Prednášky z Matematiky (4) – Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Katedra aplikovanej informatiky
FMFI UK Bratislava

Letný semester 2016/2017

3. prednáška

Vyplývanie, ekvivalentné úpravy

6. marca 2017

Obsah 3. prednášky

Ohodnotenie výrokových premenných

Definícia 3.18

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

Splnenie formuly ohodnotením premenných

Definícia 3.21

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

- v spĺňa atomickú formulu p vtt $v(p) = t$;
- v spĺňa formulu $\neg A$ vtt v nespĺňa A;
- v spĺňa formulu $(A \land B)$ vtt v spĺňa A a v spĺňa B;
- v spĺňa formulu $(A \lor B)$ vtt v spĺňa A alebo v spĺňa B;
- v spĺňa formulu $(A \to B)$ vtt v nespĺňa A alebo v spĺňa B.

Dohoda

Reláciu *ohodnotenie v spĺňa formulu X* skrátene zapisujeme $v \models X$. V ďalších definíciách a tvrdeniach predpokladáme, že sme si *pevne zvolili* nejakú množinu výrokových premenných $\mathcal{V}$ a hodnoty t, f.

Splňanie formuly ohodnoteniami

Tvrdenie 3.23

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_1 a v_2, ktoré zhodujú na množine výrokových premenných vyskytujúcich sa v X, platí $v_1 \models X$ vtt $v_2 \models X$.*

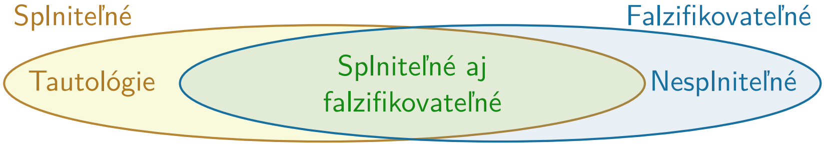
Dôsledok 3.24

Na preverenie všetkých možností splnenia a nesplnenia formuly X postačuje preveriť konečne veľa ohodnotení ($2^{|\mathrm{vars}(X)|}$), ktoré sa vzájomne líšia iba na množine výrokových premenných $\mathrm{vars}(X)$ vyskytujúcich sa v X.

Tautológia, (ne)splniteľnosť, falzifikovateľnosť

Definícia 3.25

- Formulu X nazveme *tautológiou* (skrátene $\models X$) vtt je splnená pri každom ohodnotení výrokových premenných.
- Formulu X nazveme *splniteľnou* vtt je splnená pri aspoň jednom ohodnotení výrokových premenných.
- Formulu X nazveme *nesplniteľnou* vtt nie je splniteľná.
- Formulu X nazveme *falzifikovateľnou* vtt je nesplnená pri aspoň jednom ohodnotení výrokových premenných.



Tautológie a (ne)splniteľnosť

Tvrdenie 3.26

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. Podľa definície spĺňania je teda X pri každom ohodnotení splnená, a teda je tautológia. $\square$

Teórie

Neformálne slovom *teória* označujeme nejaký súbor presvedčení o fungovaní sveta alebo jeho časti.

Definícia 3.27

(Výrokovologickou) teóriou nazývame každú množinu formúl.

Dohoda

Teórie budeme označovať písmenami T, S, podľa potreby s indexmi.

Príklad 3.28

Formalizácia problému pozývania známych na párty je teóriou:

$$\begin{aligned} T_{\text{party}} = \{\, &((\text{kim} \lor \text{jim}) \lor \text{sara}), && (\text{kim} \to \neg\text{sara}),\\ &(\text{jim} \to \text{kim}), && (\neg\text{jim} \to \neg\text{sara}) \,\} \end{aligned}$$

Splnenie teórie, model

Pojem spĺňania sa jednoducho rozšíri na teórie.

Definícia 3.29

Nech T je teória. Ohodnotenie v *spĺňa teóriu* T (skrátene $v \models T$) vtt v spĺňa každú formulu X z množiny T.
Spĺňajúce ohodnotenie nazývame *modelom* teórie T.

