

# **Teoretične osnove računalništva I**

Diskretne strukture za računalničarje

FAMNIT, Jesen 2020

## PREDGOVOR

Pred tabo so zapiski iz predavanj za predmet TOR<sub>1</sub>, ki se predava študentom prvega letnika na FAMNIT, Univerza na Primorskem. Vse od leta 2017 ko sem začel s predavanjem tega predmeta se je vsebina spreminjala, tako da kar se da ustreza potrebnemu predznanju kot ga študent računalništva potrebuje. Od leta 2020 naprej sem se odločil tale TeX projekt odpreti kot repozitorij javnosti, tako da lahko zares vsak študent predlaga svoje naloge (oz. rešitve), ki se jih ustrezno vključi v tole skripto.

Dokument je zamišljen kot dopolnjevanje predavanj, in se ga ne sme jemati kot samostojno gradivo za pripravo na izpit. Morebitna vprašanja in najdene napake, lepo prosim, sporočite na [matjaz.krnc@upr.si](mailto:matjaz.krnc@upr.si), oz. istvarite t.i. "Issue"na našem javnem repozitorij

<https://github.com/mkrnc/TCS1-course-notes.git>.

Gradivo je osnovano na nekaterih starejših izročkih od mojih predhodnih predavateljev tega istega predmeta, med katerimi so

prof. **M. Milanič**, prof. **N. Prijatelj**, ter prof. **P. Škraba**.

# KAZALO

1	MATEMATIČNA LOGIKA	5
1.0.1	Osnovne povezave in pravilnostne tabele	5
1.1	Logične ekvivalence	11
1.2	Izbrani obliki izjav	13
1.3	Preklopna vezja	14
1.4	Logične implikacije	19
1.5	Načini dokazovanja	22
1.5.1	Množice izjav	27
1.5.2	Pravila sklepanja	29
1.6	Izjave s predikati in kvantifikatorji	29
2	TEORIJA MNOŽIC	37
2.1	Množice	37
2.1.1	Podmnožice	39
2.1.2	Prazna množica	40
2.1.3	Unija	40
2.1.4	Presek	43
2.1.5	Razlika množic	46
2.1.6	Vennovi diagrami	48
2.1.7	Potenčna množica	48
2.1.8	Urejeni par	50
2.1.9	Kartezični produkt	50
2.2	O aksiomih	53
2.2.1	Russellova antinomija	53
2.2.2	Aksiomi teorije množic (po Endertonu)	54
3	RELACIJE	57
3.1	Splošno o relacijah	57
3.1.1	Inverzna relacija	60
3.1.2	Kompozitum relacij	60
3.1.3	Univerzalna, ničelna in identična relacija	62

3.2	Posebne lastnosti binarnih relacij	62
3.3	Ekvivalenčna relacija	63
3.4	Funkcije	68
3.5	Inverzna relacija, praslike	71
3.6	Kompozitum funkcij	73
3.6.1	Zožitve in razširitve	74
3.7	Kanonična dekompozicija funkcije	75
3.7.1	Strukture urejenosti	78
A	DODATNA POGlavJA IZ TEORIJE MNOŽIC	91
A.1	Aksiomi teorije množic (po Edertonu)	91
A.2	Aksiomi teorije množic (po Dugundjiju)	92
A.3	Neformalni pogled na univerzum množic	93

# 1

## MATEMATIČNA LOGIKA

Kaj je izjava? *Trdilna izjava*, ki je bodisi pravilna ali pa nepravilna.<sup>1</sup>

Prispevek logike k znanju je v odkrivanju novih izjav, ki so logične posledice drugih.

- Celotno teorijo naravnih števil je moč zgraditi iz 5 osnovnih izjav, ki jih običajno imenujemo Peanovi aksiomi. Teh pet izjav lahko z besedico "in" povežemo v eno samo izjavo.
- Hilbert je pokazal, da je vso kopico izrekov elementarne geometrije moč dokazati iz 20 aksiomov (osnovnih izjav).
- V splošnem so matematične strukture definirane s peščico aksiomov, iz katerih se s pomočjo logičnega sklepanja izpelje izreke in gradi teorije.

O razvoju logike in teorije množic si lahko preberete v Prijateljevi knjigi (Osnove matematične logike, 1. poglavje, 2. podpoglavje).

### 1.0.1 Osnovne povezave in pravilnostne tabele

**Negacija:** Ne A; ni res, da A

Oznaka:  $\neg A$ .

$\neg A$  je negacija izjave A. Izjava  $\neg A$  je pravilna, če je A nepravilna, in je nepravilna, če je A pravilna.

Zgled: *Jutri bo dež. Negacija: Jutri ne bo dežja. (Ni res, da bo jutri dež.)*

Vrednost vsake sestavljene izjave je enolično določena z vrednostmi osnovnih izjav, ki v njej nastopajo. Za nazoren pregled te odvisnosti si pomagamo s t.i. *pravilnostnimi tabelami*. Dogovorimo se, da bomo vrednost *pravilno* označevali z 1, vrednost *nepravilno* pa z 0.

<sup>1</sup> Izjave boste podrobneje obravnavali na uvodnem predavanju pri Analizi I.

Pravilnostna tabela za negacijo:

	A	$\neg A$
1.	1	0
2.	0	1

**Konjunkcija:** A in B

Oznaka:  $A \wedge B$

$A \wedge B$  je konjunkcija izjav A in B. Ta sestavljena izjava je pravilna, kadar sta obe izjavi A in B pravilni, in nepravilna sicer.

Zgled: *Sneg pada. Veter piha. Konjunkcija: Sneg pada in veter piha.*

**Disjunkcija:** A ali B (inkluzivno)

Oznaka:  $A \vee B$

$A \vee B$  je disjunkcija izjav A in B. Ta sestavljena izjava je pravilna, brž ko je ena izmed izjav A in B pravilna, in nepravilna sicer.

Zgled: *Janez bo jutri vprašan fiziko. Janez bo jutri vprašan matematiko. Disjunkcija: Janez bo jutri vprašan fiziko ali matematiko.*

**Implikacija:** Če A, potem B

Oznaka:  $A \Rightarrow B$

$A \Rightarrow B$  je implikacija izjav A in B. Ta sestavljena izjava je nepravilna, kadar je A pravilna, B pa nepravilna. V vseh ostalih primerih je pravilna.

A - antecedens, zadostni pogoj

B - konsekvens

**Zgled:** : *Če Andrej naredi maturo, potem mu kupim kolo.*

**Ekvivalenca:** A če in samo če B

Oznaka:  $A \Leftrightarrow B$

$A \Leftrightarrow B$  je ekvivalenca izjav A in B. Ta sestavljena izjava je pravilna, kadar sta izjavi A in B ali obe pravilni ali obe nepravilni. V vseh ostalih primerih je nepravilna.

" $A \Leftrightarrow B$ "beremo:

A če in samo če B

A tedaj in samo tedaj kot B

A natanko tedaj kot B

**Zgled:** *Andreju kupim kolo, če in samo če naredi maturo.*

**Pravilnostne tabele za konjuncijo, disjunkcijo, implikacijo in ekvivalenco:**

	$A, B$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
1.	1, 1	1	1	1	1
2.	1, 0	0	1	0	0
3.	0, 1	0	1	1	0
4.	0, 0	0	0	1	1

Izjave, dobljene z uprabo 5 osnovnih povezav, so *sestavljene*. V splošnem pravimo, da je dana izjava *sestavljena*, če je izid zaporedne uporabe 5 osnovnih povezav na osnovnih izjavah  $A_1, \dots, A_n$ , pa tudi na izjavah, ki smo jih že prej napravili. Dvomom o tem, katera povezava sledi prej in katera pozneje, se izognemo z uporabo oklepajev. Uporabo oklepajev pa z uporabo naslednjega dogovora omejimo, kolikor se da:

- Kadar izjava nastopa osamljeno, je ne oklenemo z oklepaji:

npr.: namesto  $(A \wedge B)$  pišemo  $A \wedge B$

- Kadar ista vrsta povezave nastopi večkrat zapored, jo obravnavamo z leve proti desni.

npr.: namesto  $((A \wedge B) \wedge C) \wedge D$  pišemo  $A \wedge B \wedge C \wedge D$

- Upoštevamo naslednji prednostni red operacij:  $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$  (v vsaki sestavljeni izjavi najprej upoštevamo negacije, za njimi disjunkcije itd.)

npr.: namesto  $(A \wedge B) \Rightarrow (\neg C)$  pišemo  $A \wedge B \Rightarrow \neg C$

Pravilnostne tabele lahko zapišemo tudi za sestavljene izjave, z uporabo poljubnega zaporedja, s katerim sestavimo izjavo.

**Zgled:**

$$(A \Rightarrow B) \wedge (B \Rightarrow C) \wedge (\neg A \vee C) \quad (1)$$

	A, B, C	$A \Rightarrow B$	$B \Rightarrow C$	$(A \Rightarrow B) \wedge (B \Rightarrow C)$	$\neg A$	$\neg A \vee C$	(1)
1.	1, 1, 1	1	1	1	0	1	1
2.	1, 1, 0	1	0	0	0	0	0
3.	1, 0, 1	0	1	0	0	1	0
4.	1, 0, 0	0	1	0	0	0	0
5.	0, 1, 1	1	1	1	1	1	1
6.	0, 1, 0	1	0	0	1	1	0
7.	0, 0, 1	1	1	1	1	1	1
8.	0, 0, 0	1	1	1	1	1	1

Naj bo  $A$  izjava, sestavljena iz osnovnih izjav  $A_1, \dots, A_n$ .

*Določilo izjave  $A$ :* določitev vrednosti 1 / 0 (pravilno / nepravilno) vsaki od izjav  $A_1, \dots, A_n$

Če je izjava sestavljena iz  $n$  osnovnih izjav, potem ima izjava natanko  $2^n$  določil.

Dve vrsti izjav si zaslužita posebno ime:

- *Tavtologija:* pri vseh določilih pravilna izjava (primer:  $A \vee \neg A$ )
- *Protislovje:* pri vseh določilih nepravilna izjava (primer:  $A \wedge \neg A$ )

**Zgled:** Za vsako od naslednjih dveh izjav s pomočjo pravilnostne tabele določi, ali je izjava tautologija in ali je protislovje.

(a)  $(A \Rightarrow B) \Rightarrow A \vee B$ ,

(b)  $(A \Rightarrow B) \Leftrightarrow A \wedge \neg B$ .

Pravilnostna tabela za prvo izjavo:

	A, B	$A \Rightarrow B$	$A \vee B$	$(A \Rightarrow B) \Rightarrow A \vee B$
1.	1, 1	1	1	1
2.	1, 0	0	1	1
3.	0, 1	1	1	1
4.	0, 0	1	0	0

Izjava ni ne tautologija ne protislovje.



Pravilnostna tabela za drugo izjavo:

	A, B	$A \Rightarrow B$	$\neg B$	$A \wedge \neg B$	$(A \Rightarrow B) \Leftrightarrow A \wedge \neg B$
1.	1, 1	1	0	0	0
2.	1, 0	0	1	1	0
3.	0, 1	1	0	0	0
4.	0, 0	1	1	0	0

Izjava ni tautologija, je pa protislovje.



### Domača naloga:

1. Dani sta izjavi A: "Andrej govori francosko." in B: "Andrej govori dansko." V naravnem jeziku zapiši naslednje sestavljene izjave:

- (a)  $A \vee B$
- (b)  $A \wedge B$
- (c)  $A \wedge \neg B$
- (d)  $\neg A \vee \neg B$
- (e)  $\neg\neg A$
- (f)  $\neg(\neg A \wedge \neg B)$

2. Dani sta izjavi A: "Janez je bogat." in B: "Janez je srečen."

Naslednje izjave zapiši simbolično:

- (a) Če je Janez bogat, potem je nesrečen.
- (b) Janez ni niti srečen niti bogat.
- (c) Janez je srečen, samo če je reven.
- (d) Janez je reven natanko tedaj, ko je nesrečen.

### Vitezi in oprode

S pomočjo pravilnostnih tabele lahko rešujemo uganke o vitezih in oprodah. Vitezi vselej govorijo resnico, oprode pa vselej lažejo.

**Naloga:** Artur in Bine podata naslednji izjavi:

- Artur: "Bine je oproda."
- Bine: "Nobeden od naju ni oproda."

Za vsakega od njiju določi, ali je vitez ali oproda!

Naj bo A izjava: "Artur je vitez," B pa izjava: "Bine je vitez."

Določimo pravilnost izjav A in B s pomočjo pravilnostne tabele. Iz Arturjeve izjave sklepamo na pravilnost izjave  $A \Leftrightarrow \neg B$ . Iz Binetove izjave sklepamo na pravilnost izjave  $B \Leftrightarrow A \wedge B$ . Torej je konjunkcija teh dveh izjav pravilna:

$$(A \Leftrightarrow \neg B) \wedge (B \Leftrightarrow A \wedge B).$$

Za kateri nabor določil za A in B je ta izjava pravilna?

A	B	$\neg B$	$A \Leftrightarrow \neg B$	$A \wedge B$	$B \Leftrightarrow A \wedge B$	$(A \Leftrightarrow \neg B) \wedge (B \Leftrightarrow A \wedge B)$
1	1	0	0	1	1	0
1	0	1	1	0	1	1
0	1	0	1	0	0	0
0	0	1	0	0	1	0

Artur je vitez, Bine pa oproda. □

**Še ena podobna naloga:** Tokrat podata Artur in Bine naslednji izjavi:

- Artur: "Jaz in Bine nisva iste vrste."
- Bine: "Natanko eden od naju je vitez."

Naslednja konjunkcija izjav je pravilna:

$$[A \Leftrightarrow (A \wedge \neg B) \vee (\neg A \wedge B)] \wedge [B \Leftrightarrow (A \wedge \neg B) \vee (\neg A \wedge B)]. \quad (2)$$

A	B	$A \wedge \neg B$	$\neg A \wedge B$	$(A \wedge \neg B) \vee (\neg A \wedge B) (*)$	$B \Leftrightarrow (*)$	$A \Leftrightarrow (*)$	(2)
1	1	0	0	0	0	0	0
1	0	1	0	1	1	0	0
0	1	0	1	1	0	1	0
0	0	0	0	0	1	1	1

Oba sta oprodi. □

**Domača naloga:** Reši naslednji nalogi o vitezi in oprodah:

- Artur: "Ni res, da je Bine oproda." Bine: "Nisva oba iste vrste."

- Artur: "Ni res, da je Cene oproda." Bine: "Cene je vitez ali pa sem jaz vitez." Cene: "Bine je oproda."

□

Videli smo, kako priredimo vsaki sestavljeni izjavi njeno pravilnostno tabelo. Obratna naloga: Če imamo dane neodvisne izjave  $A_1, \dots, A_n$ , kako konstruirati iz njih sestavljeno izjavo, ki bo imela pri vsakem izmed  $2^n$  določil *vnajprej predpisano logično vrednost*?

Da bi rešili to nalogo, si najprej pogledimo t.i. *logične ekvivalence*.

## 1.1 LOGIČNE EKVIVALENCE

Naj bosta  $B$  in  $C$  izjavi, sestavljeni iz izjav  $A_1, \dots, A_n$ . Če je izjava  $B \Leftrightarrow C$  tautologija, pravimo, da sta  $B$  in  $C$  *logično ekvivalentni*. Za logiko:  $B = C$  (dve različni obliki iste izjave).

Naštejmo najpomembnejše logične ekvivalence:

1.  $A \Leftrightarrow \neg(\neg A)$ , zakon dvakratne negacije
2.  $A \wedge B \Leftrightarrow B \wedge A$ ,  $A \vee B \Leftrightarrow B \vee A$ , komutativnost konjunkcije in disjunkcije
3.  $A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$ ,  $A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$ , asociativnostna zakona
4.  $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$ ,  $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$ , distributivnostna zakona
5.  $A \wedge A \Leftrightarrow A$ ,  $A \vee A \Leftrightarrow A$
6.  $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$
7.  $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$ , De Morganova zakona (6. in 7.)
8.  $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$
9.  $(A \Rightarrow B) \Leftrightarrow \neg A \vee B$
10.  $(A \Rightarrow B) \Leftrightarrow \neg(A \wedge \neg B)$

11.  $(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A)$
12.  $(A \Leftrightarrow B) \Leftrightarrow (B \Leftrightarrow A)$ , komutativnost ekvivalence
13.  $(A \Leftrightarrow B) \Leftrightarrow (\neg A \Leftrightarrow \neg B)$
14.  $(A \Leftrightarrow B) \Leftrightarrow (\neg A \vee B) \wedge (A \vee \neg B)$
15.  $(A \Leftrightarrow B) \Leftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B)$
16.  $\neg(A \Leftrightarrow B) \Leftrightarrow (A \Leftrightarrow \neg B)$

Za vajo se prepričajmo v pravilnost 16. ekvivalence s pomočjo pravilnostne tabele:

	A, B	$A \Leftrightarrow B$	$\neg(A \Leftrightarrow B)$	$\neg B$	$A \Leftrightarrow \neg B$
1.	1, 1	1	0	0	0
2.	1, 0	0	1	1	1
3.	0, 1	0	1	0	1
4.	0, 0	1	0	1	0

**Domača naloga:** S pomočjo pravilnostnih tabel (ali kako drugače) se prepričaj v pravilnost preostalih ekvivalenc.

S pomočjo zgornjih ekvivalenc se lahko prepričamo, da 5 osnovnih povezav med izjavami ni med seboj neodvisnih. Vse sestavljene izjave lahko izrazimo *samo* z *dvema osnovnima povezavama*, če ju le primerno izberemo. Zadošča že:

- (a) negacija  $\neg$  in disjunkcija  $\vee$
- (b) negacija  $\neg$  in konjunkcija  $\wedge$
- (c) negacija  $\neg$  in implikacija  $\Rightarrow$

Te izbire so edine mogoče.

### Zgled:

Vzemimo izjavo "Če je kakšna reč lepa, potem je minljiva."

( $\neg$  in  $\vee$ ) Reč ni lepa, ali pa je minljiva.

( $\neg$  in  $\wedge$ ) Ni res, da je kakšna reč lepa in ni minljiva.

( $\neg$  in  $\Rightarrow$ ) Če kakšna reč ni minljiva, potem ni lepa.



## 1.2 IZBRANI OBLIKI IZJAV

Od zadnjič dolgujemo še rešitev naslednje naloge: iz danih izjav  $A_1, \dots, A_n$  konstruiraj izjavo, ki bo imela pri vsakem izmed  $2^n$  določil vnaprej predpisano vrednost.

**1. način:** Vsakemu določilu  $d$  za izjave  $A_1, \dots, A_n$  priredimo konjunkcijo

$$C_1 \wedge \dots \wedge C_n,$$

in sicer takole: izjava je  $C_i = A_i$ , če ima  $A_i$  v določilu  $d$  vrednost 1, in naj bo  $C_i = \neg A_i$ , sicer. Tako dobljena konjunkcija je pravilna pri določilu  $d$  in nepravilna pri vsakem drugem določilu. Imenuje se *osnovna konjunkcija določila*  $d$ .

Sedaj pa napravimo osnovne konjunkcije natanko tistih določil, za katere naj bo iskana izjava pravilna, in jih povežimo z disjunkcijami!

Tako dobljeno izjavo imenujemo *izbrana disjunktivna oblika*.

Ta postopek deluje v vsakem primeru, le v primeru protislovja ne! Za protislovje lahko iskano izjavo konstruiramo posebej, npr.  $A_1 \wedge \neg A_1$ .

### 2. način:

$d$  - določilo

Sedaj tvorimo *osnovno disjunkcijo določila*  $d$ :

$$D_1 \vee \dots \vee D_n,$$

kjer je

$D_i = \neg A_i$ , če ima  $A_i$  v  $d$  vrednost 1 in

$D_i = A_i$ , če ima  $A_i$  v  $d$  vrednost 0.

Tako dobljena disjunkcija je nepravilna pri  $d$  in pravilna pri vsakem drugem določilu.

Napravimo osnovne disjunkcije natanko tistih določil, za katere naj bo iskana sestavljena izjava nepravilna, in jih povežimo med seboj s konjunkcijami.

Tako dobljeno izjavo imenujemo *izbrana konjunktivna oblika*.

Ta postopek deluje v vsakem primeru, le v primeru tautologije ne! Za tautologijo lahko konstruiramo iskano izjavo posebej, npr.  $A_1 \vee \neg A_1$  ("zakon izključene tretje možnosti", vsaka izjava je bodisi pravilna bodisi nepravilna).

**Zgled:** Iščemo izjavo D, sestavljeno iz izjav A, B in C, za katero velja:

A	B	C	D	osnovna konjunkcija	osnovna disjunkcija
1	1	1	1	$A \wedge B \wedge C$	
1	1	0	0		$\neg A \vee \neg B \vee C$
1	0	1	0		$\neg A \vee B \vee \neg C$
1	0	0	0		$\neg A \vee B \vee C$
0	1	1	1	$\neg A \wedge B \wedge C$	
0	1	0	0		$A \vee \neg B \vee C$
0	0	1	1	$\neg A \wedge \neg B \wedge C$	
0	0	0	1	$\neg A \wedge \neg B \wedge \neg C$	

Izbrana disjunktivna oblika izjave D je

$$(A \wedge B \wedge C) \vee (\neg A \wedge B \wedge C) \vee (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge \neg B \wedge \neg C).$$

izbrana konjunktivna oblika pa je

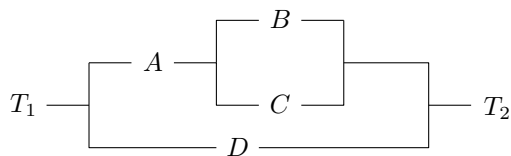
$$(\neg A \vee \neg B \vee C) \wedge (\neg A \vee B \vee \neg C) \wedge (\neg A \vee B \vee C) \wedge (A \vee \neg B \vee C).$$

□

### 1.3 PREKLOPNA VEZJA

Logične izjave lahko modeliramo s t.i. preklopnimi vezji.

