1 Matematična logika

Kaj je izjava? *Trdilna izjava*, ki je bodisi pravilna ali pa nepravilna.[1]

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).

1.1 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.
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.

[1] Izjave boste podrobneje obravnavali na uvodnem predavanju pri Analizi I.

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 $A_1, \ldots, A_n$, 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:

$$(A \Rightarrow B) \wedge (B \Rightarrow C) \wedge (\neg A \vee C) \tag{1}$$

	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 $A_1, \ldots, A_n$.

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

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 tavtologija 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 tavtologija 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 tavtologija, je pa protislovje. ▲

Domača naloga:
1. Preštudiraj dodatno gradivo o izjavah, objavljeno na e-učilnici.

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

3. 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:

$$[A \Leftrightarrow (A \wedge \neg B) \vee (\neg A \wedge B)] \wedge [B \Leftrightarrow (A \wedge \neg B) \vee (\neg A \wedge B)]\,. \tag{2}$$

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 vitezih 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 $A_1, \ldots, A_n$, kako konstruirati iz njih sestavljeno izjavo, ki bo imela pri vsakem izmed 2^n določil *vnaprej predpisano logično vrednost?*

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

1.2 Logične ekvivalence

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

Naštejmo najpoglavitnejše logične ekvivalence:

1. $A \Leftrightarrow \neg(\neg A)$, zakon dvakratne negacije
2. $A \wedge B \Leftrightarrow B \wedge A$, $\quad A \vee B \Leftrightarrow B \vee A$, komutativnost konjunkcije in disjunkcije
3. $A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$, $\quad A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$, asociativnostna zakona
4. $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$, $\quad A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$, distributivnostna zakona
5. $A \wedge A \Leftrightarrow A$, $\quad A \vee A \Leftrightarrow A$
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. ▲

1.3 Izbrani obliki izjav

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

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

$$C_1 \wedge \ldots \wedge C_n \,,$$

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:

$$D_1 \vee \cdots \vee D_n \,,$$

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 tavtologije ne! Za tavtologijo 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

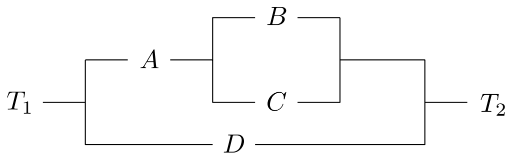
$$(\neg A \lor \neg B \lor C) \land (\neg A \lor B \lor \neg C) \land (\neg A \lor B \lor C) \land (A \lor \neg B \lor C)\,.$$

□

1.4 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).

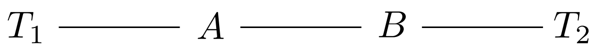


Slika 1: Primer vezja s štirimi stikali

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).

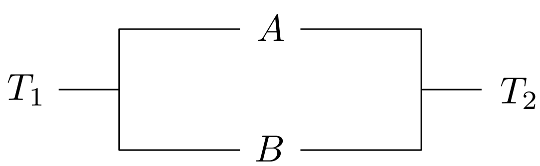
Poglejmo si dve zelo preprosti vezji:

(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

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

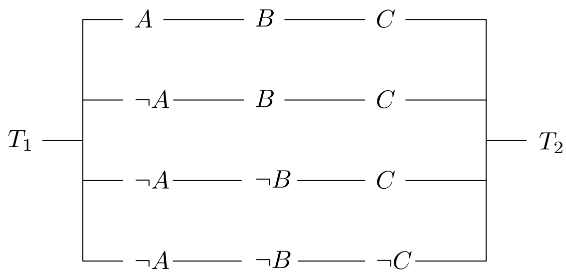
V poglavju 1.2. smo izračunali pravilnostno tabelo te izjave:

	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:

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

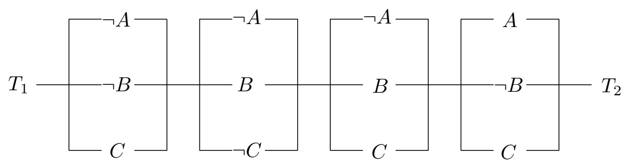
Tej obliki ustreza naslednje vezje:



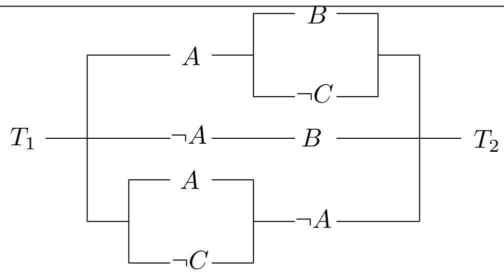
Izbrani konjunktivni obliki

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

pa ustreza vezje



Vidimo, da dani izjavi ustreza več preklopnih 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 preklopno vezje:

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

Prirejena sestavljena izjava, recimo ji D, je:

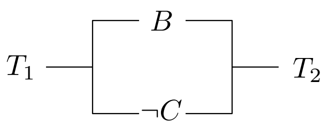
$$(A \wedge B \vee \neg C) \vee (\neg A \wedge B) \vee (A \vee \neg C \wedge \neg A)\,.$$

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

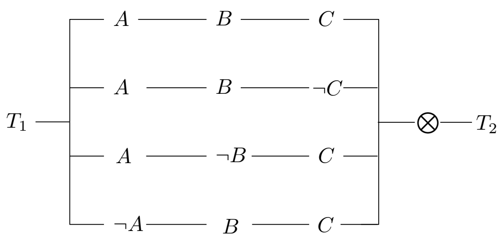
$$(A \wedge B \wedge C) \vee (A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge C)$$

v primeru (b) pa

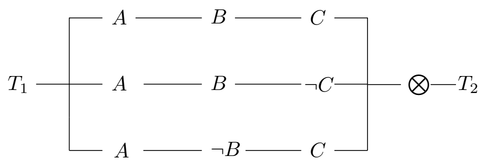
$$(A \wedge B \wedge C) \vee (A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge C)\,.$$

Ustrezni vezji pa sta:

(a)



(b)



▲

Domača naloga: Sestavite vezje, prirejeno izjavi

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

1.5 Logične implikacije

Logična implikacija je tavtologija, pri kateri je glavna povezava implikacija.

Veljajo naslednje resnice o logičnih implikacijah:

1. Če je antecedens tavtologija, mora biti tudi konsekvens tavtologija.
2. Če je konsekvens protislovje, mora biti tudi antecedens protislovje.
3. Če je konsekvens tavtologija, 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 tavtologija.

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 tavtologija. ▲

1.6 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. □

Direktni dokaz implikacije $A \Rightarrow B$
Dokaz:
Predpostavimo A.
$\vdots$
Torej, B.
Sledi $A \Rightarrow B$. □

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. □

Indirektni dokaz implikacije $A \Rightarrow B$
Dokaz:
Predpostavimo $\neg B$.
$\vdots$
Torej, $\neg A$.
Sledi $\neg B \Rightarrow \neg A$.
Posledično $A \Rightarrow B$. □

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
$4m^2 = 2q^2$.
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 $\neg A$.
⋮
Torej, B.
⋮
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 γ kot med stranicama dolžin a in b.

Dokaz.

Iz kosinusnega izreka sledi

$a^2 + b^2 = c^2$ če in samo če $2ab\cos\gamma = 0$
če in samo če $\cos\gamma = 0$
če in samo če $\gamma = 90°$.

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

Če imamo n vmesnih izjav $C_1, \ldots, C_n$, 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. $\square$

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. $\square$

1.7 Množice izjav

Dane so atomarne izjave $A_1, \ldots, A_n$ (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, sestavljene iz $A_1, \ldots, A_n$, 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, $C_1, \ldots, C_4$.

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

C_1 je tavtologija, npr. $A \lor \neg A$.
C_4 je protislovje, npr. $A \land \neg A$.
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, $C_1, \ldots, C_{16}$.

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	0	0
0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

Seveda je C_1 je tavtologija, npr. $A \lor \neg A$ in C_{16} protislovje $A \land \neg A$.

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:

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

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

- $C_8 = A \land B$

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

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

$$A \Leftrightarrow \neg B\,.$$

□

1.8 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	$A \vee B$

1.9 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 **natanko 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 $(\forall x)(x$ 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"?

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

1.9.1 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:
$\neg(\forall x)(\exists y)(y > x \wedge P(y)) \Leftrightarrow (\exists x)\neg(\exists y)(y > x \wedge P(y))$
$\Leftrightarrow (\exists x)(\forall y)\neg(y > x \wedge P(y)) \Leftrightarrow (\exists x)(\forall y)(y \leq x \vee \neg P(y))$. ▲

Zgled: Zapišimo negacijo izjave $(\forall x)(\exists y)(y < x)$.
$\neg(\forall x)(\exists y)(y < x)$
$\Leftrightarrow (\exists x)(\neg(\exists y)(y < x))$
$\Leftrightarrow (\exists x)(\forall y)\neg(y < x)$
$\Leftrightarrow (\exists x)(\forall y)(y \geq x)$ ▲

- 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 $\frac{1}{1+x^2} > 1$.

1.9.2 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. □

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. □

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 $\sin x + \cos x > 1$. □

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 $\neg A(t)$.
⋮
Torej, $B \wedge \neg B$.
Sledi, da je izjava $(\exists x)\neg A(x)$ nepravilna, torej je izjava $(\forall x)A(x)$ pravilna. □

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. □

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 četrtih potenc treh drugih naravnih števil.*

Dokaz. Tako število je npr. 20.615.673, saj velja

$$20615673^4 = 2682440^4 + 15365639^4 + 18796760^4 .$$

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

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.

$\vdots$

Torej, $y = z$.
Iz (i) in (ii) izpeljemo, da je izjava $(\exists! x)A(x)$ pravilna. $\square$

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: $a, b, \ldots, x, y, z$ (+ indeksi: a_6, x_1, z_λ)

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

Množice in elemente druži 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 $P_1, \ldots, P_n$:

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

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

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

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

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

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 $a \in \{a\}$.

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., $A \subseteq C$. □

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?

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:

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

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:

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

(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 indeksno 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 $J = \{1, 2, \ldots, n\}$ in pišemo

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

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.

$$\neg(A \cup B = B)$$

$$\Leftrightarrow$$

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

$$\Leftrightarrow$$

$$\neg(A \cup B \subseteq B) \vee \neg(B \subseteq A \cup B)$$
$$\Leftrightarrow$$
$$\neg(A \cup B \subseteq B)$$
$$\Leftrightarrow$$
$$(\exists x)(x \in A \cup B \wedge x \notin B)$$
$$\Leftrightarrow$$
$$(\exists x)((x \in A \vee x \in B) \wedge x \notin B)$$
$$\Leftrightarrow$$
$$(\exists x)((x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin B))$$
$$\Leftrightarrow$$
$$(\exists x)(x \in A \wedge x \notin B)$$
$$\Leftrightarrow$$
$$\neg(\forall x)(x \in A \Rightarrow x \in B)$$
$$\Leftrightarrow$$
$$\neg(A \subseteq B)$$

□

Domača naloga: Dokažite preostale lastnosti.

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

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

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

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 zakonoma:

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

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

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 $\cup\emptyset = \emptyset$.

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

$A \setminus B = \{2\}$ (2 je edino sodo praštevilo)
$B \setminus A = \{1, 9, 15, 21, 25, \ldots\}$ (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 $(A \setminus B) \cup B = A \cup B$:

$$
\begin{gathered}
x \in (A \setminus B) \cup B \\
\Leftrightarrow \\
x \in A \setminus B \lor x \in B \\
\Leftrightarrow \\
(x \in A \land x \notin B) \lor x \in B \\
\Leftrightarrow \\
(x \in A \lor x \in B) \land (x \notin B \lor x \in B) \\
\Leftrightarrow \\
(x \in A \lor x \in B) \\
\Leftrightarrow \\
x \in A \cup B
\end{gathered}
$$

□

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:

$$C_S A = \overline{A} = S \setminus A\,.$$

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

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

▲

Lastnosti komplementa:

- $\overline{S} = \emptyset, \quad \overline{\emptyset} = S$
- $\overline{\overline{A}} = A, \quad A \cup \overline{A} = S, \quad A \cap \overline{A} = \emptyset$
- $A \setminus B = A \cap \overline{B}$
- $A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}$
- $A = B \Leftrightarrow \overline{A} = \overline{B}$
- $\overline{A \cup B} = \overline{A} \cap \overline{B}, \quad \overline{A \cap B} = \overline{A} \cup \overline{B}$ (De Morganova zakona)

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

$$\overline{\cup_{\lambda \in J} A_\lambda} = \cap_{\lambda \in J} \overline{A_\lambda}$$

$$\overline{\cap_{\lambda \in J} A_\lambda} = \cup_{\lambda \in J} \overline{A_\lambda}$$

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). ▲

Potenčna množica

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

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

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.[2]

Lastnosti:

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

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:
$X \in \mathcal{P}(A) \cap \mathcal{P}(B) \Leftrightarrow X \in \mathcal{P}(A) \wedge A \in \mathcal{P}(B) \Leftrightarrow X \subseteq A \wedge X \subseteq B$
$\Leftrightarrow X \subseteq A \cap B \Leftrightarrow X \in \mathcal{P}(A \cap B)$

V razmislek: Ali v prvi lastnosti velja ekvivalenca?

V razmislek: Zakaj v drugi lastnosti ne velja enakost?

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 $\{\{a\}, \{a, b\}\} = \{\{u\}, \{u, v\}\} \Leftrightarrow a = u \wedge b = v\,$.

