Logika in Množice

Vid Drobnič

Kazalo

1 Množice

A - množica
$x \in A$ - x je element A

Načelo ekstenzionalnosti:

Če imata množici iste elemte, sta enaki.

Končna množica: $\{a, b, c, ...z\}$, primer:

$$A = \{1, 2, 5\}$$

$$B = \{2, 1, 1, 5\}$$
$$A = B$$

Prazna množica: $\{\}$ oznaka $\varnothing$

Enojec: $\{a\}$

Dvojec ali neurejeni par: $\{a, b\}$ za katerikoli a in b $\Rightarrow$ lahko sta enaka $\Rightarrow$ enojec je posebni primer dvojca.

$$\{c, c\} = \{c\}$$

Standardni enojec: $1 = \{()\}$

2 Preslikava ali Funkcija

(1) **domena**: množica A

(2) **kodomena**: množica B

(3) **prirejanje**: pove kako elementom iz A priredimo elemnte iz B

- **Celovitost:** vsakemu elementu iz A priredi vsaj 1 element iz B
- **Enoličnost:** če sta elementu x prirejena y_1 in y_2, potem velja $y_1 = y_2$

$A \to B$ (brezimna)preslikava iz A v B
A - domena
B - kodomena

$f : A \to B$ funkcija (preslikava) poimenovana f
$A \xrightarrow{f} B$

Funkcijski predpis

$$x \mapsto 1 + x^2$$

x se slika v $1 + x^2$

$$f : x \mapsto 1 + x^2$$
$$f(x) = 1 + x^2$$

Opomba: funkciji manjka še domena in kodomena.

$$\{1, 2, 5\} \to \{1, 2, 3, 4, ...10\}$$
$$x \mapsto 1 + x^2$$

$g(2)$: g uporabimo ali apliciramo na argumentu 2

$g : \mathbb{R} \to \mathbb{R}$: predpis
g: preslikava
$g(3)$: število
$g(x)$: število

(1) $x \mapsto ax + b$ (x je vezana spremenljivka, a in b sta parametra)

(2) $a \mapsto ax + b$

(3) $y \mapsto ay + b$

(1) in (2) sta isti preslikavi.

$$g : \mathbb{R} \to \mathbb{R}$$

$$g(x) = 1 + x^3$$
$$g(7) = 1 + 7^3$$

Opomba: ni treba izračunati.

$$\mathbb{R} \to \mathbb{R}$$
$$x \mapsto 1 + x^3$$
$$(x \mapsto 1 + x^3)(7) = 1 + 7^3$$
$$(x \mapsto ax + b)(7) = 7x + b$$

Uporaba funkcije - **aplikacija.**

Preslikave $\varnothing \to A$?

$$\varnothing \to \{1, 2, 3\}$$

Prirejanje "vsi elemtni domene se presliakjo v 1".

$$x \mapsto 1$$
$$x \mapsto 2$$

Preslikavi sta enaki.

Sklep: iz $\varnothing \to A$ imamo natanko eno preslikavo.

Opomba: Za vse elemte prazne množice velja karkoli.

$$\mathbb{R} \to \mathbb{R}$$
$$x \mapsto x \cdot x$$
$$x \mapsto x \cdot x + x - x$$

Preslikavi sta enaki.

Načelo ekstenzionalnosti preslikav:

Če imata preslkavi enaki domeni in enaki kodomeni, ter prirejata elementom domene enake vrednosti, potem sta enaki.

$$f : A \to B$$
$$g : C \to D$$

Če $A = C$ in $B = D$ in za vsak $x \in A$ velja $f(x) = g(x)$, potem $f = g$.

Drugače povedano (se izpelje):
Če $A = C$ in $B = D$ in za vsak $x_1, x_2 \in A$ velja, da iz $x_1 = x_2$ sledi: $f(x_1) = g(x_2)$, potem $f = g$.

3 Aritmetika Množic

3.1 Kartezični produkt ali zmnožek

A in B množici
$A \times B$ zmnožek

Elementi $A \times B$ so urejeni pari (a, b), kjer sta $a \in A$ in $b \in B$.

Projekciji:

$$\pi_1 : A \times B \to A$$

$$\pi_2 : A \times B \to B$$

Enačbe:

Za vse $a \in A$ in $b \in B$ velja:

$$\pi_1(a, b) = a$$

$$\pi_2(a, b) = b$$

Ekstanzionalnost za zmnožke:

Za vse $p, q \in A \times B$, če $\pi_1(p) = \pi_1(q)$ in $\pi_2(p) = \pi_2(q)$, potem $p = q$

$$f : A \times B \to C$$

$$f : p \mapsto ...$$

$$f : (x, y) \mapsto ...x...y...$$

$$g : A \to B \times C$$

$$g : a \mapsto (...a..., ...a...)$$

Kaj je $\varnothing \times A$? $\varnothing \times A = \varnothing$

3.2 Eksponentna množica

Če sta A in B množici, je B^A množica vseh preslikav z domeno A in kodomeno B.

