Prednášky z Matematiky (4) – Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Katedra aplikovanej informatiky
FMFI UK Bratislava

Letný semester 2015/2016

3. prednáška

Vyplývanie, ekvivalentné úpravy

7. marca 2016

Obsah 3. prednášky

Ohodnotenie výrokových premenných

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 $v(p) = f$.

Splĺňanie formúl pri ohodnotení premenných

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 spĺňa atomickú formulu p vtt $v(p) = t$;
- v spĺňa formulu $\neg A$ vtt v nespĺňa A;
- v spĺňa formulu $(A \wedge B)$ vtt v spĺňa A a v spĺňa B;
- v spĺňa formulu $(A \vee B)$ vtt v spĺňa A alebo v spĺňa B;
- v spĺňa formulu $(A \rightarrow B)$ vtt v nespĺňa A alebo v spĺňa B.

Vzťah *ohodnotenie v spĺňa formulu* X skrátene zapisujeme $v \models X$.

Splňanie formuly pri ohodnoteniach

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_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.

Tautológia, splniteľnosť, ekvivalencia

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.

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.

Dohoda

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

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. $\square$

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 výrokovologické 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

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

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

Splniteľnosť a výrokovologické vyplývanie

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

Definícia (Výrokovologické 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 $S_1 = \{X_1, X_2, \ldots, X_n, \neg X\}$ nesplniteľná.

Dôkaz.

($\Rightarrow$) Predpokladajme, že X vyplýva z množiny S. Nech v je nejaké ohodnotenie $\mathcal{V}$. Potrebujeme ukázať, že v nespĺňa S_1. Máme dve možnosti:

- Ak v nespĺňa S, tak nespĺňa ani S_1.
- Ak v spĺňa S, tak v musí spĺňať aj X (definícia vyplývania). To znamená, že $\neg X$ je nesplnená pri v, a teda v nespĺňa S_1.

($\Leftarrow$) Opačne, nech S_1 je nesplniteľná a nech v je nejaké ohodnotenie $\mathcal{V}$. v teda nespĺňa S_1. Potrebujeme ukázať, že ak v spĺňa S, tak potom v spĺňa aj X. Ak v spĺňa S, potom spĺňa každé X_i. Keďže ale v nespĺňa S_1, v musí nespĺňať $\neg X$ (jediná zostávajúca formula z S_1), čo znamená, že v spĺňa X. $\square$

Nezávislosť

Definícia

Formula X je *nezávislá* od množiny formúl S, ak existuje dvojica ohodnotení v_1, v_2 spĺňajúcich S, pričom v_1 spĺňa X, ale v_2 nespĺňa X.

Príklad

Atomická formula jim je nezávislá od P.

Asociativita a komutativita konjunkcie a disjunkcie

Zjednodušenie zápisu formúl

Tvrdenie

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

- $((A_1 \land A_2) \land A_3)$ *a* $(A_1 \land (A_2 \land A_3))$,
- $((A_1 \lor A_2) \lor A_3)$ *a* $(A_1 \lor (A_2 \lor A_3))$.
- $(A_1 \land A_2)$ *a* $(A_2 \land A_1)$,
- $(A_1 \lor A_2)$ *a* $(A_2 \lor A_1)$,

Dohoda

Nech A_1, A_2, $\ldots$, A_n sú formuly.
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 $\bigwedge_i A_i$.
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 $\bigvee_i A_i$.

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:
  - $\{A_1, A_2, \ldots, A_n\} \models B$
  - $\{(A_1 \land A_2 \land \cdots \land A_n)\} \models B$
  - $\{\} \models ((A_1 \land A_2 \land \cdots \land A_n) \to B)$
  - $\models ((A_1 \land A_2 \land \cdots \land A_n) \to B)$

Ekvivalentné úpravy

Ekvivalentné úpravy formúl ste robili na diskrétnej matematike.