Preklopno vezje je sistem žic in preklopov (stikal), ki vežejo dve izhodni točki, med katerima obstaja električna napetost. Vsako stikalo je bodisi "zaprto" (če skozenj teče tok) ali "odprto" (če tok ne teče).

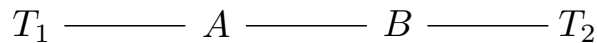


Slika 1: Primer vezja s štirimi stikali

Recimo, da imamo tako vezje in da vemo, katera stikala so odprta in katera zaprta. Zanima nas, ali je celotno vezje "zaprto" (tj., skozenj teče tok) ali "odprto" (če tok ne teče).

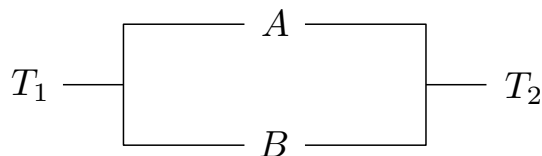
Poglejmo si dve zelo preprosti vezji:

(1) *zaporedno vezani stikali*:



Zaporedno vezje je zaprto natanko tedaj, kadar sta obe stikali zaprti:  
**konjunkcija.**

(2) *vzporedno vezani stikali*:



Vzporedno vezje je zaprto natanko tedaj, kadar je vsaj eno stikalo zaprto:  
**disjunkcija.**

Vsakemu takemu vezju ustreza neka logična izjava, sestavljena iz izjav, ki ustrezajo stikalom.

Obratno: če omogočamo *identična* in *obratna* stikala, potem lahko vsako sestavljeno izjavo predstavimo z vezjem!

Identični stikali sta taki stikali, ki sta bodisi hkrati odprti ali hkrati zaprti.

Obratni stikali sta taki stikali, da je natanko eno od njiju odprto.

Zveza med vezji in izjavami: *vezje je zaprto natanko tedaj, ko je ustrezna izjava pravilna, in odprto sicer.*

**Zgled:** Vzemimo izjavo

$$(A \Rightarrow B) \wedge (B \Rightarrow C) \wedge (\neg A \vee C)$$

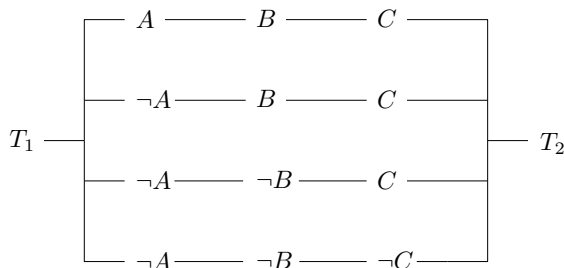
V poglavju 1.2. smo izračunali pravilnostno tabelo te izjave:

	A	B	C	$(A \Rightarrow B) \wedge (B \Rightarrow C) \wedge (\neg A \vee C)$
1.	1	1	1	1
2.	1	1	0	0
3.	1	0	1	0
4.	1	0	0	0
5.	0	1	1	1
6.	0	1	0	0
7.	0	0	1	1
8.	0	0	0	1

V prejšnjem podpoglavju smo zapisali to izjavo v izbrani disjunktivni obliki kot:

$$(A \wedge B \wedge C) \vee (\neg A \wedge B \wedge C) \vee (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge \neg B \wedge \neg C).$$

Tej obliki ustreza naslednje vezje:



Izbrani konjunktivni obliki

$$(\neg A \vee \neg B \vee C) \wedge (\neg A \vee B \vee \neg C) \wedge (\neg A \vee B \vee C) \wedge (A \vee \neg B \vee C)$$

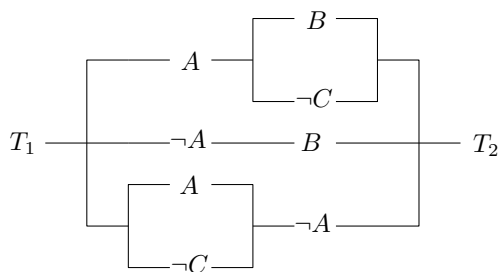
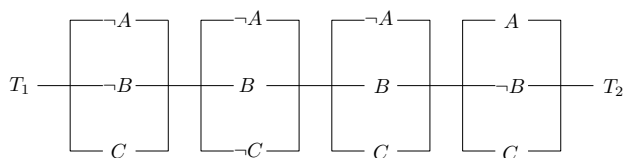
pa ustreza vezje

Vidimo, da dani izjavi ustreza več preklonnih vezij. Pri dejanski konstrukciji vezij, ki simulirajo dano izjavo, je torej utemeljena zahteva, da naj bo vezje čimbolj enostavno, da naj ustreza določenim predpisom itd. (s tem se tu ne bomo ukvarjali). ▲

**Zgled:** Dano je naslednje preklonno vezje:

*Pri katerih položajih stikal je vezje zaprto? Problem rešimo z logiko.*





Prirejena sestavljena izjava, recimo ji D, je:

$$(A \wedge B \vee \neg C) \vee (\neg A \wedge B) \vee (A \vee \neg C \wedge \neg A).$$

Njena pravilnostna tabela pa je:

	A	B	C	$A \wedge B \vee \neg C$	$\neg A \wedge B$	$A \vee \neg C \wedge \neg A$	D
1.	1	1	1	1	0	0	1
2.	1	1	0	1	0	0	1
3.	1	0	1	0	0	0	0
4.	1	0	0	1	0	0	1
5.	0	1	1	0	1	0	1
6.	0	1	0	0	1	1	1
7.	0	0	1	0	0	0	0
8.	0	0	0	0	0	1	1

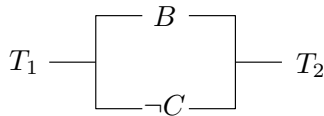
Vidimo, da je vezje odprto natanko takrat, ko je stikalo B odprto, C pa zaprto, in zaprto v vseh drugih primerih.

Torej bi vezje lahko zamenjali tudi z naslednjim preprostejšim vezjem:

Do istega rezultata lahko pridemo tudi po logični poti:

Iz pravilnostne tabele razberemo izbrano konjunktivno obliko izjave D

$$(\neg A \vee B \vee \neg C) \wedge (A \vee B \vee \neg C).$$



zaradi distributivnosti je ta izjava ekvivalentna izjavi

$$(\neg A \wedge A) \vee (B \vee \neg C)$$

ker pa je konjunkcija  $\neg A \wedge A$  vselej nepravilna, je ta izjava ekvivalentna izjavi  $B \vee \neg C$ .



Zaključimo poglavje o vezjih še z enim zgledom bolj praktične narave.

**Zgled:** Imamo odbor 3 poslancev, ki glasujejo o posameznih predlogih po določenem volilnem načelu. Konstruirati je treba tako preklopno vezje, ki bo nemudoma sporočilo, ali je predlog sprejet ali ne.

Oglejmo si dve možni volilni načeli:

(a) načelo enostavne večine

(b) načelo enostavne večine, pri čemer ima poslanec A pravico veta

Pravilnostna tabela veli:

A	B	C	(a)	(b)
1	1	1	1	1
1	1	0	1	1
1	0	1	1	1
1	0	0	0	0
0	1	1	1	0
0	1	0	0	0
0	0	1	0	0
0	0	0	0	0

Če se odločimo za izbrano disjunktivno obliko, potem se zaželena izjava v primeru (a) glasi

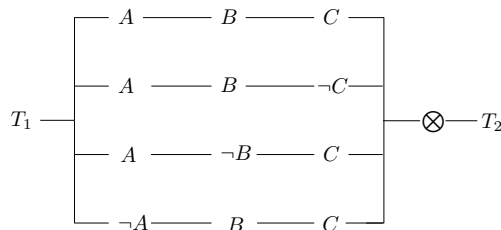
$$(A \wedge B \wedge C) \vee (A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge C)$$

v primeru (b) pa

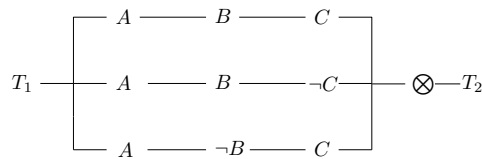
$$(A \wedge B \wedge C) \vee (A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge C).$$

Ustrezni vezji pa sta:

(a)



(b)



**Domača naloga:** Sestavite vezje, prirejeno izjavi

$$(A \Rightarrow B) \vee (\neg B \Rightarrow C) \vee (A \Leftrightarrow C).$$

## 1.4 LOGIČNE IMPLIKACIJE

*Logična implikacija* je tautologija, pri kateri je glavna povezava implikacija.

Veljajo naslednje resnice o logičnih implikacijah:

1. Če je antecedens tautologija, mora biti tudi konsekvens tautologija.
2. Če je konsekvens protislovje, mora biti tudi antecedens protislovje.
3. Če je konsekvens tautologija, je lahko antecedens katerakoli izjava.
4. Če je antecedens protislovje, je lahko konsekvens katerakoli izjava.
5. Vsaka izjava logično implicira samo sebe.

6. Vsaka izjava, ki logično implicira hkrati kakšno izjavo  $A$  in njeno negacijo  $\neg A$ , mora biti protislovje.
7. Izjava, ki logično implicira svojo negacijo, je protislovje.

Zgled logične implikacije:

$$A \Rightarrow B \Rightarrow (A \wedge C \Rightarrow B \wedge C).$$

Dokažimo jo. Ta implikacija bi bila nepravilna le pri takem določilu, pri katerem bi bila izjava  $A \Rightarrow B$  pravilna, izjava  $A \wedge C \Rightarrow B \wedge C$  pa nepravilna. To je po definiciji implikacije res samo, če sta izjavi  $A \wedge C$  pravilni, izjava  $B$  pa nepravilna. V tem primeru pa je implikacija  $A \Rightarrow B$  nepravilna, kar je v nasprotju s predpostavko, da je pravilna. Torej ne obstaja tako določilo, za katero bi bila izjava  $A \Rightarrow B$  pravilna, izjava  $A \wedge C \Rightarrow B \wedge C$  pa nepravilna. Implikacija je res tautologija.

Na vajah boste spoznali in dokazali številne druge logične implikacije.

### ***Nekaj poglavitnih logičnih implikacij***

1.  $A \wedge (A \Rightarrow B) \Rightarrow B$
2.  $\neg B \wedge (A \Rightarrow B) \Rightarrow \neg A$
3.  $\neg A \wedge (A \vee B) \Rightarrow B$
4.  $A \wedge B \Rightarrow A$
5.  $A \Rightarrow A \vee B$
6.  $A \wedge \neg A \Rightarrow B$
7.  $(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$
8.  $(A \Rightarrow B) \Rightarrow ((C \Rightarrow A) \Rightarrow (C \Rightarrow B))$
9.  $(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))$
10.  $(A \Rightarrow B) \Rightarrow (A \wedge C \Rightarrow B \wedge C)$
11.  $(A \Rightarrow B) \Rightarrow (A \vee C \Rightarrow B \vee C)$

$$12. (A \Leftrightarrow B) \wedge (B \Leftrightarrow C) \Rightarrow (A \Leftrightarrow C)$$

$$13. (A \Leftrightarrow B) \Rightarrow (A \Rightarrow B)$$

$$14. (A \Leftrightarrow B) \Rightarrow (B \Rightarrow A)$$

$$15. A \wedge (A \Leftrightarrow B) \Rightarrow B$$

$$16. \neg A \wedge (A \Leftrightarrow B) \Rightarrow \neg B$$

$$17. B \Rightarrow (A \Leftrightarrow A \wedge B)$$

$$18. \neg B \Rightarrow (A \Leftrightarrow A \vee B)$$

$$19. (A \Rightarrow (B \wedge \neg B)) \Rightarrow \neg A$$

Za vajo se prepričajte o veljavnosti teh logičnih implikacij. Namesto pravilnostnih tabel lahko uporabite tole metodo: *Izhajamo iz definicije implikacije in poskušamo konstruirati tako določilo, za katero bi bila implikacija nepravilna. Potem se mora seveda izkazati, da takega določila ni.*

**Zgled:** Dokažimo 10. logično implikacijo s seznama:

$$A \Rightarrow B \Rightarrow (A \wedge C \Rightarrow B \wedge C)$$

Ta implikacija bi bila nepravilna le pri takem določilu, pri katerem bi bila izjava  $A \Rightarrow B$  pravilna, izjava  $A \wedge C \Rightarrow B \wedge C$  pa nepravilna. To je po definiciji implikacije res samo, če sta izjavi  $A \wedge C$  pravilni, izjava  $B$  pa nepravilna. V tem primeru pa je implikacija  $A \Rightarrow B$  nepravilna, kar je v nasprotju s predpostavko, da je pravilna. Torej ne obstaja tako določilo, za katero bi bila izjava  $A \Rightarrow B$  pravilna, izjava  $A \wedge C \Rightarrow B \wedge C$  pa nepravilna. Implikacija 10. je res tautologija. ▲

## 1.5 NAČINI DOKAZOVANJA

Logične implikacije uporabljamo pri dokazovanju novih trditev iz aksiomov in že dokazanih trditev. Poglejmo si nekaj načinov dokazovanja.

### 1) *Direktni dokaz implikacije* $A \Rightarrow B$

Dokazujemo logično implikacijo  $A \Rightarrow B$ . Predpostavimo, da je  $A$  pravilna izjava in direktno izpeljemo pravilnost izjave  $B$ .

#### **Zgled:**

*Če je  $n$  liho naravno število, je tudi  $n^2$  liho število.*

**Dokaz.** Naj bo  $n$  liho naravno število. Tedaj ga lahko zapišemo kot  $n = 2k - 1$ , kjer je  $k$  naravno število. Sledi  $n^2 = (2k - 1)^2 = 4k^2 - 4k + 1 = 2(2k^2 - 2k) + 1$ , torej je  $n^2$  liho število.  $\square$

**Direktni dokaz implikacije**  $A \Rightarrow B$

**Dokaz:**

Predpostavimo  $A$ .

$\vdots$

Torej,  $B$ .

Sledi  $A \Rightarrow B$ .  $\square$

### 2) *Indirektni dokaz implikacije* $A \Rightarrow B$

Dokazujemo pravilnost logične implikacije  $A \Rightarrow B$ . Včasih se izkaže, da je ugodneje direktno dokazovati ekvivalentno implikacijo  $\neg B \Rightarrow \neg A$ .

#### **Zgled:**

*Če je  $n^2$  sodo število, je  $n$  sodo število.*

**Dokaz.** Izjava je ekvivalentna implikaciji:

Če je  $n$  število, ki ni sodo, je  $n^2$  število, ki ni sodo.

Ekvivalentno: Če je  $n$  liho število, je  $n^2$  liho število.

To pa smo že dokazali.  $\square$

Indirektni dokaz implikacije
$A \Rightarrow B$
<b>Dokaz:</b>
Predpostavimo $\neg B$ .
$\vdots$
Torej, $\neg A$ .
Sledi $\neg B \Rightarrow \neg A$ .
Posledično $A \Rightarrow B$ . <span style="float: right;">□</span>

### 3) Dokaz izjave $A$ s protislovjem

Želimo dokazati pravilnost izjave  $A$ . Predpostavimo, da je  $A$  nepravilna in pokažemo, da vodi ta predpostavka v protislovje (ki ga označimo s  $\perp$ ). S tem smo pokazali pravilnost izjave  $\neg A \Rightarrow \perp$ . Ta izjava pa je pravilna le, če je izjava  $\neg A$  nepravilna, torej je  $A$  pravilna.

#### Zgled:

*Število  $\sqrt{2}$  ni racionalno.*

**Dokaz.** Predpostavimo, da je  $\sqrt{2}$  racionalno število. Tedaj ga lahko zapišemo kot  $\sqrt{2} = p/q$ , kjer sta  $p$  in  $q$  tuji si naravni števili.

Sledi

$$2 = p^2/q^2.$$

$$p^2 = 2q^2.$$

Torej je  $p^2$  sodo število. Sledi (po prej dokazanem), da je  $p$  sodo število.

Pišimo  $p = 2m$ , kjer je  $m$  naravno število.

Dobimo

$$4m^2 = 2q^2.$$

$$\text{Sledi } 2m^2 = q^2.$$

Torej je tudi  $q$  sodo število. To pa je protislovje. (Predpostavili smo, da sta  $p$  in  $q$  tuji si števili in dokazali, da sta obe deljivi z 2, torej da si nista tuji.) □

**Dokaz izjave A s protislovjem****Dokaz:**

Predpostavimo  $\neg A$ .

$\vdots$

Torej, B.

$\vdots$

Torej,  $\neg B$ .

Sledi, da je pravilna tudi izjava  $B \wedge \neg B$ , ta pa je protislovje.

Posledično A. □

**4) Dokaz ekvivalence  $A \Leftrightarrow B$  v dveh delih**

Želimo dokazati pravilnost logične ekvivalence  $A \Leftrightarrow B$ . Dokažemo vsako od obeh implikacij.

Za dokazovanje obeh delov lahko uporabimo različne metode. Pogosto je dokaz implikacije v eno smer lažji od dokaza v drugo smer.

**Zgled:**

*Pozitivno celo število  $p > 1$  je praštevilo natanko tedaj, ko ne obstaja tako naravno število  $n$ , večje od 1 in manjše ali enako  $\sqrt{p}$ , ki deli  $p$ .*

**Dokaz.**

(i) Dokazujemo indirektno. Predpostavimo, da obstaja tako naravno število  $n$ , večje od 1 in manjše ali enako  $\sqrt{p}$ , ki deli  $p$ . Torej je  $n$  delitelj  $p$ , različen od 1 in  $p$ , in  $p$  ni praštevilo.

(ii) Tudi tu dokazujemo indirektno. Predpostavimo, da  $p$  ni praštevilo. Lahko ga torej zapišemo v obliki  $p = n_1 \cdot n_2$ , kjer sta  $n_1$  in  $n_2$  pozitivni celi števili, različni od 1 in  $p$ . Trdimo, da je vsaj eno od števil  $n_1$  in  $n_2$  manjše ali enako  $\sqrt{p}$ . Če to ne bi veljalo, bi imeli  $n_1 > \sqrt{p}$  in  $n_2 > \sqrt{p}$  in posledično  $p = n_1 n_2 > \sqrt{p} \cdot \sqrt{p} = p$ , protislovje. Naj bo torej  $n$  tako število izmed  $n_1$  in  $n_2$ , za katerega velja  $n \leq \sqrt{p}$ . Število  $n$  je tedaj naravno število, večje od 1 in manjše ali enako  $\sqrt{p}$ , ki deli  $p$ . □

**Zgled:**

*Naj bosta  $m$  in  $n$  celi števili. Tedaj sta števili  $m$  in  $n$  iste parnosti natanko tedaj, ko je število  $m^2 + n^2$  sodo.*

**Dokaz.**



(i) Predpostavimo, da sta  $m$  in  $n$  iste parnosti. Obravnavamo dva primera.

(a) Če sta  $m$  in  $n$  sodi števili, potem je  $m = 2k$  in  $n = 2j$  za neki celi števili  $k$  in  $j$ . Sledi  $m^2 + n^2 = (2k)^2 + (2j)^2 = 2(2k^2 + 2j^2)$ , kar je sodo število.

(b) Če sta  $m$  in  $n$  lihi števili, potem je  $m = 2k + 1$  in  $n = 2j + 1$  za neki celi števili  $k$  in  $j$ . Sledi  $m^2 + n^2 = (2k + 1)^2 + (2j + 1)^2 = 2(2k^2 + 2k + 2j^2 + 2j + 1)$ , kar je sodo število.

V obeh primerih je  $m^2 + n^2$  sodo število.

(ii) Predpostavimo, da je  $m^2 + n^2$  sodo število. Spet obravnavamo dva primera.

(a) Če je  $m$  sodo število, potem je tudi  $m^2$  sodo število. Torej, ker je  $m^2 + n^2$  sodo število in  $m^2$  sodo število, je sodo tudi število  $n^2 = (m^2 + n^2) - m^2$ . Od tod sledi, da je  $n$  sodo.

(b) Če je  $m$  liho število, potem je tudi  $m^2$  liho število. Torej, ker je  $m^2 + n^2$  sodo število in  $m^2$  liho število, je liho tudi število  $n^2 = (m^2 + n^2) - m^2$ . Od tod sledi, da je  $n$  liho.

V obeh primerih sta  $m$  in  $n$  iste parnosti. □

Povzemimo:

**Dokaz ekvivalence  $A \Leftrightarrow B$  v dveh delih**

**Dokaz:**

(i) Dokažemo  $A \Rightarrow B$ .

