Výroková logika – pokračovanie

Úvod do výpočtovej logiky

Jozef Šiška

2013/2014

Sémantika

- Ekvivalentné úpravy
- Konjunktívna a disjunktívna normálna forma

Hilbertovský kalkul

- Dôkaz

Značenie

$$(((A_1 \wedge A_2) \wedge \dots) \wedge A_n) \quad (A_1 \wedge A_2 \wedge \cdots \wedge A_n) \quad \bigwedge A_i$$

$$(((A_1 \vee A_2) \vee \dots) \vee A_n) \quad (A_1 \vee A_2 \vee \cdots \vee A_n) \quad \bigvee A_i$$

$$((A \to B) \wedge (B \to A)) \qquad (A \Leftrightarrow B)$$

Značenie

$$(((A_1 \wedge A_2) \wedge \dots) \wedge A_n) \quad (A_1 \wedge A_2 \wedge \cdots \wedge A_n) \quad \bigwedge A_i$$

$$(((A_1 \vee A_2) \vee \dots) \vee A_n) \quad (A_1 \vee A_2 \vee \cdots \vee A_n) \quad \bigvee A_i$$

$$((A \to B) \wedge (B \to A)) \qquad (A \Leftrightarrow B)$$

Pozorovania

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

Definícia (Substitúcia)

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

Tvrdenie (Ekvivalentné úpravy)

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

Pozorovanie

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

Tvrdenie

Nasledujúce dvojice formúl sú ekvivalentné

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

kde A, B, C sú ľubovoľné formuly.

Konjunktívna a disjunktívna normálna forma

Definícia

- Premennú alebo negáciou premennej nazývame *literál*. Disjunkciu literálov nazývame *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).

Tvrdenie

1. *Ku každej formule X existuje ekvivalentná formula A v disjunktívnej normálnej forme.*
2. *Ku každej formule X existuje ekvivalentná formula B v konjunktívnej normálnej forme.*

Dôkaz.

1. Predstavme si pravdivostnú tabuľku pre X. Zoberme všetky boolovské ohodnotenia v_i také, že $v_i(X) = t$. 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' v DNF. Znegovaním A' (a aplikáciou de Morganových pravidiel) dostaneme formulu B v CNF, ktorá je ekvivalentná s X.

CNF – trochu lepší prístup

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

Všetky úpravy sú ekvivalentné, takže výsledná formula je ekvivalentná s pôvovdnou a je v CNF.

CNF – iný prístup

1. Vytvoríme vytvárajúci strom pre formulu X.
2. Pre každú formulu X_i vo vytvárajúcom strome pre X vytvoríme novú 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 priamimi "podformulami":
   - 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).

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

Hilbertovský kalkul

Schémy axiom

A1 $(A \to (B \to A))$

A2 $((A \to (B \to C)) \to ((A \to B) \to (A \to C)))$

A3 $((\neg A \to \neg B) \to (B \to A))$

A4 $((A \land B) \to A)$, $((A \land B) \to B)$

A5 $(A \to (B \to (A \land B)))$

A6 $((A \to (A \lor B))$, $(B \to (A \lor B))$

A7 $((A \to C) \to ((B \to C) \to ((A \lor B) \to C)))$

Odvodzovacie pravidlo

MP $\dfrac{A, A \to B}{B}$

Hilbertovský kalkul – dôkaz

Definícia

Dôkaz Dôkaz formuly X z množiny predpokladov S je postupnosť formúl $Y_1, Y_2, \ldots Y_n$ taká, že každá formula Y_i je predpoklad z S, alebo je to inštancia niektorej z axiom, alebo vznikla aplikáciou odvodzovacieho pravidla na formuly ktoré sa vyskujú pred ňou.

Hovoríme, že formula X je dokázateľná z množiny predpokladov X (značíme $S \vdash X$) ak existuje dôkaz X z S.

Hilbertovský kalkul – dôkaz

Definícia

Dôkaz Dôkaz formuly X z množiny predpokladov S je postupnosť formúl $Y_1, Y_2, \dots Y_n$ taká, že každá formula Y_i je predpoklad z S, alebo je to inštancia niektorej z axiom, alebo vznikla aplikáciou odvodzovacieho pravidla na formuly ktoré sa vyskujú pred ňou.

Hovoríme, že formula X je dokázateľná z množiny predpokladov X (značíme $S \vdash X$) ak existuje dôkaz X z S.

Vety o úplnosti

- Formula X je dokázateľná z prázdnej množiny predpokladov vtt X je tautológia ($\emptyset \vdash X$ vtt $\models X$)
- Nech T je konečná množina formúl, potom formula X je dokázateľná z T vtt keď X vyplýva z T ($T \vdash X$ vtt $T \models X$).