Prednášky z Matematiky (4) – Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Katedra aplikovanej informatiky
FMFI UK Bratislava

Letný semester 2017/2018

3. prednáška

Vyplývanie, ekvivalentné úpravy

5. marca 2018

Obsah 3. prednášky

- Tautológia, (ne)splniteľnosť, falzifikovateľnosť
- Výrokovologické vyplývanie
- Ekvivalencia formúl
- Ekvivalentné úpravy
- Konjunktívna a disjunktívna normálna forma

Opakovanie

Ohodnotenie výrokových premenných

Definícia 2.19

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 2.22

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.

Spĺňanie formuly ohodnoteniami

Tvrdenie 2.25

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

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.

2.4

Tautológia, (ne)splniteľnosť, falzifikovateľnosť

Tautológia, (ne)splniteľnosť, falzifikovateľnosť

Definície 2.24, 2.27, 2.28, 2.29

- 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 každé ohodnotenie výrokových premenných nespĺňa X.
- Formulu X nazveme *falzifikovateľnou* vtt je nesplnená pri aspoň jednom ohodnotení výrokových premenných.

Tautológie a (ne)splniteľnosť

Tvrdenie 2.30

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

Dôkaz.

($\Longrightarrow$) Nech X je tautológia, teda je splnená pri každom ohodnotení výrokových premenných. To znamená, že $\neg X$ je nesplnená pri každom ohodnotení (podľa definície splnenia formuly ohodnotením), a teda $\neg X$ je nesplniteľná.
($\Longleftarrow$) 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 2.31

(Výrokovologickou) teóriou nazývame každú množinu formúl.

Dohoda

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

Príklad 2.32

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 2.33

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 2.34

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

Tvrdenie 2.35

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.

2.5

Výrokovologické vyplývanie

Splniteľnosť teórie

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

Definícia 2.36

Teória T je *súčasne výrokovologicky splniteľná* (skrátene *splniteľná*) vtt existuje aspoň jeden model T.
Teória je *nesplniteľná* vtt nie je splniteľná.

Príklad 2.37

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

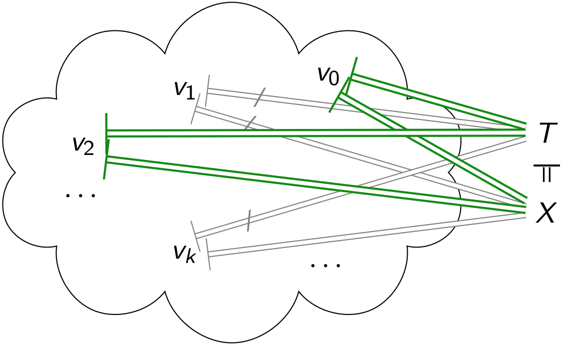
Logické dôsledky a vyplývanie

- Aký je *účel* teórií? Kedy je teória užitočná?
  - Keď z nej dokážeme *odvodiť* (uvažovaním alebo počítaním) *doteraz neznáme skutočnosti* (teda nezapísané v teórii), ktoré platia vo všetkých stavoch sveta spĺňajúcich teóriu.
- Takéto skutočnosti nazývame **logickými dôsledkami teórie** a hovoríme, že z nej *vyplývajú*.

Príklad 2.38

Všimnime si, že v *každom* ohodnotení, ktoré spĺňa T_{party},
je splnená aj premenná *kim*.
Ktorá ďalšia formula vyplýva z T_{party}?

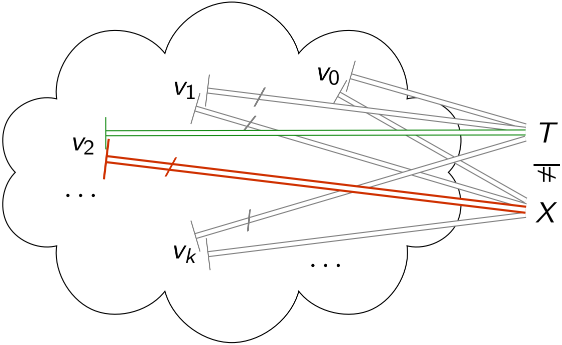
Výrokovologické vyplývanie



Definícia 2.39 (Výrokovologické vyplývanie)

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

Nevyplývanie



Príklad 2.40

Ktoré atomické formuly a ich negácie nevyplývajú z T_{party}?
Vyplýva z T_{party} formula $(kim \rightarrow jim)$?

Vyplývanie a (ne)splniteľnosť

Použitie SAT solvera na rozhodovanie vyplývania je založené na:

Tvrdenie 2.41

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

Dôkaz.

Nech $T = \{X_1, X_2, \dots, X_n, \dots\}$.
($\Rightarrow$) 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 2.42

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 2.43

Ktorá atomická formula je nezávislá od T_{party}?
Je aj jej negácia nezávislá od T_{party}?

