Diskretne strukture I

zapiski predavanj - prezentacija

doc. dr. R. Škrekovski

Izjavni račun

Vsebina

1. Enostavne in sestavljene izjave;

2. Izjavni vezniki: negacija, konjunkcija, disjunkcija, implikacija, ekvivalenca, ...;

3. Izjavni izrazi kot formalizem izjav;

4. Resničnostna tabela, tavtologija, protislovje;

5. Enakovrednost izjav, zakoni izjavnega računa;

6. Disjunktivna normalna oblika (DNO) in konjunktivna normalna oblika (KNO);

7. Polni nabori izjavnih veznikov;

8. Sklepanje: pravilni in nepravilni sklepi, sklepi iz pogovornega področja;

9. Pravila sklepanja;

10. Pomožni sklepi: pogojni sklep, sklep s protislovjem, analiza primerov.

Izjavni račun

Izjava je stavek, ki je bodisi resničen ali neresničen.

Zgledi:

- Zunaj dežuje.
- DS1 je lahko narediti.
- Če zunaj sneži, potem ne grem na faks.
- Če se ne učim, potem letnika ne naredim.

Vsak stavek **ni** izjava. Recimo:

- Zapri vrata!
- Bodi tiho!
- Kaj bo za večerjo?

Izjave po **vsebini** ločimo na

- **resnične**: 6 ni praštevilo;
- **neresnične**: 6 je praštevilo.

Izjave po **zgradbi** ločimo na

- **osnovne:** Zunaj sije sonce. Peter sedi na vrtu.
- **sestavljene:** Če zunaj sije sonce, Peter sedi na vrtu.

Izjavni vezniki

Izjave sestavljamo z **izjavnimi vezniki**. Pri tem zahtevamo, da je resničnost sestavljene izjave enolično določena z resničnostjo njenih sestavnih delov.

n-izjavni veznik je neka n-člena operacija v množici $\{0,1\}$, oziroma to je preslikava oblike $F : \{0,1\}^n \to \{0,1\}$.

Zgled: Preslikava F je trimestna operacija oz. trimestni veznik.

p	q	r	$F(p,q,r)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Ponavadi uporabljamo naslednje veznike:

- **0-mestne:** 1 (resnica) in 0 (neresnica)
- **1-mestne:** $\neg$ (negacija)
- **2-mestne:** $\wedge$ (konjunkcija) , $\vee$ (disjunkcija), $\Rightarrow$ (implikacija), $\Leftrightarrow$ (ekvivalenca) , $\oplus$ (ekskluzivna disjunkcija), $\uparrow$ (Shefferjev veznik), $\downarrow$ (Lukasiewiczev veznik).

Opomba: Dvomestne izjavne veznike pišemo infiksno.

Negacija $\neg A$

Beremo: *ne A* oz. *ni res, da (velja) A*

A	$\neg A$
0	1
1	0

Velja: $\neg A$ je resnična natanko takrat, ko je A neresnična.

Konjunkcija $A \wedge B$

Beremo: *A in B*

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

Velja: $A \wedge B$ je resnična natanko takrat, ko sta obe izjavi A in B resnični.

Disjunkcija $A \vee B$

Beremo: *A ali B*

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

Velja: $A \vee B$ je resnična natanko takrat, ko je vsaj ena od izjav A in B resnična.

Implikacija $A \Rightarrow B$

Beremo: *iz A sledi B* oz. *če A, potem B* oz. *A implicira B*

A	B	$A \Rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

Izjavi A pravimo **antecedens**, izjavi B pa **konsekvens**.

Velja: $A \Rightarrow B$ je neresnična le v primeru, ko je A resnična in B neresnična.

Ekvivalenca $A \Leftrightarrow B$

Beremo: *A ekvivalentna B* oz. *A, če in samo če B* oz. *A natanko tedaj, ko B*

A	B	$A \Leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

Velja: $A \Leftrightarrow B$ resnična, kadar imata A in B enako vrednost.

Naloga 1 *Koliko je n-mestnih izjavnih veznikov?*

Zgled: V tabeli je naštetih vseh 16 dvomestnih izjavnih veznikov.

A	0	0	1	1	
B	0	1	0	1	
	0	0	0	0	0
	0	0	0	1	$A \wedge B$
	0	0	1	0	$\neg(A \Rightarrow B)$
	0	0	1	1	A
	0	1	0	0	$\neg(B \Rightarrow A)$
	0	1	0	1	B
	0	1	1	0	$A \oplus B$
	0	1	1	1	$A \vee B$
	1	0	0	0	$A \downarrow B$
	1	0	0	1	$A \Leftrightarrow B$
	1	0	1	0	$\neg B$
	1	0	1	1	$B \Rightarrow A$
	1	1	0	0	$\neg A$
	1	1	0	1	$A \Rightarrow B$
	1	1	1	0	$A \uparrow B$
	1	1	1	1	1

Dogovor o prednosti veznikov

Če ni z oklepaji drugače določeno, potem:

- $\neg$ veže močneje kot $\wedge$
- $\wedge$ veže močneje kot $\vee$
- $\vee$ veže močneje kot $\Rightarrow$
- $\Rightarrow$ veže močneje kot $\Leftrightarrow$
- Levi nastop veznika veže močneje od desnega nastopa istega veznika

Zgledi: Izraz

$$p \wedge \neg q \Rightarrow r \Leftrightarrow \neg\neg p \vee q$$

identificiramo z

$$((p \wedge (\neg q)) \Rightarrow r) \Leftrightarrow ((\neg(\neg p)) \vee q).$$

Podobno, izraz

$$p \Rightarrow q \Rightarrow r \Rightarrow s \Rightarrow t$$

identificiramo z

$$(((p \Rightarrow q) \Rightarrow r) \Rightarrow s) \Rightarrow t.$$

Izraz

$$p \Rightarrow q \vee \neg r \Leftrightarrow p \wedge s$$

pa pomeni isto kot

$$(p \Rightarrow (q \vee (\neg r))) \Leftrightarrow (p \wedge s).$$

Naloga 2 *Poenostavi naslednje izraze tako, da odstraniš odvečne oklepaje:*

- $((p \vee (\neg q)) \Leftrightarrow (r \Rightarrow p))$

- $(((p \vee q) \Leftrightarrow (r \wedge s)) \Rightarrow (\neg t))$

Izjavni izrazi

Izjavne izraze definiramo induktivno:

1. vsaka izjavna spremenljivka je izjavni izraz;
2. če je F n-mestni izjavni veznik in so $A_1, \ldots, A_n$ izjavni izrazi, je tudi $F(A_1, \ldots, A_n)$ izjavni izraz.

