná klausule.

Pozorování

Klausule je tautologií právě tehdy, když obsahuje dvojici komplementárních literálů.

Klausule

Tvrzení

Ke každé formuli α existuje množina klausulí S_α taková, že pro každé pravdivostní ohodnocení u platí

$$u(\alpha) = 1 \text{ právě tehdy, když } u(S_\alpha) = 1.$$

Důkaz

- Pomocí CNF máme $\alpha \models\!\!\dashv C_1 \wedge C_2 \wedge \cdots \wedge C_n$, kde C_i jsou klausule.
- $C_1 \wedge C_2 \wedge \cdots \wedge C_n$ je splněna p.t.k. $S_\alpha = \{C_1, C_2, \ldots, C_n\}$ je splněna, tj. pro každé pravdivostní ohodnocení u platí

$$u(C_1 \wedge C_2 \wedge \cdots \wedge C_n) = 1 \text{ p.t.k. } u(S_\alpha) = 1\,.$$

Resolventa

Konvence

Mějme klausuli C a literál p, který se v C vyskytuje. Symbolem $C \setminus p$ označujeme klausuli, která obsahuje všechny literály jako C kromě p. Např. pro $C = \neg x \vee y \vee \neg z$ máme

$$C \setminus \neg z = \neg x \vee y\,.$$

Definice

Řekneme, že klausule D je rezolventou klausulí C_1 a C_2 podle literálu p, pokud existuje literál p takový, že p se vyskytuje v klausuli C_1, $\neg p$ se vyskytuje v klausuli C_2 a

$$D = (C_1 \setminus p) \vee (C_2 \setminus \neg p)\,.$$

D značíme $\mathrm{res}_p(C_1, C_2)$. Např. $\mathrm{res}_p(p, \neg p) = F$.

Věta

Mějme dánu množinu klausulí S a označme D rezolventu některých dvou klausulí z množiny S. Pak množiny S a $S \cup \{D\}$ jsou pravdivé ve stejných pravdivostních ohodnoceních.

Důkaz

- Nechť u je pravdivostní ohodnocení. Musíme ukázat, že $u(S) = 1$ p.t.k. $u(S \cup \{D\}) = 1$ (směr zprava doleva je triviální).
- Předpokládejme, že $u(S) = 1$ a $D = \mathrm{res}_p(C_1, C_2)$ pro $C_1, C_2 \in S$.
- Máme tedy $u(C_1) = u(C_2) = 1$ a $D = (C_1 \setminus p) \vee (C_2 \setminus \neg p)$.
- Pokud $u(p) = 1$, pak $u(C_2 \setminus \neg p) = 1$.
- Pokud $u(p) = 0$, pak $u(C_1 \setminus p) = 1$.
- V obou případech $u(D) = 1$.

Resoluční uzávěr

Definice

Označme

$$
\begin{aligned}
R(S) &= S \cup \{D \mid D \text{ je resolventa některých klausulí z } S\} \\
R^0(S) &= S \\
R^{i+1}(S) &= R(R^i(S))\,,\ i \in \mathbb{N} \\
R^\star(S) &= \bigcup \{R^i(S) \mid i \in \mathbb{N}\}
\end{aligned}
$$

Pozorování

Pro konečnou množinu klausulí S existuje $n \in \mathbb{N}$ takové, že $R^\star(S) = R^n(S)$.

Věta

Mějme dánu konečnou množinu klausulí S. Pak množiny S a $R^\star(S)$ jsou pravdivé ve stejných pravdivostních ohodnoceních.

Důkaz

- Víme, že pro každou resolventu D některých klausulí z $R^i(S)$, jsou množiny $R^i(S)$ a $R^i(S) \cup \{D\}$ splněny ve stejných ohodnoceních.
- Z toho plyne, že S a $R^i(S)$ jsou splněny ve stejných ohodnoceních pro každé $i \in \mathbb{N}$.
- Protože $R^\star(S) = R^n(S)$ pro nějaké $n \in \mathbb{N}$, je důkaz hotov.

Resoluční princip

Věta

Konečná množina klausulí S je splnitelná právě tehdy, když $R^\star(S)$ neobsahuje prázdnou klausuli F.

Důkaz

- Zleva doprava: když je S, pak je splnitelná i $R^\star(S)$. Tudíž nemůže obsahovat prázdnou klausuli (kontradikci) F.
- Zprava doleva: dokážeme později.

