Logika in množice

Luka Horjak (luka.horjak@student.fmf.uni-lj.si)

20. junij 2021

Kazalo

Uvod

V tem dokumenti so zbrani moji zapiski s predavanj predmeta Logika in množice v letu 2020/21. Predavatelj v tem letu je bil prof. dr. Marko Petkovšek.

Zapiski niso popolni. Manjka nekaj zgledov, ki pomagajo pri razumevanju definicij in izrekov. Poleg tega nisem dokazoval čisto vsakega izreka, pogosto sem ga označil kot očitnega ali pa le nakazal pomembnejše korake v dokazu.

Zelo verjetno se mi je pri pregledu zapiskov izmuznila kakšna napaka – popravki so vselej dobrodošli.

1 Izjavni račun

»Ta poved ni resnična.«

—Paradoks o lažnivcu

1.1 Izjave in izjavni vezniki

Definicija 1.1.1. *Izjava* je poved, ki je resnična ali neresnična.

Zgled 1.1.1.1. Resničnost izjav:

- Ena in ena je tri. - neresnična izjava
- Ena in ena je dva. - resnična izjava
- Koliko je ena in ena? - ni izjava
- Ta poved ni resnična. - ni izjava

Izjave po vsebini delimo na resnične (resničnostna vrednost 1) in lažne (vrednost 0). Po obliki jih delimo na osnovne (ne vsebujejo izjavnih veznikov) in sestavljene.

Zgled 1.1.1.2. Osnovne in sestavljene izjave:

- Vreme je lepo. - osnovna
- Vreme je lepo in Peter gre v hribe. - sestavljena
- Če je vreme lepo, gre Peter v hribe. - sestavljena
- Peter ne gre v hribe. - sestavljena

Resničnost sestavljene izjave je določena z resničnostjo njenih sestavnih delov.

Definicija 1.1.2. Naj bo $n \in \mathbb{N} = \{0,\ 1,\ 2,\ \dots\}$. n-mestni *izjavni veznik* je funkcija, ki vsaki urejeni n-terici ničel in enic priredi vrednost 0 ali 1.

Zgled 1.1.2.1. Izjavni vezniki:

- Negacija, simbol: $\neg$
- Konjunkcija, simbol: $\wedge$
- Disjunkcija, simbol: $\vee$
- Implikacija,[1] simbol: $\Rightarrow$
- Ekvivalenca, simbol: $\Leftrightarrow$
- 0-mestna veznika 0 in 1

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
0	0	1	0	0	1	1
0	1		0	1	1	0
1	0	0	0	1	0	0
1	1		1	1	1	1

Tabela 1: *Resničnostna tabela* izjavnih veznikov

Vseh n-mestnih veznikov je 2^{2^n}.

[1] Če $p \Rightarrow q$, pravimo, da je p *antecedens*, q pa *konsekvens*.

1.2 Izjavni izrazi

Definicija 1.2.1. Izjavni izrazi:

(i) Vsaka izjavna konstanta je izjavni izraz

(ii) Vsaka izjavna spremenljivka $p_1,\ p_2,\ p_3,\ \ldots$ je izjavni izraz

(iii) Če je f enomesten izjavni veznik in je A izjavni izraz, je tudi (fA) izjavni izraz

(iv) Če je f dvomesten izjavni veznik in sta A in B izjavna izraza, je tudi (AfB) izjavni izraz

(v) Če je f n-mesten izjavni veznik in so $A_1,\ A_2,\ \ldots,\ A_n$ izjavni izrazi, je tudi $f(A_1, A_2, \ldots, A_n)$ izjavni izraz

Zgled 1.2.1.1. Konstrukcijsko zaporedje za $((p \Rightarrow q) \wedge (\neg r))$:

1. p
2. q
3. $(p \Rightarrow q)$
4. r
5. $(\neg r)$
6. $((p \Rightarrow q) \wedge (\neg r))$

Definicija 1.2.2. Dogovor o vrstnem redu veznikov:

1. $\neg$ ima prednost pred drugimi vezniki
2. Vsak veznik iz zaporedja $(\wedge, \vee, \Rightarrow, \Leftrightarrow)$ ima prednost pred vezniki, ki so v tem zaporedju desno od njega
3. Če isti veznik nastopa večkrat, ima levi nastop prednost pred desnim
4. Zunanji par oklepajev izpuščamo

Vsak izjavni izraz določa neko resničnostno tabelo in s tem tudi nek izjavni veznik.

Zgled 1.2.2.1. $f(p, q, r) = (p \Rightarrow q) \wedge \neg r$:

p	q	r	$p \Rightarrow q$	$\neg r$	$(p \Rightarrow q) \wedge \neg r$
0	0	0	1	1	1
0	0	1	1	0	0
0	1	0	1	1	1
0	1	1	1	0	0
1	0	0	0	1	0
1	0	1	0	0	0
1	1	0	1	1	1
1	1	1	1	0	0

Tabela 2: Zgled 1.2.2.1

1.3 Tavtologije in enakovredni izrazi

Definicija 1.3.1. Izjavni izraz je

1. *tavtologija*, če je resničen pri vseh naborih vrednosti svojih spremenljivk
2. *protislovje*, če je neresničen pri vseh naborih vrednosti svojih spremenljivk
3. *kontingenten*, če ni tavtologija ali protislovje

Zgled 1.3.1.1. Tavtologije in protislovja:

p	q	$p \Rightarrow q$	$\neg p \vee q$	$p \Rightarrow q \Leftrightarrow \neg p \vee q$
1	1	1	1	1
1	0	0	0	1
0	1	1	1	1
0	0	1	1	1

Tabela 3: Primer tavtologije

p	q	$q \Rightarrow p$	$\neg(q \Rightarrow p)$	$p \wedge \neg(q \Rightarrow p)$
1	1	1	0	0
1	0	1	0	0
0	1	0	1	0
0	0	1	0	0

Tabela 4: Primer protislovja

- 1, $p \vee \neg p$ in $p \Rightarrow (q \Rightarrow p)$ so primeri tavtologij
- 0, $p \wedge \neg p$ in $p \wedge \neg(q \Rightarrow p)$ so primeri protislovij

Definicija 1.3.2. Izjavna izraza A in B sta *enakovredna*, če je $A \Leftrightarrow B$ tavtologija. S simboli to zapišemo $A \sim B$.

Zgled 1.3.2.1. Za poljubno izbiro A, B in C so naslednji izrazi enakovredni:

$A \wedge 1 \sim A$	idempotenca konjunkcije
$A \vee A \sim A$	idempotenca disjunkcije
$A \wedge B \sim B \wedge A$	komutativnost konjunkcije
$A \vee B \sim B \vee A$	komutativnost disjunkcije
$A \Leftrightarrow B \sim B \Leftrightarrow A$	komutativnost ekvivalence
$A \wedge (B \wedge C) \sim (A \wedge B) \wedge C$	asociativnost konjunkcije
$A \vee (B \vee C) \sim (A \vee B) \vee C$	asociativnost disjunkcije
$A \Leftrightarrow (B \Leftrightarrow C) \sim (A \Leftrightarrow B) \Leftrightarrow C$	asociativnost ekvivalence
$A \wedge (A \vee B) \sim A$	absorpcija konjunkcije glede na disjunkcijo
$A \vee (A \wedge B) \sim A$	absorpcija disjunkcije glede na konjunkcijo
$A \wedge (B \vee C) \sim (A \wedge B) \vee (A \wedge C)$	distributivnost konjunkcije glede na disjunkcijo
$A \vee (B \wedge C) \sim (A \vee B) \wedge (A \vee C)$	distributivnost disjunkcije glede na konjunkcijo
$\neg\neg A \sim A$	zakon dvojne negacije
$\neg(A \wedge B) \sim \neg A \vee \neg B$	prvi De Morganov zakon

$\neg(A \vee B) \sim \neg A \wedge \neg B$ drugi De Morganov zakon

$A \Rightarrow B \sim \neg B \Rightarrow \neg A$ zakon kontrapozicije

$$A \wedge 0 \sim 0 \qquad 1 \Rightarrow A \sim A \qquad A \Rightarrow B \sim \neg A \vee B$$
$$A \wedge 1 \sim A \qquad A \Leftrightarrow 0 \sim \neg A \qquad \neg(A \Rightarrow B) \sim A \wedge \neg B$$
$$A \vee 0 \sim A \qquad A \Leftrightarrow 1 \sim A \qquad A \Leftrightarrow B \sim (A \Rightarrow B) \wedge (B \Rightarrow A)$$
$$A \vee 1 \sim 1 \qquad A \Rightarrow A \sim 1 \qquad A \Leftrightarrow B \sim (\neg A \vee B) \wedge (A \vee \neg B)$$
$$A \Rightarrow 0 \sim \neg A \qquad A \Leftrightarrow A \sim 1 \qquad A \Leftrightarrow B \sim (A \wedge B) \vee (\neg A \wedge \neg B)$$
$$A \Rightarrow 1 \sim 1 \qquad \neg 0 \sim 1 \qquad \neg(A \Leftrightarrow B) \sim \neg A \Leftrightarrow B$$
$$0 \Rightarrow A \sim 1 \qquad \neg 1 \sim 0 \qquad \neg(A \Leftrightarrow B) \sim A \Leftrightarrow \neg B$$

1.4 Disjunktivna in konjunktivna normalna oblika

Definicija 1.4.1. Naj bo A kontingenten izjavni izraz in naj bo T njegova resničnostna tabela.

(i) *Disjunktivna normalna oblika* izraza A je disjunkcija osnovnih konjunkcij,[a] ki ustrezajo vrsticam tabele T, v katerih ima A vrednost 1.

(ii) *Konjuktivna normalna oblika* izraza A je konjunkcija osnovnih disjunkcij,[b] ki ustrezajo vrsticam tabele T, v katerih ima A vrednost 0.

[a] *Osnovna konjunkcija* i-te vrstice je konjunkcija tistih izjavnih spremenljivk, ki so tu resnične, in negacij tistih, ki so lažne.

[b] *Osnovna disjunkcija* i-te vrstice je disjunkcija tistih izjavnih spremenljivk, ki so tu lažne, in negacij tistih, ki so resnične.

Trditev 1.4.2. Če je A kontingenten izraz, je $A \sim \mathrm{DNO}(A) \sim \mathrm{KNO}(A)$.

