II. Kolokvij - DM

Funkcije, Relacije

Funkcija je preslikavanje $\mathbf{f:D\to K}$ takvo da $(\forall x \in D)(x\rho y_1 \wedge x\rho y_2 \Rightarrow y_1=y_2)$ (za svaki x iz domene postoji y iz kodomene i to samo jedan)
Funkcija je vrsta binarne relacije $\rho \subseteq D\times K$, što znači da je funkcija skup i da vrijedi: $x\rho y \Leftrightarrow (x,y)\in\rho \Leftrightarrow x\mapsto y \Leftrightarrow f(x)=y$
Indentiteta je funkcija $\mathbf{f:A\to A}$ odnosno $\mathbf{id:A\to A} \Leftrightarrow id(x)=x \Leftrightarrow x\rho x$ (preslikavanje iz istog skupa u isti skup)
Surjekcija je funkcija takva da $(\forall y \in K)(\exists x \in D)(x\rho y)$ (za svaki y iz kodomene postoji neki, bilo koji x iz domene)
Injekcija je funkcija takva da $(\forall x_1,x_2 \in D)(x_1\neq x_2 \Rightarrow x_1\rho y_1 \neq x_2\rho y_2)$ (različiti x-evi iz domene se ne preslikavaju u iste y iz kodomene)
Bijekcija je funkcija koja je istovremeno i surjekcija i injekcija.
Inverzna funkcija je bijekcija (ne može biti ništa drugo) za koju vrijedi $f(x)=y \Rightarrow f^{-1}(y)=x$ ili $x\rho y \Rightarrow y\rho^{-1} x$
Kompozicija funkcija ulančanih preko istog skupa je nova funkcija. $g\circ f=g(f(x))$ gdje vrijedi $(\forall x \in D_f)(\exists y \in K_f)(x\rho y \wedge y\rho z \Rightarrow x\rho z \in g\circ f)$
Kompozicija funkcije (nije isto što i komp. relacije) je preslikavanje iz D od unutrašnje funkcije u K vanjske funkcije preko međuskupa.
Zbog definicije funkcije u D kompozicije ne smije biti elemenata koji se ne preslikavaju nigdje. Cijela K unutrašnje je i K kompozicije
Kompozicija nije komutativna operacija ($g\circ f \neq f\circ g$). Ako funkcije nisu ulančane, njihova je kompozicija prazan skup.
Definicija inverzne funkcije: $f^{-1}\circ f = id_D = id$ odnosno $f\circ f^{-1} = id_K = id$ (indentiteta)
Funkcije su jednake ako imaju istu domenu, kodomenu i preslikavanja, odnosno $(f \stackrel{?}{=} g) \Rightarrow (f\circ g^{-1}) = id$
Definicija direktne slike skupa: $f(D)=K \Leftrightarrow y\in f(D) \Leftrightarrow y\in K=f(D) \Leftrightarrow x\in D$ (skup se preslikava u skup npr. f({1, 2}) = {1,4})
Definicija inverzne slike skupa: $f^{-1}(K)=D \Leftrightarrow x\in f^{-1}(K) \Leftrightarrow x\in D=f^{-1}(K) \Leftrightarrow y\in K$ (skup se preslikava u skup)
Definicija direktne i inverzne slike elementa: $f(x)=y,\ f^{-1}(y)=x$
Definicija inverza kompozicije bijekcija: $(g\circ f)^{-1} \Leftrightarrow f^{-1}\circ g^{-1}$
Partitivni skup skupa A: $\mathcal{P}(A)$ je skup svih podskupova skupa **A**, uključujući i prazan skup. Elementi su skupovi: $\mathcal{P}(A)=\{\emptyset,\{.\},\{..\}..\{...\}\}$
Definicija presjeka: $A\cap B$ **unije:** $A\cup B : (\forall x)(x\in A \wedge x\in B)$ ili $A\cap B = \{x : x\in A \wedge x\in B\}$
Definicija unije: $A\cup B : (\forall x)(x\in A \vee x\in B)$ ili $A\cup B = \{x : x\in A \vee x\in B\}$
Definicija podskupa: $A\subseteq B : (\forall x)(x\in A \Rightarrow x\in B)$ ili $A\subseteq B = \{x : x\in A \Rightarrow x\in B\}$
Definicija razlike: $A\setminus B : (\forall x)(x\in A \Rightarrow x\notin B)$ ili $A\setminus B = A\cap \overline{B} : (\forall x)(x\in A \wedge x\in \overline{B})\}$
Definicija komplementa: $\overline{A} : (\forall x)(x\notin A)$
Definicija simetrične razlike: $A\,\Delta\, B = (A\setminus B)\cup(B\setminus A)$
Definicija kartezijevog produkta: $A\times B : (\forall a\in A, b\in B)(a\,\rho\, b)$ ili $A\times B = \{(a,b) : a\in A \wedge b\in B\}$
Relacija (homogena binarna) je podskup kartezijevog produkta $\rho\subseteq A\times A$ (homogena – isti skupovi u produktu, binarna – dva skupa)
