Základy matematiky a statistiky pro humanitní obory I

Vojtěch Kovář

Fakulta informatiky, Masarykova univerzita
Botanická 68a, 602 00 Brno, Czech Republic
xkovar3@fi.muni.cz

část 2

Obsah přednášky

Matematická logika – motivace

- Jazyk matematiky
  - přirozený jazyk je víceznačný
  - „k jednání X 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

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
  - $\rightarrow$ číst a psát
  - nikoli zkoumat její temná zákoutí (viz předmět „Matematická logika“ na FI)

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

Logické funkce (1)

- Základní logické funkce
  - nechť 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

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 $A \Leftrightarrow B$
  - $(A \Rightarrow B) \wedge (B \Rightarrow A)$

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

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

- 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.: $\exists x(x = 0 \land x = 1)$

Něco z predikátové logiky (2)

- Funkční symboly
  - kombinují objekty, se kterými zacházíme (množiny, čísla)
  - výsledkem je další objekt
  - např. plus, množinové sjednocení
  - např. $+(x, y)$, resp. $x + y$”
- Predikáty
  - vyjadřují fakta o konstantách a proměnných
  - výstupem je pravdivostní hodnota
  - např. Prime(x) – „x je prvočíslo“
  - např. $\in (x, Y)$, resp. $x \in Y$ – „prvek x patří do množiny Y“

Něco z predikátové logiky (3)

- Příklady složitějších formulí
  - $\exists x(\exists k(x = 2k + 1) \land \exists m(x = 2m))$
  - $\forall x(Prime(x) \Rightarrow \exists k(x = 2k))$
  - $\exists x(Prime(x) \land \exists k(x = 2k))$
  - dokážete je přečíst?

Matematická indukce

- Obecný matematický princip
  - použitelný pro definice, důkazy
  - napřed vyrobíme/dokážeme něco jednoduchého
  - $\rightarrow$ báze indukce
  - pak vyrobíme z obecného jednoduchého objektu o krok složitější objekt
  - případně dokážeme, že z platnosti pro jednoduchý objekt vyplývá platnost pro složitější objekt
  - $\rightarrow$ indukční krok
  - tím dostaneme nekonečnou řadu definic/důkazů

Induktivní definice

- Báze indukce
  - definujeme nejjednodušší prvky
- Indukční krok
  - popíšeme, jak se z jednodušších prvků vyrobí složitější
- Příklad: induktivně definované posloupnosti
  - definujeme nekonečnou posloupnost $3, 5, 7, 9, \ldots$
  - báze indukce: $a_1 = 3$
  - indukční krok: $a_{n+1} = a_n + 2$

Induktivní definice (2)

- Bází může být víc
  - Fibonacciho posloupnost: 0, 1, 1, 2, 3, 5, 8, 13, ...
  - báze indukce: $a_1 = 0$
  - báze indukce: $a_2 = 1$
  - indukční krok: $a_{n+2} = a_{n+1} + a_n$
- Indukčních kroků může být víc
  - definice toho, jak vypadá správná výroková formule
  - báze indukce: libovolný jednoduchý výrok A je výroková formule
  - indukční krok: pokud A je výroková formule, pak $\neg(A)$ je výroková formule
  - indukční krok: pokud A a B jsou výrokové formule, pak $(A \Rightarrow B)$ je výroková formule

Důkaz matematickou indukcí

- Princip
  - potřebujeme dokázat, že pro všechny prvky nějaké posloupnosti $x_0, \ldots, x_n, \ldots$ 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:
  - $1 + 2 + ... + n = n/2 * (1 + n)$
- Báze
  - $1 = 1/2 * (1 + 1)$
- Indukční krok
  - předpokládáme: $1 + 2 + ... + k = k/2 * (1 + k)$
  - dokážeme: $1 + 2 + ... + k + (k + 1) = (k + 1)/2 * (1 + (k + 1))$

Příklad indukce (2)

- Indukční krok
  - předpokládáme: $1 + 2 + ... + k = k/2 * (1 + k)$
  - dokážeme: $1 + 2 + ... + k + (k + 1) = (k + 1)/2 * (1 + (k + 1))$
  - $1 + 2 + ... + k = k/2 * (1 + k)$
  - $1 + 2 + ... + k + (k + 1) = k/2 * (1 + k) + (k + 1)$
  - $1 + 2 + ... + k + (k + 1) = (k * (1 + k) + 2 * (k + 1))/2$
  - $1 + 2 + ... + k + (k + 1) = (k + k^2 + 2k + 2)/2$
  - $1 + 2 + ... + k + (k + 1) = (k^2 + 3k + 2)/2$
  - $1 + 2 + ... + k + (k + 1) = (k + 1)(k + 2)/2$
  - $1 + 2 + ... + k + (k + 1) = (k + 1)/2 * (1 + (k + 1))$

Proč to funguje?

- Intuitivní ověření korektnosti
  - báze → platí $A(x_0)$
  - indukční krok → platí $(A(x_0) \Rightarrow A(x_1))$
  - modus ponens → platí i $A(x_1)$
  - indukční krok → platí $(A(x_1) \Rightarrow A(x_2))$
  - modus ponens → platí i $A(x_2)$
  - atd. ad infinitum
- Formální důkaz korektnosti matematické indukce
  - sporem – předpokládáme, že nějaké $A(x_n)$ neplatí

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 $A(x_1)$

Složitější typy indukce (2)

- Strukturální indukce
  - aplikujeme na induktivně definované objekty (např. výrokové formule)
  - báze indukce: věta platí pro jednoduché výroky
  - indukční krok 1: věta platí pro formuli A $\Rightarrow$ platí i pro $\neg(A)$
  - indukční krok 2: věta platí pro formule A a B $\Rightarrow$ platí i pro $(A \Rightarrow B)$
- Princip zůstává stejný, pouze vedení důkazu je komplikovanější
- Důkaz, že každá formule 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 koních; dokážeme, že platí pro stádo o velikosti $n + 1$
  - $S_1 = \{K_1, ..., K_n\}$, $S_2 = \{K_2, ..., K_{n+1}\}$
  - podle předpokladu mají v S_1 i v S_2 všichni koně stejnou barvu
  - koně $K_2, ..., K_n$ jsou v obou stádech $\Rightarrow$ i barva obou stád je stejná
  - tedy i ve stádě $S = \{K_1, ..., K_{n+1}\}$ mají všichni koně stejnou barvu
- Kde je problém? (zřejmě existují různí koně :))