

Algebra

Ivan Prokić

Fakultet tehničkih nauka, Novi Sad

Predavanje 2

Na prethodnom času

- Ponovili osnovne pojmove iz logike
- Ponovili osnovne pojmove iz skupova
- Uređeni parovi i Dekartov proizvod
- Binarne relacije
- Osobine binarnih relacija (R S A T F)

Relacije ekvivalencije

Relacija ekvivalencije

Definicija (Relacija ekvivalencije)

Ako je binarna relacija nekog skupa refleksivna, simetrična i tranzitivna (tj. R S T), tada se ona zove relacija ekvivalencije.

Primer

Neke relacije ekvivalencije skupa $A = \{a, b, c\}$ su

1. $\rho_1 = \{(a, a), (b, b), (c, c)\}$ *(Dijagonala, jednako)*
2. $\rho_2 = A^2$ *(Puna relacija)*
3. $\rho_3 = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$

Formulacija i dokaz napomene sa prethodnog slajda

Teorema

Neka je ρ relacija ekvivalencije skupa A . Tada, za svako $x, y \in A$ važi

$$x \rho y \Leftrightarrow C_x = C_y$$

Dokaz

Ekvivalenciju (\Leftrightarrow) dokazujemo tako što dokažemo dve implikacije:

(\Rightarrow): Pretpostavka je $x \rho y$. Pokazaćemo da iz ove pretpostavke sledi

$C_x \subseteq C_y$: Neka je $z \in C_x$. Po definiciji C_x ovo znači da važi $x \rho z$. Iz $x \rho y$ i simetričnosti ρ sledi $y \rho x$. Sad imamo $y \rho x$ i $x \rho z$, pa iz tranzitivnosti ρ dobijamo $y \rho z$. Po definiciji C_y sledi $z \in C_y$. Dakle, za svako $z \in C_x$ sledi $z \in C_y$, tj. važi $C_x \subseteq C_y$.

$C_y \subseteq C_x$: Analogno (na isti način). Uzeti $z \in C_y$ i pokazati da važi $z \in C_x$.

Ovime je dokazano $C_x = C_y$.

(\Leftarrow): Pretpostavka je $C_x = C_y$. Iz refleksivnosti ρ imamo $y \rho y$, te je $y \in C_y$. Sada iz $C_y = C_x$ sledi $y \in C_x$, i zato važi $x \rho y$.

Relacija ekvivalencije određuje particiju

Teorema

Svaka relacija ekvivalencije određuje jednu particiju skupa.

Dokaz

*Neka je $A \neq \emptyset$. Neka je ρ relacija ekvivalencije na A . Iz refleksivnosti ρ možemo zaključiti da podskupovi u $\{C_x \mid x \in A\}$ sadrže sve elemente iz A i da su sve klase ekvivalencije neprazne. Da bi imali particiju potrebno je dokazati da su sve različite klase ekvivalencije disjunktne, tj. da imaju prazan presek. **Da budemo sigurni napravimo pomoćno tvrđenje (Lemu) koje ovo dokazuje!***

Relacija ekvivalencije određuje particiju

Lema

Ako je ρ relacija ekvivalencije na skupu A , tada za sve $x, y \in A$ važi $C_x = C_y$ ili $C_x \cap C_y = \emptyset$.

Dokaz

Neka je $C_x \cap C_y \neq \emptyset$ i neka je $z \in C_x \cap C_y$. Iz $z \in C_x$ i $z \in C_y$ sledi $x \rho z$ i $z \rho y$, pa iz tranzitivnosti ρ sledi $x \rho y$. Sada iz Teoreme od ranije imamo $C_x = C_y$.

Teorema

Svaka relacija ekvivalencije određuje jednu particiju skupa.

