DISKRETNE STRUKTURE 1
Odgovori na pitanja za usmeni kod profesora Ž. Mijajlovića

Nikola Ajzenhamer
Anja Bukurov
Lektor: Ludi Burekdžija

2014

Sadržaj

1 Matematička indukcija **3**
1.1 Princip matematičke indukcije 3

2 Operatori sumiranja $\sum$ i proizvoda $\prod$ **3**

3 Algebarski identiteti, binomna formula, asocijativni i komutativni zakoni **4**
3.1 BINOMNA FORMULA 4

4 Nejednakost izmedju aritmetičke i geometrijske sredine **4**

5 Rekurzivne definicije, Fibonačijev niz **5**

6 Linearna diferencna jednačina prvog reda **5**

7 Iskazna algebra **5**

8 Definicija iskaznih formula **6**

9 Tautologije - metode dokazivanja i primeri **6**

10 Teorema o disjunktivnoj normalnoj formi **6**

11 Kvantori **6**

12 Definicija predikatskih formula **6**

13 Pojam valuacije **7**

14 Valjane formule, primeri **7**

15 Teorija algebarskih polja **8**

16 Osnovne skupovne operacije, definicije i osobine **8**
16.1 Osobine skupovnih operacija 9
16.2 Beskonačne skupovne operacije 9

17 Skupovni identiteti, metode dokazivanja **10**
17.1 Metode dokazivanja skupovnih jednakosti 10

18 Aksiome teorije skupova **10**

19 Dekartov proizvod, operacija partitivnog skupa **10**
19.1 Dekartov proizvod 10
19.2 Operacija partitivnog skupa 11

20 Binarne relacije, kompozicija binarnih relacija, inverzna binarna relacija **11**

21 Funkcije, osobine (kompozicija, 1-1 i na preslikavanja) 12
21.1 Inverzna funkcija 12
21.2 Inverzna slika 13
21.3 Injekcija 13
21.4 Surjekcija 13
21.5 Kompozicija funkcija 13

22 Permutacije konačnih skupova, računanje proizvoda i inverzna permutacija 14
22.1 Proizvod permutacija 14
22.2 Inverzna permutacija 15

23 Relacije ekvivalencije i particije skupova, primeri 15
23.1 Relacija ekvivalencije 15
23.1.1 Klasa ekvivalencije 15
23.1.2 Particija skupa 15
23.2 Parcijalno i linearno uredjeni skupovi 16

24 Konačni i beskonačni skupovi i kardinalni broj 17
24.1 Dirikleov princip za konačne skupove 17

25 Bulove algebre 18

26 Bulovski identiteti, de Morganove jednakosti 18

27 Euklidov algoritam 18

28 Linearna diofantovska jednačina 19

1 Matematička indukcija

Matematička indukcija predstavlja važan i moćan metod za dokazivanje tvrđenja koja se odnose na prirodne brojeve. Ona proizilazi iz sledećeg svojstva skupa prirodnih brojeva N. Neka je $S \subseteq N$ i pretpostavimo da skup S ima sledeće dve osobine:
(1) $0 \in S$
(2) za svako n, ako $n \in S$ tada $n+1 \in S$
Tada S = N.
Zaista, prema (1) $0 \in S$, dok prema (2) tada i $1 \in S$. Opet primenjujući (2) nalazimo $2 \in S$ i tako redom $3, 4, ... \in S$, tj. $N \subseteq S$. S obzirom da je $S \subseteq N$, nalazimo S = N.
Pretpostavimo da je $\phi(n)$ formula koja se odnosi na prirodne brojeve (za takvu formulu kažemo da je aritmetički iskaz) i neka je $S = \{n \in N | \phi(n)\}$, tj. S je skup svih onih prirodnih brojeva n za koje važi $\phi(n)$. Tada se prethodna svojstva skupa S mogu preizraziti pomoću formule $\phi(n)$ na sledeći način:

1.1 Princip matematičke indukcije

Neka je $\phi(n)$ aritmetički iskaz. Pretpostavimo da za $\phi(n)$ važi:
(1) $\phi(0)$ baza indukcije
(2) $\forall n(\phi(n) \Longrightarrow \phi(n+1))$ induktivni korak

Tada je $\phi(n)$ istinito za svaki prirodan broj n.

2 Operatori sumiranja $\sum$ i proizvoda $\prod$

$$\sum_{i=m}^{n} a_i =_{def} a_m + a_{m+1} + \ldots + a_{n-1} + a_n, m \leq n$$

$$\prod_{i=m}^{n} a_i =_{def} a_m \cdot a_{m+1} \cdot \ldots \cdot a_{n-1} \cdot a_n, m \leq n$$

Osobine:

SUMIRANJE
(1) $\sum_{i=1}^{n} \alpha a_i = \alpha \sum_{i=1}^{n}$
(2) $\sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$
(3) $\sum_{i=1}^{n} = \sum_{i=1}^{n}$
(4) $\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij}$

PROIZVOD
(1) $\prod_{i=1}^{n} \alpha a_i = \alpha^n \prod_{i=1}^{n}$
(2) $\prod_{i=1}^{n} (a_i \cdot b_i) = \prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{n} b_i$
(3) $\prod_{i=1}^{n} = \prod_{i=1}^{n}$
(4) $\prod_{i=1}^{n} \prod_{j=1}^{m} a_{ij} = \prod_{j=1}^{m} \prod_{i=1}^{n} a_{ij}$

3 Algebarski identiteti, binomna formula, asocijativni i komutativni zakoni

Algebarski identiteti su formule oblika u = v, gde su u i v algebarski izrazi (termi). Algebarski identitet u = v je tačan ili istinit u nekoj algebarskoj strukturi akko se za zadate vrednosti učestvujućih promenljivih u termima u i v vrednosti u i v terma poklapaju.
Primeri:
$(x+y)^2 = x^2 + 2xy + y^2$
$x^2 - y^2 = (x-y)(x+y)$
$\vdots$

