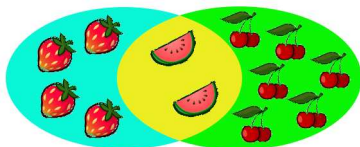


3 Množiny, Relace a Funkce

V přehledu matematických formalismů informatiky se v této lekci zaměříme na základní „datové typy“ matematiky, tj. na množiny, relace a funkce. O množinách jste sice zřejmě slyšeli už na základní škole, ale podstatou našeho předmětu je uvést povětšinou neformálně známé pojmy na patřičnou formální úroveň nutnou pro teoretické základy informatiky.



□

Stručný přehled lekce

- * Uvedení množin a operací množinového kalkulu.
- * Některé vlastnosti množin, princip inkluze a exkluze.
- * Relace a definice funkcí, základní vlastnosti.
- * Posloupnosti a rekurentní vztahy.

3.1 Pojem množiny

* Co je vlastně **množina**? □

Na tuto otázku bohužel není zcela jednoduchá odpověď. . .

- Naivní pohled: „*Množina je soubor prvků a je svými prvky plně určena.*“ □
- Pozor, není skutečného rozdílu mezi „množinami“ a „prvky“.
Množiny mohou být prvky jiných množin! □
- Příklady: \emptyset , $\{a, b\}$, $\{b, a\}$, $\{a, b, a\}$, $\{\{a, b\}\}$, $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$,
 $\{x \mid x \text{ je liché přirozené číslo}\}$ □

Značení: Počet prvků (*mohutnost*) množiny A zapisujeme $|A|$.

- $|\emptyset| = 0$, $|\{\emptyset\}| = 1$, $|\{a, b, c\}| = 3$, $|\{\{a, b\}, c\}| = 2$ □

Značení množin a jejich prvků:

- $x \in M$ „ x je *prvkem* množiny M “. □
- některé vlastnosti $a \in \{a, b\}$, $a \notin \{\{a, b\}\}$, $\{a, b\} \in \{\{a, b\}\}$,
- *prázdná* množina \emptyset , $a \notin \emptyset$, $\emptyset \in \{\emptyset\}$, $\emptyset \notin \emptyset$,
- *rovnost* množin $\{a, b\} = \{b, a\} = \{a, b, a\}$, $\{a, b\} \neq \{\{a, b\}\}$.

Definice: Množina A je *podmnožinou* množiny B , právě když každý prvek A je prvkem B . Píšeme $A \subseteq B$ nebo také $B \supseteq A$; říkáme také, že se jedná o *inkluzi*. \square

- Platí $\{a\} \subseteq \{a\} \subseteq \{a, b\} \not\subseteq \{\{a, b\}\}$, $\emptyset \subseteq \{\emptyset\}$,
- $A \subset B$ právě když $A \subseteq B$ a $A \neq B$ (A je *vlastní* podmnožinou B). \square

Definice: Dvě množiny jsou si *rovny* $A = B$ právě když $A \subseteq B$ a $B \subseteq A$.

- Podle definice jsou množiny A a B stejné, mají-li stejné prvky. \square
- Důkaz rovnosti množin $A = B$ má obvykle **dvě části**:
Odděleně se dokáží inkluze $A \subseteq B$ a $B \subseteq A$.

Značení: Některé běžné množiny v matematice se značí

- * $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ je množina přirozených čísel,
- * $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$ je množina celých čísel,
- * $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ je množina celých kladných čísel,
- * \mathbb{Q} je množina racionálních čísel (zlomků).
- * \mathbb{R} je množina reálných čísel. \square

Poznámka: Tyto uvedené číselné množiny jsou vesměs *nekonečné*, na rozdíl od konečných množin uvažovaných v předchozím „naivním“ pohledu. \square

Pojem nekonečné množiny se přímo v matematice objevil až teprve v 19. století a bylo s ním spojeno několik **paradoxů** ukazujících, že naivní pohled na teorii množin pro nekonečné množiny nedostačuje. My se k problematice nekonečných množin, Kantorově větě a Russelově paradoxu vrátíme v závěru našeho předmětu.