Zgledi: $0,\ \ 1,\ p,\ q,\ \neg p,\ q \wedge (p \Rightarrow \neg r),\ p \Rightarrow q \Rightarrow p.$

Opomba. Vsak izjavni izraz določa neko izjavo, zato jim bomo rekli kar izjave. Več različnih izjavnih izrazov lahko določa isto izjavo.

Resničnostna tabela

Naj bodo $p_1, p_2, \ldots, p_n$ izjavne spremenljivke, ki nastopajo v izjavnem izrazu A. Potem vrednosti A predstavimo v tabeli z 2^n vrsticami, ki ustrezajo vsem naborom vrednosti spremenljivk $p_1, p_2, \ldots, p_n$. Tako tabelo imenujemo **resničnostna tabela** izjave A.

Zgled:

p	q	r	$(p \vee \neg q)$	$\Leftrightarrow$	$(r \Rightarrow p)$
0	0	0	1	**1**	1
0	0	1	1	**0**	0
0	1	0	0	**0**	1
0	1	1	0	**1**	0
1	0	0	1	**1**	1
1	0	1	1	**1**	1
1	1	0	1	**1**	1
1	1	1	1	**1**	1

Tavtologija, protislovje

Izjavni izraz A je

1. **tavtologija**, če je resničen pri vseh naborih vrednosti izjavnih spremenljivk;
2. **protislovje**, če je neresničen pri vseh naborih vrednosti izjavnih spremenljivk;
3. **nevtralen**, če ni niti tavtologija niti protislovje.

Da je izjava A tavtologija, označimo z $\models A$.

Zgledi:

- tavtologije: 1, $p \vee \neg p$, $(p \Rightarrow q) \vee (q \Rightarrow p)$, ...
- protislovja: 0, $p \wedge \neg p$, ..., negacije tavtologij;
- nevtralni izrazi: p, $p \Rightarrow q \vee r$, ...

Naloga 3 *Sestavi resničnostne tabele ter ugotovi, kakšni sta naslednji dve izjavi:*

$$p \wedge (p \Rightarrow q) \Rightarrow q \qquad \textit{in} \qquad p \wedge \neg(p \vee q)$$

Enakovredne izjave

Izjavna izraza A in B sta **enakovredna**, če imata pri vseh naborih vrednosti izjavnih spremenljivk enako vrednost. V tem primeru pišemo $A \sim B$.

Zgled: Izraza $p \Rightarrow q$ in $\neg q \Rightarrow \neg p$ sta enakovredna.

p	q	$p \Rightarrow q$	$\neg q$	$\Rightarrow$	$\neg p$
0	0	**1**	1	**1**	1
0	1	**1**	0	**1**	1
1	0	**0**	1	**0**	0
1	1	**1**	0	**1**	0

Trditev 1 *Velja*

$$A \sim B \text{ natanko takrat, ko je } \models A \Leftrightarrow B$$

Dokaz. Sklepamo takole:

A in B sta enakovredna, n.t.k.

A in B sta vedno enake vrednosti (v tabeli), n.t.k.

$A \Leftrightarrow B$ ima vedno vrednost 1, n.t.k.

$A \Leftrightarrow B$ je tavtologija. □

Vprašanje 1 *Ali je izjava*

$$p \Rightarrow q \Leftrightarrow \neg q \Rightarrow \neg p$$

tavtologija?

Enakovrednost izjav $\sim$ je ekvivalenčna relacija:

- **refleksivnost:** $A \sim A$
- **simetričnost:** če je $A \sim B$, potem je tudi $B \sim A$
- **tranzitivnost:** če je $A \sim B$ in $B \sim C$, potem je tudi $A \sim C$.

Naloga 4 *S pomočjo resničnostnih tabel ugotovi ali sta izjavi enakovredni:*

$$p \vee (p \wedge q) \qquad in \qquad p \wedge (p \vee r)$$

Zakoni izjavnega računa

Naj bodo A, B, C poljubni izjavni izrazi.

- **Lastnosti** 0 **in** 1**:**

$$\begin{array}{lll} A \wedge 0 \sim 0 & A \Rightarrow 0 \sim \neg A & A \Leftrightarrow 0 \sim \neg A \\ A \wedge 1 \sim A & A \Rightarrow 1 \sim 1 & A \Leftrightarrow 1 \sim A \\ A \vee 0 \sim A & 0 \Rightarrow A \sim 1 & \neg 0 \sim 1 \\ A \vee 1 \sim 1 & 1 \Rightarrow A \sim A & \neg 1 \sim 0 \end{array}$$

- **dvojna negacija:** $\neg\neg A \sim A$
- **idempotentnost:**

$$\begin{array}{ll} A \wedge A \sim A & A \Rightarrow A \sim 1 \\ A \vee A \sim A & A \Leftrightarrow A \sim 1 \end{array}$$

- **komutativnost:**

$$\begin{array}{ll} & A \vee B \sim B \vee A \\ A \Leftrightarrow B \sim B \Leftrightarrow A & A \wedge B \sim B \wedge A \end{array}$$

- **asociativnost:**

$$\begin{aligned} (A \vee B) \vee C &\sim A \vee (B \vee C) \\ (A \wedge B) \wedge C &\sim A \wedge (B \wedge C) \\ (A \Leftrightarrow B) \Leftrightarrow C &\sim A \Leftrightarrow (B \Leftrightarrow C) \end{aligned}$$

- **absorpcija:**

$$A \vee (A \wedge B) \sim A \qquad A \wedge (A \vee B) \sim A$$

- **distributivnost:**

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

- **De Morganova zakona:**

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

- **kontrapozicija:**

$$A \Rightarrow B \ \sim \ \neg B \Rightarrow \neg A \ \sim \ \neg A \vee B$$

- **ekvivalenca:**

$$\begin{aligned} A \Leftrightarrow B \ &\sim \ (A \Rightarrow B) \wedge (B \Rightarrow A) \\ &\sim \ (\neg A \vee B) \wedge (A \vee \neg B) \\ &\sim \ (A \wedge B) \vee (\neg A \wedge \neg B) \end{aligned}$$

Zgled: Pokažimo z izpeljavo, da je $p \ \Rightarrow \ q \ \sim \ \neg q \ \Rightarrow \ \neg p$ takole:

$$p \Rightarrow q \ \sim \ \neg p \vee q \ \sim \ \neg p \vee \neg\neg q \ \sim \ \neg\neg q \vee \neg p \ \sim \ \neg q \Rightarrow \neg p \, .$$

Naloga 5 *Pokaži z izpeljavo, da je izjava*

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

tavtologija.