(ii) Dokažemo  $B \Rightarrow A$ .

Torej,  $A \Leftrightarrow B$ . □

**5) "Če in samo če" dokaz  $A \Leftrightarrow B$**

Pravilnost logične ekvivalence  $A \Leftrightarrow B$  lahko dokažemo z zaporedjem logično ekvivalentnih izjav. Začnemo z izjavo  $A$  in jo zamenjamo z zaporedjem ekvivalentnih izjav, ki se konča z izjavo  $B$ .

**Zgled:**

Dan je trikotnik  $T$  s stranicami dolžin  $a, b, c$ . S pomočjo kosinusnega izreka dokaži, da je  $T$  pravokotni trikotnik s hipotenuzo dolžine  $c$  natanko tedaj, ko je  $a^2 + b^2 = c^2$ .

Kosinusni izrek:  $a^2 + b^2 = c^2 + 2ab \cos \gamma$ , kjer je  $\gamma$  kot med stranicama dolžin  $a$  in  $b$ .

**Dokaz.**

Iz kosinusnega izreka sledi

$$a^2 + b^2 = c^2 \quad \text{če in samo če} \quad 2ab \cos \gamma = 0$$

$$\text{če in samo če} \quad \cos \gamma = 0$$

$$\text{če in samo če} \quad \gamma = 90^\circ.$$

Torej je  $a^2 + b^2 = c^2$  natanko tedaj, ko je  $T$  pravokotni trikotnik s hipotenuzo dolžine  $c$ . □

Če imamo  $n$  vmesnih izjav  $C_1, \dots, C_n$ , ima dokaz naslednjo obliko:

**“Če in samo če” dokaz  $A \Leftrightarrow B$**

**Dokaz:**

$A$  če in samo če  $C_1$

če in samo če  $C_2$

...

če in samo če  $C_n$

če in samo če  $B$ . □

**6) Analiza primerov**

Včasih nam pri dokazu pravilnosti izjave  $A$  pomaga, če pregledamo vse primere, ter ugotovimo da je  $B$  vedno pravilna.

**Dokazovanje  $A$  s pomočjo analize primerov.**

**Dokaz:**

Primer 1: predpostavimo  $B$

...

$A$ .

Primer 2: predpostavimo  $\neg B$

...

$A$ . □

### 1.5.1 Množice izjav

Dane so atomarne izjave  $A_1, \dots, A_n$  (take, da v njih ne nastopa nobena logična povezava).

Koliko različnih izjav lahko sestavimo iz njih?

Zdi se, da neskončno mnogo! Vendar pa, za logiko sta dve izjavi isti, če sta logično ekvivalentni.

Izjav, ki med seboj niso logično ekvivalentne, pa je le končno mnogo.

Vsaka izjava, sestavljena iz  $A_1, \dots, A_n$ , ima natanko  $2^n$  različnih določil. Izjava je enolično določena, brž ko so določene njene vrednosti za vsako od teh  $2^n$  določil.

Vsako določilo ima vrednost 0 ali 1, neodvisno od drugih. Sledi, da je vseh možnih izjav  $2^{(2^n)}$ .

Oglejmo si konstrukcijo vseh možnih izjav za  $n = 1$  in  $n = 2$ .

**$n = 1$**

Imamo eno samo izjavo,  $A$ . Iz nje lahko sestavimo  $2^{(2^1)} = 4$  izjave,  $C_1, \dots, C_4$ .

$A$	$C_1$	$C_2$	$C_3$	$C_4$
1	1	1	0	0
0	1	0	1	0

$C_1$  je tautologija, npr.  $A \vee \neg A$ .

$C_4$  je protislovje, npr.  $A \wedge \neg A$ .

Za  $C_2$  lahko vzamemo kar  $A$ .

Za  $C_3$  pa  $\neg A$ .

**$n = 2$**

Imamo dve izjavi,  $A$  in  $B$ . Iz njiju lahko sestavimo  $2^{(2^2)} = 16$  izjav,  $C_1, \dots, C_{16}$ .

$A$	$B$	$C_1$	$C_2$	$C_3$	$C_4$	$C_5$	$C_6$	$C_7$	$C_8$	$C_9$	$C_{10}$	$C_{11}$	$C_{12}$	$C_{13}$	$C_{14}$	$C_{15}$	$C_{16}$
1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
1	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
0	1	1	1	0	0	1	1	0	0	1	1	0	0	1	1	1	1
0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0

Seveda je  $C_1$  je tautologija, npr.  $A \vee \neg A$  in  $C_{16}$  protislovje  $A \wedge \neg A$ .

Ker so izjave  $C_2, C_3, C_5$  in  $C_9$  nepravilne le pri enem določilu, bomo v teh primerih izbrali izbrano konjunktivno obliko:

- $C_2 = A \vee B$
- $C_3 = A \vee \neg B$
- $C_5 = \neg A \vee B$
- $C_8 = \neg A \vee \neg B$

Podobno za izjave  $C_8, C_{12}, C_{14}$  in  $C_{15}$  izrazimo s pomočjo izbrane disjunktivne oblike:

- $C_8 = A \wedge B$
- $C_{12} = A \wedge \neg B$
- $C_{14} = \neg A \wedge B$
- $C_{15} = \neg A \wedge \neg B$

Vse preostale izjave pa so pravilne pri dveh določilih in prav tako nepravilne pri dveh določilih.

Za  $C_4$  vzamemo

$$(A \wedge B) \vee (A \wedge \neg B),$$

kar je ekvivalentno

$$A \wedge (B \vee \neg B)$$

in ker je disjunkcija  $B \vee \neg B$  vedno pravilna izjava, je torej izjava  $C_4$  ekvivalentna z izjavo  $A$ .

Podobno se prepričamo, da je:

- izjava  $C_6$  ekvivalentna z izjavo  $B$ ,
- izjava  $C_{11}$  ekvivalentna z izjavo  $\neg B$ ,
- izjava  $C_{13}$  ekvivalentna z izjavo  $\neg A$ .

Za  $C_7$  pišimo

$$(A \wedge B) \vee (\neg A \vee \neg B),$$

kar je ekvivalentno z

$$A \Leftrightarrow B.$$

Podobno pa lahko za  $C_{10}$  vzamemo ekvivalenco

$$A \Leftrightarrow \neg B.$$

□

### 1.5.2 Pravila sklepanja

Kako pa pokažemo pravilnost sklepa? Zapis pravilnostne tabele in preverjanje vseh naborov je časovno potraten postopek. Precej rajši bi imeli kratko izpeljavo, v kateri bi izvajali relativno enostavne, majhne korake proti cilju. Majhne, enostavne sklepe, ki jih bomo potrebovali za dokazovanje pravilnosti sklepov, imenujemo pravila sklepanja.

ime	predpostavke	sklep
modus ponens	$A, A \Rightarrow B$	$B$
modus tollens	$A \Rightarrow B, \neg B$	$\neg A$
hipotetični silogizem	$A \Rightarrow B, B \Rightarrow C$	$A \Rightarrow C$
disjunktivni silogizem	$A \vee B, \neg A$	$B$
združitev	$A, B$	$A \wedge B$
poenostavitev	$A \wedge B$	$A$
pridružitev	$A$	$A \vee B$

## 1.6 IZJAVE S PREDIKATI IN KVANTIFIKATORJI

Kvantifikatorji povedo, za koliko objektov neke vrste velja neka izjava. Pri tem moramo povedati, katere vrste objekti nas zanimajo (npr. elementi množic  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ , itd.), pogosto pa je to že razvidno iz konteksta.

Naj bo  $A(x)$  neka izjava, smiselna za vsak objekt  $x$  iz domene pogovora. Taki izjavi pravimo *predikat*. Predikati oblike  $A(x)$  so enomestni. Poznamo pa tudi dvo- in večmestne predikate, npr.  $A(x, y)$ ,  $P(x_1, x_2, x_3)$  ipd.

Za zapis izjav s kvantifikatorji bomo uporabljali naslednje oznake:

- $(\forall x)A(x)$ : to je izjava, ki je pravilna natanko tedaj, ko je za vsak  $x$  izjava  $A(x)$  pravilna

$\forall$  je t.i. *univerzalni kvantifikator*

- $(\exists x)A(x)$ : to je izjava, ki je pravilna natanko tedaj, ko obstaja vsaj en  $x$ , za katerega je izjava  $A(x)$  pravilna

$\exists$  je t.i. *eksistencialni kvantifikator*

- $(\exists!x)A(x)$ : to je izjava, ki je pravilna natanko tedaj, ko obstaja **na-tanko en**  $x$ , za katerega je izjava  $A(x)$  pravilna

Ekvivalentno:  $(\exists x)A(x) \wedge (\forall y)(\forall z)(A(y) \wedge A(z) \Rightarrow y = z)$

**Zgled:** Zadnjič smo dokazali izjavo "Če je  $n$  liho naravno število, je tudi  $n^2$  liho število." To pomeni: za vsako naravno število  $n$  velja, da če je liho, potem je tudi  $n^2$  liho število. To lahko zapišemo kot  $(\forall n)A(n)$ , kjer je  $A(n)$  izjava "Če je  $n$  liho število, potem je tudi  $n^2$  liho število." ▲

**Zgled:** Dana je izjava "Vsa jabolka so okusna." Kako bi to izjavo zapisali s predikati in kvantifikatorji?

Uporabimo  $\forall$ , a kako?

Če se omejimo le na objekte, ki so jabolka, potem zapišemo  $(\forall x)(x \text{ je okusen})$ .

Če pa je  $x$  lahko poljubno sadje, potem moramo uporabiti dve izjavi:

$A(x)$ :  $x$  je jabolko

in

$B(x)$ :  $x$  je okusen

Kako pa zapišemo izjavo vsi  $A(x)$  so  $B(x)$ ? Kot  $(\forall x)(A(x) \wedge B(x))$  ali kot  $(\forall x)(A(x) \Rightarrow B(x))$ ? Prva izjava bi pomenila, da je vsako sadje okusno jabolko, tega pa ne želimo trditi. Pravilen je drugi zapis. ▲

**Zgled:** Dana je izjava "Nekatera jabolka so okusna." Kako bi pa to izjavo zapisali s kvantifikatorji, pri čemer kot objekte upoštevamo vse vrste sadja? Naj bo spet

$A(x)$ :  $x$  je jabolko in  $B(x)$ :  $x$  je okusen

Bomo zapisali  $(\exists x)(A(x) \wedge B(x))$  ali  $(\exists x)(A(x) \Rightarrow B(x))$ ?

Prva izjava pomeni, da obstaja sadje, ki je okusno jabolko, in to je pravilen zapis. Druga izjava pa trdi, da za vsako sadje velja, da če je jabolko, potem je okusno. Ta izjava pa ne zagotavlja obstoja jabolka;

pravilna je v vsakem kontekstu, kjer obstaja objekt, ki ni jabolko ali pa je okusno. Tega pa ne želimo trditi. ▲

Povzemimo:

Izjavo oblike "vsi  $A(x)$  so  $B(x)$ " zapišemo kot  $(\forall x)(A(x) \Rightarrow B(x))$ .

Izjavo oblike "nekateri  $A(x)$  so  $B(x)$ " pa kot  $(\exists x)(A(x) \wedge B(x))$ .

### Še nekaj zgledov izjav s kvantifikatorji:

Naj bo domena pogovora množica naravnih števil. Tedaj so naslednje izjave s kvantifikatorji smiselne:

- $(\forall n)$  ( $n$  je deljiv z 2).
- $(\exists n)$  ( $n$  je deljiv z 2).
- $(\exists!n)$  ( $n$  je najmanjše naravno število).

Kako bi zapisali zgornje izjave, če bi bila domena pogovora množica realnih števil z uporabo predikata  $N(n)$  : "n je naravno število"?

- $(\forall n) (N(n) \Rightarrow n \text{ je deljiv z } 2)$ .
- $(\exists n) (N(n) \wedge n \text{ je deljiv z } 2)$ .
- $(\exists!n) (N(n) \wedge n \text{ je najmanjše naravno število})$ .

### Negacije izjav s kvantifikatorji

Negacija  $\forall$

$$\neg(\forall x)A(x) \Leftrightarrow (\exists x)(\neg A(x))$$

#### Zgled:

B: Vsak državljan Slovenije je rjavolas.

$\neg B$ : Ni res, da je vsak državljan Slovenije rjavolas.

Ekvivalentno: Obstaja vsaj en državljan Slovenije, ki ni rjavolas. ▲

Negacija  $\exists$

$$\neg(\exists x)A(x) \Leftrightarrow (\forall x)\neg A(x)$$

#### Zgled:

B: V škatli obstaja rdeča kroglica.

$\neg B$ : Ni res, da obstaja v škatli rdeča kroglica.

Ekvivalentno: Za vse kroglice v škatli velja, da niso rdeče. ▲

### Zgled:

Naj  $P(x)$  označuje izjavo "x je praštevilo".

Za vsako naravno število  $x$  obstaja naravno število  $y$ , večje od  $x$ , ki je praštevilo:  $(\forall x)(\exists y)(y > x \wedge P(y))$ .

Negacija:

$$\neg(\forall x)(\exists y)(y > x \wedge P(y)) \Leftrightarrow (\exists x)\neg(\exists y)(y > x \wedge P(y))$$

$$\Leftrightarrow (\exists x)(\forall y)\neg(y > x \wedge P(y)) \Leftrightarrow (\exists x)(\forall y)(y \leq x \vee \neg P(y)). \quad \blacktriangle$$

**Zgled:** Zapišimo negacijo izjave  $(\forall x)(\exists y)(y < x)$ .

$$\neg(\forall x)(\exists y)(y < x)$$

$$\Leftrightarrow (\exists x)(\neg(\exists y)(y < x))$$

$$\Leftrightarrow (\exists x)(\forall y)\neg(y < x)$$

$$\Leftrightarrow (\exists x)(\forall y)(y \geq x) \quad \blacktriangle$$

- Ali je izjava pravilna v realnih številih?

$$(\forall x)(\exists y)(y < x)$$

Da, izjava je pravilna!

- Ali je izjava pravilna v naravnih številih?  $(\forall x)(\exists y)(y < x)$

Ne, pravilna je njena negacija:  $(\exists x)(\forall y)(y \geq x)$ , obstaja namreč najmanjše naravno število.

### Domača naloga:

Ali je naslednja izjava pravilna?

Obstaja realno število  $x$ , za katerega velja  $\frac{1}{1+x^2} > 1$ .

### Dokazovanje izjav s kvantifikatorji

Poglejmo si nekaj načinov dokazovanja izjav s kvantifikatorji.

#### 1) Direktni dokaz izjave $(\forall x)A(x)$

Dokazujemo trditev oblike  $(\forall x)A(x)$ . Pokazati moramo torej, da je izjava  $A(x)$  pravilna za vsak objekt  $x$  iz domene pogovora.

**Zgled:** Dokaži, da za vsako naravno število  $n$  velja  $4n^2 - 4n + 1 \geq 0$ .



**Dokaz.**

Trditev je oblike  $(\forall x)A(x)$ , kjer preučujemo naravna števila,  $\mathbb{N}$ , in je  $A(x)$  izjava " $4x^2 - 4x + 1 \geq 0$ ".

Naj bo  $n$  poljubno naravno število. Zapišimo  $4n^2 - 4n + 1 = (2n - 1)^2$ . Kvadrat poljubnega realnega števila je nenegativno število. Torej je  $4n^2 - 4n + 1 \geq 0$ . Ker je bilo število  $n$  poljubno, smo pokazali, da velja  $4n^2 - 4n + 1 \geq 0$  za vsa naravna števila.  $\square$

**Direktni dokaz izjave  $(\forall x)A(x)$** **Dokaz:**

Naj bo  $x$  poljuben objekt iz domene pogovora. (Katere vrste objektov preučujemo, mora biti zapisano v trditvi ali razvidno iz konteksta.)

$\vdots$

Torej,  $A(x)$  je pravilna izjava.

Ker je bil  $x$  poljuben, je izjava  $(\forall x)A(x)$  pravilna.  $\square$

**2) Dokaz izjave  $(\forall x)A(x)$  s protislovjem**

Za dokazovanje izjav oblike  $(\forall x)A(x)$  pogosto uporabimo dokaz s protislovjem.

**Zgled:** Dokaži, da za vse  $x \in (0, \pi/2)$  velja  $\sin x + \cos x > 1$ .

**Dokaz.**

Trditev je oblike  $(\forall x)A(x)$ , kjer je  $A(x)$  izjava " $0 < x < \pi/2 \Rightarrow \sin x + \cos x > 1$ ".

Predpostavimo, da je trditev napačna. Tedaj obstaja neko realno število  $t$ , za katerega je  $0 < t < \pi/2$  in  $\sin t + \cos t \leq 1$ . Ker sta funkciji  $\sin x$  in  $\cos x$  pozitivni za vse  $x \in (0, \pi/2)$ , velja  $\sin t > 0$  in  $\cos t > 0$ . Sledi:

$$0 < \sin t + \cos t \leq 1$$

$$0 < (\sin t + \cos t)^2 \leq 1^2 = 1$$

$$0 < \sin^2 t + 2 \sin t \cos t + \cos^2 t \leq 1$$

$$0 < 1 + 2 \sin t \cos t \leq 1$$

$$-1 < 2 \sin t \cos t \leq 0$$

(Uporabili smo identiteto  $\sin^2 t + \cos^2 t = 1$ .)

Ampak  $2 \sin t \cos t \leq 0$  je nemogoče, saj sta tako  $\sin t$  kot  $\cos t$  pozitivna. Torej, če je  $0 < x < \pi/2$ , potem je  $\sin x + \cos x > 1$ .  $\square$

Ker je izjava  $\neg(\forall x)A(x)$  ekvivalentna izjavi  $(\exists x)\neg A(x)$ , ima dokaz s protislovjem naslednjo obliko:

**Dokaz izjave  $(\forall x)A(x)$  s protislovjem**

**Dokaz:**

Predpostavimo, da  $\neg(\forall x)A(x)$ .

Tedaj  $(\exists x)\neg A(x)$ .

Naj bo  $t$  objekt, za katerega velja  $\neg A(t)$ .

$\vdots$

Torej,  $B \wedge \neg B$ .

Sledi, da je izjava  $(\exists x)\neg A(x)$  nepravilna, torej je izjava  $(\forall x)A(x)$  pravilna.  $\square$

**3) Dokazovanje izjav oblike  $(\exists x)A(x)$**

Kako dokazujemo eksistenčne izreke, tj. trditve oblike  $(\exists x)A(x)$ ?

Včasih lahko kar direktno.

**Zgled:** *Dokaži, da obstaja sodo praštevilo.*

**Dokaz.** Število 2 je sodo praštevilo.  $\square$

Nekateri dokazi so težji. Znameniti matematik Euler je sredi 18. stoletja vprašal, ali obstaja tako naravno število, katerega  $n$ -to potenco lahko zapišemo kot vsoto manj kot  $n$   $n$ -tih potenc drugih števil. (Euler je postavil domnevo, da takih števil ni. Protiprimeri so znani za  $n = 4, 5$ .)

**Zgled:** *Dokaži, da obstaja naravno število, katerega četrta potenca je vsota četrlih potenc treh drugih naravnih števil.*

**Dokaz.** Tako število je npr. 20.615.673, saj velja

$$20615673^4 = 2682440^4 + 1536539^4 + 18796760^4.$$

(Zgornjo rešitev je našel Noam Elkies leta 1988. Kmalu zatem je Roger Frye našel najmanjšo rešitev:  $95.800^4 + 217.519^4 + 414.560^4 = 422.481^4$ .)  $\square$

Včasih pa je ugodneje uporabiti dokaz s protislovjem.

**Zgled:** Hribolazec krene na pot iz doline v ponedeljek ob 9:00 in prispe na vrh gore ob 15:00. Tam prenoči in v torek zjutraj krene nazaj ob 9:00 po isti poti in se vrne v dolino ob 15:00. Na poti navzdol se je vmes večkrat ustavil, ponekod pa hodil hitreje kot prejšnji dan navzgor. Dokaži, da obstaja točka na poti, na kateri je bil oba dneva ob istem času.

**Dokaz.**

Če merimo čas v urah od 0 do 6 ( $t = 0$  ustreza času 9:00,  $t = 6$  pa času 15:00, je treba dokazati:

$(\exists t \in (0, 6))$  (točka na poti ob času  $t$  v ponedeljek je enaka točki na poti ob času  $t$  v torek).

Recimo, da taka točka ne obstaja. Torej za vsak  $t \in (0, 6)$  točka na poti ob času  $t$  v ponedeljek različna od točke na poti ob času  $t$  v torek. Vzemimo dva hribolazca, ki gresta istočasno po poti od 9:00 dalje, prvi gre navzgor, in sicer z enakim tempom kot je šel naš hribolazec navzgor v ponedeljek, drugi pa navzdol, in sicer z enakim tempom kot je šel naš hribolazec navzdol v torek. Ker sta ta dva hribolazca ves čas na različnih točkah, se ne bosta nikoli srečala. To pa ni možno, enkrat se namreč morata srečati, saj gresta po isti poti. To je protislovje.

Sledi, da obstaja točka na poti, na kateri je bil hribolazec oba dneva ob istem času. □

**Dokaz izjave  $(\exists x)A(x)$  s protislovjem**

**Dokaz:**

Predpostavimo, da  $\neg(\exists x)A(x)$ .

