Prednášky z Matematiky (4) — Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Katedra aplikovanej informatiky
FMFI UK Bratislava

Letný semester 2018/2019

4. prednáška

CNF
Hilbertovský kalkul

11. marca 2018

Obsah 4. prednášky

2 Výroková logika
  - Ekvivalencia formúl
    - Konjunktívna a disjunktívna normálna forma
  - Kalkuly
  - Hilbertovský kalkul

Opakovanie

Sémantika

Teória, model a splniteľnosť

Definícia 2.31

(Výrokovologickou) teóriou nazývame každú množinu formúl.

Definícia 2.33

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

Definícia 2.36

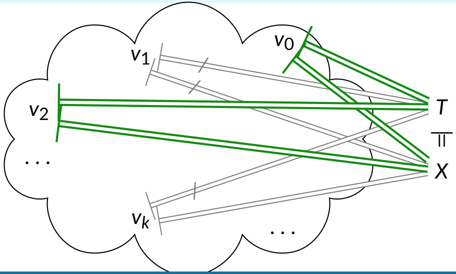
Teória T je ***súčasne výrokovologicky splniteľná*** (skrátene *splniteľná*) vtt existuje aspoň jeden model T.
Teória je ***nesplniteľná*** vtt nie je splniteľná.

Vyplývanie

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.



Tvrdenie 2.41

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

Splniteľnosť a výrokovologické vyplývanie

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.

2.6 Ekvivalencia formúl

Ekvivalentné úpravy

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.

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.

Ekvivalentné úpravy

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.

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 $v \not\models A$.*

2.6.2

Konjunktívna a disjunktívna normálna forma

Konjunkcia a disjunkcia postupnosti formúl

Dohoda

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

- ***Konjunkciu postupnosti formúl $A_1, \ldots, A_n$***,
  teda $(((A_1 \wedge A_2) \wedge A_3) \wedge \cdots \wedge A_n)$,
  skrátene zapisujeme $(A_1 \wedge A_2 \wedge A_3 \wedge \cdots \wedge A_n)$, prípadne $\bigwedge_{i=1}^{n} A_i$.
  - Konjunkciu *prázdnej* postupnosti formúl ($n = 0$) označujeme $\top$.
    Chápeme ju ako ľubovoľnú *tautológiu*, napríklad $(p_1 \vee \neg p_1)$.
- ***Disjunkciu postupnosti formúl $A_1, \ldots, A_n$***,
  teda $(((A_1 \vee A_2) \vee A_3) \vee \cdots \vee A_n)$,
  skrátene zapisujeme $(A_1 \vee A_2 \vee A_3 \vee \cdots \vee A_n)$, prípadne $\bigvee_{i=1}^{n} A_i$.
  - Disjunkciu *prázdnej* postupnosti formúl označujeme $\bot$ alebo $\square$.
    Chápeme ju ako ľubovoľnú nesplniteľnú formulu, napríklad $(p_1 \wedge \neg p_1)$.
- Pre $n = 1$ chápeme samotnú formulu A_1 ako konjunkciu aj ako disjunkciu jednoprvkovej postupnosti formúl A_1.

Konjunktívny a disjunktívny normálny tvar

Definícia 2.57

Literál je výroková premenná alebo negácia výrokovej premennej.

Klauzula (tiež „klauza“) je *disjunkcia* literálov.

Formula v disjunktívnom normálnom tvare (DNF) je *disjunkcia* formúl, z ktorých každá je konjunkciou literálov.

Formula v konjunktívnom normálnom tvare (CNF) je *konjunkcia* klauzúl.

Príklad 2.58

Literály: p, $\neg q$

Klauzuly: p, $\neg q$, $\square$, $(\neg p \lor q \lor \neg r)$

DNF: p, $\neg q$, $(p \lor \neg q)$, $\square$, $\top$, $(p \land \neg q \land r)$, $((\neg p \land q) \boldsymbol{\lor} (q \land r))$

CNF: p, $\neg q$, $\top$, $(p \lor \neg q)$, $(p \land \neg q \land r)$, $\square$, $((p \lor q) \land \square)$, $((\neg p \lor q) \boldsymbol{\land} (q \lor r))$

Existencia DNF a CNF

Veta 2.59

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

Dôkaz.