Naloga 6 *Preveri zakon asociativnosti za implikacijo:*

$$(p \Rightarrow q) \Rightarrow r \ \sim \ p \Rightarrow (q \Rightarrow r)?$$

Izbrane oblike izjav

Najprej bomo poskusili odgovoriti na naslednje vprašanje:

Vprašanje 2 *Kako za predpisano resničnostno tabelo poiščemo ustrezno izjavo?*

Naj $A(p)$ pomeni, da je vrednost (sestavljene) izjave A lahko odvisna od vrednosti enostavne izjave oz. spremenljivke p. Naj bosta $A(0)$ in $A(1)$ izjavi, ki ju dobimo, če v izjavi A zamenjamo vse nastope spremenljivke p z 0 oziroma 1.

Trditev 2 *Velja,*

$$A(p) \quad \sim \quad (p \wedge A(1)) \ \vee \ (\neg p \wedge A(0))\,.$$

Dokaz. Enostavna izjava p ima lahko le dve vrednosti 0 in 1, zato obravnavamo ti dve možnosti ločeno.

Če je $p \sim 0$, potem je desna stran

$$0 \wedge A(1) \vee \neg 0 \wedge A(0) \ \sim \ 0 \vee 1 \wedge A(0) \ \sim \ 1 \wedge A(0) \ \sim \ A(0)\,.$$

Podobno za $p \sim 1$, dobimo

$$1 \wedge A(1) \vee \neg 1 \wedge A(0) \ \sim \ A(1) \vee 0 \wedge A(0) \ \sim \ A(1) \vee 0 \ \sim \ A(1)\,.$$

V obeh primerih je izjava na desni strani enakovredna izjavi na levi strani. S tem je trditev dokazana. □

Vprašanje 3 *Kako zgornjo trditev posplošimo na primer dveh enostavnih izjav p in q,*

$A(p, q) \ = \ ?$

Zgled: Recimo da imamo predpisano spodnjo tabelo. Poiščimo A.

p	q	A
0	0	1
0	1	1
1	0	0
1	1	1

Če je A odvisna od n enostavnih izjav $p_1, p_2, \ldots, p_n$, potem A zapišemo takole

$$
\begin{aligned}
&A(p_1, p_2, \ldots, p_{n-1}, p_n) \ \sim \\
&\quad A(1,1,\ldots,1,1) \wedge p_1 \wedge p_2 \wedge \cdots \wedge p_{n-1} \wedge p_n \\
&\vee\ A(1,1,\ldots,1,0) \wedge p_1 \wedge p_2 \wedge \cdots \wedge p_{n-1} \wedge \neg p_n \\
&\vee\ A(1,1,\ldots,0,1) \wedge p_1 \wedge p_2 \wedge \cdots \wedge \neg p_{n-1} \wedge p_n \\
&\vee\ A(1,1,\ldots,0,0) \wedge p_1 \wedge p_2 \wedge \cdots \wedge \neg p_{n-1} \wedge \neg p_n \\
&\ \vdots \qquad\qquad \vdots \qquad\qquad\qquad\qquad \vdots \qquad\qquad \vdots \\
&\vee\ A(0,0,\ldots,0,1) \wedge \neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_{n-1} \wedge p_n \\
&\vee\ A(0,0,\ldots,0,0) \wedge \neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_{n-1} \wedge \neg p_n
\end{aligned}
$$

Zgornja zveza nam poda postopek, kako lahko poljubno izjavo (podano s tabelo) zapišemo v povezavi z $\neg$, $\wedge$, $\vee$. Od tukaj sklepamo da velja:

Izrek 3 *Vsaka izjava se da zapisati samo z vezniki* $\neg$, $\wedge$, $\vee$ *ter enostavnimi izjavami od katerih je odvisna.*

Disjunktivna normalna oblika - DNO

Osnovna konjunkcija je konjunkcija izjavnih spremenljivk in/ali njihovih negacij.

Zgled: $p \wedge q$, $p \wedge \neg q \wedge r$ so osnovne konjunkcije; izjava $p \wedge (q \vee r)$ pa ni.

Disjunktivna normalna oblika (krajše **DNO**) izjave A je enakovredni izjavni izraz, ki je disjunkcija osnovnih konjunkcij.

Zgled: Izraz $\neg p \wedge q \ \vee \ p \wedge q$ je DNO za izjavo A iz tabele:

p	q	A
0	0	0
0	1	1
1	0	0
1	1	1

Kako naredimo DNO

DNO za s tabelo podano izjavo A zgradimo tako, da za vsak nabor pravilnostne tabele, pri katerem je izraz A resničen, priredimo eno osnovno konjunkcijo spremenljivk in/ali njihovih negacij glede na to ali je ustrezni nastop 1 oz. 0. Na koncu naredimo disjunkcijo izbranih osnovnih konjunkcij.

Zgled: Poiščimo DNO za izjavo A iz tabele:

p	q	r	A
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

Opazimo, da je A resnična v 2., 4., 5., 6. ter 8. vrstici. Za vsako od teh vrstic vzamemo ustrezno konjunkcijo ter vse te konjunkcije združimo z disjunkcijo ter tako dobimo A. Torej,

$$\begin{aligned} A \sim \quad & (\neg p \wedge \neg q \wedge r) \\ \vee \; & (\neg p \wedge q \wedge r) \\ \vee \; & (p \wedge \neg q \wedge \neg r) \\ \vee \; & (p \wedge \neg q \wedge r) \\ \vee \; & (p \wedge q \wedge r) \end{aligned}$$

Izrek 4 *Vsak izjavni izraz, ki ni protislovje, ima DNO.*

Konjunktivna normalna oblika - KNO

Osnovna disjunkcija je disjunkcija izjavnih spremenljivk in/ali njihovih negacij.

Zgled: $p \vee q$, $p \vee \neg q \vee r$ so osnovne disjunkcije; izjava $p \vee (q \wedge r)$ pa ni.

Konjunktivna normalna oblika (krajše **KNO**) izjave A je enakovredni izjavni izraz, ki je konjunkcija osnovnih disjunkcij.

