Algebra a diskrétna matematika
Prehľad z 9. prednášky
Algebraické štruktúry - Úvod

Binárna relácia

Nech M je neprázdna množina a nech $M \times M$ je **kartézsky súčin** množiny M samej so sebou, t.j. $M \times M = \{(x,y); x,y \in M\}$.

Pod **binárnou reláciou** na množine M rozumieme ľubovoľnú podmnožinu súčinu $M \times M$. Formálne, $\mathcal{R}$ je binárna relácia na M, ak $\mathcal{R} \subseteq M \times M$.

Vzťah medzi x a y v relácii $\mathcal{R}$ zapisujeme $(x,y) \in \mathcal{R}$ alebo $x\mathcal{R}y$.

Ak M má veľkosť n, body v relácii môžeme znázorniť vyznačením zodpovedajúcich bodov na mriežke $n \times n$ alebo pomocou orientovaného grafu s n vrcholmi, v ktorom je dvojica bodov $x\mathcal{R}y$ reprezetovaná šípkou z x do y. Reláciu na n prvkovej množine $M = \{x_1, x_2, \ldots, x_n\}$ je tiež možné popísať pomocou *matice susednosti* A relácie $\mathcal{R}$, pričom $A_{n\times n} = (a_{ij})$, kde $a_{ij} = 1$, ak $x_i\mathcal{R}x_j$, inak $a_{ij} = 0$.

<u>Príklad 1</u>: Ilustrácia binárnych relácií na daných množinách.
a) $M = \{0,1,2\}$, $\mathcal{R} = \{(0,0),(1,0),(1,1),(1,2),(2,0),(2,2)\}$.
b) $M = \{a,b,c,d,e\}$, $\mathcal{R} = \{(a,b),(a,c),(b,b),(c,d),(e,b),(e,e)\}$
c) $M = \mathbb{Z}$, $\mathcal{R} = \{(z, z+9); z \in \mathbb{Z}\}$.
d) $\mathcal{R}$ na $\mathbb{R}$: $\quad x\mathcal{R}y \Leftrightarrow y = x^3 - x$

<u>Poznámka:</u> Funkcia je špeciálnym typom relácie.

Vlastnosti binárnej relácie

Hovoríme, že relácia $\mathcal{R}$ je na množine M

(R) **reflexívna**, ak pre každé $x \in M$ platí $x\mathcal{R}x$

(S) **symetrická**, ak $x\mathcal{R}y$ implikuje $y\mathcal{R}x$ pre každé $x,y \in M$

(A) **antisymetrická**, ak $x\mathcal{R}y$ a $y\mathcal{R}x$ implikuje $x = y$ pre každé $x,y \in M$

(T) **tranzitívna**, ak $x\mathcal{R}y$ a $y\mathcal{R}$z implikuje $x\mathcal{R}z$ pre každé $x,y,z \in M$

Príklad 2: Overte vlastnosti relácií na daných množinách

a) $M = \{0,1,2\}$, $\mathcal{R} = \{(0,0),(1,0),(1,1),(1,2),(2,0),(2,2)\}$

b) $\mathcal{R}$ na $\mathbb{R}$: $x\mathcal{R}y \Leftrightarrow |x-y| \geq 6$

c) $\mathcal{R}$ na $\mathbb{Z}$: $x\mathcal{R}y \Leftrightarrow x \leq y$

d) M je množina všetkých priamok v rovine a $\mathcal{R}$ je relácia rovnobežnosti priamok, t. j. $\forall\, p,q \in M;\ p\mathcal{R}q \ \Leftrightarrow\ p \,||\, q$

Odpoveď:

a) (R), (A), (T)
b) (S)
c) (R), (A), (T)
d) (R), (S), (T)

Čiastočne usporiadaná množina (poset)

Binárna relácia $\mathcal{R} \subseteq M \times M$ sa nazýva **čiastočným usporiadaním** na M, ak je na M *reflexívna, antisymetrická* a *tranzitívna.*

Ak $\mathcal{R}$ je čiastočné usporiadanie na M, tak namiesto $x\mathcal{R}y$ používame označenie $x \preceq_{\mathcal{R}} y$ alebo sa index $\mathcal{R}$ vynecháva.

Často sa jednoducho píše $x \leq y$.