Relacija se zadaje kao $\rho = \{(x_1,x_2), (x_3,y_4)..., (x_n,y_n)\}$ na skupu $A=\{(x_1,x_2,...x_n)\}$ (bitno je naglasiti na kojem skupu definira relacija)
Relacija parc. poretka se može zadati i kao PUS (A, ρ) (A je skup, a ρ daje pravilo po kojem su el. skupa u relaciji $(..., =, \leq, |...)$
Refleksivnost $(\forall x\in A)\, x\rho x$
Simetričnost $(\forall x,y\in A)(x\rho y \Rightarrow y\rho x)$
Antisimetričnost $(\forall x,y\in A)(x\rho y \wedge y\rho x \Rightarrow x=y)$
Tranzitivnost $(\forall x,y,z\in A)(x\rho y \wedge y\rho z \Rightarrow x\rho z)$
Potpunost $(\forall x,y\in A)(x\rho y \wedge y\rho x)$
Logično je da ako je refleksivna, onda je i simetrična ili antisimetrična. Ako je simetrična onda ne može biti antisim. i obratno (osim $\rho^{=}$)
Relacija ekvivalencije je relacija koja zadovoljava svojstva: refleksivnost, simetričnost i tranzitivnost. Zapis: $x\sim y \in \rho^{\sim}=\{...\}$
Primjeri relacije ekvivalencije su: kongruencije, ekvipotentnost skupova, sukladnost trokuta, ekvivalencija u analizi, ekvivalencija redova
Klase ekvivalencije dijele cijeli skup A u disjunktivne podskupove (particije skupa A). Skup svih onih koji su međusobno u relaciji
Klase ekvivalencije se mogu definirati relacijom ekvivalencije. Unija klasa ekvivalencija daje cijeli skup A
Faktorski/Kvocjentni skup je skup klasa ekvivalencija, odnosno njihovih predstavnika. $A/_{\rho\sim} = \{[x_1],[x_2],...,[x_n]\}$
Kardinalni broj faktorskog skupa je broj elemenata kvocjentnog skupa: $card(A/_{\rho\sim}) = k(A/_{\rho\sim}) = n$
Relacija parcijalnog poretka je ralacija koja zadovoljava svojstva: refleksivnost, antisimetričnost i tranzitivnost Zapis: $x\preccurlyeq y \in \rho^{\preccurlyeq}=\{...\}$
Hasseovim dijagramom možemo predočavati samo relacije parcijalnog poretka
Primjeri relacije parcijalnog poretka su: podskup na partitivnom skupu, skup svih realnih funkcija, $\leq$ jest, no $<$ nije jer nije refleksivna
Relacija jednakosti (A,=) je jedina relacija koja je istovremeno i relacija parcijalnog poretka i relacija ekvivalencije
Usporedivi elementi u relaciji su x i y ako vrijedi: $x\rho y \vee y\rho z$ (bilo da je x u relaciji sa y ili y sa x oni su usporedivi)
PUS – parcijalno uređen skup je skup A nad kojim je definirana relacija parcijalnog poretka $\rho^{\preccurlyeq}$. Zapis: (A,$\preccurlyeq$). Svaki podskup ima min
TUS – totalno (linearno) uređen skup ili lanac je skup nad kojim je definirana $\rho^{\preccurlyeq}$ ako su svaka dva elementa skupa A usporediva
DUS – dobro uređen skup je totalno uređen skup u kojem svaki neprazan podskup ima minimalni element (minimum)
Dolnja međa podskupa S PUS-a A je svaki $x\in A$ takav da vrijedi: $(\forall s\in S)(x\rho s)$ (x iz A je u relaciji sa svakim s iz S)
INF – infimum – najmanji element podskupa S PUS-a A je onaj za kojeg su svi iz S veći i koji je donja međa podskupa S
Gornja međa podskupa S PUS-a A je svaki $x\in A$ takav da vrijedi: $(\forall s\in S)(s\rho x)$ (svaki s iz S je u relaciji sa x iz A)
SUP – supermum – najveći element podskupa S PUS-a A je onaj za kojeg su svi iz S manji i koji je gornja međa podskupa S
inf i sup su najmanja gornja ili najveća donja međa skupa A, a one ne moraju biti elementi podskupa S na kojem tražimo inf i sup koji ako postoje su jedinstveni za taj podskup S. Omeđen podskup S odozgo ili odozdo je koji ima baram jednu gornju ili donju među.
Gornja i donja međa podskupa S PUS-a A su elementi skupa A koji su u relaciji sa svim elementima iz tog podskupa S.

