Prednášky z Matematiky (4) – Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Katedra aplikovanej informatiky
FMFI UK Bratislava

Letný semester 2015/2016

2. prednáška

Sémantika výrokovej logiky

29. februára 2016

Obsah 2. prednášky

1. Výroková logika
   - Opakovanie – Syntax
   - Sémantika výrokovej logiky
   - Tautológie, splniteľnosť, ekvivalencia

Syntax – Symboly jazyka výrokovej logiky

Syntax výrokovej logiky definuje,
aké symboly používa jazyk výrokovej logiky
a aké postupnosti týchto symbolov považujeme za správne vytvorené formuly jazyka výrokovej logiky.

Definícia

Symbolmi jazyka výrokovej logiky sú:

- *výrokové premenné* z nejakej nekonečnej spočítateľnej množiny $\mathcal{V} = \{p_1, p_2, \dots, p_n, \dots\}$ neobsahujúcej symboly ¬, ∧, ∨, →, (a);
- *logické* symboly (*logické spojky*): ¬, ∧, ∨, →, „*ak . . . , tak . . .* “);
- *pomocné* symboly: (a).

Spojka ¬ je *unárna* (má jeden argument).
Spojky ∧, ∨, → sú *binárne* (majú dva argumenty).

Syntax – Formuly a jednoznačnosť rozkladu

Definícia

Formulou výrokovej logiky (skrátene *formulou*) je postupnosť symbolov vytvorená nasledovnými rekurzívnymi pravidlami:

- Každá výroková premenná je (*atomická*) formula.
- Ak A je formula, tak aj $\neg A$ je formula.
- Ak A a B sú formuly, tak aj $(A \wedge B)$, $(A \vee B)$ a $(A \rightarrow B)$ sú formuly.

Nič iné nie je formulou.

Veta (o jednoznačnosti rozkladu)

Pre každú formulu X platí práve jedna z nasledujúcich možností:

- *X je výroková premenná.*
- *Existuje práve jedna formula A taká, že $X = \neg A$.*
- *Existujú práve jedna dvojica formúl A, B a jedna spojka $b \in \{\wedge, \vee, \rightarrow\}$ také, že $X = (A\, b\, B)$.*

Stupeň formuly a indukcia

Definícia (Stupeň formuly $\deg(X)$)

- Výroková premenná je stupňa 0.
- Ak A je stupňa n, tak $\neg A$ je stupňa $n + 1$.
- Ak A je stupňa n_1 a B je stupňa n_2, tak $(A \land B)$, $(A \lor B)$ a $(A \to B)$ sú stupňa $n_1 + n_2 + 1$.

Veta (Princíp indukcie na stupeň formuly)

Nech P je ľubovoľná vlastnosť formúl ($P \subseteq \mathcal{E}$). Ak platí, že

1° *každá formula stupňa* 0 *má vlastnosť P,*

2° *z predpokladu, že X je formula a všetky formuly menšieho stupňa ako* $\deg(X)$ *majú vlastnosť P, vyplýva, že aj X má vlastnosť P,*

tak všetky formuly majú vlastnosť P ($P = \mathcal{E}$).

Množina výrokových premenných formuly

Definícia (vars(X))

- Ak p je výroková premenná, množinou výrokových premenných atomickej formuly p je $\{p\}$.
- Ak V je množina výrokových premenných formuly A, tak V je tiež množinou výrok. prem. formuly $\neg A$.
- Ak V_1 je množina výrok. prem. formuly A a V_2 je množina výrok. prem. formuly B, tak $V_1 \cup V_2$ je množinou výrok. prem. formúl $(A \land B)$, $(A \lor B)$ a $(A \to B)$.

Definícia (vars(X) stručnejšie)

- Ak p je výroková premenná, tak $\mathrm{vars}(p) = \{p\}$.
- Ak A a B sú formuly, tak $\mathrm{vars}(\neg A) = \mathrm{vars}(A)$ a $\mathrm{vars}((A \land B)) = \mathrm{vars}((A \lor B)) = \mathrm{vars}((A \to B)) = \mathrm{vars}(A) \cup \mathrm{vars}(B)$.

Sémantika výrokovej logiky

Syntax jazyka výrokovej logiky hovorí iba o postupnostiach symbolov.
Samé o sebe tieto postupnosti nemajú žiaden ďalší *význam*.
Ten im dáva *sémantika* jazyka výrokovej logiky.
Za význam výrokov považujeme ich pravdivostnú hodnotu.

