Prednášky z Matematiky (4) – Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Katedra aplikovanej informatiky
FMFI UK Bratislava

Letný semester 2015/2016

4. prednáška

CNF, Hilbertovský kalkul

14. marca 2016

Obsah 4. prednášky

Splniteľnosť a výrokovologické vyplývanie

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.

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.

Tvrdenie

Formula X výrokovologicky vyplýva z množiny formúl $S = \{X_1, X_2, \dots, X_n\}$ vtt keď je množina $S_1 = \{X_1, X_2, \dots, X_n, \neg X\}$ nesplniteľná.

Ekvivalentné úpravy

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.

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.

Ekvivalentné úpravy

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.

Ekvivalencie pre ekvivalentné úpravy

Veta

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

$(A \land (B \land C))$ $(A \lor (B \lor C))$	$((A \land B) \land C)$ $((A \lor B) \lor C)$	*asociatívne pravidlá*
$(A \land B)$ $(A \lor B)$	$(B \land A)$ $(B \lor A)$	*komutatívne pravidlá*
$(A \land (B \lor C))$ $(A \lor (B \land C))$	$((A \land B) \lor (A \land C))$ $((A \lor B) \land (A \lor C))$	*distributívne pravidlá*
$\neg(A \land B)$ $\neg(A \lor B)$	$(\neg A \lor \neg B)$ $(\neg A \land \neg B)$	*de Morganove pravidlá*
$\neg\neg A$	A	*pravidlo dvojitej negácie*

Konjunkcie a disjunkcie formúl

Dohoda

Nech $A_1, A_2, \dots, A_n$ je konečná postupnosť formúl.
Formulu $((\cdots((A_1 \land A_2) \land A_3) \land \cdots) \land A_n)$ budeme skrátene zapisovať $(A_1 \land A_2 \land A_3 \land \cdots \land A_n)$, prípadne $\bigwedge_i A_i$ a nazývať *konjunkcia postupnosti formúl* $A_1, \dots, A_n$.
Formulu $((\cdots((A_1 \lor A_2) \lor A_3) \lor \cdots) \lor A_n)$ budeme skrátene zapisovať $(A_1 \lor A_2 \lor A_3 \lor \cdots \lor A_n)$, prípadne $\bigvee_i A_i$ a nazývať *disjunkcia postupnosti formúl* $A_1, \dots, A_n$.
Pre $n = 1$ chápeme samotnú formulu A_1 ako konjunkciu aj ako disjunkciu jednoprvkovej postupnosti formúl A_1.
Pre $n = 0$ chápeme ako konjunkciu prázdnej postupnosti formúl ľubovoľnú tautológiu (napríklad $(p_1 \lor \neg p_1)$) a ako disjunkciu prázdnej postupnosti formúl ľubovoľnú nesplniteľnú formulu (napríklad $(p_1 \land \neg p_1)$).

Konjunktívna a disjunktívna normálna forma

Definícia

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

Inak povedané: Formula X je v CNF vtt, keď existujú postupnosti literálov $\ell_{1,1}, \ldots, \ell_{1,n_1}, \ell_{2,1}, \ldots, \ell_{2,n_2}, \ldots, \ell_{k,1}, \ldots, \ell_{k,n_k}$ také, že $X = \bigwedge_{i=1}^{k} \bigvee_{j=1}^{n_i} \ell_{i,j}$.

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. Zoberme všetky ohodnotenia v_i také, že $v_i \models X$ a $v_i(q) = f$ pre všetky premenné q nevyskytujúce sa v X. Pre každé v_i zostrojme formulu C_i ako konjunkciu obsahujúcu p, ak $v_i(p) = t$, alebo $\neg p$, ak $v_i(p) = f$, pre každú premennú p z X. Očividne formula $A = \bigvee_i C_i$ je v DNF a je ekvivalentná s X (vymenúva všetky možnosti, kedy je X splnená).
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 CNF_1

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

Tvrdenie

Výsledná formula alg. CNF_1 je ekvivalentná s pôvodnou a je v CNF.

