

Diskretne strukture

Gašper Fijavž

Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

6. november 2025

Moč končnih množic

Naj bo A končna množica. Potem $|A|$ označuje *število elementov* ali *moč* množice A .

Naj bosta A in B končni množici. Pravimo, da sta A in B *enako močni*, $A \sim B$, če $|A| = |B|$.

Zgledi:

1. $|\emptyset| = 0$
2. $|\{0, 1\}| = 2$
3. $|\{\{0, 1\}\}| = 1$

Moč končnih množic

Trditev

Naj bodo A, B, C končne množice.

1. $|A \times B| = |A| \cdot |B|$
2. $|\{f ; f : A \rightarrow B\}| = |B^A| = |B|^{|A|}$
3. $|\mathcal{P}A| = 2^{|A|}$
4. Če je $B \subseteq A$, potem je $|A \setminus B| = |A| - |B|$.
V splošnem je $|A \setminus B| = |A| - |A \cap B|$.
5. Če je $A \cap B = \emptyset$, potem je $|A \cup B| = |A| + |B|$.
V splošnem je $|A \cup B| = |A| + |B| - |A \cap B|$.
6. $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

Načelo vključitev in izključitev

Izrek

Naj bo A končna množica in $A_1, A_2, \dots, A_n \subseteq A$. Potem je

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= \\ & \quad |A_1| + |A_2| + \dots + |A_n| \\ & \quad - |A_1 \cap A_2| - |A_1 \cap A_3| - \dots - |A_{n-1} \cap A_n| \\ & \quad + \dots \\ & \quad \dots \\ & \quad + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n| \\ &= \sum_{i=0}^n (-1)^i S_i, \end{aligned}$$

$$\text{kjer je } S_k = \sum_{\substack{\mathcal{J} \subseteq \{1, \dots, n\} \\ |\mathcal{J}|=k}} \left| \bigcap_{i \in \mathcal{J}} A_i \right|.$$

Nalogi

Naloga: Koliko je števil na celoštevilskem intervalu $[1 \dots 96]$, ki so deljiva s 6 in niso deljiva niti s 24 niti z 32?

Naloga: Zaposleni v nekem podjetju programirajo v treh jezikih: Java, C in Python. V vsakem jeziku programira tri petine programerjev, v C in Pythonu dve petini, v C-ju in Javi tri desetine ter v jezikih Java in Python ena petina. V vseh treh jezikih programira 10 programerjev.
Koliko programerjev je zaposlenih v podjetju?
Koliko jih programira v natanko dveh jezikih?

Kaj je relacija

Množica R je *(dvomestna) relacija*, če je vsak njen element urejen par.

$$R \text{ je relacija.} \iff \forall x \in R \exists u, v : x = (u, v)$$

Množica R je *(dvomestna) relacija v množici* A , če je $R \subseteq A \times A$.

Zgledi

1. $A = \{e, f, g, h\} \quad R = \{(e, f), (f, g), (g, h)\}$

2. $A = \mathbb{N} \quad R = \{(x, y) ; x, y \in \mathbb{N} \wedge x \leq y\}$

3. $\text{id}_A = \{(x, x) ; x \in A\}$

4. $\emptyset \subseteq A \times A$

5. $A \times A \subseteq A \times A$

Namesto $(x, y) \in R$ pišemo xRy .

Domena in zaloga vrednosti

Naj bo R relacija v A .

$\mathcal{D}_R = \{x ; \exists y : xRy\}$ *domena* ali *definicijsko območje* relacije R .

$\mathcal{Z}_R = \{y ; \exists x : xRy\}$ *zaloga vrednosti* relacije R .

