Provozně ekonomická fakulta

Teoretická informatika
Tomáš Foltýnek
foltynek@pef.mendelu.cz

Výroková logika

Mendelova zemědělská a lesnická univerzita v Brně

Opakování z minulé přednášky

- Co je to formalismus a co je jeho cílem?
- Formulujte Russelův paradox naivní teorie množin
- V čem spočívaly tzv. krize matematiky?
- Jak se buduje axiomatická teorie?
- Jaký je rozdíl mezi teorií a jejím modelem?
- Co je to neeuklidovská geometrie?
- Co je to nezávislost, úplnost a bezespornost axiomatického systému?
- Formulujte Gödelovy věty o neúplnosti

Literatura

- J. Rosický: Teorie množin (MU) – úvod
  ftp://www.math.muni.cz/pub/math/people/Rosicky/lectures/tma.ps
- J. Rosický: Logika (MU)
  ftp://www.math.muni.cz/pub/math/people/Rosicky/lectures/l.ps
- M. Kuba: ZKUSTO Logika I. (MU)
  http://www.fi.muni.cz/zkusto/logika.ps.gz
- M. Marvan: Algebra I. (SLU)
  http://www.math.slu.cz/studmat/Algebra0203z/I-m1tvrzeni.pdf
- J. Šerák: ZKUSTO Logika II. (MU)
  http://www.fi.muni.cz/zkusto/l2.ps.gz
- use Google;

Opakování: Jazyk VL

- Výroky označíme symboly
  - výrokové proměnné
  - logické proměnné
  - atomické výrokové formule
  - *a, b, c, p, q, r, s, x, y, z, …*
- Pro logické spojky zavedeme symboly
  - $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$
- Pro zápis priority slouží kulaté závorky
  - (,)

Opakování: Výrokové formule

- Za **výrokovou formuli (VF)** budeme považovat takovou posloupnost symbolů jazyka VL, pro kterou platí:
  - Každá výroková proměnná je (atomická) VF
  - Je-li a VF, pak také $\neg a$ je VF
  - Jsou-li a, b VF, pak také $(a \wedge b)$, $(a \vee b)$, $(a \Rightarrow b)$, $(a \Leftrightarrow b)$ jsou VF
  - Nic jiného není VF

Opakování: Podformule

- Formule *b* se nazývá **bezprostřední podformulí** formule *c*, má-li *c* jeden z následujících tvarů:
  $\neg b$, $(a \wedge b)$, $(b \wedge a)$, $(a \vee b)$, $(b \vee a)$, $(a \Rightarrow b)$, $(b \Rightarrow a)$, $(a \Leftrightarrow b)$, $(b \Leftrightarrow a)$
- Formule *b* se nazývá (běžnou) **podformulí** formule *c*, jestliže existuje taková posloupnost formulí
  $c_1, c_2, \ldots, c_m$, $m \geq 1$,
  že $c_1 = b$, $c_m = c$ a c_{i-1} je bezprostřední podformulí formule c_i pro každé $i = 2, 3, \ldots m$.
- Rozklad formule na podformule tvoří stromovou strukturu až k atomickým formulím

Opakování: Pravdivostní hodnota I.

- **Pravdivostní hodnotou** (elementárního) výroku je zobrazení

$$v: V_0 \rightarrow \{0,1\}$$

kde V_0 je množina výrokových proměnných

- Zobrazení přiřazuje každému výroku (výrokové proměnné) hodnotu PRAVDA/NEPRAVDA, TRUE/FALSE, 0/1
  - tedy jednobitovou informaci

Opakování: Pravdivostní hodnota II.

- Zobrazení *v* rozšíříme na množinu všech VF. Dostáváme zobrazení

  $$v' : V \rightarrow \{0,1\}$$

  definované takto:
  - $v'(a) = v(a)$ pro $a \in V_0$
  - jsou-li a,b VF, pak $v'(\neg a)$, $v'(a \wedge b)$, $v'(a \vee b)$, $v'(a \Rightarrow b)$, $v'(a \Leftrightarrow b)$ jsou definovány tabulkou:

a	b	¬a	a∧b	a∨b	a⇒b	a⇔b
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

Opakování: Tautologie a kontradikce

- Výrokovou formuli nazveme **tautologie**, pokud je vždy pravdivá bez ohledu na pravdivostní hodnotu výrokových proměnných, které obsahuje.
- Výrokovou formuli nazveme **kontradikce**, pokud je vždy nepravdivá bez ohledu na pravdivostní hodnotu výrokových proměnných, které obsahuje
- Formule, která není ani tautologie, ani kontradikce, se nazývá **splnitelná formule**