Dokaz. The proof is obvious and need not be mentioned. □

Zgled 1.4.2.1. Podana je naslednja tabela:

p	q	r	D
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	1

Tabela 5: Zgled 1.4.2.1

D mora biti resničen natanko v 2., 6. in 8. vrstici. Dovolj je tako nastaviti

$$D = (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge \neg r).$$

Izraz lahko poenostavimo:

$$\begin{aligned} D &\sim ((p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)) \wedge \neg r \\ &\sim ((p \vee \neg p) \wedge q \vee \neg p \wedge \neg q) \wedge \neg r \\ &\sim (q \vee p) \wedge (q \vee q) \wedge \neg r \\ &\sim (q \vee \neg p) \wedge \neg r \\ &\sim (q \Rightarrow p) \wedge \neg r \\ &\sim \neg(p \Rightarrow q \Rightarrow r) \end{aligned}$$

1.5 Sklepanje v izjavnem računu

Definicija 1.5.1. *Sklep* je končno zaporedje izjav $p_1,\ p_2,\ \ldots,\ p_k,\ z$, kjer so p_i *predpostavke* sklepa, z pa zaključek. Sklep je *pravilen* ali *veljaven*, če je zaključek resničen vedno, ko so resnične vse predpostavke. Pišemo

$$p_1,\ p_2,\ \ldots,\ p_k \models z.$$

Zgled 1.5.1.1. Primer sklepa:

Če je ta žival ptič, potem ima krila.	$p \Rightarrow q$
Ta žival nima kril.	$\neg q$
Torej ta žival ni ptič.	$\neg p$

Trditev 1.5.2. Za vse izjavne izraze A, B in C velja

$A,\ A \Rightarrow B \models B$	modulus ponens (MP)
$A \Rightarrow B,\ \neg B \models \neg A$	modulus tollens (MT)
$A \vee B,\ \neg B \models A$	disjunktivni silogizem (DS)
$A \Rightarrow B,\ B \Rightarrow C \models A \Rightarrow C$	hipotetični silogizem (HS)
$A \wedge B \models A$	poenostavitev (Po)
$A,\ B \models A \wedge B$	združitev (Zd)
$A \models A \vee B$	pridružitev (Pr)

Dokaz. Pravilnost sledi iz pravilnostnih tabel. □

Izrek 1.5.3 (Izrek o naravni dedukciji)**.** Naj bodo $A_1,\ A_2,\ \ldots,\ A_k$ izjavni izrazi. Če obstaja zaporedje izjavnih izrazov $B_1,\ B_2,\ \ldots,\ B_n$, tako da za vsak $i \in \{1, 2, \ldots, n\}$ velja vsaj ena izmed naslednjih možnosti:

a) B_i je eden od A_j,

b) B_i je tavtologija,

c) $B_i \sim B_j$ za nek $j < i$ ali

d) B_i logično sledi iz predhodnih izrazov B_j po enem izmed osnovnih pravil sklepanja,

potem $A_1,\ A_2,\ \ldots,\ A_k \models B_n$.

Dokaz. The proof is obvious and need not be mentioned. □

Sklep ni pravilen, če obstaja taka izbira izjavnih spremenljivk, da so vse predpostavke resnične, zaključek pa ne.

Zgled 1.5.3.1. Ali $p \Rightarrow q,\ p \vee r,\ q \Rightarrow s,\ r \Rightarrow t,\ \neg s \models t$?

i	B_i	Utemeljitev
1	$p \Rightarrow q$	Predpostavka
2	$p \vee r$	Predpostavka
3	$q \Rightarrow s$	Predpostavka
4	$r \Rightarrow t$	Predpostavka
5	$\neg s$	Predpostavka
6	$p \Rightarrow s$	HS iz 1, 3
7	$\neg p$	MT iz 6, 5
8	$r \vee p$	$\sim$ 2
9	r	DS iz 8, 7
10	t	MP iz 9, 4

Tabela 6: Zgled 1.5.3.1

Zgled 1.5.3.2. Nepravilni sklep:

Ta žival ima krila ali pa ni ptič.
Če je ta žival ptič, potem leže jajca.

Torej ta žival ne leže jajc.

Sklep ni pravilen, žival lahko ni ptič, nima kril in leže jajca. Našli smo *protiprimer* – vse predpostavke so resnične, zaključek pa ne.

Izrek 1.5.4. Sklep je pravilen natanko tedaj, ko je implikacija konjunkcije predpostavk in zaključka sklepa tavtologija.

Dokaz. The proof is obvious and need not be mentioned. □

Izrek 1.5.5. $A_1, \ldots, A_k \models B \Rightarrow C$ natanko tedaj, ko $A_1, \ldots, A_k, B \models C$. Takemu sklepu pravimo *pogojni sklep* (PS).

Dokaz. Naj bo $A = A_1 \wedge A_2 \wedge \cdots \wedge A_k$. Uporabimo izrek 1.5.4. Velja namreč

$$A \Rightarrow (B \Rightarrow C) \sim \neg A \vee (\neg B \vee C) \sim (\neg A \vee \neg B) \vee C \sim \neg(A \wedge B) \vee C \sim A \wedge B \Rightarrow C. \quad \square$$

Izrek 1.5.6. $A_1, \ldots, A_k \models B$ natanko tedaj, ko $A_1, \ldots, A_k, \neg B \models 0$. Takemu sklepu pravimo *sklep s protislovjem* (RA – *reductio ad absurdum*).

Dokaz. Naj bo $A = A_1 \wedge A_2 \wedge \cdots \wedge A_k$. Znova uporabimo izrek 1.5.4. Velja

$$A \Rightarrow B \sim \neg A \vee B \sim \neg(A \wedge \neg B) \sim A \wedge \neg B \Rightarrow 0. \quad \square$$

1.6 Polni nabori izjavnih veznikov

Definicija 1.6.1. Množica M izjavnih veznikov je *poln nabor*, če za vsak izjavni izraz A obstaja nek enakovreden izjavni izraz B, ki vsebuje le veznike iz M.

Izrek 1.6.2. $\{\neg, \wedge, \vee\}$ je poln nabor.

Dokaz. Vzamemo eno izmed normalnih oblik, $p \wedge \neg p$ ali $p \vee \neg p$. □

Da dokažemo, da je M poln nabor, naredimo naslednje:

1. Izberemo nek znan poln nabor P
2. Vsak veznik iz P izrazimo z vezniki iz M

Definicija 1.6.3. Definiramo še naslednje dvomestne veznike:

- $p + q \sim \neg(p \Leftrightarrow q)$ – stroga disjunkcija
- $p \uparrow q \sim \neg(p \wedge q)$ – Shefferjev veznik
- $p \downarrow q \sim \neg(p \vee q)$ – Łukasiewiczev veznik

Za zgornje izjavne veznike veljajo naslednje enakovrednosti:

$A + 0 \sim A$	$A \uparrow 0 \sim 1$	$A \downarrow 0 \sim \neg A$
$A + 1 \sim \neg A$	$A \uparrow 1 \sim \neg A$	$A \downarrow 1 \sim 0$
$A + A \sim 0$	$A \uparrow A \sim \neg A$	$A \downarrow A \sim \neg A$

$A + B \sim B + A$	komutativnost stroge disjunkcije
$A \uparrow B \sim B \uparrow A$	komutativnost Shefferjevega veznika
$A \downarrow B \sim B \downarrow A$	komutativnost Łukasiewiczevega veznika
$A + (B + C) \sim (A + B) + C$	asociativnost stroge disjunkcije

Trditev 1.6.4. Množice $\{\neg, \wedge\}$, $\{\neg, \vee\}$, $\{\neg, \Rightarrow\}$, $\{0, \Rightarrow\}$, $\{1, +, \wedge\}$, $\{0, \Leftrightarrow, \vee\}$, $\{\uparrow\}$ in $\{\downarrow\}$ so polni nabori.

Dokaz. The proof is obvious and need not be mentioned. □

Kako pokazati, da neka množica M ni poln nabor? Poiščemo *invarianto*:[2]

Definicija 1.6.5. Naj bo f n-mestni izjavni veznik.

1. f *ohranja vrednost 1*, če je $f(1, 1, \ldots, 1) = 1$.
2. f *ohranja vrednost 0*, če je $f(0, 0, \ldots, 0) = 0$.

Zgled 1.6.5.1. Množici $\{1, \wedge, \vee, \Rightarrow, \Leftrightarrow\}$ in $\{0, \wedge, \vee, +\}$ nista polna nabora, saj prva ohranja 1, druga pa 0.

[2] Invarianta je značilnost, ki ostane nespremenjena pri določenih transformacijah.

2 Predikatni račun

»Takoj, ko gremo v realni svet, se zadeve zakomplicirajo.«
—prof. dr. Marko Petkovšek

2.1 Motivacija

Zgled 2.1.0.1. Z izjavnim računom ne moremo opisati celotne logike:

Vsak zajec ljubi korenje.
Feliks je zajec.

Torej Feliks ljubi korenje.

V zgornjem primeru nimamo izjavnih veznikov, sklep pa zato ni pravilen, saj izjave v formalnem smislu niso povezane. Definiramo dodatne simbole:

$Z(x)$	x je zajec
$K(x)$	x ljubi korenje
a	Feliks
$\forall x$	za vsak x

Zgornji sklep lahko tako formaliziramo:

$\forall x \colon (Z(x) \Rightarrow K(x))$
$Z(a)$

$K(a)$

Tu označimo

x	individualna spremenljivka
a	individualna konstanta
Z, K	enomestna predikata
$\forall x$	univerzalni kvantifikator
$: ()$	ločila

Zgled 2.1.0.2. S predikati lahko izrazimo več izjav:

1. (a) Vsi gasilci so hrabri.
   (b) Nekateri gasilci so hrabri.
   (c) Nekateri gasilci niso hrabri.
   (d) Noben gasilec ni hraber.

   Naj $G(x)$ označuje »x je gasilec« in $H(x)$ označuje »x je hraber«. Potem lahko zgornje izjave prevedemo v sledeče:

(a) $\forall x\colon (G(x) \Rightarrow H(x))$

(b) $\exists x\colon (G(x) \wedge H(x))$

(c) $\exists x\colon (G(x) \wedge \neg H(x))$

(d) $\forall x\colon (G(x) \Rightarrow \neg H(x))$

2. Praštevil je neskončno mnogo. Ekvivalentno obstajajo poljubno velika praštevila.

   Naj $P(x)$ označuje »p je praštevilo« in naj $V(x, y)$ označuje $x > y$. Določimo še *domeno*, ki je v tem primeru $\mathbb{N}$. Zgornjo izjavo lahko tako prevedemo v

   $$\forall n\ \exists p\colon (V(p, n) \wedge P(p)).$$

3. Naravno število n je praštevilo, če in samo če ima natanko dva naravna delitelja.

   Naj $E(x)$ označuje »$x = y$« in $f(x, y)$ označuje $x \cdot y$. Zgornjo izjavo lahko tako prevedemo v

   $$\forall x\colon (P(x) \Leftrightarrow V(x, 1) \wedge \forall u\ \forall v\colon (E(x, f(u, v)) \Rightarrow E(u, 1) \vee E(v, 1))),$$

   oziroma

   $$\forall x\colon ((P(x) \Leftrightarrow x > 1 \wedge \forall u\ \forall v\colon (x = u \cdot v \Rightarrow u = 1 \vee v = 1)).$$

2.2 Sintaksa

A) Simboli:

(a) individualne konstante: $a, b, c, \ldots$

(b) individualne spremenljivke: $x, y, z, \ldots$

(c) predikati: $P, Q, R, \ldots$

(d) funkcijski simboli: $f, g, h, \ldots$

(e) izjavni vezniki

(f) simbola kvantifikacije

B) Termi:

(a) Vsaka individualna konstanta je term

(b) Vsaka individualna spremenljivka je term

(c) Naj bo f neki n-mesten funkcijski simbol in $t_1, t_2, \ldots, t_n$ termi. Potem je $f(t_1, t_2, \ldots, t_n)$ term

Term je *zaprt*, če ne vsebuje individualnih spremenljivk.

C) Izjavne formule:

(a) Naj bo P neki n-mesten predikat in $t_1, t_2, \ldots, t_n$ poljubni termi. Potem je $P(t_1, t_2, \ldots, t_n)$ izjavna formula. Taki formuli pravimo *atomarna*.

(b) Če je F neki n-mesten izjavni veznik in so $\varphi_1, \varphi_2, \ldots, \varphi_n$ izjavne formule. je tudi $F(\varphi_1, \varphi_2, \ldots, \varphi_n)$ izjavna formula.

(c) Če je φ izjavna formula in x poljubna individualna spremenljivka, sta $(\forall x \colon \varphi)$ in $(\exists x \colon \varphi)$ izjavni formuli. Pri tem je $\forall x$ *univerzalni kvantifikator* in $\exists x$ *eksistenčni kvantifikator*, φ pa doseg kvantifikatorja.