1. Zoberme všetky ohodnotenia $v_1, \dots, v_n$ také, že $v_i \models X$ a $v_i(q) = f$ pre všetky premenné $q \notin \mathrm{vars}(X)$. 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 $p \in \mathrm{vars}(X)$. Očividne formula $D = \bigvee_{1 \leq i \leq n} C_i$ je v DNF a je ekvivalentná s X (vymenúva všetky možnosti, kedy je X splnená).
2. K $\neg X$ teda existuje ekvivalentná formula D v DNF. Znegovaním D a aplikáciou de Morganových pravidiel dostaneme formulu C v CNF, ktorá je ekvivalentná s X. □

CNF — trochu lepší prístup

- Skúmanie všetkých ohodnotení nie je ideálny spôsob ako upraviť formulu do CNF — najmä keď má veľa premenných a jej splniteľnosť chceme rozhodnúť SAT solverom.
- Je nejaký lepší *systematický* postup?
- Všimnime si:
  CNF je konjunkcia disjunkcií literálov — výrokových premenných alebo ich negácií
  Teda:
  - CNF **neobsahuje implikácie** — ako sa ich zbavíme?
  - **Negácia** sa vyskytuje **iba pri výrokových premenných** — ako ju tam dostaneme, ak to tak nie je (napr. $\neg(A \lor B)$)?
  - **Disjunkcie** sa nachádzajú iba **vnútri konjunkcií** — ako presunieme „vonkajšie“ disjunkcie „dovnútra“ konjunkcií (napr. $(A \lor (B \land C))$)?

CNF — trochu lepší prístup — algoritmus

Algoritmus CNF

1. Nahradíme implikáciu disjunkciou:
   - $(A \rightarrow B) \quad \Leftrightarrow \quad (\neg A \vee B)$.
2. Presunieme $\neg$ dovnútra pomocou de Morganových pravidiel a pravidla dvojitej negácie.
3. „Roznásobíme“ $\wedge$ s $\vee$ podľa distributívnosti a komutatívnosti:
   - $(A \vee (B \wedge C)) \quad \Leftrightarrow \quad ((A \vee B) \wedge (A \vee C))$
   - $((B \wedge C) \vee A) \quad \Leftrightarrow (A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C)) \Leftrightarrow ((B \vee A) \wedge (A \vee C)) \Leftrightarrow \quad ((B \vee A) \wedge (C \vee A))$
4. Prezátvorkujeme na požadovaný tvar pomocou asociatívnych pravidiel.

Tvrdenie 2.60

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

Príklad behu algoritmu CNF

Príklad 2.61

1. $((a \lor \neg b) \to \neg(c \lor (d \land \neg e)))$
2. $(\neg(a \lor \neg b) \lor \neg(c \lor (d \land \neg e)))$ [1 — nahradenie implikácie]
3. $((\neg a \land \neg\neg b) \lor \neg(c \lor (d \land \neg e)))$ [2 — de Morganovo pravidlo]
4. $((\neg a \land b) \lor \neg(c \lor (d \land \neg e)))$ [2 — dvojitá negácia]
5. $((\neg a \land b) \lor (\neg c \land \neg(d \land \neg e)))$ [2 — de Morganovo pravidlo]
6. $((\neg a \land b) \lor (\neg c \land (\neg d \lor \neg\neg e)))$ [2 — de Morganovo pravidlo]
7. $((\neg a \land b) \lor (\neg c \land (\neg d \lor e)))$ [2 — dvojitá negácia]
8. $(((\neg a \land b) \lor \neg c) \land ((\neg a \land b) \lor (\neg d \lor e)))$ [3 — distributívnosť]
9. $(((\neg a \lor \neg c) \land (b \lor \neg c)) \land ((\neg a \lor (\neg d \lor e)) \land (b \lor (\neg d \lor e))))$ [3]
10. $((\neg a \lor \neg c) \land (b \lor \neg c) \land (\neg a \lor (\neg d \lor e)) \land (b \lor (\neg d \lor e)))$ [4]
11. $((\neg a \lor \neg c) \land (b \lor \neg c) \land (\neg a \lor \neg d \lor e) \land (b \lor \neg d \lor e))$ [4 — asoc.]