Dokaz

Neka je $A \neq \emptyset$. Neka je ρ relacija ekvivalencije na A . Iz refleksivnosti ρ možemo zaključiti da podskupovi u $\{C_x \mid x \in A\}$ sadrže sve elemente iz A i da su sve klase ekvivalencije neprazne. Da bi imali particiju potrebno je dokazati da su sve različite klase ekvivalencije disjunktne, tj. da imaju prazan presek. **Da budemo sigurni napravimo pomoćno tvrđenje (Lemu) koje ovo dokazuje!**

Relacija ekvivalencije određuje particiju

Lema

Ako je ρ relacija ekvivalencije na skupu A , tada za sve $x, y \in A$ važi $C_x = C_y$ ili $C_x \cap C_y = \emptyset$.

Dokaz

Neka je $C_x \cap C_y \neq \emptyset$ i neka je $z \in C_x \cap C_y$. Iz $z \in C_x$ i $z \in C_y$ sledi $x \rho z$ i $z \rho y$, pa iz tranzitivnosti ρ sledi $x \rho y$. Sada iz Teoreme od ranije imamo $C_x = C_y$.

Teorema

Svaka relacija ekvivalencije određuje jednu particiju skupa.

Dokaz

Neka je $A \neq \emptyset$. Neka je ρ relacija ekvivalencije na A . Iz refleksivnosti ρ možemo zaključiti da podskupovi u $\{C_x \mid x \in A\}$ sadrže sve elemente iz A i da su sve klase ekvivalencije neprazne. Da bi imali particiju potrebno je dokazati da su sve različite klase ekvivalencije disjunktne, tj. da imaju prazan presek. **Na osnovu leme gore ovo sledi.**

Particija određuje relaciju ekvivalencije

Teorema

Svaka particija skupa određuje jednu relaciju ekvivalencije.

Dokaz

Neka je $A \neq \emptyset$. Neka je \mathcal{P} jedna particija skupa A . Za svako $C \in \mathcal{P}$ uzmimo C^2 (punu) relaciju. Unija svih ovakvih punih relacija je relacija ekvivalencije na A . Dokažite sami.

Particija \Leftrightarrow relacija ekvivalencije: primer

Primer

Neka je $A = \{a, b, c, d, e, f\}$.

1. Za $\rho = \{(a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (a, b), (b, a), (a, c), (c, a), (b, c), (c, b), (d, f), (f, d)\}$ proveriti da je ρ relaciju ekvivalencije, pronaći klase ekvivalencije i faktor skup A/ρ .
2. Za particiju $\{\{a, b\}, \{c, d, e\}, \{f\}\}$ skupa A napisati relaciju ekvivalencije koja joj odgovara (čiji je faktor skup baš ova particija).

Particija \Leftrightarrow relacija ekvivalencije: primer

Primer

Neka je $A = \{a, b, c, d, e, f\}$.

1. Za $\rho = \{(a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (a, b), (b, a), (a, c), (c, a), (b, c), (c, b), (d, f), (f, d)\}$ proveriti da je ρ relaciju ekvivalencije, pronaći klase ekvivalencije i faktor skup A/ρ .
2. Za particiju $\{\{a, b\}, \{c, d, e\}, \{f\}\}$ skupa A napisati relaciju ekvivalencije koja joj odgovara (čiji je faktor skup baš ova particija).

Rešenje.

1. Klase ekvivalencije su $C_1 = \{a, b, c\}$, $C_2 = \{d, f\}$, $C_3 = \{e\}$, a faktor skup $A/\rho = \{\{a, b, c\}, \{d, f\}, \{e\}\}$
2. Relacija ekvivalencije je $\rho_1 = \{(a, a), (b, b), (a, b), (b, a), (c, c), (d, d), (e, e), (c, d), (d, c), (c, e), (e, c), (d, e), (e, d), (f, f)\}$

Ostatak pri deljenju u \mathbb{Z}

Napomena

Setimo se iz 6. razreda relacije $|$ na skupu \mathbb{Z} , npr. $2|4$ i $2 \nmid 5$ (malo kasnije ćemo o njenim osobinama)

Ostatak pri deljenju u \mathbb{Z}

Napomena

Setimo se iz 6. razreda relacije $|$ na skupu \mathbb{Z} , npr. $2 | 4$ i $2 \nmid 5$ (malo kasnije ćemo o njenim osobinama)

Definicija

Na skupu \mathbb{Z} uvodimo relaciju \equiv_3 **kongruentno po modulu 3** sa: $x \equiv_3 y$ akko $3 | x - y$ (tj. x i y **daju isti ostatak pri deljenju sa 3**). Piše se i $x \equiv y \pmod{3}$.