Kartezični produkt

Pojem kartezičnega produkta ste spoznali že pri Analizi I.

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

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

[2] 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.

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 $A_1, \ldots, A_n$ definiramo kot množico vseh urejenih n-teric:

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

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

$$S^n = \Pi_{i=1}^{n} S = S \times \cdots \times S \quad n \text{ faktorjev}\,.$$

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

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

Kratka diskusija o aksiomih

Vsaka matematična teorija temelji na množici aksiomov — osnovnih trditev, 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 poglejmo, zakaj množica vseh množic ne obstaja.

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 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 φ o množicah $t_1, \ldots, t_k$, ki ne vsebuje črke B, je naslednji izraz aksiom:

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

   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.

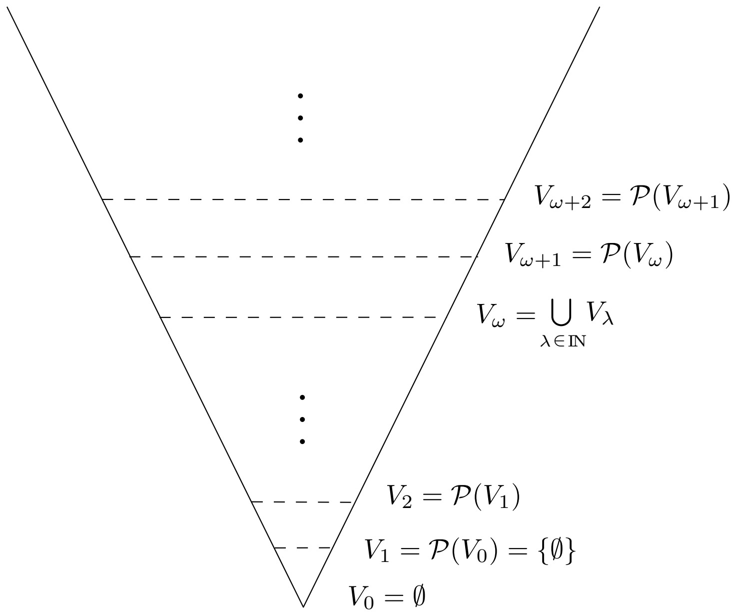
Neformalni pogled na univerzum množic

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 $V_0, V_1, V_2, \ldots$

To pa še ni vse. Napravimo unijo vseh the množic: $V_\omega = \cup_{\lambda\in\mathbb{N}} V_\lambda$. 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_ω je neskončna množica in vse nad njo prav tako.

Pomen hiererhije: Vsaka hereditarna množica se pojavi (kot element) v eni od množic V_λ 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 $V_{i+1} = V_i \cup \mathcal{P}(V_i)$.

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)

———

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:

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

———

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.,
$(\exists k)(k$ 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 $\mathrm{Im}R$)

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 $\mathcal{Z}R = \mathcal{P}(X) \setminus \{\emptyset\}$. ▲

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:

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

▲

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:

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

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

brat $\circ$ oče $\subseteq$ oče

oče $\circ$ brat $\subseteq$ stric

(oče $\circ$ brat)$\cup$(mati $\circ$ brat) $=$ stric

sestra $\circ$ mati $\subseteq$ mati

(žena $\circ$ mati) $\cup$ (mož $\circ$ mati) $=$ 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.

$$(x,y) \in V \circ (T \circ R) \Leftrightarrow xV \circ (T \circ R)y \Leftrightarrow$$
$$(\exists u)(x(T \circ R)u \wedge uVy) \Leftrightarrow (\exists u)(\exists v)(xRv \wedge vTu \wedge uVy) \Leftrightarrow$$
$$(\exists v)(xRv \wedge (\exists u)(vTu \wedge uVy)) \Leftrightarrow (\exists v)(xRv \wedge v(V \circ T)y) \Leftrightarrow$$
$$x((V \circ T) \circ R)y \Leftrightarrow (x,y) \in (V \circ T) \circ R\,.$$

□

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.

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

□

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 $(T \circ R)^{-1} = R \circ T$. ▲

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 $(S \times S) \circ R = (\mathcal{D}R) \times S$.

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 *intranzitivna* $\Leftrightarrow (\forall x)(\forall y)(\forall z)(x \in S \wedge y \in S \wedge z \in S \wedge xRy \wedge yRz \Rightarrow \neg(xRz))$
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 $\mathcal{D}R = S$).

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 $y \in R[x]$.

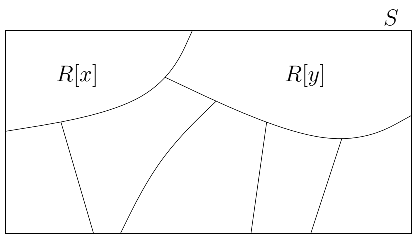
  $z \in R[y] \Rightarrow zRy \wedge yRx \Rightarrow zRx \Rightarrow z \in R[x]$.

  $z \in R[x] \Rightarrow zRx \wedge yRx \Rightarrow zRx \wedge xRy \Rightarrow zRy \Rightarrow z \in R[y]$.
- $y \notin R[x] \Rightarrow R[x] \cap R[y] = \emptyset$.

  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 $\mathcal{A}$ sovpada 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 $xR'y \Leftrightarrow (\exists X)(X \in \mathcal{A} \wedge x \in X \wedge y \in Y)$. Velja
$R' = \{(1, 1), (1, 3), (3, 1), (2, 2), (3, 3)\} = R$ in $S/R' = \{\{1, 3\}, \{2\}\} = \mathcal{A}$. ▲

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 druži 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*.

3.1 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: $f : A \to B$.

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 $f, g, h, \ldots$

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: $f : A \to B$.

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".

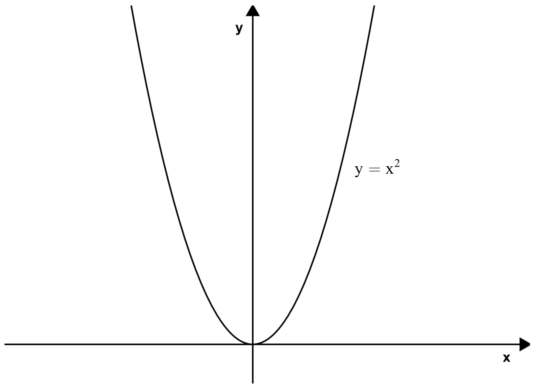
Zgledi funkcij:

- $A = \{1, 2, 3\}$, $B = \{2, 4, 6\}$
  $f = \{(1, 2), (2, 4), (3, 4)\}$
- $A = \{$točke na površju planeta Zemlja$\}$, $B = \mathbb{R}$,
  $f(x) =$ temperatura v $°C$ v kraju x dne 1. 1. 2015 ob 6:00 po lokalnem času
- $A = \{$ljudje, živeči na Zemlji ob času $T\}$, $B = \mathbb{N}$,
  $f(x) =$ starost (v sekundah) osebe x v času T.

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

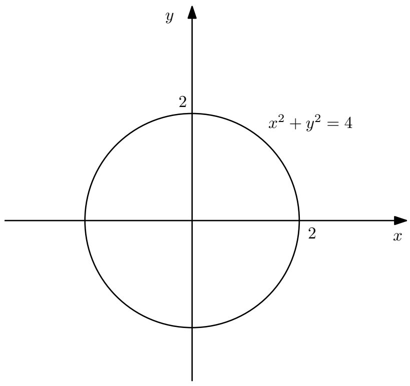
Upodobitve funkcij. V primeru, ko je $A \subseteq \mathbb{R}$ in $B = \mathbb{R}$, lahko graf funkcije upodobimo kot množico točk v ravnini.

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



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 $f : A \to B$. 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. $g : A \to B$, $g = \{(1,2),(2,6),(3,4)\}$, 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:

$$\begin{aligned} f \text{ je } \textit{injektivna} &\Leftrightarrow (\forall y)(y \in \mathcal{Z}f \Rightarrow (\exists! x)(x \in A \wedge f(x) = y)) \\ &\Leftrightarrow (\forall x)(\forall y)(f(x) = f(y) \Rightarrow x = y) \end{aligned}$$

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:

- $f(\emptyset) = \emptyset, \quad f(A) = \mathcal{Z}f$.
- $U \subseteq V \Rightarrow f(U) \subseteq f(V)$.

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.

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:

- $f^{-1}(\mathcal{Z}f) = A$

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

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

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

□

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

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

Kompozitum funkcij

Naj bosta f in g parcialni funkciji. Tedaj velja

$$g \circ f = \{(x, z); (\exists y)((x, y) \in f \wedge (y, z) \in g)\}$$

$$= \{(x, z); (\exists y)(f(x) = y \wedge g(y) = z)\}\,.$$

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 $\mathcal{D}g = \mathcal{Z}f$.) $g \circ f = \{(1, 3), (2, 5), (3, 5)\}$

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

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

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 $f : A \to B$ 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.

Kanonična dekompozicija funkcije

Dana je funkcija $f : A \to B$. 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:

$$p : A \to A/R$$

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

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, $f = g \circ p$:

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

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

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:

$$\begin{tikzcd} A \arrow[r, "p", "\text{surj.}"'] \arrow[rr, bend right, "f"'] & A/R \arrow[r, "g", "\text{inj.}"'] & B \end{tikzcd}$$

To dekompozicijo lahko še malce izpopolnimo, tako da vpeljemo preslikavo h, ki je podana z istim predpisom kot g, le da slika v množico $\mathcal{Z}f$. Preslikava h je potem bijektivna:
$$h : A/R \to \mathcal{Z}f$$
$$h(u) = g(u)\,.$$
Množico $\mathcal{Z}f$ pa nazadnje preslikamo v množico B z *identično preslikavo* i, ki pribije vsak element:
$$i : \mathcal{Z}f \to B$$
$$i(y) = y\,.$$

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:

$$\begin{tikzcd} A \arrow[r, "p", "\text{surj.}"'] \arrow[rrr, bend right, "f"'] & A/R \arrow[r, "h", "\text{bij.}"'] & \mathrm{Im} f \arrow[r, "i", "\text{inj. (identična)}"'] & B \end{tikzcd}$$

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: $A/R = \{\{1\},\{2,3\}\}$
$\mathcal{Z}f = \{2,4\}$

Naravna preslikava p: $p(1) = \{1\}$, $p(2) = p(3) = \{2,3\}$.
Preslikava $g : \{\{1\},\{2,3\}\} \to \{2,4,6\}$:
$g(\{1\}) = f(1) = 2$, $g(\{2,3\}) = f(2) = f(3) = 4$.
Preslikava $h : \{\{1\},\{2,3\}\} \to \{2,4\}$: $h(\{1\}) = g(\{1\}) = 2$, $h(\{2,3\}) = g(\{2,3\}) = 4$.
Identična preslikava $i : \{2,4\} \to \{2,4,6\}$: $i(2) = 2$, $i(4) = 4$.

$$\begin{tikzcd}
\{1,2,3\} \arrow[r, "p", "\text{surj.}"'] \arrow[rrr, bend right, "f"'] & \{\{1\},\{2,3\}\} \arrow[r, "h", "\text{bij.}"'] & \{2,4\} \arrow[r, "i", "\text{inj. (identična)}"'] & \{2,4,6\}
\end{tikzcd}$$

3.2 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 našteli 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.

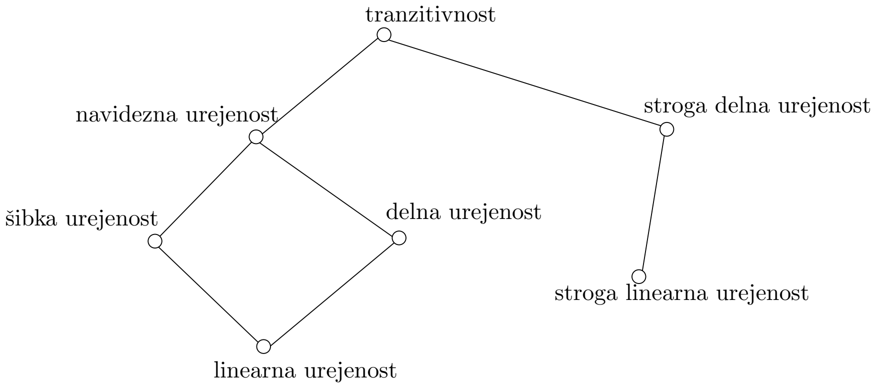
- Primer:

  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.

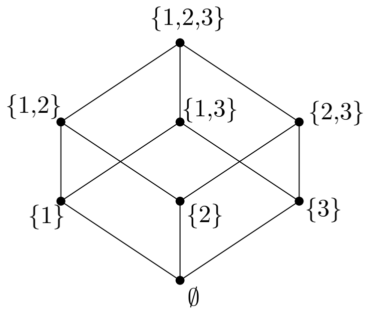
Delno urejenost pa moremo prikazati s t.i. *Hassejevim diagramom:*



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*.

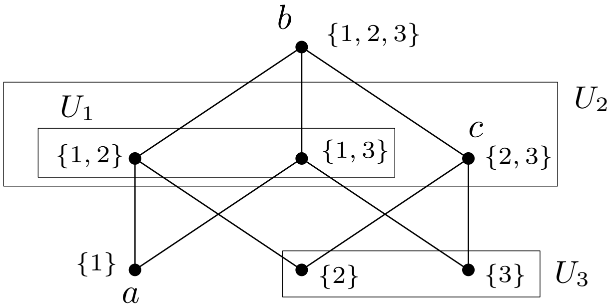
Če ima U kakšno R-zgornjo mejo in kakšno R-spodnjo mejo, potem je U *R-omejena*.