Opakování: Význačné tautologie

- Zákon sporu: $\neg(p \wedge \neg p)$
- Zákon vyloučení třetího: $p \vee \neg p$
- Zákon totožnosti: $p \Leftrightarrow p$
- Zákon dvojí negace: $\neg\neg p \Leftrightarrow p$
- Claviův zákon (reductio ad absurdum):
  - $(\neg p \Rightarrow p) \Rightarrow p$
  - $(p \Rightarrow \neg p) \Rightarrow \neg p$
- Zákon Dunse Scota: $(p \wedge \neg p) \Rightarrow q$
- …

Opakování: Logická ekvivalence

- Řekneme, že formule p a q jsou **logicky ekvivalentní**, jestliže výroková formule $a \Leftrightarrow b$ je tautologie
- Logicky ekvivalentní výroky mají tedy vždy stejnou pravdivostní hodnotu
- Příklady logicky ekvivalentních výroků
  - $(p \Rightarrow (q \Rightarrow r))) \Leftrightarrow ((p \wedge q) \Rightarrow r))$
  - $(p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p))$

Opakování: Pravidla úpravy VF

- Obměna implikace
  - $(a \Rightarrow b) \Leftrightarrow (\neg b \Rightarrow \neg a)$
- Tranzitivita implikace
  - Zákon hypotetického sylogismu
  - $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
- Komutativita
  - $(a \wedge b) \Leftrightarrow (b \wedge a)$
  - $(a \vee b) \Leftrightarrow (b \vee a)$
  - $(a \Leftrightarrow b) \Leftrightarrow (b \Leftrightarrow a)$
  - NE implikace!
- Asociativita
  - $((a \wedge b) \wedge c) \Leftrightarrow (a \wedge (b \wedge c))$
  - $((a \vee b) \vee c) \Leftrightarrow (a \vee (b \vee c))$
  - $((a \Leftrightarrow b) \Leftrightarrow c) \Leftrightarrow (a \Leftrightarrow (b \Leftrightarrow c))$
  - Ne implikace!
- Distributivní zákony
  - $(a \wedge (b \vee c)) \Leftrightarrow ((a \wedge b) \vee (a \wedge c))$
  - $(a \vee (b \wedge c)) \Leftrightarrow ((a \vee b) \wedge (a \vee c))$
- Konjunkce implikuje každý ze svých členů
  - $(p \wedge q) \Rightarrow p$
  - $(p \wedge q) \Rightarrow q$
- Disjunkce je implikována každým ze svých členů
  - $p \Rightarrow (p \vee q)$
  - $q \Rightarrow (p \vee q)$
- deMorganovy zákony
  - $\neg(a \wedge b) \Leftrightarrow (\neg a \vee \neg b)$
  - $\neg(a \vee b) \Leftrightarrow (\neg a \wedge \neg b)$
- Pravidla pro negování
  - $\neg(a \Rightarrow b) \Leftrightarrow (a \wedge \neg b)$
  - $\neg(a \Leftrightarrow b) \Leftrightarrow ((a \wedge \neg b) \vee (b \wedge \neg a))$

Opakování: Úplný systém spojek

- Řekneme, že množina logických spojek L tvoří **úplný systém**, jestliže ke každé formuli existuje formule s ní ekvivalentní a obsahující pouze spojky z L.
- Úplný systém log. spojek tvoří:
  - negace a implikace
  - negace a konjunkce
  - negace a disjunkce
- Otázka: Kolik různých (binárních) logických spojek můžeme definovat?
  - Netvoří některá z nich sama o sobě úplný systém?