Príklad 3.30

Aké ohodnotenie spĺňa (teda je modelom) T_{party}?

Tvrdenie 3.31

Splnenie teórie T pri ohodnotení výrokových premenných závisí iba od ohodnotenia výrokových premenných, ktoré sa vyskytujú vo formulách v T.

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

Splniteľnosť teórie

- Kedy je teória „zlá“?
- Keď nepopisuje žiaden svet (stav sveta).
- „Dobrá“ je teda taká teória, ktorá má aspoň jeden model.

Definícia 3.32

Teória T je *súčasne (výrokovologicky) splniteľná* vtt existuje aspoň jeden model T, (t.j. ohodnotenie výrokových premenných, ktoré spĺňa všetky formuly z T).
Teória je *nesplniteľná* vtt nie je splniteľná.

Príklad 3.33

T_{party} je súčasne splniteľná množina formúl.
$T_{\text{party}} \cup \{\text{sara}\}$ je súčasne nesplniteľná množina formúl.

Výrokovologické vyplývanie

- Aký je účel teórií? Kedy je teória užitočná?
- Keď pomocou z nej dokážeme odvodiť doteraz neznáme skutočnosti, zistiť *uvažovaním* (alebo počítaním), čo vo svete platí, aj keď to priamo v teórii nie je zapísané.
- Takéto skutočnosti nazývame dôsledkami teórie a hovoríme, že z nej vyplývajú.

Príklad 3.34

Všimnime si, že v *každom* ohodnotení, ktoré spĺňa T_{party}, je premenná kim pravdivá.

Definícia 3.35 (Výrokovologické vyplývanie)

Z teórie T *výrokovologicky vyplýva* formula X (X je *výrokovologickým dôsledkom* T, skrátene $T \models X$) vtt každé ohodnotenie výrokových premenných, ktoré spĺňa T, spĺňa aj X.

Vyplývanie a (ne)splniteľnosť

Tvrdenie 3.36

Formula X výrokovologicky vyplýva z teórie T vtt množina $T_1 = T \cup \{\neg X\}$ je nesplniteľná.

Dôkaz.

Nech $T = \{X_1, X_2, \ldots, X_n, \ldots\}$.
($\Rightarrow$) Predpokladajme, že X vyplýva z množiny T. Nech v je nejaké ohodnotenie $\mathcal{V}$. Potrebujeme ukázať, že v nespĺňa T_1. Máme dve možnosti:

- Ak v nespĺňa T, tak nespĺňa ani T_1.
- Ak v spĺňa T, tak v musí spĺňať aj X (definícia vyplývania). To znamená, že $\neg X$ je nesplnená pri v, a teda v nespĺňa T_1.

($\Leftarrow$) Opačne, nech T_1 je nesplniteľná a nech v je nejaké ohodnotenie $\mathcal{V}$. v teda nespĺňa T_1. Potrebujeme ukázať, že ak v spĺňa T, tak potom v spĺňa aj X. Ak v spĺňa T, potom spĺňa každé X_i. Keďže ale v nespĺňa T_1, v musí nespĺňať $\neg X$ (jediná zostávajúca formula z T_1), čo znamená, že v spĺňa X. $\square$

Nezávislosť

Definícia 3.37

Formula X je *nezávislá* od teórie T, ak existuje dvojica ohodnotení v_1, v_2 spĺňajúcich T, pričom v_1 spĺňa X, ale v_2 nespĺňa X.

Príklad 3.38

Atomická formula jim je nezávislá od T_{party}.

Vzťahy vyplývania, implikácií a tautológií

Tvrdenia

- $T \cup \{A\} \models B$ vtt $T \models A \to B$
- $\{\} \models A$ vtt $\models A$ (A je tautológia)
- Nasledujúce tvrdenia sú ekvivalentné:
  - $\{A_1, A_2, \ldots, A_n\} \models B$
  - $\{((\cdots(A_1 \land A_2) \land \cdots) \land A_n)\} \models B$
  - $\{\} \models ((\cdots(A_1 \land A_2) \land \cdots) \land A_n) \to B)$
  - $\models (((\cdots(A_1 \land A_2) \land \cdots) \land A_n) \to B)$

Hlasujte

Spomeňte si III.1

Formula X vyplýva z teórie T vtt každý model T spĺňa X.
Pravda alebo nepravda?