Ohodnotenie výrokových premenných

Výrokové premenné predstavujú jednoduché výroky.
Ich *význam* (pravdivosť) nie je pevne daný.
Môže závisieť od situácie, stavu sveta
(Sára ide na párty, svieti slnko, zobral som si dáždnik, ...).
Pravdivosť výrokových premenných v nejakej situácii matematicky popíšeme ohodnotením.

Definícia

Nech $\{t, f\}$ je množina dvoch rôznych pravdivostných hodnôt, pričom hodnota t predstavuje pravdu a f nepravdu.
Ohodnotením množiny výrokových premenných $\mathcal{V}$ nazveme každé zobrazenie (funkciu) v množiny $\mathcal{V}$ do množiny $\{t, f\}$.
Výroková premenná p je *pravdivá* pri ohodnotení v, ak $v(p) = t$.
Výroková premenná p je *nepravdivá* pri ohodnotení v, ak $v(p) = f$.

Ohodnotenie výrokových premenných

Príklad

Zoberme $t \neq f$ (napr. $t = 1$, $f = 0$), $\mathcal{V} = \{\text{a}, \text{á}, \text{ä}, \dots, \text{ž}, 0, \dots, 9, \_\}^+$.
Dnešné ráno by popísalo ohodnotenie v množiny $\mathcal{V}$, kde (okrem iného):

$$v(\text{svieti\_slnko}) = f \qquad v(\text{zobral\_som\_si\_dáždnik}) = f$$

včerajšie

$$v(\text{svieti\_slnko}) = t \qquad v(\text{zobral\_som\_si\_dáždnik}) = f$$

Jednu zo situácií v probléme pozývania kamarátov na párty by popísalo ohodnotenie, v ktorom (okrem iného):

$$v(\text{sara}) = t \qquad v(\text{kim}) = f \qquad v(\text{jim}) = t$$

Prečo „okrem iného“?

Splĺňanie výrokových formúl

Definícia

Nech v je ohodnotenie množiny výrokových premenných $\mathcal{V}$. Pre všetky výrokové premenné p z $\mathcal{V}$ a všetky formuly A, B nad $\mathcal{V}$ definujeme:

- v splĺňa atomickú formulu p vtt $v(p) = t$;
- v splĺňa formulu $\neg A$ vtt v nesplĺňa A;
- v splĺňa formulu $(A \wedge B)$ vtt v splĺňa A a v splĺňa B;
- v splĺňa formulu $(A \vee B)$ vtt v splĺňa A alebo v splĺňa B;
- v splĺňa formulu $(A \to B)$ vtt v nesplĺňa A alebo v splĺňa B.

Skratka *vtt* znamená *vtedy a len vtedy, keď*.
Vzťah *ohodnotenie v splĺňa formulu X* skrátene zapisujeme $v \models X$, *ohodnotenie v nesplĺňa formulu X* zapisujeme $v \not\models X$.

Splňanie výrokových formúl

Príklad

Nech v je ohodnotenie množiny $\mathcal{V} = \{\mathsf{a}, \ldots, \mathsf{z}\}^+$, také že

$$v(\mathsf{kim}) = t \qquad v(\mathsf{jim}) = f \qquad v(\mathsf{sara}) = t.$$

Zistime, ktoré z formúl

$$((\mathsf{kim} \lor \mathsf{jim}) \lor \mathsf{sara})$$
$$(\mathsf{kim} \to \neg\mathsf{sara}) \qquad (\mathsf{jim} \to \mathsf{kim}) \qquad (\neg\mathsf{jim} \to \neg\mathsf{sara})$$

ohodnotenie v spĺňa a ktoré nespĺňa:

0. Spĺňa atomické formuly kim a sara, a nespĺňa jim;
1. spĺňa formuly $\neg\mathsf{jim}$, $(\mathsf{kim} \lor \mathsf{jim})$, $(\mathsf{jim} \to \mathsf{kim})$, a nespĺňa $\neg\mathsf{sara}$;
2. spĺňa formulu $((\mathsf{kim} \lor \mathsf{jim}) \lor \mathsf{sara})$, a nespĺňa $(\mathsf{kim} \to \neg\mathsf{sara})$;
3. nespĺňa $(\neg\mathsf{jim} \to \neg\mathsf{sara})$.