Lema

Na skupu \mathbb{Z} relacija \equiv_3 je relacija ekvivalencije.

Ostatak pri deljenju u \mathbb{Z}

Napomena

Setimo se iz 6. razreda relacije $|$ na skupu \mathbb{Z} , npr. $2 | 4$ i $2 \nmid 5$ (malo kasnije ćemo o njenim osobinama)

Definicija

Na skupu \mathbb{Z} uvodimo relaciju \equiv_3 **kongruentno po modulu 3** sa: $x \equiv_3 y$ akko $3 | x - y$ (tj. x i y daju isti ostatak pri deljenju sa 3). Piše se i $x \equiv y \pmod{3}$.

Lema

Na skupu \mathbb{Z} relacija \equiv_3 je relacija ekvivalencije.

Dokaz

(R) $(\forall x \in \mathbb{Z}) x \equiv_3 x$ jer $3 | x - x$

(S) $(\forall x, y \in \mathbb{Z})$ ako je $x \equiv_3 y$ (tj. $3 | x - y$) tada je i $y \equiv_3 x$ (jer $3 | y - x$)

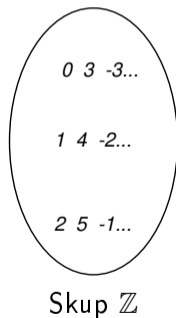
(T) $(\forall x, y, z \in \mathbb{Z})$ ako $x \equiv_3 y$ i $y \equiv_3 z$ tada je $x \equiv_3 z$ (jer x i y i z daju isti ostatak pri deljenju sa 3)

Skup \mathbb{Z}_3

Relacija \equiv_3 na \mathbb{Z} vrši particiju: kako izgleda faktor skup?

Klase ekvivalencije

Faktor skup \mathbb{Z}/\equiv_3 ćemo označavati sa \mathbb{Z}_3



Skup \mathbb{Z}_3

Relacija \equiv_3 na \mathbb{Z} vrši particiju: kako izgleda faktor skup?

Klase ekvivalencije

1. $C_0 = \{0, 3, -3, \dots\}$ - deljivi sa 3
2. $C_1 = \{1, 4, -2, \dots\}$ - ostatak 1
3. $C_2 = \{2, 5, -1, \dots\}$ - ostatak 2

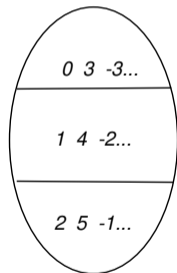
Faktor skup \mathbb{Z}/\equiv_3 ćemo označavati sa \mathbb{Z}_3

$$\mathbb{Z}_3 = \{C_0, C_1, C_2\}$$

Pošto su klase ekvivalencije određene bilo kojim svojim elementom pišaćemo i

$$\mathbb{Z}_3 = \{0, 1, 2\}$$

Isto smo mogli uraditi da dobijemo $\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_5, \dots, \mathbb{Z}_n$



Faktor skup \mathbb{Z}_3

Relacije poretka

Relacija poretka

Definicija (Relacija poretka)

Ako je binarna relacija nekog skupa A refleksivna, antisimetrična i tranzitivna (tj. $R A T$), tada se ona zove relacija poretka i kažemo da je (A, ρ) **(parcijalno) uređen skup**.