$a \in S$ 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-sup in kvečjemu en R-inf. Lahko ju pa nima (tudi če je omejena)!

Zgled:

$S = \mathbb{Q}$, $R = \leq$

$$U = \{x \ ; \ x \in \mathbb{Q} \land 0 \leq x \land x^2 \leq 2\}$$

Množica U je navzdol in navzgor omejena!
$\inf U = 0$, $\sup U$ pa ne obstaja!

$$V = \{x \ ; \ x \in \mathbb{Q} \land 0 \leq x \land 2 \leq x^2 \leq 5\}$$

Množica V je omejena, ne obstajata pa niti $\inf V$ niti $\sup V$. ▲

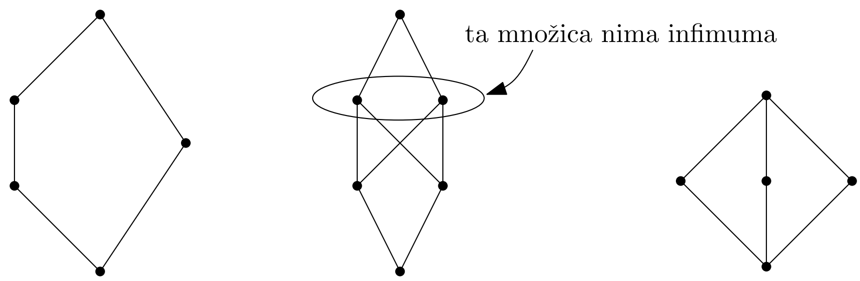
Definicija. *Množica S ima strukturo* mreže *glede na relacijo R $\Leftrightarrow$ R delno ureja S in vsaka* dvoelementna *podmnožica $X \subseteq S$ ima tako R-supremum kot R-infimum.*

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. $S = \mathbb{N} \backslash \{0\}$, $R = |$ (relacija deljivosti).
   - delna urejenost ✓
   - $x, y \in \mathbb{N} \setminus \{0\}$, $x \neq y$
     $\inf\{x, y\} =$ največji skupni delitelj x in y
     $\sup\{x, y\} =$ najmanjši skupni večkratnik x in y

Še nekaj zgledov s Hassejevimi diagrami:



mreža ni mreža mreža

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

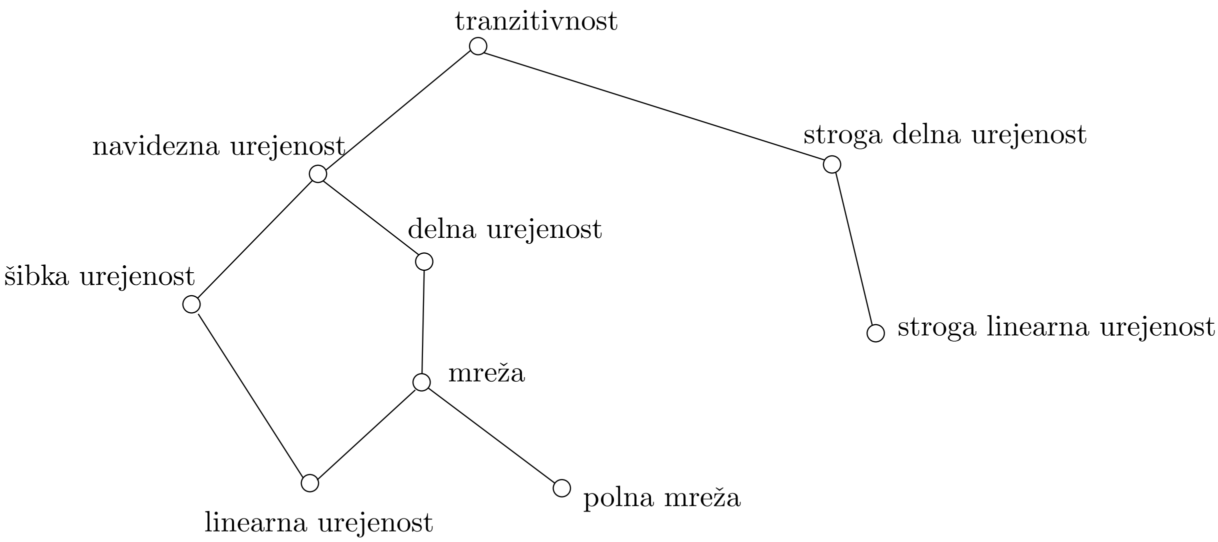
$$(\subseteq)\text{- }\sup \mathcal{A} = \cup \mathcal{A}\,.$$

▲

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 dopolnemo do polne mreže, tako da ji dodamo elementa ∞ 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.

Dobra urejenost

Prav tako kakor množica realnih števil $\mathbb{R}$ je tudi množica naravnih števil $\mathbb{N}$ z relacijo "$<$" strogo linearno urejena.

Ima pa še dodatno lastnost:

V vsaki neprazni podmnožici naravnih števil obstaja najmanjši element!

Primer:

- V množici vseh naravnih števil je tak element kar element 0.
- V množici vseh praštevil je najmanjši element število 2.

Množica realnih števil pa take lastnosti nima!

- množica $\mathbb{R}$ nima najmanjšega elementa

- množica $\{x\ ;\ x \in \mathbb{R} \wedge x > 0\}$ tudi ne

Lastnosti, da ima vsaka neprazna množica najmanjši element, pravimo *dobra urejenost.*

R – relacija na množici S (običajno delna ali stroga delna urejenost)

- $a \in S$ je *minimalen element* množice S glede na relacijo R (ali *R-minimalen element* množice S) $\Leftrightarrow$ $(\forall y)(y \in S \wedge y \neq a \Rightarrow \neg(yRa))$

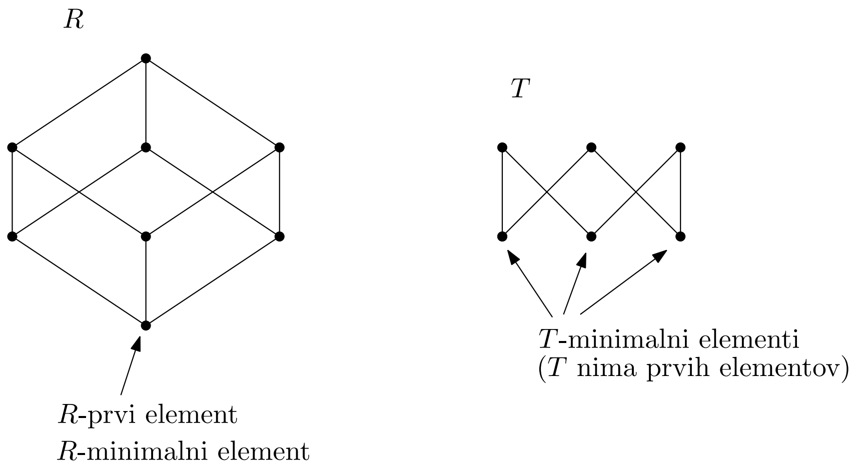
- $b \in S$ je *prvi element* množice S glede na relacijo R (ali *R-prvi element* množice S) $\Leftrightarrow$ $(\forall y)(y \in S \wedge y \neq b \Rightarrow bRy)$

Spomnimo se terminologije:
xRy in $x \neq y$: "x je pod y"

Noben element množice S ni pod minimalnim elementom.
Prvi element je pod vsakim drugim elementom.

- Vsak element, ki ni primerljiv z nobenim drugim, je minimalen.

Zgled – prvi in minimalni elementi
Delni urejenosti R in T sta podani z naslednjima Hassejevima diagramoma:



Trditev. *Naj bo R antisimetrična. Potem je vsak R-prvi element tudi R-minimalen.*

Dokaz. S protislovjem. Recimo, da obstaja nek R-prvi element b, ki ni R-minimalen.
b ni R-minimalen:
$\neg(\forall y)(y \in S \wedge y \neq b \Rightarrow \neg(yRb))$
$\Rightarrow (\exists y)(y \in S \wedge y \neq b \wedge yRb)$
Ker je b R-prvi, velja bRy. Ker pa je R antisimetrična, iz $bRy \wedge yRb$ sledi $y = b$. To pa je protislovje z dejstvom $y \neq b$. $\square$

Trditev. *Naj bo R sovisna. Potem je vsak R-minimalen element tudi R-prvi.*

Dokaz. x je R-minimalen za $S \Rightarrow (\forall y)(y \in S \wedge y \neq x \Rightarrow \neg(yRx))$
Sovisnost: $y \neq x \wedge \neg(yRx) \Rightarrow xRy$
Posledično: $(\forall y)(y \in S \wedge y \neq x \Rightarrow xRy)$
Torej je x R-prvi element. □

Definicija. R dobro ureja $S \Leftrightarrow$ *R je sovisna, irefleksivna in*
$(\forall X)(X \subseteq S \wedge X \neq \emptyset \Rightarrow X$ *ima R-minimalen element*$)$

Trditev. *R dobro ureja S* $\Rightarrow$ *R strogo linearno ureja S.*

Dokaz. Pokazati je treba, da je R tranzitivna, asimetrična in sovisna.
Sovisnost sledi iz definicije dobre urejenosti.
Asimetričnost: Recimo, da velja xRy in yRx. Ker je R irefleksivna, je $y \neq x$. Potem pa množica $\{x, y\}$ nima R-minimalnega elementa:

- $xRy \Rightarrow y$ ni R-minimalen
- $yRx \Rightarrow x$ ni R-minimalen

R je torej asimetrična.
Tranzitivnost dokažemo podobno: Recimo, da velja

$$xRy \wedge yRz \wedge \neg(xRz)\,.$$

Ker je R irefleksivna, sledi $x \neq y$ in $y \neq z$. Če je $x = z$, potem velja $xRy \wedge yRx$, kar je v protislovju z asimetričnostjo (ki smo jo že dokazali). Torej $x \neq z$. Množica $\{x, y, z\}$ ima R-minimalen element, vendar:

- ta element ni y, saj velja $xRy \wedge x \neq y$,
- ta element ni z, saj velja $yRz \wedge y \neq z$.

Sledi: R-minimalen element množice $\{x, y, z\}$ je x. Ker $z \neq x$, iz sovisnosti in $\neg(xRz)$ sledi zRx. To pa je protislovje z dejstvom, da je x minimalen element. R je torej tranzitivna. □

Iz zgornjih trditev sledi:

Posledica. *Naj R dobro ureja S. Potem za vse $x \in S$ velja:*

$$x \text{ je } R\text{-prvi} \Leftrightarrow x \text{ je } R\text{-minimalen}\,.$$

Velja tudi enoličnost:

Trditev. *Naj relacija R dobro ureja neprazno množico X. Potem v množici X eksistira en sam R-prvi (ali R-minimalen) element.*

Dokaz. Recimo, da obstajata dva različna R-prva elementa x in y. Potem velja xRy (ker je x R-prvi in $x \neq y$) in podobno yRx. To pa je protislovje z asimetričnostjo! □

Glede na zgornje trditve lahko dobro urejenost definiramo tudi s pomočjo R-prvih elementov:

Posledica. *R dobro ureja S natanko takrat, ko je R sovisna, asimetrična in velja:*
$(\forall X)(X \subseteq S \wedge X \neq \emptyset \Rightarrow X$ *ima R-prvi element).*

Pojem dobre urejenosti je pomemben zato, ker posploši urejenost $<$ na množici naravnih števil. Tudi princip popolne indukcije se da posplošiti na dobro urejene množice (to je t.i. *transfinitna indukcija*).

Neposredni naslednik. Zadnji element.

V naravnih številih, urejenih glede na relacijo "$<$", ima vsako število svojega (enolično določenega) neposrednega naslednika. Kaj pa karakterizira neposrednega naslednika y danega števila x?

- $x < y$
- za vsako drugo naravno število z, za katerega je tudi $x < z$, mora veljati hkrati $y < z$.

Naj relacija R dobro ureja množico S. Element y je *neposredni naslednik* elementa x $\Leftrightarrow$ xRy in $(\forall z)(z \in S \wedge z \neq y \wedge xRz \Rightarrow yRz)$.

Vsaka končna neprazna podmnožica naravnih števil ima poleg prvega tudi *zadnji element*. To je pač tisto število te množice, imenujmo ga x, s katerim je vsako drugo število y v relaciji $y < x$.

Definicijo posplošimo:
Naj R dobro ureja S in naj bo $X \subseteq S$. Element $x \in X$ je *R-zadnji element* množice X $\Leftrightarrow$ $(\forall y)(y \in X \wedge y \neq x \Rightarrow yRx)$.

Trditev. *Naj R dobro ureja S in naj bo $x \in S$. Če x ni R-zadnji element množice S, potem ima x natanko enega neposrednega naslednika.*

Dokaz. Oglejmo si množico

$$X = \{z \,; z \in S \wedge xRz\}\,.$$

Ker x ni R-zadnji, je množica X neprazna.
Množica X ima zato natanko en R-prvi element y.
Dokažimo, da je y neposredni naslednik x:

- Ker je $y \in X$, je xRy.
- Če pa je $z \in S$ tak element, da je xRz in $z \neq y$, potem je yRz (ker je $z \in X$ in je y R-prvi element množice X).