Splňanie výrokových formúl

Dohoda

V ďalších definíciách a tvrdeniach predpokladáme, že sme si *pevne zvolili* nejakú množinu výrokových premenných $\mathcal{V}$ a hodnoty t, f.
Všetky formuly sú skonštruované nad množinou výrokových premenných $\mathcal{V}$.
„Ohodnotením“ rozumieme ohodnotenie množiny výrokových premenných $\mathcal{V}$.

Tvrdenie

Splnenie výrokovej formuly pri ohodnotení výrokových premenných závisí iba od ohodnotenia (konečného počtu) výrokových premenných, ktoré sa v nej vyskytujú.
Presnejšie: *Pre každú formulu X a všetky ohodnotenia v a v', ktoré zhodujú na množine výrokových premenných vyskytujúcich sa v X, platí $v \models X$ vtt $v' \models X$.*

Splňanie výrokových formúl

Dôkaz.

Indukciou na stupeň formuly X.

Báza: Nech X je stupňa 0. Podľa vety o jednoznačnosti rozkladu a definície stupňa musí byť $X = p$ pre nejakú výrokovú premennú. Zoberme ľubovoľné ohodnotenia v a v', ktoré sa zhodujú na premenných v X, teda na p. Podľa definície splňania $v \models p$ vtt $v(p) = t$ vtt $v'(p) = t$ vtt $v' \models p$.

Krok: Nech X je stupňa $n > 0$ a tvrdenie platí pre všetky formuly stupňa nižšieho ako n (indukčný predpoklad). Zoberme ľubovoľné ohodnotenia v a v', ktoré sa zhodujú na premenných v X. Podľa definície stupňa a jednoznačnosti rozkladu nastáva práve jeden z prípadov:

- $X = \neg A$ pre práve jednu formulu A. Pretože $\deg(X) = \deg(A) + 1 > \deg(A)$, podľa ind. predpokladu tvrdenie platí pre A. Ohodnotenia v a v' sa zhodujú na premenných v A (rovnaké ako v X). Preto $v \models A$ vtt $v' \models A$, a teda $v \models \neg A$ vtt $v \not\models A$ vtt $v' \not\models A$ vtt $v' \models \neg A$.
- $X = A \wedge B$ pre práve jednu dvojicu formúl A, B. ...

$\square$

Tautológia a splniteľnosť

Definícia

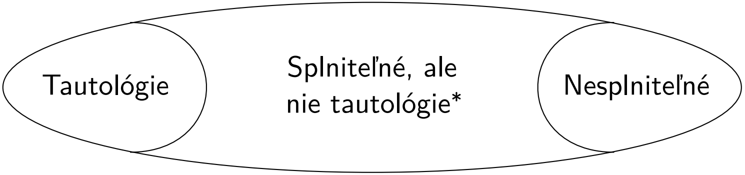
Formulu X nazveme *tautológiou* (skrátene $\models X$) vtt je splnená pri každom ohodnotení výrokových premenných.

Definícia

Formulu X nazveme *splniteľnou* vtt je splnená pri aspoň jednom ohodnotení výrokových premenných.

Tautológie sú výrokovologické pravdy. Sú zaujímavé najmä pre klasický pohľad na logiku ako skúmanie správneho usudzovania. Vo výpočtovej logike je zaujímavá splniteľnosť a konkrétne spĺňajúce ohodnotenia.

„Geografia“ výrokových formúl podľa splňania



(Papadimitriou, 1994)

* „Občas splnené“

Tautológie a (ne)splniteľnosť

Tvrdenie

Formula X je tautológia vtt keď $\neg X$ je nesplniteľná.

Dôkaz.

($\Rightarrow$) Nech X je tautológia, teda je splnená pri každom ohodnotení výrokových premenných. To znamená, že $\neg X$ je nesplnená pri každom boolovskom ohodnotení (podľa definície spĺňania pri ohodnotení) a teda neexistuje žiadne ohodnotenie, pri ktorom by $\neg X$ bola splnená, teda $\neg X$ nie je splniteľná.
($\Leftarrow$) Opačne, nech $\neg X$ je nesplniteľná. To znamená, že pri každom ohodnotení výrokových premenných je $\neg X$ nesplnená a podľa definície spĺňania je teda X pri každom ohodnotení splnená a teda je tautológia. $\square$

Ekvivalencia formúl

Definícia

Dve formuly X a Y sú *výrokovologicky ekvivalentné* vtt ak pri každom ohodnotení výrokových premenných je X splnená vtt je splnená Y.