Primer

Neke relacije poretka

1. Na skupu $A = \{a, b, c\}$: $\rho_1 = \{(a, a), (b, b), (c, c)\}$ (Dijagonala, jednako)
2. Na skupu $A = \{a, b, c\}$: $\rho_1 = \{(a, a), (b, b), (c, c), (a, b), (b, c), (a, c)\}$ (Lanac)
3. $(\mathcal{P}(A), \subseteq)$, za $A \neq \emptyset$ (Partitivni skup i relacija podskup)
4. $(\mathbb{N}, |)$ (Prirodni brojevi i relacija deli)
5. (\mathbb{R}, \leq) (Realni brojevi i relacija manje-jednako)

Parcijalno uređeni skupovi $(\mathcal{P}(A), \subseteq)$ i $(\mathbb{N}, |)$

Primer

Neka je $A \neq \emptyset$. Tada je $(\mathcal{P}(A), \subseteq)$ je parcijalno uređen skup

$$(R) (\forall X \in \mathcal{P}(A)) \quad X \subseteq X$$

$$(A) (\forall X, Y \in \mathcal{P}(A)) \quad (X \subseteq Y \wedge Y \subseteq X) \Rightarrow X = Y$$

$$(T) (\forall X, Y, Z \in \mathcal{P}(A)) \quad (X \subseteq Y \wedge Y \subseteq Z) \Rightarrow X \subseteq Z$$

Parcijalno uređeni skupovi $(\mathcal{P}(A), \subseteq)$ i $(\mathbb{N}, |)$

Primer

Neka je $A \neq \emptyset$. Tada je $(\mathcal{P}(A), \subseteq)$ je parcijalno uređen skup

$$(R) (\forall X \in \mathcal{P}(A)) \quad X \subseteq X$$

$$(A) (\forall X, Y \in \mathcal{P}(A)) \quad (X \subseteq Y \wedge Y \subseteq X) \Rightarrow X = Y$$

$$(T) (\forall X, Y, Z \in \mathcal{P}(A)) \quad (X \subseteq Y \wedge Y \subseteq Z) \Rightarrow X \subseteq Z$$

Primer

$(\mathbb{N}, |)$ je parcijalno uređen skup

$$(R) (\forall x \in \mathbb{N}) \quad x | x$$

$$(A) (\forall x, y \in \mathbb{N}) \quad (x | y \wedge y | x) \Rightarrow x = y$$

$$(T) (\forall x, y, z \in \mathbb{N}) \quad (x | y \wedge y | z) \Rightarrow x | z$$

Napomena

Da li je $(\mathbb{Z}, |)$ parcijalno uređen skup?

Haseov dijagram

Parcijalno uređeni skup (A, ρ) možemo grafički da predstavimo kao graf (tzv. Haseov dijagram)

- Elemente skupa A crtamo kao tačke (čvorove) i povezujemo ih linijama (granama)
- Ako imamo $x \rho y$ onda x crtamo **ispod**, a y **iznad**
- Ako je $x \rho y$ i ne postoji $z \in A$ takvo da je z **između** x i y , tj. takvo da važi $x \rho z$ i $z \rho y$, onda x i y direktno spajamo granom

Haseov dijagram

Parcijalno uređeni skup (A, ρ) možemo grafički da predstavimo kao graf (tzv. Haseov dijagram)

- Elemente skupa A crtamo kao tačke (čvorove) i povezujemo ih linijama (granama)
- Ako imamo $x \rho y$ onda x crtamo **ispod**, a y **iznad**
- Ako je $x \rho y$ i ne postoji $z \in A$ takvo da je z **između** x i y , tj. takvo da važi $x \rho z$ i $z \rho y$, onda x i y direktno spajamo granom

Primer

Nacrtati Haseov dijagram za parcijalno uređen skup (A, ρ) ,
gde je $A = \{a, b, c, d, e\}$ i $\rho_1 = \{(a, a), (b, b), (c, c), (d, d),$
 $(e, e), (a, b), (a, c), (a, d), (a, e), (c, d), (c, e)\}$

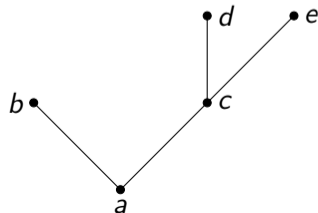
Haseov dijagram

Parcijalno uređeni skup (A, ρ) možemo grafički da predstavimo kao graf (tzv. Haseov dijagram)

- Elemente skupa A crtamo kao tačke (čvorove) i povezujemo ih linijama (granama)
- Ako imamo $x \rho y$ onda x crtamo **ispod**, a y **iznad**
- Ako je $x \rho y$ i ne postoji $z \in A$ takvo da je z **između** x i y , tj. takvo da važi $x \rho z$ i $z \rho y$, onda x i y direktno spajamo granom