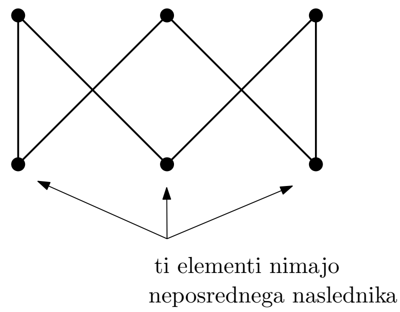
y je tudi edini neposredni naslednik elementa x:

Recimo, da obstaja $z \neq y$, ki je neposredni naslednik elementa x. Ker je xRz, je $z \in X$.

Ker je y R-prvi element množice X, $z \in X \wedge z \neq y$, je tudi yRz.

To pa je protislovje z definicijo neposrednega naslednika x. □

Definiciji neposrednega naslednika in R-zadnjega elementa lahko vpeljemo tudi za splošne delno urejene in strogo delno urejene množice. Vendar analog zgornje trditve v splošnem ne drži:

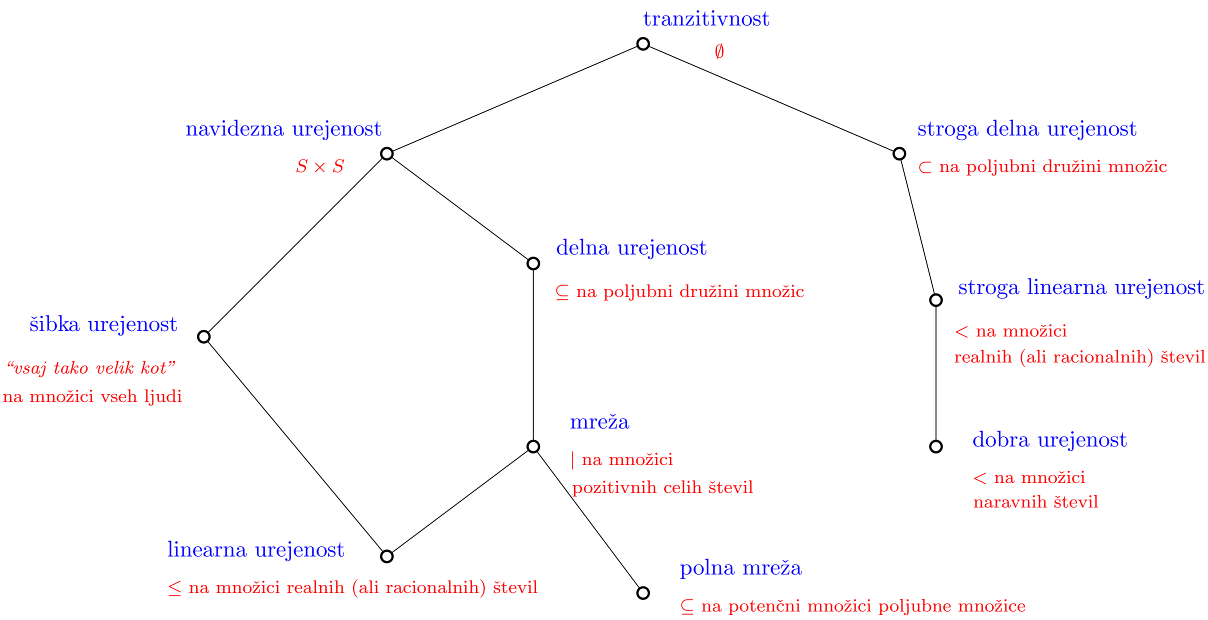


Tudi v strogo linearno urejenih množicah se lahko zgodi, da nek element nima nobenega neposrednega naslednika. V množici realnih števil $\mathbb{R}$ število 0 (kot tudi katerokoli drugo realno število) nima nobenega neposrednega naslednika glede na relacijo "$<$" (čim je $0 < y$, za število $z = y/2$ velja $z \neq y$, $0 < z$, vendar pa $\neg(y < z)$). Podobno velja tudi za relacijo "$<$" na množici racionalnih števil $\mathbb{Q}$.

Pojem neposrednega predhodnika definiramo podobno kot pojem neposrednega naslednika. Vendar pa analogna trditev za dobro urejenost R, ki pravi, da ima vsak element x, ki ni R-prvi, natanko enega neposrednega predhodnika, ne drži!

Zgled: Naj bo $S = \mathbb{N} \cup \{\infty\}$. Za R pa vzemimo običajno urejenost $<$ na $\mathbb{N}$, razširjeno s pravilom $n < \infty$ za vse $n \in \mathbb{N}$. Tedaj R dobro ureja S. Vendar pa element ∞ nima nobenega neposrednega predhodnika. ▲

Zaključimo poglavje o strukturah urejenosti s Hassejevim diagramom 10 struktur urejenosti, ki smo jih spoznali. Ob vsaki strukturi je naveden zgled modela strukture.



$$x \text{ je pod } y \iff x \text{ je poseben primer } y$$

3.3 Aksiom izbire

A_1, A_2: množici

$A_1 \times A_2 = \{(x,y)\ ;\ x \in A_1,\ y \in A_2\}$

Vsak urejeni par je določen tako, da prvi element izberemo iz množice A_1, drugega pa iz A_2. Tako izbiro lahko ponazorimo s funkcijo:

$f : \{1,2\} \to A_1 \cup A_2$, za katero velja

$$f(1) \in A_1 \text{ in } f(2) \in A_2\,.$$

Torej

$$A_1 \times A_2 = \{f : \{1,2\} \to A_1 \cup A_2, f(1) \in A_1, f(2) \in A_2\}\,.$$

Podobno lahko zapišemo za kartezične produkte končnega števila faktorjev:

$$A_1 \times \cdots \times A_n = \{f : \{1,\ldots,n\} \to A_1 \cup \cdots \cup A_n, f(1) \in A_1, \ldots, f(n) \in A_n\}\,.$$

Na ta način moremo posplošiti definicijo kartezičnega produkta na produkt poljubne družine množic.

Naj bo

$$\mathcal{A} = \{A_\lambda\ ;\ \lambda \in I\}$$

poljubna družina množic. *Kartezični produkt* družine $\mathcal{A}$ definiramo kot

$$\prod \mathcal{A} = \prod_{\lambda \in I} A_\lambda = \{f : I \to \cup_{\lambda \in I} A_\lambda,\ (\forall \lambda)(\lambda \in I \Rightarrow f(\lambda) \in A_\lambda)\}\,.$$

$f \in \prod_{\lambda \in I} A_\lambda$ se imenuje *funkcija izbire.*

Če je vsaj ena od množic A_λ prazna, je tudi produkt $\prod_{\lambda \in I} A_\lambda$ prazna množica (saj v primeru $A_\lambda = \emptyset$ pogoj $f(\lambda) \in A_\lambda$ prav gotovo ne more biti izpolnjen)!

- $(\exists \lambda)(\lambda \in I \wedge A_\lambda = \emptyset) \Rightarrow \prod_{\lambda \in I} A_\lambda = \emptyset$.

V končnem primeru velja tudi obrat:

$$(\forall \lambda)(\lambda \in I \Rightarrow A_\lambda \neq \emptyset) \Rightarrow \prod_{\lambda \in I} A_\lambda \neq \emptyset\,.$$

Kaj pa v neskončnem primeru??

"Če je $A_\lambda \neq \emptyset$ za vse $\lambda \in I$, potem obstaja vsaj ena funkcija izbire."

Ali lahko to dokažemo?

Cohen (1963): ta trditev je nedokazljiva iz drugih aksiomov teorije množic.

Aksiom o kartezičnem produktu:

Če je $\mathcal{A}$ poljubna družina nepraznih množic, potem je $\prod \mathcal{A}$ neprazna množica.

Aksiom izbire:

Če je $\mathcal{A} = \{A_\lambda\ ;\ \lambda \in I\}$ poljubna družina nepraznih množic, potem obstaja vsaj ena funkcija $f : I \to \cup_{\lambda \in I} A_\lambda$, za katero velja $f(\lambda) \in A_\lambda$ za vsak $\lambda \in I$.

Zermelo, 1904 – uporabil AI pri dokazu izreka o dobri urejenosti množic

(Zermelov aksiom)

Gödlov izrek (1940): Aksiom izbire je konsistenten z drugimi aksiomi teorije množic:[3]

- *Če pridemo do protislovja v sistemu, kjer poleg drugih aksiomov privzamemo tudi aksiom izbire, potem je mogoče protislovje konstruirati tudi v sistemu, ki sloni le na drugih aksiomih in nima aksioma izbire.*

S pomočjo aksioma izbire je moč dokazati številne pomembne izreke na različnih področjih matematike (algebra, analiza, topologija, ...), pa tudi nekatere manj intuitivne izreke, npr. **paradoks Banacha in Tarskega:** Tridimenzionalno kroglo je moč razkosati na končno mnogo paroma disjunktnih delov, ki se jih s translacijami in rotacijami sestavi v *dve* identični kopiji prvotne krogle!

Aksiom izbire je ekvivalenten mnogim drugim trditvam, npr. naslednjima dvema:

- Vsaka binarna relacija vsebuje funkcijo z isto domeno.
- Če je $\mathcal{A}$ družina paroma disjunktnih nepraznih množic, potem obstaja taka množica X, da za vsak $A \in \mathcal{A}$ množica $X \cap A$ vsebuje natanko en element.

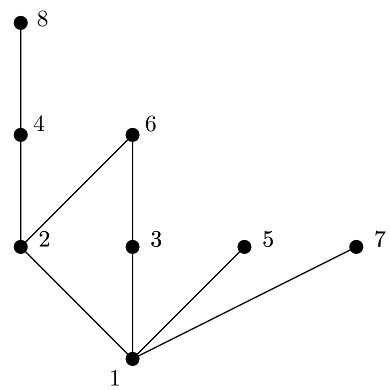
Principi maksimalnosti

Podali bomo štiri t.i. principe maksimalnosti in pokazali, da so med seboj logično ekvivalentni. Ekvivalentni so tudi aksiomu izbire.

Najprej navedimo dve definiciji:

- Naj R delno ureja S. Če v S obstaja element m, tako da za noben drug element $x \in S$ *ne velja* mRx, potem pravimo, da je m *R-maksimalen element* množice S.
- Podmnožica X množice S, ki je z relacijo R delno urejena, je *veriga* v množici S, če jo R linearno ureja.

Zgled: Naj bo $S = \{1, 2, \ldots, 8\}$ in naj bo R delacija deljivosti na S (xRy natanko tedaj, ko x deli y). To delno urejenost prikazuje naslednji Hassejev diagram:



[3] Kurt Gödel je istočasno s konsistentnostjo aksioma izbire dokazal tudi konsistentnost hipoteze kontinuuma z drugimi aksiomi teorije množic. S tem je rešil prvega od znamenitih 23 problemov, ki jih je leta 1900 matematični javnosti zastavil nemški matematik David Hilbert.

Ima 4 maksimalne elemente (5, 6, 7, 8), vsebuje pa naslednje verige:

- $\emptyset$ (1 veriga brez elementov)
- $\{1\}, \{2\}, \ldots, \{8\}$ (8 enoelementnih verig)
- $\{1,2\}, \{1,3\}, \ldots, \{1,8\}, \{2,4\}, \{2,6\}, \{2,8\}, \{3,6\}, \{4,8\}$ (12 dvoelementnih verig)
- $\{1,2,4\}, \{1,2,6\}, \{1,2,8\}, \{1,3,6\}, \{1,4,8\}, \{2,4,8\}$ (6 troelementnih verig)
- $\{1,2,4,8\}$ (1 štirielementna veriga)

1. Hausdorffov princip maksimalnosti.

Naj bo S z relacijo R delno urejena. Naj bo $\mathcal{V}$ družina vseh verig:

$$\mathcal{V} = \{X \subseteq S \ ; \ X \text{ je veriga}\}\,.$$

Množica $\mathcal{V}$ je delno urejena glede na relacijo $\subseteq$.

Kdaj je X maksimalen element $\mathcal{V}$?

Ko za vsak drug $Y \in \mathcal{V}$ velja, da X ni podmnožica Y: $X \nsubseteq Y$. Takemu elementu pravimo *maksimalna veriga*.

Hausdorffov princip maksimalnosti:
Množica $\mathcal{V}$ ima vsaj en maksimalen element glede na $\subseteq$.
Vsaka delno urejena množica ima vsaj eno maksimalno verigo.

2. Zornova lema.

Zornova lema pravi, da je pogoj, da je vsaka veriga v delno urejeni množici navzgor omejena, zadosten pogoj za obstoj maksimalnega elementa dane množice.

Zornova lema: *Naj bo S z relacijo R delno urejena in naj ima vsaka veriga v S vsaj eno R-zgornjo mejo. Potem ima množica S vsaj en R-maksimalen element.*

3. Tukeyev princip maksimalnosti.

Naj bo S poljubna množica in $\mathcal{D}$ poljubna (neprazna) družina podmnožic množice S (torej $\mathcal{D} \subseteq \mathcal{P}(S)$).

