Lineární modely - 3. přednáška

Základní pojmy z teorie množin

Ondřej Klíma

7. 3. 2013

Osnova přednášky

- Množiny: kartézský součin množin, podmnožiny
- Zobrazení: injektivní, surjektivní, bijektivní
- Relace: uspořádání, relace ekvivalence
- Matice

Množiny

- Intuitivní definice: množina je soubor prvků.
  Pouze nahrazujeme jedno slovo druhým.
  Formálně se teorie množin buduje jinak.
- My si potřebujeme rozumnět, když řekneme, že:

$$a \text{ je prvek množiny } X \quad \dots \quad a \in X\,.$$

- Kdy jsou dvě množiny stejné?
  Když mají stejné prvky.

Kartézský součin množin

- Kartézský součin množin $A \times B$: prvky uspořádané dvojice. Dvě uspořádané dvojice se rovnají, když mají stejné obě složky.
- Formální zápis:

$$A \times B = \{(x, y) \mid x \in A, y \in B\}$$

- Příklady: $\mathbb{R} \times \mathbb{R}$, $\{1, \dots, 6\} \times \{1, \dots, 6\}$.
- Obecněji $A_1 \times A_2 \times \cdots \times A_n$, prvky $a = (a_1, a_2, \dots, a_n)$.
  Příklad: $\mathbb{R}^n$ ($n = 3$).
  $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|$.

Podmnožiny

Systém všech podmnožin: pro X klademe $\mathcal{P}(X) = \{A \mid A \subseteq X\}$.

Pro počet prvků platí: je-li $|X| = n$ pak $|\mathcal{P}(X)| = 2^n$. Víme, že k prvkových podmnožin n-prvkové množiny je $\binom{n}{k}$. Tedy

$$|\mathcal{P}(X)| = \sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n$$

dle Binomické věty.

Jde i přímo. Když „vyrábíme“ podmnožinu, procházíme množinu X a pro každý prvek zvlášť se rozhodujeme, zda jej do budované podmnožiny dáme nebo ne. Pro každý prvek z množiny X tedy máme dvě možnosti. Proto celkem 2^n.

Pozn.: Předvedli jsme kombinatorický důkaz rovnosti $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Zobrazení

- Zobrazení f z množiny A do množiny B, $f : A \to B$, je předpis, který pro každý prvek $a \in A$ jednoznačně určuje jeden prvek $b = f(a)$ z množiny B.
- Definujeme $Im(f) = \{f(a) \mid a \in A\} \subseteq B$, tzv. obor hodnot.
- Někdy se zobrazení chápe obecněji: pro každé $a \in A$ určuje f *nejvýše* jeden prvek $b = f(a)$ z množiny B. (Potom se také definuje $Dom(f) = \{a \in A \mid \exists\ f(a)\}$.)
- Příklady:
  - transformace roviny – shodnosti (rotace, translace), podobnosti, promítání (projekce)
  - konjugování (sdruženost): $\alpha : \mathbb{C} \to \mathbb{C}$, $\alpha(z) = \bar{z}$
  - operace na množině: $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
  - $vol : \mathcal{A} \to \mathbb{R}$, zde $\mathcal{A} \subseteq \mathcal{P}(\mathbb{R}^2)$
  - pravděpodobnost $P : \mathcal{A} \to \mathbb{R}$, $Im(P) =< 0, 1 >$.
- Formálně: f je podmnožina $A \times B$ – graf zobrazení.

Skládání zobrazení

- Máme-li zobrazení $f : A \to B$ a $g : B \to C$, pak jejich složení $g \circ f$ je definováno takto:

  $$\text{pro } a \in A \text{ klademe } \quad (g \circ f)(a) = g(f(a))\,.$$

  Tedy $g \circ f$ je zobrazení z A do C.
  Skutečně je, pro libovolné $a \in A$, jednoznačně určeno $(g \circ f)(a) \in C$.

  Pozn.: Anglická literatura často používá zápis skládání zleva doprava.

- Příklad: $f, g : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + 2$, $g(x) = x^3 + 3$.

  Pak $$(f \circ g)(x) = f(g(x)) = f(x^3 + 3) = \\ = (x^3 + 3)^2 + 2 = x^6 + 6x^3 + 11.$$

  $$(g \circ f)(x) = g(f(x)) = g(x^2 + 2) = (x^2 + 2)^3 + 3 \\ = x^6 + 6x^4 + 12x^2 + 11.$$

  Tedy $f \circ g \neq g \circ f$.

Injektivní, surjektvní a bijektivní zobrazení

Říkáme, že zobrazení f z množiny A do množiny B je

- surjektivní, jestliže $Im(f) = B$,
- injektivní, jestliže pro každé $b \in Im(f)$ existuje právě jeden vzor $a \in A$, tak že $f(a) = b$,
  (Alternativně: pro libovolná $a, a' \in A$ z $f(a) = f(a')$ plyne $a = a'$.)
- bijektivní, jestliže je surjektivní a injektivní zároveň.