Definicija 2.2.1. Dogovor o prednostnem redu in opuščanju ločil:

1. Za izjavne veznike in zunanje oklepaje veljajo prejšnji dogovori
2. Kvantifikatorji imajo prednost pred izjavnimi vezniki
3. Ločila med zaporednimi kvantifikatorji opuščamo

Definicija 2.2.2. Nastop neke individualne spremenljivke v izjavni formuli je *vezan*, če je del nekega kvantifikatorja ali pa leži v dosegu nekega kvantifikatorja, ki vsebuje to spremenljivko, sicer pa je *prost*.

Definicija 2.2.3. Izjavna formula je *zaprta*, če so vsi nastopi individualnih spremenljivk v njej vezani.

Izjavno formulo φ lahko zapišemo v obliki $\varphi(x)$, kjer je x individualna spremenljivka. Če je t term, s $\varphi(t)$ označimo izjavno formulo, ki jo dobimo iz φ, če *vse* proste nastope x v φ zamenjamo s termom t – naredimo *substitucijo*.

Izjavno formulo φ lahko zapišemo kot $\varphi(x_1, x_2, \ldots, x_n)$, kjer so $x_1, \ldots, x_n$ *različne* individualne spremenljivke. Če so $t_1, t_2, \ldots, t_n$ termi, je $\varphi(t_1, t_2, \ldots, t_n)$ izjavna formula, ki jo dobimo, če v φ zamenjamo vse proste nastope x_i s termom t_i za $i = 1, 2, \ldots, n$.

2.3 Semantika

Definicija 2.3.1. Naj bo $\mathcal{F}$ množica izjavnih formul, ki nas zanimajo. *Interpretacijo* I formul iz $\mathcal{F}$ podamo tako, da

1. izberemo *neprazen* razred objektov D (*domena* ali *področje pogovora*),
2. vsaki individualni konstanti a iz $\mathcal{F}$ priredimo nek $\overline{a} \in D$,
3. vsakemu n-mestnemu predikatu P iz $\mathcal{F}$ priredimo neko n-mestno relacijo $\overline{P}$ v D,
4. vsakemu n-mestnemu funkcijskemu simbolu f iz $\mathcal{F}$ priredimo preslikavo, ki vsako urejeno n-terico elementov domene D preslika v natanko določen element D.

Izjavne veznike interpretiramo enako kot prej, kvantifikatorja pa kot »za vsak x iz D« in »obstaja x iz D«.

Zgled 2.3.1.1. Podano imamo

$$\mathcal{F} = \{P(a), P(x), \forall x\colon P(x), P(f(a,b))\}\,.$$

Primer interpretacije:

- $D = \mathbb{N}$
- $\overline{a} = 2$, $\overline{b} = 3$
- $\overline{P}(x) \ldots$ x je praštevilo
- $\overline{f}(x,y) = 2x + y$

Potem je

$$\overline{f(a,b)} = \overline{f}(\overline{a}, \overline{b}) = 7.$$

Izjavna formula φ	Poved $\overline{\varphi}$	Komentar
$P(a)$	2 je praštevilo	Resnična izjava
$P(x)$	x je praštevilo	Ni izjava
$\forall x\colon P(x)$	Vsako naravno število je praštevilo	Neresnična izjava
$P(f(a,b))$	7 je praštevilo	Resnična izjava

Tabela 7: Interpretacija izjavnih formul

»x je praštevilo« ni izjava, saj ji ne moremo določiti pravilnosti, dokler x ne zavzame številske vrednosti.

Opazimo sledeče:

1. zaprtim termom ustrezajo elementi D,
2. vsaki izjavni formuli φ ustreza neka poved $\overline{\varphi}$,

3. vsaki zaprti izjavni formuli φ ustreza izjava $\overline{\varphi}$ o elementih D.

Zgled 2.3.1.2. Podana je izjavna formula $\varphi = \forall x\ \exists y\colon R(x, y)$.

Interpretacija	Izjava $\overline{\varphi}$	Komentar
$D = \mathbb{N}$, $\overline{R}(x, y) \ldots x < y$	Za vsako naravno število obstaja večje naravno število	Resnična izjava
$D = \mathbb{N}$, $\overline{R}(x, y) \ldots x > y$	Za vsako naravno število obstaja manjše naravno število	Neresnična izjava
$D = \mathbb{Z}$, $\overline{R}(x, y) \ldots x > y$	Za vsako celo število obstaja manjše celo število	Resnična izjava
$D = \{\text{vsi ljudje}\}$, $\overline{R}(x, y) \ldots x$ ima rad y	Vsak ima nekoga rad	Izjava

Tabela 8: Zgled 2.3.1.2

Pogosto uporabljamo izjavne formule, ki niso zaprte. »Tihi privzetek« je, da je to izjavna formula, ki velja za vse individualne spremenljivke.

Definicija 2.3.2. Naj bo φ izjavna formula in $x_1, \ldots, x_n$ vse individualne spremenljivke, ki nastopajo v φ. Potem je

$$z(\varphi) = \forall x_1 \ldots \forall x_n\colon \varphi$$

univerzalno zaprtje formule φ.

Definicija 2.3.3. Izjavna formula φ je *resnična* v interpretaciji I, če je resnična izjava $\overline{z(\varphi)}$. Pišemo $I \models \varphi$.

2.4 Logično veljavne formule in enakovrednosti

Definicija 2.4.1. Izjavna formula φ je

1. *logično veljavna*, če je resnična v vseh možnih interpretacijah
2. *protislovna*, če je neresnična v vseh interpretacijah

Zgled 2.4.1.1. Naj bosta P, Q enomestna predikata in $\varphi = (\forall x\colon P(x) \vee \forall x\colon Q(x) \Rightarrow \forall x\colon (P(x) \vee Q(x)))$. φ je logično veljavna:

Naj bo I poljubna interpretacija φ. Uporabimo pogojni sklep. Predpostavimo

$$I \models \forall x\colon P(x) \vee \forall x\colon Q(x).$$

Vzemimo poljuben $x_0 \in D$. Ločimo dva primera:

a) $I \models \forall x\colon P(x)$. Potem $I \models P(x_0)$

b) $I \models \forall x\colon Q(x)$. Potem $I \models Q(x_0)$

Ker je $x_0 \in D$ poljuben, sledi

$$I \models \forall x\colon (P(x) \vee Q(x)).$$

Ker je I poljubna interpretacija, je φ logično veljavna. □

Zgled 2.4.1.2. Naj bo $\psi = \forall x\colon (P(x) \vee Q(x)) \Rightarrow \forall x\colon P(x) \vee \forall x\colon Q(x)$. ψ ni logično veljavna. Kot protiprimer lahko namreč izberemo $D = \mathbb{N}$, $P(x) \ldots$ x je sod in $Q(x) \ldots$ x je lih.

Zgled 2.4.1.3. Naj bo $\chi = \exists y\ \forall x\colon (R(x, y) \Leftrightarrow \neg R(x, x))$. χ je protislovje:

Naj bo I poljubna interpretacija. Recimo $I \models \chi$. Torej obstaja y_0, da je $\forall x\colon (R(x, y_0) \Leftrightarrow \neg R(x, x))$. Sledi, da je $R(y_0, y_0) \Leftrightarrow \neg R(y_0, y_0)$, kar pa je protislovje. Ker je I poljubna, je χ protislovna.

Definicija 2.4.2. Izjavni formuli φ in ψ sta *enakovredni*, če je formula $\varphi \Leftrightarrow \psi$ logično veljavna. Pišemo $\varphi \sim \psi$.

Izrek 2.4.3. Naj bosta φ, ψ poljubni izjavni formuli in x, y poljubni individualni spremenljivki. Potem:

1. $\neg\forall x\colon \varphi \sim \exists x\colon \neg\varphi$
2. $\neg\exists x\colon \varphi \sim \forall x\colon \neg\varphi$
3. $\forall x\ \forall y\colon \varphi \sim \forall y\ \forall x\colon \varphi$
4. $\exists x\ \exists y\colon \varphi \sim \exists y\ \exists x\colon \varphi$
5. $\forall x\colon (\varphi \wedge \psi) \sim \forall x\colon \varphi \wedge \forall x\colon \psi$
6. $\exists x\colon (\varphi \vee \psi) \sim \exists x\colon \varphi \vee \exists x\colon \psi$
7. $\forall x\colon (\varphi \vee \psi) \sim \forall x\colon \varphi \vee \psi$, če x ne nastopa prosto v ψ
8. $\exists x\colon (\varphi \wedge \psi) \sim \exists x\colon \varphi \wedge \psi$, če x ne nastopa prosto v ψ

9. $\forall x\colon \varphi \sim \varphi$, če x ne nastopa prosto v φ
10. $\exists x\colon \varphi \sim \varphi$, če x ne nastopa prosto v φ
11. $\forall x\colon \varphi(x) \sim \forall y\colon \varphi(y)$, če y ne nastopa v $\varphi(x)$
12. $\exists x\colon \varphi(x) \sim \exists y\colon \varphi(y)$, če y ne nastopa v $\varphi(x)$

Definicija 2.4.4. Za vsako izjavno formulo φ obstaja enakovredna formula ψ, pri kateri vsi kvantifikatorji stojijo na začetku. Taki formuli pravimo *preneksna oblika*.

Zgled 2.4.4.1. Izjavne formule lahko na naslednji način pretvorimo v preneksno obliko:

a) $\begin{aligned}\neg\forall x\ \exists y\colon R(x,y) &\sim \exists x\colon (\neg\exists y\colon R(x,y))\\ &\sim \exists x\ \forall y\colon \neg R(x,y)\end{aligned}$

b) $\begin{aligned}\exists x\colon P(x) \wedge \exists x\colon Q(x) &\sim \exists x\colon P(x) \wedge \exists y\colon Q(y)\\ &\sim \exists x\colon (\exists y\colon Q(y) \wedge P(x))\\ &\sim \exists x\ \exists y\colon (P(x) \wedge Q(y))\end{aligned}$

2.5 Sklepanje in dokazovanje v predikatnem računu

Definicija 2.5.1. Končno zaporedje izjavnih formul $\varphi_1, \ldots, \varphi_k, \psi$ je *pravilen* ali *veljaven sklep*, če je izjavna formula

$$\varphi_1 \wedge \cdots \wedge \varphi_k \Rightarrow \psi$$

logično veljavna.

Zgled 2.5.1.1. Velja

$$P(a), \forall x\colon (P(x) \Rightarrow Q(x)) \models Q(a).$$

Dokaz. Naj bo I poljubna interpretacija. Dokažimo, da

$$I \models P(a) \wedge \forall x\colon (P(x) \Rightarrow Q(x)) \Rightarrow Q(a).$$

Uporabimo pogojni sklep. Privzemimo, da

$$I \models P(a) \wedge \forall x\colon (P(x) \Rightarrow Q(x)),$$

torej velja

$$I \models P(a) \quad \text{in} \quad I \models \forall x\colon (P(x) \Rightarrow Q(x)).$$

To pomeni, da

$$I \models P(a) \Rightarrow Q(a),$$

zato $I \models Q(a)$ (modus ponens). S tem je dokaz končan. □

3 Množica

»Brijem vse tiste može iz mesta in samo tiste može, ki se ne brijejo sami.«

—Paradoks o brivcu

3.1 Podajanje množic

V teoriji množic je edini osnovni pojem *množica*. Vse druge matematične objekte lahko definiramo z množicami. Tako lahko na primer naravna števila definiramo na sledeč način:

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \{0\} \\ 2 &= \{0, 1\} \\ &\vdots \\ n+1 &= \{0, 1, 2, \ldots, n\} \\ &\vdots \end{aligned}$$

V teoriji množic je osnovna relacija *pripadnost* ($\in$).