Prečo iba *trochu* lepší prístup?

Distribúcia $\lor$ cez $\land$ spôsobuje nárast formuly:

- $A_2 = ((p_1 \land q_1) \lor (p_2 \land q_2))$
  $C_2 = ((p_1 \lor p_2) \land (p_1 \lor q_2) \land (q_1 \lor p_2) \land (q_1 \lor q_2))$
  $A_2 \Leftrightarrow C_2, \quad \deg(A_2) = 3, \quad \deg(B_2) = 7$
- $A_3 = ((p_1 \land q_1) \lor (p_2 \land q_2) \lor (p_3 \land q_3))$
  $$\begin{aligned} C_3 = \big(&(p_1 \lor p_2 \lor p_3) \land (p_1 \lor p_2 \lor q_3) \\ &\land (p_1 \lor q_2 \lor p_3) \land (p_1 \lor q_2 \lor q_3) \\ &\land (q_1 \lor p_2 \lor p_3) \land (q_1 \lor p_2 \lor q_3) \\ &\land (q_1 \lor p_2 \lor p_3) \land (q_1 \lor p_2 \lor q_3)\big), \end{aligned}$$
  $A_3 \Leftrightarrow C_3, \qquad \deg(A_3) = 5, \qquad \deg(C_3) = 23$
- $A_n = ((p_1 \land q_1) \lor \cdots \lor (p_n \land q_n))$
  Koľko klauzúl bude obsahovať C_n?
  Akého bude stupňa?

Obmedzenie exponenciálneho rastu CNF

Otázka

Dá sa vyhnúť exponenciálnemu nárastu formuly
$A_n = ((p_1 \land q_1) \lor \cdots \lor (p_n \land q_n))$ kvôli distributívnosti?

1. Zoberme *nové* výrokové premenné $r_1, \ldots, r_n, s$
2. Vyjadrime, že r_i je ekvivalentným zástupcom konjunkcie $(p_i \land q_i)$: $(r_i \leftrightarrow (p_i \land q_i))$
3. Použime r_i na vyjadrenie, že s je ekvivalentným zástupcom disjunkcie A_n: $(s \leftrightarrow (r_1 \lor \cdots \lor r_n))$
4. A_n teda môžeme nahradiť formulou $(s \land (s \leftrightarrow (r_1 \lor \cdots \lor r_n)) \land (r_1 \leftrightarrow (p_1 \land q_1)) \land \cdots \land (r_n \leftrightarrow (p_n \land q_n)))$

Ekvivalentnými úpravami

- druhý konjunkt upravíme na $n + 1$ klauzúl,
- ďalších n na 3 klauzuly každý

} spolu iba $4{\cdot}n + 2$ klauzúl!

Cejtinova transformácia do CNF

Cejtinova transformácia (angl. Tseytin transformation)

- algoritmus nájdenia CNF použitím tohto princípu na všetky podformuly
- výsledok Cejtinovej transformácie **nie je ekvivalentný** s X, iba **ekvisplniteľný**

Ekvisplniteľnosť

Definícia 2.62

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

Tvrdenie 2.63

Ak X a Y sú ekvivalentné, sú aj rovnako splniteľné.

Príklad 2.64 (Ekvivalentnosť vs. ekvisplniteľnosť)

Sú $(p \longrightarrow q)$ a $(p \land r)$ rovnako splniteľné? Sú ekvivalentné?