Tedaj  $(\forall x)\neg A(x)$ .

⋮

Torej,  $B \wedge \neg B$ , protislovje.

Sledi, da je izjava  $(\forall x)\neg A(x)$  nepravilna, torej je izjava  $(\exists x)A(x)$  pravilna. □

**4) Dokazovanje izjav oblike  $(\exists! x)A(x)$**

**Zgled:** Vsako neničelno realno število ima enoličen multiplikativni inverz.

**Dokaz.**

Izjava ima obliko  $(\forall x)(x \neq 0 \Rightarrow (\exists! y)(xy = 1))$ , domena pogovora je množica realnih števil.

Naj bo  $x \neq 0$ . Obstoj inverza bomo pokazali v dveh korakih: najprej bomo pokazali, da tako število  $y$  obstaja, potem pa še, da  $x$  ne more imeti dveh različnih inverzov.

(i) Naj bo  $y = 1/x$ . Ker je  $x \neq 0$ , je  $y$  realno število. Tedaj je  $xy = x \cdot (1/x) = 1$ . Število  $x$  torej ima multiplikativni inverz.

(ii) Naj bosta  $y$  in  $z$  multiplikativna inverza števila  $x$ . (Tu ne predpostavimo, da je ta  $y$  enak  $y$  iz točke (i).)

Sledi  $xy = 1$  in  $xz = 1$  in od tod

$$xy = xz$$

$$xy - xz = 0$$

$$x(y - z) = 0.$$

Ker je  $x \neq 0$ , sledi  $y - z = 0$ , torej  $y = z$ . □

**Dokaz izjave  $(\exists! x)A(x)$**

**Dokaz:**

(i) Dokaži pravilnost izjave  $(\exists x)A(x)$  (s katerokoli metodo).

(ii) Dokaži pravilnost izjave  $(\forall y)(\forall z)(A(y) \wedge A(z) \Rightarrow y = z)$ .

Predpostavi, da sta  $y$  in  $z$  obravnavana objekta, za katera sta izjavi  $A(y)$  in  $A(z)$  pravilni.

⋮

Torej,  $y = z$ .

Iz (i) in (ii) izpeljemo, da je izjava  $(\exists! x)A(x)$  pravilna. □

# 2

## TEORIJA MNOŽIC

### 2.1 MNOŽICE

Množice so osnovni matematični objekti. Pojma množice ne definiramo. Množice imajo elemente (ki so lahko tudi sami množice), običajno jih bomo označevali z malimi črkami:  $a, b, \dots, x, y, z$  (+ indeksi:  $a_6, x_1, z_\lambda$ )

Množice pa bomo običajno pisali z velikimi črkami:  $A, B, \dots, X, Y, Z$  (+ indeksi)

Množice in elemente družijo relacija pripadnosti:

$a \in F$ : element  $a$  *pripada* množici  $F$ ,  $a$  *je element* množice  $F$ .

$\in$ : znak pripadnosti

$a \notin F$ :  $a$  ni element (ne pripada) množici  $F$ .

**Zgled:** Če je  $G$  množica vseh sodih števil, je  $16 \in G$  in  $3 \notin G$ .

*Enakost množic:* Množici  $A$  in  $B$  sta enaki natanko takrat, kadar imata iste reči za elemente:

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

Ta definicija je potrebna, saj podaja pomembno lastnost, ki ji mora relacija pripadnosti ustrezati!

**Primer:** Recimo, da so objekti, ki jih preučujemo, ljudje, in zapišimo  $x \in A$  natanko tedaj, ko je  $x$  prednik  $A$ -ja. Ali lahko to definicijo uporabimo, da definiramo ljudi kot množice? Zgornja ekvivalenca pravi:

- Če sta dva človeka enaka, potem imata iste prednike. To drži.
- Če imata dva človeka iste prednike, potem sta enaka. To pa ne drži!

**Načini podajanja množic:**

1. Množico lahko podamo tako, da navedemo vse njene elemente:

$$A = \left\{ 1, \frac{1}{2}, \frac{\pi}{3}, 2i + 8 \right\}.$$

Vrstni red *ni pomemben*! Včasih pa je ta zapis nepraktičen (kadar je množica neskončna ali pa končna, a prevelika).

2. Množico lahko podamo tudi tako, da jo opišemo. Opis pa mora biti **nedvoumen**: za vsako reč mora veljati bodisi, da je element dane množice, ali pa da ni element te množice.

V splošnem lahko zapišemo:

$$A = \{x; P(x)\},$$

kjer je  $P(x)$  nek enomestni predikat. *Množica A je množica vseh elementov x, za katere je izjava  $P(x)$  pravilna.* Ali pa, če imamo več izjav  $P_1, \dots, P_n$ :

$$A = \{x; P_1(x) \wedge \dots \wedge P_n(x)\}$$

$$A = \{x; P_1(x) \vee \dots \vee P_n(x)\}$$


Kot bomo kmalu videli, lahko take množice tvorimo le z elementi množic, ki jih že poznamo (oz. za katere vemo, da obstajajo).

**Zgled:** Naj bo A množica vseh takih kompleksnih števil  $x$ , ki so rešitev kakšne enačbe oblike

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0,$$

kjer je  $n \in \mathbb{N}$  in  $a_i \in \mathbb{Z}$  za vse  $i = 0, 1, \dots, n$ .

A - množica vseh algebraičnih števil.

Ali je  $2^\pi \in A$ ? Ne vemo (današnja matematika še ne more odgovoriti na to vprašanje). 

Pozor: škatla, ki vsebuje klobuk, ni ista reč kot klobuk. Tako tudi množica  $\{a\}$  ni ista reč kot  $a$ . Za vsako reč  $a$  pa velja  $a \in \{a\}$ .

### 2.1.1 Podmnožice

Dani sta množici  $A$  in  $B$ .

Pravimo, da je  $A$  *podmnožica* množice  $B$  natanko takrat, ko je vsak element množice  $A$  tudi element množice  $B$ .

Oznaka:  $A \subseteq B$

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

Seveda je vsaka množica podmnožica same sebe:

$$(\forall A)(A \subseteq A).$$

Če je  $A \subseteq B$  in  $A \neq B$ , potem je  $A$  *prava podmnožica* množice  $B$ :  $A \subset B$ .

$$A \subset B \Leftrightarrow (A \subseteq B \wedge A \neq B)$$

Očitno velja:

- $A \subseteq B \wedge B \subseteq A \Leftrightarrow A = B$ .

Ta ekvivalenca je izjemno pomembna za dokazovanje enakosti dveh množic!

- $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$  (tranzitivnost inkluzije)

Dokažimo tranzitivnost inkluzije:  $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$

*Direkten dokaz:*

Privzemimo, da je  $A \subseteq B$  in  $B \subseteq C$ . Dokazati moramo:  $(\forall x)(x \in A \Rightarrow x \in C)$ .

Vzemimo poljuben  $x \in A$ .

- Ker je  $x \in A$  in  $A \subseteq B$ , sledi  $x \in B$ .
- Ker je  $x \in B$  in  $B \subseteq C$ , sledi  $x \in C$ .

Ker je bil  $x$  poljuben, smo dokazali  $(\forall x)(x \in A \Rightarrow x \in C)$ , tj.,  $A \subseteq C$ .  $\square$

**V razmislek:** Ali obstajata množici  $A$  in  $B$ , za kateri velja  $A \subset B$  in  $B \subset A$ ?

**Pozor:** Relacija inkluzije  $\subseteq$  in relacija pripadnosti  $\in$  sta povsem različna pojma!

$1 \in \{1, 2, 3\}$ , toda 1 ni podmnožica množice  $\{1, 2, 3\}$ . Množica  $\{1\}$  pa je podmnožica množice  $\{1, 2, 3\}$ , toda  $\{1\}$  ni element množice  $\{1, 2, 3\}$ .

**V razmislek:** Naj bo  $X = \{1, 2, \{1\}, \{2\}\}$ . Ali je 1 element množice  $X$ ? Ali je 1 podmnožica množice  $X$ ? Ali je  $\{1\}$  element množice  $X$ ? Ali je  $\{1\}$  podmnožica množice  $X$ ?

### 2.1.2 Prazna množica

Množico, ki nima nobenega elementa, označimo s simbolom  $\emptyset$  — *prazna množica*.

$$X = \emptyset \Leftrightarrow (\forall x)(x \notin X)$$

Seveda velja:

$$(\forall X)(\emptyset \subseteq X)$$

**Domača naloga:** Dokažite, da velja:

$$X = \emptyset \Leftrightarrow (\forall Y)(X \subseteq Y).$$

### 2.1.3 Unija

Dani sta množici  $A$  in  $B$ . *Unija* teh dveh množic je množica  $A \cup B$ , ki ima za elemente natanko tiste reči, ki so elementi množice  $A$  ali množice  $B$ :

$$A \cup B = \{x; x \in A \vee x \in B\}.$$

**Zgled:**  $A = \{1, 3, 5, 7\}$ ,  $B = \{1, 2, 4, 8\}$ .

$$A \cup B = \{1, 3, 5, 7, 2, 4, 8\}.$$

Posplošimo sedaj pojem unije dveh množic na unijo poljubne družine množic.  $A \cup B$  je unija družine množic  $\{A, B\}$ . Tvorimo lahko množice množic (oziroma družine množic).

**Zgled:**  $\mathbb{Q}$ : množica racionalnih števil je množica množic:

$$0,5 = \left\{ \frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \dots \right\}$$



(Ulomek razumemo kot urejen par celih števil. Urejen par  $(a, b)$  pa lahko, kot bomo videli kmalu, definiramo kot množico  $\{\{a\}, \{a, b\}\}$ .) ▲

### Unija več množic:

V splošnem lahko družino množic zapišemo na naslednji način:

$\mathcal{A} = \{A_\lambda; \lambda \in J\}$  - družina množic z indekso množico  $J$

Indeksna množica je poljubna množica!

**Zgled:** Za  $J = \{1, 2\}$  dobimo

$\mathcal{A} = \{A_\lambda; \lambda \in \{1, 2\}\} = \{A_1, A_2\}$ . ▲

Unijo družine  $\mathcal{A}$  definiramo kot

$$\cup \mathcal{A} = \cup_{\lambda \in J} A_\lambda = \{x; (\exists \lambda)(\lambda \in J \wedge x \in A_\lambda)\}$$

**Zgled:**  $J = \{1, 2\}$

$$\cup_{\lambda \in \{1, 2\}} A_\lambda = \{x; (\exists \lambda)(\lambda \in \{1, 2\} \wedge x \in A_\lambda)\} = \{x; x \in A_1 \vee x \in A_2\} = A_1 \cup A_2.$$

**Zgled:** Vzemimo družino  $\mathcal{A} = \{A_\lambda; \lambda \in J\}$ , kjer je  $J = \mathbb{Z}$  množica celih števil in  $A_\lambda = [\lambda, \lambda + 1] = \{x; x \in \mathbb{R} \wedge \lambda \leq x \leq \lambda + 1\}$  za vse  $\lambda \in \mathbb{Z}$ . Tedaj je

$$\cup \mathcal{A} = \cup_{\lambda \in \mathbb{Z}} A_\lambda = \{x; (\exists \lambda)(\lambda \in \mathbb{Z} \wedge \lambda \leq x \leq \lambda + 1)\} = \mathbb{R},$$

saj vsako realno število leži med dvema zaporednima celima številoma. ▲

Če je  $J$  končna, vzamemo po navadi  $J = \{1, 2, \dots, n\}$  in pišemo

$$\cup \mathcal{A} = \cup_{j=1}^n A_j = A_1 \cup \dots \cup A_n.$$

### Osnovne lastnosti unije:

- $A \cup B = B \cup A$ , komutativnost
- $(A \cup B) \cup C = A \cup (B \cup C)$ , asociativnost
- $A \cup A = A$ , idempotentnost
- $A \cup \emptyset = A$

- $A \subseteq A \cup B, B \subseteq A \cup B$
- $A \subseteq B \Leftrightarrow A \cup B = B$
- $A \subseteq C \wedge B \subseteq C \Rightarrow A \cup B \subseteq C$

Dokažimo lastnost

$$A \subseteq B \Leftrightarrow A \cup B = B :$$

Ekvivalenco bomo dokazali tako, da dokažemo obratno ekvivalenco  $\neg(A \subseteq B) \Leftrightarrow \neg(A \cup B = B)$  : Izkaže se, da je ugodneje obravnati najprej negacijo izjave na desni.

$$\begin{aligned}
 & \neg(A \cup B = B) \\
 & \Leftrightarrow \\
 & \neg((A \cup B \subseteq B) \wedge (B \subseteq A \cup B)) \\
 & \Leftrightarrow \\
 & \neg(A \cup B \subseteq B) \vee \neg(B \subseteq A \cup B) \\
 & \Leftrightarrow \\
 & \neg(A \cup B \subseteq B) \\
 & \Leftrightarrow \\
 & (\exists x)(x \in A \cup B \wedge x \notin B) \\
 & \Leftrightarrow \\
 & (\exists x)((x \in A \vee x \in B) \wedge x \notin B) \\
 & \Leftrightarrow \\
 & (\exists x)((x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin B)) \\
 & \Leftrightarrow \\
 & (\exists x)(x \in A \wedge x \notin B) \\
 & \Leftrightarrow \\
 & \neg(\forall x)(x \in A \Rightarrow x \in B) \\
 & \Leftrightarrow
 \end{aligned}$$

$$\neg(A \subseteq B)$$

□

**Domača naloga:** Dokažite preostale lastnosti.

#### 2.1.4 Presek

Dani sta množici  $A$  in  $B$ . *Presek* teh dveh množic je množica  $A \cap B$ , ki ima za elemente natanko tiste reči, ki so elementi množice  $A$  in množice  $B$ :

$$A \cap B = \{x; x \in A \wedge x \in B\}.$$

**Zgled:**  $A = \{1, 3, 5, 7\}$ ,  $B = \{1, 2, 4, 8\}$ .

$$A \cap B = \{1\}.$$

**Presek več množic:**

$\mathcal{A} = \{A_\lambda; \lambda \in J\}$  - družina množic z indeksno množico  $J$ ,  $J \neq \emptyset$ !

Indeksna množica je poljubna **neprazna** množica!

Presek neprazne družine  $\mathcal{A}$  definiramo kot

$$\cap \mathcal{A} = \cap_{\lambda \in J} A_\lambda = \{x; (\forall \lambda)(\lambda \in J \Rightarrow x \in A_\lambda)\}$$

(Če bi bil  $J = \emptyset$ , bi  $\cap \mathcal{A} = \text{vse}$ . To pa ni možno zaradi Russellove antinomije (ki ste jo že spoznali pri Analizi 1)!) )

Če je  $J$  končna, vzamemo po navadi  $J = \{1, 2, \dots, n\}$  in pišemo

$$\cap \mathcal{A} = \cap_{j=1}^n A_j = A_1 \cap \dots \cap A_n.$$

Če velja  $A \cap B = \emptyset$ , pravimo, da sta si množici  $A$  in  $B$  *tuji* (ali da sta *disjunktni*).

**Osnovne lastnosti preseka:**

- $A \cap B = B \cap A$ , komutativnost
- $(A \cap B) \cap C = A \cap (B \cap C)$ , asociativnost
- $A \cap A = A$ , idempotentnost

- $A \cap \emptyset = \emptyset$
- $A \cap B \subseteq A, A \cap B \subseteq B,$
- $A \subseteq B \Leftrightarrow A \cap B = A$
- $A \subseteq B \wedge A \subseteq C \Rightarrow A \subseteq B \cap C$

**Domača naloga:** Dokažite te lastnosti. (Dokazi so podobni dokazom analognih lastnosti za unijo.)

Unija in presek sta povezana z distributivnostnima zakonom:

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$

Dokažimo prvi distributivnostni zakon:  $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ .  
Kako dokažemo enakost dveh množic,  $X = Y$ ? Možnih je več načinov:

1. Po definiciji. Torej direktno dokažemo pravilnost izjave  $(\forall x)(x \in X \Leftrightarrow x \in Y)$ .

*ALI*

2. S pomočjo ekvivalence  $X = Y \Rightarrow X \subseteq Y \wedge Y \subseteq X$ .

a) Dokažemo  $X \subseteq Y$ , tj., pravilnost izjave  $(\forall x)(x \in X \Rightarrow x \in Y)$ .

b) Dokažemo še  $Y \subseteq X$ , tj., pravilnost izjave  $(\forall x)(x \in Y \Rightarrow x \in X)$ .

Poglejmo si 1. način:

$$\begin{aligned}
 x &\in (A \cup B) \cap C \\
 &\Leftrightarrow \\
 (x &\in A \cup B) \wedge (x \in C) \\
 &\Leftrightarrow \\
 (x &\in A \vee x \in B) \wedge (x \in C) \\
 &\Leftrightarrow \\
 (x &\in A \wedge x \in C) \vee (x \in B \wedge x \in C)
 \end{aligned}$$

$$\Leftrightarrow$$

$$(x \in A \cap C) \vee (x \in B \cap C)$$

$$\Leftrightarrow$$

$$x \in (A \cap C) \cup (B \cap C).$$

Ker gornja veriga ekvivalenc velja za poljuben  $x$ , je izjava

$$(\forall x)(x \in (A \cup B) \cap C \Leftrightarrow x \in (A \cap C) \cup (B \cap C))$$

pravilna. Torej sta množici enaki. □

Distributivnostna zakona veljata tudi bolj splošno, za neprazne družine množic:

$$\left(\bigcup_{\lambda \in J} A_\lambda\right) \cap \left(\bigcup_{\mu \in K} B_\mu\right) = \bigcup_{\lambda \in J, \mu \in K} (A_\lambda \cap B_\mu).$$

$$\left(\bigcap_{\lambda \in J} A_\lambda\right) \cup \left(\bigcap_{\mu \in K} B_\mu\right) = \bigcap_{\lambda \in J, \mu \in K} (A_\lambda \cup B_\mu).$$

**Domača naloga:** Dokažite, da za poljubne tri množice  $A, B, C$  velja:

$$(A \cap B) \cup C = A \cap (B \cup C) \Leftrightarrow C \subseteq A.$$

(Pogoj na desni je neodvisen od množice  $B$ !)

Ponovimo: Unijo družine množic  $\mathcal{A} = \{A_\lambda; \lambda \in J\}$  smo definirali kot  $\cup \mathcal{A} = \{x; (\exists \lambda)(\lambda \in J \wedge x \in A_\lambda)\}$ , presek neprazne družine množic pa kot  $\cap \mathcal{A} = \{x; (\forall \lambda)(\lambda \in J \Rightarrow x \in A_\lambda)\}$ .

Kaj dobimo v primeru  $\mathcal{A} = \{A_1\}$ ?  $J = \{1\}$ .

$$\cup \{A_1\} = \{x; (\exists \lambda)(\lambda \in \{1\} \wedge x \in A_\lambda)\} = \{x; (\exists \lambda)(\lambda = 1 \wedge x \in A_\lambda)\} = \{x; x \in A_1\} = A_1.$$

$$\cap \{A_1\} = \{x; (\forall \lambda)(\lambda \in \{1\} \Rightarrow x \in A_\lambda)\} = \{x; (\forall \lambda)(\lambda = 1 \Rightarrow x \in A_\lambda)\} = \{x; x \in A_1\} = A_1.$$

Pisano brez indeksov:  $\cup \{A\} = \cap \{A\} = A$ .

Podobno velja tudi  $\cup \{\emptyset\} = \cap \{\emptyset\} = \emptyset$  in  $\cup \emptyset = \emptyset$ .

### 2.1.5 Razlika množic

Dani sta množici  $A$  in  $B$ .

*Razlika* množic  $A$  in  $B$  je množica, ki ima za elemente natanko tiste reči, ki so elementi množice  $A$ , niso pa elementi množice  $B$ .

$$A \setminus B = \{x; x \in A \wedge x \notin B\}.$$

**Zgled:** Naj bo  $A$  množica praštevil,  $B$  pa množica vseh pozitivnih lihih števil. Tedaj je

$$A \setminus B = \{2\} \text{ (2 je edino sodo praštevilo)}$$

$$B \setminus A = \{1, 9, 15, 21, 25, \dots\} \text{ (množica vseh lihih števil, ki niso praštevila)}$$

Osnovne lastnosti:

- $A \setminus A = \emptyset$
- $A \setminus (A \cap B) = A \setminus B$
- $A \cap (A \setminus B) = A \setminus B$
- $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
- $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
- $(A \setminus B) \cup B = A \cup B$
- $(A \cup B) \setminus B = A \setminus B$
- $(A \cap B) \setminus B = \emptyset$
- $(A \setminus B) \cap B = \emptyset$

Dokažimo enakost  $(A \setminus B) \cup B = A \cup B$ :

$$x \in (A \setminus B) \cup B$$

$$\Leftrightarrow$$

$$x \in A \setminus B \vee x \in B$$

$$\Leftrightarrow$$

$$\begin{aligned}
& (x \in A \wedge x \notin B) \vee x \in B \\
& \Leftrightarrow \\
& (x \in A \vee x \in B) \wedge (x \notin B \vee x \in B) \\
& \Leftrightarrow \\
& (x \in A \vee x \in B) \\
& \Leftrightarrow \\
& x \in A \cup B
\end{aligned}$$

□

**Domača naloga:** Dokažite preostale lastnosti.

Zelo pogosto smo v matematiki v temle položaju: podana je neka *univerzalna množica*  $S$ , zanimamo se izključno za elemente in podmnožice množice  $S$ .