Příklad

Buď $n > 0$ přirozené číslo a $X = \{1, \dots, n\}$. Uvažme $\alpha : \mathcal{P}(X) \to \{0, 1\}^n$, dané takto: $f(B) = (a_1, \dots, a_n)$, kde pro každé $1 \le i \le n$ platí $a_i = 1 \iff i \in B$. Dokažte, že α je bijekce.

Pozn.: Funguje i pro nekonečné množiny.

Bijektivní zobrazení – příklad

Pro konečné množiny A, B existuje bijekce $f : A \to B$ právě tehdy, když mají stejný počet prvků.

Příklad

Buď $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \setminus \{0\}$ dané vztahem $\varphi(x, y) = 2^x \cdot (2y + 1)$. Dokažte, že φ je bijekce.

Inverzní zobrazení

Identita na množině A je zobrazení $\mathrm{id}_A \colon A \to A$, dané předpisem $\mathrm{id}_A(x) = x$, pro všechna $x \in A$.

Jestliže zobrazení f z množiny A do množiny B je bijektivní, pak lze definovat zobrazení $g : B \to A$ předpisem

$$g(b) = a \iff f(a) = b, \text{ kde } a \in A, b \in B\,.$$

Toto zobrazením se nazývá inverzní zobrazení a značí se f^{-1}. Existence inverzního zobrazení je ekvivalentní s bijektivitou f: pokud k zobrazení $f : A \to B$ existuje zobrazení $g : B \to A$, takové, že $g \circ f = \mathrm{id}_A$ a $f \circ g = \mathrm{id}_B$, pak f i g jsou bijekce.

Příklad

Pro zobrzení $\alpha : \mathbb{C} \to \mathbb{C}$, $\alpha(a + b.i) = a - b.i$, máme $\alpha \circ \alpha = \mathrm{id}_{\mathbb{C}}$.

Příklad

Shodná zobrazení v rovině.

Relace

- Intuitivně lze relaci chápat jako „vícehodnotové zobrazení“. Formálně: naopak – zobrazení je speciální případ relace.
- Binární relací mezi množinami A a B rozumíme podmnožinu R kartézského součinu $A \times B$.
  Často píšeme $a \simeq_R b$ pro vyjádření skutečnosti, že $(a, b) \in R$, tj. že prvky $a \in A$ a $b \in B$ jsou v relaci R.
- Definičním oborem relace je množina

  $$Dom(R) \subseteq A, \quad Dom(R) = \{a \in A \mid \exists b \in B, (a, b) \in R\} .$$

  Podobně oborem hodnot relace je množina

  $$Im(R) \subseteq B, \quad Im(R) = \{b \in B \mid \exists a \in A, (a, b) \in R\} .$$

- Obecně: n-ární relace, tj. podmnožiny $A_1 \times \cdots \times A_n$.

Relace – příklady

- Databáze: A_1 kódy předmětů, A_2 vyučující, A_3 semestr, ...

Nás zajímají nejvíce binární relace, a to jednak zobrazení, a dále relace na množině, tj. situace, kdy $A = B$.

- $\mathrm{id}_A = \{(a, a) \in A \times A \mid a \in A\}$,
- $R_< = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a < b\}$, relace „menší“
- $R_| = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid (\exists c \in \mathbb{N})\ (b = a \cdot c)\}$, relace „dělí“.
- $\subseteq$ na množině $\mathcal{P}(X)$
- $R = \{(A, B) \mid |A| = |B|\}$ na $\mathcal{P}(X)$, „stejná mohutnost“
- grafy ...

Skládání relací, inverzní relace

- Skládání relací se definuje podobně jako u zobrazení, jen je třeba uvažovat „víc hodnot“.
- Pro relace $R \subseteq A \times B$ a $S \subseteq B \times C$. Definujeme $S \circ R \subseteq A \times C$ takto:

$$S \circ R = \{(a, c) \mid (\exists b \in B)\ (\ (a, b) \in R, (b, c) \in S\ )\}.$$

- Pro každou relaci $R \subseteq A \times B$ definujeme inverzní relaci

$$R^{-1} = \{(b, a) \mid (a, b) \in R\} \subseteq B \times A.$$

- Pozor, pro každé zobrazení máme takto definovánu jeho inverzní relaci, ta však nemusí být zobrazením!
- Pro zobrazení $f : A \to B$ platí: f je bijekce právě tehdy, když inverzní relace je zobrazení. V tom případě je inverzní relace inverzním zobrazením.
- Obecně $R \circ R^{-1}$ není identita. Např: $R_<^{-1} \circ \mathbb{R}_< = \mathbb{N} \times \mathbb{N}$.

Základní vlastnosti relací

Definice

O relaci R na množině A řekneme, že je:

- reflexivní, pokud $\mathrm{id}_A \subseteq R$,
  tj. pokud pro všechny $a \in A$ platí $(a, a) \in R$,
- symetrická, pokud $R^{-1} = R$, tj. pokud pro všechny $a, b \in A$ platí $(a, b) \in R \implies (b, a) \in R$,
- antisymetrická, pokud $R^{-1} \cap R \subseteq \mathrm{id}_A$, tj. pokud pro všechny $a, b \in A$ platí $((a, b) \in R, (b, a) \in R) \implies a = b$,
- tranzitivní, pokud $R \circ R \subseteq R$, tj. pokud pro všechny $a, b, c \in A$ platí $((a, b) \in R, (b, c) \in R) \implies (a, c) \in R$.