Primer

Nacrtati Haseov dijagram za parcijalno uređen skup (A, ρ) , gde je $A = \{a, b, c, d, e\}$ i $\rho_1 = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (a, c), (a, d), (a, e), (c, d), (c, e)\}$



Najmanji, najveći, min i max elementi

Definicija

U parcijalno uređenom skupu (A, ρ) definišemo specijalne elemente

- *a je najmanji element* akko $(\forall x \in A) \quad a \rho x$ *(Ispod svih drugih)*
- *a je najveći element* akko $(\forall x \in A) \quad x \rho a$ *(Iznad svih drugih)*
- *a je minimalni element* akko $(\forall x \in A \setminus \{a\}) \quad x \not\rho a$ *(Nema drugih ispod)*
- *a je maksimalni element* akko $(\forall x \in A \setminus \{a\}) \quad a \not\rho x$ *(Nema drugih iznad)*

Najmanji, najveći, min i max elementi

Definicija

U parcijalno uređenom skupu (A, ρ) definišemo specijalne elemente

- a je najmanji element akko $(\forall x \in A) \quad a \rho x$ (Ispod svih drugih)
- a je najveći element akko $(\forall x \in A) \quad x \rho a$ (Iznad svih drugih)
- a je minimalni element akko $(\forall x \in A \setminus \{a\}) \quad x \not\rho a$ (Nema drugih ispod)
- a je maksimalni element akko $(\forall x \in A \setminus \{a\}) \quad a \not\rho x$ (Nema drugih iznad)

Primer

Za parcijalno uređen skup (A, ρ) , gde je $A = \{a, b, c, d, e\}$ i

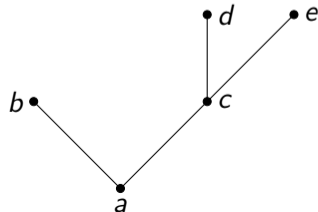
$\rho_1 = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (a, c), (a, d), (a, e), (c, d), (c, e)\}$ odrediti

najmanji: ,

minimalne: ,

najveći: ,

maksimalne:



Najmanji, najveći, min i max elementi

Definicija

U parcijalno uređenom skupu (A, ρ) definišemo specijalne elemente

- a je najmanji element akko $(\forall x \in A) \quad a \rho x$ (Ispod svih drugih)
- a je najveći element akko $(\forall x \in A) \quad x \rho a$ (Iznad svih drugih)
- a je minimalni element akko $(\forall x \in A \setminus \{a\}) \quad x \not\rho a$ (Nema drugih ispod)
- a je maksimalni element akko $(\forall x \in A \setminus \{a\}) \quad a \not\rho x$ (Nema drugih iznad)

Primer

Za parcijalno uređen skup (A, ρ) , gde je $A = \{a, b, c, d, e\}$ i

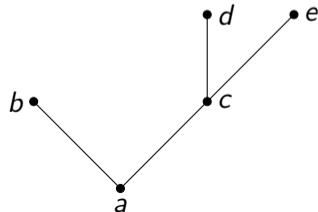
$\rho_1 = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (a, c), (a, d), (a, e), (c, d), (c, e)\}$ odrediti

najmanji: a ,

minimalne: a ,

najveći: nema,

maksimalne: b, d, e



Najmanji (najveći) je jedinstven

Teorema

Ako postoji, najmanji (najveći) element parcijalno uređenog skupa je jedinstven.

Dokaz

*Dokaz izvodimo **svođenjem na kontradikciju** (reductio ad absurdum: ako pretpostavimo da je neka izjava istinita, doći ćemo do logičke kontradikcije). Suprotno tvrđenju teoreme, pretpostavimo da postoji parcijalno uređen skup (A, ρ) koji ima bar dva različita najmanja elementa a i b . Po definiciji najmanjeg elementa to znači da važi $a \rho b$ i $b \rho a$. Ovo je u kontradikciji sa pretpostavkom da je (A, ρ) parcijalno uređen skup (ρ mora biti antisimetrično), pa je zaključak da parcijalno uređen skup ne može imati više različitih najmanjih elemenata.*

Supremum i infimum

Definicija

Neka je (A, ρ) parcijalno uređen skup i $M \subseteq A$.