Ekvivalencia formúl

Ako vieme pomocou doterajších sémantických pojmov vyjadriť, že dve formuly sú ekvivalentné?

Definícia 3.39

Dve formuly X a Y sú *(výrokovologicky) ekvivalentné* vtt pre každé ohodnotenie v výrokových premenných platí, že v spĺňa X vtt v spĺňa Y.

Ako súvisí ekvivalencia formúl so „spojkou" *práve vtedy, keď* $(\leftrightarrow)$?

Dohoda

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

Tvrdenie 3.40

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

Asociativita a komutativita konjunkcie a disjunkcie

Zjednodušenie zápisu formúl

Tvrdenie 3.41 (Asociativita a komutativita $\wedge$ a $\vee$)

Nech A_1, A_2, A_3 sú formuly.
Nasledujúce dvojice formúl sú ekvivalentné:

- $((A_1 \wedge A_2) \wedge A_3)$ *a* $(A_1 \wedge (A_2 \wedge A_3))$,
- $((A_1 \vee A_2) \vee A_3)$ *a* $(A_1 \vee (A_2 \vee A_3))$.

- $(A_1 \wedge A_2)$ *a* $(A_2 \wedge A_1)$,
- $(A_1 \vee A_2)$ *a* $(A_2 \vee A_1)$,

Ekvivalentné úpravy

Na Matematike (1) ste ekvivalente upravovali formuly.
Cieľom je zvyčajne formulu zjednodušiť alebo upraviť do požadovaného tvaru (napr. vstup pre SAT solver), prípadne ukázať, že je tautológia upravením na známu tautológiu.
Čo to ale vlastne je ekvivalentná úprava?

Definícia 3.42

Zobrazenie $u\colon \mathcal{E} \to \mathcal{E}$ nazveme *ekvivalentnou úpravou* vtt pre každú formulu A platí, že formuly A a $u(A)$ sú ekvivalentné.

Príklad *syntaktickej manipulácie* formúl s predvídateľným sémantickým výsledkom.

Ekvivalentné úpravy

Ekvivalentné úpravy zvyčajne pozostávajú z kombinácie:

- nahradenia podformuly A vo formule X formulou B, ktorá je ekvivalentná s A;

Príklad 3.43

$$A = \neg\neg p \qquad B = p \qquad (q \to \neg\neg\neg p) \rightsquigarrow (q \to \neg p)$$

- nahradenia formuly, ktorá vznikne dosadením formuly A za nejakú výrokovú premennú p vo formule X,
  formulou, ktorá vznikne dosadením A za rovnakú premennú vo formule Y ekvivalentnej s X.

Príklad 3.44

$$(\neg(r \to s) \land \neg q) \quad \rightsquigarrow \quad \neg((r \to s) \lor q)$$

$$X = (\neg p \land \neg q) \qquad Y = \neg(p \lor q)$$

$$A = (r \to s)$$

Substitúcia a ekvivalentné úpravy

Oba druhy ekvivalentných úprav sú založené na *substitúcii*.

Definícia 3.45 (Substitúcia)

Nech X, A, B sú formuly.
Substitúciou B *za* A *v* X (skrátene $X[A|B]$)) nazývame formulu, ktorá vznikne nahradením každého výskytu A v X formulou B.

Veta 3.46 (Ekvivalentné úpravy)

Nech X je formula, A a B sú ekvivalentné formuly.
Potom X a $X[A|B]$ sú tiež ekvivalentné.

Tvrdenie 3.47

Nech X je tautológia, a výroková premenná a Y ľubovoľná formula.
Potom $X[a|Y]$ je tiež tautológia.