Algoritmus

Předchozí věta dává návod, jak zjistit, zda daná konečná množina klausulí je spnitelná nebo je nesplnitelná:

1. Formule množiny M převedeme do CNF a množinu M pak nahradíme množinou S všech klausulí vyskytujících se v některé formuli v CNF. Klausule, které jsou tautologiemi, vynecháme. Jestliže nám nezbyde žádná klausule, množina M se skládala z tautologií a je pravdivá v každém pravdivostním ohodnocení.
2. Vytvoříme $R^{\star}(S)$.
3. Obsahuje-li $R^{\star}(S)$ prázdnou klausuli, je množina S (a tedy i množina M) nesplnitelná, v opačném případě je M splnitelná.

Je zřejmé, že konstrukce celé množiny $R^{\star}(S)$ může být zbytečná. Stačí pouze zjistit, zda $R^{\star}(S)$ obsahuje F.

Davis–Putnam algoritmus

Algoritmus DP(S)

Vstup: konečná množina klausulí S
Výstup: S je splnitelná $\times$ nesplnitelná

- Pokud S obsahuje tautologie, tak je vyřaď.
- Vyber libovolnou výrokovou proměnnou x v některé z klausulí v S.
- Nechť $M \subseteq S$, která obsahuje klausule bez x.
- Nechť N je množina všech resolvent množiny S podle x.
- Pokud $F \in N$, pak vrať S není splnitelná a skonči.
- Pokud $N \cup M = \emptyset$, pak vrať S je splnitelná a skonči.
- DP($N \cup M$).

Tvrzení

Algoritmus DP skončí po konečně mnoha krocích.

Důkaz

- Klausule v $N \cup M$ neobsahují x, tj. každé volání DP obsahujeme méně a méně proměnných.
- Protože klausule v S obsahují jen konečně mnoho výrokových proměnných, algoritmus skončí po konečně mnoha krocích.

Tvrzení

Nechť $S, N \cup M$ jsou množiny klausulí z algoritmu DP. Pak

$$N \cup M \text{ je splnitelná p.t.k. } S \text{ je splnitelná.}$$

Důkaz

- Protože $M \subseteq S$ a N jsou rezolventy z S, je směr zprava doleva triviální.
- Nechť u splňuje $N \cup M$, tj. $u(N \cup M) = 1$.
- Nechť $M_1 \subseteq S$ je množina klausulí, které obsahují x a $M_2 \subseteq S$ množina klausulí, které obsahují $\neg x$.
- Zkonstruujeme ohodnocení v, které splní $S = M \cup M_1 \cup M_2$.

Důkaz pokračování

- Nechť $v(y) = u(y)$ pro všechny výrokové proměnné y různé od x.
- Pokud $u(C \setminus x) = 1$ pro všechny $C \in M_1$, pak definujeme $v(x) = 0$, tj. $v(M_2) = 1$ a tudíž $v(S) = 1$.
- Jinak existuje $C \in M_1$ taková, že $u(C \setminus x) = 0$.
- Definujeme $v(x) = 1$ (tj. $v(M_1) = 1$) a ukážeme, že $v(M_2) = 1$.
- Nechť $D \in M_2$. Pak $\mathrm{res}_x(C, D) \in N$, tj. $u(\mathrm{res}_x(C, D)) = 1$.
- Protože $u(\mathrm{res}_x(C, D)) = u((C \setminus x) \vee (D \setminus \neg x)) = 1$ a $u(C \setminus x) = 0$, dostaneme $u(D \setminus \neg x) = 1$.
- Takže $v(D) = v(D \setminus \neg x) = u(D \setminus \neg x) = 1$.

Věta

Algoritmus DP je korektní a úplný, tj.

DP(S) vrátí "S je splnitelná" právě tehdy, když S je splnitelná.

Důkaz

- Zprava doleva: DP(S) vrátí "S je nesplnitelná", pokud v některém kroku $F \in N \cup M$.
- Z předchozího tvrzení plyne, že S je nesplnitelná.
- Zleva doprava: DP(S) vrátí "S je splnitelná", pokud v posledním kroku $N \cup M = \emptyset$ ($\emptyset$ je triviálně splnitelná).
- Konstrukce z důkazu předchozího tvrzení nám dává ohodnocení, které splní S.