Vlastnosti z definície čiastočného usporiadania potom majú tvar

(R) $x \leq x$ (reflexívnosť)

(A) ak $x \leq y$ a $y \leq x$, tak $x = y$ (antisymetria)

(T) ak $x \leq y$ a $y \leq z$, tak $x \leq z$ (tranzitívnosť)

pre každé $x, y, z \in M$.

Dvojicu $(M, \leq)$, kde $\leq$ je binárna relácia čiastočného usporiadania, nazývame **čiastočne usporiadaná množina**.

Príklad 3: Nech S je neprázdna množina a nech M je ľubovoľná množina *podmnožín* množiny S. Nech $\leq$ je binárna relácia inklúzie, t.j. ak $X, Y \in M$, tak $X \leq Y$, ak X je podmnožinou množiny Y. Potom $(M, \leq)$ je čiastočne usporiadaná množina.

Príklad 4: Nech M je ľubovoľná neprázdna podmnožina množiny $\mathbb{N}$ a nech pre každé $x, y \in M$ symbol $x \leq y$ označuje fakt, že číslo x je deliteľom čísla y. Potom $(M, \leq)$ je opäť čiastočne usporiadaná množina.

Ak $(M, \leq)$ je čiastočne usporiadaná množina, tak dva rôzne prvky $x, y \in M$ sú **porovnateľné**, ak buď $x \leq y$, alebo $y \leq x$.

(Oba vzťahy nemôžu platiť súčasne pre $x \neq y$.)

Budeme písať $x < y$, ak $x \leq y$ a $x \neq y$.

- Prvok $a \in M$ sa nazýva **najmenší**, ak $a \leq x$ pre každé $x \in M$.
- Prvok $b \in M$ sa nazýva **najväčší**, ak $x \leq b$ pre *každé* $x \in M$.
- Prvok $a \in M$ je **minimálny**, ak neexistuje žiadne $x \in M$, že $x < a$.
- Prvok $b \in M$ je **maximálny**, ak neexistuje žiadne $x \in M$, že $b < x$.

Ak v $(M, \leq)$ existuje najmenší (najväčší) prvok, tak tento je určený *jednoznačne*.

Najmenší (najväčší) prvok v $(M, \leq)$ je zároveň minimálnym (maximálnym) prvkom; vo všeobecnosti to neplatí obrátene.

Ak $(M, \leq)$ obsahuje viac ako jeden minimálny (maximálny) prvok, tak žiadne dva minimálne (maximálne) prvky nemôžu byť porovnateľné.

Príklad 5: Pre čiastočne usporiadanú množinu $(\{1, 2, \ldots, 10\}, |)$, kde $x \mid y$ označuje fakt, že x delí y, nájdite všetky minimálne a maximálne prvky, najmenší a najväčší prvok.

Odpoveď: Najmenší a zároveň minimálny prvok je 1, maximálne prvky sú $6, 7, 8, 9, 10$ a najväčší prvok neexistuje.

Čiastočne usporiadané množiny znázorňuje pomocou **Hasseho diagramu**.

V Hasseho diagrame čiastočne usporiadanej množiny $(M, \leq)$:

- sa nevyskytujú slučky,
- spojnica je medzi x, y iba ak x je bezprostredným predchodcom prvku y, t.j. $x < y$ a neexistuje žiadne $z \in M$, že $x < z < y$,
- ak $x < y$, tak x sa umiestňuje pod y.

Z Hasseho diagramu je možné jednoznačne zrekonštruovať reláciu $\leq$ čiastočného uporiadania na množine M.

Zväzy

Nech $(M, \leq)$ je čiastočne usporiadaná množina a nech $x, y \in M$.

- Prvok $z \in M$ je **dolným ohraničením** prvkov x a y, ak $z \leq x$ a $z \leq y$.
- Prvok $c \in M$ je **najväčším dolným ohraničením** prvkov x a y, ak $c \leq x$, $c \leq y$, a ak $z \leq c$ pre každé dolné ohraničenie z prvkov x, y.

  Označenie: $c = \inf(x, y)$, alebo $c = x \wedge y$, *priesek* x a y.