3.3 Vsota množic

Če sta A in B množici je vsota $A + B$ množica.

Za vsak $a \in A$ je $\iota_1(a) \in A + B$

Za vsak $b \in B$ je $\iota_2(b) \in A + B$

Elementa u in v iz $A + B$ sta enaka, če bodisi obstaja $a \in A$ da je $u = \iota_1(a)$ in $v = \iota_1(a)$, bodisi obstaja $b \in B$ da je $u = \iota_2(b)$ in $v = \iota_2(b)$.

$$\{1, 2\} + \{1, 2\} = \{\iota_1(1), \iota_1(2), \iota_2(1), \iota_2(2)\}$$

3.4 Izomorfni množici

<u>Def.:</u> Izomorfizem je preslikava $f : A \to B$, za katero obstaja preslikava $g : B \to A$, da je:

- za vsak $x \in A$ je $g(f(x)) = x$ in
- za vsak $y \in B$ je $f(g(y)) = y$

Pravimo da je g inverz f.

Če obstaja izomorfizem $X \to Y$, pravimo, da sta X in Y **izomorfni**, pišemo $X \cong Y$

3.5 Kompozitum

B^A je množica preslikav iz A v B.

Kompozicija preslikav $g \circ f$.

$$A \xrightarrow{f} B \xrightarrow{g} C$$

$$\circ : C^B \times B^A \to C^A$$
$$\circ : (g, f) \mapsto (x \mapsto g(f(x))) \text{ (ugnezden funkcijski prepis)}$$

Pišemo $g \circ f$

<u>Zakaj ne raje $f \bullet g$?</u>

Npr, da imamo:

$$\bullet : B^A \times C^B \to C^A$$
$$\bullet : (f, g) \mapsto (x \mapsto g(f(x)))$$

Računsko pravilo za $\circ$:

$(g \circ f)(a) = g(f(a))$ ✓izberemo, ker se ohrani vrstni red.
$(f \bullet g)(a) = g(f(a))$

Imamo dve preslikavi:

$$\mathbb{R} \to \mathbb{R} \qquad\qquad \mathbb{R} \to \mathbb{R}$$
$$x \mapsto 4 - x^2 \qquad\qquad x \mapsto 2 - x$$

$$(x \mapsto 4 - x^2) \circ (x \mapsto 2 - x) = (x \mapsto (x \mapsto 4 - x^2)((x \mapsto 2 - x)x))$$

Zaradi dvoumnosti preimenujemo vezane spremenljivke:

$$x \mapsto 4 - x^2 \Rightarrow y \mapsto 4 - y^2 \qquad\qquad x \mapsto 2 - x \Rightarrow z \mapsto 2 - z$$

$$(y \mapsto 4 - y^2) \circ (z \mapsto 2 - z) = (x \mapsto (y \mapsto 4 - y^2)((z \mapsto 2 - z)x))$$

Identiteta na množici A je preslikava:

$$id_A : A \to A$$
$$id_A : x \mapsto x$$

<u>Def:</u> $f : A \to B, g : B \to A$ rečemo, da je g **inverz** f, ko velja:

$$f \circ g = id_B \wedge g \circ f = id_A$$

Če ime f inverz, pravimo, da je $izomorfizem$.

Če obstaja izomorfizem $A \to B$, pravimo, da sta A in B **izomorfni** množici.
Pišemo $A \cong B$

<u>Primeri:</u>

(a) $A \times \varnothing \cong \varnothing$
$f : A \times \varnothing \to \varnothing$
Predpis ni potreben, ker ni nobenih elementov.
$g : \varnothing \to A \times \varnothing$
Iz prazne množice obstaja ena sama preslikava.

(b) $1 = \{()\}$
$A \times 1 \cong A$

$$f : A \times 1 \to A \qquad (x, y) \mapsto x$$

$$g : A \to A \times 1 \qquad x \mapsto (x, ())$$

$$A \times 1 \to A \to A \times 1$$
$$(x, y) \overset{f}{\mapsto} x \overset{g}{\mapsto} (x, ())$$

(c) $A^{B\times C} \cong (A^B)^C$

$$\theta : A^{B\times C} \to (A^B)^C$$
$$\theta : \star \mapsto (c \mapsto (b \mapsto \star(b, c)))$$

$$\phi : (A^B)^C \to A^{B\times C}$$
$$\phi : \leftmoon \mapsto ((\beta, \gamma) \mapsto (\leftmoon(\gamma))(\beta))$$