Zgled: Izraz $p \vee q \ \wedge \ \neg p \vee q$ je KNO za izjavo A iz tabele:

p	q	A
0	0	0
0	1	1
1	0	0
1	1	1

Kako naredimo KNO

KNO za s tabelo podano izjavo A zgradimo tako, da za vsak nabor pravilnostne tabele, pri katerem je izraz A **ne**resničen, priredimo eno osnovno disjunkcijo spremenljivk in/ali njihovih negacij glede na to ali je ustrezni nastop 0 oz. 1. Na koncu naredimo konjunkcijo izbranih osnovnih disjunkcij.

Zgled: Poiščimo KNO za izjavo A iz tabele:

p	q	r	A
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

Opazimo, da je A neresnična v 1., 3., ter 7. vrstici. Za vsako od teh vrstic vzamemo ustrezno disjunkcijo, ter vse te disjunkcije združimo s konjunkcijo. Torej,

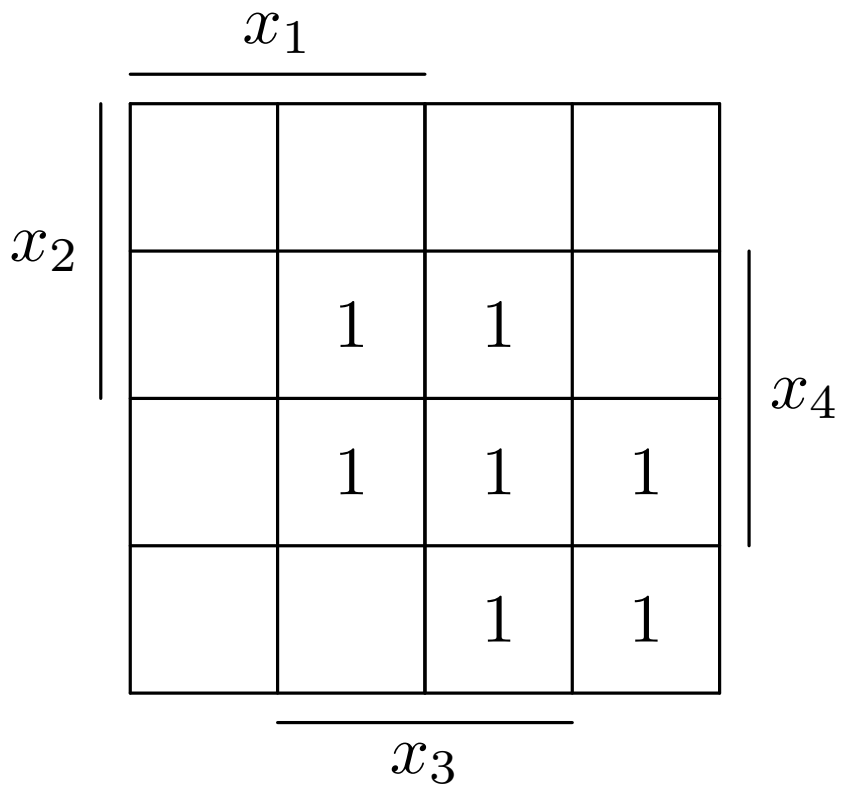
$$\begin{aligned} A \sim \quad & (p \quad \vee \quad q \vee r) \\ \wedge \; & (p \quad \vee \neg q \vee r) \\ \wedge \; & (\neg p \vee \neg q \vee r) \end{aligned}$$

Izrek 5 *Vsak izjavni izraz, ki ni tavtologija, ima KNO.*

Trditev 6 *Velja naslednja zveza*

$$\mathrm{KNO}(A) = \neg \mathrm{DNO}(\neg A)$$

Veitchevi diagrami



Veitchev postopek minimizacije:

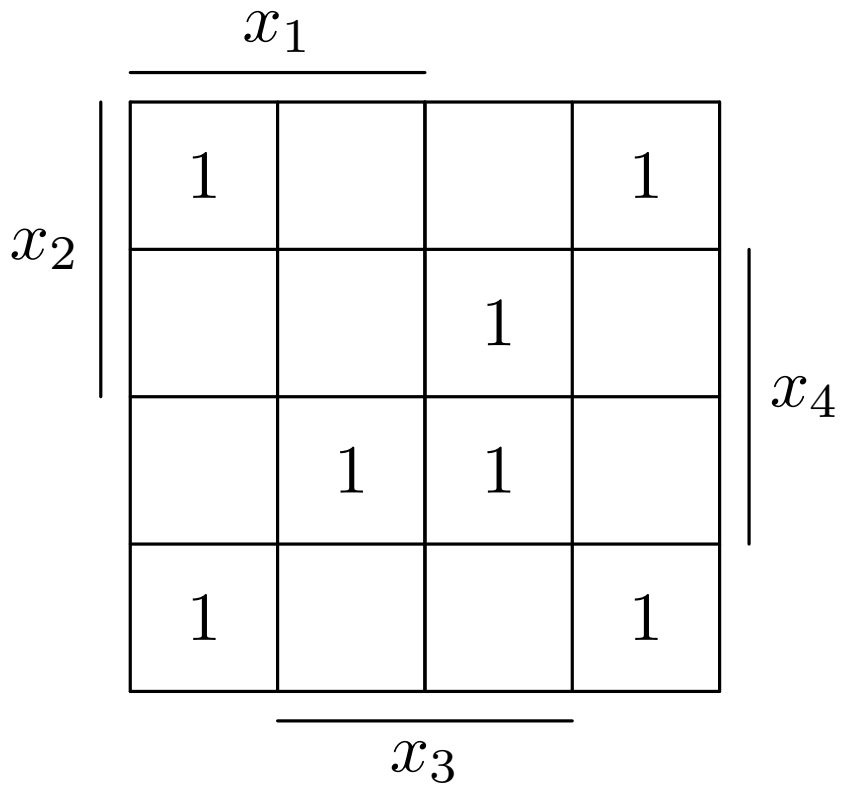
- Resničnostno tabelo napišemo v dvorasežni obliki (na torusu).
- Enojke pokrijemo s pravokotniki, ki vsebujejo 1, 2, 4, 8, 16, ... kvadratkov. Pri tem uporabimo:
  - čim manj pravokotnikov;
  - čim večje pravokotnike.
- Vsak pravokotnik ustreza neki konjunkciji. Dobljene konjunkcije povežemo disjunktivno.