Naj bo  $A \subseteq S$ . Tedaj lahko definiramo *komplement množice*  $A$  (glede na množico  $S$ ) kot:

$$C_S A = \bar{A} = S \setminus A.$$

Če množice  $S$  ne definiramo, ne moremo govoriti o komplementu:  $\bar{\emptyset} =$  množica vseh množic — ta pa ne obstaja (Russellova antinomija)!

**Zgled:** Naj bo  $S = \{0, 1, 2, 3, \dots\}$  množica naravnih števil, množica  $A$  pa množica praštevil. Potem je  $\bar{A} = \{0, 1, 4, 6, 8, 9, 10, 12, \dots\}$ .



Lastnosti komplementa:

- $\bar{S} = \emptyset, \quad \bar{\emptyset} = S$
- $\overline{\bar{A}} = A, \quad A \cup \bar{A} = S, \quad A \cap \bar{A} = \emptyset$
- $A \setminus B = A \cap \bar{B}$
- $A \subseteq B \Leftrightarrow \bar{B} \subseteq \bar{A}$
- $A = B \Leftrightarrow \bar{A} = \bar{B}$

- $\overline{A \cup B} = \overline{A} \cap \overline{B}$ ,  $\overline{A \cap B} = \overline{A} \cup \overline{B}$  (De Morganova zakona)

De Morganova zakona veljata tudi za poljubno družino množic  $\mathcal{A} = \{A_\lambda; \lambda \in J\}$ :

$$\overline{\bigcup_{\lambda \in J} A_\lambda} = \bigcap_{\lambda \in J} \overline{A_\lambda}$$

$$\overline{\bigcap_{\lambda \in J} A_\lambda} = \bigcup_{\lambda \in J} \overline{A_\lambda}$$

Zaradi De Morganovih zakonov se izreki v teoriji množic pogosto pojavljajo v parih. Če v neki inkluziji, enakosti ali ekvivalenci o unijah, presekih in komplementih podmnožic neke množice zamenjamo vsako množico z njenim komplementom, zamenjamo vse unije in preseke in obrnemo vse inkluzije, je rezultat spet neka veljavna inkluzija, enakost ali ekvivalenca. Temu principu pravimo **princip dualnosti**.

### Zgled:

Trditev

$$(A \cap B) \cup C = A \cap (B \cup C) \Leftrightarrow C \subseteq A.$$

postane

$$(\overline{A} \cup \overline{B}) \cap \overline{C} = \overline{A} \cup (\overline{B} \cap \overline{C}) \Leftrightarrow \overline{A} \subseteq \overline{C},$$

kar je ekvivalentno trditvi

$$(A \cup B) \cap C = A \cup (B \cap C) \Leftrightarrow A \subseteq C$$

(zamenjali smo vloge množic in njihovih komplementov). ▲

## 2.1.6 Vennovi diagrami

Vse odnose in operacije med podmnožicami dane univerzalne množice lahko nazorno prikažemo s t.i. *Vennovimi diagrami*.

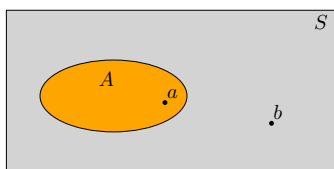
Seveda pa tako "slikanje" nima nobene zveze z dokazovanjem.

## 2.1.7 Potenčna množica

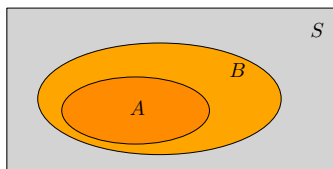
*Potenčna množica* dane množice  $A$  je družina množic, ki ima za svoje elemente natanko podmnožice množice  $A$ :

$$\mathcal{P}(A) = \{X; X \subseteq A\}$$

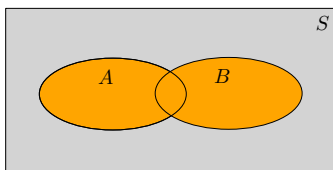




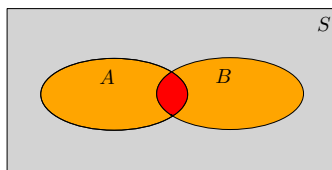
$$a \in A; b \notin A$$



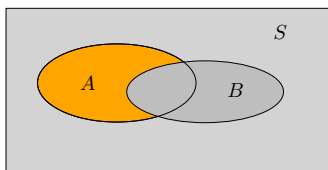
$$A \subseteq B$$



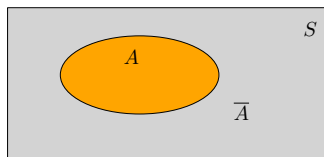
$$A \cup B$$



$$A \cap B$$



$$A \setminus B$$



$$\bar{A}$$

### Zgled:

- $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
- $\mathcal{P}(\emptyset) = \{\emptyset\}$ .
- $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$ .

Če ima množica  $A$   $n$  elementov, potem ima njena potenčna množica  $\mathcal{P}(A)$   $2^n$  elementov.<sup>1</sup>

### Lastnosti:

<sup>1</sup> Za vsakega od  $n$  elementov množice  $A$  je potrebno določiti, neodvisno od ostalih, ali ga množica  $X \subseteq A$  vsebuje ali ne. Skupaj imamo torej  $n$  neodvisnih izbir ene izmed dveh možnosti, kar nam da, za vse podmnožice  $X \subseteq A$ , ravno  $2^n$  možnosti.

- $A \subseteq B \Rightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$ .
- $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$ .
- $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$ .

Prva lastnost sledi iz tranzitivnosti inkluzije:

$$X \in \mathcal{P}(A) \wedge A \subseteq B \Leftrightarrow X \subseteq A \subseteq B \Rightarrow X \subseteq B \Leftrightarrow X \in \mathcal{P}(B).$$

Dokaz druge lastnosti:

$$X \in \mathcal{P}(A) \cup \mathcal{P}(B) \Leftrightarrow X \subseteq A \vee X \subseteq B \Rightarrow X \subseteq A \cup B \Leftrightarrow X \in \mathcal{P}(A \cup B).$$

Dokaz tretje lastnosti:

$$\begin{aligned} X \in \mathcal{P}(A) \cap \mathcal{P}(B) &\Leftrightarrow X \in \mathcal{P}(A) \wedge X \in \mathcal{P}(B) \Leftrightarrow X \subseteq A \wedge X \subseteq B \\ &\Leftrightarrow X \subseteq A \cap B \Leftrightarrow X \in \mathcal{P}(A \cap B) \end{aligned}$$

**V razmislek:** Ali v prvi lastnosti velja ekvivalenca?

**V razmislek:** Zakaj v drugi lastnosti ne velja enakost?

### 2.1.8 Urejeni par

Vzemimo dve reči  $a$  in  $b$ .

Za množico  $\{a, b\}$  vrstni red ni pomemben,  $\{a, b\} = \{b, a\}$ .

Kadar je vrstni red pomemben, govorimo o *urejenem paru*:

$(a, b)$  - urejen par,  $(a, b) \neq (b, a)$

$a$  - prva koordinata

$b$  - druga koordinata

Kdaj sta dva urejena para enaka?

$$(a, b) = (u, v) \Leftrightarrow a = u \wedge b = v.$$

Urejeni par  $(a, b)$  definiramo kot množico  $\{\{a\}, \{a, b\}\}$ .

**Domača naloga:** Dokažite, da velja  $\{\{a\}, \{a, b\}\} = \{\{u\}, \{u, v\}\} \Leftrightarrow a = u \wedge b = v$ .

### 2.1.9 Kartezični produkt

Pojem kartezičnega produkta ste spoznali že pri Analizi I.

Kartezični produkt množic  $A$  in  $B$  je množica, ki ima za elemente natančno vse urejene pare  $(x, y)$ , kjer je prva koordinata iz množice  $A$ , druga koordinata pa iz množice  $B$ :

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

**Zgled:**  $\{1\} \times \{2, 3\} = \{(1, 2), (1, 3)\}$ ,  
 $\{2, 3\} \times \{1\} = \{(2, 1), (3, 1)\}$ .

Lastnosti kartezičnega produkta:

- $A \times B \neq B \times A$  (razen če je  $A = B$ )
- $A \times B = \emptyset \Leftrightarrow A = \emptyset \vee B = \emptyset$ .
- $A \times (B \cup C) = (A \times B) \cup (A \times C)$ .
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$ .
- $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$ .

Kartezični produkt treh množic definiramo kot:

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

Po navadi pišemo kar:  $((x, y), z) = (x, y, z)$  (urejena trojica).

Kartezični produkt množic  $A_1, \dots, A_n$  definiramo kot množico vseh urejenih  $n$ -teric:

$$A_1 \times A_2 \times \dots \times A_n = \prod_{i=1}^n A_i = \{(x_1, \dots, x_n) ; x_1 \in A_1 \wedge x_2 \in A_2 \wedge \dots \wedge x_n \in A_n\}.$$

Če so vsi faktorji enaki,  $A_1 = A_2 = \dots = A_n = S$ , dobimo  $n$ -kratni kartezični produkt množice  $S$  s samo seboj,

$$S^n = \prod_{i=1}^n S = S \times \dots \times S \text{ } n \text{ faktorjev.}$$

**Zgled:** Če je  $S = \mathbb{R}$  množica realnih števil, dobimo za  $n = 2$  množico točk v ravnini ( $\mathbb{R}^2$ ), za  $n = 3$  pa množico točk v prostoru ( $\mathbb{R}^3$ ). ▲

**Rešitev dveh domačih nalog:**

Dokažimo, da za poljubne tri množice  $A, B, C$  velja:

$$(A \cap B) \cup C = A \cap (B \cup C) \Leftrightarrow C \subseteq A.$$

$(\Rightarrow)$ : Naj bo  $(A \cap B) \cup C = A \cap (B \cup C)$ .

$C \subseteq (A \cap B) \cup C = A \cap (B \cup C) \subseteq A$ . Uporabimo tranzitivnost inkluzije.

$(\Leftarrow)$ : Naj bo  $C \subseteq A$ . Tedaj je  $A \cup C = A$ .

Torej je  $(A \cap B) \cup C = (A \cup C) \cap (B \cup C) = A \cap (B \cup C)$ . ▲

Dokažimo implikacijo

$$A \subseteq C \wedge B \subseteq C \Rightarrow A \cup B \subseteq C :$$

Dokaz s protislovjem:

$$\neg(A \cup B \subseteq C)$$

$$\Leftrightarrow$$

$$(\exists x)(x \in A \cup B \wedge x \notin C)$$

$$\Leftrightarrow$$

$$(\exists x)((x \in A \vee x \in B) \wedge x \notin C)$$

$$\Leftrightarrow$$

$$(\exists x)((x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C))$$

$$\Leftrightarrow$$

$$(\exists x)((x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C))$$

$$\Leftrightarrow$$

$$(\exists x)(x \in A \wedge x \notin C) \vee (\exists x)(x \in B \wedge x \notin C)$$

$$\Leftrightarrow$$

$$\neg(\forall x)(x \in A \Rightarrow x \in C) \vee \neg(\forall x)(x \in B \Rightarrow x \in C)$$

$$\Leftrightarrow$$

$$\neg(A \subseteq C) \vee \neg(B \subseteq C)$$

$\Leftrightarrow$

$$\neg(A \subseteq C \wedge B \subseteq C).$$

□

Dokazali smo ne samo implikacijo, ampak ekvivalenco

$$A \subseteq C \wedge B \subseteq C \Leftrightarrow A \cup B \subseteq C.$$

## 2.2 O AKSIOMIH

Vsaka matematična teorija temelji na množici aksiomov — osnovnih trditvah, ki jih *privzamemo* za pravilne. Ti aksiomi opredeljujejo osnovne lastnosti, ki jim morajo zadoščati objekti obravnavane teorije (npr. naravna števila, realna števila, grupe, vektorski prostori, topološki prostori, ...) Iz aksiomov pa potem s pomočjo logičnega sklepanja izpeljujemo nove resnice, ki jim pravimo trditve, posledice, izreki.

V teoriji množic ni nič drugače! Obstaja več družin aksiomov, najbolj pa je uveljavljenih 7 aksiomov, imenovanih *aksiomi ZFC* (Zermelo–Fraenkel–(Axiom of) Choice).

Aksiomi zagotavljajo obstoj množic in tvorjenje novih množic iz že obstoječih.

Da bi razumeli, zakaj potrebujemo aksiome, si pogledjmo, zakaj množica vseh množic ne obstaja.

### 2.2.1 Russellova antinomija

Ali obstaja *množica vseh množic*?

Recimo, da obstaja. Naj bo  $A$  množica vseh množic.

Za vsako množico se lahko vprašamo, ali ima samo sebe za element.  $\mathbb{N}$  nima same sebe za element! Množica vseh abstraktnih pojmov pa ima samo sebe za element.

Naj bo  $B \subseteq A$  tista podmnožica množice  $A$ , ki ima za elemente natanko tiste množice iz  $A$ , ki nimajo same sebe za element.

Ali ima množica  $B$  samo sebe za element?

Če ja, potem nima same sebe za element!

Kaj pa če B nima same sebe za element? Potem pa po definiciji  $B \in B$ . Protislovje.

*Množica vseh množic ne obstaja!*

Nič ne vsebuje vsega. (*Matematično*) *vesolje ne obstaja.*

Torej pri oblikovanju množic ne smemo preveč zaupati svoji intuiciji. Potrebni so aksiomi, ki zagotavljajo obstoj nekaterih množic.

### 2.2.2 Aksiomi teorije množic (po Endertonu)

1. Aksiom o ekstenzionalnosti (enakost množic)

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

2. Aksiom o prazni množici: *Obstaja prazna množica.*

$$\exists B \forall x (x \notin B)$$

3. Aksiom o paru: *Obstajajo dvoelementne množice.*

$$\forall u \forall v \exists B \forall x (x \in B \Leftrightarrow x = u \text{ ali } x = v)$$

4. Aksiom o uniji: *Obstaja unija poljubne družine množic.*

$$\forall A \exists B \forall x (x \in B \Leftrightarrow (\exists b \in A) x \in b)$$

5. Aksiom o potenčni množici: *Obstaja potenčna množica vsake množice.*

$$\forall a \exists B \forall x (x \in B \Leftrightarrow x \subseteq a)$$

6. Aksiomska shema o podmnožicah: *Obstajajo raznovrstne podmnožice.*

Za vsako predikatno formulo  $\varphi$  o množicah  $t_1, \dots, t_k$ , ki ne vsebuje črke B, je naslednji izraz aksiom:

$$\forall t_1 \dots \forall t_k \forall c \exists B \forall x (x \in B \Leftrightarrow x \in c \wedge \varphi)$$

**Zgled:** (Za  $k = 1$ ):

$$\forall a \forall c \exists B \forall x (x \in B \Leftrightarrow x \in c \wedge x \in a)$$

To pomeni, da za vsaki dve množici  $a$  in  $c$  obstaja množica  $B = a \cap c$ , njun presek.

Zgornja aksiomska shema omogoča opisovanje množic v obliki

$$\{x \in A; P(x)\}.$$

**Zgled:**  $\{x \in \mathbb{R}; x \geq 0\}$ .

7. Aksiom o neskončnosti: *Obstaja neskončna množica.*

$$\exists A (\emptyset \in A \wedge (\forall a \in A) (a \cup \{a\} \in A))$$

8. Aksiom izbire: *Vsaka relacija vsebuje funkcijo z isto domeno.*

$$(\forall \text{ relacijo } R)(\exists \text{ funkcija } F)(F \subseteq R \wedge \mathcal{D}(F) = \mathcal{D}(R))$$

Ta aksiom bomo podrobno obravnavali v poglavju 2.5.

Nekatere aksiome oz. aksiomske sheme, in sicer 2., 3. in 6. z zgornjega seznama, je moč izpeljati iz preostalih 7 aksiomov.





# 3

## RELACIJE

Znotraj vsake matematične teorije  $\mathcal{T}$  z univerzalno množico  $S$  lahko vsako smiselno lastnost  $P(x)$  predstavimo z množico

$$\{x ; x \in S \wedge P(x)\}.$$

Tudi odnose ali *relacije* moremo predstaviti z množicami.

Primeri dvomestnih (binarnih) relacij:  $\in, \subseteq, =, \leq, >$ , vzporeden, skladen

- Primer: 3 in 5 sta v relaciji "manjši".

Trimestne relacije: vsota, razlika, produkt

---

"Družinske" relacije: oče, sin, mati, sestra, mož, tašča, ...

starši - trimestna relacija  $(x, y, z)$  so v relaciji natanko tedaj, ko sta  $x$  in  $y$  starša  $z$ )

### 3.1 SPLOŠNO O RELACIJAH

Naj bo  $R$  neka smiselna binarna relacija za neko matematično teorijo  $\mathcal{T}$  z univerzalno množico  $S$ .

$R$  bomo predstavili z množico natanko tistih urejenih parov množice  $S$ , katerih prva koordinata je v relaciji  $R$  z drugo koordinato.

$x$  je v relaciji  $R$  z  $y$ :  $xRy$  ali  $R(x, y)$ .

$$R = \{(x, y) ; x, y \in S \wedge xRy\}$$

ali krajše (če se razume, kaj je univerzalna množica  $S$ ):

$$R = \{(x, y) ; xRy\}.$$

Če je  $R$   $n$ -mestna relacija, pa uporabimo  $n$ -terice:

$$R = \{(x_1, \dots, x_n) ; R(x_1, \dots, x_n)\}$$

---

Dvomestna relacija je torej **podmnožica kartezičnega produkta**  $S \times S =: S^2$ .

$n$ -mestna relacija pa je podmnožica  $n$ -kratnega kartezičnega produkta množice  $S$  s samo seboj,  $S^n$ .

**Zgled:**

$$S = \{1, 2, 3, 4\},$$

Dvomestna relacija "manjši",  $< (x, y) \Leftrightarrow x < y$ :

$$< = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}.$$

Trimestna relacija "vsota",  $+(x, y, z) \Leftrightarrow x + y = z$ :

$$+ = \{(1, 1, 2), (1, 2, 3), (1, 3, 4), (2, 1, 3), (2, 2, 4), (3, 1, 4)\}.$$



**Zgled:**

$$S = \{1, 2, 3, 4, 5, 6\},$$

Dvomestna relacija  $R$  "je večkratnik",  $R(x, y) \Leftrightarrow x$  je večkratnik  $y$ , tj.,

$(\exists k)(k \text{ je pozitivno naravno število in } x = k \cdot y)$ :

$$R = \{(1, 1), (2, 1), (2, 2), (3, 1), (3, 3), (4, 1), (4, 2), (4, 4), (5, 1), (5, 5), (6, 1), (6, 2), (6, 3), (6, 6)\}.$$

Trimestna relacija "produkt",  $\cdot (x, y, z) \Leftrightarrow z = x \cdot y$ :

$$\cdot = \{(1, 1, 1), (1, 2, 2), (1, 3, 3), (1, 4, 4), (1, 5, 5), (1, 6, 6), (2, 1, 2),$$

$$(2, 2, 4), (2, 3, 6), (3, 1, 3), (3, 2, 6), (4, 1, 4), (5, 1, 5), (6, 1, 6)\}.$$

Enomestna relacija "praštevilo",  $P(x) \Leftrightarrow x$  je praštevilo:

$$P = \{2, 3, 5\}.$$



Ker smo relacije predstavili z množicami, lahko govorimo tudi o relacijah  $R \cup T$ ,  $R \cap T$ ,  $R \setminus T$  (če sta relaciji  $R$  in  $T$  obe  $n$ -mestni relaciji za isti  $n$ ).

**Zgled:** Če z  $R_{\leq}$ ,  $R_{<}$ ,  $R_{=}$ ,  $R_{\geq}$ ,  $R_{>}$  in  $R_{\neq}$  zaporedoma označimo relacije “manjši ali enak”, “manjši”, “enak”, “večji ali enak”, “večji” in “neenak” (npr. na množici naravnih števil), potem velja:

$$R_{\leq} = R_{<} \cup R_{=}$$

$$R_{>} = R_{\geq} \setminus R_{=} = R_{\geq} \cap R_{\neq}$$



Osredotočimo se sedaj na **binarne relacije** (te so posebnega pomena, kot bomo videli v poglavju o strukturah urejenosti).

Naj bo  $R$  binarna relacija v univerzalni množici  $S$ :

$$R = \{(x, y) ; xRy\}.$$

Množico vseh prvih koordinat elementov iz  $R$  imenujemo *domena relacije*  $R$ .

Množico vseh drugih koordinat elementov iz  $R$  pa imenujemo *zaloga vrednosti (kodomena) relacije*  $R$ .