Aksiom ekstenzionalnosti (AE):

$$\forall x \colon (x \in A \Leftrightarrow x \in B) \Rightarrow A = B$$

Če imata množici iste elemente, sta enaki.

Majhne končne množice lahko tako podamo z naštevanjem vseh elementov, na primer $A = \{1, 4, 9\}$. Sicer množice podamo z neko izjavno formulo $\varphi(x)$, kjer prosto nastopa le spremenljivka x: $A = \{x \mid \varphi(x)\}$. To je okrajšava za formulo

$$\forall x \colon (x \in A \Leftrightarrow \varphi(x)).$$

Russellovo vprašanje: Ali za množico $E = \{x \mid x \notin x\}$ velja $E \in E$?

Po definiciji E velja $E \in E \Leftrightarrow \varphi(E) \Leftrightarrow E \notin E$. Naj bo

$$\psi \colon \exists y \; \forall x \colon (R(x, y) \Leftrightarrow \neg R(x, x)).$$

Vzamemo interpretacijo I, pri kateri je $D = \{x \mid x = x\}$ razred vseh množic in $xRy \ldots x \in y$. Vemo, da je ψ protislovna, zato je $\neg\psi$ logično veljavna in resnična tudi v I. To pomeni, da

$$\neg \exists E \; \forall x \colon (x \in E \Leftrightarrow x \notin x),$$

torej Russellova množica ne obstaja.

Kako »popraviti« način podajanja množic?

A) *NMG* (von Neumann–Bernays–Gödel):

Osnovni pojem je *razred*. Nekateri razredi so množice, drugi pa *pravi razredi*. Razred A je *množica*, če $\exists B\colon A \in B$. Označimo $M(x) \dots x$ je množica. Množico A podamo kot

$$A = \{x \mid \varphi(x) \wedge M(x)\}\,.$$

Vzemimo $R = \{x \mid x \notin x \wedge M(x)\}$. Potem lahko izpeljemo $R \notin R \wedge \neg M(R)$. R je pravi razred.

B) *ZFC* (Zermelo–Fraenklova teorija z aksiomom izbire):

Edini osnovni pojem je *množica*. Privzamemo *eksistenčne aksiome*, ki nam zagotavljajo obstoj dovolj »majhnih« množic.

Standardna interpretacija formul teorije ZFC:

- $D = V = \{x;\ x = x\}$ je razred vseh množic
- $x \in y$ je relacija pripadnosti
- $x = y$ je relacija enakosti

3.2 Relacije med množicami

3.2.1 Relacija enakosti

Enakost v matematiki pojmujemo kot istost.

Načelo zamenljivosti enakega z enakim (EE): Če je $A = B$, potem vse tisto, kar velja za A, velja tudi za B in obratno.

Trditev 3.2.1. $A = B \Leftrightarrow \forall x \colon (x \in A \Leftrightarrow x \in B)$.

Dokaz. Trditev je direktna posledica aksioma ekstenzionalnosti in načela zamenljivosti enakega z enakim. □

Posledica 3.2.1.1. Veljajo naslednje lastnosti:

(i) $A = A$ (refleksivnost)

(ii) $A = B \Rightarrow B = A$ (simetričnost)

(iii) $A = B \wedge B = C \Rightarrow A = C$ (tranzitivnost)

Dokaz. The proof is obvious and need not be mentioned. □

3.2.2 Relacija inkluzije

Definicija 3.2.2. *Relacija inkluzije* ($\subseteq$) je definirana kot

$$A \subseteq B \Leftrightarrow \forall x\colon (x \in A \Rightarrow x \in B).$$

To preberemo kot »A je *podmnožica* B«. Namesto $\neg(A \subseteq B)$ pišemo $A \not\subseteq B$.

Trditev 3.2.3. $A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$.

Dokaz. The proof is obvious and need not be mentioned. □

Aksiomska shema o podmnožicah (ASP): Če B obstaja in je $\varphi(x)$ izjavna formula, v kateri prosto nastopa le x, obstaja tudi množica

$$A = \{x \mid x \in B \wedge \varphi(x)\},$$

oziroma

$$\forall B\ \exists A\ \forall x\colon (x \in A \Leftrightarrow x \in B \wedge \varphi(x)).$$

Definicija 3.2.4. Množica A je *prazna*, če $\forall x\colon x \notin A$.

Posledica 3.2.4.1. Prazna množica obstaja. Imamo namreč množico A, za katero je

$$\forall B\ \exists A\ \forall x\colon (x \in A \Leftrightarrow x \in B \wedge x \neq x),$$

od koder sledi $\exists A\ \forall x\colon x \notin A$.

Posledica 3.2.4.2. Razred vseh množic V ni množica (je pravi razred).

Dokaz. Predpostavimo, da je V množica. Potem obstaja $A = \{x \mid x \in V \wedge x \notin x\}$, kar je protislovje. □

Aksiom o paru (AP): Če obstajata u in v, obstaja tudi

$$A = \{u, v\} = \{x \mid x = u \vee x = v\}.$$

Posledica 3.2.4.3. Če obstaja u, obstaja $A = \{u\}$.

Dokaz. V aksiomu o paru vzamemo $u = v$. □

Izrek 3.2.5. Veljajo naslednje lastnosti:

(i) $A \subseteq A$ (refleksivnost)

(ii) $A \subseteq B \wedge B \subseteq A \Rightarrow A = B$ (antisimetričnost)

(iii) $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$ (tranzitivnost)

(iv) $\emptyset \subseteq A$

(v) $A \subseteq \emptyset \Rightarrow A = \emptyset$

Dokaz. The proof is obvious and need not be mentioned. □

3.2.3 Relacija stroge inkluzije

Definicija 3.2.6. *Relacija stroge inkluzije* ($\subset$) je definirana kot

$$A \subset B \Leftrightarrow A \subseteq B \wedge A \neq B.$$

Pravimo, da je A *prava podmnožica* B. Namesto $\neg(A \subset B)$ pišemo $A \not\subset B$.

Trditev 3.2.7. Velja $A \subset B \Leftrightarrow A \subseteq B \wedge \exists x \colon (x \in B \wedge x \notin A)$.

Dokaz. The proof is obvious and need not be mentioned. □

Izrek 3.2.8. Za vse množica A, B in C velja:

(i) $A \not\subset A$ (irefleksivnost)

(ii) $A \subset B \Rightarrow B \not\subset A$ (asimetričnost)

(iii) $A \subset B \wedge B \subset C \Rightarrow A \subset C$ (tranzitivnost)

Dokaz. The proof is obvious and need not be mentioned. □

3.3 Operacije z množicami

3.3.1 Unija, presek, razlika, Boolova vsota

Definicija 3.3.1. Definiramo naslednje operacije:

$A \cup B = \{x \mid x \in A \vee x \in B\}$ –*unija*

$A \cap B = \{x \mid x \in A \wedge x \in B\}$ –*presek*

$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$ –*razlika*

$A \oplus B = \{x \mid x \in A + x \in B\}$ –*Boolova vsota* ali –*simetrična razlika*

Trditev 3.3.2. Za poljubni množici A in B obstajata $A \cap B$ in $A \setminus B$.

Dokaz. The proof is obvious and need not be mentioned. □

Izrek 3.3.3. Za vse množice A, B in C velja:

(i) Operacije s prazno množico:
- $A \cup \emptyset = A$
- $A \setminus \emptyset = A$
- $A \oplus \emptyset = A$
- $A \cap \emptyset = \emptyset$
- $\emptyset \setminus A = \emptyset$

(ii) Idempotenci:
- $A \cup A = A$
- $A \cap A = A$

(iii) Komutativnosti:
- $A \cup B = B \cup A$
- $A \cap B = B \cap A$
- $A \oplus B = B \oplus A$

(iv) Asociativnosti:
- $(A \cup B) \cup C = A \cup (B \cup C)$
- $(A \cap B) \cap C = A \cap (B \cap C)$
- $(A \oplus B) \oplus C = A \oplus (B \oplus C)$

(v) Absorpciji:
- $A \cup (A \cap B) = A$
- $A \cap (A \cup B) = A$

(vi) Distributivnosti:
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$

(vii) Monotonosti:
- $A \subseteq B \Rightarrow A \cup C \subseteq B \cup C$
- $A \subseteq B \Rightarrow A \cap C \subseteq B \cap C$

(viii) $A \oplus B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$

(ix) $A \cap B \subseteq A \subseteq A \cup B$

(x) $A \subseteq B \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B = A \Leftrightarrow A \setminus B = \emptyset$

Dokaz. The proof is obvious and need not be mentioned. □

Definicija 3.3.4. Naj bo A množica in φ izjavna formula. Potem sta formuli

$$\forall x \in A \colon \varphi \qquad \text{in} \qquad \exists x \in A \colon \varphi$$

okrajšavi za $\forall x \colon (x \in A \Rightarrow \varphi)$ in $\exists x \colon (x \in A \wedge \varphi)$ zaporedoma.

Opomba 3.3.4.1. Če $A \neq \emptyset$, za kvantifikatorja $\forall x \in A$ in $\exists x \in A$ veljajo analogne enakovrednosti kot za $\forall x$ in $\exists x$.

Definicija 3.3.5. Naj bo A neprazna množica. Potem je

$$\bigcup A = \{x \mid \exists y \in A \colon x \in y\} \qquad \text{in} \qquad \bigcap A = \{x \mid \forall y \in A \colon x \in y\}$$

Trditev 3.3.6. $\forall y \in A \colon y \subseteq \bigcup A$ in $\forall y \in A \colon \bigcap A \subseteq y$ za neprazen A.

Dokaz. The proof is obvious and need not be mentioned. □

Aksiom o uniji (AU):

$$\forall A \; \exists B \; \forall x \colon (x \in B \Leftrightarrow \exists y \in A \colon x \in y)$$

Za vsako množico A obstaja njena unija.

Posledica 3.3.6.1. Za poljubni množici A in B obstajata množici $A \cup B$ in $A \oplus B$.

Dokaz. Obstaja unija $\{A, B\}$, ki obstaja po aksiomu o paru. Ker velja $A \oplus B \subseteq A \cup B$, smo končali. □

Trditev 3.3.7. Naj bo $A \neq \emptyset$. Potem obstaja $\bigcap A$.

Dokaz. Vzemimo poljuben element $y_0 \in A$. Potem obstaja množica

$$P = \{x \mid x \in y_0 \wedge \forall y \in A \colon x \in y\} = \{x \mid \forall y \in A \colon x \in y\} = \bigcap A.$$ □

3.3.2 Komplement množice

Pogosto se omejimo na neko *univerzalno množico* ali *svet* S in gledamo le njene podmnožice.