3.2 Množinové operace

Definice: *Sjednocení* \cup a *průnik* \cap dvou množin A, B definujeme

$$A \cup B = \{x \mid x \in A \text{ nebo } x \in B\} \square,$$

$$A \cap B = \{x \mid x \in A \text{ a současně } x \in B\} \square$$

- Příklady $\{a, b, c\} \cup \{a, d\} = \{a, b, c, d\}$, $\{a, b, c\} \cap \{a, d\} = \{a\}$. \square
- Vždy platí „distributivita“ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
a $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. \square

Definice: Pro libovolný počet množin indexovaných pomocí I rozšířeně

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ pro nějaké } i \in I\} \square,$$

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ pro každé } i \in I\} \square$$

- Nechť $A_i = \{2 \cdot i\}$ pro každé $i \in \mathbb{N}$. Pak $\bigcup_{i \in \mathbb{N}} A_i$ je množina všech sudých přirozených čísel. \square
- Nechť $B_i = \{x \mid x \in \mathbb{N}, x \geq i\}$ pro každé $i \in \mathbb{N}$. Pak $\bigcap_{i \in \mathbb{N}} B_i = \emptyset$.

Definice: *Rozdíl* \setminus a *symetrický rozdíl* Δ dvou množin A, B definujeme

$$A \setminus B = \{x \mid x \in A \text{ a současně } x \notin B\} \square,$$

$$A \Delta B = (A \setminus B) \cup (B \setminus A). \square$$

- Příklady $\{a, b, c\} \setminus \{a, b, d\} = \{c\}$, $\{a, b, c\} \Delta \{a, b, d\} = \{c, d\}$. \square
- Vždy platí například $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$ apod. \square

Definice: Necht' $A \subseteq M$. *Doplňěk* A *vzhledem k* M je množina $\overline{A} = M \setminus A$.

- Jedná se o poněkud specifickou operaci, která **musí být vztažena** vzhledem k *nosné množině* M ! \square
- Je-li $M = \{a, b, c\}$, pak $\overline{\{a, b\}} = \{c\}$. Je-li $M = \{a, b\}$, pak $\overline{\{a, b\}} = \emptyset$. \square
- Vždy pro $A \subseteq M$ platí $\overline{\overline{A}} = A$ („dvojitý“ doplňěk). \square
- Vždy pro $A, B \subseteq M$ platí $\overline{A \cup B} = \overline{A} \cap \overline{B}$ a $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
(Viz Vennovy diagramy.)

Uspořádané dvojice a kartézský součin

Definice: *Uspořádaná dvojice* (a, b) je zadána množinou $\{\{a\}, \{a, b\}\}$. \square

Fakt: Platí $(a, b) = (c, d)$ právě když $a = c$ a současně $b = d$. \square

Příklad 3.1. *Co je podle definice (a, a) ?* \square

$$(a, a) = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}. \quad \square$$

Definice 3.2. Kartézský součin dvou množin A, B definujeme jako množinu všech uspořádaných dvojic ze složek z A a B

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

\square

- Příklady $\{a, b\} \times \{a\} = \{(a, a), (b, a)\}$,
 $\{c, d\} \times \{a, b\} = \{(c, a), (c, b), (d, a), (d, b)\}$. \square
- Platí $\emptyset \times X = \emptyset$ pro každou množinu X . \square
- Mnemotechnická pomůcka

$$|A \times B| = |A| \cdot |B|.$$

Skládání součinu

Definice: Pro každé $k \in \mathbb{N}, k > 0$ definujeme *uspořádanou k -tici* (a_1, \dots, a_k) induktivně takto

- $(a_1) = a_1,$
- $(a_1, \dots, a_i, a_{i+1}) = ((a_1, \dots, a_i), a_{i+1}). \square$

Fakt: Platí $(a_1, \dots, a_k) = (b_1, \dots, b_k)$ právě když $a_i = b_i$ pro každé $1 \leq i \leq k$. \square

Definice *kartézského součinu* více množin: Pro každé $k \in \mathbb{N}$ definujeme

$$A_1 \times \dots \times A_k = \{(a_1, \dots, a_k) \mid a_i \in A_i \text{ pro každé } 1 \leq i \leq k\}. \square$$

- Příklad $\mathbb{Z}^3 = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} = \{(i, j, k) \mid i, j, k \in \mathbb{Z}\}.$
- Co je A^0 ? $\square \quad \{\emptyset\}$, neboť jediná uspořádaná 0-tice je právě prázdná \emptyset .