- $a \in A$ je **donja granica** skupa M akko $(\forall m \in M) a \rho m$
- $a \in A$ je **gornja granica** skupa M akko $(\forall m \in M) m \rho a$
- Skup M je **ograničen** akko ima bar jednu gornju i donju granicu
- Ako postoji najmanji element skupa svih gornjih granica skupa M , tada se on zove **supremum** i obeležava se $\sup M$
- Ako postoji najveći element skupa svih donjih granica skupa M , tada se on zove **infimum** i obeležava se $\inf M$

Primer

U parcijalno uređenom skupu (\mathbb{R}, \leq) , za otvoren interval $M = (0, 1)$ imamo $\sup M = 1$
i $\inf M = 0$

Totalno i dobro uređeni skupovi

Definicija (Totalno uređen skup ili lanac)

Ako u parcijalno uređenom skupu za svaka dva elementa a i b važi $a \rho b$ ili $b \rho a$, tada se on naziva totalno uređen skup ili lanac.

Definicija (Dobro uređen skup)

Ako u parcijalno uređenom skupu svaki neprazan podskup ima najmanji element, tada se on naziva dobro uređen skup.

Totalno i dobro uređeni skupovi

Definicija (Totalno uređen skup ili lanac)

Ako u parcijalno uređenom skupu za svaka dva elementa a i b važi $a \rho b$ ili $b \rho a$, tada se on naziva totalno uređen skup ili lanac.

Definicija (Dobro uređen skup)

Ako u parcijalno uređenom skupu svaki neprazan podskup ima najmanji element, tada se on naziva dobro uređen skup.

Primer

(\mathbb{R}, \leq) i (\mathbb{Z}, \leq) su lanaci, a (\mathbb{N}, \leq) je dobro uređen skup i lanac

Totalno i dobro uređeni skupovi

Definicija (Totalno uređen skup ili lanac)

Ako u parcijalno uređenom skupu za svaka dva elementa a i b važi $a \rho b$ ili $b \rho a$, tada se on naziva totalno uređen skup ili lanac.

Definicija (Dobro uređen skup)

Ako u parcijalno uređenom skupu svaki neprazan podskup ima najmanji element, tada se on naziva dobro uređen skup.

Primer

(\mathbb{R}, \leq) i (\mathbb{Z}, \leq) su lanaci, a (\mathbb{N}, \leq) je dobro uređen skup i lanac

Teorema

Svaki dobro uređeni skup je i lanac.

Dokaz

Neka je (A, ρ) dobro uređen skup. Ako uzmemo $a, b \in A$ i skup $\{a, b\}$ sledi da taj skup ima najmanji element.

Tada je taj najmanji element u relaciji sa onim drugim elementom skupa $\{a, b\}$, tj. imamo $a \rho b$ ili $b \rho a$.

Primeri

Nacrtati Haseove dijagrame i odrediti najmanji, najveći, minimalne i maksimalne elemente sledećih parcijalno uređenih skupova:

1. $(\mathcal{P}(A), \subseteq)$, gde je $A = \{a, b, c\}$
2. $(\mathcal{P}(A) \setminus \{\emptyset\}, \subseteq)$, gde je $A = \{a, b, c\}$
3. $(\mathbb{N}, |)$
4. $(\mathbb{N} \setminus \{1\}, |)$
5. $(D_{30}, |)$, gde je $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$
6. $(D_{30} \setminus \{30\}, |)$, gde je $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$

Šta smo danas radili

- Relacije ekvivalencije
 - Klase ekvivalencije i faktor skup (particije)
 - Skup \mathbb{Z}_n
- Relacije poretka (parcijalno uređeni skupovi)
 - Haseov dijagram
 - Najmanji, najveći, min i max elementi
 - Supremum i infimum
 - Lanci i dobro uređeni skupovi