Definicija 3.3.8. Naj bo $A \subseteq S$. *Komplement množice* A je definiran kot

$$A^{\mathsf{c}} = \{x \in S \mid x \notin A\} = S \setminus A.$$

Izrek 3.3.9. Za vse $A, B, C \subseteq S$ velja:

1. $(A^{\mathsf{c}})^{\mathsf{c}} = A$
2. $(A \cup B)^{\mathsf{c}} = A^{\mathsf{c}} \cap B^{\mathsf{c}}$
3. $(A \cap B)^{\mathsf{c}} = A^{\mathsf{c}} \cup B^{\mathsf{c}}$
4. $A \setminus B = A \cap B^{\mathsf{c}}$
5. $A \subseteq B \Leftrightarrow B^{\mathsf{c}} \subseteq A^{\mathsf{c}}$
6. $A \cap B = \emptyset \Leftrightarrow A \subseteq B^{\mathsf{c}} \Leftrightarrow B \subseteq A^{\mathsf{c}}$
7. $A \cup A^{\mathsf{c}} = S$, $A \cap A^{\mathsf{c}} = \emptyset$
8. $A \cup S = S$, $A \cap S = A$

Dokaz. The proof is obvious and need not be mentioned. □

Opomba 3.3.9.1. Za $A \subseteq S$ lahko definiramo

$$\bigcap A = \{x \in S \mid \forall y \in A \colon x \in y\}.$$

Potem je

$$\bigcap \emptyset = \{x \mid x \in S\} = S.$$

3.3.3 Potenčna množica

Definicija 3.3.10. *Potenčna množica* množice A je definirana kot

$$\mathcal{P}A = \{x \mid x \subseteq A\}.$$

Opomba 3.3.10.1. Velja ekvivalenca

$$x \in \mathcal{P}A \Leftrightarrow x \subseteq A.$$

Aksiom o potenčni množici (APM):

$$\forall A\ \exists B\ \forall x\colon (x \in B \Leftrightarrow x \subseteq A)$$

Za vsako množico A obstaja njena potenčna množica.

Izrek 3.3.11. Za vse A, B velja

1. $\emptyset \in \mathcal{P}A$, $A \in \mathcal{P}A$
2. $\bigcup \mathcal{P}A = A$, $\bigcap \mathcal{P}A = \emptyset$
3. $A \subseteq B \Rightarrow \mathcal{P}A \subseteq \mathcal{P}B$
4. $\mathcal{P}A \cap \mathcal{P}B = \mathcal{P}(A \cap B)$
5. $\mathcal{P}A \cup \mathcal{P}B \subseteq \mathcal{P}(A \cup B)$

Dokaz. The proof is obvious and need not be mentioned. □

3.3.4 Urejeni pari in kartezični produkt

Definicija 3.3.12. *Urejen par* definiramo kot

$$(a, b) = \{\{a, b\}, \{a\}\}.$$

Izrek 3.3.13. Za vse a, b, c, d velja

$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d.$$

Dokaz. Če je $a = c$ in $b = d$, je očitno $(a, b) = (c, d)$. Zdaj predpostavimo, da je $(a, b) = (c, d)$. To pomeni, da je

$$\{\{a, b\}, \{a\}\} = \{\{c, d\}, \{c\}\}.$$

Sledi, da je $\{a\} = \{c\}$ ali $\{a\} = \{c, d\}$. V obeh primerih sledi $a = c$. Zdaj ločimo dva primera:

1. $a = b$: Sledi, da je

   $$\{\{a, d\}, \{a\}\} = \{\{a, b\}, \{a\}\} = \{\{a\}\},$$

   torej je $d = a$ in $a = b = c = d$.

2. $a \neq b$: Ker je

   $$\{\{a, b\}, \{a\}\} = \{\{a, d\}, \{a\}\},$$

   je $\{a, b\} = \{a\}$ ali $\{a, d\}$. Ker $b \neq a$, je edina možnost $b = d$. □

Trditev 3.3.14. Za vse a, b obstaja (a, b).

Dokaz. Dvakrat uporabimo aksiom o paru. □

Definicija 3.3.15. Množica vseh parov, kjer prva komponenta pripada A, druga pa B,je *kartezični produkt* množic A in B:

$$A \times B = \{(x, y) \mid x \in A \wedge y \in B\}.$$

Trditev 3.3.16. Za poljubni množici A in B obstaja $A \times B$.

Dokaz. Dovolj je opaziti $A \times B \subseteq \mathcal{PP}(A \cup B)$. Velja namreč

$$\begin{aligned} A \times B &= \{x \mid x \in \mathcal{PP}(A \cup B) \wedge \exists u\, \exists v \colon (u \in A \wedge v \in B \wedge x = (u, v))\} \\ &= \{x \mid \exists u\, \exists v \colon (u \in A \wedge v \in B \wedge x = (u, v))\}. \end{aligned}$$ □

Izrek 3.3.17. Za vse A, B, C, D velja:

1. Produkt s prazno množico:
   - $A \times \emptyset = \emptyset \times A = \emptyset$
2. Distributivnost:

- $A \times (B \cup C) = (A \times B) \cup (A \times C)$
- $(A \cup B) \times C = (A \times C) \cup (B \times C)$

3. Superdistributivnost:
   - $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$
4. $A \times B = \emptyset \Leftrightarrow A = \emptyset \vee B = \emptyset$
5. Monotonost:
   - $A \subseteq C \wedge B \subseteq D \Rightarrow A \times B \subseteq C \times D$
6. $A \times B \subseteq C \times D \wedge A \times B \neq \emptyset \Rightarrow A \subseteq C \wedge B \subseteq D$

Definicija 3.3.18. Naj bo $n \in \mathbb{N}$, $n \geq 3$. Induktivno definiramo urejeno n-terico:

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n).$$

Izrek 3.3.19. Za vse $n \in \mathbb{N}$, $n \geq 2$, velja

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \Leftrightarrow \forall i \in \{1, 2, \ldots, n\} : a_i = b_i.$$

Dokaz. Indukcija po n. □

Definicija 3.3.20. Za $n \in \mathbb{N}$, $n \geq 2$ je kartezični produkt množic A_1, A_2, $\ldots$, A_n definiran kot

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid \forall i \in \{1, 2, \ldots, n\} : a_i \in A_i\}$$

4 Relacije in funkcije

»Tukaj se bo Gregor gotovo pritožil.«
—prof. dr. Marko Petkovšek

4.1 Relacije in njihove lastnosti

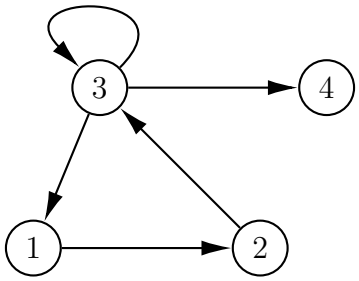
Definicija 4.1.1. Množica R je *dvomestna relacija*, če so njeni elementi urejeni pari, oziroma

$$\forall x \in R\ \exists a\ \exists b\colon x = (a, b).$$

Množica R je *dvomestna relacija v* A, če $R \subseteq A \times A$.

Posebej definiramo *prazno relacijo* kot $\emptyset$, *univerzalno relacijo* kot $A \times A$ in *relacijo enakosti* ali *identitete* kot $\mathrm{id}_A = \{(x, x) \mid x \in A\}$.

Relacijo na »majhni« množici lahko predstavimo z usmerjenim grafom.



Slika 1: Relacija $R = \{(1,2), (2,3), (3,1), (3,3), (3,4)\}$

Namesto $(x, y) \in R$ lahko pišemo $x\ R\ y$.

Definicija 4.1.2. Naj bo $R \subseteq A \times A$. Potem označimo *domeno* oziroma *definicijsko območje* R

$$\mathcal{D}_R = \{x \in A \mid \exists y \in A\colon x\ R\ y\}$$

in *zalogo vrednosti* R

$$\mathcal{Z}_R = \{y \in A \mid \exists x \in A\colon x\ R\ y\}\,.$$

Definicija 4.1.3. Pravimo, da je relacija $R \subseteq A \times A$:

1. *refleksivna*, če $\forall x \in A\colon x\ R\ x$
2. *irefleksivna*, če $\forall x \in A\colon \neg x\ R\ x$
3. *simetrična*, če $\forall x, y \in A\colon (x\ R\ y \Rightarrow y\ R\ x)$
4. *antisimetrična*, če $\forall x, y \in A\colon (x\ R\ y \wedge y\ R\ x \Rightarrow x = y)$
5. *asimetrična*, če $\forall x, y \in A\colon (x\ R\ y \Rightarrow \neg y\ R\ x)$
6. *tranzitivna*, če $\forall x, y, z \in A\colon (x\ R\ y \wedge y\ R\ z \Rightarrow x\ R\ z)$
7. *intranzitivna*, če $\forall x, y, z \in A\colon (x\ R\ y \wedge y\ R\ z \Rightarrow \neg x\ R\ z)$

8. *strogo sovisna*, če $\forall x, y \in A\colon x\ R\ y \vee y\ R\ x$
9. *sovisna*, če $\forall x, y \in A\colon (x \neq y \Rightarrow x\ R\ y \vee y\ R\ x)$
10. *enolična*, če $\forall x, y, z \in A\colon (x\ R\ y \wedge x\ R\ z \Rightarrow y = z)$

Trditev 4.1.4. Naj bo $R \subseteq A \times A$. Potem je

1. R je asimetrična $\Leftrightarrow$ R je antisimetrična in irefleksivna,
2. R je strogo sovisna $\Leftrightarrow$ R je sovisna in refleksivna.

Dokaz. The proof is obvious and need not be mentioned. □

4.2 Ekvivalenčne relacije

Definicija 4.2.1. Relacija $R \subseteq A \times A$ je *ekvivalenčna*, če je refleksivna, simetrična in tranzitivna.

Definicija 4.2.2. Naj bo $R \subseteq A \times A$ ekvivalenčna relacija.

1. Vsakemu $x \in A$ priredimo *ekvivalenčni razred* $R[x] = \{y \in A \mid y\ R\ x\}$. Elementu x je *predstavnik* $R[x]$.
2. *Faktorska* ali *kvocientna množica* A po R je množica vseh ekvivalenčnih razredov R v A:
$$A/R = \{R[x] \mid x \in A\}\,.$$

Lema 4.2.3. Naj bo $R \subseteq A \times A$ ekvivalenčna relacija. Potem je
$$\forall x, y \in A\colon (R[x] = R[y] \Leftrightarrow x\ R\ y).$$

Dokaz. The proof is obvious and need not be mentioned. □

Posledica 4.2.3.1. Vsak element ekvivalenčnega razreda je tudi njegov predstavnik.

Izrek 4.2.4. Naj bo $R \subseteq A \times A$ ekvivalenčna relacija. Potem R razdeli množico A na paroma tuje neprazne množice, oziroma:

1. $\forall x \in A\colon R[x] \neq \emptyset$
2. $\forall x, y \in A\colon (R[x] \neq R[y] \Rightarrow R[x] \cap R[y] = \emptyset)$
3. $\bigcup(A/R) = A$

Dokaz. The proof is obvious and need not be mentioned. □

4.3 Operacije z relacijami

Trditev 4.3.1. Naj bosta $R, S \subseteq A \times A$ relaciji. Potem so tudi

$$R \cup S, R \cap S, R \setminus S, R \oplus S \subseteq A \times A$$

relacije v A in velja:

1. $x\ R \cup S\ y \Leftrightarrow x\ R\ y \vee x\ S\ y$
2. $x\ R \cap S\ y \Leftrightarrow x\ R\ y \wedge x\ S\ y$
3. $x\ R \setminus S\ y \Leftrightarrow x\ R\ y \wedge \neg(x\ S\ y)$
4. $x\ R \oplus S\ y \Leftrightarrow x\ R\ y + x\ S\ y$

Definicija 4.3.2. Naj bo $R \subseteq A \times A$. *Komplement relacije* R je relacija

$$R^{\mathsf{c}} = (A \times A) \setminus R.$$

Transponirana relacija relacije R je relacija

$$R^{\top} = \{(x, y) \mid (y, x) \in R\}.$$

Kompozitum relacij $R, S \subseteq A \times A$ je relacija

$$R \circ S = \{(x, y) \mid \exists u \in A \colon (x\ S\ u \wedge u\ R\ y)\}.$$

Trditev 4.3.3. Za vse $x, y \in A$ velja:

1. $x\ R^{\mathsf{c}}\ y \Leftrightarrow \neg x\ R\ y$
2. $x\ R^{\top}\ y \Leftrightarrow y\ R\ x$

Izrek 4.3.4. Za poljubne $R, S, T \subseteq A \times A$ velja

1. $(R^{\top})^{\top} = R$
2. - $(R \cup S)^{\top} = R^{\top} \cup S^{\top}$
   - $(R \cap S)^{\top} = R^{\top} \cap S^{\top}$
   - $(R \setminus S)^{T} = R^{\top} \setminus S^{\top}$
   - $(R \oplus S)^{\top} = R^{\top} \oplus S^{\top}$
3. $R \circ \mathrm{id}_A = \mathrm{id}_A \circ R = R$
4. $(R \circ S) \circ T = R \circ (S \circ T)$
5. $(R \circ S)^{\top} = S^{\top} \circ R^{\top}$
6. - $R \circ (S \cup T) = R \circ S \cup R \circ T$
   - $(R \cup S) \circ T = T \circ T \cup S \circ T$
7. $R \subseteq S \Rightarrow R \circ T \subseteq S \circ T \wedge T \circ R \subseteq T \circ S$

Dokaz. The proof is obvious and need not be mentioned. □

Izrek 4.3.5. Naj bo $R \subseteq A \times A$.

