Logika v informatice

2. ledna 2013

Obsah

1 Rezoluce

Týká se výrokové logiky.

Výroková logika má dvě části. Syntax a sémantiku. Syntax jsou formule, proměnné, spojky a tak dále. Sémantika je dána ohodnocením (zobrazení z proměnných do množiny $\{0,1\}$). Když máme formuli φ, tak nám stačí jen její proměnné a umíme určit její hodnotu. Pokud je pravdivá, říkáme, že je ***splněna*** v daném ohodnocení. Formule je ***splnitelná***, pokud existuje ohodnocení, ve kterém je splněná. Formule je ***tautologie***, pokud je pravdivá v každém ohodnocení. φ je tautologije $\Leftrightarrow \neg\varphi$ je nesplnitelná.

Výrokový rezoluční systém nebo rezoluce je systém, který slouží k dokazování formulí ve tvaru „disjunkce konjunkcí literálů“, kde literály jsou proměnné nebo jejich negace. Máme tedy DNF. Resoluční systém je založen na důkazu sporem. Negací ji převedeme na CNF. Disjunkci literálů budeme říkat ***klauzule***. Zavedeme pravidlo rezoluce. Máme klauzuli $\{P_1, \ldots, P_k, p_i\}$ a $\{Q_1, \ldots, Q_l, \neg p_i\}$, z toho vyvodíme $\{P_1, \ldots, P_k\} \cup \{Q_1, \ldots, Q_l\}$. Postupně dojdeme k prázdné klauzuli, čímž získáme spor.

Toto pravidlo zachovává splnitelnost.

Obecný důkaz je posloupnost. Lépe se analyzuje důkaz stromový – klauzule se slévají, až zbude jen kořen. Listy (původní klauzule) se mohou opakovat. Existují tautologie v DNF takové, že mají exponenciálně velké stromové důkazy, ale polynomiálně velké lineární – to opakování může nastat na všech hladinách, kopíruje se to moc.

Složitost splňování v CNF je NP-úplné, tautologie DNF coNP-úplné. Hypotéza je, že NP není coNP, což je silnější, než že P není stejně jako coNP. Z této hypotézy plyne, že žádný důkazový systém pro DNF nemá polynomiálně omezené důkazy.

Příklady, které vyžadují exponenciálně velké důkazy v rezoluci:

- Šuplíkový princip (PHP_n^{n+1}). Říká, že neexistuje prosté zobrazení z množiny $1 \ldots n+1$ do $1 \ldots n$. Ala Holubnikuv princip.
- G je neorientovaný graf. Nechť $c : V \to \{0,1\}$, počet 1 lichý. Potom pro každé ohodnocení hran $e : E \to \{0,1\}$. $\sum_{(u,v)\in E} \neq c(v)(mod 2)$.

Důkazový systém S se nazývá ***automatizovatelný***, pokud existuje algoritmus A takový, že pro zadanou pravdivou formuli φ a danou mez m A sestrojí důkaz d délky $\leq m$ v čase polynomiálně omezeném m.

Věta 1 (Alechuvich, Rcetfov) *Pro určitou pravděpodobnou hypotézu H platí. Je-li H pravdivá, potom obecná automatizace není obecně automatizovatelná. Stejně tak stromová.*

1.1 Davis-Putmanova procedura

Slouží k nalezení splňujícího ohodnocení, je až exponenciální, ale ořezává.

Máme klauzule $\mathcal{C} := \{C_1, \ldots, C_n\}$ a proměnné $p_1, \ldots, p_n$. Konstruujeme lineární strom způsobem – nechť v je kořen. Zvolíme v něm proměnnou p_i a větvíme se podle toho, jestli dosadíme 0 nebo 1.

Když dosadíme 0, vypustíme všechny klauzule obsahující $\neg p_i$. Z těch, které obsahují p_i vypustíme p_i. Když zbude $\mathcal{C}$ jako prázdné, označíme toto částečné ohodnocení jako splňující. Pokud se některá klauzule zkrátí na prázdnou, pak tuto větev ukončíme.

Když dosadíme 1, tak postupujeme duálně.

Tvrzení 1 *Pokud existuje splňující ohodnocení, potom ji tato procedura najde (všechny).*

Naopak, pokud neexistuje, pak jsou všechny větve uzavřeny sporem a lze sestrojit důkaz ve stromové resoluci stejné velikosti.

Důkaz:
Na každý list dáme klauzuli, která je nesplněná. Dále jdeme zpět ke kořeni a provádíme rezoluci podle proměnných, podle kterých se větvilo. Pokud to nejde, vezmeme klauzuli, která neobsahuje literál s danou proměnnou.

☻

Důsledek 1 *Stromová (tudíž i obecná) resoluce je úplný důkazový systém pro DNF, tj. pro konečnou nesplnitelnou množinu klauzulí existuje stromový resoluční důkaz sporu.*

Věta 2 (Efektivní interpolace pro resoluci) *Existuje efektivní algoritmus A, který pro daný důkaz sporu z množiny klauzulí ve speciálním tvaru:*

$$\mathcal{C} = \{\varphi_i(\overline{p}, \overline{r})\}_{i \in I} \cup \{\psi_q(\overline{p}, \overline{q})\}_{j \in J}$$

Kde $\overline{p}, \overline{q}, \overline{r}$ jsou disjunktní množiny proměnných a z daného ohodnocení $\overline{a}$: $\overline{p} \to \{0, 1\}$ sestrojí důkaz sporu buď z první nebo druhé množiny v polynomiálním čase.

Poznámka 1 *Pokud je $\mathcal{C}$ nesplnitelná, potom alespoň jedna z těchto množin nesplnitelná.*