3.1 BINOMNA FORMULA

$$(x+y)^n =_{def} \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) x^{n-k}y^k = x^n + \left(\begin{array}{c} n \\ 1 \end{array} \right) x^{n-1}y^1 + \ldots + \left(\begin{array}{c} n \\ n-1 \end{array} \right) x^1 y^{n-1} + y^n$$

Binomni koeficijenti: $C_k^n = \left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!}$; $\left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n \\ n-k \end{array} \right)$

ASOCIJATIVNI ZAKONI: $(x+y)+z = x+(y+z)$ redosled izračunavanja
KOMUTATIVNI ZAKONI: $x+y = y+x$ ne utiče na rezultat

4 Nejednakost izmedju aritmetičke i geometrijske sredine

n=2:
$\sqrt{a_1 a_2} \leq \frac{a_1+a_2}{2}$ $\qquad x = \sqrt{a_1}, y = \sqrt{a_2}$

x, y :
$(x-y)^2 \geq 0$
$x^2 - 2xy + y^2 \geq 0$
$x^2 + y^2 \geq 2xy$
$a_1 + a_2 \geq 2\sqrt{a_1}\sqrt{a_2} / : 2$
$\frac{a_1+a_2}{2} \geq \sqrt{a_1 a_2}$

n=4:
$\sqrt[4]{a_1 a_2 a_3 a_4} \leq \frac{a_1+a_2+a_3+a_4}{4}$
$\frac{a_1+a_2+a_3+a_4}{4} = \frac{\frac{a_1+a_2}{2} + \frac{a_3+a_4}{2}}{2} \geq \sqrt{\sqrt{a_1 a_2} \cdot \sqrt{a_3 a_4}} \geq \sqrt[4]{a_1 a_2 a_3 a_4}$

$G(a_1, ..., a_n) \leq A(a_1, ..., a_n) \Longrightarrow G(b_1, ..., b_n) \leq A(b_1, ..., b_n)$

$\frac{b_1+b_2+...+b_{2n}}{2n} = \frac{\frac{b_1+...+b_n}{n} + \frac{b_{n+1}+...+b_{2n}}{n}}{2} \geq \frac{\sqrt[n]{b_1 \cdot ... \cdot b_n} + \sqrt[n]{b_{n+1} \cdot ... \cdot b_{2n}}}{2} \geq \sqrt{\sqrt[n]{b_1 \cdot ... \cdot b_n} \cdot \sqrt[n]{b_{n+1} \cdot ... \cdot b_{2n}}} =$
$\sqrt[2n]{b1 \cdot ... \cdot b_{2n}}$

Ovim smo dokazali nejednakost za sve brojeve n, oblika $n = 2^k; k \in \mathbf{N}^+$.

n=bilo koji broj koji nije oblika 2^k:
$\exists m \in \mathbf{N} \qquad 2^{m-1} < n < 2^m$
$n + l = 2^m$

Dati su nam brojevi $a_1, ..., a_n$
$a_{n+1} = a_{n+2} = ... = a_{2^m} = \frac{a_1+a_2+...+a_n}{n}$

2^m :
$\sqrt[2^m]{a_1 \cdot a_2 \cdot ... \cdot a_n \cdot a_{n+1} \cdot ... \cdot a_{2^m}} \leq \frac{a_1+...+a_n+a_{n+1}+...+a_{2^m}}{2^m}$
$\sqrt[2^m]{a_1 \cdot a_2 \cdot ... \cdot a_n \cdot (\frac{a_1+...+a_n}{n})^l} \leq \frac{n\cdot(\frac{a_1+...+a_n}{n})+l\cdot(\frac{a_1+...+a_n}{n})}{2^m} \Big/ ^{2^m}$
$a_1 \cdot a_2 \cdot ... \cdot a_n \cdot (\frac{a_1+...+a_n}{n})^l \leq (\frac{(n+l)(\frac{a_1+...+a_n}{n})}{2^m})^{2^m}$
$a_1 \cdot a_2 \cdot ... \cdot a_n \cdot (\frac{a_1+...+a_n}{n})^l \leq (\frac{a_1+...+a_n}{n})^{n+l}$
$a_1 \cdot a_2 \cdot ... \cdot a_n \leq (\frac{a_1\cdot a_2\cdot ....\cdot a_n}{n})^n \Big/ \sqrt[n]{}$
$\sqrt[n]{a_1 \cdot a_2 \cdot ... \cdot a_n} \leq \frac{a_1\cdot a_2\cdot ....\cdot a_n}{n}$

5 Rekurzivne definicije, Fibonačijev niz

Pomoću matematičke indukcije mogu se definisati i uvoditi novi matematički objekti. Definicije u kojima se koristi indukcija nazivamo induktivnim ili rekurzivnim definicijama.
Fibonačijev niz je niz brojeva čiji su početni elementi $f_1 = 0, f_2 = 1$, a svaki sledeći broj u nizu dobija se sabiranjem prethodna dva: $f_n = f_{n-1} + f_{n-2}$.

6 Linearna diferencna jednačina prvog reda

Jednačina oblika A(x)y' + B(x)y + C(x) = 0 koja deljenjem sa A(x) $\neq$ 0, postaje y' + P(x)y + Q(x) = 0 naziva se linearna diferencna jednačina prvog reda. Ukoliko je funkcija Q(x)=0, linearna diferencna jednačina se naziva homogenom.