Minimum (sl. maksimum) podskupa S PUS-a A je infinum koji je sadržan upravo u skupu S, a ne A. (Žubrinić)
Minimum (sl. maksimum) podskupa S PUS-a A je bilo koji element za koji nema manji, od koga su svi iznad njega. (Dževad)
Min i max može biti više, dok su sup i inf jedinstveni ako postoje. sup i inf su ujedno i min i max. (Dževad)
Mreža je PUS gdje vrijedi da svaka dva elementa (svaki par x_1, x_2) imaju inf i sup. U mreži vrijedi: $a+b=\sup\{a,b\}$ i $ab=\inf\{a,b\}$
Potpuna (totalna) mreža je PUS gdje svaki njegov podskup ima sup i inf. U potpunoj mreži supA se zove jedinica, a infA nula mreže
Distributivna mreža je potpuna mreža u kojoj vrijedi distributivnost: $a(b+c)=ab+ac$ ili $(a+b)(a+c)=a+ab$
Komplement elementa $\bar{a}$ u potpunoj mreži je neki x takav da vrijedi: a+(x)="1 – jedinica mreže" i a(x)="0" i tada je $\bar{a} = x$
Komplementarna mreža je mreža u kojoj svaki element PUS-a A ima svoj komplement
Relacija jednakosti je relacija gdje vrijedi: $id_A = \Delta_A = \{(x,x) : \forall x \in X\}$ Ta se relacija zove dijagonala u $X\times X$
Kartezijev produkt relacija je moguć samo sa relacijama parcijalnog poretka. Produkt relacija je opet relacija parcijalnog poretka
Definicija iz Žubrinićeve knjige je drugačija od Dževadove: Imamo PUS-ove: $(A, \preccurlyeq)$ i $(B, \preccurlyeq)$ i relacije $p \subseteq A\times A$ i $q \subseteq B\times B$. Kartezijev produkt relacija $p\times q \in (A,\preccurlyeq)\times(B,\preccurlyeq)$ je: $(\{ [(a_1,a_2)\in p, (b_1,b_2)\in q] : (a_1,b_1)\in p \wedge (a_2,b_2)\in q \}, \preccurlyeq)$ (Žubrinić)
Kompozicija binarnih relacija je skup svih (x,y) parova za koje postoji neki z takav da: $\rho^1\circ\rho^2 = \{(x,y)\in X\times X : (\exists z\in X)(x\rho^1 z \wedge z\rho^2 y)\}$
Inverzna relacija je relacija gdje vrijedi: $\rho^{-1}=\{ (x,y)\in X\times X : (y,x)\in \rho \}$. Vrijede inverzna pravila kao i za funkcije
Primjerom možemo opovrgnuti tvrdnju, dokazati ne valjanost, no ne možemo dokazivati valjanost. Primjer nije dokaz
Ekvivalentne zamjene su tipa $(x,y)\in \rho \Leftrightarrow (y,x)\in \rho^{-1}$, a ne ekvivalentne zamjene tipa $(x,y)\in \rho \Rightarrow (y,x)\in \rho$ treba dokazivati logički
Jednake relacije su ako zadovoljavaju: $\rho = q$ ako $\rho\subseteq q \wedge q\subseteq\rho$