Vzťahy vyplývania, implikácií a tautológií

Tvrdenie 2.44

Nech S a T sú teórie, $S \subseteq T$, A je formula.
Ak $S \models A$, tak $T \models A$.

Tvrdenie 2.45

Nech T je teória, nech A, B, $A_1, A_2, \ldots, A_n$ sú formuly.

a. $T \cup \{A\} \models B$ *vtt* $T \models (A \to B)$.
b. $\{\} \models A$ *vtt* A *je tautológia* ($\models A$).
c. *Nasledujúce tvrdenia sú ekvivalentné:*
    i. $\{A_1, A_2, \ldots, A_n\} \models B$
    ii. $\{((\cdots(A_1 \land A_2) \land \cdots) \land A_n)\} \models B$
    iii. $\{\} \models ((\cdots(A_1 \land A_2) \land \cdots) \land A_n) \to B)$
    iv. $\models (((\cdots(A_1 \land A_2) \land \cdots) \land A_n) \to B)$

Hlasujte

Spomeňte si III.1

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

2.6

Ekvivalencia formúl

Ekvivalencia formúl

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

Definícia 2.46

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

Ako súvisí takto sémanticky zadefinovaná ekvivalencia formúl so skratkou $\leftrightarrow$?

Podľa dohody z 2. prednášky je $(X \leftrightarrow Y)$ je skráteným zápisom $((X \rightarrow Y) \wedge (Y \rightarrow X))$.

Tvrdenie 2.47

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

Ekvivalencia a vyplývanie

Ako súvisí ekvivalencia formúl s vyplývaním?

Tvrdenie 2.48

Formuly X a Y sú ekvivalentné vtt $\{X\} \models Y$ a $\{Y\} \models X$.

Dôkaz.

($\Rightarrow$) Nech X a Y sú ekvivalentné formuly. Chceme dokázať, že $\{X\} \models Y$, teda že (podľa definície vyplývania) pre každé ohodnotenie v platí, že ak $v \models \{X\}$, tak $v \models Y$.
Nech v je ľubovoľné ohodnotenie, nech $v \models \{X\}$. Potom $v \models X$ (podľa definície splnenia teórie), a teda $v \models Y$ (z predpokladu a podľa definície ekvivalencie). Teda platí, že ak $v \models \{X\}$, tak $v \models Y$. Pretože v bolo ľubovoľné, môžeme túto vlastnosť zovšeobecniť na všetky ohodnotenia, a teda $\{X\} \models Y$.
Dôkaz $\{Y\} \models X$ je podobný.
($\Leftarrow$) Nech X a Y sú formuly a nech $\{X\} \models Y$ a $\{Y\} \models X$. Chceme dokázať, že X a Y sú ekvivalentné.
Nech v je ľubovoľné ohodnotenie. Ak $v \models X$, tak $v \models \{X\}$ a podľa prvého predpokladu $v \models Y$. Ak $v \models Y$, tak $v \models \{Y\}$ a podľa druhého predpokladu $v \models X$. Teda $v \models X$ vtt $v \models Y$. Pretože v bolo ľubovoľné, môžeme túto vlastnosť zovšeobecniť na všetky ohodnotenia, a teda X a Y sú ekvivalentné. $\square$

Tranzitivita ekvivalencie

Tvrdenie 2.49 (Tranzitivita ekvivalencie)

Nech X, Y a Z sú formuly.
Ak X je ekvivalentná s Y a Y je ekvivalentná so Z,
tak X je ekvivalentná so Z.

Dôkaz.

Nech X, Y a Z sú formuly. Nech X je ekvivalentná s Y a Y je ekvivalentná so Z.
Nech v je ľubovoľné ohodnotenie.
Ak $v \models X$, tak $v \models Y$ podľa prvého predpokladu, a teda $v \models Z$ podľa druhého predpokladu.
Nezávisle od toho, ak $v \models Z$, tak $v \models Y$ podľa druhého predpokladu, a teda $v \models X$ podľa prvého predpokladu.
Preto $v \models X$ vtt $v \models Z$. Zovšeobecnením na všetky ohodnotenia dostávame, že X a Z sú ekvivalentné. $\square$

2.7

Ekvivalentné úpravy

Ekvivalentné úpravy

- Už ste určite ekvivalente upravovali formuly
- Aké kroky ste pri tom robili?