7 Iskazna algebra

Iskazna algebra ili račun iskaza je dvoelementni skup 0,1, zajedno sa jednom unarnom i pet binarnih operacija. Služi za utvrđivanje tačnosti nekog iskaza.
p, q, r, ... su iskazna slova (promenljive čije su vrednosti matematički izrazi)
$\wedge, \vee, \Longrightarrow, \neg, \Longleftrightarrow, \veebar$ su iskazni veznici
Operacije su definisane iskaznim tablicama:

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

$\neg$	
0	1
1	0

$\Longrightarrow$	0	1
0	1	1
1	0	1

$\Longleftrightarrow$	0	1
0	1	0
1	0	1

$\veebar$	0	1
0	0	1
1	1	0

8 Definicija iskaznih formula

(1) 0, 1 su iskazne formule
(2) iskazne promenljive p, q, r, ... su iskazne formule
(3) ako su A i B iskazne formule, tada su i ¬A, A ∧ B, A ∨ B, A $\Longrightarrow$ B, A $\Longleftrightarrow$ B i A $\veebar$ B iskazne formule.
(4) svaka iskazna formula dobija se primenom prethodna tri pravila

9 Tautologije - metode dokazivanja i primeri

Iskazna formula A (p, q, r, ...) je tautologija akko za sve vrednosti p=α, q=β, r=γ, ... (α, β, $\gamma \in \{0,1\}$), vrednost A je 1, odn. A (α, β, γ, ...) $\equiv 1$.
Metode dokazivanja: tablični metod, metod diskusije po iskaznom slovu, metod tabloa, metod svođenja na apsurd.
Primeri tautologija:

p $\Longrightarrow$ p, p ∨ ¬p (princip isključenja trećeg), (p ∧ q) ∧ r $\Longleftrightarrow$ p ∧ (q ∧ r) (asocijativnost konjukcije), (p ∧ q) $\Longleftrightarrow$ (q ∧ p) (komutativnost konjukcije), ¬¬p $\Longleftrightarrow$ p, ¬(p∧q) $\Longleftrightarrow$ ¬p ∨ ¬q, ¬(p∨q) $\Longleftrightarrow$ ¬p ∧ ¬q (de Morganovi zakoni)

10 Teorema o disjunktivnoj normalnoj formi

Literal je p ili ¬p. Atom je konjukcija literala. Disjunktivna normalna forma (DNF) je disjunkcija atoma A.
Formula F je u DNF, ako je F = A1 ∨ A2 ∨ ... ∨ An ; A = $p_1^{\alpha_1} \wedge p_1^{\alpha_2} \wedge ... \; p_1^{\alpha_k}$, p je iskazno slovo, α_1, ..., $\alpha_k \in \{0,1\}$.

$$p^{\alpha} = \begin{cases} p & \text{ako je } \alpha = 1 \\ \neg p & \text{ako je } \alpha = 0 \end{cases}$$

Teorema: Svaka iskazna formula ima SDNF. Razlika između DNF i SDNF je u tome da u SDNF u svakom atomu postoje svi literali te iskazne formule.

11 Kvantori

Kvantori su kvalifikatori u jeziku. Njihova semantika je:
∀ - 'za svaki', univerzalni kvantor
∃ - 'postoji', egzistencijalni kvantor
Uglavnom su vezani za promenljivu: ∀x, ∃x.

12 Definicija predikatskih formula

*****
Neka je skup L jezik predikatskog računa. L = ConstL U FunL U RelL , pri čemu su ConstL skup simbola konstanti ({0, 1, ...}), FunL skup simbola algebarskih operacija ({+, *, ...}) i RelL skup simbola relacija ({≤, ∼, ...}).
*****

Termi (algebarski izrazi) se grade od simbola konstanti, operacija i relacija, npr. L = {0, 1} U {+ ,*} U {$\leq$}.
(1) Promenljive (dodeljuju im se vrednosti iz domena) su termi i simboli konstanti su termi
(2) Ako su u i v termi, onda su u+v, u*v termi
(3) Svaki term dobija se konačnom primenom prethodna dva pravila
Atomične formule su: u = v, u $\leq$ v, ...

Predikatske formule su:
(1) Atomične formule su predikatske formule
(2) Ako su ϕ i λ predikatske formule, tada su i $\phi \wedge \lambda$, $\phi \vee \lambda$, $\neg\phi$, $\phi \Longrightarrow \lambda$, ... takođe predikatske formule
(3) Ako je ϕ formula, tada su i $\forall x\phi$ i $\exists x\phi$ takođe predikatske formule
(4) Svaka predikatska formula dobija se konačnom primenom prethodna 3 pravila
Primeri:
$\forall x \exists y(x + y = 1)$
$\forall x(\neg x = 0) \Longrightarrow \exists y(x \cdot y = 1)$
$\exists x(x^2 - 2x + 2 = 0)$
L $\cup$ {1,2,3,. . . ,-1,-2,-3,. . . }=L'

13 Pojam valuacije

Valuacija je bilo koja funkcija koja skupu iskaznih primenljivih dodeljuje vrednosti 0 ili 1.
ϕ(p1,. . . ,pn)
$\phi(\alpha 1, \ldots, \alpha n)$
Valuacija je svako preslikavanje

$$\alpha = \begin{pmatrix} p_1, \ldots, p_n \\ \alpha_1, \ldots, \alpha_n \end{pmatrix}$$

α : P $\longrightarrow$ 2, gde je P skup iskaznih slova $\{p_1, p_2, ...\}$

14 Valjane formule, primeri

Valjane formule su formule čija opšte važeća istinitost nije uslovljena načinom interpretacije nelogičkih simbola, već samoj logičkoj strukturi formule. Valjane formule izražavaju zakone ispravnog logičkog zaključivanja na jeziku relacijskih struktura.
Ako je formula A tačna u nekoj interpretaciji D, onda ona opisuje izvesno svojstvo strukture D. Međutim, ako je formula A tačna u svakoj interpretaciji, onda ona više ne opisuje svojstvo neke strukture, već opšte svojstvo svih struktura, tj. opšte pravilo zaključivanja. Takve formule, koje su tačne u svim interpretacijama nazivaju se opšte važećim formulama ili valjanim formulama.
Primeri:
$\neg\exists x\phi(x) \Longrightarrow \forall x\ \neg\phi(x)$
$\neg\forall x\phi(x) \Longrightarrow \exists x\ \neg\phi(x)$
$\neg\forall x\ \neg\phi(x) \Longrightarrow \exists x\phi(x)$