Dobljeno obliko izraza imenujemo **minimalna disjunktivna normalna oblika (MDNO).**

Zgled: Poišči MDNO za izraz podan s tabelo:

p	q	r	F
0	0	0	**1**
0	0	1	**0**
0	1	0	**0**
0	1	1	**1**
1	0	0	**1**
1	0	1	**1**
1	1	0	**1**
1	1	1	**1**

Zgled: Poišči MDNO za izraz podan z diagramom:



Polni nabori

Množica N izjavnih veznikov je **poln nabor**, če za vsak izjavni izraz A obstaja enakovreden izjavni izraz B, ki vsebuje samo veznike iz N.

Zgledi: $\{\neg, \wedge, \vee\}$ je poln nabor po izreku 3.

Ker

$$a \vee b \ \sim \ \neg(\neg a \wedge \neg b)$$

sledi, da je $\{\neg, \wedge\}$ poln nabor.

Podobno, ker

$$a \wedge b \ \sim \ \neg(\neg a \vee \neg b)$$

sledi, da je $\{\neg, \vee\}$ poln nabor.

Kako ugotovimo, da je dani nabor poln?

Trditev 7 *Naj bo Z znan poln nabor izjavnih veznikov in N neka množica izjavnih veznikov. Če lahko vsak veznik iz Z izrazimo samo z vezniki iz N, je tudi N poln nabor.*

Dokaz. Naj bo A poljuben izjavni izraz. Ker je Z poln nabor, obstaja izraz B, ki je enakovreden A ter vsebuje samo veznike iz Z. V B vsak veznik iz Z izrazimo z vezniki iz N, dobimo izraz $C \sim B$. Ker je $C \sim A$, sklepamo, da je N poln nabor. □

Naloga 7 *Pokaži, da sta $\{\neg, \Rightarrow\}$ in $\{0, \Rightarrow\}$ polna nabora.*

Rešitev:

Še trije izjavni vezniki

Stroga (ekskluzivna) disjunkcija $A \oplus B$ oz. $A \veebar B$ oz. A XOR B

Beremo: *bodisi A bodisi B* oz. *natanko ena izmed izjav A in B je resnična*

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Velja: $A \oplus B$ je resnična natanko takrat, ko je $A \Leftrightarrow B$ neresnična.

Velja tudi

$$(A \oplus B) \oplus C \quad \sim \quad A \oplus (B \oplus C)\,.$$

Shefferjev veznik $A \uparrow B$ oz. A NAND B

Beremo: *ne A ali ne B* oz. *vsaj ena od izjav A, B ni resnična*

A	B	$A \uparrow B$
0	0	1
0	1	1
1	0	1
1	1	0

Velja: $A \uparrow B$ je resnična natanko takrat, ko je $A \wedge B$ neresnična.

Lukasiewiczev veznik $A \downarrow B$ oz. $A \operatorname{NOR} B$

Beremo: *niti A niti B* oz. *nobena od izjav A, B ni resnična*

A	B	$A \downarrow B$
0	0	1
0	1	0
1	0	0
1	1	0

Velja: $A \downarrow B$ je resnična natanko takrat, ko je $A \vee B$ neresnična.

Dogovor o prednosti veznikov $\oplus$, $\uparrow$ ter $\downarrow$

- Ekskluzivna disjunkcija $\oplus$ veže tako močno kot navadna disjunkcija $\vee$;
- Shefferjev in Lukasiewiczev veznik vežeta enako močno kot konjunkcija $\wedge$.

Zgledi: Izraz

$$A \vee B \oplus C \vee D$$

identificiramo z

$$((A \vee B) \oplus C) \vee D\,.$$

Izraz

$$A \uparrow B \wedge C \downarrow D \uparrow E$$

pa pomeni isto kot

$$(((A \uparrow B) \wedge C) \downarrow D) \uparrow E\,.$$

Izrek 8 $\{\uparrow\}$ *in* $\{\downarrow\}$ *sta polna nabora izjavnih veznikov.*

Dokaz. Pokažimo najprej, da je $\{\uparrow\}$ poln nabor. Spomnimo se, da je $A \uparrow B \sim \neg(A \wedge B)$.

Vemo, da je $\{\neg, \wedge\}$ poln nabor. Zato bo dovolj, če izrazimo $\neg$ in $\wedge$ s $\uparrow$.
Negacijo izpeljemo takole

$$A \uparrow A \sim \neg(A \wedge A) \sim \neg A\,.$$

Ker je

$$\neg(A \uparrow B) \sim \neg\neg(A \wedge B) \sim A \wedge B,$$

konjunkcijo zapišemo takole:

$$A \wedge B \sim (A \uparrow B) \uparrow (A \uparrow B).$$

Zdaj se lotimo nabora $\{\downarrow\}$ podobno kot $\{\uparrow\}$. Vemo, da je $\{\neg, \vee\}$ poln nabor. Zato bo dovolj, če izrazimo $\neg$ in $\vee$ z $\downarrow$.
Negacijo izpeljimo takole

$$A \downarrow A \sim \neg(A \vee A) \sim \neg A\,.$$

Ker je

$$\neg(A \downarrow B) \sim \neg\neg(A \vee B) \sim A \vee B\,,$$

disjunkcijo zapišemo takole:

$$A \vee B \sim (A \downarrow B) \downarrow (A \downarrow B)\,.$$

□

Trditev 9 *Nabor* $\{\wedge, \Rightarrow\}$ *ni poln.*

Dokaz. Uporabimo naslednjo lastnost: če imata spremenljivki p in q vrednost 1, potem imata vrednost 1 tudi izjavi $p \wedge q$ ter $p \Rightarrow q$. Naj bo sedaj $A(p_1, p_2, \ldots, p_n)$ poljuben izjavni izraz, v katerem nastopata kot izjavna veznika samo $\wedge$ in $\Rightarrow$. Po omenjeni lastnosti, velja $A(1, 1, \ldots, 1) \sim 1$.

Iz tega sledi, da izjave B za katero velja $B(1, 1, \ldots, 1) \sim 0$ ni možno zapisati v naboru $\{\wedge, \Rightarrow\}$. □

Naloga 8 *Pokaži, da nabor* $\{\neg, \Leftrightarrow\}$ *ni poln.*

Naloga 9 *V naboru* $\{\downarrow\}$ *zapiši izjave*

$$p \Rightarrow q \wedge r \quad \text{in} \quad p \Rightarrow q \Rightarrow r\,.$$

Sklepanje

Zgled: Ali je spodnji sklep pravilen?