Domena:

$$\mathcal{D}R = \{x ; (\exists y)(xRy)\}$$

Zaloga vrednosti:

$$\mathcal{Z}R = \{y ; (\exists x)(xRy)\}$$

(v uporabi sta tudi oznaki  $\mathcal{R}R$  in  $\text{Im}R$ )

**Zgled:**

$$R = \{(1, 2), (2, 3), (2, 4)\}.$$

$$\mathcal{D}R = \{1, 2\},$$

$$\mathcal{Z}R = \{2, 3, 4\}$$



**Zgled:** Naj bo  $X$  poljubna množica in  $S = X \cup \mathcal{P}(X)$ . Relacija  $R$  je podmnožica  $S \times S$ , definirana s predpisom

$$xRy \Leftrightarrow x \in X \wedge y \in \mathcal{P}(X) \wedge x \in y.$$

Tedaj je  $\mathcal{D}R = X$  in  $\mathcal{Z}R = \mathcal{P}(X) \setminus \{\emptyset\}$ .



### 3.1.1 Inverzna relacija

$$R^{-1} = \{(y, x) ; xRy\}$$

Očitno je:

- $yR^{-1}x \Leftrightarrow xRy$ .
- $\mathcal{D}R^{-1} = \mathcal{Z}R$  in  $\mathcal{Z}R^{-1} = \mathcal{D}R$ .
- $(R^{-1})^{-1} = R$ .

**Zgled:**

$$\begin{aligned} R_{\leq}^{-1} &= R_{\geq}, \\ R_{<}^{-1} &= R_{>}, \\ R_{=}^{-1} &= R_{=}, \\ R_{\neq}^{-1} &= R_{\neq}. \end{aligned}$$



### 3.1.2 Kompozitum relacij

Dani sta binarni relaciji  $R$  in  $T$ .

$T \circ R$ : kompozitum relacije  $R$  z relacijo  $T$

$$xT \circ Ry \Leftrightarrow (\exists u)(xRu \wedge uTy)$$

$$T \circ R = \{(x, y) ; (\exists u)(xRu \wedge uTy)\}$$

Očitno velja:  $T \circ R \subseteq (\mathcal{D}R) \times (\mathcal{Z}T)$ .

**Zgled:**

$$R = \{(1, 3), (2, 3)\}, T = \{(3, 1), (2, 1)\}$$

$$T \circ R = \{(1, 1), (2, 1)\}, R \circ T = \{(3, 3), (2, 3)\}.$$

$$\text{brat} \circ \text{oče} \subseteq \text{oče}$$

$$\text{oče} \circ \text{brat} \subseteq \text{stric}$$

$$(\text{oče} \circ \text{brat}) \cup (\text{mati} \circ \text{brat}) = \text{stric}$$

$$\text{sestra} \circ \text{mati} \subseteq \text{mati}$$

$$(\text{žena} \circ \text{mati}) \cup (\text{mož} \circ \text{mati}) = \text{tašča}$$

Torej v splošnem  $T \circ R \neq R \circ T$ . Velja pa asociativnost.



**Trditev.** Naj bodo  $V, T, R$  binarne relacije v univerzalni množici  $S$ . Tedaj velja

$$V \circ (T \circ R) = (V \circ T) \circ R.$$

*Dokaz.*

$$\begin{aligned} (x, y) \in V \circ (T \circ R) &\Leftrightarrow xV \circ (T \circ R)y \Leftrightarrow \\ (\exists u)(x(T \circ R)u \wedge uVy) &\Leftrightarrow (\exists u)(\exists v)(xRv \wedge vTu \wedge uVy) \Leftrightarrow \\ (\exists v)(xRv \wedge (\exists u)(vTu \wedge uVy)) &\Leftrightarrow (\exists v)(xRv \wedge v(V \circ T)y) \Leftrightarrow \\ x((V \circ T) \circ R)y &\Leftrightarrow (x, y) \in (V \circ T) \circ R. \end{aligned}$$

□

Inverz kompozituma je enak kompozitumu inverzov v obratnem vrstnem redu:

**Trditev.** Naj bosta  $T$  in  $R$  binarni relaciji v univerzalni množici  $S$ . Tedaj velja

$$(T \circ R)^{-1} = R^{-1} \circ T^{-1}.$$

*Dokaz.*

$$\begin{aligned} (x, y) \in (T \circ R)^{-1} &\Leftrightarrow (y, x) \in T \circ R \Leftrightarrow \\ (\exists u)(yRu \wedge uTx) &\Leftrightarrow (\exists u)(uR^{-1}y \wedge xT^{-1}u) \Leftrightarrow \\ (\exists u)(xT^{-1}u \wedge uR^{-1}y) &\Leftrightarrow x(R^{-1} \circ T^{-1})y \Leftrightarrow (x, y) \in R^{-1} \circ T^{-1}. \end{aligned}$$

□

### Zgled:

Naj bosta  $a, b \in \mathbb{R}$ .

Definirajmo relaciji

$$R = \{(x, y) ; x + y = a\},$$

$$T = \{(x, y) ; x + y = b\}.$$

Tedaj je

$$T \circ R = \{(x, y) ; (\exists u)(x + u = a \wedge u + y = b)\} = \{(x, y) ; x - y = a - b\}.$$

$$R \circ T = \{(x, y) ; x - y = b - a\}.$$

$$R^{-1} = R, T^{-1} = T.$$

Enakost v zgornji trditvi v tem primeru postane  $(T \circ R)^{-1} = R \circ T$ . ▲

### 3.1.3 Univerzalna, ničelna in identična relacija

V vsaki množici  $S$  imamo tri posebne relacije:

$S \times S$  – univerzalna relacija

$\emptyset$  – ničelna relacija

$I = \{(x, x) ; x \in S\}$  – identična relacija (relacija identitete)

**Trditev.** Naj bo  $R$  binarna relacija v univerzalni množici  $S$ .

Tedaj velja  $I \circ R = R \circ I = R$ .

*Dokaz.*  $xI \circ Ry \Leftrightarrow (\exists u)(xRu \wedge uIy) \Leftrightarrow xRy$ .

$xR \circ Iy \Leftrightarrow (\exists u)(xIu \wedge uRy) \Leftrightarrow xRy$ . □

Velja tudi:

- $\emptyset \circ R = R \circ \emptyset = \emptyset$
- $(S \times S) \circ R = (\mathcal{D}R) \times S$  in  $R \circ (S \times S) = S \times \mathcal{Z}R$ .

Dokažimo enakost  $R \circ (S \times S) = S \times \mathcal{Z}R$ :

$x(R \circ (S \times S))y \Leftrightarrow (\exists u)(x(S \times S)u \wedge uRy) \Leftrightarrow (\exists u)(uRy) \Leftrightarrow y \in \mathcal{Z}R \Leftrightarrow x \in S \wedge y \in \mathcal{Z}R \Leftrightarrow x(S \times \mathcal{Z}R)y$ .

**Domača naloga:** Dokažite enakost  $(S \times S) \circ R = (\mathcal{D}R) \times S$ .

## 3.2 POSEBNE LASTNOSTI BINARNIH RELACIJ

Nekatere lastnosti binarnih relacij so še posebej pomembne:

$R$  je *refleksivna*  $\Leftrightarrow (\forall x)(x \in S \Rightarrow xRx)$

**Zgled:** relacija  $\leq$  v realnih številih

$R$  je *irefleksivna*  $\Leftrightarrow (\forall x)(x \in S \Rightarrow \neg(xRx))$

**Zgled:** relacija  $<$  v realnih številih

$R$  je *simetrična*  $\Leftrightarrow (\forall x)(\forall y)(x \in S \wedge y \in S \wedge xRy \Rightarrow yRx)$

**Zgled:** vzporednost premic

$R$  je *asimetrična*  $\Leftrightarrow (\forall x)(\forall y)(x \in S \wedge y \in S \wedge xRy \Rightarrow \neg(yRx))$

**Zgled:** relacija  $<$  v realnih številih

$R$  je *antisimetrična*  $\Leftrightarrow (\forall x)(\forall y)(x \in S \wedge y \in S \wedge xRy \wedge yRx \Rightarrow x = y)$

**Zgled:** relacija  $\leq$  v realnih številih

relacija  $\subseteq$  v množicah

$R$  je *tranzitivna*  $\Leftrightarrow (\forall x)(\forall y)(\forall z)(x \in S \wedge y \in S \wedge z \in S \wedge xRy \wedge yRz \Rightarrow xRz)$

**Zgled:** relacija  $<$  v realnih številih

relacija  $\subset$  v množicah

$R$  je *intransitivna*  $\Leftrightarrow (\forall x)(\forall y)(\forall z)(x \in S \wedge y \in S \wedge z \in S \wedge xRy \wedge yRz \Rightarrow \neg(xRz))$

**Zgled:** relacija  $R$  v realnih številih, definirana s predpisom  $xRy \Leftrightarrow x =$

$y + 1$

pravokotnost premic v ravnini

$R$  je *sovisna*  $\Leftrightarrow (\forall x)(\forall y)(x \in S \wedge y \in S \wedge x \neq y \Rightarrow (xRy) \vee (yRx))$

**Zgled:** relacija  $<$  v realnih številih

$R$  je *strogo sovisna*  $\Leftrightarrow (\forall x)(\forall y)(x \in S \wedge y \in S \Rightarrow (xRy) \vee (yRx))$

**Zgled:**

relacija  $\leq$  v realnih številih

**Domača naloga:** Izberite si nekaj sorodstvenih relacij in za vsako od njih ugotovite, katere od zgornjih lastnosti imajo.

Nekatere od zgornjih lastnosti niso med seboj neodvisne:

- $R$  je strogo sovisna  $\Rightarrow R$  je sovisna.
- $R$  je asimetrična  $\Rightarrow R$  je irefleksivna.
- $R$  je simetrična in tranzitivna  $\Rightarrow R$  je refleksivna (če je  $\mathcal{D}R = S$ ).

### 3.3 EKVIVALENČNA RELACIJA

$R$  je *ekvivalenčna*  $\Leftrightarrow R$  je refleksivna, simetrična in tranzitivna.

**Zgled:** relacija identitete

Ekvivalenčne relacije lahko karakteriziramo na naslednji način.

**Trditev.**  $R$  je ekvivalenčna  $\Leftrightarrow \mathcal{D}R = S$  in  $R^{-1} \circ R = R$ .

*Dokaz.* Pogoj je potreben:

$$xRx \Rightarrow \mathcal{D}R = S$$

$$xR^{-1} \circ Ry \Rightarrow (\exists z)(xRz \wedge zR^{-1}y) \Rightarrow (\exists z)(xRz \wedge yRz) \Rightarrow (\exists z)(xRz \wedge zRy) \Rightarrow xRy.$$

$$xRy \Rightarrow (xRy \wedge yRy) \Rightarrow (xRy \wedge yR^{-1}y) \Rightarrow xR^{-1} \circ Ry.$$

Torej  $R^{-1} \circ R = R$ .

Pogoj je pa tudi zadosten:

Naj bo  $\mathcal{D}R = S$  in  $R^{-1} \circ R = R$ .

**Refleksivnost:** dokazujemo  $(\forall x)(x \in S \Rightarrow xRx)$ . Naj bo  $x \in S$ . Ker je  $\mathcal{D}R = S$ , je  $x \in \mathcal{D}R \Rightarrow (\exists y)(y \in S \wedge xRy)$ .

$$xRy \Rightarrow xRy \wedge yR^{-1}x \Rightarrow xR^{-1} \circ Rx \Rightarrow xRx.$$

**Simetričnost:** dokazujemo  $(\forall x)(\forall y)(x \in S \wedge y \in S \wedge xRy \Rightarrow yRx)$ .

Naj bo  $x \in S \wedge y \in S \wedge xRy$ . Tedaj je

$$xRy \Rightarrow (xRy \wedge yRy) \Rightarrow (yRy \wedge yR^{-1}x) \Rightarrow yR^{-1} \circ Rx \Rightarrow yRx.$$

**Tranzitivnost:** dokazujemo  $(\forall x)(\forall y)(\forall z)(x \in S \wedge y \in S \wedge z \in S \wedge xRy \wedge yRz \Rightarrow xRz)$ .

Naj bo  $x \in S \wedge y \in S \wedge z \in S \wedge xRy \wedge yRz$ . Tedaj je

$$xRy \wedge yRz \Rightarrow xRy \wedge zRy \Rightarrow xRy \wedge yR^{-1}z \Rightarrow xR^{-1} \circ Rz \Rightarrow xRz.$$

□

Ekvivalenčna relacija ima to lepo lastnost, da razdeli množico  $S$ , na kateri je definirana, na *same neprazne in paroma disjunktne množice, katerih unija je prav množica  $S$ .*

### **Ekvivalenčni razredi.**

Naj bo  $R$  ekvivalenčna relacija, definirana v množici  $S$ . Naj bo  $x \in S$ . *Ekvivalenčni razred elementa  $x$  glede na ekvivalenčno relacijo  $R$  je množica vseh elementov, ki so v relaciji z  $x$ :*

$$R[x] = \{y ; y \in S \wedge yRx\}.$$

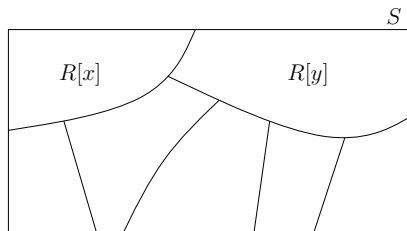
Za ekvivalenčne razrede velja naslednje:



- Ker je  $R$  refleksivna relacija, velja  $x \in R[x]$ . Posledično je  $R[x] \neq \emptyset$ .
- $y \in R[x] \Rightarrow R[y] = R[x]$ .  
Res: Naj bo  $y \in R[x]$ .  
 $z \in R[y] \Rightarrow zRy \wedge yRx \Rightarrow zRx \Rightarrow z \in R[x]$ .  
 $z \in R[x] \Rightarrow zRx \wedge yRx \Rightarrow zRx \wedge xRy \Rightarrow zRy \Rightarrow z \in R[y]$ .
- $y \notin R[x] \Rightarrow R[x] \cap R[y] = \emptyset$ .  
Res:  $(\exists z)(z \in R[x] \cap R[y]) \Rightarrow (\exists z)(R[z] = R[x] \wedge R[z] = R[y]) \Rightarrow y \in R[y] = R[x]$ . Protislovje z domnevo  $y \notin R[x]$ .

Sledi:

1. Vsak element množice  $S$  je v natanko enem ekvivalenčnem razredu. Namreč v tistem, v katerem so združeni vsi elementi množice  $S$ , ki so z njim v relaciji  $R$ .
2. Vsak ekvivalenčni razred je povsem določen s poljubnim elementom, ki mu pripada. Zato pravimo, da je poljuben element danega razreda *predstavnik* tega razreda.
3. Z ekvivalenčnimi razredi dane ekvivalenčne relacije  $R$  je množica  $S$  razdeljena na same neprazne in paroma tuje podmnožice, katerih unija je množica  $S$ .



Takim razdelitvam pravimo particije. *Particija množice  $S$*  = družina nepraznih in paroma disjunktnih množic, katerih unija je množica  $S$ .

Vsaki ekvivalenčni relaciji torej ustreza neka particija množice  $S$ . Velja pa tudi obratno. Vsaka particija  $\mathcal{A}$  množice  $S$  določa natanko eno ekvivalenčno relacijo  $R$ , in sicer tako, da so množice v particiji ravno ekvivalenčni razredi glede na relacijo  $R$ :

- Poljubna elementa  $x$  in  $y$  sta v relaciji  $R$  natanko takrat, ko pripadata isti množici iz particije:

$$xRy \Leftrightarrow (\exists X)(X \in \mathcal{A} \wedge x \in X \wedge y \in X).$$

Premislimo, da je tako definirana relacija ekvivalenčna:

- **refleksivna:**  $x \in S \Rightarrow (\exists X)(X \in \mathcal{A} \wedge x \in X) \Rightarrow xRx$ .
- **simetrična:**  $xRy \Rightarrow (\exists X)(X \in \mathcal{A} \wedge x \in X \wedge y \in X) \Rightarrow (\exists X)(X \in \mathcal{A} \wedge y \in X \wedge x \in X) \Rightarrow yRx$ .
- **tranzitivna:**  $xRy \wedge yRz \Rightarrow (\exists X)(X \in \mathcal{A} \wedge x \in X \wedge y \in X) \wedge (\exists Y)(Y \in \mathcal{A} \wedge y \in Y \wedge z \in Y)$ .

Torej je  $y$  hkrati v množici  $X$  in  $Y$ . Ker pa so množice paroma disjunktne, sledi  $X = Y$ . Potem pa je element  $z$  tudi v množici  $X$ . Sledi  $xRz$ .

**V razmislek:** Utemelji, da particija  $\mathcal{A}$  sovпада z množico ekvivalenčnih razredov relacije  $R$ .

Vsaki množici  $S$ , v kateri je definirana kakšna ekvivalenčna relacija  $R$ , moremo prirediti neko novo množico, katere elementi so ekvivalenčni razredi relacije  $R$ :

*Faktorska množica množice  $S$  glede na relacijo  $R$ :*

$$S/R = \{R[x] ; x \in S\} = \{X ; (\exists x)(x \in S \wedge X = R[x])\}$$

- Faktorska množica predstavlja matematično formulacijo logičnega principa *abstrakcije*: S tem ko iz dane množice  $S$  preidemo na faktorsko množico, abstrahiramo vse razlike med rečmi, ki pripadajo istemu ekvivalenčnemu razredu!

### Zgled:

Naj bo  $S = \{1, 2, 3\}$  in  $R = \{(1, 1), (1, 3), (2, 2), (3, 1), (3, 3)\}$ .

Relacija  $R$  je ekvivalenčna.

$$R[1] = R[3] = \{1, 3\}, R[2] = \{2\}.$$

$$S/R = \{R[1], R[2], R[3]\} = \{R[1], R[2]\} = \{\{1, 3\}, \{2\}\}.$$

Če definiramo particijo  $\mathcal{A} = \{\{1, 3\}, \{2\}\}$  množice  $S$ , potem lahko definiramo relacijo  $R'$  s predpisom  $xR'y \Leftrightarrow (\exists X)(X \in \mathcal{A} \wedge x \in X \wedge y \in X)$ . Velja

$$R' = \{(1, 1), (1, 3), (3, 1), (2, 2), (3, 3)\} = R \text{ in } S/R' = \{\{1, 3\}, \{2\}\} = \mathcal{A}. \quad \blacktriangle$$

## Zgledi ekvivalenčnih relacij

### 1. Ulomki.

V množici ulomkov

$$a/b,$$

kjer sta  $a$  in  $b$  poljubni celi števili in je  $b \neq 0$ , je definicija enakosti dveh ulomkov

$$a/b = c/d \Leftrightarrow ad = bc$$

očitno ekvivalenčna relacija. Vsak ekvivalenčni razred glede na to relacijo družijo vse med seboj enake ulomke in predstavlja tedaj ustrezno *racionalno število*. Prirejena faktorska množica je *množica racionalnih števil*.

### 2. Kongruence.

V množici *celih števil* je relacija *kongruence po modulu*  $m$ , kjer je  $m > 0$  poljubno pozitivno celo število,

$$a \equiv b \pmod{m} \Leftrightarrow m \text{ deli } a - b,$$

ekvivalenčna relacija.

Ekvivalenčni razredi so v tem primeru *razredi ostankov* po modulu  $m$ . V vsakem ekvivalenčnem razredu so vsa tista števila, ki dajo pri deljenju z  $m$  isti ostanek.

Očitno je takih razredov natanko  $m$ . Te razrede imenujemo *cela števila po modulu*  $m$ . Faktorska množica je množica celih števil po modulu  $m$ .

### 3. Vzporednost premic.

V množici *vseh premic* je relacija "vzporeden" ekvivalenčna relacija. V vsakem ekvivalenčnem razredu so torej vse premice, ki so med seboj vzporedne, in predstavljajo potemtakem določeno *smer*. Faktorska množica je tukaj *množica vseh smeri*.

### 3.4 FUNKCIJE

*Funkcija je osrednji pojem klasične in moderne matematike. Od 18. stoletja naprej je pojem funkcije postajal vse bolj precizen in splošen. Definicijo funkcije, kot jo poznamo danes, sta uvedla Cauchy in Riemann:*

Za dani množici  $A$  in  $B$  je *funkcija iz  $A$  v  $B$*  predpis, ki vsakemu elementu množice  $A$  priredi natanko določen element množice  $B$ . Oznaka:  $f : A \rightarrow B$ .

Da pa se izognemo dvomu, kaj je mišljeno z besedo "predpis", funkcije lahko definiramo kot posebne vrste relacij.

Binarna relacija  $R$  je *enolična*, če velja:

$$(x, y) \in R \wedge (x, z) \in R \Rightarrow y = z$$

*Parcialna funkcija* je enolična binarna relacija. Parcialne funkcije navadno označujemo s črkami  $f, g, h, \dots$

*Funkcija, ki preslika množico  $A$  v množico  $B$  (ali krašje: funkcija iz  $A$  v  $B$ ), je taka parcialna funkcija  $f$ , da velja*

$$\mathcal{D}f = A \quad \text{in} \quad (x, y) \in f \Rightarrow x \in A \wedge y \in B.$$

Oznaka:  $f : A \rightarrow B$ .

Funkcijam pravimo tudi *preslikave, upodobitve, transformacije*. Množico vseh funkcij iz  $A$  v  $B$  označimo z  $B^A$ .

Pišemo

$$y = f(x) \Leftrightarrow (x, y) \in f.$$

$$f = \{(x, y) ; x \in A \wedge y = f(x) \in B\}.$$

$x \in A$ : neodvisna spremenljivka, original, argument

$y (= f(x))$ : odvisna spremenljivka, slika elementa  $x$ .