15 Teorija algebarskih polja

Teorija polja je matematička disciplina koja proučava polja.
(1) (x + y) + z = x + (y + z) asocijativni zakon (u aditivnoj formi)
(2) x + y = y + x komutativni zakon
(3) x + 0 = 0 + x = x zakon neutralnog elementa
(4) x + (-x) = (-x) + x = 0 zakon suprotnog elementa

Svaka algebarska struktura **A** na kojoj su definisane algebarske operacije + i – i postoji konstanta 0, tj. **A** = (A, +, –, 0) i u kojoj važe identiteti (1) – (4) naziva se Abelovom ili komutativnom grupom. Skup A je domen algebre **A**, dakle skup na kojem su definisane operacije +, · i 0 ∈ A.

Komutativni prsteni su algebre **A** = (A, +, –, ·, 0, 1) koje zadovoljavaju sledeće zakone:

(1) – (4)
(5)$(x \cdot y) \cdot z = x \cdot (y \cdot z)$
(6)$x \cdot y = y \cdot x$
(7)$x \cdot 1 = 1 \cdot x = x$
(8)$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ distributivni zakon

Uzimamo da je $x - y =_{def} x + (-y)$
Polja su komutativni prsteni koji zadovoljavaju i ovu aksiomu:
$x \neq 0 \Longrightarrow \exists y(x \cdot y = 1)$
ili $x \neq 0 \Longrightarrow x \cdot x^{-1}$ ako je uvedena operacija inverznog elementa.

16 Osnovne skupovne operacije, definicije i osobine

Skupovna operacija može biti shvaćena kao postupak kojim se skupu/skupovima pridružuje skup. Georg Kantor je 1873. godine formulisao koncept skupova:
$X = \{a|\phi(a)\}$
Skupovne operacije su: unarna operacija, tzv. komplementiranje i četiri binarne, tzv. presek, unija, razlika i simetrična razlika.
(1) Komplement skupa A, u oznaci A^c, je skup svih elemenata univerzalnog skupa koji ne pripadaju skupu A.

$$A^c = \{x \in U | x \notin A\}$$

(2) Presek skupova A i B, u oznaci $A \cap B$, je skup svih elemenata univerzalnog skupa koji pripadaju i skupu A i skupu B.

$$A \cap B = \{x \in U | x \in A \wedge x \in B\}$$

(3) Unija skupova A i B, u oznaci $A \cup B$, je skup svih elemenata univerzalnog skupa koji pripadaju skupu A ili skupu B.

$$A \cup B = \{x \in U | x \in A \vee x \in B\}$$

(4) Razlika skupova A i B, u oznaci $A\backslash B$, je skup svih elemenata univerzalnog skupa koji pripadaju skupu A, a ne pripadaju skupu B.

$$A\backslash B = \{x \in U | x \in A \wedge x \notin B\}$$

U opštem slučaju ne važi jednakost $A\backslash B = B\backslash A$.

(5) Simetrična razlika skupova A i B, u oznaci $A \triangle B$ je skup svih elemenata univerzalnog skupa koji pripadaju ili skupu A ili skupu B.

$$A \triangle B = \{x \in U | x \in A \veebar x \in B\}$$

Uredjen par $(x, y) =_{def} \{\{x\}, \{x, y\}\}$

16.1 Osobine skupovnih operacija

Za svaki skup A važi:

- Idempotentnost: $A \cup A = A, A \cap A = A$

Za svaka dva skupa A i B važi:

- Komutativnost: $A \cap B = B \cap A$, A i B važi $A \cup B = B \cup A$

Za svaka tri skupa A, B, i C važi:

- Asocijativnost: $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$
- Distributivnost: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Osobine komplementa, univerzalnog skupa i praznog skupa:

- $(A^c)^c = A, A^c = U\backslash A, A \cup A^c = U, A \cap A^c = \oslash, \oslash^c = U, U^c = \oslash, (A \cap B)^c = A^c \cup B^c, (A \cup B)^c = A^c \cap B^c$
- $A \cup U = U, A \cap U = A$
- $A \cup \oslash = A, A \cap \oslash = \oslash$

16.2 Beskonačne skupovne operacije

$$A_1 \cup A_2 \cup \ldots \cup A_n = \bigcup_{n \in \mathbf{N}} A_n$$

$$A_1 \cap A_2 \cap \ldots \cap A_n = \bigcap_{n \in \mathbf{N}} A_n$$

$$x \in \bigcup_{n \in \mathbf{N}} A_n \Longleftrightarrow (\exists n \in \mathbf{N}) x \in A_n$$

$$x \in \bigcap_{n \in \mathbf{N}} A_n \Longleftrightarrow (\forall n \in \mathbf{N}) x \in A_n$$

17 Skupovni identiteti, metode dokazivanja

Skupovni identiteti predstavljaju jednakost dva skupa. To su dobro zapisani izrazi u kojima učestvuju skupovi $A, B, C, \ldots$, operacije $\cap, \cup, ^c, \ldots$

Formalna definicija skupovnog izraza (terma):

(1) $\oslash, A, B, C, \ldots$ su skupovni izrazi.

(2) Ako su u i v skupovni izrazi, onda su i $u \cap v, u \cup v, u^c, u \backslash v, u \triangle v$ skupovni izrazi.

(3) Svaki skupovni izraz dobija se primenom prethodna dva pravila.

Skupovni izraz L = D važi akko vrednost od L jeste identički jednaka vrednosti od D za ma kakav izbor skupova (skupovne promenljive zameniti konkretnim skupovima).

