Diskretne strukture

Deveti sklop izročkov

Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

2. december 2021

Lastnosti operacij z relacijami

Naj bodo R, S, T relacije na A.

- $(R^{-1})^{-1} = R$.
- $(R * S)^{-1} = S^{-1} * R^{-1}$.

  Dokaz.

$$\begin{aligned}(x,y) \in (R*S)^{-1} &\Leftrightarrow (y,x) \in R*S \\ &\Leftrightarrow \exists z \in A : (y,z) \in R \wedge (z,x) \in S \\ &\Leftrightarrow \exists z \in A : (z,y) \in R^{-1} \wedge (x,z) \in S^{-1} \\ &\Leftrightarrow \exists z \in A : (x,z) \in S^{-1} \wedge (z,y) \in R^{-1} \\ &\Leftrightarrow (x,y) \in S^{-1} * R^{-1}.\end{aligned}$$

- $(R * S) * T = R * (S * T) =: R * S * T$. Produkt relacij je *asociativen*.
- $R * (S \cup T) = R * S \cup R * T$. Produkt je *distributiven nad* $\cup$ v drugem faktorju.

  Dokaz.

$$\begin{aligned}(x,y) \in R*(S\cup T) &\Leftrightarrow \exists z \in A : (x,z) \in R \wedge (z,y) \in S \cup T \\ &\Leftrightarrow \exists z \in A : (x,z) \in R \wedge ((z,y) \in S \vee (z,y) \in T) \\ &\Leftrightarrow \exists z \in A : ((x,z) \in R \wedge (z,y) \in S) \vee ((x,z) \in R \wedge (z,y) \in T) \\ &\Leftrightarrow (x,y) \in R*S \vee (x,y) \in R*T \\ &\Leftrightarrow (x,y) \in R*S \cup R*T.\end{aligned}$$

- $(R \cup S) * T = R * T \cup S * T$. Produkt je *distributiven nad* $\cup$ v prvem faktorju.

- $R * \mathrm{id}_A = \mathrm{id}_A * R = R$.
- $R \subseteq S \implies R * T \subseteq S * T$ in $T * R \subseteq T * S$.

Produkt relacij *ni distributiven nad* $\cap$, tj.

$$R * (S \cap T) \neq R * S \cap R * T.$$

Primer

Naj bo $A = \{a, b\}$ *in*

$$R = \{(a, a), (a, b)\}, \quad S = \{(a, b)\} \quad \textit{in} \quad T = \{(b, b)\}.$$

Velja

$$R * S = \{(a, b)\} = R * T$$
$$R * (T \cap S) = R * \emptyset = \emptyset.$$

Torej je

$$\emptyset = R * (S \cap T) \neq R * S \cap R * T = \{(a, b)\}.$$

Ovojnice relacij

Naj bo R relacija v A.

Motivacija: Včasih nas zanima, kaj manjka relaciji, da bi imela neko lastnost, npr. refleksivnost, simetričnost, tranzitivnost.

S $\mathrm{Cl}_*(R)$ označujemo relacijo v A, ki vsebuje relacijo R ($R \subseteq \mathrm{Cl}_*(R)$) in je najmanjša med vsemi relacijami v A, ki vsebujejo R in imajo lastnosti $*$. Relaciji $\mathrm{Cl}_*(R)$ pravimo *ovojnica* ali *zaprtje* relacije R glede na lastnosti $*$.

V nadaljevanju bo $\mathrm{Cl}_{\mathrm{ref}}(R)$, $\mathrm{Cl}_{\mathrm{sim}}(R)$, $\mathrm{Cl}_{\mathrm{tr}}(R)$ pomenilo zaprtja relacije R glede na lastnosti refleksivnosti, simetričnosti oz. tranzitivnosti, $\mathrm{Cl}_{\text{ref-tr}}(R)$ pa zaprtje glede na lastnosti refleksivnosti in tranzitivnosti.

Trditev

1. $\mathrm{Cl}_{\mathrm{ref}}(R) = R \cup \mathrm{id}_A$.
2. $\mathrm{Cl}_{\mathrm{sim}}(R) = R \cup R^{-1}$.
3. $\mathrm{Cl}_{\mathrm{tr}}(R) = \bigcup_{n=1}^{\infty} R^n$.
4. $\mathrm{Cl}_{\text{ref-tr}}(R) = \bigcup_{n=0}^{\infty} R^n$.

