Třetí přednáška

NAIL062 Výroková a predikátová logika

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2023

Třetí přednáška

Program

- algebra výroků
- problém splnitelnosti
- 2-SAT a implikační grafů
- Horn-SAT a jednotková propagace
- algoritmus DPLL

Materiály

Zápisky z přednášky, Sekce 2.5 z Kapitoly 2, Kapitola 3

2.5 Algebra výroků

Výroky až na ekvivalenci

Kolik existuje výroků nad $\mathbb{P} = \{p, q, r\}$? Nekonečně mnoho. Až na ekvivalenci? Tolik, kolik je možných množin modelů: $2^{2^3} = 256$.

Výroky až na ekvivalenci studujeme pomocí jejich množin modelů.

Ekvivalenční třídy: $\mathrm{VF}_{\mathbb{P}}/\sim$, např. $[p \to q]_\sim = \{p \to q, \neg p \vee q, \dots\}$

Přiřazení modelů: $h : \mathrm{VF}_{\mathbb{P}}/\sim \;\to \mathcal{P}(\mathrm{M}_{\mathbb{P}})$ definované $h([\varphi]_\sim) = \mathrm{M}(\varphi)$ (je dobře definované, prosté, pro konečný jazyk bijekce)

Na $\mathrm{VF}_{\mathbb{P}}/\sim$ zavedeme operace $\neg, \wedge, \vee$ pomocí reprezentantů:

$$\neg[\varphi]_\sim = [\neg\varphi]_\sim$$
$$[\varphi]_\sim \wedge [\psi]_\sim = [\varphi \wedge \psi]_\sim$$
$$[\varphi]_\sim \vee [\psi]_\sim = [\varphi \vee \psi]_\sim$$

přidáme konstanty $\bot = [\bot]_\sim, \top = [\top]_\sim$, máme *Booleovu algebru*: algebru výroků jazyka $\mathbb{P}$; totéž relativně k teorii T (použijeme $\sim_T$)

Algebra výroků

Algebra výroků jazyka $\mathbb{P}$ resp. teorie T:

$$\mathbf{AV}_{\mathbb{P}} = \langle {}^{\mathrm{VF}_{\mathbb{P}}}/{\sim}; \neg, \wedge, \vee, \bot, \top \rangle$$

$$\mathbf{AV}_{\mathbb{P}}(T) = \langle {}^{\mathrm{VF}_{\mathbb{P}}}/{\sim_T}; \neg_T, \wedge_T, \vee_T, \bot_T, \top_T \rangle$$

přiřazení modelů h je prosté zobrazení algebry výroků jazyka do potenční algebry $\mathcal{P}(\mathrm{M}_{\mathbb{P}}) = \langle \mathcal{P}(\mathrm{M}_{\mathbb{P}}); \overline{}, \cap, \cup, \emptyset, \mathrm{M}_{\mathbb{P}} \rangle$ zachovávající operace a konstanty: $h(\bot) = \emptyset$, $h(\top) = \mathrm{M}_{\mathbb{P}}$, a

$$h(\neg[\varphi]_{\sim}) = \overline{h([\varphi]_{\sim})} = \overline{\mathrm{M}(\varphi)} = \mathrm{M}_{\mathbb{P}} \setminus \mathrm{M}(\varphi)$$

$$h([\varphi]_{\sim} \wedge [\psi]_{\sim}) = h([\varphi]_{\sim}) \cap h([\psi]_{\sim}) = \mathrm{M}(\varphi) \cap \mathrm{M}(\psi)$$

$$h([\varphi]_{\sim} \vee [\psi]_{\sim}) = h([\varphi]_{\sim}) \cup h([\psi]_{\sim}) = \mathrm{M}(\varphi) \cup \mathrm{M}(\psi)$$

tj. je to homomorfismus Booleových algeber, a nad konečným jazykem bijekce, tzv. izomorfismus; stejně pro algebru výroků teorie

Důsledek: Pro bezespornou teorii T nad *konečným* jazykem $\mathbb{P}$ je algebra výroků $\mathbf{AV}_{\mathbb{P}}(T)$ izomorfní potenční algebře $\mathcal{P}(\mathrm{M}_{\mathbb{P}}(\mathbf{T}))$ prostřednictvím zobrazení $h([\varphi]_{\sim_T}) = M(T, \varphi)$.

Počítání až na ekvivalenci

Tvrzení: Mějme n-prvkový jazyk $\mathbb{P}$ a bezespornou teorii T mající právě k modelů. Potom v jazyce $\mathbb{P}$ existuje až na ekvivalenci:

- 2^{2^n} výroků (resp. teorií),
- 2^{2^n-k} výroků pravdivých (resp. lživých) v T,
- $2^{2^n} - 2 \cdot 2^{2^n-k}$ výroků nezávislých v T,
- 2^k jednoduchých extenzí teorie T (z toho 1 sporná),
- k kompletních jednoduchých extenzí T.

Dále až na T-ekvivalenci existuje:

- 2^k výroků,
- 1 výrok pravdivý v T, 1 lživý v T,
- $2^k - 2$ výroků nezávislých v T.

Důkaz: stačí spočítat možné množiny modelů $\square$

Kapitola 3: Problém splnitelnosti

Problém splnitelnosti Booleovských formulí

Problém SAT:

- vstup: výrok φ v CNF
- otázka: je φ splnitelný?

univerzální problém: každou teorii nad konečným jazykem lze převést do CNF

Cook-Levinova věta: SAT je NP-úplný (důkaz: formalizuj výpočet nedeterministického Turingova stroje ve výrokové logice)

ale některé *fragmenty* jsou v P, efektivně řešitelné, např. 2-SAT a Horn-SAT (viz Sekce 3.2 a 3.3)

praktický problém: moderní *SAT solvery* (viz Sekce 3.1) se používají v řadě odvětví aplikované informatiky, poradí si s obrovskými instancemi

3.1 SAT solvery

SAT solvery

- existují od 60. let 20. století, v 21. století dramatický rozvoj dnes až 10^8 proměnných, viz www.satcompetition.org.
- nejčastěji založeny na jednoduchém algoritmu DPLL (viz Sekce 3.4), umí i najít řešení (model)
- řada technologií pro efektivnější řešení instancí pocházejících z různých aplikačních domén, heuristiky pro řízení prohledávání (za použití ML, NN) — desítky tisíc řádků kódu

Praktická ukázka:

Boardomino: Lze pokrýt šachovnici s chybějícími dvěma protilehlými rohy perfektně pokrýt kostkami domina?

těžká instance SATu (proč?), jak zakódovat?

řešič Glucose, formát vstupu: DIMACS CNF

3.2 2-SAT a implikační graf

3.3 Horn-SAT a jednotková propagace

3.4 DPLL algoritmus pro řešení problému SAT