Za svako proizvoljno x važi $x \in L \Longleftrightarrow x \in D$, tj. L i D imaju iste elemente.

A = B akko za svako svojstvo ϕ važi: $\phi(A) \Longleftrightarrow \phi(B)$ (jednakost po intenziji = značenju).

A = B akko A i B imaju iste elemente: $x \in A \Longleftrightarrow x \in B$ (jednakost po ekstenziji = obimu).

17.1 Metode dokazivanja skupovnih jednakosti

(1) Dijagram za ograničen broj skupova
(2) Tabele pripadnosti (svođenje na tablični metod dokazivanja tautologija)
(3) Dokaz izraza na osnovu definicija, aksioma, ...
(4) Metod karakterističnih funkcija

18 Aksiome teorije skupova

Ove aksiome su naveli Rasel, Frenkel i Zermelov početkom 20. veka.

(A1) Ako su a, b skupovi, tada je {a, b} takodje skup.

(A2) Ako su a, b skupovi, tada su $\{a \cup b\}$, $\{a \cap b\}$, ... takodje skupovi.

(A3) Ako je a skup, tada je i $P(a) = \{X | X \subseteq a\}$ takodje skup i on se naziva Partitivni skup skupa a.

(A4) Prazan skup ($\oslash$) je takodje skup.

(A5) Aksioma beskonačnosti: Postoji skup X takav da u njemu leži $\oslash$. Ako $y \in X$, tada $y' \in X$; $y' = y \cup \{y\}$.

(A6) Aksioma restrikcije: Ako je X skup, ϕ neko svojstvo, tada je i $Y = \{x \in X | \phi(x)\}$ takodje skup.

(A7) Ako je data disjunktna familija skupova, svi su neprazni, tada postoji X koji bira tačno po jedan element iz svakog člana('relacija transferzale').

19 Dekartov proizvod, operacija partitivnog skupa

19.1 Dekartov proizvod

Ako su A i B skupovi, onda se skup uredjenih parova sa prvom koordinatom iz A, a drugom koordinatom iz B naziva Dekartov proizvod skupova A i B, i označava se sa AxB:

$$AxB =_{def} \{(a,b)|a \in A, b \in B\}$$

AxBxC = (AxB)xC

Važi distributivnost Dekartovog proizvoda u odnosu na operacije presek, unija, ...: Ax(B $\cup$ C) = (AxB) $\cup$ (AxC)

Dekartov proizvod n skupova $A_1, \ldots, A_n$ u oznaci $A_1 x \ldots x A_n$ ili

$$\prod_{i=1}^{n} A_i =_{def} \{f : I \longrightarrow \bigcup_{i \in I} A_i | f(i) \in A_i, \forall i \in I\}$$

je skup svih uredjenih n-torki sa koordinatama iz odgovarajućih skupova.

$$A_1 x \ldots x A_n =_{def} \{(a_1, ..., a_n)|a_1 \in A_1, ..., a_n \in A_n\}$$

Ako je bilo koji od skupova $A_1, ..., A_n$ prazan, onda je po definiciji prazan i skup $A_1 x \ldots x A_n$. Ako je $A_1 = A_2 = ... = A_n = A$, onda se odgovarajući Dekartov proizvod obeležava sa A^n i zove se Dekartov n-ti stepen skupa A, gde je $A^1 = A$. Ako je $A \neq \oslash$, onda je Dekartov stepen zgodno proširiti i za n=0, na sl. način: $A^0 =_{def} \{\oslash\}$, odakle sledi da A^0 je jednoelementni skup.

19.2 Operacija partitivnog skupa

Skup čiji su elementi svi podskupovi jednog skupa naziva se partitivni skup.

$$P(X) =_{def} \{A|A \subseteq X\}$$

Prazan skup je element svakog partitivnog skupa. Skup X je element P(X). Za razliku od praznog skupa koji nema elemenata, njegov partitivni skup se sastoji od jednog elementa: $P(\oslash) = \{\oslash\}$. Broj elemenata P(X) je 2^n, ukoliko skup X ima N elemenata.

20 Binarne relacije, kompozicija binarnih relacija, inverzna binarna relacija

Binarne relacije izmedju skupova A i B su podskupovi Dekartovog proizvoda dva skupa A i B.

$$\rho = \{(a,x),(b,y),...\} \in AxB \qquad (A = \{a,b,c\}, B = \{x,y\})$$

Inverzna relacija: Neka je ρ neka binarna relacija izmedju A i B. Relacija σ koja je relacija izmedju B i A, takva da je $(x,y) \in \sigma$ akko $(y,x) \in \rho$, tj. $\sigma = \{(x,y)|(y,x) \in \rho, y \in A, x \in B\}$ naziva se inverzna relacija relacije ρ. Nekada se označava i kao ρ^{-1}.

Kompozicija relacija: Neka je σ relacija izmedju skupova A i B, i ρ relacija izmedju skupova B i C. Tada je relacija τ kompozicija relacija izmedju relacija ρ i σ u oznaci $\tau = \rho \circ \sigma$, ako za

$$(a,c) \in \tau \Longleftrightarrow_{def} \exists b((a,b) \in \sigma \wedge (b,c) \in \rho),$$

odnosno

$$\tau = \rho \circ \sigma = \{(a,c) \in A\text{x}C | \exists b \in B, (a,b) \in \sigma \wedge (b,c) \in \rho\}$$

Važi:

Asocijativnost kompozicije: $(\rho \circ \sigma) \circ \tau = \rho \circ (\sigma \circ \tau)$

21 Funkcije, osobine (kompozicija, 1-1 i na preslikavanja)

Neka su A i B skupovi. Funkcija iz A u B je $f \subseteq A\text{x}B$ tako da za svako $x \in A$ postoji tačno jedno $y \in B$, tako da $(x,y) \in f$. Funkcija ili preslikavanje je uredjena trojka (A, B, f), gde su prve dve koordinate dati skupovi A i B, a treća je f kojom se svakom elementu skupa A dodeljuje tačno jedan element skupa B. Zapisuje se $f : A \longrightarrow B$.

