

Základy matematiky a statistiky pro humanitní obory

Vojtěch Kovář

Fakulta informatiky, Masarykova univerzita
Botanická 68a, 60200 Brno, Czech Republic
xkovar3@fi.muni.cz

část 2

Obsah přednášky

Obsah přednášky

Matematická logika

Výroková logika

Něco z predikátové logiky

Matematická indukce

Vojtěch Kovář (FI MU Brno)

PLIN004

část 2 1 / 18

Vojtěch Kovář (FI MU Brno)

PLIN004

část 2 2 / 18

Matematická logika Matematická logika – motivace

Matematická logika – motivace

► Jazyk matematiky

- přirozený jazyk je víceznačný
- „k jednání XY na úřadě YZ potřebujete pas a řidičský průkaz nebo občanský průkaz“
- matematická fakta potřebujeme zapisovat přesně

► Formalizace pojmu důkaz

- důkaz = posloupnost elementárních kroků
- to, co je „elementární“ je individuální
- logika zavádí přesnou definici elementárního kroku

Vojtěch Kovář (FI MU Brno)

PLIN004

část 2 3 / 18

Matematická logika Typy logik

Typy logik

► Výroková logika

- výroky, logické funkce, pravidlo modus ponens

► Predikátová logika

- predikáty, kvantifikátory

► Další typy logik

- modální, temporální, fuzzy, intenzionální, ...
- nebudeme se jimi zabývat

► Naším cílem je naučit se logiku prakticky používat

- → Číst a psát
- nikoli zkoumat její temná zákoutí (viz předmět „Matematická logika“ na FI)

Vojtěch Kovář (FI MU Brno)

PLIN004

část 2 4 / 18

Výroková logika Výroková logika

Výroková logika

► Výrok

- základní jednotka
- tvrzení, jemuž lze přiřadit pravdivostní hodnotu
- např. „ $a = 1$ “, „4 je prvočíslo“

► Pravdivost

- přiřazení hodnoty 0 nebo 1 každému výroku
- zapisujeme $v(A) = 1$ („výrok A platí“)
- $v(A) = 0$ („výrok A neplatí“)

► Logické funkce

- konstrukce složitějších výroků z výroků jednodušších

Vojtěch Kovář (FI MU Brno)

PLIN004

část 2 5 / 18

Výroková logika Logické funkce

Logické funkce (1)

► Základní logické funkce

- necht' A, B jsou výroky
- **negace** $\neg A$
- $v(\neg A) = 0$, je-li $v(A) = 1$
- $v(\neg A) = 1$, je-li $v(A) = 0$
- **implikace** $A \Rightarrow B$
- $v(A \Rightarrow B) = 0$, je-li $v(A) = 1$ a $v(B) = 0$
- $v(A \Rightarrow B) = 1$ v ostatních případech
- kombinací těchto funkcí lze vyjádřit všechny ostatní logické funkce

Vojtěch Kovář (FI MU Brno)

PLIN004

část 2 6 / 18

Výroková logika Logické funkce

Logické funkce (2)

► Odvozené logické funkce

- **konjunkce** $A \wedge B$ (logické „a“)
- $v(A \wedge B) = 1$, je-li $v(A) = 1$ a $v(B) = 1$
- $v(A \wedge B) = 0$ v ostatních případech
- **disjunkce** $A \vee B$ (logické „nebo“)
- $v(A \vee B) = 0$, je-li $v(A) = 0$ a $v(B) = 0$
- $v(A \vee B) = 1$ v ostatních případech
- **ekvivalence** $A \Leftrightarrow B$
- $(A \Rightarrow B) \wedge (B \Rightarrow A)$

Vojtěch Kovář (FI MU Brno)

PLIN004

část 2 7 / 18

Výroková logika Odvozování

Odvozování

► Schémata axiomů

- pro libovolné výroky A, B, C platí
- $A \Rightarrow (B \Rightarrow A)$
- $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$
- $(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$
- dosazením konkrétních výroků vzniknou **axiomy**

► Odvozovací pravidlo modus ponens

- pokud platí A a platí $A \Rightarrow B$, pak platí B

► Formální definice důkazu

- posloupnost výroků, z nichž každý je buď axiom nebo výsledek aplikace odvozovacího pravidla na předchozí výroky

Vojtěch Kovář (FI MU Brno)

PLIN004

část 2 8 / 18

Příklad důkazu: $X \Rightarrow X$

► Schémata axiomů

- $A \Rightarrow (B \Rightarrow A)$
- $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$
- $(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$

► Dokazujeme, že pro libovolný výrok X platí $X \Rightarrow X$

1. $(X \Rightarrow ((X \Rightarrow X) \Rightarrow X)) \Rightarrow ((X \Rightarrow (X \Rightarrow X)) \Rightarrow (X \Rightarrow X))$ / axiom 2
2. $X \Rightarrow ((X \Rightarrow X) \Rightarrow X)$ / axiom 1
3. $(X \Rightarrow (X \Rightarrow X)) \Rightarrow (X \Rightarrow X)$ / aplikace modus ponens na 2. a 1.
4. $X \Rightarrow (X \Rightarrow X)$ / axiom 1
5. $X \Rightarrow X$ / aplikace modus ponens na 4. a 3.

