NAIL062 V&P Logika: 3. sada příkladů – Algebra výroků, Problém SAT

Výukové cíle: Po absolvování cvičení student

- rozumí souvislosti výroků/teorií až na $[T$-]ekvivalenci a množin modelů (tzv. algebra výroků), umí aplikovat v konkrétních příkladech
- umí zakódovat daný problém jako instanci problému SAT
- získal praktickou zkušenost s použitím SAT solveru
- rozumí algoritmu pro řešení 2-SAT pomocí implikačního grafu (včetně nalezení všech modelů), umí aplikovat na příkladě
- rozumí algoritmu pro řešení Horn-SAT pomocí jednotkové propagace , umí aplikovat na příkladě
- rozumí algoritmu DPLL a umí jej aplikovat na příkladě

Příklady na cvičení

Příklad 1. Nechť $|\mathbb{P}| = n$ a mějme výrok $\varphi \in \mathrm{VF}_{\mathbb{P}}$ takový, že $|M(\varphi)| = k$. Určete počet až na ekvivalenci:

(a) výroků ψ takových, že $\varphi \models \psi$ nebo $\psi \models \varphi$,
(b) teorií nad $\mathbb{P}$, ve kterých platí φ,
(c) kompletních teorií nad $\mathbb{P}$, ve kterých platí φ,
(d) teorií T nad $\mathbb{P}$ takových, že $T \cup \{\varphi\}$ je bezesporná.

Uvažme navíc spornou teorii $\{\varphi, \psi\}$ kde $|M(\psi)| = p$. Spočtěte až na ekvivalenci:

(e) výroky χ takové, že $\varphi \vee \psi \models \chi$,
(f) teorie, ve kterých platí $\varphi \vee \psi$.

Řešení. *(a) Podmínku vyjádříme pomocí množin modelů:* $\mathrm{M}(\varphi) \subseteq \mathrm{M}(\psi)$ *nebo* $\mathrm{M}(\psi) \subseteq \mathrm{M}(\varphi)$. *Víme, že všech modelů je* 2^n, *a* $|\mathrm{M}(\varphi)| = k$. *Chceme spočítat, kolik je možných množin* $\mathrm{M}(\psi)$. *Podmínku* $\mathrm{M}(\varphi) \subseteq \mathrm{M}(\psi)$ *splňuje* 2^{2^n-k} *množin (tj. tolik je nadmnožin dané k-prvkové množiny uvnitř* 2^n*-prvkové množiny), podmínku* $\mathrm{M}(\psi) \subseteq \mathrm{M}(\varphi)$ *splňuje* 2^k *množin. Musíme ale být opatrní, abychom případ* $\mathrm{M}(\psi) = \mathrm{M}(\varphi)$ *nezapočítali dvakrát. Celkem máme* $2^{2^n-k} + 2^k - 1$ *možných množin modelů, tedy výroků* ψ *až na ekvivalenci.*

(b) $T \models \varphi$ *právě když* $\mathrm{M}(T) \subseteq \mathrm{M}(\varphi)$, *takových množin* $\mathrm{M}(T)$ *je* 2^k

(c) Navíc máme podmínku $|\mathrm{M}(T)| = 1$, *1-prvkových podmnožin k-prvkové množiny je k.*

(d) Přeloženo do řeči modelů, podmínka říká, že $\mathrm{M}(T \cup \{\varphi\}) \neq \emptyset$. *Máme* $\mathrm{M}(T \cup \{\varphi\}) = \mathrm{M}(T, \varphi) = \mathrm{M}(T) \cap \mathrm{M}(\varphi)$ *(jde o modely, ve kterých platí zároveň* T *a* φ*). Počítáme tedy kolik možných množin* $\mathrm{M}(T)$ *má neprázdný průnik s k-prvkovou množinou* $\mathrm{M}(\varphi)$. *To lze vyjádřit např. jako* $(2^k - 1) \cdot (2^{2^n-k})$, *kde* $2^k - 1$ *je počet možných (neprázdných) "průniků"* $\mathrm{M}(T) \cap \mathrm{M}(\varphi)$, *a* 2^{2^n-k} *znamená, že pro modely, ve kterých neplatí* φ, *si můžeme libovolně zvolit, zda budou v naší množině.*

(e) Protože $\{\varphi, \psi\}$ *je sporná, víme, že* $\emptyset = \mathrm{M}(\varphi, \psi) = \mathrm{M}(\varphi) \cap \mathrm{M}(\psi)$. *Počítáme množiny* $\mathrm{M}(\chi)$ *takové, že* $\mathrm{M}(\varphi \vee \psi) \subseteq \mathrm{M}(\chi)$. *Díky Lindenbaum-Tarského algebře víme, že* $\mathrm{M}(\varphi \vee \psi) = \mathrm{M}(\varphi) \cup \mathrm{M}(\psi)$. *Z disjunktnosti máme* $|\mathrm{M}(\varphi) \cup \mathrm{M}(\psi)| = k + p$, *snadno spočítáme, že množných množin modelů* $\mathrm{M}(\chi)$ *je* $2^{2^n-(k+p)}$.