Cijeli Brojevi

a dijeli b ako $a\neq 0$ pišemo $a|b \Rightarrow b = ak$ gdje je **a** djelitelj broja **b**, a **b** višekratnik broja **a**, a **k** je količnik
refleksivnost ako $a|a \Rightarrow a|a$
antisimetričnost ako $a|b \wedge b|a \Rightarrow a = b$ jer je $b = ak$ i $a = bl$ zato $a = akl$ a kako $a|b \Rightarrow a\neq 0$ dakle **kl** može biti isključivo **1**
tranzitivnost ako $a|b \wedge b|c \Rightarrow a|c$ jer zbog $b = ak$ i $c = bl \Rightarrow c = (ak)l$ ili $c = (kl)a$ što znači i da $c|a$
Nzm ako je barem jedan od brojeva $\neq 0$ onda postoji najveći zajednički djelitelj **a=Nzm** od tih brojeva. Npr. **Nzm(21,14)=7**
nzv ako su svi brojevi $\neq 0$ onda postoji najmanji $b\in N$ čiji su ti brojevi djelitelji **b=nzv** od tih brojeva. Npr. **nzv(3,4)=12**
Nzm i nzv su prirodni brojevi **N** za koje vrijedi vrijedi relacija $ab=nzv(a,b)\ Nzm(a,b)$ i $Nzm(a,b) \leq \min\{a,b\} \leq \mathrm{Max}\{a,b\} \leq nzv(a,b)$
Euklidov algoritam a=bq +r a = b [a/b] kvocjent + (a mod b) ostatak
Teorem o djeljenju neka su $a\in Z$ i $b\in N$ onda postoje jedinstveni kvocjent $q=(a/b)$, $q\in Z$ i ostatak $r\in\{0,\dots,b-1\}$ takvi da vrijedi $a=bq+r$

$d\|a \wedge d\|b \Rightarrow d\|a\pm b$	$d\|a\pm b \wedge d\|b \Rightarrow d\|a\pm b\pm b \Rightarrow d\|a$	$d\|a \wedge d\|b \Rightarrow d\|Nzm(a,b)$	$Nzm(ca, cb) = c\,Nzm(a,b)$
$d\|a \Rightarrow d\|ka$	$d\|a \Rightarrow d\|(-a)$	$d\|Nzm(a,b) \Rightarrow d\|a \wedge d\|b$	$Nzm(a/c, b/c) = Nzm(a,b)/c$
$d\|ab \Rightarrow d\|b$; $Nzm(a,b)=1$	$d\|a \wedge s\|a \Rightarrow d\|nzv(d,s)$	$d\|a \wedge s\|a \Rightarrow ds\|a$; $Nzm(d,s)=1$	$d\|a \wedge s\|a \Rightarrow nzv(d,s)\|a$