1. R je refleksivna $\Leftrightarrow \mathrm{id}_A \subseteq R$

2. R je irefleksivna $\Leftrightarrow R \cap \mathrm{id}_A = \emptyset$
3. R je simetrična $\Leftrightarrow R = R^\top$
4. R je asimetrična $\Leftrightarrow R \cap R^\top = \emptyset$
5. R je antisimetrična $\Leftrightarrow R \cap R^\top \subseteq \mathrm{id}_A$
6. R je tranzitivna $\Leftrightarrow R \circ R \subseteq R$
7. R je intranzitivna $\Leftrightarrow R \circ R \cap R = \emptyset$
8. R je strogo sovisna $\Leftrightarrow R \cup R^\top = A \times A$
9. R je sovisna $\Leftrightarrow R \cup R^\top \cup \mathrm{id}_A = A \times A$
10. R je enolična $\Leftrightarrow R \circ R^\top \subseteq \mathrm{id}_A$

Dokaz. The proof is obvious and need not be mentioned. □

4.4 Potence in ovojnice relacij

Definicija 4.4.1. Naj bo $R \subseteq A \times A$ relacija. *Kompozicijsko potenco* definiramo induktivno:

1. $R^0 = \mathrm{id}_A$
2. $\forall n \in \mathbb{N}\colon R^{n+1} = R^n \circ R$

Ekvivalentno je za $n \geq 1$

$$R^n = \underbrace{R \circ R \circ \cdots \circ R}_{n}.$$

Trditev 4.4.2. Za vse $n, m \in \mathbb{N}$ velja:

1. $R^n \circ R^m = R^{n+m}$
2. $(R^n)^m = R^{nm}$

Dokaz. Indukcija. □

Definicija 4.4.3. Naj bo $R \subseteq A \times A$ relacija.

1. $R^+ = \bigcup \left\{ R^k \mid k \in \mathbb{N} \setminus \{0\} \right\}$
2. $R^* = \bigcup \left\{ R^k \mid k \in \mathbb{N} \right\}$

Trditev 4.4.4. Veljajo naslednje trditve:

1. $R^* = R^+ \cup \mathrm{id}_A$
2. $\forall x, y \in A\colon (x\ R^+\ y \Leftrightarrow \exists k \in \mathbb{N} \setminus \{0\} : x\ R^k\ y)$
3. $\forall x, y \in A\colon (x\ R^*\ y \Leftrightarrow \exists k \in \mathbb{N}\colon x\ R^k\ y)$

Dokaz. The proof is obvious and need not be mentioned. □

Definicija 4.4.5. Naj bo $R \subseteq A \times A$ relacija in L neka lastnost relacij v množici A (torej $L \subseteq \mathcal{P}(A \times A)$). Relacija R^L je *L-ovojnica* relacije R, če velja:

1. $R \subseteq R^L$
2. $R^L \in L$
3. $\forall S \subseteq A \times A\colon (R \subseteq S \wedge S \in L \Rightarrow R^L \subseteq S)$

Opomba 4.4.5.1. Če je $R \in L$, je $R^L = R$.

Opomba 4.4.5.2. R^L ne obstaja vedno.

Izrek 4.4.6. Za vsako relacijo $R \subseteq A \times A$ obstajajo ovojnice

$$R^{\text{refl.}},\ R^{\text{sim.}},\ R^{\text{tranz.}},\ R^{\text{refl. in tranz.}} \text{ in } R^{\text{ekvival.}}.$$

Izrazimo jih lahko kot

1. $R^{\text{refl.}} = R \cup \mathrm{id}_A$
2. $R^{\text{sim.}} = R \cup R^{\top}$
3. $R^{\text{tranz.}} = R^{+}$
4. $R^{\text{refl. in tranz.}} = R^{*}$
5. $R^{\text{ekvival.}} = (R \cup R^{\top})^{*}$

Dokaz. The proof is obvious and need not be mentioned. □

4.5 Funkcije ali preslikave

Definicija 4.5.1. *Funkcija* ali *preslikava* je enolična dvomestna relacija.

Definicija 4.5.2. Urejena trojica (f, A, B) je funkcija ali preslikava množice A v množico B, če velja:

1. f je enolična relacija v $A \cup B$
2. $\mathcal{D}_f = A$
3. $\mathcal{Z}_f \subseteq B$

Namesto (f, a, b) pišemo $f\colon A \to B$, namesto $(x, y) \in f$ ali $x\ f\ y$ pišemo $f(x) = y$ ali $f\colon x \mapsto y$. Formula $f(x) = f(y)$ je okrajšava za formulo

$$\exists z\colon (x\ f\ z \wedge y\ f\ z).$$

4.5.1 Lastnosti funkcij

Definicija 4.5.3. Naj bo $f\colon A \to B$ funkcija.

1. f je *injektivna*, če $\forall x, y \in A\colon (f(x) = f(y) \Rightarrow x = y)$
2. f je *surjektivna*, če $\forall y \in B\ \exists x \in A\colon f(x) = y$
3. f je *bijektivna*, če je injektivna in surjektivna.

Definicija 4.5.4. Posebej definiramo naslednje funkcije:

1. $\emptyset$ je *prazna preslikava*
2. $\mathrm{id}_A\colon A \to A$, $\forall x \in A\colon \mathrm{id}_A(x) = x$ je *identična preslikava* na A
3. $i\colon A \to B$, kjer je $A \subseteq B$ in $\forall x \in A\colon i(x) = x$, je *vložitev* A v B
4. $p_i\colon A_1 \times A_2 \times \cdots \times A_n \to A_i$, kjer je $p_i((a_1, a_2, \ldots, a_n)) = a_i$, je *projekcija* na i-to komponento
5. $p\colon A \to A/R$, kjer je $R \subseteq A \times A$ ekvivalenčna relacija in $\forall x \in A\colon p(x) = R[x]$ je *naravna kvocientna projekcija*
6. Za $A \subseteq S$ je $\chi_A\colon S \to \{0, 1\}$, kjer je

$$\forall x \in S\colon \chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A, \end{cases}$$

karakteristična funkcija množice A glede na S

Definicija 4.5.5. Preslikavo $f\colon A_1 \times \cdots \times A_n \to B$ imenujemo funkcija n *spremenljivk*. Namesto $f((x_1, \ldots, x_n))$ pišemo $f(x_1, \ldots, x_n)$.

Definicija 4.5.6. Naj bo $f\colon A \to B$ funkcija in $C \subseteq A$. Preslikava $g\colon C \to B$, kjer je $\forall x \in C\colon g(x) = f(x)$, je *zožitev* f na C. Pišemo $g = f|_C$.

4.5.2 Operacije s funkcijami

Trditev 4.5.7. $\mathcal{D}_{f^\top} = \mathcal{Z}_f$ in $\mathcal{Z}_{f^\top} = \mathcal{D}_f$.

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 4.5.8. Naj bo $f\colon A \to B$ funkcija.

1. $f^\top$ je funkcija natanko tedaj, ko je f injektivna.
2. $f^\top\colon B \to A$ natanko tedaj, ko je f bijektivna.

Dokaz. Dokažimo prvo trditev. Velja

$$\begin{aligned} f^\top \text{ je funkcija} &\Leftrightarrow \forall x, y, z\colon (x\ f^\top\ y \wedge x\ f^\top\ z \Rightarrow y = z) \\ &\Leftrightarrow \forall x, y, z\colon (y\ f\ x \wedge z\ f\ x \Rightarrow y = z) \\ &\Leftrightarrow \forall x, y, z\colon (\neg(y\ f\ x \wedge z\ f\ x) \vee y = z) \\ &\Leftrightarrow \forall y, z\colon (\neg\exists x\colon (y\ f\ x \wedge z\ f\ x) \vee y = z) \\ &\Leftrightarrow \forall y, z\colon (\neg(f(y) = f(z)) \vee y = z) \\ &\Leftrightarrow \forall y, z\colon (f(y) = f(z) \Rightarrow y = z). \end{aligned}$$

□

Definicija 4.5.9. Če je f injektivna, je $f^\top$ tudi funkcija, ki jo imenujemo *inverzna funkcija* in označimo $f^\top = f^{-1}$.

Definicija 4.5.10. Preslikavi $f\colon A \to B$ priredimo relacijo $K_f \subseteq A \times A$ tako:

$$\forall x, y \in A\colon x\ K_f\ y \Rightarrow f(x) = f(y).$$

Tej ekvivalenčni relaciji pravimo *kongruenca* funkcije f.

Trditev 4.5.11. Naj bo $f\colon A \to B$.

1. $f^\top \circ f = K_f$
2. $f \circ f^\top = \mathrm{id}_{\mathcal{Z}_f}$
3. f je injektivna $\Rightarrow f^\top \circ f = \mathrm{id}_A$
4. f je surjektivna $\Rightarrow f \circ f^\top = \mathrm{id}_B$

Dokaz. The proof is obvious and need not be mentioned. □

Posledica 4.5.11.1. Naj bo $f\colon A \to B$ bijekcija. Potem je $f^{-1} \circ f = \mathrm{id}_A$ in $f \circ f^{-1} = \mathrm{id}_B$.

Izrek 4.5.12. Veljata naslednji trditvi:

1. Če sta f in g funkciji, je tudi $f \circ g$ funkcija in
$$\forall x \in \mathcal{D}_{f\circ g}\colon (f \circ g)(x) = f(g(x)).$$
2. Naj bo $g\colon A \to B$ in $f\colon B \to C$. Potem $f \circ g\colon A \to C$.

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 4.5.13. Naj bo $f\colon A \to B$. Potem je

$$f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f.$$

Trditev 4.5.14. Naj bosta $f\colon B \to C$ in $g\colon A \to B$ funkciji.

1. Če sta f in g injektivni, je $f \circ g$ injektivna.
2. Če sta f in g surjektivni, je $f \circ g$ surjektivna.
3. Če je $f \circ g$ injektivna, je g injektivna.
4. Če je $f \circ g$ surjektivna, je f surjektivna..

Dokaz. The proof is obvious and need not be mentioned. □

Izrek 4.5.15. Naj bo $f\colon A \to B$ in $g\colon B \to A$. Če je $f \circ g = \mathrm{id}_B$ in $g \circ f = \mathrm{id}_A$, sta f in g bijekciji in je $g = f^{-1}$.