Príklad 2.50

$$A = \neg\neg(r \land q) \qquad B = (r \land q) \qquad X = (p \to \neg\, \neg\neg(r \land q)\,)$$

$$\rightsquigarrow$$

$$Y = (p \to \neg\, (r \land q)\,)$$

Nahradenie podformuly A vo formule X formulou B, ktorá je ekvivalentná s A

Pravidlá ekvivalentných úprav

Príklad 2.50

$$A = \neg\neg(r \land q) \qquad B = (r \land q) \qquad X = (p \rightarrow \neg\neg\neg(r \land q))$$

$$\rightsquigarrow \quad (p \rightarrow \neg(r \land q))$$

- Ako vieme, že A a B sú ekvivalentné?
  - Môžeme odvodiť sémanticky
  - Naozaj ste *dosadili* $(r \land q)$ za p v *známej ekvivalencii* medzi $\neg\neg p$ a p (princíp dvojitej negácie)

Príklad 2.51

$$C = \neg\neg p \qquad D = p$$

$$\rightsquigarrow \qquad \rightsquigarrow$$

$$A = \neg\neg(r \land q) \qquad B = (r \land q)$$

Korektnosť ekvivalentných úprav

Príklad 2.50

$A = \neg\neg(r \land q)$ $\qquad B = (r \land q)$ $\qquad X = (p \rightarrow \neg\neg\neg(r \land q))$

$$\rightsquigarrow$$

$$(p \rightarrow \neg(r \land q))$$

Príklad 2.51

$C = \neg\neg p$ $\qquad D = p$

$$\rightsquigarrow \qquad \rightsquigarrow$$

$A = \neg\neg(r \land q)$ $\qquad B = (r \land q)$

- *Prečo* sú tieto úpravy *korektné* (správne)?
- Teda:
  Prečo, ak je C ekvivalentné s D,
  tak je aj A ekvivalentné s B a X ekvivalentné s Y?

Substitúcia a ekvivalentné úpravy

Oba druhy dosadení pri ekvivalentných úpravách sú *substitúcie*

Definícia 2.52 (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.

Substitúciu si vieme predstaviť ako cyklus prechádzajúci cez X alebo ako rekurzívne definovanú operáciu: (cv02)
Pre všetky formuly A, B, X, Y, všetky výrokové premenné p a všetky binárne spojky $b \in \{\land, \lor, \to\}$:

$$
\begin{aligned}
A[A|B] &= B \\
p[A|B] &= p && \text{ak } A \neq p \\
(\neg X)[A|B] &= \neg(X[A|B]) && \text{ak } A \neq \neg X \\
(X\, b\, Y)[A|B] &= ((X[A|B])\; b\; (Y[A|B])) && \text{ak } A \neq (X\, b\, Y)
\end{aligned}
$$

Korektnosť ekvivalentných operácií

Korektnosť ekvivalentných úprav vyjadrujú nasledujúce tvrdenia:

Tvrdenie 2.53 (Dosadenie do ekvivalentných formúl)

Nech A a B sú navzájom ekvivalentné formuly, p je výroková premenná a Y je formula. Potom formuly $A[p|Y]$ a $B[p|Y]$ sú ekvivalentné.

Veta 2.54 (Ekvivalentné úpravy)

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

Sémantické vlastnosti substitúcie

Obe tvrdenia o korektnosti sú dôsledkami nasledujúcej lemy:

Lema 2.55

Nech X je výroková formula, p je výroková premenná, A je formula a v je ohodnotenie výrokových premenných.
Potom $v \models X[p|A]$ vtt $v_{p|A} \models X$, kde $v_{p|A}$ je ohodnotenie, pre ktoré platí:

- $v_{p|A}(r) = v(r)$, *ak r je výroková premenná a $p \neq r$;*
- $v_{p|A}(p) = t$, *ak $v \models A$;*
- $v_{p|A}(p) = f$, *ak $v \not\models A$.*

O jej platnosti sa môžeme presvedčiť indukciou na stupeň formuly X.

Ekvivalencie pre ekvivalentné úpravy

Veta 2.56

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

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

Ekvivalencie pre ekvivalentné úpravy

Veta 2.56 (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 $\top$	*vylúčenie tretieho*
$(A \land \neg A)$ a $\bot$	*spor*
$(A \to B)$ a $(\neg A \lor B)$	*nahradenie* $\to$

2.8

Konjunktívna a disjunktívna normálna forma

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 $\square$.

Konjunktívny a disjunktívny normálny tvar

Definícia 2.53

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

Príklad 2.54

Ktoré z nasledujúcich formúl sú literálmi, klauzulami, sú v CNF, v DNF:

$$A_1 = p \qquad A_6 = ((p \land \neg q) \lor (\neg p \land r) \lor (\neg p \land q \land \neg r))$$

$$A_2 = \neg q \qquad A_7 = ((\neg p \lor q \lor \neg r) \land (q \to r))$$

$$A_3 = \square \qquad A_8 = ((\neg p \lor \neg q) \land (p \lor r) \land (p \lor q \lor \neg r))$$

$$A_4 = (p \lor \neg q) \qquad A_9 = ((\neg p \lor (p \land r)) \land (p \lor q \lor \neg r))$$

$$A_5 = (p \land \neg q) \qquad A_{10} = ((\neg p \lor p \lor r) \land (\neg(p \lor q) \lor \neg r))$$

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.

Vítězslav Švejdar. *Logika: neúplnost, složitost, nutnost*. Academia, 2002. Prístupné aj na http://www1.cuni.cz/~svejdar/book/LogikaSve2002.pdf.