Opakování: Piercova a Shefferova spojka

- Shefferova spojka (NAND)
  - $(a \uparrow b) \Leftrightarrow \neg(a \wedge b)$
- Piercova spojka (NOR)
  - $(a \downarrow b) \Leftrightarrow \neg(a \vee b)$
- Všechny logické spojky je možné vyjádřit pouze pomocí Shefferovy/ Piercovy spojky

Opakování: DNF

- Výroková formule je v **disjunktivní normální formě** (DNF), je-li disjunkcí formulí, pro které platí:
  - každá je konjunkcí atomických výrokových formulí a jejich negací
  - v žádné se nevyskytuje žádná atomická formule současně se svou negací
- DNF je **úplná**, pokud jsou ve všech konjunkcích stejné atomické formule

Opakování: KNF

- Výroková formule je v **konjunktivním normálním tvaru** (KNF), je-li konjunkcí formulí, pro které platí:
  - každá je disjunkcí atomických výrokových formulí a jejich negací
  - v žádné se nevyskytuje žádná atomická formule současně se svou negací
- KNF je **úplná**, pokud jsou ve všech konjunkcích stejné atomické formule

Opakování: DNF a KNF

- Ke každé výrokové formuli lze nalézt ekvivalentní formuli v úplném DNF a KNF
- Úplný DNF/KNF je určen jednoznačně až na volbu a pořadí proměnných
- I prázdná disjunkce (disjunkce prázdné množiny konjunkcí) je v DNF a v KNF
- Jaký je algoritmus převodu do DNF/KNF?

Opakování: postfixový zápis

- Jakoukoliv formuli obsahující binární operátory lze psát
  - infixově 2 + 3 a ∨ b
  - prefixově + 2 3 ∨ a b
  - postfixově 2 3 + a b ∨
- Formule zapsané v postfixu lze vyhodnocovat pomocí **zásobníkového automatu**
  - Protože jazyk VL i jazyk aritmetických výrazů (atd.) jsou CFL

Formální výstavba výrokové logiky

- **Abeceda** – množina symbolů jazyka výrokové logiky (definováno dříve)
- **Formule** – definujeme analogicky pomocí základní dvojice log. spojek
- **Jazyk** – tvořen abecedou a formulemi
- **Axiomy** – je jich nekonečně mnoho, lze je však zadat pomocí základních schémat axiomů výrokové logiky

Pozor!

- V axiomatické výstavbě se neptáme na význam
- Podobnost s reálným světem je „čistě náhodná a je jen vaší představou“
- Axiomatická výstavba zná jen negaci a implikaci
  - ostatní spojky jsou definovány pomocí nich
  - pravdivostní tabulka implikace není definována, ale plyne z axiomů
- **Otázka**: Co z dosud probraných částí VL byla axiomatická teorie (syntaxe) a co model (sémantika)?

Schémata pro axiomy VL

- Pro libovolné formule A, B, C je každá formule některého z následujících tří tvarů **axiomem VL**:

(A1) $A \Rightarrow (B \Rightarrow A)$

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

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

Odvozovací pravidlo

- Jediné pravidlo (jediná operace) podporovaná v axiomatice VL
- **modus ponens** (pravidlo odloučení)
- značíme MP
- Čteme: „Z formulí A, (A ⇒ B) se odvodí B”
  - záležitost sémantiky (interpretace)
- *A*, (*A* ⇒ *B*) se nazývají **předpoklady**
- *B* se nazývá **závěr** odvozovacího pravidla

Substituce

- **Substituce** je konečné zobrazení množiny proměnných na formule
- A[φ/ϕ] značí nahrazení každého výskytu proměnné φ formulí ϕ
- Jazyk VL je uzavřen vzhledem k substituci
  - tj. jsou-li A a ϕ formule a φ výroková proměnná, pak i A[φ/ϕ] je formule.

Syntaktická dokazatelnost ve VL

- **(Syntaktickým) důkazem ve VL** rozumíme konečnou posloupnost VF takovou, že pro danou VF jsou všechny předcházející VF buď axiomem, nebo závěrem pravidla MP, jehož předpoklady jsou mezi předcházejícími VF
- **Formule *A* je (syntakticky) dokazatelná**, jestliže existuje důkaz, jehož poslední VF je *A*
  Syntaktickou dokazatelnost značíme $\vdash A$

Příklad: Důkaz formule $A \Rightarrow A$

- Pro lib. formuli A je $\vdash A \Rightarrow A$
- Důkazem je posloupnost formulí