4 Simbolni zapis

4.1 Izjavni račun:

- konstanti
  - $\bot$ - neresnica
  - $\top$ - resnica
- logični vezniki:
  - $p \wedge q$ - p in q (p, q sta izjavi)
  - $p \vee q$ - p ali q
  - $p \Rightarrow q$

    če p potem q
    iz p sledi q
    p je zadosten (pogoj) za q
    q je potreben (pogoj) za p
  - $p \Leftrightarrow q$

    p če in samo če q
    p čee q
    p iff q (if and only if) p in q sta enakovredna ali ekvivalentna
  - $\neg p$ - ne p

4.2 Predikatni račun:

Izjavni + **kvantifikatorja**

- univerzalni kvantifikator:

  $\forall x \in B.p$
  $(\forall x \in B)p$
  $\forall x \in B : p$
  $\forall x \in B(p)$

  "za vsak x iz B velja p"
  "vsi x-i iz B zadoščajo p"
- eksistenčni kvalifikator

$\exists x \in B.p$	"obstaja x iz B, da velja p"
	"obstaja x iz B, za katerega p"
	"za neki x iz B velja p"

4.3 Prednosti veznikov:

Vezniki si po prednosti sledijo od tistega z največjo, do tistega z najmanjšo v naslednjem vrstnem redu:

$$\neg, \wedge, \vee, (\Rightarrow, \Leftrightarrow), (\forall, \exists)$$

5 Dokazovanje

Dokaz ima drevesno strukturo in more biti končen.

Vedeti moramo:

1. Kaj trenutno dokazujemo
2. Katere *spremenljivke* in *predpostavke* imamo na voljo (kontekst).

5.1 Oblika dokaza

Za obliko glej zvezek. Žal se mi ne da prepisovati vseh različnih dokazov in skic kako naj izgledajo.

5.2 Pravila sklepanja

5.2.1 Pravila upeljave

1. *Resnica* $\top$*:* je res
2. *Neresnica* $\bot$*:* ni pravila
3. *Konjunkcija:* da dokažemo $p \wedge q$ moramo dokazati p, nato pa še q.

4. *Disjunkcija:* da dokažemo $p \vee q$ lahko dokažemo p, ali pa q.

5. *Implikacija:* da dokažemo $p \Rightarrow q$, predpostavimo p in nato dokažemo q.

6. *Ekvivalenca:* ker je $p \Leftrightarrow q$ okrajšava za $(p \Rightarrow q) \wedge (q \Rightarrow p)$, to dokažemo tako, da po pravilu 5. najprej dokažemo $p \Rightarrow q$, nato pa še $q \Rightarrow p$.

7. *Negacija:* za dokaz $\neg p$ predpostavimo p in nato dokažemo $\perp$. Drugače povedano: "iščemo protislovje".

8. *Zakon o izključeni tretji možnosti:*[1] vemo da je q ali pa $\neg q$. Ne more biti oboje.

9. *Univerzalni kvalifikator:* za dokaz $\forall x \in A : p(x)$, najprej izberemo poljubni x s trditvijo: "Naj bo $x \in A$"[2], nato pa dokažemo $p(x)$.

10. *Eksistenčni kvalifikator:* da dokažemo $\exists x \in A : p(x)$, si izberemo x s trditvijo: "Vzemimo $x := a$". Nato najprej dokažemo $a \in A$ in potem še $p(a)$.

5.2.2 Pravila uporabe

1. *Resnica* $\top$*:* ni uporabno.

2. *Neresnica* $\perp$*:* če vemo neresnico, lahko dokažemo katerokli izjavo tako, da uporabimo neresnico.

3. *Konjunkcija:* če vemo $p \wedge q$, lahko rečemo da vemo p, ali pa da vemo q.

4. *Disjunkcija:* če vemo $p \vee q$, lahko dokažemo izjavo tako da "Obravnavamo primera p, q zaradi $p \vee q$". Nato imamo dva primera. V enem predpostavimo p, v drugem pa q.

5. *Implikacija:* če vemo $p \Rightarrow q$ in vemo p, potem vemo q.

6. *Ekvivalenca:* če vemo $p \Leftarrow q$ vemo $p \Rightarrow q$ in $q \Rightarrow p$. Prav tako imamo tudi *pravilo zamenjave*, ki pravi, da lahko p nadomestimo s q in obratno.

7. *Negacija:* če vemo q in vemo $\neg q$, velja $\perp$.

[1] posebno, osnovno pravilo

[2] x mora bit "svež", t.j: trenutno še ne uporabljen.

8. *Univerzalni kvantifikator:* če vemo $\forall a \in A : p(a)$ in vemo $a \in A$, potem vemo $p(a)$.
9. *Eksistenčni kvantifikator:* če vemo $\exists x \in A : p(x)$. lahko rečemo da imamo $x \in A$. Potem vemo $p(x)$.