Pri úprave formuly do CNF pre SAT solver

- *nepotrebujeme* zachovať ekvivalenciu
- *stačí* ekvisplniteľnosť

Cejtinova transformácia

Cejtinova transformácia

1. Zostrojíme vytvárajúci strom pre formulu X a označíme formuly v ňom X_0, $X_1, X_2, \ldots$ tak, aby $X_0 = X$.
2. Pre každú formulu X_i, ak $X_i = p$ pre nejakú $p \in \mathcal{V}$, označíme $x_i = p$, inak označíme ako x_i novú výrokovú premennú, ktorá bude „reprezentovať" formulu X_i.
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 $(x_i \leftrightarrow (x_j \to x_k))$,
4. Pridáme formulu x_0 (chceme aby formula X bola pravdivá).
5. Všetky nové formuly z krokov 3 a 4 prevedieme do CNF (je to jednoduché) a spojíme konjunkciou.

Príklad Cejtinovej transformácie

Príklad 2.65

$$X_0 = ((a \lor \neg b) \to \neg(c \lor (d \land \neg e)))$$

$$X_1 = (a \lor \neg b) \qquad X_2 = \neg(c \lor (d \land \neg e))$$

$$a \qquad X_3 = \neg b \qquad X_4 = (c \lor (d \land \neg e))$$

$$b \qquad c \qquad X_5 = (d \land \neg e)$$

$$d \qquad X_6 = \neg e$$

$$e$$

$$x_0$$

$$(x_0 \leftrightarrow (x_1 \to x_2))$$

$$x_1 \leftrightarrow (a \lor x_3) \quad x_2 \leftrightarrow \neg x_4$$

$$x_3 \leftrightarrow \neg b \quad x_4 \leftrightarrow (c \lor x_5)$$

$$x_5 \leftrightarrow (d \land x_6)$$

$$x_6 \leftrightarrow \neg e$$

Korektnosť Cejtinovej transformácie

Tvrdenie 2.66

Pre výslednú formulu Y algoritmu Cejtinovej transformácie formuly X platí:

- *Y je v CNF,*
- *stupeň Y je lineárny vzhľadom na stupeň X,*
- *Y je ekvisplniteľná s X.*

Lema 2.67

Nech $X = (A \, c \, B)$ je formula, kde $c \in \{\land, \lor, \rightarrow\}$. Nech $p, q, r \in \mathcal{V}$ sa nevyskytujú v X.
Potom X a $Y = (p \land (p \leftrightarrow (q \, c \, r)) \land (q \leftrightarrow A) \land (r \leftrightarrow B))$ sú ekvisplniteľné.

2.7
Kalkuly

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 veľkým počtom premenných.
- 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.
- Zároveň sme dokázali, že X a Y sú ekvivalentné.
- Na dôkaz ich ekvivalencie tabuľkovou metódou by sme potrebovali vyšetriť 32 prípadov.

Ekvivalencia syntakticky vs. sémanticky

- Tabuľková metóda je **sémantická**
  - využíva ohodnotenia výrokových premenných a spĺňanie formúl ohodnoteniami
- Substitúcie ekvivalentných formúl sú **syntaktickou** metódou
  - pracujú iba s postupnosťami symbolov, nie s ohodnoteniami
- Navyše sú **deduktívnou** metódou
  - odvodíme *iba* formuly ekvivalentné s pôvodnou

Kalkuly — dokazovanie vyplývania syntakticky

- Ak začneme nejakou formulou a budeme substituovať ekvivalentné podformuly, dostávame postupne rôzne formuly, ktoré sú ale stále ekvivalentné s pôvodnou formulou.
- Čo keby sme začali s tautológiou?
  - Dostávame stále tautológie.
- Logiku viac zaujíma vyplývanie ako ekvivalencia a tautológie
- Vyplývanie dôsledkov z teórií sme doteraz dokazovali sémanticky — vyšetrovaním všetkých ohodnotení.
- Na tento účel ale existujú aj syntaktické metódy — *kalkuly*.
- Ukážeme si tri kalkuly:

hilbertovský	— klasický, lineárny, pomerne ťažkopádny
tablový	— stromový, prirodzenejší
rezolvenciu	— lineárny, strojový

2.8

Hilbertovský kalkul

Hilbertovský kalkul — axiómy a pravidlo

Definícia 2.68

Hilbertovský kalkul sa skladá z axióm vytvorených podľa nasledujúcich schém axióm pre všetky formuly A, B, C:

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

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

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

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

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

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

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

a pravidla ***modus ponens***:

MP $$\frac{A \quad (A \to B)}{B}$$

pre všetky formuly A a B.