V uporabi sta tudi oznaki

$x \mapsto f(x)$  "x se preslika v  $f(x)$ ",

$A \xrightarrow{f} B$  "f preslika  $A$  v  $B$ ".

**Zgledi funkcij:**

- $A = \{1, 2, 3\}, B = \{2, 4, 6\}$

$$f = \{(1, 2), (2, 4), (3, 4)\}$$

- $A = \{\text{točke na površju planeta Zemlja}\}, B = \mathbb{R},$

$$f(x) = \text{temperatura v } ^\circ\text{C v kraju } x \text{ dne 1. 1. 2015 ob 6:00 po lokalnem času}$$

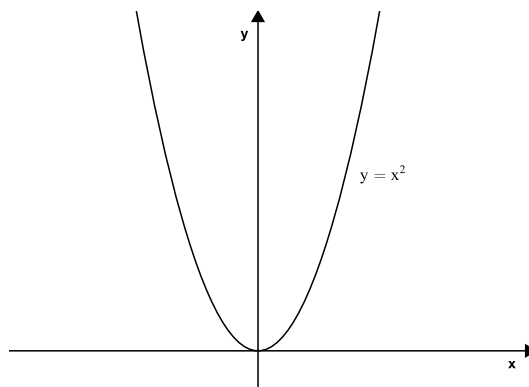
- $A = \{\text{ljudje, živeči na Zemlji ob času } T\}, B = \mathbb{N},$

$$f(x) = \text{starost (v sekundah) osebe } x \text{ v času } T.$$

Množici  $\{(x, y) ; x \in A \wedge y = f(x)\}$  včasih pravimo tudi *graf funkcije*.

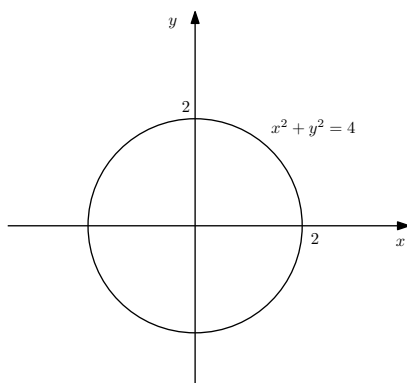
**Upodobitve funkcij.** V primeru, ko je  $A \subseteq \mathbb{R}$  in  $B = \mathbb{R}$ , lahko graf funkcije upodobimo kot množico točk v ravnini.

**Zgled:**  $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^2$ .



Na enak način lahko upodobimo tudi *relacije* na množici  $S = \mathbb{R}$ :

Naj bo  $xRy \Leftrightarrow x^2 + y^2 = 4$ . Tedaj relacijo  $R$  predstavlja krožnica z radijem 2 in s središčem v koordinatnem izhodišču.



Naj bo  $f : A \rightarrow B$ . Domena funkcije  $f$ :

$$\mathcal{D}f = \{x ; (\exists y)((x, y) \in f)\} = A$$

Zaloga vrednosti funkcije  $f$ :

$$\mathcal{Z}f = \{y ; y \in B \wedge (\exists x)(x \in A \wedge (x, y) \in f)\} \subseteq B.$$

Množici  $B$  pravimo *kodomena* funkcije  $f$ .

**Zgled:** Naj bo  $f = \{(1, 2), (2, 4), (3, 4)\}$ ,  $A = \{1, 2, 3\}$ ,  $B = \{2, 4, 6\}$ .

Tedaj je  $\mathcal{D}f = \{1, 2, 3\}$ ,  $\mathcal{Z}f = \{2, 4\}$ . ▲

Pri analizi ste obravnavali tudi realne funkcije, ki jih običajno podamo kar s predpisom  $f(x)$ , ne da bi navajali domeno in kodomeno. Za domeno v tem primeru vzamemo množico  $\{x \in \mathbb{R}; f(x) \in \mathbb{R}\}$ , ki ji pravimo *(naravno) definicijsko območje* funkcije  $f$ .

V splošnem je  $\mathcal{Z}f \subseteq B$ . Če je  $\mathcal{Z}f = B$ , pravimo, da je  $f$  *surjektivna* funkcija. V tem primeru pravimo, da  $f$  preslika množico  $A$  na množico  $B$ .

**Zgled:**  $A = \{1, 2, 3\}$ ,  $B = \{2, 4, 6\}$ .  $f = \{(1, 2), (2, 4), (3, 4)\}$  ni surjektivna.  $g : A \rightarrow B$ ,  $g = \{(1, 2), (2, 6), (3, 4)\}$ , pa je.

Definicija funkcije dopušča, da ima več originalov isto  $f$ -sliko. V skrajnem primeru preslika  $f$  vse elemente množice  $A$  v isti element množice  $B$ . Tako funkcijo imenujemo *konstanta*.

Drugo skrajnost (ko imata dva različna originala vselej različni sliki) pa opisuje naslednja definicija:

$$f \text{ je injektivna} \Leftrightarrow (\forall y)(y \in Zf \Rightarrow (\exists! x)(x \in A \wedge f(x) = y))$$

$$\Leftrightarrow (\forall x)(\forall y)(f(x) = f(y) \Rightarrow x = y)$$

**Zgled:**  $f = \{(1, 2), (2, 4), (3, 4)\}$  ni injektivna.  $g = \{(1, 2), (2, 6), (3, 4)\}$  pa je.

Naj bo  $U \subseteq A$ . Tedaj pišemo:

$$f(U) = \{y ; y \in B \wedge (\exists x)(x \in U \wedge f(x) = y)\}$$

$f(U)$  – slika podmnožice  $U$  pri preslikavi  $f$

**Zgled:**  $f = \{(1, 2), (2, 4), (3, 4)\}$ .  $U = \{2, 3\}$ .  $f(U) = \{f(2), f(3)\} = \{4\}$ .

Očitno je:

- $f(\emptyset) = \emptyset$ ,  $f(A) = Zf$ .
- $U \subseteq V \Rightarrow f(U) \subseteq f(V)$ .

Slike se takole obnašajo glede na unije in preseke:

- $f(U \cup V) = f(U) \cup f(V)$ ,
- $f(U \cap V) \subseteq f(U) \cap f(V)$ .

**Domača naloga:** Dokažite zgornji dve lastnosti.

### 3.5 INVERZNA RELACIJA, PRASLIKE

**Inverzna relacija:**

$$f^{-1} = \{(y, x) ; f(x) = y\}.$$

$f^{-1}$  ni nujno parcialna funkcija!

**Zgled:**  $f = \{(1, 2), (2, 4), (3, 4)\}$ .  $f^{-1} = \{(2, 1), (4, 2), (4, 3)\}$  - ni parcialna funkcija.

Praslika elementa  $y$ :

$$f^{-1}(y) = \{x ; x \in A \wedge f(x) = y\}.$$

Naj bo  $E \subseteq B$ . Praslika podmnožice  $E$  (pri preslikavi  $f$ ):

$$f^{-1}(E) = \{x ; x \in A \wedge f(x) \in E\}$$

**Zgled:**  $f = \{(1,2), (2,4), (3,4)\}$ .  $f^{-1}(2) = \{1\}$ ,  $f^{-1}(4) = \{2,3\}$ ,  $f^{-1}(\{2,4\}) = \{1,2,3\}$

Očitno:

- $f^{-1}(zf) = A$

Velja še:

- $E \subseteq F \Rightarrow f^{-1}(E) \subseteq f^{-1}(F)$

Praslike so v dobrih odnosih z unijami, preseki in razlikami:

- $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$
- $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$
- $f^{-1}(E \setminus F) = f^{-1}(E) \setminus f^{-1}(F)$

**Dokaz lastnosti**  $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$ :

$$\begin{aligned} x \in f^{-1}(E \cap F) &\Leftrightarrow f(x) \in E \cap F \Leftrightarrow f(x) \in E \wedge f(x) \in F \Leftrightarrow \\ &\Leftrightarrow x \in f^{-1}(E) \wedge x \in f^{-1}(F) \Leftrightarrow x \in f^{-1}(E) \cap f^{-1}(F) \end{aligned}$$

□

**Domača naloga:** Dokažite še drugi dve lastnosti.

Podobno se lahko prepričamo, da velja:

- za vsak  $U \subseteq A$  je

$$U \subseteq f^{-1}(f(U))$$



- za vsak  $E \subseteq B$  je

$$f(f^{-1}(E)) \subseteq E$$

Naj bo  $f : A \rightarrow B$ . Kdaj je inverzna relacija  $f^{-1}$  (parcialna) funkcija?

$f^{-1}$  je funkcija iz  $\mathcal{Z}f$  v  $A \Leftrightarrow f$  je injektivna.

(Res: da bo  $f^{-1}$  parcialna funkcija, ne smeta obstajati dva različna urejena para v  $f^{-1}$ , ki bi imela isto prvo koordinato  $\Leftrightarrow$  ne smeta obstajati dva različna urejena para v  $f$ , ki bi imela isto drugo koordinato, tj.  $f$  je injektivna.)

Če je torej  $f^{-1}$  funkcija, potem za vsak element  $y \in \mathcal{Z}f$  obstaja natanko določen  $x \in \mathcal{D}f$ , da velja  $f^{-1}(y) = x$ . Velja zveza

$$f^{-1}(y) = x \Leftrightarrow f(x) = y.$$

Torej:

$$f^{-1}(f(x)) = x$$

in

$$f(f^{-1}(y)) = y.$$

Posebno zanimiv primer nastane, ko je funkcija  $f$  ne samo injektivna, ampak tudi surjektivna. V tem primeru rečemo, da je funkcija  $f$  *bijektivna*.

Če je  $f$  bijektivna, je  $\mathcal{Z}f = B$  in  $f^{-1}$  je funkcija, ki preslika  $B$  v  $A$ .

### 3.6 KOMPOZITUM FUNKCIJ

Naj bosta  $f$  in  $g$  parcialni funkciji. Tedaj velja

$$\begin{aligned} g \circ f &= \{(x, z); (\exists y)((x, y) \in f \wedge (y, z) \in g)\} \\ &= \{(x, z); (\exists y)(f(x) = y \wedge g(y) = z)\}. \end{aligned}$$

Torej, če je  $\mathcal{Z}f \cap \mathcal{D}g = \emptyset$ , potem je  $g \circ f = \emptyset$ . Ta primer ni posebej zanimiv, zato po navadi zahtevamo:  $\mathcal{Z}f \subseteq \mathcal{D}g$ , torej obstajajo take množice  $A, B, C$ , da velja

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

Zdaj pa velja:

$$g \circ f = \{(x, z) ; z = g(f(x))\}$$

Relacija  $g \circ f$  je prav tako funkcija (ki preslika  $A$  v  $C$ ):  $(g \circ f)(x) = g(f(x))$ .

**Zgled:**  $f = \{(1, 2), (2, 4), (3, 4)\}$ ,  $g = \{(2, 3), (4, 5)\}$  (Opazimo, da je  $\mathcal{D}g = \mathbb{Z}f$ .)  $g \circ f = \{(1, 3), (2, 5), (3, 5)\}$

Tako kot za kompozitume binarnih relacij tudi za kompozitume funkcij velja

**Asociativnost:**

Če je

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D,$$

potem je

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

### 3.6.1 Zožitve in razširitve

Kdaj sta dve parcialni funkciji  $f$  in  $g$  enaki?

Po definiciji enakosti množic le tedaj, kadar imata za elemente iste urejene pare. To pa je res natanko tedaj, ko velja dvoje:

- $\mathcal{D}f = \mathcal{D}g$
- za vsak element  $x$  te skupne domene velja  $f(x) = g(x)$ .

Poseben način, kako moremo spremeniti funkcijo:

**Zožitev:** Dana je funkcija  $f : A \rightarrow B$  in podmnožica domene  $U \subseteq A$ .

*Zožitev* ali *restrikcija* funkcije  $f$  na množico  $U$  je funkcija  $g$ , ki ima za svojo domeno množico  $U$  in za vse  $x \in U$  velja  $g(x) = f(x)$ . Oznaka:

$$g = f|_U$$

**Zgled:**  $f = \{(1, 2), (2, 4), (3, 4)\}$ ,  $A = \{1, 2, 3\}$ ,  $U = \{1, 2\}$ .  $f|_U = \{(1, 2), (2, 4)\}$

Če je funkcija  $g$  zožitev funkcije  $f$ , pravimo, da je funkcija  $f$  *razširitev* funkcije  $g$ .

### 3.7 KANONIČNA DEKOMPOZICIJA FUNKCIJE

Dana je funkcija  $f : A \rightarrow B$ . Vpeljimo na množici  $A$  naslednjo relacijo  $R$ :

$$xRy \Leftrightarrow f(x) = f(y).$$

Očitno je  $R$  ekvivalenčna relacija:

- za vsak  $x \in A$  je  $xRx$ ,
- $xRy \Rightarrow f(x) = f(y) \Rightarrow f(y) = f(x) \Rightarrow yRx$ ,
- $xRy \wedge yRz \Rightarrow f(x) = f(y) \wedge f(y) = f(z) \Rightarrow f(x) = f(z) \Rightarrow xRz$ .

Zdaj pa napravimo faktorsko množico  $A/R$  (množico vseh ekvivalenčnih razredov).

Preslikajmo najprej množico  $A$  na množico  $A/R$ :

$$p : A \rightarrow A/R$$

$$p(a) = R[a]$$

Preslikava  $p$  je očitno surjektivna. Imenujemo jo *naravna preslikava*.

Zdaj pa preslikajmo še množico  $A/R$  v množico  $B$  s takšno preslikavo  $g$ , da bo funkcija  $f$  kompozitum funkcij  $p$  in  $g$ ,  $f = g \circ p$ :

$$g : A/R \rightarrow B$$

$$g(u) = f(x),$$

kjer je  $x$  poljuben predstavnik razreda  $u$  (torej  $x \in u$ ).

- Preslikava  $g$  je dobro definirana (vrednost  $g(u)$  je neodvisna od izbire predstavnika razreda  $u$ ):

$$x \in u \wedge y \in u \Rightarrow xRy \Rightarrow f(x) = f(y).$$

- Preslikava  $g$  je injektivna:

$$g(u) = g(v) \wedge g(u) = f(x) \wedge g(v) = f(y) \Rightarrow f(x) = f(y) \Rightarrow xRy \Rightarrow u = v.$$

- Po definicijah funkcij  $g$  in  $p$  je  $f = g \circ p$ :

Naj bo  $x \in A$ .

$$(g \circ p)(x) = g(p(x)) = g(R[x]) = f(x).$$

Preslikavo  $f$  lahko razstavimo takole:

$$\begin{array}{ccccc} A & \xrightarrow[p_{\text{surj.}}]{p} & A/R & \xrightarrow[g_{\text{inj.}}]{g} & B \\ & \searrow & & \nearrow & \\ & & f & & \end{array}$$

To dekompozicijo lahko še malce izpopolnimo, tako da vpeljemo preslikavo  $h$ , ki je podana z istim predpisom kot  $g$ , le da slika v množico  $\mathbb{Z}f$ . Preslikava  $h$  je potem bijektivna:

$$h : A/R \rightarrow \mathbb{Z}f$$

$$h(u) = g(u).$$

Množico  $\mathbb{Z}f$  pa nazadnje preslikamo v množico  $B$  z *identično preslikavo*  $i$ , ki pribije vsak element:

$$i : \mathbb{Z}f \rightarrow B$$

$$i(y) = y.$$

Očitno je, da za vse  $x \in A$  velja

$$i(h(p(x))) = h(p(x)) = g(p(x)) = f(x).$$

Torej je

$$f = i \circ h \circ p.$$

Tako dobimo *kanonično dekompozicijo* funkcije  $f$ :

$$\begin{array}{ccccccc} A & \xrightarrow[p_{\text{surj.}}]{p} & A/R & \xrightarrow[bij.]{h} & \text{Im } f & \xrightarrow[i_{\text{inj. (identična)}}]{i} & B \\ & \searrow & & & & \nearrow & \\ & & & & f & & \end{array}$$

**Zgled:**  $A = \{1, 2, 3\}$ ,  $B = \{2, 4, 6\}$ ,  $f = \{(1, 2), (2, 4), (3, 4)\}$

(tj.,  $f(1) = 2$ ,  $f(2) = f(3) = 4$ )

Ekvivalenčna relacija:  $R = \{(1, 1), (2, 2), (3, 3), (2, 3), (3, 2)\}$

Faktorska množica:  $A/R = \{\{1\}, \{2, 3\}\}$

$\mathbb{Z}.f = \{2, 4\}$

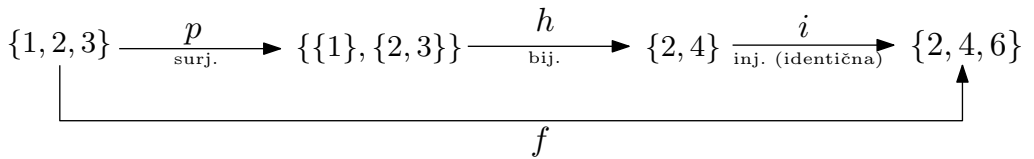
Naravna preslikava  $p$ :  $p(1) = \{1\}$ ,  $p(2) = p(3) = \{2, 3\}$ .

Preslikava  $g : \{\{1\}, \{2, 3\}\} \rightarrow \{2, 4, 6\}$ :

$g(\{1\}) = f(1) = 2$ ,  $g(\{2, 3\}) = f(2) = f(3) = 4$ .

Preslikava  $h : \{\{1\}, \{2, 3\}\} \rightarrow \{2, 4\}$ :  $h(\{1\}) = g(\{1\}) = 2$ ,  $h(\{2, 3\}) = g(\{2, 3\}) = 4$ .

Identična preslikava  $i : \{2, 4\} \rightarrow \{2, 4, 6\}$ :  $i(2) = 2$ ,  $i(4) = 4$ .



### 3.7.1 Strukture urejenosti

*Poleg ekvivalenčnih relacij in funkcij so v matematiki posebno pomembne tudi relacije, ki ustvarjajo med elementi dane množice red ali urejenost. Red je lahko bolj ali manj strog, zato imamo opravka z različnimi strukturami urejenosti. Kot bomo videli, te strukture urejenosti tvorijo hierarhijo in so tudi same po svoje urejene.*

Začnimo pri najsplošnejših strukturah.

Dana je univerzalna množica  $S$  in relacija  $R$  na  $S$ .

Najsplošnejšo strukturo dobimo, če zahtevamo le tranzitivnost. To ni posebej zanimiva struktura: ničelna relacija, identična relacija in univerzalna relacija so vse tranzitivne!

$R$  navidezno ureja  $S \Leftrightarrow R$  je tranzitivna in refleksivna.

Beseda "navidezno" se nanaša na našo intuitivno predstavo o urejenosti, saj je že univerzalna relacija  $S \times S$  navidezna urejenost, pa čeprav ničesar ne ureja!

$R$  delno ureja  $S \Leftrightarrow R$  je tranzitivna, refleksivna in antisimetrična.

Naj  $R$  delno ureja  $S$ .

$xRy$ : " $x$  je vsebovan v  $y$ " ali

" $x$  je manjši ali enak  $y$ " ali

" $y$  vsebuje  $x$ " ali

" $y$  je večji ali enak  $x$ ".

**Zgled za relacijo delne urejenosti:** relacija inkluzije " $\subseteq$ ", definirana na poljubni družini podmnožic dane univerzalne množice  $\mathcal{U}$ .

Lahko se zgodi, da množici  $A$  in  $B$  nista primerljivi glede na relacijo inkluzije!

To velja tudi v splošnem. Od tod tudi ime "delna urejenost".

**Zgled:** Relacija deljivosti na množici pozitivnih naravnih števil.

Tudi to je delna urejenost. Lahko se zgodi, da dve števili nista primerljivi glede na to relacijo (npr. 5 in 7).

Tudi relacija " $\leq$ " na množici realnih števil izpolnjuje vse pogoje za delno urejenost.

Velja pa še več: ta relacija je tudi strogo sovisna, saj za vsaki dve realni števili  $x$  in  $y$  velja  $x \leq y$  ali  $y \leq x$ .

$R$  popolno ali linearno ureja  $S \Leftrightarrow R$  je tranzitivna, refleksivna, antisimetrična in strogo sovisna.

Toda:  $R$  je strogo sovisna  $\Rightarrow R$  je refleksivna!

(če v pogoju  $(\forall x)(\forall y)(xRy \vee yRx)$  vzamemo  $y = x$ , dobimo  $(\forall x)(xRx)$ ).

Torej:

$R$  popolno (linearno) ureja  $S \Leftrightarrow R$  je tranzitivna, antisimetrična in strogo sovisna.

---

Relaciji stroge inkluzije " $\subset$ " in stroge neenakosti " $<$ ":

- obe sta tranzitivni, a irefleksivni
- obe sta asimetrični
- relacija stroge inkluzije določa le *delno* urejenost (obstajajo namreč pari neprimerljivih množic)
- relacija stroge neenakosti pa določa popoln red: je *sovisna*, poljubni dve *različni* realni števili sta med seboj primerljivi glede na  $<$ .

Vsaka asimetrična relacija je tudi irefleksivna. Torej lahko definiramo  $R$  *strogo delno ureja*  $S \Leftrightarrow R$  je tranzitivna in asimetrična.