6 Boolova algebra

Izjava p ima *pomen* in *resničnostno vrednost* ($\bot$ ali $\top$).

V izjavi $\neg p \vee q$ sta p in q *izjavna simbola.*

Množica $2 = \{\bot, \top\}$ je *množica resničnostnih vrednosti.*

n-členi Boolova preslikava je

$$\underbrace{2 \times 2 \times \cdots \times 2}_{n} \to 2$$

Primer:

$$\begin{aligned} 2 \times 2 &\to 2 \\ (p, q) &\mapsto \neg p \vee q \end{aligned}$$

Tavtologija je izjava, ki je resnična ne glede na vrednosti parametrov.

Zakon o zamenjavi ekvivalentnih izjav

Če $p \iff q$ potem lahko p nadomestimo s q, če gledamo le na resničnostno vrednost izjav.

6.1 Zakoni Boolove algebre

Operacije:

- Konstanti: $\top, \bot$
- Negacija: $\lneq$

- Konjunkcija: $\wedge$
- Disjunkcija: $\vee$

Konjunkcija:

- $p \wedge q = q \wedge p$
- $p \wedge (q \wedge r) = (p \wedge q) \wedge r$
- $p \wedge \top = p$
- $p \wedge p = p$

Disjunkcija:

- $p \vee q = q \vee p$
- $p \vee (q \vee r) = (p \vee q) \vee r$
- $p \vee \bot = p$
- $p \vee p = p$

Distributivnost:

- $(p \wedge q) \vee r = (p \vee r) \wedge (q \vee r)$
- $(p \vee q) \wedge r = (p \wedge r) \vee (q \wedge r)$

Absorpcija:

- $(q \wedge p) \vee p = p$
- $(q \vee q) \wedge p = p$

Negacija:

- $p \wedge \neg p = \bot$
- $p \vee \neg p = \top$

Izrek: (za izjavo p v kateri nastopajo samo izjavni simboli $q_1 \dots q_n$)

1. Če ima izjava dokaz je tavtologija.
2. Če je izjava tavtologija ima dokaz.

Izrek ne velja za izjave, ki vsebujejo parametre iz množic.

6.2 Polni nabori

Nabor operacij je *poln*, če lahko z njim dobimo poljubno resničnostno tabelo.

Primeri:

- $\top, \bot, \wedge, \vee, \neg$ je poln
- $\top, \neg, \wedge$ je poln
- $\bot, \uparrow$ (nand) je poln

6.3 Računska pravila

Pravila za $\top$:

- $p \vee \top = \top$
- $p \wedge \top = p$
- $\neg\top = \bot$

Pravila za $\bot$:

- $p \vee \bot = p$
- $p \wedge \bot = \bot$
- $\neg\bot = \top$

Pravila za negacijo:

- $\neg\neg p = p$
- de Morganova pravila:
  - $\neg(p \wedge q) = \neg p \vee \neg q$
  - $\neg(p \vee q) = \neg p \wedge \neg q$

Ostalo (*kontrapozitivna oblika*):

- $(p \Rightarrow q) = (\neg q \Rightarrow \neg p)$
- $(p \vee q) = (\neg p \Rightarrow q)$
- $(p \Rightarrow q) = (\neg p \vee q)$

Izjava ima lahko dve obliki:

- *konjunktivna* oblika: $(\neg p \vee q) \wedge r \wedge (r \vee \neg p)$
- *disjunktivna* oblika: $(u \wedge \neg v) \vee (u \wedge w \wedge \neg u)$

6.4 Pravila za kvantifikatorje

- $(\neg\exists x \in A.p(x)) \iff (\forall x \in A.\neg p(x))$
- $(\neg\forall x \in A.p(x)) \iff (\exists x \in A.\neg p(x))$
- $(\forall x \in \varnothing.p(x)) \iff \top$
- $(\exists x \in \varnothing.p(x)) \iff \bot$
- $(p \Rightarrow \forall x \in A.q(x)) \iff (\forall x \in A.p \Rightarrow q(x))$
- $(\forall u \in A \times B.p(u)) \iff (\forall x \in A \forall y \in B.p(x, y))$
- $(\exists u \in A \times B.p(u)) \iff (\exists x \in A \exists y \in B.p(x, y))$
- $(\forall u \in A + B.p(u)) \iff (\forall x \in A.p(\iota_1(x))) \wedge (\forall y \in B.p(\iota_2(y)))$
- $(\forall u \in A \cup B.p(u)) \iff (\forall a \in A.p(a)) \wedge (\forall b \in B.p(b))$
- $(\forall x \in \{a\}.p(x)) \iff p(a)$
- $(\exists x \in \{a\}.p(x)) \iff p(a)$