Relace se nazývá ekvivalence, pokud je současně reflexivní, symetrická i tranzitivní.
Relace se nazývá uspořádání jestliže je reflexivní, tranzitivní a antisymetrická.

Relace ekvivalence a uspořádání – příklady

- id_A relace ekvivalence i uspořádání.
- $R_<$ není uspořádání (není reflexivní).
- $R_\leq = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a \leq b\}$ je uspořádání.
- $R_|$ je uspořádání.
- $\subseteq$ na množině $\mathcal{P}(X)$ je uspořádání.
- $R = \{(A, B) \mid |A| = |B|\}$ na $\mathcal{P}(X)$ je relace ekvivalence.

Příklad

Buď $n > 1$ přirozené číslo. Definujeme relaci $\sim_n$ na množině $\mathbb{Z}$ takto: pro libovolná $a, b \in \mathbb{Z}$ máme

$$a \sim_n b \quad \iff \quad n \mid a - b\,.$$

Potom $\sim_n$ je relace ekvivalence.

Rozklad podle relace ekvivalence

Každá relace ekvivalence R na množině A zadává tzv. rozklad množiny A na disjunktní podmnožiny vzájemně ekvivalentních prvků (tzv. třídy ekvivalance). Klademe pro $a \in A$ libovolné

$$[a]_R = \{b \in A \mid (a, b) \in A\}.$$

Potom $A/R = \{[a]_R \mid a \in A\}$.

Příklad

Pro $n = 4$ a relaci $R = \sim_n = \sim_4$ máme

$$\begin{aligned}
[0]_4 &= \{0, 4, 8, \dots, -4, -8, \dots\} = \{4k \mid k \in \mathbb{Z}\} \\
[1]_4 &= \{1, 5, 9, \dots, -3, -7, \dots\} = \{4k + 1 \mid k \in \mathbb{Z}\} \\
[2]_4 &= \{2, 6, 10, \dots, -2, -6, \dots\} = \{4k + 2 \mid k \in \mathbb{Z}\} \\
[3]_4 &= \{3, 7, 11, \dots, -1, -5, \dots\} = \{4k + 3 \mid k \in \mathbb{Z}\}
\end{aligned}$$

$\mathbb{Z}/\sim_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$

Matice – definice

- Co je matice? Neformálně: Obdélníkové schéma s prvky z R (pole skalárů).
- Matice typu $m \times n$ má m řádků a n sloupců:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

- Formálně: $A : \{1, \dots, m\} \times \{1, \dots, n\} \to R$
- My budeme pracovat s maticemi nad $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Obecně se někdy hodí i jiné množiny R: např. $R = \{0, 1\}$ v teorii grafů.

Sčítání a násobení matic

- $Mat_{mn}(R)$ množina všech matic typu $m \times n$ nad R.
- Pro $A, B \in Mat_{mn}(R)$ definujeme matici $A + B \in Mat_{mn}(R)$, vztahem

$$A + B = (c_{ij}), \text{ kde } c_{ij} = a_{ij} + b_{ij}, 1 \leq i \leq m, 1 \leq j \leq n\,.$$

- $(R, +)$ (kom.) grupa, pak $(Mat_{mn}(R), +)$ je (kom.) grupa.
- Nulová matice, opačná matice ...
- Pro $A \in Mat_{mn}(R)$ a $r \in R$ definujeme násobek $r \cdot A$ jako matici $(c_{ij}) \in Mat_{mn}(R)$, kde $c_{ij} = r \cdot a_{ij}$.
- Pro matici $A = (a_{ij})$ typu $m \times n$ a matici $B = (b_{kl})$ typu $n \times p$ definujeme součin $A \cdot B$ jako matici (c_{st}) typu $m \times p$, kde

$$c_{st} = \sum_{j=1}^{n} a_{sj} b_{jt}\,.$$

Vlastnosti násobení matic

- Násobení matic je asociativní: Je-li A typu $m \times n$, B typu $n \times p$ a C typu $p \times q$, pak $(A \cdot B) \cdot C = A \cdot (B \cdot C)$.
- Pro $Mat_{nn}(R)$ – čtvercové matice – je $\cdot$ operací na této množině.
    - Neutrální prvek vzhledem k násobení – jednotková matice

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

    - Násobení matic není obecně komutativní

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Shrnutí, požadavky

- Skládat zobrazení.
- Poznat injektivní, surjektivní a bijektivní zobrazení.
- Poznat relaci ekvivalenci a uspořádání (tj. základní vlastnosti: reflexivní, ...).
- Maticový počet: sčítání, násobení a další operace s maticemi (bude časem víc: inverzní matice).