$A.1$	Ta žival ima krila ali pa ni ptič.
$A.2$	Če je ta žival ptič, potem leže jajca.
$A.3$	Ta žival nima kril!
$B.$	Torej ta žival ne leže jajc.

Formalizirajmo sklep tako, da vpeljemo naslednje spremenljivke:

- $p \equiv$ ta žival ima krila;
- $q \equiv$ ta žival je ptič;
- $r \equiv$ ta žival leže jajca.

Končno lahko sklep zapišemo v izjavnem računu takole:

$A1.$	$p \vee \neg q$
$A2.$	$q \Rightarrow r$
$A3.$	$\neg p$
$B.$	$\neg r$

Zgornji sklep je veljaven, če velja: kadar so vse predpostavke A_1, A_2, A_3 resnične, je resničen tudi zaključek B.

Zaporedje izjavnih izrazov $A_1, A_2, \ldots, A_n, B$ je **pravilen sklep** s **predpostavkami** $A_1, A_2, \ldots, A_n$ in **zaključkom** B, če je zaključek resničen pri vseh tistih naborih vrednosti izjavnih spremenljivk, pri katerih so resnične vse prepodstavke.

Pišemo:

$$A_1,\ A_2,\ \ldots,\ A_n \ \models\ B$$

in beremo:

Iz predpostavk A_1, A_2, ..., A_n logično sledi zaključek B.

Zgled: Preverimo sklep

$$p \vee \neg q,\ r \Rightarrow q,\ \neg p \ \models\ \neg r$$

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

Naslednji izrek nam prevede problem sklepanja na problem ugotavljanja tavtologije.

Izrek 10 *Sklep*

$$A_1,\, A_2,\, \ldots,\, A_n \;\models\; B$$

velja natanko tedaj, ko

$$\models A_1 \,\wedge\, A_2 \wedge \cdots \wedge A_n \Rightarrow B$$

Dokaz. Naj bo $\mathcal{A} = A_1 \wedge A_2 \wedge \cdots \wedge A_n$. Najprej predpostavimo, da je sklep veljaven. Iz definicije veljavnosti sklepa izhaja: če je zaključek B lažen, potem je lažna vsaj ena od predpostavk A_i. Torej v tem primeru

$$\mathcal{A} \Rightarrow B \;\sim\; 0 \Rightarrow 0 \;\sim\; 1\,.$$

V nasprotnem primeru, ko je zaključek B resničen, pa vedno velja

$$\mathcal{A} \Rightarrow B \;\sim\; \mathcal{A} \Rightarrow 1 \;\sim\; 1\,.$$

Tako pridemo do zaključka, da je izjava $\mathcal{A} \Rightarrow B$ tavtologija.

Zdaj pokažimo izrek v drugo smer. Naj bo $\models \mathcal{A} \Rightarrow B$ in naj bodo vse predpostavke A_i resnične. Tedaj je resnična tudi izjava $\mathcal{A}$. Ker je $\mathcal{A} \Rightarrow B \;\sim\; 1$ sledi, da je $B \;\sim\; 1$. To pa pomeni, da je sklep $\mathcal{A} \;\models\; B$ veljaven. □

Zgled: Po izreku sledi, da je naš sklep

$$p \vee \neg q,\, r \Rightarrow q,\, \neg p \;\models\; \neg r$$

pravilen natanko takrat, ko je izjava

$$(p \vee \neg q) \wedge (r \Rightarrow q) \wedge \neg p \Rightarrow \neg r$$

tavtologija.

Pravila sklepanja

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

Zgled: Preverimo veljavnost sklepa (HS)

A	B	C	$A \Rightarrow B$	$B \Rightarrow C$	$A \Rightarrow C$
0	0	0			
0	0	1			
0	1	0			
0	1	1			
1	0	0			
1	0	1			
1	1	0			
1	1	1			

Dokazovanje pravilnosti sklepov

Pravilnost sklepa

$$A_1,\ A_2,\ \ldots,\ A_n \ \models\ B$$

lahko dokažemo tudi tako, da sestavimo zaporedje izjavnih izrazov

$$C_1,\ C_2,\ C_3, \ldots, C_{m-1}, C_m$$

kjer je $C_m = B$ in za $i = 1, \ldots, m$ velja:

(a) C_i je ena od predpostavk; ali

(b) C_i je tavtologija; ali

(c) C_i je enakovreden enemu od predhodnih izrazov v zaporedju; ali

(d) C_i logično sledi iz predhodnih izrazov v zaporedju po enem od osnovnih pravilnih sklepov.

Zgled: Dokažimo naslednji sklep:

$$p \Rightarrow q,\ p \vee r,\ q \Rightarrow s,\ r \Rightarrow t,\ \neg s \ \models\ t\,.$$

1.	$p \Rightarrow q$	predpostavka
2.	$p \vee r$	predpostavka
3.	$q \Rightarrow s$	predpostavka
4.	$r \Rightarrow t$	predpostavka
5.	$\neg s$	predpostavka
6.	$p \Rightarrow s$	HS$(1, 3)$
7.	$\neg p$	MT$(6, 5)$
8.	r	DS$(2, 7)$
9.	t	MP$(4, 8)$

Kako pokažemo, da sklep NI pravilen?

Poiščimo protiprimer, t.j. nabor vrednosti izjavnih spremenljivk, pri katerem so vse predpostavke resnične, zaključek pa ne.

Zgled: Preverimo veljavnost začetnega sklepa o ptičih, jajcih in krilih:

$$p \vee \neg q,\ q \Rightarrow r,\ \neg p \ \models\ \neg r$$

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

Pomožni sklepi

Pogojni sklep (PS)

Pogojni sklep uporabljamo, kadar ima zaključek sklepa obliko implikacije.