Hilbertovský kalkul — dôkaz

Definícia 2.69

(Formálnym hilbertovským) dôkazom z množiny predpokladov S je postupnosť formúl $Y_1, Y_2, \dots, Y_n$, v ktorej každá formula Y_i je

- predpoklad z množiny S, alebo
- záver odvodzovacieho pravidla, ktorého premisy sa nachádzajú v postupnosti pred Y_i, teda špeciálne
  - Y_i je axióma, inštancia jednej zo schém (A1)–(A7), alebo
  - existujú $j < i$ a $k < i$ také, že Y_i je záver pravidla (MP) pre formuly Y_j a $Y_k = (Y_j \to Y_i)$.

Dôkazom formuly X z S je taký dôkaz z S, ktorého posledným členom je X.
Formula X je ***dokázateľná*** z množiny predpokladov S (skrátene $\boldsymbol{S \vdash X}$) vtt existuje dôkaz X z S.

[Švejdar, 2002, §1.3]

Príklad dôkazu v hilbertovskom kalkule

Príklad 2.70

Nájdime dôkaz formuly $Z = (X \to X)$ z množiny predpokladov $\{\}$ (pre ľubovoľnú formulu X):

1. Y_1 $(X \to (X \to X))$ — inštancia (A1) pre $A = B = X$
2. Y_2 $(X \to ((X \to X) \to X))$ — inšt. (A1) pre $A = X$, $B = (X \to X)$
3. Y_3 $((X \to ((X \to X) \to X)) \to ((X \to (X \to X)) \to (X \to X)))$ — inšt. (A2) pre $A = C = X$, $B = (X \to X)$
4. Y_4 $((X \to (X \to X)) \to (X \to X))$ — záver (MP) pre Y_2 a Y_3
5. Y_5 $(X \to X)$ — záver (MP) pre Y_1 a Y_4

Veta o dedukcii

Veta 2.71 (o dedukcii)

$S \cup \{X\} \vdash Y$ *vtt* $S \vdash (X \rightarrow Y)$

Dôkaz.

($\Leftarrow$) Nech $Y_1, \ldots, Y_n$ je dôkaz $(X \rightarrow Y)$ z S. Potom $Y_1, \ldots, Y_n, X, Y$ je dôkaz Y z $S \cup \{X\}$.
($\Rightarrow$) Nech $Y_1, \ldots, Y_n$ je dôkaz Y z $S \cup \{X\}$. Úplnou indukciou na k dokážeme, že $S \vdash (X \rightarrow Y_k)$.
Báza: Nech $k = 1$. Y_1 nemohla byť odvodená pravidlom (MP), takže je buď axióma, alebo patrí do S, alebo je X. V treťom prípade použijeme dôkaz $(X \rightarrow X)$ z predchádzajúceho príkladu 2.70. V prvých dvoch prípadoch je postupnosť $Y_1, (Y_1 \rightarrow (X \rightarrow Y_1)), (X \rightarrow Y_1)$ dôkazom $(X \rightarrow Y_1)$.
Ind. krok: Nech $k > 1$ a platí IP: pre všetky $j < k$ máme $S \vdash (X \rightarrow Y_j)$.
Ak Y_k je axióma, patrí do S, alebo je X, postupujeme ako pre $k = 1$.
Ak je Y_k záverom pravidla (MP) pre Y_i a $Y_j = (Y_i \rightarrow Y_k)$, tak $i, j < k$ a platí pre ne IP. Teda existuje dôkaz $A_1, \ldots, A_a$ formuly $A_a = (X \rightarrow Y_i)$ z S a dôkaz $B_1, \ldots, B_b$ formuly $B_b = (X \rightarrow (Y_i \rightarrow Y_k))$ z S. Dôkazom formuly $(X \rightarrow Y_k)$ potom je: $A_1, \ldots, A_a, B_1, \ldots, B_b, ((X \rightarrow (Y_i \rightarrow Y_k)) \rightarrow ((X \rightarrow Y_i) \rightarrow (X \rightarrow Y_k))), ((X \rightarrow Y_i) \rightarrow (X \rightarrow Y_k)), (X \rightarrow Y_k)$. $\square$