- Prvok $z \in M$ je **horným ohraničením** prvkov x a y, ak $x \leq z$ a $y \leq z$.
- Prvok $d \in M$ je **najmenším horným ohraničením** prvkov x a y, ak $x \leq d$, $y \leq d$, a ak $d \leq z$ pre každé horné ohraničenie z prvkov x, y.

  Označenie: $d = \sup(x, y)$, alebo $d = x \vee y$, *spojenie* prvkov x a y.

Čiastočne usporiadaná množina $(M, \leq)$ sa nazýva **zväz**, ak pre každé $x, y \in M$ existuje ich priesek $x \wedge y$ a aj ich spojenie $x \vee y$.

Príklad 6: Nech $M = \{0, 1, 2\} \times \{0, 1\}$ a relácia usporiadania $\leq$ je daná predpisom $(a, b) \leq (c, d) \Leftrightarrow a \leq c$ a $b \leq d$. Dvojica $(M, \leq)$ tvorí zväz.

Príklad 7: Nech $(\mathbb{N}, |)$ je čiastočne usporiadaná množina, kde $\mathbb{N}$ je množina prirodzených čísiel a $x \mid y$ označuje fakt, že x delí y. Potom $x \wedge y$ je najväčší spoločný deliteľ a $x \vee y$ je najmenší spoločný násobok čísiel x a y; čiastočne usporiadaná množina $(\mathbb{N}, |)$ je tiež zväz.

Príklad 8: Nech S je neprázdna množina a nech 2^S označuje množinu *všetkých* podmnožín množiny S. V čiastočne usporiadanej množine $(2^S, \subseteq)$ je priesek dvoch prvkov rovný prieniku a spojenie je rovné zjednoteniu príslušných množín a teda $(2^S, \subseteq)$ je zväz.
Takéto zväzy sa nazývajú **boolovské**.

Čiastočne usporiadaná množina $(M, \leq)$ sa nazýva **reťazec**, ak pre každé $x, y \in M$ platí, že $x \leq y$ alebo $y \leq x$; skrátene, ak každé dva prvky v M sú *porovnateľné*.

Príslušné čiastočné usporiadanie $\leq$ sa nazýva aj **lineárne**.

Tvrdenie 1: Každý reťazec je zväz.

Príklad 9: Dané čiastočne usporiadané množiny sú reťazce.
a) $(\{1,2,3,4,5,6\},\leq)$
b) $M=\{1,2,3,4\}$, $\mathcal{R}=\{(2,3),(2,1),(1,4),(1,3),(2,4),(4,3)\}$

Binárna operácia a algebraická štruktúra

Binárna operácia je "dvojčlenná" operácia, ktorá každej usporiadanej dvojici prvkov z nejakej množiny priraďuje jediný tretí prvok z tej istej množiny; t. j. binárna operácia φ na množine M je zobrazenie $\varphi: M\times M\to M$.

Z faktu, že φ je zobrazenie vyplýva, že

- každá binárna operácia je *uzavretá*; t. j. $\forall x,y\in M:\varphi(x,y)\in M$,
- výsledok operácie je definovaný pre *každú* usporiadanú dvojicu z $M\times M$, t. j. $\forall x,y\in M\ \exists z\in M:\varphi(x,y)=z$.

Známe príklady:

Číselné operácie: sčítanie, odčítanie, násobenie, max, min.

Množinové operácie: prienik, zjednotenie, rozdiel.

Označenie: Ak sa nejedná o známe operácie, najčastejšie používané označenie binárnej operácie je $*$, $\circ,\oplus$ alebo $\otimes$; píšeme $x*y, x\circ y$ atď.

Vlastnosti binárnych operácií

Nech $*$ je binárna operácia na množine M. Hovoríme, že operácia $*$ je

- **komutatívna**, ak $\forall x,y\in M: x*y=y*x$
- **asociatívna**, ak $\forall x,y,z\in M:(x*y)*z=x*(y*z)$

Nech $*,\circ$ sú dve binárne operácie na M. Hovoríme, že

- operácia $*$ je **zľava distributívna** vzhľadom na operáciu $\circ$, ak $\forall x,y,z\in M: x*(y\circ z)=(x*y)\circ(x*z)$,

- operácia $*$ je **sprava distributívna** vzhľadom na operáciu $\circ$, ak $\forall x, y, z \in M : (x \circ y) * z = (x * z) \circ (y * z)$,

- operácia $*$ je **distributívna** vzhľadom na operáciu $\circ$, ak je vzhľadom na $\circ$ distributívna zľava aj sprava.