Dokaz točke (1). Po definiciji velja $R \subseteq \mathrm{Cl}_{\mathrm{ref}}(R)$. Ker mora biti $\mathrm{Cl}_{\mathrm{ref}}(R)$ refleksivna, velja tudi $\mathrm{id}_A \subseteq \mathrm{Cl}_{\mathrm{ref}}(R)$. Ker je $\mathrm{Cl}_{\mathrm{ref}}(R)$ najmanjša refleksivna relacija, ki vsebuje R in id_A, je $\mathrm{Cl}_{\mathrm{ref}}(R) = R \cup \mathrm{id}_A$.

Dokaz točke (2). Po definiciji velja $R \subseteq \mathrm{Cl}_{\mathrm{sim}}(R)$. Ker mora biti $\mathrm{Cl}_{\mathrm{sim}}(R)$ simetrična, velja tudi $R^{-1} \subseteq \mathrm{Cl}_{\mathrm{sim}}(R)$. Najmanjša relacija, ki vsebuje R in R^{-1}, je $R \cup R^{-1}$. Ker je ta relacija tudi simetrična, je $\mathrm{Cl}_{\mathrm{sim}}(R) = R \cup R^{-1}$.

Dokaz točke (3). Po definiciji velja $R \subseteq \mathrm{Cl}_{\mathrm{tr}}(R)$. Ker mora biti $\mathrm{Cl}_{\mathrm{tr}}(R)$ tranzitivna, velja tudi:

- $R^2 \subseteq \mathrm{Cl}_{\mathrm{tr}}(R)$, saj je $R^2 = R * R$.
- $R^3 \subseteq \mathrm{Cl}_{\mathrm{tr}}(R)$, saj je $R^3 = R^2 * R$.

$\vdots$

- $R^n \subseteq \mathrm{Cl}_{\mathrm{tr}}(R)$ za vsak $n \geq 2$, saj je $R^n = R^{n-1} * R$.

Najmanjša relacija, ki vsebuje R^n za vsak $n \geq 1$, je $\bigcup_{n=1}^{\infty} R^n$. Za enakost $\mathrm{Cl}_{\mathrm{tr}}(R) = \bigcup_{n=1}^{\infty} R^n$ moramo preveriti še, da je $\bigcup_{n=1}^{\infty} R^n$ res tranzitivna:

Naj bodo $x, y, z \in A$ taki elementi, za katere velja $(x, y) \in \bigcup_{n=1}^{\infty} R^n$ in $(y, z) \in \bigcup_{n=1}^{\infty} R^n$. Preveriti moramo, da je potem tudi $(x, z) \in \bigcup_{n=1}^{\infty} R^n$. Ker je $(x, y) \in \bigcup_{n=1}^{\infty} R^n$, obstaja neko naravno število N, za katero velja $(x, y) \in R^N$. Podobno obstaja neko naravno število M, za katero velja $(y, z) \in R^M$. Po definiciji produkta je zato $(x, z) \in R^N * R^M = R^{N+M}$. Torej je (x, z) res element $(x, z) \in \bigcup_{n=1}^{\infty} R^n$, kar smo želeli preveriti.

Dokaz točke (4). Praktično enak dokazu (3), le da moramo zaradi refleksivnosti dodati še $R^0 = \mathrm{id}_A$.

Grafično določanje ovojnic relacije

Naj bo R relacija v končni množici A. Z $\mathcal{G}_R$ označimo graf relacije R.

Trditev

- $\mathcal{G}_{\mathrm{Cl}_{\mathrm{ref}}(R)}$ *dobimo iz grafa* $\mathcal{G}_R$ *tako, da mu dodamo vse zanke, ki manjkajo.*
- $\mathcal{G}_{\mathrm{Cl}_{\mathrm{sim}}(R)}$ *dobimo iz grafa* $\mathcal{G}_R$ *tako, da vse povezave usmerimo v obe smeri.*
- $\mathcal{G}_{\mathrm{Cl}_{\mathrm{tr}}(R)}$ *dobimo iz grafa* $\mathcal{G}_R$ *z naslednjim postopkom:*

```
1  Oznacimo z G := G_R in naj bo G_s graf brez povezav.
2
3  if G = G_S
4      return G
5
6  while G_s ≠ G
7      G_s := G
8      for (x, y, z) ∈ A × A × A
9          if (x, y) ∈ G ∧ (y, z) ∈ G ∧ (x, z) ∉ G
10             Dodaj (x, z) v G.
11
12 return G
```

- $\mathcal{G}_{\mathrm{Cl}_{\text{ref-tr}}(R)}$ *dobimo iz grafa* $\mathcal{G}_R$ *tako, da določimo graf* $\mathcal{G}_{\mathrm{Cl}_{\mathrm{tr}}(R)}$ *in mu dodamo vse zanke.*

Pomen potenc relacije R in $\mathrm{Cl}_{\mathrm{tr}}(R)$

Pot dolžine n v relaciji R od elementa a do b je zaporedje urejenih parov

$$(a, x_1), (x_1, x_2), \ldots, (x_{n-1}, b)$$

iz R.