Definicija. $\mathcal{D}$ *ima* karakter končnosti $\Leftrightarrow$ *poljubna množica $X \subseteq S$ je v $\mathcal{D}$ natanko takrat, ko je v $\mathcal{D}$ vsaka* končna *podmnožica množice X.*

Zgled: Naj bo S množica vseh pozitivnih celih števil in $\mathcal{D}$ družina vseh množic paroma tujih naravnih števil: $X \in \mathcal{D}$ natanko tedaj, ko velja:

$$(\forall x)(\forall x)(x \in X \wedge y \in X \wedge x \neq y \Rightarrow n.s.d.(x,y) = 1)\,,$$

kjer $n.s.d.(x,y)$ označuje največjega skupnega delitelja števil x in y. Družina $\mathcal{D}$ ima karakter končnosti, saj za vsak $X \subseteq S$ velja: $X \notin \mathcal{D}$ natanko tedaj, ko obstajata **dve** različni števili $x, y \in \mathcal{X}$, ki nista tuji.

Po drugi strani pa družina $\mathcal{D}'$, definirana kot

$$\mathcal{D}' = \{X \subseteq S; X \text{ je končna}\},$$

nima karakterja končnosti. Množica S namreč ni v družini $\mathcal{D}'$, čeprav so v $\mathcal{D}$ vse končne podmnožice S. ▲

Tukeyev princip maksimalnosti:
Če ima $\mathcal{D}$ karakter končnosti, potem ima $\mathcal{D}$ vsaj en maksimalen element glede na relacijo "$\subseteq$"(ki $\mathcal{D}$ delno ureja).

4. Lema Kuratowskega.
Naj bo S delno urejena z relacijo R. Naj bo $V \subseteq S$ veriga v S.

$$\mathcal{U}_V = \{X \subseteq S\ ;\ X \text{ je veriga v } S \text{ in } V \subseteq X\}.$$

$\mathcal{U}_V$ je delno urejena z relacijo "$\subseteq$".
Lema Kuratowskega: *$\mathcal{U}_V$ ima vsaj en maksimalen element glede na inkluzijo $\subseteq$.*

Vsaka veriga je vsebovana v neki maksimalni verigi.

Vsi ti principi maksimalnosti so med seboj logično ekvivalentni. Velja:

$$(\text{Hausdorff}) \Rightarrow (\text{Zorn}) \Rightarrow (\text{Tukey}) \Rightarrow (\text{Kuratowski}) \Rightarrow (\text{Hausdorff})$$

1. etapa: (Hausdorff) $\Rightarrow$ (Zorn)
Naj R delno ureja S in naj ima vsaka veriga v S R-zgornjo mejo. Po Hausdorffu obstaja v S vsaj ena maksimalna veriga V.
Po hipotezi Zornove leme ima V neko R-zgornjo mejo m.
Trdimo, da je m R-maksimalen element.
Pa recimo, da to ni res. Tedaj obstaja nek element $x \in S$, da velja $x \neq m$ in mRx.
Naj bo $y \in V$. Ker je m zgornja meja verige V, velja yRm in tudi mRx in posledično, zaradi tranzitivnosti, yRx. Sledi $y \neq x$, saj bi iz $y = x$ sledilo mRx in xRm in tudi $x = m$.
Potemtakem pa je veriga V prava podmnožica množice $V \cup \{x\}$. Množica $V \cup \{x\}$ pa je z relacijo R linearno urejena, torej je veriga. To pa je v protislovju z zahtevo, da je V maksimalna veriga.
S tem smo pokazali, da ima množica S nek R-maksimalen element. □

2. etapa: (Zorn) $\Rightarrow$ (Tukey)
Naj bo $\mathcal{D}$ neprazna družina podmnožic dane množice S in naj ima karakter končnosti.
Družina $\mathcal{D}$ je delno urejena glede na relacijo "$\subseteq$".
Preverimo, da ima vsaka veriga v tej družini zgornjo mejo!
Naj bo V poljubna veriga v družini $\mathcal{D}$. Elementi množice V so podmnožice množice S, ki so z relacijo $\subseteq$ linearno urejene (saj je V veriga). Napravimo unijo vseh elementov te verige, $W = \cup V$. Očitno je W zgornja meja verige V (saj za vsak element $X \in V$ velja $X \subseteq \cup V = W$).

Pokažimo, da je $W \in \mathcal{D}$. Ker ima $\mathcal{D}$ karakter končnosti, je dovolj pokazati, da je vsaka končna podmnožica množice W vsebovana v $\mathcal{D}$. Naj bo $A = \{a_1, \ldots, a_n\} \subseteq W$. Torej obstajajo take množice $A_1, \ldots, A_n \in V$, da velja $a_i \in A_i$ za vse i. Ker pa so te množice linearno urejene, morajo nujno v eni izmed teh n podmnožic, recimo ji A_j, biti vse druge. V množici A_j je potem tudi množica A. Ker je $A \subseteq A_j \in V$ in torej tudi $A_j \in \mathcal{D}$, pa sledi, da je tudi $A \in \mathcal{D}$, saj je A končna podmnožica množice V, ki je element $\mathcal{D}$, družina $\mathcal{D}$ pa ima karakter končnosti.

Pokazali smo torej, da ima vsaka veriga zgornjo mejo glede na relacijo inkluzije. Po Zornovi lemi od tod sledi, da ima družina $\mathcal{D}$ vsaj en maksimalen element. □

3. etapa: (Tukey) $\Rightarrow$ (Kuratowski)

Naj relacija R delno ureja množico S in naj bo V poljubna veriga v S.

Naj bo $\mathcal{D}$ družina vseh tistih podmnožic X množice S, za katere je $X \cup V$ veriga v množici S.

Prepričajmo se, da ima $\mathcal{D}$ karakter končnosti!

Naj bo $X \in \mathcal{D}$. Potem je tudi vsaka končna podmnožica X' množice X v $\mathcal{D}$: $V \cup X$ je namreč veriga, torej je tudi $V \cup X'$ veriga.

In obratno: naj bo X taka podmnožica množice S, da je v $\mathcal{D}$ vsaka končna podmnožica množice X. Potem za vsaka dva elementa $x, y \in X$ velja, da je $\{x, y\} \cup V$ veriga. Torej je očitno tudi $X \cup V$ veriga. Torej je $X \in \mathcal{D}$.

Po Tukeyu torej v množici $\mathcal{D}$ eksistira vsaj en maksimalen element M glede na relacijo inkluzije $\subseteq$.

Po definiciji družine $\mathcal{D}$ pa je potem $M \cup V$ maksimalna veriga v množici S, v kateri je veriga V. To pa je trditev leme Kuratowskega. □

4. etapa: (Kuratowski) $\Rightarrow$ (Hausdorff)

Naj relacija R delno ureja množico S. Izberimo za verigo v množici S prazno množico. Ta je prav gotovo veriga, saj je zahteva po linearni urejenosti na prazno izpolnjena.

Toda prazna množica je podmnožica vsake verige množice S. Po lemi Kuratowskega maksimalna veriga obstaja in je hkrati tudi maksimalen element družine $\mathcal{V}$ vseh verig glede na relacijo inkluzije $\subseteq$. To pa je vsebina Hausdorffovega principa maksimalnosti. □

Principi maksimalnosti so tudi ekvivalentni aksiomu izbire:

(Tukey) $\Rightarrow$ (aksiom izbire) $\Rightarrow$ (Hausdorff)

(Tukey) $\Rightarrow$ (aksiom izbire)

Naj bo $\mathcal{A} = \{A_\lambda\ ;\ \lambda \in I\}$ poljubna družina nepraznih množic.

Naj bo $\mathcal{F}$ množica vseh (parcialnih) funkcij, katerih domena $\mathcal{D}f$ je podmnožica množice I in ki priredijo vsakemu $\lambda \in \mathcal{D}f$ določen element $f(\lambda) \in A_\lambda$.

Vsaka taka funkcija je množica urejenih parov, torej

$$f \subseteq I \times \cup\mathcal{A}\,.$$

Množica $\mathcal{F}$ pa je družina podmnožic kartezičnega produkta $I \times \cup\mathcal{A}$.

Trditev: $\mathcal{F}$ ima karakter končnosti.

Dokaz trditve: Naj bo funkcija $f \in \mathcal{F}$. Očitno je tudi vsaka končna podmnožica funkcije f element $\mathcal{F}$.

Zdaj pa vzemimo poljubno podmnožico g kartezičnega produkta $I \times \cup\mathcal{A}$, ki ima lastnost, da je vsaka njena končna podmnožica element družine $\mathcal{F}$.

V tem primeru je tudi g funkcija in je element družine $\mathcal{F}$. Če bi namreč v množici g obstajala različna para (λ, a) in (λ, b) z isto prvo koordinato, potem bi dvoelementna podmnožica $\{(\lambda, a), (\lambda, b)\}$ ne bila funkcija, kar pa je v nasprotju s predpostavko.

Podobno ugotovimo, da je $g \in \mathcal{F}$, saj za vsak $(\lambda, a) \in g$ velja, da je $\{(\lambda, a)\} \in \mathcal{F}$, torej $\lambda \in I$ in $a \in A_\lambda$.

Pokazali smo trditev, da ima $\mathcal{F}$ karakter končnosti. Po Tukeyjevem principu maksimalnosti ima $\mathcal{F}$ vsaj en maksimalen element F glede na relacijo "$\subseteq$".

Prepričajmo se, da je prav ta F funkcija izbire!

Ker je $F \in \mathcal{F}$, je F funkcija. Dovolj je torej pokazati, da je domena funkcije F množica I. Pa recimo, da ni. Tedaj obstaja nek indeks $\lambda \in I \backslash \mathcal{D}f$. Naj bo a poljuben element neprazne množice A_λ in napravimo urejeni par (λ, a) in nato unijo $F \cup \{(\lambda, a)\}$. Ta unija je element družine $\mathcal{F}$, ki vsebuje funkcijo F kot pravo podmnožico. To pa je v nasprotju s trditvijo, da je F maksimalen element družine $\mathcal{F}$.

Potem pa je $\mathcal{D}F = I$ in je F res funkcija izbire. □

Da se pokazati, da **(aksiom izbire)** $\Rightarrow$ **(Hausdorff)**.

Dokaz opustimo, glej *Niko Prijatelj: Matematične strukture I, str. 135–142.*

Za dokaz implikacije **(aksiom izbire)** $\Rightarrow$ **(Zornova lema)** glej *Paul Halmos: Naive Set Theory, str. 63–65.*

Izrek o dobri ureditvi

Morda najgloblji razlog, zaradi katerega se zdi mnogim matematikom aksiom izbire problematičen, tiči v tem, da je mogoče iz njega izpeljati izrek o dobri ureditvi, ki pravi, da je vsako množico mogoče dobro urediti.

Izrek o dobri ureditvi: Za vsako množico S obstaja neka relacija R, ki to množico dobro ureja.

Izrek o dobri ureditvi $\Leftrightarrow$ aksiom izbire.

Pokažimo enostavnejšo od obeh implikacij:

Izrek o dobri ureditvi $\Rightarrow$ aksiom izbire.

Naj bo $\mathcal{A} = \{A_\lambda \ ; \ \lambda \in I\}$ poljubna družina nepraznih množic. Po izreku o dobri ureditvi obstaja neka relacija R, ki dobro ureja *unijo družine* $\mathcal{A}$, $\cup\mathcal{A}$.

Ker pa je vsaka množica A_λ družine $\mathcal{A}$ neprazna podmnožica unije $\cup\mathcal{A}$, ima zato neki R-prvi element. Funkcijo izbire f zdaj lahko definiramo tako, da vsakemu elementu $\lambda \in I$ priredi R-prvi element množice A_λ:

$$f(\lambda) = R\text{-prvi element v } A_\lambda\,.$$

S to konstrukcijo je aksiom izbire potrjen. □

Da se pokazati tudi implikacijo **(aksiom izbire)** $\Rightarrow$ **(izrek o dobri ureditvi)**.

Dokaz opustimo, glej *Niko Prijatelj: Matematične strukture I, str. 143–151.*

Za dokaz implikacije **(Zornova lema)** $\Rightarrow$ **(izrek o dobri ureditvi)** glej *Paul Halmos: Naive Set Theory, str. 68.*

3.4 Ekvipolentne množice

Kdaj imata dve končni množici enako mnogo elementov?

Odstranimo iz vsake množice po en element in postopek ponavljamo. Množici imata enako mnogo elementov natanko tedaj, kadar se pri tem postopku sočasno "izčrpata". Na ta način smo poiskali bijektivno preslikavo med množicama.

V splošnem:

Množica A je *ekvipolentna* množici B natanko takrat, ko obstaja vsaj ena bijektivna preslikava množice A na množico B.

Oznaka:

$$A \sim B\,.$$

Pravimo tudi, da imata množici A in B isto moč.

Zgled:

$2\mathbb{N} = \{0, 2, 4, \ldots\}$, $\quad \mathbb{N} = \{0, 1, 2, \ldots\}$

$f : 2\mathbb{N} \to \mathbb{N}$, $f(2n) = 2n$, ni bijektivna preslikava.

$g : 2\mathbb{N} \to \mathbb{N}$, $g(2n) = n$, pa je! Torej sta množici ekvipolentni. ▲

Zgled:

Dana je množica X. Naj bo $\{0, 1\}^X$ množica vseh funkcij oblike $f : X \to \{0, 1\}$. Potem je $\{0, 1\}^X \sim \mathcal{P}(X)$.

Res: Oglejmo si preslikavo $F : \{0, 1\}^X \to \mathcal{P}(X)$, definirano s predpisom

$$F(f) = f^{-1}(1) = \{x \in X \ : \ f(x) = 1\}$$

za vse $f \in \{0, 1\}^X$. Preslikava F je bijektivna preslikava množice $\{0, 1\}^X$ na množico $\mathcal{P}(X)$:

- injektivnost:

  Pokazali bomo $(\forall f, g \in \{0, 1\}^X)(f \neq g \Rightarrow F(f) \neq F(g))$.