Definícia

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

Cieľom je zvyčajne formulu zjednodušiť alebo upraviť do požadovaného tvaru, prípadne ukázať, že je tautológia upravením na známu tautológiu.
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

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

- 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

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

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

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

Substitúcia a ekvivalentné úpravy

Definícia (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 (Ekvivalentné úpravy)

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

Tvrdenie

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

Veta

Nech A, B, C sú ľubovoľné formuly.
Nasledujúce dvojice formúl sú ekvivalentné:

$(A \land (B \land C))$	$((A \land B) \land C)$	*asociatívne pravidlá*
$(A \lor (B \lor C))$	$((A \lor B) \lor C)$	
$(A \land (B \lor C))$	$((A \land B) \lor (A \land C))$	*distributívne pravidlá*
$(A \lor (B \land C))$	$((A \lor B) \land (A \lor C))$	
$\neg(A \land B)$	$(\neg A \lor \neg B)$	*de Morganove pravidlá*
$\neg(A \lor B)$	$(\neg A \land \neg B)$	
$\neg\neg A$	A	*dvojitá negácia*

Konjunktívna a disjunktívna normálna forma

Definícia

- 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).

Existencia DNF, CNF

Veta

1. *Ku každej formule X existuje ekvivalentná formula A v disjunktívnom normálnom tvare.*
2. *Ku každej formule X existuje ekvivalentná formula B v konjunktívnom normálnom tvare.*

Dôkaz.

1. Predstavme si pravdivostnú tabuľku pre X. Zoberme všetky boolovské ohodnotenia v_i také, že $v_i \models X$. Pre každé v_i zostrojme formulu C_i ako konjunkciu obsahujúcu a ak $v_i(a) = t$ pre premennú a, alebo $\neg a$, ak $v_i(a) = f$. Očividne formula $A = \bigvee C_i$ je v DNF a je ekvivalentná s X (vymenuváva všetky možnosti, kedy je X pravdivá).
2. K $\neg X$ teda existuje ekvivalentná formula A_1 v DNF. Znegovaním A_1 (a aplikáciou de Morganových pravidiel) dostaneme formulu B v CNF, ktorá je ekvivalentná s X. $\square$

CNF – trochu lepší prístup

Algoritmus

1. Prepíšeme implikácie:
   - $(A \to B) \quad \rightsquigarrow \quad (\neg A \wedge B)$.
2. Presunieme $\neg$ dovnútra pomocou de Morganových pravidiel a dvojitej negácie.
3. Roznásobíme $\wedge$ s $\vee$ podľa distributívneho pravidla:
   - $((A \wedge B) \vee C) \quad \rightsquigarrow \quad ((A \vee B) \wedge (A \vee C))$
4. Prezátvorkujeme na požadovaný tvar pomocou asociatívnych pravidiel.

Všetky úpravy sú ekvivalentné, takže:

Tvrdenie

Výsledná formula algoritmu je ekvivalentná s pôvodnou a je v CNF.

CNF – iný prístup

Algoritmus

1. Vytvoríme vytvárajúci strom pre formulu X.
2. Pre každú formulu X_i vo vytvárajúcom strome pre X vytvoríme novú výrokovú premennú x_i, ktorá bude „reprezentovať“ formulu X_i (nech x_0 reprezentuje celkovú formulu X).
3. Vytvoríme formuly, ktoré popisujú vzťah medzi X_i a jej priamymi podformulami prostredníctvom „reprezentačných“ premenných:
   - ak X_i je tvaru $\neg X_j$ pre nejaké X_j, pridáme $(x_i \leftrightarrow \neg x_j)$,
   - ak X_i je tvaru $(X_j \wedge X_k)$, pridáme $(x_i \leftrightarrow (x_j \wedge x_k))$,
   - ak X_i je tvaru $(X_j \vee X_k)$, pridáme $(x_i \leftrightarrow (x_j \vee x_k))$,
   - ak X_i je tvaru $(X_j \rightarrow X_k)$ pridáme $(x_i \leftrightarrow (x_j \rightarrow x_k))$,
   - ak X_i je premenná a, pridáme $(x_i \leftrightarrow a)$.

   Všetky uvedené formuly idú jednoducho prepísať do CNF.
4. Pridáme formulu x_0 (chceme aby celková formula X bola pravdivá).

CNF – iný prístup

Definícia

Formuly X a Y sú *rovnako splniteľné* (ekvisplniteľné, equisatisfiable) vtt, keď X je splniteľná vtt Y je splniteľná.

Tvrdenie

Výsledná formula predchádzajúceho algoritmu je v CNF, jej veľkosť je lineárna voči veľkosti X a je ekvisplniteľná s X.

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.