Trditev 11 *Sklep*

$$A_1,\, A_2,\, \ldots,\, A_n \;\models\; B \Rightarrow C$$

velja natanko tedaj, ko velja sklep

$$A_1,\, A_2,\, \ldots,\, A_n,\, B \;\models\; C\,.$$

Dokaz. Označimo $\mathcal{A} = A_1 \wedge A_2 \wedge \cdots \wedge A_n$. Zadošča pokazati, da je

$$\models \mathcal{A} \Rightarrow (B \Rightarrow C)$$

natanko tedaj, ko je

$$\models \mathcal{A} \wedge B \Rightarrow C\,.$$

To pa je res, saj velja

$$\begin{aligned} \mathcal{A} \Rightarrow (B \Rightarrow C) &\sim \neg\mathcal{A} \vee (\neg B \vee C) \\ &\sim (\neg\mathcal{A} \vee \neg B) \vee C \\ &\sim \neg(\mathcal{A} \wedge B) \vee C \\ &\sim (\mathcal{A} \wedge B) \Rightarrow C \end{aligned}$$

□

Zgled: S pomočjo pogojnega sklepa dokažimo naslednji sklep

$$p \Rightarrow q \vee r,\ \neg r \ \models\ p \Rightarrow q\,.$$

1.	$p \Rightarrow q \vee r$	predpostavka
2.	$\neg r$	predpostavka
3.1.	$\quad p$	predpostavka PS
3.2.	$\quad q \vee r$	MP$(1, 3.1)$
3.3.	$\quad q$	DS$(3.2, 2)$
3.	$p \Rightarrow q$	PS$(3.1, 3.3)$

Sklepanje s protislovjem - reduction ad absurdum (RA)

Sklepanje s protislovjem lahko uporabimo kadarkoli.

Trditev 12 *Sklep*

$$A_1,\, A_2,\, \ldots,\, A_n \;\models\; B$$

velja natanko tedaj, ko velja sklep

$$A_1,\, A_2,\, \ldots,\, A_n,\, \neg B \;\models\; 0\,.$$

Dokaz. Kot prej naj bo $\mathcal{A} = A_1 \wedge A_2 \wedge \cdots \wedge A_n$. Zadošča pokazati, da je

$$\models \mathcal{A} \Rightarrow B$$

natanko tedaj, ko je

$$\models \mathcal{A} \wedge \neg B \Rightarrow 0\,.$$

To pa je res, saj velja

$$\begin{aligned} \mathcal{A} \wedge \neg B \;\Rightarrow\; 0 \;&\sim\; \neg(\mathcal{A} \wedge \neg B) \vee 0 \\ &\sim\; \neg\mathcal{A} \vee B \\ &\sim\; \mathcal{A} \Rightarrow B\,. \end{aligned}$$

□

Zgled: S pomočjo RA dokažimo naslednji sklep:

$$p \Rightarrow \neg(q \Rightarrow r),\ (s \wedge q) \Rightarrow r,\ s \ \models\ \neg p\,.$$

1.	$p \Rightarrow \neg(q \Rightarrow r)$		predpostavka
2.	$(s \wedge q) \Rightarrow r$		predpostavka
3.	s		predpostavka
4.1.		$\neg\neg p$	predpostavka(RA)
4.2.		p	$\sim$ 4.1
4.3.		$\neg(q \Rightarrow r)$	MP$(1, 4.2)$
4.4.		$q \wedge \neg r$	$\sim$ 4.3
4.5.		q	Po(4.4)
4.6.		$\neg r$	Po(4.4)
4.7.		$s \wedge q$	Zd$(3, 4.5)$
4.8.		r	MP$(2, 4.7)$
4.9.		0	Zd$(4.8, 4.6)$
4.	$\neg p$		RA$(4.1, 4.9)$

Zgled: S pomočjo RA dokažimo naslednji sklep:

> Če nočem jutri zamuditi pouka, moram zgodaj vstati; če pa grem nocoj na žur, se bom vrnil pozno. Če se bom pozno vrnil in zgodaj vstal, bom spal le 5 ur. Ne morem si privoščiti samo 5 ur spanja. Potemtakem bom moral zamuditi pouk ali pa se odpovedati žuru.

Označimo enostavne izjave, ki nastopajo v sklepu, takole:

- $p \equiv$ jutri ne bom zamudil pouka;
- $q \equiv$ zjutraj bom zgodaj vstal;
- $r \equiv$ nocoj grem na žur;
- $s \equiv$ nocoj se bom pozno vrnil;
- $t \equiv$ spal bom le 5 ur.

Potem sklep zapišemo takole:

$$(p \Rightarrow q) \wedge (r \Rightarrow s),\ (s \wedge q) \Rightarrow t,\ \neg t \ \models\ \neg(p \wedge r)\,.$$

1.	$(p \Rightarrow q) \wedge (r \Rightarrow s)$	predpostavka
2.	$(s \wedge q) \Rightarrow t$	predpostavka
3.	$\neg t$	predpostavka
4.1.	$p \wedge r$	predpostavka(RA)
4.2.	p	Po(4.1)
4.3.	$p \Rightarrow q$	Po(1)
4.4.	q	MP(4.2, 4.3)
4.5.	r	Po(4.1)
4.6.	$r \Rightarrow s$	Po(1)
4.7.	s	MP(4.5, 4.6)
4.8.	$s \wedge q$	Zd(4.4, 4.7)
4.9.	t	MP(2, 4.8)
4.10.	$\neg t \wedge t \sim 0$	Zd(3, 4.9)
4.	$\neg(p \wedge r)$	RA(4.1, 4.10)

Analiza primerov (AP)

Analizo primerov uporabljamo, kadar ima ena od predpostavk obliko disjunkcije.

Trditev 13 *Sklep*

$$A_1,\, A_2,\, \ldots,\, A_n,\, B_1 \vee B_2 \;\models\; C$$

velja natanko tedaj, ko veljata oba sklepa

$$A_1,\, A_2,\, \ldots,\, A_n,\, B_1 \;\models\; C \quad \textit{in} \quad A_1,\, A_2,\, \ldots,\, A_n,\, B_2 \;\models\; C\,.$$

Dokaz. Spet naj bo $\mathcal{A} = A_1 \wedge A_2 \wedge \cdots \wedge A_n$. Zadošča pokazati, da je

$$\models \mathcal{A} \wedge (B_1 \vee B_2) \Rightarrow C$$

natanko tedaj, ko je

$$\models \mathcal{A} \wedge B_1 \Rightarrow C \quad \text{in} \quad \models \mathcal{A} \wedge B_2 \Rightarrow C\,.$$

oziroma, ko je

$$\models (\mathcal{A} \wedge B_1 \Rightarrow C) \;\wedge\; (\mathcal{A} \wedge B_2 \Rightarrow C)\,.$$