  Vzemimo različni funkciji f in g iz $\{0, 1\}^X$. Ker velja $\mathcal{D}f = \mathcal{D}g = X$, funkciji pa sta različni, obstaja tak $x \in X$, da velja $f(x) \neq g(x)$.

  Če je $f(x) = 1$, potem je $g(x) = 0$ in je $x \in f^{-1}(1) \setminus g^{-1}(1) = F(f) \setminus F(g)$, torej $F(f) \neq F(g)$.

  Če pa je $f(x) = 0$, potem je $g(x) = 1$ in je $x \in g^{-1}(1) \setminus f^{-1}(1) = F(g) \setminus F(f)$, torej spet $F(f) \neq F(g)$.

  V vsakem primeru je torej $F(f) \neq F(g)$.

- surjektivnost:

  Naj bo $A \in \mathcal{P}(X)$. Tedaj je očitno $F(\chi_A) = A$, kjer je $\chi_A : X \to \{0, 1\}$, **karakteristična funkcija** množice A, definirana s predpisom

$$\chi_A(x) = \begin{cases} 1, & \text{če je } x \in A; \\ 0, & \text{če je } x \notin A. \end{cases}$$

▲

Lastnosti ekvipolentne relacije

- $A \sim A$ *(refleksivnost)*

  (identiteta $i : A \to A$ je bijektivna)

- $A \sim B \Rightarrow B \sim A$ *(simetričnost)*

  (inverz bijektivne preslikave je bijektivna preslikava!

  Če je $f : A \stackrel{bij.}{\to} B$, potem je $f^{-1} : B \stackrel{bij.}{\to} A$)

- $A \sim B$ in $B \sim C \Rightarrow A \sim C$ *(tranzitivnost)*

  (Kompozitum bijektivnih preslikav je bijektivna preslikava!

  Če je $f : A \stackrel{bij.}{\to} B$ in $g : B \stackrel{bij.}{\to} C$, potem je $g \circ f : A \stackrel{bij.}{\to} C$)

Relacija ekvipolence $\sim$ je torej *ekvivalenčna relacija*!

$\boxed{A \sim B \text{ in } C \sim D \text{ in } A \cap C = \emptyset \text{ in } B \cap D = \emptyset \;\Rightarrow\; A \cup C \sim B \cup D}$

Dokaz. Naj bo $f : A \stackrel{bij.}{\to} B$ in $g : C \stackrel{bij.}{\to} D$.
Definirajmo $h : A \cup C \to B \cup D$ s predpisom

$$h(x) = \begin{cases} f(x), & \text{če je } x \in A; \\ g(x), & \text{če je } x \in C. \end{cases}$$

Preslikava h je bijektivna preslikava množice $A \cup C$ na množico $B \cup D$, vsak element iz množice $B \cup D$ je namreč slika natanko enega elementa iz množice $A \cup C$. □

$\boxed{A \sim B \text{ in } C \sim D \;\Rightarrow\; A \times C \sim B \times D}$

Dokaz. Naj bo $f : A \stackrel{bij.}{\to} B$ in $g : C \stackrel{bij.}{\to} D$.
Definirajmo $h : A \times C \to B \times D$ s predpisom

$$h(x, y) = (f(x), g(y)) \,.$$

Preslikava h je bijektivna preslikava množice $A \times C$ na množico $B \times D$:

- injektivnost:

  $h(x, y) = h(x', y') \Rightarrow (f(x), g(y)) = (f(x'), g(y')) \Rightarrow f(x) = f(x')$ in $g(y) = g(y')$

  $\Rightarrow x = x'$ in $y = y' \Rightarrow (x, y) = (x', y')$

- surjektivnost:

  Naj bo $(b, d) \in B \times D$. Ker sta f in g surjektivni, obstajata taka elementa $a \in A$ in $c \in C$, da velja $f(a) = b$ in $g(c) = d$. Torej je $(b, d) = (f(a), g(c)) = h(a, c)$.

□

$\boxed{A \times B \sim B \times A}$

Dokaz. Definirajmo $f : A \times B \to B \times A$ s predpisom

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

Preslikava f je bijektivna:

- injektivnost:

  $f(x, y) = f(x', y') \Rightarrow (y, x) = (y', x') \Rightarrow y = y'$ in $x = x' \;\Rightarrow (x, y) = (x', y')$.

- surjektivnost: $(b, a) \in B \times A$ je slika elementa (a, b).

□

Brez dokaza navedimo še nekaj lastnosti:

1. $(A \times B) \times C \sim A \times (B \times C)$.
2. $A \times \{a\} \sim A$.
3. Poljubnima dvema množicama X in Y lahko vedno priredimo dve *disjunktni* množici U in V, tako da velja $X \sim U$ in $Y \sim V$.

   Res: $U = X \times \{\emptyset\}$, $V = Y \times \{\{\emptyset\}\}$.
4. Spomnimo se, da s simbolom A^B označujemo množico vseh funkcij iz množice B v množico A.

   $A \sim C$ in $B \sim D \;\Rightarrow\; A^B \sim C^D$.

Domača naloga: Dokažite lastnosti 1. in 2.
V razmislek: Kako bi dokazali 4. lastnost?

Primerljivost množic

Ali bi lahko nad množicami definirali relacije, podobne relacijam $\leq, <, \geq, >$? Ali je možno množice smiselno primerjati med seboj glede na množino njihovih elementov?

Naj bosta A in B poljubni množici. V poštev pridejo naslednje štiri logične možnosti:

(1) Množica A ima vsaj eno podmnožico A_1, ki je ekvipolentna množici B, množica B pa nima nobene podmnožice, ki bi bila ekvipolentna množici A.

(2) Množica B ima vsaj eno podmnožico B_1, ki je ekvipolentna množici A, množica A pa nima nobene podmnožice, ki bi bila ekvipolentna množici B.

(3) Množica A ima vsaj eno podmnožico A_1, ki je ekvipolentna množici B, množica B pa ima vsaj eno podmnožico B_1, ki je ekvipolentna množici A.

(4) Množica A nima nobene podmnožice, ki bi bila ekvipolentna množici B, množica B pa nima nobene podmnožice, ki bi bila ekvipolentna množici A.

(1): Pravimo, da ima množica A *večjo moč* kot množica B.
(2): Množica B ima *večjo moč* kot množica A.
(1): $A > B$, (2): $B > A$

Neposredno iz definicije sledi, da je relacija $>$ irefleksivna, asimetrična in tranzitivna (je torej stroga delna urejenost)!

- $A \not> A$
- $A > B \Rightarrow B \not> A$
- $A > B$ in $B > C \Rightarrow A > C$

Če je $B > A$, potem zapišemo tudi $A < B$ in pravimo, da ima množica A *manjšo moč* kot množica B.

$$A < B \Leftrightarrow B > A\,.$$

Primer (3) obravnava naslednji izrek.

Schröder-Bernsteinov izrek: $$(3) \Rightarrow A \sim B\,.$$

(Dokaz kasneje.)
Komentar: Očitno velja $A \sim B \Rightarrow (3)$. (Lahko vzamemo kar $A_1 = A$, $B_1 = B$.) Schröder-Bernsteinov izrek pa trdi, da velja implikacija tudi v drugo smer.

Najbolj "problematičen" pa je primer (4):
(4): "A in B nista primerljivi niti glede na relacijo ekvipolence $\sim$ niti glede na relacijo "ima večjo moč kot" $>$"
Brž ko sprejmemo aksiom izbire, pa ta možnost dejansko nikoli ne nastopi!
Aksiom izbire $\Rightarrow$ Od poljubnih dveh množic A in B je vsaj ena izmed njiju ekvipolentna neki podmnožici druge.
(Brez dokaza. Za dokaz glej A.A. Fraenkel: Abstract Set Theory, North-Holland Publishing Company, Amsterdam 1953, str. 319–321.)

Zakon trihotomije:
Poljubni dve množici A in B sta primerljivi glede na njuno moč. Velja natanko ena izmed možnosti

$$A > B, \quad B > A \quad \textit{ali } A \sim B\,.$$

Velja:

Aksiom izbire $\Leftrightarrow$ zakon trihotomije.

Izrek (Schröder-Bernsteinov izrek)**.** *Dani sta množici A in B. Naj ima množica A vsaj eno podmnožico A_1, ki je ekvipolentna množici B, množica B pa vsaj eno podmnožico B_1, ki je ekvipolentna množici A. Potem je*

$$A \sim B\,.$$

Schröder-Bernsteinov izrek lahko ekvivalentno formuliramo na naslednji način, z obstojem injektivnih in bijektivnih preslikav med množicami.

Izrek. *Dani sta množici A in B. Če obstajata injektivni preslikavi $f : A \to B$ in $g : B \to A$, potem obstaja tudi bijektivna preslikava $h : A \to B$.*

Dokaz. Obstaja množica $A_1 \subseteq A$, da velja $A_1 \sim B$.

Obstaja množica $B_1 \subseteq B$, da velja $B_1 \sim A$.

Naj bosta $f : A \to B_1$ in $g : B \to A_1$ bijekciji.

Poiskali bomo taki podmnožici $A_0 \subseteq A$ in $B_0 \subseteq B$, da bo $f|_{A_0} : A_0 \to B_0$ bijekcija in $g|_{B \setminus B_0} : B \setminus B_0 \to A \setminus A_0$ bijekcija.

Potem bo sledilo:

$$A = A_0 \cup (A \setminus A_0) \sim B_0 \cup (B \setminus B_0) = B\,,$$

saj je $A_0 \cap (A \setminus A_0) = \emptyset$ in $B_0 \cap (B \setminus B_0) = \emptyset$.

Priredimo najprej vsaki podmnožici X množice A neko podmnožico X' množice A, in sicer takole:

$$X' = A \setminus g(B \setminus f(X))\,.$$

Velja:

$$X_1 \subseteq X_2 \Rightarrow X_1' \subseteq X_2'\,.$$

Res:

$X_1 \subseteq X_2 \Rightarrow Y_1 = f(X_1) \subseteq f(X_2) = Y_2 \Rightarrow$

$\Rightarrow B \setminus Y_2 \subseteq B \setminus Y_1 \Rightarrow g(B \setminus Y_2) \subseteq g(B \setminus Y_1) \Rightarrow$

$\Rightarrow X_1' = A \setminus g(B \setminus Y_2) \subseteq A \setminus g(B \setminus Y_1) = X_2'$.

$- - -$

Podmnožica $Z \subseteq A$ je *izbrana podmnožica*, če je

$$Z \subseteq Z'\,.$$

$\emptyset$ je izbrana podmnožica množice A!

Naj bo A_0 *unija vseh izbranih podmnožic množice* A!

Če je Z izbrana podmnožica, potem velja $Z \subseteq A_0 \Rightarrow Z' \subseteq A_0' \Rightarrow$

$$Z \subseteq Z' \subseteq A_0'\,.$$

Torej je tudi A_0 zajeta v A_0':

$$A_0 \subseteq A_0'$$

A_0 je torej izbrana podmnožica!

$A_0 \subseteq A_0' \Rightarrow A_0' \subseteq (A_0')' \Rightarrow A_0'$ je izbrana podmnožica $\Rightarrow A_0' \subseteq A_0$.

Dobimo torej

$$A_0 = A_0'\,.$$

S tem pa smo prišli do iskane množice A_0, ki jo funkcija f preslika bijektivno na množico B_0:

$$B_0 = f(A_0) \subseteq B\,.$$

Funkcija g pa preslika množico $B \setminus B_0$ bijektivno na množico $A \setminus A_0$:

$$g(B \setminus B_0) = g(B \setminus f(A_0)) = A \setminus A_0\,,$$

saj je $A_0 = A \setminus g(B \setminus f(A_0))$. □

Relacija $>$ je stroga delna urejenost.
V razmislek: Privzemimo zakon trihotomije.

- Naj bo $\gtrsim$ relacija na množicah, definirana s predpisom $A \gtrsim B \Leftrightarrow (A > B$ ali $A \sim B)$. Ali je ta relacija strogo sovisna? Ali je delna urejenost?
- Naj bo $\geq$ relacija na množicah, definirana s predpisom $A \geq B \Leftrightarrow (A > B$ ali $A = B)$. Ali je ta relacija strogo sovisna? Ali je delna urejenost?

Končne in neskončne množice

Za definicijo (nes)končnih množic je več možnosti. Če privzamemo aksiom izbire, so vse te možnosti med seboj ekvivalentne.

(S pomočjo naravnih števil.) Dana množica S je končna tedaj in le tedaj, ko obstaja tako naravno število n, da ima ta množica natanko n elementov. Če množica ni končna, je neskončna.

Slabosti:

– Definicija sloni na pojmu naravnega števila.

– Za nekatere množice lahko prav gotovo trdimo, da so končne, pa čeprav ne poznamo natančnega števila njihovih elementov. Npr.: množica vseh knjig, natisnjenih na Zemlji do leta 2015, je prav gotovo končna.

(Peirce in Dedekind.) Dana množica S je neskončna tedaj in le tedaj, če ima vsaj eno pravo podmnožico, ki ji je ekvipolentna. Če množica ni neskončna, je končna.