(1) $A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$
A1

(2) $(A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$
A2

(3) $(A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)$
(1),(2) MP

(4) $A \Rightarrow (A \Rightarrow A)$
A1

(5) $A \Rightarrow A$
(3),(4) MP

Sémantická dokazatelnost ve VL

- Pravdivostní hodnota výrokových proměnných odpovídá interpretaci (realizaci) jazyka VL.
- Řekneme, že formule ϕ **(sémanticky) vyplývá** z formule φ právě tehdy, když v každé interpretaci, v níže je pravdivá formule φ, je pravdivá i formule ϕ.
- Sémantickou dokazatelnost značíme $\varphi \models \phi$

Zobecnění dokazatelnosti

- Dokazatelnost zobecníme na $T \vdash A$
- Definici dokazatelnosti rozšíříme. Na místě předcházejících formulí mohou být
  - axiomy
  - závěry pravidla MP
  - formule z konečné množiny formulí T
- Množina T nazýváme **teorie**

Věta o dedukci

- Připomeňme, že matematika je deduktivní věda – potřeba dedukce
- Nechť T je množina formulí VL a A, B jsou výrokové formule. Pak

$$(T \vdash (A \Rightarrow B) \Leftrightarrow (T \cup \{A\} \vdash B)$$

- Zavedeme zápis T, A místo $T \cup \{A\}$
- Věta o dedukci je další operace, kterou můžeme používat v důkazech

Příklad: Důkaz VF $\neg A \Rightarrow (A \Rightarrow B)$

- Pro lib. VF A, B je $\vdash \neg A \Rightarrow (A \Rightarrow B)$
- Důkazem je posloupnost formulí

(1)	$\vdash \neg A \Rightarrow (\neg B \Rightarrow \neg A)$	A1
(2)	$\neg A \vdash \neg B \Rightarrow \neg A$	VD
(3)	$\vdash (\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$	A3
(4)	$\neg A \vdash A \Rightarrow B$	(2),(3) MP
(5)	$\vdash \neg A \Rightarrow (A \Rightarrow B)$	VD

Věta o neutrální formuli

- Nechť *T* je množina VF a nechť *A*, *B* jsou výrokové formule. Pak

$$(T, A \vdash B) \wedge (T, \neg A \vdash B) \Rightarrow (T \vdash B)$$

- Nástin důkazu:
  - $(T, A \vdash B) \wedge (T, \neg A \vdash B)$
  - $(T, A, \neg A \vdash B)$
  - $(T \vdash (A \wedge \neg A) \Rightarrow B$
  - $(T \vdash B)$

Věta o úplnosti

- **Libovolná formule VL je dokazatelná právě tehdy, když je to tautologie**
- Most mezi axiomatickou a intuitivní VL
- Důkaz $\Rightarrow$
  - Všechny axiomy jsou tautologie
  - Odvozovací pravidlo odvodí tautologii jen z tautologií
- Důkaz $\Leftarrow$
  - Je třeba ukázat úplnost axiomatického systému
  - Mimo rámec předmětu

K procvičení I.

- Nalezněte tři další tautologie a tři kontradikce ve výrokové logice
- Formuli $(a \Rightarrow (b \vee c) \vee ((\neg a \wedge c) \Leftrightarrow b)$
  - negujte
  - převeďte do DNF a KNF
  - převeďte do postfixu
- Vyjádřete $\Rightarrow$ pomocí $\neg$, $\wedge$, $\vee$
- Vyjádřete $\wedge$, $\vee$, $\Leftrightarrow$ pomocí $\neg$, $\Rightarrow$
- Vyjádřete $\neg$, $\wedge$, $\vee$, $\Leftrightarrow$, $\Rightarrow$, $\downarrow$ pomocí $\uparrow$
- Vyjádřete $\neg$, $\wedge$, $\vee$, $\Leftrightarrow$, $\Rightarrow$, $\uparrow$ pomocí $\downarrow$

K procvičení II.

- Dokažte ve výrokové logice
  - zákon dvojí negace $\neg\neg A \Rightarrow A$
  - obrácený zákon dvojí negace $A \Rightarrow \neg\neg A$
  - obměnu implikace $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$
  - formuli $A \Rightarrow (\neg B \Rightarrow \neg(A \Rightarrow B))$
    - čili pravidlo pro negování implikace
  - formuli $(\neg A \Rightarrow A) \rightarrow A$
    - čili Claviův zákom