Veta 3.48

Nech A, B a C sú ľubovoľné formuly, $\top$ je ľubovoľná tautológia a $\perp$ je ľubovoľná nesplniteľná formula.
Nasledujúce dvojice formúl sú ekvivalentné:

$(A \wedge (B \wedge C))$ a $((A \wedge B) \wedge C)$	*asociatívnosť*
$(A \vee (B \vee C))$ a $((A \vee B) \vee C)$	
$(A \wedge (B \vee C))$ a $((A \wedge B) \vee (A \wedge C))$	*distributívnosť*
$(A \vee (B \wedge C))$ a $((A \vee B) \wedge (A \vee C))$	
$(A \wedge B)$ a $(B \wedge A)$	*komutatívnosť*
$(A \vee B)$ a $(B \vee A)$	
$\neg(A \wedge B)$ a $(\neg A \vee \neg B)$	*de Morganove*
$\neg(A \vee B)$ a $(\neg A \wedge \neg B)$	*pravidlá*
$\neg\neg A$ a A	*dvojitá negácia*

Veta 3.48 (Pokračovanie)

$(A \land A)$ a A	*idempotencia*
$(A \lor A)$ a A	
$(A \land \top)$ a A	*identita*
$(A \lor \bot)$ a A	
$(A \lor (A \land B))$ a A	*absorpcia*
$(A \land (A \lor B))$ a A	
$(A \lor \neg A)$ a $\top$	*vylúč. tretieho*
$(A \land \neg A)$ a $\bot$	*spor*
$(A \to B)$ a $(\neg A \lor B)$	*nahradenie* $\to$

Dohoda

Nech $A_1, A_2, \ldots, A_n$ je konečná postupnosť formúl.

- Formulu $(((A_1 \land A_2) \land A_3) \land \cdots \land A_n)$ budeme skrátene zapisovať $(A_1 \land A_2 \land A_3 \land \cdots \land A_n)$, prípadne $\bigwedge_{i=1}^{n} A_i$ a nazývať *konjunkcia postupnosti formúl* $A_1, \ldots, A_n$.
- Formulu $(((A_1 \lor A_2) \lor A_3) \lor \cdots \lor A_n)$ budeme skrátene zapisovať $(A_1 \lor A_2 \lor A_3 \lor \cdots \lor A_n)$, prípadne $\bigvee_{i=1}^{n} A_i$ a nazývať *disjunkcia postupnosti formúl* $A_1, \ldots, A_n$.
- Pre $n = 1$ chápeme samotnú formulu A_1 ako konjunkciu aj ako disjunkciu jednoprvkovej postupnosti formúl A_1.
- Konjunkciu prázdnej postupnosti formúl ($n = 0$) chápeme ako ľubovoľnú tautológiu (napríklad $(p_1 \lor \neg p_1)$) a označujeme ju $\top$.
- Disjunkciu prázdnej postupnosti formúl chápeme ako ľubovoľnú nesplniteľnú formulu (napríklad $(p_1 \land \neg p_1)$) a označujeme ju $\bot$ alebo $\Box$.

Konjunktívna a disjunktívna normálna forma

Definícia 3.49

- Výrokovú premennú alebo negáciou premennej nazývame *literál*. Disjunkciu literálov nazývame *klauzula* (tiež „klauza“).
- Hovoríme, že formula X je v *disjunktívnom normálnom tvare* (DNF), ak X je disjunkciou formúl, z ktorých každá je konjunkciou literálov.
- Hovoríme, že formula X je v *konjunktívnom normálnom tvare* (CNF), ak X je konjunkciou klauz (formúl, z ktorých každá je disjunkciou literálov).

Príklad 3.50

- Literály: p, $\neg q$, ...
- Klauzuly: $(p \vee \neg q)$, ale aj p, $\perp$
- DNF: $((p \wedge \neg q) \vee (\neg p \wedge r) \vee (\neg p \wedge q \wedge \neg r))$,
  ale aj $(p \wedge \neg q)$, $(p \vee \neg q)$, q, $\neg p$
- CNF: $((\neg p \vee \neg q) \wedge (p \vee r) \wedge (p \vee q \vee \neg r))$,
  ale aj $(p \vee \neg q)$, $(p \wedge \neg q)$, q, $\neg p$

Literatúra

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

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