Tvrdenie

Formuly X a Y sú výrokovologicky ekvivalentné vtt formula $((X \to Y) \land (Y \to X))$ je tautológia.

Dôkaz na cvičeniach.

Dohoda

Formulu $((X \to Y) \land (Y \to X))$ budeme skrátene zapisovať $(X \leftrightarrow Y)$.

Spĺňanie množín výrokových formúl

Pojem spĺňania sa jednoducho rozšíri na množiny výrokových formúl.

Definícia

Nech S je množina formúl. Ohodnotenie *v spĺňa množinu formúl S* (alebo *je modelom S*; skrátene $v \models S$) práve vtedy, keď v spĺňa každú formulu X z množiny S.

Tvrdenie

Splnenie množiny výrokových formúl S pri ohodnotení výrokových premenných závisí iba od ohodnotenia výrokových premenných, ktoré sa vyskytujú vo formulách v S.

Presná formulácia je podobná ako pri spĺňaní formúl. Dôkaz sporom, lebo množina formúl môže byť nekonečná. Cvičenia?

Splniteľnosť a vyplývanie

Definícia

Množina formúl S je *súčasne výrokovologicky splniteľná* vtt existuje aspoň jedno ohodnotenie výrokových premenných, pri ktorom sú všetky formuly z S splnené.

Príklad

Párty príklad P – súčasne splniteľná množina formúl.
$P \cup \{\text{sara}\}$ – súčasne nesplniteľná množina formúl.

Všimnime si, že v každom ohodnotení, ktoré spĺňa P je premenná kim pravdivá.

Definícia (Vyplývanie)

Z množiny formúl S *výrokovologicky vyplýva* formula X (X je *výrokovologickým dôsledkom* S, skrátene $S \models X$) ak X je pravdivá pri každom ohodnotení výrokových premenných, ktoré spĺňa S.

Vyplývanie a (ne)splniteľnosť

Tvrdenie

Formula X výrokovologicky vyplýva z množiny formúl $S = \{X_1, X_2, \ldots, X_n\}$ vtt keď je množina $S' = \{X_1, X_2, \ldots, X_n, \neg X\}$ nesplniteľná.

Dôkaz možno na cvičeniach.

Dôkaz.

TODO: prehodiť na ohodnotenia premenných

($\Rightarrow$) Predpokladajme, že X vyplýva z množiny S, nech v je nejaké boolovské ohodnotenie. Potrebujeme ukázať, že v nespĺňa S'. Máme dve možnosti:

- Ak v nespĺňa S, tak nespĺňa ani S'.
- Ak v spĺňa S, tak X musí byť pravdivá pri v (definícia splniteľnosti). To znamená, že $\neg X$ je nepravidvá pri v a teda v nespĺňa S'.

($\Leftarrow$) Opačne, nech S' je nesplniteľná a nech v je nejaké boolovské ohodnotenie. v teda nespĺňa S'. Potrebujeme ukázať, že ak v spĺňa S, tak potom X je pravdivé pri v. Ak v spĺňa S, tak každé X_i je pravdivé pri v. Keďže ale v nespĺňa S', musí byť $\neg X$ (jediná zostávajúca formula z S') nepravdivé pri v, čo znamená, že X je

Nezávislosť

Definícia

Formula X je *nezávislá* od množiny formúl S, ak existuje dvojica ohodnotení v, v' spĺňajúcich S, pričom v spĺňa X, ale v' nespĺňa X.

Príklad

Atomická formula jim je nezávislá od P.

Pretože splnenie formuly závisí iba od ohodnotenia konečného počtu výrokových premenných, ktoré sa v nej nachádzajú, dá sa v konečnom čase určiť, či je formula splniteľná, či je tautológiou, či sú dve formuly ekvivalentné.
Treba preveriť 2^n prípadov, kde n je počet vyskytujúcich sa premenných.
Podobne pre konečné množiny formúl a vyplývanie z nich.
To ste už síce vedeli, ale teraz viete aj to, prečo je to tak.

Literatúra

PAPADIMITRIOU, C. H. *Computational complexity*. Addison-Wesley, 1994. ISBN 978-0-201-53082-7.

SMULLYAN, R. M. *Logika prvého rádu*. Alfa, 1979. Z angl. orig. *First-Order Logic*, Berlin-Heidelberg: Springer-Verlag, 1968 preložil Svätoslav Mathé.