Skup A je domen funkcije f. To je skup sa kojeg vršimo preslikavanje. Skup B je kodomen funkcije f. To je skup na koji vršimo preslikavanje.

Preslikavanje ili funkcija je zapravo relacija sa osobinom da svaki element skupa A stavlja u relaciju sa tačno jednim elementom skupa B.

$(\forall x \in A)(\exists y \in B)(x,y) \in f$ i $(\forall x \in A)(\forall y,z \in B)(x,y) \in f \wedge (x,z) \in f \Longrightarrow y = z$.

Postoji različit zapis funkcija:

$f = \{(x,x^2) | x \in \mathbf{N}\}$
$f = \{(0,0),(1,1),(2,4),...\}$
$f : \mathbf{N} \longrightarrow \mathbf{N}$
$f = \begin{pmatrix} 0 & 1 & 2 & \dots \\ 0 & 1 & 4 & \dots \end{pmatrix}$
f $= \begin{pmatrix} x \\ x^2 \end{pmatrix}$
$f =< f(x) | x \in \mathbf{N} >$
$f =< x^2 | x \in \mathbf{N} >$
Najčešći zapis je: $f(x) = x^2$

Formalna definicija:
(1) $f \subseteq A\text{x}B$
(2) $\forall a \in A : \exists b \in B, t.d.(a,b) \in f$
(3) $\forall a \in A \wedge \forall b,b' \in B \wedge (a,b),(a,b') \in f \Longrightarrow b = b'$

Skup vrednosti funkcije f: $f(A) = \{f(a) | a \in A\}$

Može da važi i za podskup $X \subseteq A$ i to je slika skupa X: $f[X] = \{f(x) | x \in X\}$

21.1 Inverzna funkcija

Dati su skupovi A i B i funkcija $f : A \longrightarrow^{na}_{1-1} B$. Možemo uvesti funkciju $f^{-1} : B \longrightarrow A$.
$y = g(x) \Longleftrightarrow x = f(y) \qquad g = f^{-1} = \{(x,y) | (y,x) \in f\}$.

Inverzne funkcije su simetrične u odnosu na $x = y$ pravu.

21.2 Inverzna slika

Ako imamo skupove A i B i preslikavanje $f : A \longrightarrow B$, inverzna slika funkcije f je funkcija u oznaci f^{-1}.
$f^{-1}[Y] = \{x \in A | f(x) \in Y\}$.

Osobine:

$\forall X, Y \subseteq A$
$f[X \cup Y] = f[X] \cup f[Y]$
$f[X \cap Y] \subseteq f[X] \cap f[Y]$

$\forall X, Y \subseteq B$
$f^{-1}[X \cup Y] = f^{-1}[X] \cup f^{-1}[Y]$
$f^{-1}[X \cap Y] \subseteq f^{-1}[X] \cap f^{-1}[Y]$

21.3 Injekcija

Preslikavanje ili funkcija f skupa A u skup B, u oznaci $f : A \longrightarrow B$ je injekcija ili '1-1' ako za bilo koja dva razlicita elementa $x_1, x_2 \in A$ i njihove slike su različite, tj. $f(x_1) \neq f(x_2)$:

$$(\forall x_1, x_2 \in A)(x_1 \neq x_2) \Longrightarrow (f(x_1) \neq f(x_2))$$

Ponekad pišemo $f : A \longrightarrow_{1-1} B$.

21.4 Surjekcija

Preslikavanje ili funkcija f skupa A u skup B, u oznaci $f : A \longrightarrow B$ je surjekcija ili 'na' ako za svaki element $b \in B$ postoji $a \in A$ takav da je $b = f(a)$, tj:

$$(\forall b \in B)(\exists a \in A) \ \ t.d. \ \ (b = f(a))$$

Ponekad pišemo $f : A \longrightarrow^{na} B$.

Funkcija koja je istovremeno i '1-1' i 'na' zove se bijekcija.

21.5 Kompozicija funkcija

Kompozicija funkcija, proizvod ili slaganje funkcija je binarna operacija:

$$f : A \longrightarrow B \wedge g : B \longrightarrow C \Longrightarrow h = g \circ f, h : A \longrightarrow C$$

za bilo koje date skupove A, B, i C.

$$h(x) =_{def} g(f(x)) \quad odnosno \quad (g \circ f)(x) =_{def} g(f(x))$$

Slaganje funkcija je asocijativnog karaktera:

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

Dokaz:

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

Ako su date funkcije $f : A \longrightarrow B$ i $g : X' \longrightarrow B$,
$f = g$ akko $X = X' \wedge \forall x \in X\ f(x) = g(x)$
$f = g$ akko: (1) $dom(f) = dom(g)$ i (2) f i g imaju iste vrednosti za elemente domena

Funkcije (A, B, f) i (C, D, g) su jednake akko je $A = C, B = D$ i $f = g(\Longleftrightarrow \forall x \in A = C, f(x) = g(x))$

$g \circ f \neq f \circ g$, u opštem slučaju.

Teorema: Neka su $f : A \longrightarrow B$, $g : B \longrightarrow C$:
(1) proizvod 1-1 funkcija je 1-1 funkcija (2) proizvod na funkcija je na funkcija (3) proizvod bijektivnih funkcija je bijektivna funkcija

22 Permutacije konačnih skupova, računanje proizvoda i inverzna permutacija

Dat je skup X i funkcija $f : X \longrightarrow^{na}_{1-1} X$. Funkciju f nazivamo permutacijom skupa X.
Skup svih permutacija skupa X označavamo:
$Sym(x) = \{p | p : X \longrightarrow^{na}_{1-1} X\}$.