Dokazovanie s vetou o dedukcii

Príklad 2.72

Ukážme $\{\} \vdash ((A \to B) \to ((B \to C) \to (A \to C)))$
(pre ľubovoľné formuly A, B a C).
Podľa vety o dedukcii máme $\{\} \vdash ((A \to B) \to ((B \to C) \to (A \to C)))$ vtt
$\{(A \to B)\} \vdash ((B \to C) \to (A \to C))$ vtt $\{(A \to B), (B \to C)\} \vdash (A \to C)$ vtt
$\{(A \to B), (B \to C), A\} \vdash C$.
Posledný dôkaz nájdeme veľmi ľahko:

Y_1	A	predpoklad
Y_2	$(A \to B)$	predpoklad
Y_3	B	(MP) pre Y_1 a Y_2
Y_4	$(B \to C)$	predpoklad
Y_5	C	(MP) pre Y_3, Y_4

Podľa úvodnej úvahy teda $\{\} \vdash ((A \to B) \to ((B \to C) \to (A \to C)))$
(ale nevieme, ako tento dôkaz presne vyzerá).

Dokazovanie s vetou o dedukcii

Príklad 2.73

Ukážme $\{\} \vdash (\neg X \to (X \to Y))$ (pre ľubovoľné formuly X a Y).

Y_1 $(\neg X \to (\neg Y \to \neg X))$ — (A1) pre $A = \neg X$, $B = \neg Y$

Y_2 $((\neg Y \to \neg X) \to (X \to Y))$ — (A3) pre $A = Y$, $B = X$

$\vdots$ — dôkaz z príkladu 2.72

Y_n $\big((\neg X \to (\neg Y \to \neg X)) \to (((\neg Y \to \neg X) \to (X \to Y)) \to (\neg X \to (X \to Y)))\big)$

Y_{n+1} $\big(((\neg Y \to \neg X) \to (X \to Y)) \to (\neg X \to (X \to Y))\big)$ — (MP) pre Y_1 a Y_n

Y_{n+2} $(\neg X \to (X \to Y))$ — (MP) pre Y_2 a Y_{n+1}

Korektnosť a úplnosť hilbertovského kalkulu

Veta 2.74

Pre každú množinu formúl S a každú formulu X platí:

(korektnosť) *ak je X dokázateľná z S ($S \vdash X$), tak X výrokovologicky vyplýva z S ($S \models X$);*

(úplnosť) *ak X výrokovologicky vyplýva z S ($S \models X$), tak X je dokázateľná z S ($S \vdash X$).*

Korektnosť a úplnosť hilbertovského kalkulu

Korektnosť (angl. soundness) hilbertovského kalkulu vyplýva matematickou indukciou na dĺžku dôkazu z korektnosti pravidiel:

> Ak S je množina výrokových formúl a ak
>
> $$\frac{A_1 \quad \cdots \quad A_n}{A}$$
>
> je pravidlo (axióma alebo (MP)), potom ak $A_1, \ldots, A_n$ súčasne vyplývajú z S, tak aj A vyplýva z S.

Úplnosť (angl. completeness) je komplikovanejšia.

Vyskúšajte si IV.1

Ukážte $\{\} \vdash (\neg\neg X \to X)$.

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 $((A \wedge B) \to A), \quad ((A \wedge B) \to B)$

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

A6 $((A \to (A \vee B)), \quad (B \to (A \vee B))$

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

MP $\dfrac{A \quad (A \to B)}{B}$

$S \cup \{X\} \vdash Y$ vtt $S \vdash (X \to Y)$

$\{\} \vdash (X \to X)$

$\{\} \vdash ((A \to B) \to ((B \to C) \to (A \to C)))$

$\{\} \vdash (\neg X \to (X \to Y))$

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.