(f) $\mathrm{M}(T)$ *musí být podmnožinou* $(k + p)$*-prvkové* $\mathrm{M}(\varphi \vee \psi)$, *je jich tedy* 2^{k+p}.

Příklad 2. Sestrojte implikační graf daného 2-CNF výroku. Je splnitelný? Pokud ano, najděte nějaké řešení: (a) výrok φ níže, (b) $\varphi \wedge \neg p_1$, (c) $\varphi \wedge \neg p_1 \wedge (p_1 \vee p_2)$.

$$\varphi = (p_1 \vee \neg p_2) \wedge (p_2 \vee p_3) \wedge (\neg p_3 \vee \neg p_1) \wedge (\neg p_3 \vee \neg p_4) \wedge (p_4 \vee p_5) \wedge (\neg p_5 \vee \neg p_1)$$

Řešení. *(a) Sestrojíme implikační graf. Zjistíme, že má dvě komponenty silné souvislosti:* $C = \{p_1, p_2, \neg p_3, p_4, \neg p_5\}$ *a* $\overline{C} = \{\neg p_1, \neg p_2, p_3, \neg p_4, p_5\}$*, nevede mezi nimi žádná hrana. Po kontrakci komponent tedy máme dvouvrcholový graf* $\mathcal{G}^*$ *bez hran, ten má dvě topologická uspořádání:* $(C, \overline{C})$ *a* $(\overline{C}, C)$*, která odpovídají modelům* $(0,0,1,0,1)$ *a* $(1,1,0,1,0)$.

(b) Komponenty jsou stejné, ale do $\mathcal{G}^*$ *přibude hrana* $C \to \overline{C}$*, tedy jediné topologické uspořádání je* $(C, \overline{C})$*, což odpovídá modelu* $(0,0,1,0,1)$.

(c) Implikační graf je nyní silně souvislý, tedy jeho jediná komponenta obsahuje (všechny) dvojice opačných literálů. To znamená, že výrok je nesplnitelný.

Příklad 3. Pomocí jednotkové propagace zjistěte, zda je následující Hornův výrok splnitelný. Pokud ano, najděte nějaké splňující ohodnocení.

$$(\neg p_1 \vee p_2 \vee \neg p_3) \wedge (\neg p_1 \vee p_2) \wedge p_1 \wedge (\neg p_1 \vee \neg p_2 \vee p_3) \wedge$$
$$(p_1 \vee \neg p_2 \vee \neg p_4) \wedge (\neg p_2 \vee \neg p_3 \vee \neg p_4) \wedge (p_4 \vee \neg p_5 \vee \neg p_6)$$

Řešení. *Provádíme postupně jednotkovou propagaci přes literály* $p_1, p_2, p_3, \neg p_4$*, zbývá výrok* $\neg p_5 \vee \neg p_6$*. Ten stačí ohodnotit tak, aby alespoň jedna z výrokových proměnných* p_5, p_6 *byla ohodnocená nulou. Modely výroku jsou tedy:* $\{(1,1,1,0,0,1), (1,1,1,0,1,0), (1,1,1,0,1,1)\}$

Příklad 4. Pomocí algoritmu DPLL rozhodněte, zda je následující CNF formule splnitelná:

$$(\neg p_1 \vee \neg p_2) \wedge (\neg p_1 \vee p_2) \wedge (p_1 \vee \neg p_2) \wedge (p_2 \vee \neg p_3) \wedge (p_1 \vee p_3)$$

Řešení. *Výrok neobsahuje jednotkovou klauzuli ani literál s čistým výskytem, musíme tedy větvit, např. přes* p_1*:*

- *Z* $\varphi \wedge p_1$ *dostáváme po jednotkové propagaci* $\neg p_2 \wedge p_2 \wedge (p_2 \vee \neg p_3)$*, po jednotkové propagaci přes* $\neg p_2$ *dostáváme* $\square \wedge \neg p_3$*, což obsahuje prázdnou klauzuli* $\square$*, tedy je nesplnitelné.*
- *Z* $\varphi \wedge \neg p_1$ *dostáváme po jednotkové propagaci* $\neg p_2 \wedge (p_2 \vee \neg p_3) \wedge p_3$*, po jednotkové propagaci přes* $\neg p_2$ *dostáváme* $\neg p_3 \wedge p_3$*, po jednotkové propagaci přes* $\neg p_3$ *dostáváme prázdnou klauzuli* $\square$*, tedy opět je nesplnitelné.*

V obou (všech) větvích výpočtu jsme dokázali nesplnitelnost, výrok je tedy nesplnitelný.

Příklad 5. Mějme daný orientovaný graf. Chceme zjistit, zda je acyklický, a pokud ano, nalézt nějaké jeho topologické uspořádání. Zakódujte tento problém do SAT.