Něco z predikátové logiky (1)

► Ohodnocení proměnných

- formule („výroky“) mohou obsahovat proměnné ($x = 1$)
- pravdivost pak závisí na ohodnocení, tj. přiřazení hodnot proměnným

► Kvantifikátory

- \exists – existuje alespoň jedno ohodnocení, při kterém formule platí
- \forall – výrok platí pro všechna možná ohodnocení
- např.: $\exists x(x = 0 \wedge x = 1)$

Něco z predikátové logiky (2)

► Predikáty

- funkční symboly – vyjadřují fakta o konstantách a proměnných
- např. $\text{Prime}(x)$ – „ x je prvočíslo“
- např. $\in(x, Y)$, resp. $x \in Y$ – „prvek x patří do množiny Y “

► Příklady složitějších formulí

- $\exists x(\exists k(x = 2k + 1) \wedge \exists m(x = 2m))$
- $\forall x(\text{Prime}(x) \Rightarrow \exists k(x = 2k))$
- $\exists x(\text{Prime}(x) \wedge \exists k(x = 2k))$
- dokážete je přečíst?

Matematická indukce

► Princip

- potřebujeme dokázat, že pro všechny prvky nějaké posloupnosti x_0, \dots, x_n, \dots platí nějaký výrok A
- $\forall n(A(x_n))$
- dokážeme výrok pro x_0
- \rightarrow **báze indukce**
- dokážeme, že pokud výrok platí pro x_{i-1} , pak platí i pro x_i pro libovolné i
- $A(x_{i-1}) \Rightarrow A(x_i)$
- \rightarrow **indukční krok**
- levá strana implikace výše se nazývá **indukční předpoklad**

Příklad indukce

► Dokážeme, že pro všechna přirozená $n \geq 1$ platí:

- $1 + 2 + \dots + n = n/2 * (1 + n)$

► Báze

- $1 = 1/2 * (1 + 1)$

► Indukční krok

- předpokládáme: $1 + 2 + \dots + k = k/2 * (1 + k)$
- dokážeme: $1 + 2 + \dots + k + (k + 1) = (k + 1)/2 * (1 + (k + 1))$

Příklad indukce (2)

► Indukční krok

- předpokládáme: $1 + 2 + \dots + k = k/2 * (1 + k)$
- dokážeme: $1 + 2 + \dots + k + (k + 1) = (k + 1)/2 * (1 + (k + 1))$
- $1 + 2 + \dots + k + (k + 1)$
- $k/2 * (1 + k) + (k + 1)$
- $(k + k^2)/2 + (k + 1)$
- $(k + k^2 + 2k + 2)/2$
- $(k^2 + 3k + 2)/2$
- $(k + 2) * (k + 1)/2$
- $(k + 1)/2 * (k + 2)$
- $(k + 1)/2 * (1 + (k + 1))$

Proč to funguje?

► Intuitivní ověření korektnosti

- báze \rightarrow platí $A(x_0)$
- indukční krok \rightarrow platí $(A(x_0) \Rightarrow A(x_1))$
- modus ponens \rightarrow platí i $A(x_1)$
- indukční krok \rightarrow platí $(A(x_1) \Rightarrow A(x_2))$
- modus ponens \rightarrow platí i $A(x_2)$
- atd. ad infinitum

► Formální důkaz korektnosti matematické indukce

- existuje, ale nad rámec předmětu

Složitější typy indukce (1)

► Složitější indukční předpoklad

- např. platí $A(x_{i-1})$ i $A(x_{i-2})$
- musíme dokázat odpovídající bázi
- tj. $A(x_0)$ i $A(x_1)$

► Induktivní definice

- umožňují popsat potenciálně nekonečné struktury
- př.: definice číselných výrazů se sčítáním a násobením
- číslo je výraz
- $(x + y)$, kde x a y jsou výrazy, je výraz
- $(x * y)$, kde x a y jsou výrazy, je výraz

Složitější typy indukce (2)

► Strukturální indukce

- aplikujeme na induktivně definované objekty (např. výrazy)
- báze indukce: výrok platí pro čísla
- indukční krok 1: výrok platí pro x a $y \Rightarrow$ platí i pro $(x + y)$
- indukční krok 2: výrok platí pro x a $y \Rightarrow$ platí i pro $(x * y)$

► Princip zůstává stejný, pouze vedení důkazu je komplikovanější

► Důkaz, že každý výraz podle definice výše má sudý počet závorek?

Všichni koně mají stejnou barvu

► **Věta:** V každém stádě mají všichni koně stejnou barvu.

► **Důkaz:** indukcí vzhledem k velikosti stáda

- **báze:** Ve stádě o 1 koni mají všichni stejnou barvu.
- **indukční krok:** Předp., že věta platí pro dvě stáda o $n - 1$ koních; dokážeme, že platí pro stádo o velikosti n
- $S_1 = \{K_1, \dots, K_{n-1}\}$, $S_2 = \{K_2, \dots, K_n\}$
- podle I. P. mají v S_1 i v S_2 všichni koně stejnou barvu
- koně K_2, \dots, K_{n-1} jsou v obou stádech \Rightarrow i barva obou stád je stejná
- tedy i ve stádě $S = \{K_1, \dots, K_n\}$ mají všichni koně stejnou barvu

► Kde je problém?