Grupa permutacija je simetrična grupa skupa X, npr.
Grupa $(Sym(X), 0, -1, i)$

$X = \{1, 2, ..., n\}$, $p : X \longrightarrow^{na}_{1-1} X$, $q : X \longrightarrow^{na}_{1-1} X \Longrightarrow q \circ p$ je takodje 1-1 i na funkcija.

$p, q \in Sym(X) \Longrightarrow q \circ p \in Sym(X)$

Ako je $p : X \longrightarrow^{na}_{1-1} X$ i $p^{-1} : X \longrightarrow^{na}_{1-1} X$, onda $p \in Sym(X) \Longrightarrow p^{-1} \in Sym(X)$

22.1 Proizvod permutacija

Ako su date dve permutacije p i q, primenjivanjem prvo q, a zatim i p bi dalo isti rezultat kao i primena samo jedne neke permutacije r. Proizvod permutacija p i q se tada definiše kao permutacija r.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$

Rešenje: Prvo se primeni permutacija q na element 1, odnosno $1 \longrightarrow 3$, pa se onda primeni permutacija p na dobijeni element, odnosno $3 \longrightarrow 1$, pa se na kraju dobije $1 \longrightarrow 1$. Postupak se ponavlja za ostale elemente.

22.2 Inverzna permutacija

Inverzna permutacija je permutacija funkcija, tačnije bijekcija, dakle ima svoju inverznu funkciju. To je permutacija u kojoj se razmenjuje svaki broj i broj mesta koji on zauzima.

$p^{-1} = \begin{pmatrix} 2 & 3 & 1 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$

23 Relacije ekvivalencije i particije skupova, primeri

23.1 Relacija ekvivalencije

Binarna relacija $\sim$ ('tilda') je relacija ekvivalencije domena A ako ispunjava sledeće karakteristike:

- refleksivnost: $a \sim a, \forall a \in A$
- simetričnost: $a \sim b \Longrightarrow b \sim a, \forall a, b \in A$
- tranzitivnost: $(a \sim b \wedge b \sim c) \Longrightarrow a \sim c, \forall A, b, c \in A$

Relacija ekvivalencije je binarna relacija nad domenom A: $\sim \subseteq A \mathrm{x} A; (a, b) \in \sim$ za neke $a, b \in A$.

Primeri:

(1) jednakost
(2) paralelnost pravih: $p \sim q$ akko $p||q$.
(3) kongruencija po modulu n ($n \in \mathbf{N}$): $x =_n y$ ili $x \equiv y(modn)$.

23.1.1 Klasa ekvivalencije

Klasa ekvivalencije elementa $x \in A$, u oznaci $x/\sim$, [x] ili C_x, je skup svih elemenata y koji su u relaciji sa kojima je x u relaciji:

$$x/\sim =_{def} \{y \in A | x \sim y\}, x \in A$$

23.1.2 Particija skupa

Particija skupa A je familija χ podskupova od A:
(1) $X \in \chi \Longrightarrow X \notin \oslash$
(2) $X, Y \in \chi, X \neq Y \Longrightarrow X \cap Y \neq \oslash$
(3) $\bigcup_{X \in \chi} X = A$

Transverzala ili izborni skup particije χ je $T \subseteq A$ tako da T bira tačno po jedan element iz svakog člana particije χ.

$\chi = \{X_t | t \in T\}, t \in X_t$

Broj članova skupa A jednak je sumi broja članova svakog elementa: $|A| = \sum_{t \in T} |X_t|$

23.2 Parcijalno i linearno uredjeni skupovi

Relacija $\preceq$ je relacija uređenja na A ako je refleksivna, antisimetrična i tranzitivna

- refleksivnost: $a \preceq a, \forall a \in A$
- antisimetričnost: $a \preceq b \wedge b \preceq a \Longrightarrow a = b, \forall a, b \in A$
- tranzitivnost: $(a \sim b \wedge b \sim c) \Longrightarrow a \sim c, \forall A, b, c \in A$

Primeri:

(1) Haseovi dijagrami

(2) $(P(x), \subseteq)$
$y \in P(x)$
$y \subseteq y$
$y \subseteq z, z \subseteq y \Longrightarrow y = z$
$y \subseteq z, z \subseteq u \Longrightarrow y \subseteq u$

(3) Puno binarno drvo: Drvo $(T, \leq, v)$ predstavlja parcijalan uredjen sistem koji ima:
- najmanji element
- (u smislu konačnih skupova) $\forall a \in T$, [v, a] je lanac tj. linearno uredjen skup (svaki ima svog pretka)
$[v, a] = \{x \in T | 0 \leq x \leq a\}$ $\qquad x, y < a \Longrightarrow (x \leq y) \vee (y \leq x)$

(4) Grupa $(N, |)$, gde je | relacija $x|y$:
$x|x$
$x|y, y|x \Longrightarrow x = y$
$x|y, y|z \Longrightarrow x|z$

- a ∈ A je najmanji element ako za x ∈ A važi $a \preceq x$
- b ∈ A je najveći element ako za x ∈ A važi $x \preceq b$
- a ∈ A je minimalni element ako za x ∈ A za koje važi $a \preceq x$, važi i $x = a$
- b ∈ A je maksimalni element ako za x ∈ A za koje važi $x \preceq b$, važi i $x = b$

Linearno uredjeni skupovi su oni koji zajedno sa relacijom $\leq$ čine grupu $(A, \leq)$, takvu da je:
(1) $\leq$ je relacija uredjenja (RAT)
(2) $\leq$ ispunjava još i:
$x \leq y \vee y \leq x, x, y \in A$
$x < y \vee x = y \vee y < x$

24 Konačni i beskonačni skupovi i kardinalni broj

Skupovi X i Y su ekvipotentni (iste kardinalnosti, iste moći) akko$_{def}$ postoji $f : X \longrightarrow^{na}_{1-1} Y$. Ako skupovi imaju istu kardinalnost, to se zapisuje: $|X| = |Y|, X \approx Y$, gde je oznaka $|X|$ kardinalni broj skupa X (isto važi i za skup Y).

$$f : X \longrightarrow^{na}_{1-1} Y \Longrightarrow |X| = |Y|$$

$$X \approx Y \Longleftrightarrow_{def} \bigvee_{f} g : X \longrightarrow^{na}_{1-1} Y$$

$\approx$ je relacija ekvivalencije.