CNF – trochu lepší prístup

Príklad

$((a \lor \neg b) \to \neg(c \lor (d \land \neg e)))$

$\overset{1}{\leadsto} (\neg(a \lor \neg b) \lor \neg(c \lor (d \land \neg e)))$

$\overset{2}{\leadsto} ((\neg a \land \neg\neg b) \lor \neg(c \lor (d \land \neg e)))$

$\overset{2}{\leadsto} ((\neg a \land b) \lor \neg(c \lor (d \land \neg e)))$

$\overset{2}{\leadsto} ((\neg a \land b) \lor (\neg c \land \neg(d \land \neg e)))$

$\overset{2}{\leadsto} ((\neg a \land b) \lor (\neg c \land (\neg d \lor \neg\neg e)))$

$\overset{2}{\leadsto} ((\neg a \land b) \lor (\neg c \land (\neg d \lor e)))$

$\overset{3}{\leadsto} (((\neg a \land b) \lor \neg c) \land ((\neg a \land b) \lor (\neg d \lor e)))$

$\overset{3}{\leadsto} (((\neg a \lor \neg c) \land (b \lor \neg c)) \land ((\neg a \lor (\neg d \lor e)) \land (b \lor (\neg d \lor e))))$

$\overset{4}{\leadsto} ((((\neg a \lor \neg c) \land (b \lor \neg c)) \land (\neg a \lor (\neg d \lor e))) \land (b \lor (\neg d \lor e)))$

$\overset{4}{\leadsto} ((((\neg a \lor \neg c) \land (b \lor \neg c)) \land ((\neg a \lor \neg d) \lor e)) \land ((b \lor \neg d) \lor e))$

CNF – iný prístup

Algoritmus CNF_2

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 $(X_j \to X_k)$ pridáme $(x_i \leftrightarrow (x_j \to x_k))$,
   - 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 Y algoritmu CNF_2 je v CNF, jej dĺžka je lineárna voči veľkosti X a Y je ekvisplniteľná s X.

CNF – trochu lepší prístup

Príklad

$$X_0 = ((a \vee \neg b) \to \neg(c \vee (d \wedge \neg e)))$$

$X_1 = (a \vee \neg b)$ $X_2 = \neg(c \vee (d \wedge \neg e))$

$X_3 = a$ $X_4 = \neg b$ $X_5 = (c \vee (d \wedge \neg e))$

$X_6 = b$ $X_7 = c$ $X_8 = (d \wedge \neg e)$

$X_9 = d$ $X_{10} = \neg e$

$X_{11} = e$

x_0

$x_0 \leftrightarrow (x_1 \to x_2)$

$x_1 \leftrightarrow (x_3 \vee x_4)$ $x_2 \leftrightarrow \neg x_5$

$x_3 \leftrightarrow a$ $x_4 \leftrightarrow \neg x_6$ $x_5 \leftrightarrow (x_7 \vee x_8)$

$x_6 \leftrightarrow b$ $x_7 \leftrightarrow c$ $x_8 \leftrightarrow (x_9 \wedge x_{10})$

$x_9 \leftrightarrow d$ $x_{10} \leftrightarrow \neg x_{11}$

$x_{11} \leftrightarrow e$

Dokazovanie ekvivalencie syntakticky vs. sémanticky

Pomocou substitúcie ekvivalentných formúl vieme dokázať, že dve formuly sú ekvivalentné bez toho, aby sme vyšetrovali všetky ohodnotenia ich výrokových premenných.
Výhodné pri formulách s veľa premennými.
Napr. formulu $X = ((a \lor \neg b) \to \neg(c \lor (d \land \neg e)))$ sme upravili do CNF $Y = ((((\neg a \lor \neg c) \land (b \lor \neg c)) \land ((\neg a \lor \neg d) \lor e)) \land ((b \lor \neg d) \lor e))$ pomocou 12 substitúcií ekvivalentných podformúl. Tým sme zároveň dokázali, že X a Y sú ekvivalentné.
Na dôkaz ich ekvivalencie tabuľkovou metódou by sme potrebovali vyšetriť 32 prípadov.
Substitúcie sú *syntaktickou metódou* dokazovania ekvivalencie, pracujú iba s reťazcami symbolov.
Tabuľková metóda je *sémantická metóda*, využíva ohodnotenia výrokových premenných a spĺňanie formúl ohodnoteniami.

Dokazovanie vyplývania a tautológií syntakticky vs. sémanticky — kalkuly

Tautológie a vyplývanie formúl z množín sme doteraz dokazovali sémanticky — vyšetrovaním všetkých ohodnotení.
Na tento účel ale existujú aj syntaktické metódy — *kalkuly*.
Ukážeme si dva kalkuly:

hilbertovský — klasický, lineárny, pomerne ťažkopádny

tablový — modernejší, stromový, prirodzenejší

Literatúra

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