Cikel dolžine n v relaciji R je pot dolžine n z $a = b$.

Trditev

- *Med elementoma a in b iz A obstaja pot dolžine n v R natanko tedaj, ko je* $(a, b) \in R^n$.
- R^n *je množica urejenih parov, med katerimi obstaja usmerjena pot dolžine n.*
- $\mathrm{Cl}_{\mathrm{tr}}(R)$ *je množica urejenih parov, med katerimi obstaja usmerjena pot pozitivne dolžine.*
- $\mathrm{Cl}_{\text{ref-tr}}(R)$ *je množica urejenih parov, med katerimi obstaja usmerjena pot nenegativne dolžine.*

Ekvivalenčna relacija

Spomnimo se, da je relacija R v množici A *ekvivalenčna*, če je refleksivna, simetrična in tranzitivna.

Naj bo $\mathrm{Cl}_{\mathrm{ekv}}(R)$ najmanjša ekvivalenčna relacija, ki vsebuje R.

Trditev

Velja:

1. $\mathrm{Cl}_{\mathrm{ekv}}(R) = \mathrm{Cl}_{\mathrm{tr}}(\mathrm{Cl}_{\mathrm{sim}}(\mathrm{Cl}_{\mathrm{ref}}(R)))$.
2. *R je ekvivalenčna natanko tedaj, ko je* $R = \mathrm{Cl}_{\mathrm{ekv}}(R)$.

Primer

1. *Relacija $||$ vzporednosti v množici vseh premic v ravnini.*
2. $A = \{ljudje\}$, $xRy \iff$ *x ima enako barvo oči kot y.*
3. $f : \mathbb{R} \to \mathbb{R}$ *naj bo funkcija.* $xR_f y \Leftrightarrow f(x) = f(y)$
4. *Naj bo* $m \in \mathbb{N}$, $m \geq 2$. *Definirajmo relacijo R v množici* $\mathbb{Z}$*:*

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

Relacija R se imenuje kongruenca po modulu m in je izrednega pomena v kriptografskih algoritmih!

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.

$A/R = \{R[x]\,;\, x \in A\}$ je množica vseh ekvivalenčnih razredov, ki jo imenujemo *faktorska oz. kvocientna množica* množice A po relaciji R.

Trditev

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

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

Dokaz.

Smer ($\Rightarrow$): Ker je R refleksivna, velja xRx. Iz enakosti $R[x] = R[y]$ sledi $x \in R[y]$ oz. xRy.

Smer ($\Leftarrow$): Naj bo $z \in R[x]$. Torej je zRx. Skupaj z xRy in tranzitivnostjo R sledi $z \in R[y]$. Torej je $R[x] \subseteq R[y]$. Iz simetričnosti sklepamo tudi obratno, tj. $R[y] \subseteq R[x]$. □

Trditev

Naj bo R ekvivalenčna relacija na A. Potem so ekvivalenčni razredi paroma disjunktne podmnožice v A, katerih unija je A. Pravimo, da je A/R razbitje množice A.

Primer (Ekvivalenčne relacije)

- *"ljudje"/"ista barva oči"* $=$
  $\{\{$*ljudje z očmi rjave b.*$\}, \{$*ljudje z očmi zelene b.*$\}, \ldots\} \cong$
  $\{$*rjava,zelena*$, \ldots\}$
- $\mathbb{Z}/$ *"isti ostanek pri deljenju s 5"* $=$
  $\{\{\ldots, 0, 5, 10, \ldots\}, \{\ldots, 1, 6, 11, \ldots\}, \ldots\} =$
  $\{R[0], R[1], R[2], R[3], R[4]\} \cong \{0, 1, 2, 3, 4\}$

Primer (Neekvivalenčne relacije)

Naslednje relacije niso ekvivalenčne:

- *Relacija "imata bankovec z isto vrednostjo v denarnici" v množici ljudi.*
- *Prazna relacija na (neprazni) množici A.*
- *"Je deljiv z istim praštevilom kot" v množici naravnih števil.*
- *"Je približno enak" v množici realnih števil.*