Skup je konačan akko postoji postoji bijekcija $F : \{1, 2, ..., n\} \longrightarrow X$ za neko $n \in N$.

$|X| = n; X = \{f(1), f(2), ..., f(n)\} = \{x_1, x_2, ..., x_n\}$

Primeri konačnih skupova:
(1) $|\{1, 2, ..., n\}| = n$
(2) $X = \{k \in \mathbf{N} | n \leq k \leq m\}$
(3) $|A| = n; |P(A)| = 2^n$
(4) $\mathbf{S}_n$ - permutacije skupa $\{1, 2, ..., n\}; |\mathbf{S}_n| = n!$
(5) $|A| = n; C = \{X \subseteq A | |x| = k\}; |C| = \begin{pmatrix} n \\ k \end{pmatrix}$ - kombinacije bez ponavljanja

BESKONAČNI SKUPOVI

Definicije beskonačnih skupova:

Skup je beskonačan ako nije konačan.
Skup je beskonačan ako možemo uslikati N u njega funkcijom 1-1.
Ako možemo preslikati skup u njegov pravi deo, onda je on beskonačan.

Primeri beskonačnih skupova:
1) N={1,2,...}
2) $X \subseteq Y$, X je beskonačan skup, pa je i Y beskonačan
3) $f : N \longrightarrow Y$, Z je beskonačno

24.1 Dirikleov princip za konačne skupove

Ako $|x_1 \cup ... \cup x_n| \geq n + 1$ tada za neko i važi $|x|_i \geq 2$.

Posledice:
(1) $f : A \longrightarrow A$; A je konačan skup, tada $f : A \longrightarrow^{na}_{1-1} A$

$a_1, a_2, ..., a_n$	$A \setminus \{a_i\}$	$n - 1$
$a'_1, a'_2, ..., a'_n$	$A \setminus \{a'_i\}$	$n - 1$

(2) $f : A \longrightarrow^{na} A$ tada $f : A \longrightarrow^{na}_{1-1} A$.

25 Bulove algebre

Bulova algebra je algebarska struktura $\mathbf{B} = (B, \vee, \wedge, ', 0, 1)$.

B - domen (neprazan skup)
$\vee$ - bulovska disjunkcija
$\wedge$ - bulovska konjunkcija
' - bulovski komplement
0,1 - Bulove konstante, $0, 1 \in B$

Struktura zadovoljava sledeće aksiome:
1) $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ - zakon asocijacije
$(x \vee y) \vee z = x \vee (y \vee z)$
2) $x \wedge y = y \wedge x$ - zakon komutativnosti
$x \vee y = y \vee x$
3) $x \wedge (x \vee y) = x$ - zakon apsorpcije
$x \vee (x \wedge y) = x$
4) $x \vee 0 = x$ - zakon neutralnog elementa
$x \wedge 1 = x$
5) $x \vee x' = 1$ - zakon komplementa
$x \wedge x' = 0$
6) $0 \neq 1$ - svaka Bulova algebra ima dva elementa

Primeri:
(1) Iskazna logika: $\mathbf{B}_2 = (B_2, \vee, \wedge, ', 0, 1)$
(2) $\mathbf{B}_2^n = (B_2^n, \vee, \wedge, ', 0, 1), B_n^2 = \{(\alpha_1, ..., \alpha_n) | \alpha_1, ..., \alpha_n \in \{0, 1\}\}$

26 Bulovski identiteti, de Morganove jednakosti

Svi identiteti iz aksioma bi mogli da se ubace i ovde
$x \wedge x = x$
$x \vee x = x$
$x \wedge 0 = 0$
$x \vee 1 = 1$
$0' = 1$
$1' = 0$
$(x')' = x$

De Morganove jednakosti:
$(x \wedge y)' = x' \vee y'$
$(x \vee y)' = x' \wedge y'$

27 Euklidov algoritam

Euklidov algoritam se koristi za određivanje najvećeg zajedničkog delioca dva cela broja. NZD dva cela broja je broj koji deli ta dva broja bez ostatka.
$a, b \in N, b \neq 0$

$a = b \cdot q_1 + r_1, 0 \leq r_1 < b$
$b = r_1 \cdot q_2 + r_2, r_2 < r_1$
$r_1 = r_2 \cdot q_3 + r_3, r_3 < r_2$
$\vdots$
$r_{n-2} = r_{n-1} \cdot q_n + r_n, r_n < r_{n-1}$
$r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}, r_{n+1} = 0$
Postupak se mora završiti jer u **N** nema beskonačnih regresija (opadajućeg niza).
NZD je poslednji nenula ostatak, pa je NZD(a,b) = r_n

28 Linearna diofantovska jednačina

$$d = \alpha a + \beta b$$

Opšti oblik linearne diofantovske jednačine: $ax + by = c$
Diofantovska jednačina $ax + by = c$ ima rešenje akko $d = NZD(a, b) \wedge d|c$ oblika $x = (\frac{c}{d}) \cdot \alpha + (\frac{b}{d}) \cdot t$ i $y = (\frac{c}{d}) \cdot \beta - (\frac{a}{d}) \cdot t$,
gde je t neki ceo broj, a α i β su dobijeni iz Euklidovog algoritma. Ako d ne deli c, onda jednačina nema rešenja.