Poznámka: Podle uvedené definice **není** součin asociativní, tj. obecně nemusí platit, že $A \times (B \times C) = (A \times B) \times C$. \square

V matematické praxi je někdy výhodnější uvažovat „upravenou“ definici, podle níž součin **asociativní je**. Pro účely této přednášky není podstatné, k jaké definici se přikloníme. Prezentované definice a věty „fungují“ pro obě varianty.

Potenční množina

Definice 3.3. Potenční množina množiny A , neboli množina všech podmnožin, je definovaná vztahem

$$2^A = \{B \mid B \subseteq A\}.$$

-
- Platí například $2^{\{a,b\}} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$,
 - $2^\emptyset = \{\emptyset\}$, $2^{\{\emptyset, \{\emptyset\}\}} = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$,
 - $2^{\{a\} \times \{a,b\}} = \{\emptyset, \{(a, a)\}, \{(a, b)\}, \{(a, a), (a, b)\}\}$. □

Věta 3.4. Počet prvků potenční množiny splňuje $|2^A| = 2^{|A|}$. □

Důkaz: Stručně indukcí podle $|A|$: Pro $A = \emptyset$ platí $|2^A| = |\{\emptyset\}| = 1$.

Pro každý další prvek $b \notin A$ rozdělíme všechny podmnožiny $A \cup \{b\}$ „napolovic“ na ty neobsahující b a na ty obsahující b , tudíž

$$|2^{A \cup \{b\}}| = 2 \cdot |2^A| = 2^{|A|+1}.$$

□

3.3 Porovnávání a určení množin

Věta 3.5. Pro každé dvě množiny $A, B \subseteq M$ platí $\overline{A \cup B} = \overline{A} \cap \overline{B}$. \square

Důkaz v obou směrech rovnosti.

• $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$: \square

- * Pro $x \in M$ platí $x \in \overline{A \cup B}$, právě když $x \notin A \cup B$, neboli když zároveň $x \notin A$ a $x \notin B$.
- * To znamená $x \in \overline{A}$ a zároveň $x \in \overline{B}$, z čehož vyplývá požadované $x \in \overline{A} \cap \overline{B}$. \square

• $\overline{A \cup B} \supseteq \overline{A} \cap \overline{B}$:

- * Pro $x \in M$ platí $x \in \overline{A} \cap \overline{B}$, právě když $x \in \overline{A}$ a zároveň $x \in \overline{B}$, neboli když zároveň $x \notin A$ a $x \notin B$. \square
- * To znamená $x \notin A \cup B$, z čehož vyplývá požadované $x \in \overline{A \cup B}$.

\square

Věta 3.6. Pro každé tři množiny A, B, C platí

$$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C). \square$$

Důkaz.

- $A \setminus (B \cap C) \subseteq (A \setminus B) \cup (A \setminus C)$:
 - * Je-li $x \in A \setminus (B \cap C)$, pak $x \in A$ a zároveň $x \notin (B \cap C)$, neboli $x \notin B$ nebo $x \notin C$.
 - * Pro první možnost máme $x \in (A \setminus B)$, pro druhou $x \in (A \setminus C)$. \square
- Naopak $A \setminus (B \cap C) \supseteq (A \setminus B) \cup (A \setminus C)$:
 - * Je-li $x \in (A \setminus B) \cup (A \setminus C)$, pak $x \in (A \setminus B)$ nebo $x \in (A \setminus C)$.
 - * Pro první možnost máme $x \in A$ a zároveň $x \notin B$, z čehož plyne $x \in A$ a zároveň $x \notin (B \cap C)$, a tudíž $x \in A \setminus (B \cap C)$. \square
 - * Druhá možnost je analogická.

\square

Charakteristický vektor (pod)množiny

V případech, kdy všechny uvažované množiny jsou podmnožinami nějaké *nosné množiny* X , což není neobvyklé v programátorských aplikacích, s výhodou využijeme následující reprezentaci množin.