Lastnosti relacij

Naj bo R relacija v A . Pravimo, da je

1. R *refleksivna* $\iff \forall x \in A : xRx$
2. R *simetrična* $\iff \forall x, y \in A : xRy \Rightarrow yRx$
3. R *antisimetrična* $\iff \forall x, y \in A : xRy \wedge yRx \Rightarrow x = y$
4. R *tranzitivna* $\iff \forall x, y, z \in A : xRy \wedge yRz \Rightarrow xRz$
5. R *sovisna* $\iff \forall x, y \in A : x \neq y \Rightarrow xRy \vee yRx$
6. R *enolična* $\iff \forall x, y, z \in A : xRy \wedge xRz \Rightarrow y = z$

Zgledi

1. Relacija id_A v A
2. Relacija $\leq$ v $\mathbb{N}$
3. Relacija $<$ v $\mathbb{N}$
4. Relacija $\subseteq$ v $\mathcal{P}A$
5. Relacija "oče" v množici ljudi (x oče y preberemo kot x je oče y -ona.)

Grafična predstavitev relacije

R naj bo relacija v *končni* množici A .

Elemente množice A narišemo kot *točke* v ravnini. Če velja aRb , narišemo usmerjeno puščico od a do b .

elementi A ... točke v ravnini

aRb ... usmerjena puščica od a do b .

Zgled: $A = \{e, f, g, h\}$ $R = \{(e, f), (f, g), (g, h)\}$

Operacije z relacijami

Relacije so posebne vrste množic. Vemo, kako so definirane operacije $\cup$, $\cap$ in $\setminus$.

Ponavadi se pogovarjamo o družini relacij na isti množici A . V takem primeru je *komplement* smiselno definirati kot

$$R^c := (A \times A) \setminus R = U_A \setminus R$$

Operacije z relacijami

Poleg navedenih operacij definiramo tudi:

- ▶ *inverzna relacija* relacije R , označimo jo z R^{-1} :

$$R^{-1} := \{(y, x) ; (x, y) \in R\}$$

- ▶ *produkt relacij* R in S , označimo ga z $R * S$:

$$R * S := \{(x, z) ; \exists y (xRy \wedge ySz)\}$$

Operacije z relacijami

Zgled: sorodstvene relacije med ljudmi

Relacija *oče* v množici ljudi je definirana kot

$$x \text{ oče } y \Leftrightarrow x \text{ je oče } y\text{-ona}.$$

Naloga: Izrazi relacije *roditelj*, *zet*, *snaha*, *ded*, *vnuk*, *tašča*, *svak* z “bolj elementarnimi” sorodstvenimi relacijami *oče*, *mati*, *sin*, *hči*, *mož*, *žena*, ...

Lastnosti operacij z relacijami

Naj bodo R, S, T relacije na A .

1. $(R^{-1})^{-1} = R$
2. $(R * S)^{-1} = S^{-1} * R^{-1}$
3. $(R * S) * T = R * (S * T) =: R * S * T$
4. $R * (S \cup T) = R * S \cup R * T$
5. $(R \cup S) * T = R * T \cup S * T$
6. $R * \text{id}_A = \text{id}_A * R = R$
7. $R \subseteq S \implies R * T \subseteq S * T$ in $T * R \subseteq T * S$

Potence relacij

Zaradi asociativnosti množenja relacij lahko definiramo potence relacij. Naj bo $R \subseteq A \times A$.

$$\begin{aligned} R^0 &:= \text{id}_A \\ R^{n+1} &:= R^n * R, \text{ če je } n \geq 0. \end{aligned}$$

Velja $R^1 = R$, $R^2 = R * R$, ter za $m, n \geq 0$ tudi $R^m * R^n = R^{m+n}$.

Potence relacij

Definiramo lahko tudi potence z negativnimi eksponenti, če je $n > 0$, potem

$$R^{-n} := (R^{-1})^n$$

Toda če sta m in n celi števili različnih predznakov, potem $R^n * R^m$ ni nujno enako R^{m+n} .

Potence relacij

Zgled: sorodstvene relacije med ljudmi

Naloga: Definiraj relacije *prednik*, *potomec*, *sorodnik*.