Dokaz. Oba kompozituma sta bijektivna in velja

$$g = \mathrm{id}_A \circ g = (f^{-1} \circ f) \circ g = f^{-1} \circ \mathrm{id}_B = f^{-1}.$$ □

4.5.3 Družine množic

Definicija 4.5.16. Naj bo M množica množic in $\mathcal{I}$ poljubna množica. Surjektivna preslikava $\mathcal{A}\colon \mathcal{I} \to M$ je *družina množic* z *indeksno množico* $\mathcal{I}$.

Za $\lambda \in \mathcal{I}$ namesto $\mathcal{A}(\lambda)$ pišemo $\mathcal{A}_\lambda$, družino pa označujemo tudi z $(\mathcal{A}_\lambda)_{\lambda\in\mathcal{I}}$.

Družino množic $(A_n)_{n\in\mathbb{N}}$ imenujemo *zaporedje*. Vsaka množica A je družina množic z indeksno množico A. Pravimo, da je družina množic *prazna*, če je $\mathcal{I} = \emptyset$.

Definicija 4.5.17. Naj bo $\mathcal{A} = (A_\lambda)_{\lambda\in\mathcal{I}}$ družina množic. Preslikava

$$f\colon \mathcal{I} \to \bigcup_{\lambda\in\mathcal{I}} A_\lambda,$$

pri kateri za vse $\lambda \in \mathcal{I}$ velja $f(\lambda) \in A_\lambda$, je *funkcija izbire* za družino $\mathcal{A}$.

Definicija 4.5.18. Podobno kot pri množicah lahko tudi za družine množic definiramo naslednje pojme:

1. Unija: $\displaystyle\bigcup_{\lambda\in\mathcal{I}} A_\lambda = \{x \mid \exists\lambda \in \mathcal{I}\colon x \in A_\lambda\}$
2. Presek: $\displaystyle\bigcap_{\lambda\in\mathcal{I}} A_\lambda = \{x \mid \forall\lambda \in \mathcal{I}\colon x \in A_\lambda\}$
3. Kartezični produkt: $\displaystyle\prod_{\lambda\in\mathcal{I}} A_\lambda = \left\{ f\colon \mathcal{I} \to \bigcup_{\lambda\in\mathcal{I}} A_\lambda \mid \forall\lambda \in \mathcal{I}\colon f(\lambda) \in A_\lambda \right\}$

Opomba 4.5.18.1. Če je indeksna množica prazna, je kartezični produkt enak

$$\prod_{\lambda\in\emptyset} A_\lambda = \{\emptyset\},$$

saj je $f\colon \emptyset \to \bigcup_{\lambda\in\emptyset} A_\lambda = \emptyset$ prazna funkcija.

Opomba 4.5.18.2. Vsako urejeno n-terico lahko identificiramo s funkcijo izbire z indeksno množico $\mathcal{I} = \{1, 2, \ldots, n\}$.

Očitno velja implikacija

$$\exists\lambda \in \mathcal{I}\colon A_\lambda = \emptyset \Rightarrow \prod_{\lambda\in\mathcal{I}} A_\lambda = \emptyset.$$

Obratnega ne moremo dokazati.

Aksiom izbire (AC): Kartezični produkt poljubne družine nepraznih množic je neprazen:

$$\forall\lambda \in \mathcal{I}\colon A_\lambda \neq \emptyset \Rightarrow \prod_{\lambda\in\mathcal{I}} A_\lambda \neq \emptyset.$$

4.5.4 Slike in praslike

Definicija 4.5.19. Naj bo $f\colon A \to B$ preslikava, $A_1 \subseteq A$ in $B_1 \subseteq B$.

1. $f_*(A_1) = \{y \in B \mid \exists x \in A_1 \colon y = f(x)\}$ je *slika* množice A_1 pri f.
2. $f^*(B_1) = \{x \in A \mid f(x) \in B_1\}$ je *praslika* množice B_1 pri f.

Velja $f_*\colon \mathcal{P}(A) \to \mathcal{P}(B)$ in $f^*\colon \mathcal{P}(B) \to \mathcal{P}(A)$.

Trditev 4.5.20. Naj bo $f\colon A \to B$, $A_1, A_2 \subseteq A$ in $B_1, B_2 \subseteq B$.

1. $A_1 \subseteq f^*(f_*(A_1))$ z enakostjo, če je f injektivna
2. $f_*(f^*(B_1)) \subseteq B_1$ z enakostjo, če je f surjektivna
3. $A_1 \subseteq A_2 \Rightarrow f_*(A_1) \subseteq f_*(A_2)$
4. $B_1 \subseteq B_2 \Rightarrow f^*(B_1) \subseteq f^*(B_2)$

Trditev 4.5.21. Naj bo $f\colon X \to Y$, $(A_\lambda)_{\lambda\in\mathcal{I}}$ neka družina podmnožic množice X in $(B_\mu)_{\mu\in\mathcal{J}}$ neka družina podmnožic Y.

1. $f_*\left(\bigcup_{\lambda\in\mathcal{I}} A_\lambda\right) = \bigcup_{\lambda\in\mathcal{I}} f_*(A_\lambda)$
2. $\mathcal{I} \neq \emptyset \Rightarrow f_*\left(\bigcap_{\lambda\in\mathcal{I}} A_\lambda\right) \subseteq \bigcap_{\lambda\in\mathcal{I}} f_*(A_\lambda)$ z enakostjo, ko je f injektivna
3. $f^*\left(\bigcup_{\mu\in\mathcal{J}} A_\mu\right) = \bigcup_{\mu\in\mathcal{J}} f^*(A_\mu)$
4. $\mathcal{J} \neq \emptyset \Rightarrow f^*\left(\bigcap_{\mu\in\mathcal{J}} A_\mu\right) = \bigcap_{\mu\in\mathcal{J}} f^*(A_\mu)$

5 Strukture urejenosti

»Del tega, da postanete matematiki je, da se naučite komunicirati z drugimi matematiki, kar včasih pomeni, da morate žrtvovati del svoje integritete.«

—asist. dr. Davorin Lešnik

5.1 Delna in linearna urejenost

Definicija 5.1.1. Naj bo $R \subseteq A \times A$ relacija.

1. R *delno ureja* A, če je
   - refleksivna,
   - antisimetrična,
   - tranzitivna.
2. R *linearno ureja* A, če je
   - relacija delne urejenosti,
   - sovisna.

Za splošno relacijo delne urejenosti namesto R pišemo $\leq$. Formulo $x \leq y$ preberemo kot »x je pod y«.

Definicija 5.1.2. Naj $\leq$ delno ureja A. Priredimo ji relacijo *stroge delne urejenosti* $<$ in *relacijo neposrednega predhodnika* $\lessdot$ v A:

1. $\forall x, y \in A \colon (x < y \Leftrightarrow x \leq y \wedge x \neq y)$
2. $\forall x, y \in A \colon (x \lessdot y \Leftrightarrow x < y \wedge \neg \exists z \in A \colon (x < z \wedge z < y))$

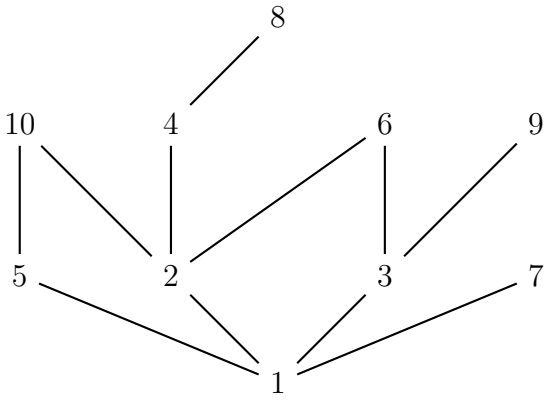
Trditev 5.1.3. Naj $\leq$ delno ureja A.

1. $<$ je irefleksivna, asimetrična in tranzitivna.
2. $\lessdot$ je irefleksivna, asimetrična ter intranzitivna.

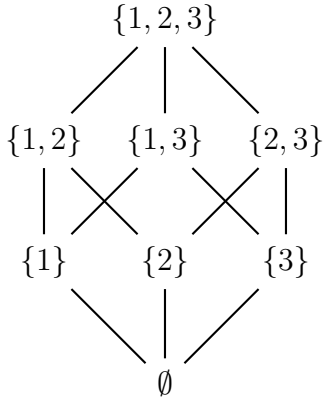
Končno delno urejeno množico lahko grafično predstavimo s tako imenovanim *Hassejevim diagramom*:

1. elemente A narišemo kot točke v ravnini
2. če je $x < y$, točko x narišemo niže kot y
3. če je $x \lessdot y$, ju povežemo

Velja $x \leq y \Leftrightarrow$ v diagramu obstaja vzpenjajoča se pot od x do y.



(a) Relacija deljivosti za $\{x \in \mathbb{N} \mid x \leq 10\}$.



(b) Relacija inkluzije za $\mathcal{P}\{1, 2, 3\}$.

Slika 2: Hassejeva diagrama

5.2 Posebni elementi v delno urejenih množicah

Definicija 5.2.1. Naj $\leq$ delno ureja A in naj bo $a \in A$.

1. a je *minimalen* v $A \Leftrightarrow \forall x \in A\colon (x \leq a \Rightarrow x = a)$
2. a je *maksimalen* v $A \Leftrightarrow \forall x \in A\colon (a \leq x \Rightarrow x = a)$
3. a je *prvi* ali *najmanjši* element v $A \Leftrightarrow \forall x \in A\colon a \leq x$
4. a je *zadnji* ali *največji* element v $A \Leftrightarrow \forall x \in A\colon x \leq a$

Trditev 5.2.2. Naj bo A delno urejena z $\leq$.

1. Vsak prvi element A je minimalen.
2. Vsak zadnji element A je maksimalen.
3. Če v A obstaja prvi element, je enoličen.
4. Če v A obstaja zadnji element, je enoličen.

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 5.2.3. Naj bo A linearno urejena z $\leq$. Potem je $a \in A$ prvi natanko tedaj, ko je minimalen in zadnji natanko tedaj, ko je maksimalen.

Dokaz. The proof is obvious and need not be mentioned. □

Opomba 5.2.3.1. Naj R delno ureja A in naj bo $B \subseteq A$. Potem je B delno urejena z *zožitvijo* $R|_B = R \cap (B \times B)$ relacije R na B.

1. Če ima $B \subseteq A$ prvi element, ga imenujemo tudi *minimum* množice B, ki ga označimo z $\min B$.
2. Če ima $B \subseteq A$ zadnji element, ga imenujemo tudi *maksimum* množice B, ki ga označimo z $\max B$.

Definicija 5.2.4. Naj bo A delno urejena z $\leq$ in $B \subseteq A$.

1. $a \in A$ je *zgornja meja* za B, če $\forall x \in B\colon x \leq a$
2. $a \in A$ je *spodnja meja* za B, če $\forall x \in B\colon a \leq x$

Definicija 5.2.5. Naj bo A delno urejena z $\leq$.

1. Naj bo $M = \{a \in A \mid a \text{ je zgornja meja za } B\}$. Če ima M prvi element, je to *supremum* ali *najmanjša (natančna) zgornja meja* za B in ga označimo z $\sup B$.
2. Naj bo $M = \{a \in A \mid a \text{ je spodnja meja za } B\}$. Če ima M zadnji element, je to *infimum* ali *največja (natančna) spodnja meja* za B in ga označimo z $\inf B$.

Opomba 5.2.5.1. Naj bo $B \subseteq A$ z delno urejenostjo.

1. Če ima B zadnji element, je $\max B = \sup B$.
2. Če ima B prvi element, je $\min B = \inf B$.

5.3 Dobra urejenost

Definicija 5.3.1. Naj bo $R \subseteq A \times A$. Relacija R *dobro ureja* množico A, če velja

1. R delno ureja A
2. Vsaka neprazna podmnožica $B \subseteq A$ ima prvi element glede na R_B.

Trditev 5.3.2. Vsaka dobra urejenost je linearna urejenost.