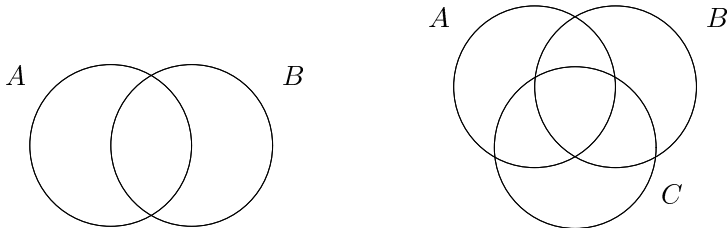
Definice: Mějme nosnou množinu $X = \{x_1, x_2, \dots, x_n\}$. Pro $A \subseteq X$ definujeme charakteristický vektor χ_A jako

$$\chi_A = (c_1, c_2, \dots, c_n), \text{ kde } c_i = 1 \text{ pro } x_i \in A \text{ a } c_i = 0 \text{ jinak. } \square$$

- Platí $A = B$ právě když $\chi_A = \chi_B$.
- Množinové operace jsou realizovány „bitovými funkcemi“
sjednocení \sim OR, průnik \sim AND, symetrický rozdíl \sim XOR.

Princip inkluze a exkluze

Tento důležitý a zajímavý kombinatorický princip je někdy také nazýván „princip zapojení a vypojení“.



Věta 3.7. Počet prvků ve sjednocení dvou či tří množin spočítáme:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \square$$

Všimněte si, že větu lze stejně tak využít k výpočtu počtu prvků v průniku množin...

Příklad 3.8. Z 1000 televizí jich při první kontrole na výrobní lince má 5 vadnou obrazovku, 10 je poškrábaných a 12 má jinou závadu. Přitom 3 televize mají současně všechny tři vady a 4 jiné jsou poškrábané a mají jinou vadu. Kolik televizí je celkem vadných? □

Řešení: Dosazením $|A| = 5$, $|B| = 10$, $|C| = 12$, $|A \cap B \cap C| = 3$, $|A \cap B| = 3 + 0$, $|A \cap C| = 3 + 0$, $|B \cap C| = 3 + 4$ do Věty 3.7 zjistíme výsledek 17. □□

Poznámka. Jen stručně, bez důkazu a bližšího vysvětlení, si uvedeme obecnou formu principu inkluze a exkluze:

$$\left| \bigcup_{j=1}^n A_j \right| = \sum_{\emptyset \neq I \subseteq \{1, \dots, n\}} (-1)^{|I|-1} \cdot \left| \bigcap_{i \in I} A_i \right|$$

(Jeho znalost nebude v předmětu vyžadována.)

3.4 Relace a funkce mezi (nad) množinami

Dalším důležitým základním „datovým typem“ matematiky jsou relace, kterým vzhledem k jejich rozsáhlému použití v informatice věnujeme zvýšenou pozornost.

Definice 3.9. Relace mezi množinami A_1, \dots, A_k , pro $k \in \mathbb{N}$, je **libovolná** podmnožina kartézského součinu

$$R \subseteq A_1 \times \dots \times A_k. \square$$

Pokud $A_1 = \dots = A_k = A$, hovoříme o **k -ární relaci R na A** . \square

Příklady relací.

- $\{(1, a), (2, a)\}$ je relace mezi $\{1, 2, 3\}$ a $\{a, b\}$.
- $\{(i, 2i) \mid i \in \mathbb{N}\}$ je binární relace na \mathbb{N} . \square
- $\{(i, j, i + j) \mid i, j \in \mathbb{N}\}$ je ternární relace na \mathbb{N} .
- $\{3i \mid i \in \mathbb{N}\}$ je unární relace na \mathbb{N} . \square
- Jaký význam vlastně mají unární a nulární relace na A ?

Funkce mezi množinami

Definice 3.10. (Totální) funkce z množiny A do množiny B je relace f mezi A a B taková, že pro každé $x \in A$ existuje **právě jedno** $y \in B$ takové, že $(x, y) \in f$. \square

Množina A se nazývá **definiční obor** a množina B **obor hodnot** funkce f .

Neformálně řečeno, ve funkci f je každé „vstupní“ hodnotě x přiřazena **jednoznačně** „výstupní“ hodnota y .