Řešení. *Řešení jen naznačíme. Jako jazyk zvolme* $\mathbb{P} = \{p_{uv} \mid u, v \in V\}$*, kde* p_{uv} *bude znamenat, že vrchol* u *je v topologickém uspořádání (ostře) před* v*. To, že jde o ostré uspořádání, vyjádříme pomocí následujících axiomů:*

- $\neg p_{vv}$ *pro všechna* $v \in V$
- $p_{uv} \to \neg p_{vu}$ *pro všechna* $u, v \in V$
- $p_{uv} \wedge p_{vw} \to p_{uw}$ *pro všechna* $u, v, w \in V$

Zbývá vyjádřit, že všechny grafové hrany vedou v topologickém uspořádání dopředu:

- p_{uv} *pro všechny hrany* $(u, v) \in E$

Nakonec axiomy výše převedeme do CNF, v množinovém zápisu dostáváme:

$$S = \{\{\neg p_{vv}\}, \{\neg p_{uv}, \neg p_{vu}\}, \{\neg p_{uv}, \neg p_{vw}, \neg p_{uw}\} \mid u, v, w \in V\} \cup \{\{p_{uv}\} \mid (u, v) \in E\}$$

Další příklady k procvičení

Příklad 6. Uvažme následující výroky φ a ψ nad $\mathbb{P} = \{p, q, r, s\}$:

$$\varphi = (\neg p \vee q) \rightarrow (p \wedge r)$$
$$\psi = s \rightarrow q$$

(a) Určete počet (až na ekvivalenci) výroků χ nad $\mathbb{P}$ takových, že $\varphi \wedge \psi \models \chi$.
(b) Určete počet (až na ekvivalenci) úplných teorií T nad $\mathbb{P}$ takových, že $T \models \varphi \wedge \psi$.
(c) Najděte nějakou axiomatizaci pro každou (až na ekvivalenci) kompletní teorii T nad $\mathbb{P}$ takovou, že $T \models \varphi \wedge \psi$.

Příklad 7. Pomocí algoritmu jednotkové propagace najděte všechny modely:

$$(\neg a \vee \neg b \vee c \vee \neg d) \wedge (\neg b \vee c) \wedge d \wedge (\neg a \vee \neg c \vee e) \wedge$$
$$(\neg c \vee \neg d) \wedge (\neg a \vee \neg d \vee \neg e) \wedge (a \vee \neg b \vee \neg e)$$

Příklad 8. Řešte pomocí implikačního grafu jako v Příkladu 2, a také pomocí algoritmu DPLL jako v Příkladu 4:

(a) $(p_1 \vee \neg p_2) \wedge (p_2 \vee p_3) \wedge (\neg p_3 \vee p_1) \wedge (\neg p_3 \vee \neg p_4) \wedge (p_4 \vee p_5) \wedge (\neg p_5 \vee p_1)$
(b) $(p_0 \vee p_2) \wedge (p_0 \vee \neg p_3) \wedge (p_1 \vee \neg p_3) \wedge (p_1 \vee \neg p_4) \wedge (p_2 \vee \neg p_4) \wedge (p_0 \vee \neg p_5) \wedge (p_1 \vee \neg p_5) \wedge (p_2 \vee \neg p_5) \wedge (\neg p_1 \vee \neg p_6) \wedge (p_4 \vee p_6) \wedge (p_5 \vee p_6) \wedge p_1 \wedge \neg p_7$

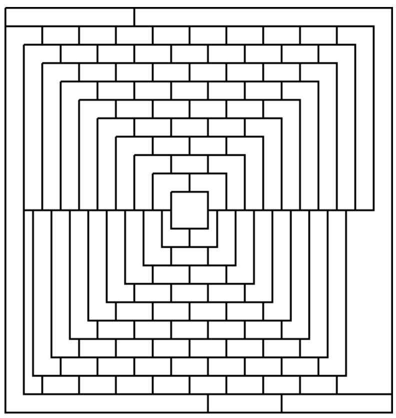
Příklad 9. Lze obarvit čísla od 1 do n dvěma barvami tak, že neexistuje monochromatické řešení rovnice $a + b = c$ pro žádná $1 \leq a < b < c \leq n$? Sestrojte výrokovou formuli φ_n v CNF která je splnitelná, právě když to lze. Zkuste nejprve $n = 8$.

Zkuste si doma: Napište skript generující φ_n v DIMACS CNF formátu. Použijte SAT solver k nalezení nejmenšího n pro které takové obarvení neexistuje (tj. každé 2-obarvení obsahuje monochromatickou trojici $a < b < c$ takovou, že $a + b = c$).

Příklad 10. Věta o čtyřech barvách říká, že následující mapy lze obarvit 4 barvami tak, že žádné dva sousedící regiony nemají stejnou barvu. Najděte takové obarvení pomocí SAT solveru.

(a) Mapa krajů Česka

(b) Těžší instance



K zamyšlení

Příklad 11. Pro danou formuli φ v CNF najděte a 3-CNF formuli φ' takovou, že φ' je splnitelná, právě když φ je splnitelná. Popište efektivní algoritmus konstrukce φ' je-li dána φ (tj. *redukci* z problému SAT do problému 3-SAT).

Příklad 12. Zakódujte problém setřídění dané n-tice celých čísel do SAT.

Příklad 13. Zakódujte do SAT známou hádanku o farmáři, který potřebuje přepravit přes řeku vlka, kozu, a hlávku zelí.