To definicijo lepo ponazarja t.i. *Hilbertov Veliki hotel:*

V hotelu z neskončno mnogo sobami (oštevilčenimi zaporedoma z $1, 2, 3, \ldots$) je v vsaki sobi nek gost. V hotel pride še nekaj gostov. Ali jih lahko razporedimo v sobe?

Oglejmo si dva primera:

- Pride končno mnogo gostov. Recimo, da jih pride 10.
  Gosta v sobi j premaknemo v sobo $j + 10$ za vse $j = 1, 2, 3, \ldots$
  Novih 10 gostov pa razporedimo v sobe $1, 2, \ldots, 10$, ki so medtem postale proste.
- Pride neskončno mnogo gostov $g_1, g_2, g_3, \ldots$
  Gosta v sobi j premaknemo v sobo $2j$ za vse $j = 1, 2, 3, \ldots$
  Nove goste pa razporedimo na naslednji način:
  $g_1 \mapsto 1$
  $g_2 \mapsto 3$

$g_3 \mapsto 5$

$\dots$

$g_j \mapsto 2j - 1$

Pri prerazporejanju "starih" gostov smo uporabili dejstvi, da je

$\{1, 2, 3, \dots\} \sim \{1, 2, 3, \dots\} \setminus \{1, \dots, 10\}$ in

$\{1, 2, 3, \dots\} \sim \{2, 4, 6, \dots\}$.

Pri razporejanju neskončno mnogo novih gostov pa še dejstvo, da je $\{1, 2, 3, \dots\} \sim \{1, 3, 5, \dots\}$.

(Tarski.) Minimalni element: a je minimalen element v S glede na relacijo R, če za noben drug element y te množice ne velja yRa.

Če je S poljubna množica, potem je vsaka družina njenih podmnožic z relacijo inkluzije $\subseteq$ delno urejena. Glede na to relacijo pa ta družina lahko ali ima ali pa nima minimalnega elementa. Minimalni element je v tem primeru taka podmnožica, ki nima nobene druge podmnožice iz te družine za svojo podmnožico!

Zgled: $A = \{1, 2, 3\}$.

Družina $\mathcal{D}_1 = \{\{1\}, \{1, 2\}, \{1, 2, 3\}\}$ ima en minimalen element: množico $\{1\}$.

Družina $\mathcal{D}_2 = \{\{1\}, \{2\}, \{1, 2\}, \{2, 3\}\}$ ima dva minimalna elementa: množico $\{1\}$ in množico $\{2\}$.

Vsaka neprazna družina podmnožic množice A ima vsaj en minimalen element glede na relacijo $\subseteq$.

Zgled: $\mathbb{N}^+ = \{1, 2, 3, \dots\}$.

Za $k \geq 1$ naj bo

$$\mathbb{N}_k = \mathbb{N}^+ \setminus \{1, 2, \dots, k\} = \{k + 1, k + 2, \dots\}.$$

Oglejmo si neprazno družino podmnožic

$$\mathcal{D} = \{\mathbb{N}_1, \mathbb{N}_2, \mathbb{N}_3, \dots\}.$$

Opazimo, da za vse $k \geq 1$ velja $\mathbb{N}_{k+1} \subseteq \mathbb{N}_k$. Torej $\mathcal{D}$ nima minimalnega elementa glede na $\subseteq$.

Definicija Tarskega: Dana množica S je končna tedaj in le tedaj, kadar ima vsaka neprazna družina podmnožic množice S vsaj en minimalen element glede na relacijo inkluzije "$\subseteq$". Če množica ni končna, je neskončna.

Končne množice

Primer:

- Množica $\{a, b\}$ je končna.
- Prazna množica $\emptyset$ je končna.

Očitno: Če je A končna množica in je $B \subseteq A$, potem je tudi B končna množica.

Posledica. *Če je A končna množica in B poljubna množica, potem sta $A \cap B$ in $A \setminus B$ končni množici.*

Lema. *Če sta A in B končni množici, potem je tudi njuna unija $A \cup B$ končna množica.*

Brez dokaza. Iz zgornje leme sledi:

Izrek. *Če je A končna množica, potem je tudi $A \cup \{x\}$ končna množica.*

Izrek. *Vsaka neprazna družina podmnožic kakšne končne množice ima vsaj en maksimalen element glede na relacijo inkluzije $\subseteq$.*

Dokaz. S protislovjem. Recimo, da obstajata končna množica A in taka neprazna družina $\mathcal{D}$ podmnožic množice A, ki nima nobenega maksimalnega elementa glede na relacijo inkluzije $\subseteq$.

Oglejmo si družino

$$\mathcal{F} = \{Z \ ; \ (Z = A \setminus X) \wedge X \in \mathcal{D}\} .$$

Ta družina očitno nima nobenega minimalnega elementa:

- Če bi bil $Z \in \mathcal{F}$ minimalen element družine $\mathcal{F}$, potem bi bil $X = A \setminus Z$ maksimalen element družine $\mathcal{D}$.

To pa je v protislovju s hipotezo, da je množica A končna. □

Izrek (Princip indukcije)**.** *Naj bo A končna množica in naj bo P lastnost, ki je smiselna za podmnožice množice A.*

Če velja $P(\emptyset)$ in če za vsak $x \in A$ in za vsak $X \subseteq A$ velja

$$P(X) \Rightarrow P(X \cup \{x\}) ,$$

potem

$$P(A) .$$

Dokaz. Naj bo

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

Ta družina podmnožic je neprazna, saj je $\emptyset \in \mathcal{D}$. Torej ima $\mathcal{D}$ vsaj en maksimalen element, označimo ga z M!

Če $M \neq A$, potem obstaja nek element $x \in A \setminus M$. Ker pa je $P(M)$, po predpostavki sledi $P(M \cup \{x\})$ in torej $M \cup \{x\} \in \mathcal{D}$. Ker je $M \subset M \cup \{x\}$, je to v nasprotju s predpostavko, da je M maksimalen.

Torej mora veljati $M = A \Rightarrow A \in \mathcal{D} \Rightarrow P(A)$. □

Posledica. *Naj bo A končna množica in $\mathcal{F}$ poljubna družina množic. Če velja $\emptyset \in \mathcal{F}$ in če za vsak $X \subseteq A$ in za vsak $x \in A$ velja sklep*

$$X \in \mathcal{F} \Rightarrow X \cup \{x\} \in \mathcal{F} ,$$

potem je $A \in \mathcal{F}$.

Dokaz. Uporabimo zgornji izrek za lastnost $P(X) =$ "$X \in \mathcal{F}$". □

Zgled:
Naj bo A končna množica, f pa funkcija, ki množico A *surjektivno* preslika na neko množico B. Potem je tudi B končna množica.

Res: naj bo $\mathcal{F} = \{X \ ; \ X \subseteq A \wedge f(X) \text{ končna}\}$.
$\emptyset \in \mathcal{F}$ ✓
$X \in \mathcal{F}, x \in A \Rightarrow f(X)$ končna $\Rightarrow f(X \cup \{x\}) = f(X) \cup \{f(x)\}$ končna!
Torej je $A \in \mathcal{F}$ in zato $f(A) = B$ končna množica. ✓ □

Poseben primer: f je bijektivna:

- A končna in $A \sim B \;\Rightarrow\; B$ končna.

Posledično:

- A neskončna in $A \sim B \;\Rightarrow\; B$ neskončna.

Brez dokaza navedimo še nekaj zanimivih lastnosti končnih množic:

- A končna $\;\Rightarrow\; \mathcal{P}(A)$ končna
- $\mathcal{D}$ končna družina končnih množic $\;\Rightarrow\; \cup\mathcal{D}$ končna.
- A končna, B neskončna $\;\Rightarrow\; A < B$
- A končna, B končna $\;\Rightarrow A \times B$ končna

Neskončne množice

Množica naravnih števil $\mathbb{N}$ je neskončna, saj je $\mathbb{N} \sim 2\mathbb{N}$.
$\mathbb{N}$ – model množice, ki ustreza *Peanovim aksiomom*:

1.) V množici $\mathbb{N}$ obstaja nek element, ki ga označimo z 0.

2.) Če $x \in \mathbb{N}$, potem obstaja natanko en element $x' \in \mathbb{N}$, ki ga imenujemo *neposredni naslednik* elementa x.

3.) Ne obstaja tak $x \in \mathbb{N}$, za katerega bi veljalo $x' = 0$.

4.) $x' = y' \Rightarrow x = y$.

5.) Če je $M \subseteq \mathbb{N}$ taka podmnožica, da velja (i) $0 \in M$ in (ii) $(x \in M \Rightarrow x' \in M)$, potem je $M = \mathbb{N}$.

Primer:
Množica
$$N = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots\}\,.$$
je *Peanova množica* (množica, ki ustreza vsem petim Peanovim aksiomom)!

1. $0 = \emptyset$
2. $A \in N \Rightarrow A' = A \cup \{A\}$.
3. $A \in N$, $A' = A \cup \{A\} = \emptyset$ – nesmisel!
4. $A \cup \{A\} = B \cup \{B\} \;\; \Rightarrow \;\; A = B$

   Če bi veljalo $A \neq B$, bi imeli $A \in B$ in $B \in A$, kar pa ni možno zaradi *aksioma regularnosti: Vsaka neprazna množica A ima vsaj en tak element x, da A in x nimata nobenega skupnega elementa.*

   Res: če je $A \neq B$, potem je $A \in B \cap \{A, B\}$ in $B \in A \cap \{A, B\}$. Po aksiomu regularnosti pa mora biti $A \cap \{A, B\} = \emptyset$ ali $B \cap \{A, B\} = \emptyset$.
5. Po konstrukciji: naj bo $N' \subseteq N$ taka podmnožica, da velja $0 \in N'$ in $(A \in N' \Rightarrow A \cup \{A'\} \in N')$. Potem je $N' = N$.

Na Peanovi množici

$$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots\} .$$

lahko definiramo strukturo stroge linearne urejenosti! Postavimo $A < B$ natanko tedaj, ko je množica A hkrati element in podmnožica množice B.

- Zgled:

  $\{\emptyset\} < \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$,

  saj je $\{\emptyset\} \in \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$,

  pa tudi $\{\emptyset\} \subseteq \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

Vsaka množica, ki je ekvipolentna množici naravnih števil, je *števno neskončna*.

Če je A števno neskončna množica, potem obstaja neka bijektivna preslikava $f : \mathbb{N} \to A$. Torej lahko množico A zapišemo kot

$$A = \{f(0), f(1), f(2), \ldots\} .$$

Izrek. *Vsaka neskončna množica ima vsaj eno števno neskončno podmnožico.*

Dokaz. Naj bo S neskončna množica in naj bo $S' \subset S$ prava podmnožica, ekvipolentna množici S.

Naj bo $f : S \to S'$ bijekcija.

Po predpostavki je $S \setminus S' \neq \emptyset$. Izberimo nek $a_0 \in S \setminus S'$.

$a_1 = f(a_0) \in S' \subset S$

$a_2 = f(a_1) \in S' \subset S$

$a_3 = f(a_2) \in S' \subset S$

itd.

$- - - - - - - - - - - - - - - - - -$

Na ta način dobimo množico

$$A = \{a_0, a_1, a_2, \ldots\}\,.$$

Pokažimo, da so vsi elementi $a_0, a_1, a_2, \ldots$ med seboj različni.

Pa recimo, da niso. Naj bo j prvi indeks, da je $a_i = a_j$ za nek $i < j$.

$a_0 \in S \setminus S'$ in $a_k \in S'$ za $k \geq 1 \;\Rightarrow\; i \neq 0$.

$a_i = f(a_{i-1})$, $a_j = f(a_{j-1})$

Ker je $a_i = a_j$ in je f injektivna $\Rightarrow$ $a_{i-1} = a_{j-1}$, to pa je protislovje z definicijo indeksa j.

Preslikava

$$g : A \to \mathbb{N}$$

$$g(a_i) = i$$

je torej bijekcija.

Sledi $A \sim \mathbb{N}$. □

Lastnosti števno neskončnih množic

Kako iz danih števno neskončnih množic "pridelamo" nove števno neskončne množice?

(1.) Če je A končna množica, B števno neskončna množica in $A \cap B = \emptyset$, potem je njuna unija $A \cup B$ števno neskončna.

$A = \{a_1, \ldots, a_k\}$, $B = \{b_0, b_1, \ldots, b_i, \ldots\}$

$A \cup B = \{a_1, \ldots, a_k, b_0, b_1, \ldots, b_i, \ldots\}$

$f : A \cup B \to B$

$f(a_1) = b_0$

$f(a_2) = b_1$

$\ldots$

$f(a_k) = b_{k-1}$

$f(b_0) = b_k$

$f(b_1) = b_{k+1}$

$\ldots$

Ta funkcija je očitno bijekcija!

Torej je množica $A \cup B$ števno neskončna.

(2.) Če sta A in B števno neskončni množici z $A \cap B = \emptyset$, potem je njuna unija $A \cup B$ števno neskončna množica.

$A \cup B = \{a_0, b_0, a_1, b_1, \ldots\}$

$f : A \cup B \to A$

$f(a_0) = a_0$

$f(b_0) = a_1$

$f(a_1) = a_2$

$f(b_1) = a_3$

...

f je bijekcija!

Torej je množica $A \cup B$ števno neskončna.

(3.) (nadaljevanje (2.))