(V obecné relaci počty „přiřazených“ dvojic neomezujeme. . .) \square

Značení: Místo $(x, y) \in f$ píšeme obvykle $f(x) = y$.

Zápis $f : A \rightarrow B$ říká, že f je funkce s def. oborem A a oborem hodnot B . \square

Funkcím se také říká **zobrazení**.

- Definujeme funkci $f : \mathbb{N} \rightarrow \mathbb{N}$ předpisem $f(x) = x + 8$. Tj. $f = \{(x, x + 8) \mid x \in \mathbb{N}\}$. \square
- Definujeme funkci $plus : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ předpisem $plus(i, j) = i + j$. Tj. $plus = \{(i, j, i + j) \mid i, j \in \mathbb{N}\}$.

Definice: Pokud naši definici funkce upravíme tak, že požadujeme pro každé $x \in A$ **nejvýše jedno** $y \in B$ takové, že $(x, y) \in f$, obdržíme definici **parciální funkce** z A do B . \square

V parciální funkci p nemusí být pro některé „vstupní“ hodnoty x funkční hodnota definována.

Pro **nedefinovanou** hodnotu používáme znak \perp . \square

Další příklady funkcí.

- Definujeme parciální funkci $f : \mathbb{Z} \rightarrow \mathbb{N}$ předpisem

$$f(x) = \begin{cases} 3 + x & \text{jestliže } x \geq 0, \\ \perp & \text{jinak.} \end{cases}$$

Tj. $f = \{(x, 3 + x) \mid x \in \mathbb{N}\}$. \square

- Také funkce $f : \mathbb{R} \rightarrow \mathbb{R}$ daná běžným analytickým předpisem

$$f(x) = \sqrt{x}$$

je jen parciální – není definována pro $x < 0$. \square

- Co je relace, přiřazující lidem v ČR jejich rodná čísla?

3.5 Posloupnosti a rekurentní vztahy

Definice: Funkce $p : \mathbb{N} \rightarrow \mathbb{R}$ se nazývá *posloupnost*.

Mimo „funkčního“ zápisu $p(n)$ často používáme „indexovou“ formu zápisu p_n . □

Poznámka: Obor hodnot posloupnosti může být i **jiný než reálná** čísla. Na posloupnost se také díváme jako na „seřazení“ vybraných prvků z oboru hodnot, s povoleným opakováním hodnot (nemusí být prostá). □

Také def. obor posl. může začínat od nuly nebo i od jedničky, jak je v aplikacích potřeba.

- Příklady posloupností:

- * $p_0 = 0, p_1 = 2, \dots, p_i = 2i, \dots$ je posloupnost sudých nezáporných čísel. □

- * $3, 3.1, 3.14, 3.141, \dots$ je posloupnost postupných dekadických rozvoju π .

- * $1, -1, 1, -1, \dots$ je posloupnost určená vztahem $p_i = (-1)^i, i \geq 0$. □

- * Pokud chceme stejnou posloupnost $1, -1, 1, -1, \dots$ zadat jako $q_i, i \geq 1$, tak ji určíme vzorcem $q_i = (-1)^{i-1}$. □

- Posloupnost je *rostoucí* či *klesající*, pokud $p_{n+1} > p_n$ či $p_{n+1} < p_n$ pro všechna n .

Rekurentní definice posloupnosti

Slovem *rekurentní* označujeme takové definice (či popisy), které se v jistých bodech odvolávají samy na sebe.

(Už jste se setkali s „rekurzí“ při programování? A víte, co znamená?) □

Ukázky **rekurentních vztahů**:

- Zadáme-li posloupnost p_n vztahy $p_0 = 1$ a $p_n = 2p_{n-1}$ pro $n > 0$, pak platí $p_n = 2^n$ pro všechna n . □
- Obdobně můžeme zadat posloupnost q_n vztahy $q_1 = 1$ a $q_n = q_{n-1} + n$ pro $n > 1$. Potom platí $q_n = \frac{1}{2}n(n+1)$ pro všechna n .
Uměli byste toto dokázat indukcí? □
- Známa Fibonacciho posloupnost je zadaná vztahy $f_1 = f_2 = 1$ a $f_n = f_{n-1} + f_{n-2}$ pro $n > 2$.