Potence relacij

Naj bo R relacija v A .

Relacijo R^+ imenujemo *tranzitivna ovojnica* relacije R in jo definiramo s predpisom

$$R^+ = \bigcup_{k=1}^{\infty} R^k$$

Relacijo R^* imenujemo *tranzitivno-refleksivna ovojnica* relacije R in jo definiramo s predpisom

$$R^* = \bigcup_{k=0}^{\infty} R^k$$

Vprašanje: Kako s pomočjo grafa relacije R opišemo grafa relacij R^+ in R^* ?

Algebraična karakterizacija lastnosti relacij

Naj bo R relacija v A . Relacija R je

1. *refleksivna* $\iff \text{id}_A \subseteq R$
2. *simetrična* $\iff R^{-1} = R$
3. *antisimetrična* $\iff R^{-1} \cap R \subseteq \text{id}_A$
4. *tranzitivna* $\iff R^2 \subseteq R$
5. *sovisna* $\iff \text{id}_A \cup R \cup R^{-1} = U_A$
6. *enolična* $\iff R^{-1} * R \subseteq \text{id}_A$

Preslikave

Relacija $f \subseteq A \times B$ je *preslikava iz A v B*, če velja:

- ▶ f je enolična
- ▶ $\mathcal{D}_f = A$
- ▶ $(\mathcal{Z}_f \subseteq B)$

Pišemo tudi $f : A \rightarrow B$.

Preslikave

Namesto $x f y$ pišemo $y = f(x)$,

in pravimo, da f *(pre)slika* x v y ,

x je *argument*, y pa *vrednost* preslikave f pri x .

Tudi: y je *slika* x -a.

Preslikave

Naj bo f preslikava iz A v B .

- ▶ $A = \mathcal{D}_f$... domena ali definicijsko območje f
- ▶ $\mathcal{Z}_f$... zaloga vrednosti f
- ▶ B ... kodomena f

Preslikave

Zgled: Naj bo X množica nepraznih bitnih besed

$\{0, 1, 00, 01, 10, 11, 000, 001, \dots\}$ in Y množica naravnih števil $\{0, 1, 2, 3, \dots\}$.

Definirajmo relacije $f_1, f_2, f_3 \subseteq X \times Y$, $f_4 \subseteq X \times X$ in $f_5 \subseteq Y \times X$ z naslednjimi opisi:

- ▶ $x f_1 y$ natanko tedaj, ko je y število enic v x -u.
- ▶ $x f_2 y$ natanko tedaj, ko je y prvi bit niza x .
- ▶ $x f_3 y$ natanko tedaj, ko je y mesto najbolj leve ničle v x -u.
- ▶ $x_1 f_4 x_2$ natanko tedaj, ko x_2 dobimo tako, da nizu x_1 dodamo na koncu 0 ali 1.
- ▶ $y f_5 x$ natanko tedaj, ko je x niz y zaporednih enic.

Katere izmed relacij f_1, f_2, f_3, f_4, f_5 so preslikave?

Lastnosti preslikav

Naj bo $f : A \rightarrow B$. Pravimo, da je

- ▶ f *injektivna*, če $\forall x, y \in A : (f(x) = f(y) \Rightarrow x = y)$
- ▶ f *surjektivna*, če $Z_f = B$ (pravimo tudi, da je f preslikava iz A **na** B)
- ▶ f *bijektivna*, če je injektivna in surjektivna.

Zgledi preslikav

1. $\text{id}_A : A \rightarrow A$, *identiteta na A*
 $\text{id}_A(x) = x$, je bijektivna
2. $p_i : A_1 \times \cdots \times A_n \rightarrow A_i$, *projekcija na i-to komponento*
 $p_i((a_1, \dots, a_n)) = a_i$, je surjektivna
3. $A_1 \subseteq A$, $i = \text{id}_A|_{A_1}$
 $i : A_1 \hookrightarrow A$, $i(x) = x$ je injektivna, *vložitev* A_1 v A
4. $A \subseteq B$, $\chi_A : B \rightarrow \{0, 1\}$
$$\chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases},$$
karakteristična funkcija množice A (v B)

Inverzna preslikava

Vprašanje: Kdaj je f^{-1} tudi preslikava?