Dokaz. Ker ima $\{a, b\}$ prvi element za vse $a, b \in A$, je R sovisna. □

Opomba 5.3.2.1. Vsaka končna linearno urejena množica je dobro urejena. Prav tako je $(\mathbb{N}, \leq)$ dobro urejena.

Definicija 5.3.3. Naj R delno ureja A in naj bo $V \subseteq A$. Če $R|_V$ linearno ureja V, je V *veriga* v A.

Izrek 5.3.4 (O dobri urejenosti)**.** Za vsako množico A obstaja relacija R, ki A dobro ureja.

Lema 5.3.5 (Zorn)**.** Naj relacija R delno ureja A. Če ima vsaka veriga v A zgornjo mejo, ima A maksimalni element.

Opomba 5.3.5.1. Aksiom izbire, izrek o dobri urejenosti in Zornova lema so v teoriji ZF med seboj ekvivalentni.

5.4 Mreža

Definicija 5.4.1. Delno urejena množica A je *mreža*, če

$$\forall a, b \in A\colon (\exists \inf\{a, b\} \wedge \exists \sup\{a, b\}).$$

Posledica 5.4.1.1. Vsaka linearno urejena množica je mreža.

Dokaz. Velja $\inf\{a, b\} = \min\{a, b\}$ in $\sup\{a, b\} = \max\{a, b\}$. □

Opomba 5.4.1.2. Dobra urejenost je poseben primer linearne urejenosti, ki je poseben primer mreže, ta pa je poseben primer delne urejenosti.

6 Moč množic

»A lahko naredimo dokaz tega aksioma?«

—Jan Kamnikar

6.1 Množica naravnih števil

Peanovi aksiomi:

P1. 0 je naravno število.

P2. Vsako naravno število n ima točno določenega neposrednega naslednika n'.

P3. Število 0 ni naslednik nobenega števila.

P4. Različni naravni števili imata različna neposredna naslednika.

P5. Naj bo L enomestni predikat. Če velja $L(0)$ in za vsako naravno število n velja $L(n) \Rightarrow L(n')$, potem za vsako naravno število n velja $L(n)$.

V ZFC imamo naslednjo konstrukcijo:

Definicija 6.1.1. Za poljubno množico A je $A' = A \cup \{A\}$ njen *naslednik*.

Za 0 vzamemo kar $\emptyset$, kot naslednika števila pa vzamemo naslednika množice.

Aksiom regularnosti (AR):

$$\forall A\colon (A \neq \emptyset \Rightarrow \exists x \in A\colon x \cap A = \emptyset).$$

Vsaka neprazna množica vsebuje element, s katerim ima prazen presek.

Posledica 6.1.1.1. Veljata naslednji trditvi:

1. $\forall a\colon a \notin a$
2. $\forall a, b\colon \neg(a \in b \wedge b \in a)$

Dokaz. Uporabimo aksiom regularnosti:

1. Naj bo $A = \{a\}$. Potem je $A \neq \emptyset$ in $a \cap A = \emptyset$. Če je $a \in a$, pa je $a \in a \cap A$, kar je protislovje.
2. Predpostavimo nasprotno. Po aksiomu o paru obstaja $A = \{a, b\}$. Tako je $a \in A \cap b$ in $b \in A \cap a$, kar je v protislovju z aksiomom regularnosti. □

Definicija 6.1.2. Množica M je *induktivna*, če velja:

1. $\emptyset \in M$
2. $\forall x \in M\colon x' \in M$

Trditev 6.1.3. Naj bo A neprazna množica induktivnih množic. Potem je $\cap A$ induktivna množica.

Dokaz. The proof is obvious and need not be mentioned. □

Aksiom neskončnosti (AN):

Obstaja induktivna množica.

Izrek 6.1.4. Obstaja natanko ena množica $\mathbb{N}$, da velja:

1. $\mathbb{N}$ je induktivna
2. $\forall A$: (A induktivna $\Rightarrow \mathbb{N} \subseteq A$)

Dokaz. Naj bo M induktivna množica in $D = \{A \subseteq M \mid A \text{ je induktivna}\}$. Vzemimo $\mathbb{N} = \bigcap D$. Potem je $\mathbb{N}$ induktivna, za vsako induktivno množico A pa je $A \cap M$ induktivna, zato je $\mathbb{N} \subseteq A \cap M$. Ni težko videti, da je to edina taka množica (v nasprotnem primeru je $\mathbb{N}_1 \subseteq \mathbb{N}_2$ in $\mathbb{N}_2 \subseteq \mathbb{N}_1$). □

Izrek 6.1.5 (O indukciji)**.** Naj bo $L \subseteq \mathbb{N}$. Če velja

1. $0 \in L$ in
2. $\forall n \in \mathbb{N}$: ($n \in L \Rightarrow n' \in L$),

je $L = \mathbb{N}$.

Dokaz. Vidimo, da je L induktivna, zato je $\mathbb{N} \subseteq L$. Ker je $L \subseteq \mathbb{N}$, je $L = \mathbb{N}$. □

6.2 Relaciji $\sim$ in $\preccurlyeq$

Definicija 6.2.1. Množici A in B *imata enako moč* ali sta *ekvipolentni*, če obstaja bijekcija $f\colon A \to B$. To zapišemo kot $A \sim B$.

Trditev 6.2.2. $\sim$ je ekvivalenčna relacija v razredu vseh množic V.

Dokaz. The proof is obvious and need not be mentioned. □

Definicija 6.2.3. A ima *manjšo ali enako moč* kot B, če obstaja injekcija $f\colon A \to B$. Pišemo $A \preccurlyeq B$.

Trditev 6.2.4. Za vse množice A, B in C velja

1. $A \subseteq B \Rightarrow A \preccurlyeq B$
2. $A \preccurlyeq B \Rightarrow \exists C \subseteq B\colon A \sim C$
3. $\preccurlyeq$ je refleksivna in tranzitivna

Dokaz. The proof is obvious and need not be mentioned. □

Izrek 6.2.5 (Schröder-Bernsteinov izrek)**.** Za poljubni množici A in B velja

$$A \preccurlyeq B \wedge B \preccurlyeq A \Rightarrow A \sim B.$$

Izrek 6.2.6. Če obstaja surjekcija $f\colon A \to B$, je $A \succcurlyeq B$.

Dokaz. Naj bo $f\colon A \to B$ surjekcija. Vsakemu elementu $y \in B$ lahko z aksiomom izbire priredimo en element praslike $\{y\}$. Dobimo funkcijo izbire

$$g\colon B \to \bigcup_{y\in B} f^*(\{y\}) = f^*\left(\bigcup_{y\in B}\{y\}\right) = f^*(B) = A,$$

kjer je $g(y) \in f^*(\{y\})$ za vse $y \in B$. Ker je $f(g(y)) \in \{y\}$, je $f \circ g$ injektivna, zato je g injektivna. □

Definicija 6.2.7. A ima *strogo manjšo moč* kot B, če velja

$$A \preccurlyeq B \wedge A \not\sim B.$$

V tem primeru pišemo $A \prec B$.

Izrek 6.2.8 (O trihotomiji)**.** Za vse A, B velja natanko ena izmed naslednjih možnosti:

1. $A \prec B$
2. $A \sim B$
3. $A \succ B$

Posledica 6.2.8.1. Za vse A, B je $A \preccurlyeq B \vee B \preccurlyeq A$.

6.3 Končne in neskončne množice

Definicija 6.3.1 (Dedekind)**.** Množica A je *neskončna* natanko tedaj, ko

$$\exists B \subset A \colon A \sim B.$$

Sicer je A *končna*.

Izrek 6.3.2. A je neskončna natanko tedaj, ko je $A \succcurlyeq \mathbb{N}$.

Dokaz. Če je A neskončna, obstaja $B \subset A$, da je $A \sim B$. Naj bo $f \colon A \to B$ bijekcija. Naj bo $a \in A \setminus B$. Potem definiramo funkcijo $g \colon \mathbb{N} \to A$ na sledeč način:

$$\forall n \colon g(n) = f^n(a).$$

Ni težko videti, da je g injektivna.

Če je $A \succcurlyeq \mathbb{N}$, obstaja injekcija $f \colon \mathbb{N} \to A$. Potem je

$$\forall a \in A \colon g(a) = \begin{cases} a, & a \notin \mathcal{Z}_f \\ f\left(f^{-1}(a) + 1\right), & a \in \mathcal{Z}_f \end{cases}$$

injekcija iz A v $A \setminus \{f(0)\}$. □

Definicija 6.3.3. Množica A je *štev no neskončna* natanko tedaj, ko je $A \sim \mathbb{N}$. A je *Števna*, če je končna ali števno neskončna. A je *neštevna* natanko tedaj, ko ni števna.

Izrek 6.3.4. Za vse A velja:

1. A je končna natanko tedaj, ko je $A \prec \mathbb{N}$
2. A je števna natanko tedaj, ko je $A \preccurlyeq \mathbb{N}$
3. A je števno neskončna natanko tedaj, ko je $A \sim \mathbb{N}$
4. A je neskončna natanko tedaj, ko je $A \succcurlyeq \mathbb{N}$
5. A je neštevna natanko tedaj, ko je $A \succ \mathbb{N}$

6.4 Lastnosti števnih množic

Trditev 6.4.1. Če obstaja surjekcija $g\colon \mathbb{N} \to A$, je A števna.

Dokaz. The proof is obvious and need not be mentioned. □

Posledica 6.4.1.1. Če lahko elemente A razvrstimo v zaporedje tako, da vsak element A v njem nastopi vsaj enkrat, je A števna.

Definicija 6.4.2. Za družino $(A_\lambda)_{\lambda\in\mathcal{I}}$ pravimo, da je končna (neštevna, končna, neskončna, števno neskončna), natanko tedaj, ko je takšna $\mathcal{I}$.

Izrek 6.4.3. Unija vsake števno neskončne družine števno neskončnih množic je števno neskončna.

Dokaz. Diagonalni argument. □

Posledica 6.4.3.1. Unija vsake števne družine števnih množic je števna.

6.5 Neštevne množice

Izrek 6.5.1 (Cantor)**.** Za vsako množico A je $\mathcal{P}A \succ A$.

Dokaz. Ni težko najti injekcije $f\colon A \to \mathcal{P}A$. Vzamemo lahko kar

$$\forall x \in A\colon f(x) = \{x\}\,.$$

Predpostavimo, da med A in $\mathcal{P}A$ obstaja bijekcija g. Zdaj vzamemo množico

$$C = \{x \mid x \notin g(x)\}\,.$$

Ker je $C \subseteq A$, obstaja x_0, da je $C = g(x_0)$, kar je protislovje, saj velja

$$x_0 \in C \Leftrightarrow x_0 \notin g(x_0) \Leftrightarrow x_0 \notin C.$$ □

Posledica 6.5.1.1. $\mathbb{R} \succ \mathbb{N}$, saj je $\mathbb{R} \sim \mathcal{P}\mathbb{N}$.

Posledica 6.5.1.2. Obstaja neskončno zaporedje neskončnih množic različnih moči

$$\mathbb{N} \prec \mathcal{P}\mathbb{N} \prec \mathcal{P}\mathcal{P}\mathbb{N} \prec \dots$$

Posebej označimo moč $\mathbb{N}$ z $\aleph_0$ in moč kontinuuma (moč $\mathbb{R}$) s $\mathfrak{c} = 2^{\aleph_0}$.

»Auf Wiedersehen!«

—Jan Kamnikar

Stvarno kazalo