Neprázdna množina M spolu s jednou alebo viacerými binárnymi operáciami tvorí **algebraickú štruktúru**.

Rozoznávame veľa rôznych algebraických štruktúr podľa toho, aké vlastnosti spĺňajú ich binárne operácie.

Zväz ako algebraická štruktúra

V každom zväze $(M, \leq)$ pre všetky $x, y, z \in M$ platia nasledujúce vzťahy:

$$
\begin{array}{lrcllrcl}
(1) & x \wedge x & = & x & \quad & x \vee x & = & x \\
(2) & x \wedge y & = & y \wedge x & & x \vee y & = & y \vee x \\
(3) & (x \wedge y) \wedge z & = & x \wedge (y \wedge z) & & (x \vee y) \vee z & = & x \vee (y \vee z) \\
(4) & (x \wedge y) \vee y & = & y & & (x \vee y) \wedge y & = & y \\
(5) & x \leq y & \Leftrightarrow & x \wedge y = x & & x \leq y & \Leftrightarrow & x \vee y = y
\end{array}
$$

Dá sa ukázať, že na zväz $(M, \leq)$ je ekvivalentne možné hľadieť aj ako na *algebraickú štruktúru* $(M, \wedge, \vee)$ s dvoma binárnymi operáciami $\wedge$ a $\vee$: $M \times M \to M$, ktoré majú vlastnosti (1) – (4).

Príslušné čiastočné usporiadanie je potom definované vzťahom (5).

Načrtneme fakt, že ak $(M, \wedge, \vee)$ je algebraická štruktúra spĺňajúca (1) – (4), tak predpisom (5) je naozaj definované čiastočné usporiadanie.

- Na odvodenie (R) treba ukázať, že $x \leq x$, čiže treba overiť, že $x \wedge x = x$, ale to je vzťah (1).

- Na odvodenie (A) predpokladajme, že $x \leq y$ a $y \leq x$, teda $x \wedge y = x$ a $y \wedge x = y$; potom ale z (2) máme $x = y$, čím dostávame (A).

- Na odvodenie (T) predpokladajme, že $x \leq y$ a $y \leq z$, teda $x \wedge y = x$ a $y \wedge z = y$. Z vlastnosti (3) máme $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$, ale $x \wedge z = x$ znamená, že $x \leq z$, z čoho vyplýva (T).

Ďalšie vlastnosti zväzu

Z faktu, že $(M, \leq)$ je zväz, je možné odvodiť mnoho ďalších nerovností a vlastností. Uvedieme tu tri dôležité príklady:

Vo zväze $(M, \leq)$ pre všetky $x, y, z, w \in M$ platí

(I) $x \leq y$ a $z \leq w$ implikuje $x \wedge z \leq y \wedge w$ a $x \vee z \leq y \vee w$
(izotónnosť)

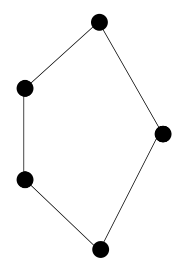
(D) $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$, $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$
(distributívne nerovnosti)

(M) $x \leq z$ implikuje $x \vee (y \wedge z) \leq (x \vee y) \wedge z$
(modulárna nerovnosť)

Modulárny a distributívny zväz

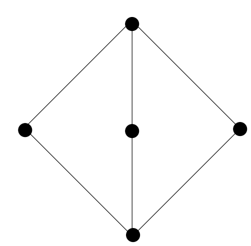
Zväz $(M, \leq)$ sa nazýva **distributívny**, ak platia rovnosti v (D),
a **modulárny**, ak platí rovnosť v (M).

<u>Príklad 10</u>: Najmenší nemodulárny zväz je "pentagon".



Tvrdenie 2: Zväz je modulárny práve vtedy, keď neobsahuje podzväz izomorfný s pentagonom.

<u>Príklad 11</u>: Najmenší modulárny nedistributívny zväz je "diamant".



Tvrdenie 3: Modulárny zväz je distributívny práve vtedy, keď neobsahuje podzväz izomorfný s diamantom.