Trditev

$f : A \rightarrow B$

1. f^{-1} je enolična natanko tedaj, ko je f injektivna,
2. $f^{-1} : B \rightarrow A$ natanko tedaj, ko je f bijektivna.

Kompozitum preslikav

Naj bosta $g : A \rightarrow B$ in $f : B \rightarrow C$. Potem je $f \circ g$ preslikava iz A v C določena s predpisom

$$f \circ g = g * f.$$

Velja $(f \circ g)(a) = f(g(a))$ za vse $a \in A$.

Trditev

Kompozitum preslikav je asociativna operacija, velja namreč:

$$(f \circ g) \circ h = f \circ (g \circ h).$$

Lastnosti kompozituma

Trditev

Naj bo $f : A \rightarrow B$. Potem je

$$f \circ \text{id}_A = \text{id}_B \circ f = f$$

Trditev

$f : B \rightarrow C, g : A \rightarrow B$

1. f, g injektivni $\implies f \circ g$ injektivna
2. f, g surjektivni $\implies f \circ g$ surjektivna
3. $f \circ g$ injektivna $\implies g$ injektivna
4. $f \circ g$ surjektivna $\implies f$ surjektivna

Lastnosti kompozituma

Trditev

Naj bo $f : B \rightarrow A, g : A \rightarrow B$. Če je $f \circ g = \text{id}_A$ in $g \circ f = \text{id}_B$, potem sta f in g bijekciji in je $g = f^{-1}$.

Dirichletov princip

Izrek

Naj bo A končna množica in $f : A \rightarrow A$. Potem so naslednje trditve enakovredne:

- ▶ f je injektivna.
- ▶ f je surjektivna.
- ▶ f je bijektivna.

Ekvivalenčna relacija

$R \subseteq A \times A$ je *ekvivalenčna*, če je

- ▶ refleksivna,
- ▶ simetrična in
- ▶ tranzitivna.

Ekvivalenčna relacija

Zgledi:

1. Relacija $\parallel$ vzporednosti v množici vseh premic v ravnini.
2. $A = \{\text{ljudje}\}$, $xRy \iff x$ ima enako barvo oči kot y .
3. $f : A \rightarrow B$, $x, y \in A : xR_f y \iff f(x) = f(y)$
 x in y imata isto funkcijsko vrednost.
4. Naj bo $m \in \mathbb{N}$, $m \geq 2$. Definirajmo relacijo R v množici $\mathbb{Z}$:

$$xRy \iff m \text{ deli } |x - y|$$

Ekvivalenčni razredi

Naj bo $R \subseteq A \times A$ ekvivalenčna in $x \in A$.

$R[x] = \{y \in A ; yRx\}$ je *ekvivalenčni razred* elementa x .

$A/R = \{R[x] ; x \in A\}$ (množica vseh ekvivalenčnih razredov) je *faktorska (kvocientna) množica* množice A po relaciji R .

Ekvivalenčni razredi, razbitje

Trditev

Naj bo R ekvivalenčna relacija na A . Potem za poljubna $x, y \in A$ velja

$$R[x] = R[y] \iff xRy$$

Izrek

Naj bo R ekvivalenčna relacija na A . Potem je A/R razbitje množice A .

Zgledi faktorskih množic

- ▶ “premise v ravnini” / “vzporedne premise” =
 $\{\{\text{navpične pr.}\}, \{\text{vodoravne pr.}\}, \{\text{pr. pod kotom } 45^\circ\}, \dots\} \cong$
“množica vseh smeri v ravnini” $\cong [-\pi/2, \pi/2)$