Če množici A in B nista disjunktni, pa zapišemo unijo $A \cup B$ kot unijo dveh disjunktnih množic: $A \cup B = A \cup (B \setminus A)$. Če je množica $B \setminus A$ končna, uporabimo zgornji premislek, če pa je neskončna, potem je števno neskončna. V vsakem primeru je unija $A \cup B$ števno neskončna množica.

V razmislek: Pokažite veljavnost naslednje trditve:

Vsaka neskončna podmnožica števno neskončne množice je števno neskončna.

Posledica:

$A_1, \ldots, A_k$ množice, vsaka od njih je končna ali števno neskončna

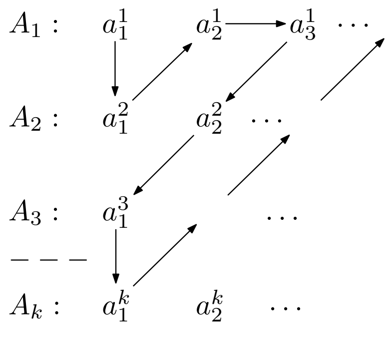
$\Rightarrow$ $A_1 \cup \cdots \cup A_k$ je števno neskončna (če je le vsaj ena od A_i števno neskončna), saj je

$$A_1 \cup \cdots \cup A_k = (\cdots((A_1 \cup A_2) \cup A_3) \cup \cdots \cup A_k)\,.$$

(4.) Danih je števno neskončno paroma disjunktnih števno neskončnih množic

$$A_1, A_2, A_3 \ldots$$

Njihova unija je števno neskončna:



Funkcija

$$f : \cup_k A_k \to \mathbb{N}$$

definirana s predpisom:

$f(a_1^1) = 0$

$f(a_1^2) = 1$

$f(a_2^1) = 2$

$f(a_3^1) = 3$

$f(a_2^2) = 4$

$f(a_1^3) = 5$

$\ldots$

je bijekcija!

Predpostavka, da so množice paroma disjunktne, ni bistvena. Če imajo te množice kakšne skupne elemente, potem preslikamo vsak tak element samo enkrat, namreč takrat, ko pride prvič na vrsto (pri nadaljnih pojavitvah pa ga preprosto izpustimo).

Zgledi števno neskončnih množic

Množica celih števil $\mathbb{Z}$ je števno neskončna (saj je $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$).

$- - - - - - - - - - - - - - - - - - - -$

Tudi *množica racionalnih števil* $\mathbb{Q}$ je števno neskončna!

Očitno je dovolj pokazati, da je množica pozitivnih racionalnih števil $\mathbb{Q}_+$ števno neskončna, saj je $\mathbb{Q} = \mathbb{Q}_- \cup \{0\} \cup \mathbb{Q}_+$ in je $\mathbb{Q}_- \sim \mathbb{Q}_+$.

Množico $\mathbb{Q}_+$ pa lahko zapišemo kot števno unijo števno neskončnih množic:

$$\mathbb{Q}_+ = A_1 \cup A_2 \cup \cdots$$

kjer je:

$A_1 = \{\frac{1}{1}, \frac{2}{1}, \frac{3}{1}, \ldots\}$,

$A_2 = \{\frac{1}{2}, \frac{2}{2}, \frac{3}{2}, \ldots\}$,

$A_3 = \{\frac{1}{3}, \frac{2}{3}, \frac{3}{3}, \ldots\}$, $\ldots$

Algebraično število: tako kompleksno število x, ki je rešitev kake enačbe oblike

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

kjer je $n \in \mathbb{N}$, $n \neq 0$, $a_n \neq 0$ in $a_i \in \mathbb{Z}$ za vse i. Tudi množica algebraičnih števil je števno neskončna. Zapišemo jo namreč lahko kot (števno neskončno) unijo končnih množic:

$$A_1 \cup A_2 \cup A_3 \cup \cdots\,,$$

kjer je A_k množica vseh kompleksnih števil, ki so rešitve kakšne enačbe zgornje oblike, pri čemer za njene koeficiente velja $n + |a_0| + |a_1| + \ldots + |a_n| \leq k$. Vsaka množica A_k je končna, saj vsebuje le ničle kvečjemu $(2k+1)^{k+1}$ polinomov stopnje $\leq k$ s koeficienti iz množice $\{-k, -(k-1), \ldots, k-1, k\}$, vsak od takih polinomov pa ima $\leq k$ ničel.

Neštevno neskončne množice

Množica realnih števil pa *ni števno neskončna*!

Pokažimo, da že množica realnih števil na intervalu

$$(0,1] = \{x \ ; \ x \in \mathbb{R} \land 0 < x \leq 1\}$$

ni števno neskončna.

$x \in (0,1] \Rightarrow$ x se da zapisati v obliki neskončnega decimalnega števila

$$0, a_1 a_2 a_3 \cdots ,$$

pri čemer se nikoli ne zgodi, da bi bila vsa števila od nekod naprej enaka 0:

$\frac{1}{2} = 0,5000\cdots = 0,4999\cdots$

$1 = 0,9999\cdots$

Recimo, da je $f : \mathbb{N} \to (0,1]$ bijekcija!

$f(0) = 0, a_1^0 a_2^0 \cdots$

$f(1) = 0, a_1^1 a_2^1 \cdots$

$- - --$

$f(k) = 0, a_1^k a_2^k \cdots a_{k-1}^k$

Definirajmo število $b \in (0,1]$, na naslednji način:

$$b = 0, b_1 b_2 b_3 \cdots$$

Če je $a_1^0 \neq 1$, naj bo $b_1 = 1$, če pa je $a_1^0 = 1$, naj bo $b_1 = 2$.

Če je $a_2^1 \neq 1$, naj bo $b_2 = 1$, če pa je $a_2^1 = 1$, naj bo $b_2 = 2$.

$- - --$

Če je $a_k^{k-1} \neq 1$, naj bo $b_k = 1$, če pa je $a_k^{k-1} = 1$, naj bo $b_k = 2$.

Očitno je $b \in (0,1]$ in

$b \neq f(0)$ (saj $b_1 \neq a_1^0 = (f(0))_1$),

$b \neq f(1)$ (saj $b_2 \neq a_2^1 = (f(1))_2$),

$- - --$

$b \neq f(k)$ (saj $b_{k+1} \neq a_{k+1}^k = (f(k))_{k+1}$).

Število b torej ni v zalogi vrednosti preslikave f. To pa je protislovje s surjektivnostjo!

Interval $(0,1]$ torej ni števno neskončna množica (in zato tudi $\mathbb{R}$ ni). $\square$

Pravkar podanemu argumentu pravimo "Diagonalni dokaz" (tudi diagonalizacija, diagonalni argument, ... Cantor, 1891).

Poiščimo sedaj nekaj pravih podmnožic množice realnih števil, ki so vse ekvipolentne množici realnih števil.

Naslednje preslikave so vse bijektivne:

- $f_1 : (0,1] \to [0,1)$, $f_1(x) = 1 - x$
- $f_2 : [0,1) \to [0,\infty)$, $f_2(x) = \frac{x}{1-x}$
- $f_3 : (-1,0] \to (-\infty,0]$, $f_3(x) = \frac{x}{1+x}$
- $f_4 : (-1,1) \to \mathbb{R}$, $f_4(x) = \begin{cases} f_2(x), & \text{če je } x \geq 0; \\ f_3(x), & \text{sicer.} \end{cases}$

Domača naloga: preverite bijektivnost preslikav f_1, f_2, f_3, f_4.

– – – – – – – – – – – – – – – – – –

Sledi:

$$(0,1] \sim [0,1) \sim [0,\infty)$$

$$(-1,0] \sim (-\infty,0]$$

Ker je tudi $(-1,0] \sim [0,1)$ (saj je preslikava $f:(-1,0] \to [0,1)$, $f(x) = -x$ bijektivna), sledi

$$(0,1] \sim [0,1) \sim [0,\infty) \sim (-1,0] \sim (-\infty,0]\,.$$

Zaradi preslikave f_4 pa je

$$(-1,1) \sim \mathbb{R}\,.$$

Ali so morda vse te množice med seboj ekvipolentne? Do pritrdilnega odgovora nam pomaga naslednja

Trditev. *Če neskončni množici S odvzamemo končno ali števno neskončno mnogo elementov, potem je dobljena množica ekvipolentna S, če je le neskončna.*

Dokaz. Naj bo $S_0 \subseteq S$ taka končna ali števno neskončna podmnožica množice S, da je množica $S_1 = S \setminus S_0$ neskončna. Naj bo S_2 števno neskončna podmnožica v S_1. Lahko zapišemo

$$S_1 = S_2 \cup S_3\,,$$

kjer je $S_2 \cap S_3 = \emptyset$. (Vzamemo $S_3 = S_1 \setminus S_2$.)

$S = S_0 \cup S_1 = S_0 \cup S_2 \cup S_3$

Definirajmo preslikavo f:

$$f : S = S_0 \cup S_2 \cup S_3 \to S_1 = S_2 \cup S_3$$

- Na S_3 naj bo f identiteta:

  $f(x) = x$ za vse $x \in S_3$.

- Množici $S_0 \cup S_2$ in S_2 sta obe števno neskončni, torej obstaja bijekcija $g : S_0 \cup S_2 \to S_2$.

  Za $x \in S_0 \cup S_2$ pa definiramo $f(x) = g(x)$.

Očitno je f bijekcija. □

– – – – – – – – – – – – – – – – – –

Sledi:

$$[0,1] \sim [0,1) \sim (0,1] \sim (0,1) \sim (-1,1) \sim \mathbb{R}$$

(Ekvipolenco $(0,1) \sim (-1,1)$ lahko dokažemo npr. z bijektivno preslikavo $f:(0,1) \to (-1,1)$, $f(x) = 2x - 1$. [4])

[4] Podobno bi lahko pokazali tudi v splošnem, da sta poljubna dva intervala (a,b) in (c,d) ekvipolentna.

ž Vsaka množica, ki je ekvipolentna množici realnih števil $\mathbb{R}$, ima **moč kontinuuma**. Ker množica realnih števil ni števno neskončna, velja:

$$\mathbb{R} > \mathbb{N}!$$

$- - - - - - - - - - - - - - - - - - -$

Tudi množica vseh realnih števil, ki niso algebraična (to so t.i. *transcendentna števila*), ima, po prejšnji trditvi, moč kontinuuma! Torej je transcendentnih števil prav toliko kot realnih, algebraičnih pa bistveno manj.

Izkaže se, da obstajajo množice, ki imajo večjo moč kot množica realnih števil.

Izrek (Cantorjev izrek)**.** *Naj bo S poljubna množica. Potem velja*

$$\mathcal{P}(S) > S\,.$$

Dokaz. 1. Množica $\mathcal{P}(S)$ ima vsaj eno podmnožico, ki je ekvipolentna množici S.

- Taka množica je npr. množica vseh enoelementnih podmnožic

$$\{\{x\}\ ;\ x \in S\}\,.$$

2. Množica S nima nobene podmnožice, ki bi bila ekvipolentna množici $\mathcal{P}(S)$.
Recimo, da obstaja $S' \subseteq S$ in bijektivna preslikava $f : S' \to \mathcal{P}(S)$.
$s' \in S' \Rightarrow f(s') \in \mathcal{P}(S) \Rightarrow f(s') \subseteq S$.
Dve možnosti: $s' \in f(s')$ ali pa $s' \notin f(s')$.
Naj bo

$$X = \{s'\ ;\ s' \in S' \wedge s' \notin f(s')\}\,.$$

S tem smo definirali množico $X \subseteq S$ oziroma $X \in \mathcal{P}(S)$. Ker je f surjektivna preslikava, obstaja tak element $x \in S'$, da je $f(x) = X$.
Toda:

$$x \in X \quad \text{ali} \quad x \in S' \setminus X\,.$$

- $x \in X \Rightarrow x \notin f(x) = X$. Protislovje.
- $x \in S' \setminus X \Rightarrow x \in f(x) = X$. Protislovje.

Torej f ni bijekcija! □

$- - - - - - - - -$

Velja $\mathcal{P}(\mathbb{N}) \sim \mathbb{R}$.

Domneva kontinuuma: *Ne obstaja množica X, za katero bi veljalo*

$$\mathbb{N} < X < \mathbb{R}\,.$$

(*Ne obstaja množica, ki bi imela večjo moč kot $\mathbb{N}$, a manjšo kot $\mathbb{R}$.*)
Gödel (1940): domneva kontinuuma je konsistentna z drugimi aksiomi teorije množic.

Cohen (1963): domneva kontinuuma je nedokazljiva iz drugih aksiomov teorije množic!

Posplošena domneva kontinuuma: *Naj bo S neskončna množica. Ne obstaja množica X, za katero bi veljalo*

$$S < X < \mathcal{P}(S)\,.$$

Za konec omenimo še nekaj pojmov, povezanih z neskončnimi množicami (ki jih ne bomo obravnavali):

- *kardinalna števila* ("moči" množic; omogočajo študij hierarhije različnih neskončnosti),
- *tipi urejenosti* (različni "načini", kako so lahko množice strogo linearno urejene, npr. $(\mathbb{N},<)$, $(\mathbb{N},>)$, $(\mathbb{Q},<)$, $(\mathbb{R},<)$),
- *ordinalna števila* (tipi urejenosti dobro urejenih množic),
- *princip transfinitne indukcije* (posplošitev principa indukcije na poljubne dobro urejene množice).

Za uvodno obravnavo teh pojmov glej knjigi Nika Prijatelja in Paula Halmosa.

Konec.