Analogno definiramo:

$R$  *strogo linearno ureja*  $S \Leftrightarrow R$  je tranzitivna, asimetrična in sovisna.

Naj  $R$  strogo delno ureja  $S$ .

$xRy$ : "x je pod y" ali

"x je manjši od y" ali

"y je nad x" ali

"y je večji od x".

To terminologijo uporabljamo tudi za primer, ko je  $xRy$ , kjer je relacija  $R$  delna urejenost in je  $x \neq y$ .

---

Oglejmo si še eno relacijo urejenosti: **šibka urejenost**.

Njen model je na primer relacija "vsaj tako velik kot" v množici vseh ljudi.

Je tranzitivna, strogo sovisna (torej tudi refleksivna).

Ni pa antisimetrična!

Če je  $x$  "vsaj tako velik kot"  $y$  in  $y$  "vsaj tako velik kot"  $x$ , potem smemo sklepati le, da sta  $x$  in  $y$  enako velika, nikakor pa ni nujno, da je  $x = y$ .

$R$  *šibko ureja*  $S \Leftrightarrow R$  je tranzitivna in strogo sovisna.

---



Doslej smo našeli 7 različnih struktur urejenosti. Definirajmo v množici, ki ima za elemente teh 7 struktur, relacijo "je poseben primer".

$x$  je poseben primer  $y$ , če ima vsaka relacija  $R_x$ , ki določa strukturo  $x$ , tudi vse lastnosti strukture  $y$ .

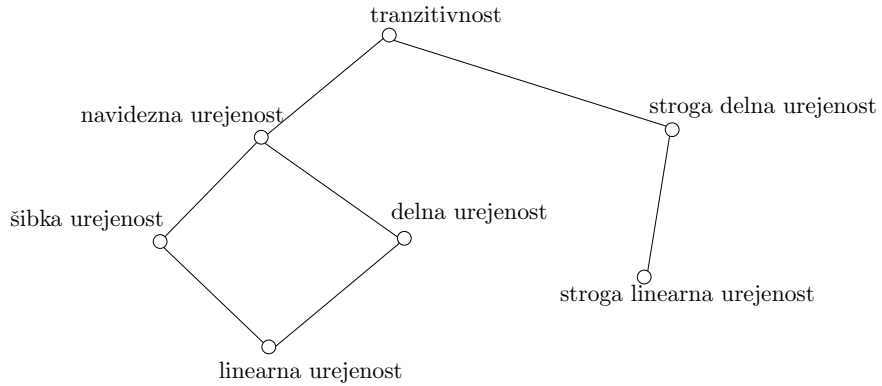
- Primer:

Linearna urejenost je poseben primer delne urejenosti.

Stroga linearna urejenost je poseben primer stroge delne urejenosti.

Relacija "je poseben primer" je tranzitivna, refleksivna in antisimetrična, torej določa delno urejenost med temi strukturami.

Delno urejenost pa moremo prikazati s t.i. *Hassejevim diagramom*:

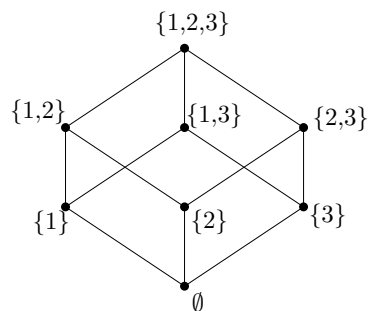


Hassejev diagram

$R$  - relacija, ki delno ali strogo delno ureja  $S$

$xRy \Leftrightarrow$  od  $x$  do  $y$  lahko pridem od spodaj navzgor po črtah v diagramu

**Zgled:**  $A = \{1, 2, 3\}$ ,  $S = \mathcal{P}(A)$ ,  $R$ : stroga inkluzija



**Primer:** Hassejev diagram množice s 6 elementi, ki je linearno ali strogo linearno urejena



## MREŽA

Struktura *mreže* je delna urejenost s posebej lepimi lastnostmi. Da bi jo definirali, potrebujemo nekaj definicij.

Množica  $S$  naj bo delno urejena z relacijo  $R$  in naj bo  $U \subseteq S$ .

Če obstaja tak  $a \in S$ , da za vsak  $x \in U$  velja  $aRx$ , potem je  $a$  *R-spodnja meja* za  $U$ .

Če obstaja tak  $b \in S$ , da je  $xRb$  za vsak  $x \in U$ , potem je  $b$  *R-zgornja meja* za  $U$ .

Če ima  $U$  kakšno *R-spodnjo* mejo, potem je  $U$  *R-navzdol omejena*.

Če ima  $U$  kakšno *R-zgornjo* mejo, potem je  $U$  *R-navzgor omejena*.

Če ima  $U$  kakšno *R-zgornjo* mejo in kakšno *R-spodnjo* mejo, potem je  $U$  *R-omejena*.

$a \in S$  je *R-največja spodnja meja* (*R-infimum*) podmnožice  $U \Leftrightarrow a$  je *R-spodnja meja* in za vsako *R-spodnjo* mejo  $x$  za  $U$  velja  $xRa$ .

Oznaka:  $a = R\text{-inf } U$ .

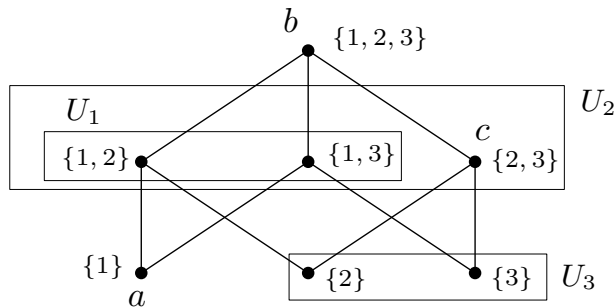
$b \in S$  je *R-najmanjša zgornja meja* (*R-supremum*) podmnožice  $U \Leftrightarrow b$  je *R-zgornja meja* in za vsako *R-zgornjo* mejo  $x$  za  $U$  velja  $bRx$ .

Oznaka:  $b = R\text{-sup } U$ .

**Zgled:** Vzemimo množico  $S = \mathcal{P}(\{1, 2, 3\}) \setminus \{\emptyset\}$ , delno urejeno glede na relacijo inkluzije,  $R = \subseteq$ .

Za podmnožice  $U_1 = \{\{1, 2\}, \{1, 3\}\}$ ,  $U_2 = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$  in  $U_3 = \{\{2\}, \{3\}\}$  in elemente  $a = \{1\}$ ,  $b = \{1, 2, 3\}$  in  $c = \{2, 3\}$  velja:

- Množica  $U_1$  ima eno samo spodnjo mejo,  $a$ , in eno samo zgornjo mejo,  $b$ . Posledično je  $\subseteq\text{-inf } U_1 = a$  in  $\subseteq\text{-sup } U_1 = b$ .
- Množici  $U_2$  in  $U_3$  nimata nobene spodnje meje, torej nista navzdol omejeni (in posledično nimata infimuma).
- Množica  $U_2$  ima eno samo zgornjo mejo,  $b$ , zato je  $\subseteq\text{-sup } U_2 = b$ .
- Množica  $U_3$  ima dve zgornji meji,  $b$  in  $c$ , in  $\subseteq\text{-sup } U_3 = c$ .



Zaradi antisimetričnosti ima vsak  $U \subseteq S$  kvečjemu en  $R\text{-sup}$  in kvečjemu en  $R\text{-inf}$ .

Lahko ju pa nima (tudi če je omejena)!

**Zgled:**

$S = \mathbb{Q}$ ,  $R = \leq$

$$U = \{x ; x \in \mathbb{Q} \wedge 0 \leq x \wedge x^2 \leq 2\}$$

Množica  $U$  je navzdol in navzgor omejena!

$\inf U = 0$ ,  $\sup U$  pa ne obstaja!

$$V = \{x ; x \in \mathbb{Q} \wedge 0 \leq x \wedge 2 \leq x^2 \leq 5\}$$

Množica  $V$  je omejena, ne obstajata pa niti  $\inf V$  niti  $\sup V$ . ▲

**Definicija.** Množica  $S$  ima strukturo mreže glede na relacijo  $R \Leftrightarrow R$  delno ureja  $S$  in vsaka dvoelementna podmnožica  $X \subseteq S$  ima tako  $R$ -supremum kot  $R$ -infimum.

Opomba: Strukturo mreže je moč definirati tudi povsem algebraično.

### Zgledi mrež:

#### 1. $A$ - množica

$\mathcal{P}(A)$  – potenčna množica

$\mathcal{P}(A)$  je mreža glede na  $R = \subseteq$ :

- delna urejenost ✓
- $E, F \subseteq A, E \neq F$ :  
 $\inf\{E, F\} = E \cap F$   
 $\sup\{E, F\} = E \cup F$

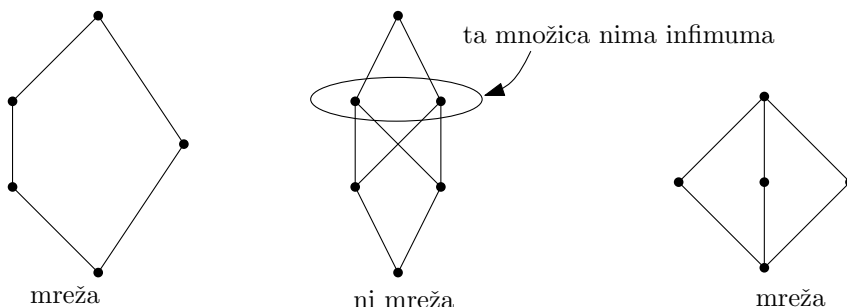
#### 2. Naj $R$ linearno ureja $S$ .

- delna urejenost ✓
- $a, b \in S, a \neq b \Rightarrow aRb$  ali  $bRa$   
 $aRb \Rightarrow R\text{-}\inf\{a, b\} = a, R\text{-}\sup\{a, b\} = b.$   
 $bRa \Rightarrow R\text{-}\inf\{a, b\} = b, R\text{-}\sup\{a, b\} = a.$

#### 3. $S = \mathbb{N} \setminus \{0\}, R = |$ (relacija deljivosti).

- delna urejenost ✓
- $x, y \in \mathbb{N} \setminus \{0\}, x \neq y$   
 $\inf\{x, y\} = \text{največji skupni delitelj } x \text{ in } y$   
 $\sup\{x, y\} = \text{najmanjši skupni večkratnik } x \text{ in } y$

Še nekaj zgledov s Hassejevimi diagrami:



V mreži ima tudi vsaka končna neprazna podmnožica množice  $S$  infimum in supremum!

**Trditev.** Naj ima  $S$  strukturo mreže glede na  $R$ . Tedaj za vsake tri elemente  $a_1, a_2, a_3 \in S$  velja

$$R\text{-inf}\{a_1, a_2, a_3\} = R\text{-inf}\{R\text{-inf}\{a_1, a_2\}, a_3\}.$$

*Dokaz.* Naj bo  $a = R\text{-inf}\{R\text{-inf}\{a_1, a_2\}, a_3\}$ .

$a$  je spodnja meja množice  $\{a_1, a_2, a_3\}$ :

$aRa_3$ , saj je  $a$  spodnja meja množice  $\{R\text{-inf}\{a_1, a_2\}, a_3\}$ .

Podobno je  $aR(R\text{-inf}\{a_1, a_2\})$ , ker pa je  $(R\text{-inf}\{a_1, a_2\})Ra_1$  in je  $R$  tranzitivna, je  $aRa_1$ . Podobno je tudi  $aRa_2$ .

$a$  je največja spodnja meja množice  $\{a_1, a_2, a_3\}$ :

Naj bo  $x$  poljubna spodnja meja množice  $\{a_1, a_2, a_3\}$ . Torej je  $xRa_1, xRa_2$  in  $xRa_3$ .

$$xRa_1, xRa_2 \Rightarrow xR(R\text{-inf}\{a_1, a_2\}).$$

$$xR(R\text{-inf}\{a_1, a_2\}) \wedge xRa_3 \Rightarrow xRa.$$

□

Podobno za supremum. Postopek lahko ponavljamo in pokažemo obstoj infimuma in supremuma poljubne končne neprazne množice.

**Posledica.** Če je  $S$  mreža glede na  $R$ , ima vsaka končna neprazna množica  $R\text{-inf}$  in  $R\text{-sup}$ .

Obstoj infimuma in supremuma pa moremo zahtevati tudi za vse neprazne podmnožice (ne le za končne):

**Definicija.** Množica  $S$  ima strukturo polne mreže glede na relacijo  $R \Leftrightarrow R$  delno ureja množico  $S$  in vsaka neprazna podmnožica  $X$  množice  $S$  ima  $R$ -inf in  $R$ -sup.

Očitno je vsaka polna mreža tudi mreža glede na isto relacijo  $R$ . Vsaka končna mreža pa je tudi polna mreža.

### Zgled:

$A$  – poljubna množica

$\mathcal{P}(A)$  je polna mreža za  $\subseteq$ :

Če je  $\mathcal{A}$  neprazna družina podmnožic množice  $A$ , potem je

$$(\subseteq)\text{-inf } \mathcal{A} = \cap \mathcal{A}$$

in

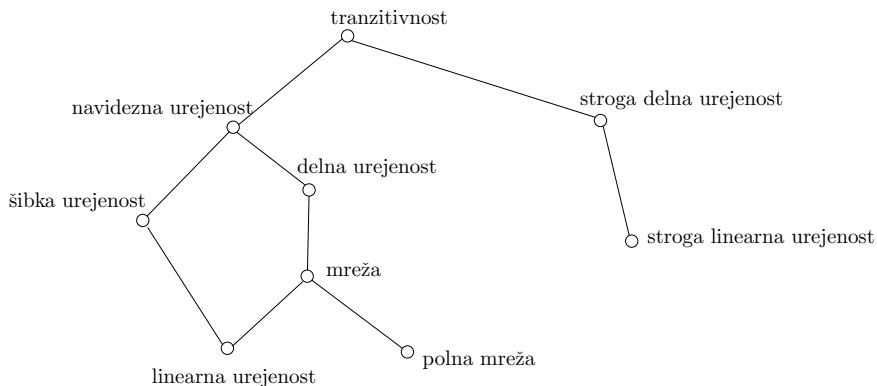
$$(\subseteq)\text{-sup } \mathcal{A} = \cup \mathcal{A}.$$



Množica realnih števil  $\mathbb{R}$  ni polna mreža glede na  $\leq$ : cela množica  $\mathbb{R}$  namreč ni omejena! (nima ne supremuma ne infimuma)

Množico realnih števil lahko dopolnimo do polne mreže, tako da ji dodamo elementa  $\infty$  in  $-\infty$ , s pravilom  $x \leq \infty$  za vse  $x \in \mathbb{R}$  in  $-\infty \leq x$  za vse  $x \in \mathbb{R}$ .

Hassejev diagram 9 struktur urejenosti, ki smo jih spoznali:



$x$  je pod  $y \Leftrightarrow x$  je poseben primer  $y$ .





# Dodatek





## DODATNA POGLAVJA IZ TEORIJE MNOŽIC

### A.1 AKSIOMI TEORIJE MNOŽIC (PO EDERTONU)

1. Aksiom ekstenzionalnosti (enakost množic)

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

2. Aksiom o prazni množici

$$\exists B \forall x (x \notin B)$$

3. Aksiom o paru

$$\forall u \forall v \exists B \forall x [x \in B \Leftrightarrow x = u \text{ ali } x = v]$$

4. Aksiom o uniji

$$\forall A \exists B \forall x [x \in B \Leftrightarrow (\exists b \in A) x \in b]$$

5. Aksiom o potenčni množici

$$\forall a \exists B \forall x [x \in B \Leftrightarrow x \subseteq a]$$

6. Aksiomi o podmnožicah

Za vsako formulo  $\varphi$  o množicah, ki ne vsebuje črke  $B$ , je naslednji izraz aksiom:

$$\forall t_1 \dots \forall t_k \forall c \exists B \forall x [x \in B \Leftrightarrow x \in c \wedge \varphi]$$

7. Aksiom neskončnosti

$$\exists A [\emptyset \in A \wedge (\forall a \in A) a^+ \in A]$$

(Pri tem je  $a^+ = a \cup \{a\}$ .)

## 8. Aksiom izbire

$$(\forall \text{ relacija } R)(\exists \text{ funkcija } F)(F \subseteq R \wedge \mathcal{D}(F) = \mathcal{D}(R))$$

## 9. Aksiomi o zamenjavi

Za vsako formulo  $\varphi(x, y)$ , ki ne vsebuje črke  $B$ , je naslednji izraz aksiom:

$$\begin{aligned} \forall t_1 \dots \forall t_k \forall A [(\forall x \in A) \forall y_1 \forall y_2 (\varphi(x, y_1) \wedge \varphi(x, y_2) \Rightarrow y_1 = y_2) \\ \Rightarrow \exists B \forall y [y \in B \Leftrightarrow (\exists x \in A) \varphi(x, y)]] \end{aligned}$$

## 10. Aksiom regularnosti

$$(\forall A \neq \emptyset) (\exists m \in A) (m \cap A = \emptyset)$$

## A.2 AKSIOMI TEORIJE MNOŽIC (PO DUGUNDJIJU)

1. Aksiom individualnosti:  $(x \in A) \wedge (x = y) \Rightarrow y \in A$
2. Aksiom o formaciji razredov = Aksiom o podmnožicah po Endertonu
3. Aksiom o prazni množici
4. Aksiom o paru
5. Aksiom o uniji
6. Aksiom o potenčni množici
7. Aksiom o zamenjavi: slika vsake preslikave je množica.
8. Aksiomi ("Sifting"): Presek vsake množice z razredom je množica.
9. Aksiom regularnosti
10. Aksiom neskončnosti
11. Aksiom izbire

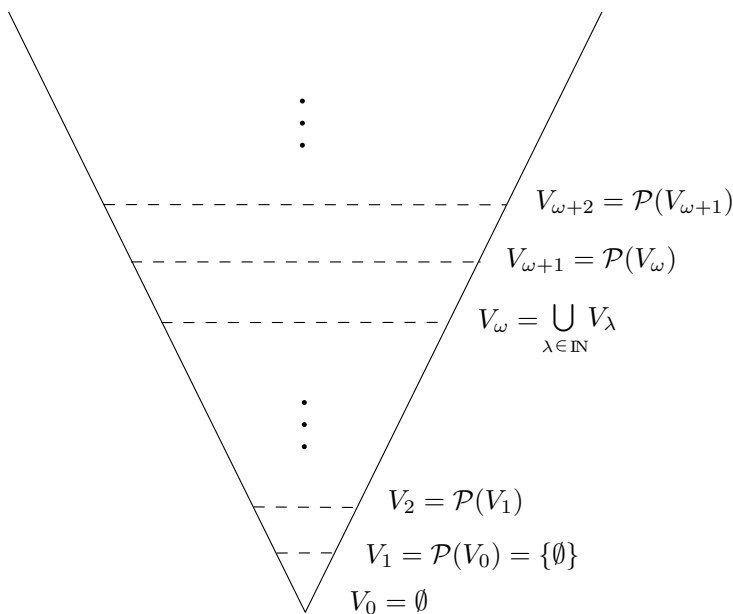
### A.3 NEFORMALNI POGLED NA UNIVERZUM MNOŽIC

Množice lahko obravnavamo bodisi kot **hereditarne množice** (induktivno definirane kot množice, katerih vsi elementi so spet hereditarne množice –  $\emptyset$  je hereditarna množica) ali pa imamo podano še neko množico *atomov*, ki niso množice, so pa lahko elementi množic.

Za abstraktno, matematično obravnavo zadoščajo že hereditarne množice. Te tvorijo t.i. *von Neumannovo hierarhijo množic*.

Na dnu hierarhije je le prazna množica,  $V_0 = \emptyset$ . Če imamo dano množico  $V_i$ , pa je  $V_{i+1} = \mathcal{P}(V_i)$ . Na ta način dobimo  $V_0, V_1, V_2, \dots$

To pa še ni vse. Napravimo unijo vseh množic:  $V_\omega = \bigcup_{\lambda \in \mathbb{N}} V_\lambda$ . In postopek ponovimo:  $V_{\omega+1} = \mathcal{P}(V_\omega)$  itd. Ponavljamo v nedogled:



Slika 2: von Neumannova hierarhija hereditarnih množic

Množice v hierarhiji postanejo zelo hitro nepredstavljivo velike.  $V_0$  ima 1 element,  $V_1$  ima 2 elementa,  $V_2$  ima 4 elemente,  $V_3$  ima  $2^4 = 16$  elementov,  $V_4$  ima  $2^{16} = 65536$  elementov,  $V_5$  pa ima že  $2^{65536}$  elementov, itd.  $V_\omega$  je neskončna množica in vse nad njo prav tako.

**Pomen hiererhije:** Vsaka hereditarna množica se pojavi (kot element) v eni od množic  $V_\lambda$  v zgornji hierarhiji.

Podobno hierarhijo lahko zgradimo za obravnavo množic z atomi. Edina razlika je v tem, da postavimo  $V_0 = A$  (kjer je  $A$  množica atomov) in naslednji element hierarhije tvorimo iz prejšnjega s pravilom  $V_{i+1} = V_i \cup \mathcal{P}(V_i)$ .