Kongruencije ako $d\nmid a$ ali $d|(a-r)$ onda $a = dq + r$ a to je ekvivalentno $a \equiv r \pmod d$ i tada $d\nmid r$, $d\nmid a$. Također vrijedi $a=a+mk \pmod d$
a = r (mod d) gdje $d\nmid a$ i $d\nmid r$ ali pri djeljenju daju **isti ostatak** i to manji od d samo ako su kongruentni
a = r (mod d) skup cijelih brojeva dijeli u d klasa ekvivalencije. Broj može biti samo u jednoj klasi, i to preko kongruencije
Rješavanje kongruencije: kako **a** i **r** pri djeljenju sa **d** daju isti ostatak, treba pronaći sličnu kongruenciju po modulu **d** kojoj ostatak znamo (eulerova kongruencija, mali fermatov, na silu...), zatim tu sličnu kongruenciju izvesti (potenciranje, množenje) do **a**
Rješavanje na silu: kako **a** predstavlja ostatak pri djeljenju sa **d**, možemo smanjiti **a** (oduzeti sa **d** ili **dx**) tako da taj ostatak ostane isti.
Npr. $3^{16} \equiv x \pmod 7$ Rješenje: $(3^2)^8 \equiv 9^8$ (radimo 9 mod 7)$\equiv 2^8 \equiv (2^4)^2 \equiv 16^2$ (16 mod 7) $\equiv 2^2 \equiv 4 \pmod 7$
Npr. $13^{16} \equiv x \pmod{73}$ Rješenje: $(13^2)^8 \equiv 169^8 \equiv 23^8 \equiv (23^2)^4 \equiv 529^4 \equiv 18^4 \equiv 324^2 \equiv 32^2 \equiv 1024 \equiv 2 \pmod{73}$

$a+nk \equiv b+nl \pmod n$	imamo: $a \equiv b \pmod n$ i $c \equiv d \pmod n$	kraćenje kongruencije: $a, b, k \in \mathbb{Z}$ i $n \in \mathbb{N}$
$ak \equiv bk \pmod n$	vrijedi:	neka je: $ak \equiv bk \pmod n$; $Nzm(k,n)=1$ ili $Nzm(k,n)=d$
$a^m \equiv b^m \pmod n$, $m \in N$	$a\pm c \equiv b\pm d \pmod n$	vrijedi:
$p(a) \equiv p(b) \pmod n$	$ac \equiv bd \pmod n$	$a \equiv b \pmod d$ (Žubrinić) ili $a \equiv b \pmod{n/d}$

Prosti brojevi su oni koji nisu djeljivi sa niti jednim drugim brojem (osim naravno sami sobom i sa 1) $p\in\mathbb{N}, p > 1$
Složeni brojevi su svi ostali brojevi brojevi osim 0,1 koji nisu niti jedno niti drugo, $a\in\mathbb{N}, a > 1$
Relativno prosti mogu biti dva broja (x, y) ako ima je $Nzm(x, y) = 1$. Oni sami ne moraju biti prosti. Ne mogu skratiti u razlomku
Rastav ℕ broja za $a > 1$ $a= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ gdje je α kratnost odgovarajućeg prostog broja **p** u rastavu poredanih po <
Djelitelja ℕ broja $a= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ ima ukupno $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_n+1)$
Eulerova funkcija svakom ℕ pridružuje broj brojeva **x** koji su $<n$ i $Nzm(x, n)=1$, vrijedi: $\varphi(p) = p-1$ i $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, **p** je prost broj
Eulerova kongruencija: $Nzm(a, n)=1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod n$
Mali fermatov stavak: p-prost $\Rightarrow (\forall a)p|a^p - a \Rightarrow a^p \equiv a \pmod p$, posebno, ako **a** nije višekratnik od **p**: $a^{p-1} \equiv 1 \pmod p$