To pa velja

$$\begin{aligned}
\mathcal{A} \wedge (B_1 \vee B_2) \Rightarrow C \;&\sim\; \neg(\mathcal{A} \wedge (B_1 \vee B_2)) \vee C \\
&\sim\; \neg(\mathcal{A} \wedge B_1 \vee \mathcal{A} \wedge B_2) \vee C \\
&\sim\; (\neg(\mathcal{A} \wedge B_1) \wedge \neg(\mathcal{A} \wedge B_2)) \vee C \\
&\sim\; (\neg(\mathcal{A} \wedge B_1) \vee C) \wedge (\neg(\mathcal{A} \wedge B_2)) \vee C) \\
&\sim\; (\mathcal{A} \wedge B_1 \Rightarrow C) \wedge (\mathcal{A} \wedge B_2 \Rightarrow C)\,.
\end{aligned}$$

□

Zgled: S pomočjo AP dokažimo naslednji sklep:

$$p \Rightarrow r,\ q \Rightarrow r,\ p \vee q \models\ r\,.$$

1.	$p \Rightarrow r$		predpostavka
2.	$q \Rightarrow r$		predpostavka
3.	$p \vee q$		predpostavka
4.1.1.		p	predpostavka AP
4.1.2.		r	MP(1, 4.1.1)
4.2.1.		q	predpostavka AP
4.2.2.		r	MP(2, 4.2.1)
4.	r		AP(3, 4.1.2, 4.2.2)

Opomba. Analizo primerov lahko posplošimo na disjunkcijo večih členov takole:

Trditev 14 *Sklep*

$$\mathcal{A}, B_1 \vee B_2 \vee \cdots \vee B_m\ \models\ C$$

velja natanko tedaj, ko velja vsak od sklepov

$$\mathcal{A}, B_1\ \models\ C \quad in \quad \mathcal{A}, B_2\ \models\ C \quad in \cdots in \quad \mathcal{A}, B_m\ \models\ C\,.$$

Opomba. Analiza primerov je zelo priročna, kadar imamo dve ali več predpostavk disjunkcije. Velja namreč tole:

Trditev 15 *Sklep*

$$\mathcal{A}, B_1 \vee B_2, C_1 \vee C_2 \models D$$

velja natanko tedaj, ko velja vsak od štirih sklepov

$$\mathcal{A}, B_1, C_1 \models D\,, \qquad \mathcal{A}, B_1, C_2 \models D\,,$$
$$\mathcal{A}, B_2, C_1 \models D\,, \qquad \mathcal{A}, B_2, C_2 \models D\,.$$

Predikatni račun

Vsebina

1. Domena in predikati;
2. Kvantifikatorji;
3. Sintaksa predikatnega računa;
4. Zaprte izjavne formule;
5. Interpretacija oz. semantika predikatnega računa;
6. Tavtologije ter enakovredne izjave;
7. Prenexna normalna oblika;
8. Sklepanje v predikatnem računu.

Predikatni račun

Ali je spodnji sklep pravilen?

1. Vsi zajci ljubijo korenje.
2. Feliks je zajec.

---

3. Torej Feliks ljubi korenje.

Zgornji sklep se nam po občutku zdi pravilen, vendar ga v izjavnem računu prevedemo le takole:

1. p
2. q

---

3. r

ker nobena od izjav ne vsebuje veznikov. Izjavni sklep je očitno nepravilen za $p = q = 1$, $r = 0$.

Težava je v tem, da v izjavnem računu izgubimo zveze med izjavami oz. njihovo notranjo zgradbo:

- p in q govorita o "zajcih";
- q in r govorita o "Feliksu";
- p in r pa o "ljubezni do korenja";

V predikatnem računu to popravimo z upoštevanjem notranje zgradbe osnovnih izjav. Najprej označimo:

- $Z(x) \equiv x$ je zajec;
- $L(x) \equiv x$ ljubi korenje;
- $a \equiv$ Feliks;

Zdaj zgornji sklep zapišemo v obliki:

$$\begin{array}{ll} 1. & \forall x : (Z(x) \Rightarrow L(x)) \\ 2. & Z(a) \\ \hline 3. & L(a) \end{array}$$

V predikatnem računu je to pravilen sklep.

Nastopajoči simboli:

- Z, L sta enomestna **predikata**;
- x je **individualna spremenljivka**;
- a je **individualna konstanta**;
- $\forall$ je univerzalni **kvantifikator**.

Domena in predikati

Domena oz. **področje pogovora** $\mathcal{D}$ je neprazna množica, iz katere izbiramo individualne konstante oz. individue.

n-mestni predikat $P : \mathcal{D}^n \to \{0, 1\}$ je n-mestna funkcija iz pogovornega področja $\mathcal{D}$, ki vsaki n-terici individuov priredi vrednost 1 (resnica) oz. 0 (neresnica).

Manj formalno: V izjavah predikati predstavljajo lastnosti oz. odnose med individui iz področja pogovora.

Če je P 1-mestni predikat potem predstavlja neko lastnost individuov iz področja pogovora.

Zgled: Naj bo $P(x)$ predikat "x je praštevilo", področje pogovora pa naj bo množica naravnih števil $\mathbb{N}$. Potem,

- $P(6) = 0$;
- $P(3) = 1$.

Če je P n-mestni predikat za $n \geq 2$, potem predstavlja relacijo oz. odnos med n individui iz področja pogovora. Tako za $P(a_1, a_2, \ldots, a_n)$ rečemo, da so $a_1, a_2, \ldots, a_n$ v odnosu oz. relaciji P.

Zgled: Naj bo $V(x, y, z)$ predikat "x je vsota y in z", področje pogovora pa naj bo množica naravnih števil $\mathbb{N}$.

- $V(6, 3, 2) = 0$;
- $V(6, 4, 2) = 1$.

Kvantifikatorji

Poznamo dva kvantifikatorja: $\forall$ - univerzalni ter $\exists$ - eksistenčni.

$\forall x \equiv$ za vsak x,

$\exists x \equiv$ obstaja tak x, da

Ko hočemo poudariti, da je x iz področja pogovora $\mathcal{D}$, zapišemo:

$$\forall x \in \mathcal{D} \qquad \text{in} \qquad \exists x \in \mathcal{D}$$

Zgled: Naj bo $P(x)$ predikat "x je praštevilo", področje pogovora pa naj bodo naravna števila $\mathbb{N}$:

$\forall x : P(x)$	Vsako naravno število je praštevilo.
$\exists x : P(x)$	Vsaj eno naravno število je praštevilo.
$\forall x : \neg P(x)$	Nobeno naravno število ni praštevilo.
$\neg \exists x : P(x)$	Ni res, da obstaja vsaj eno praštevilo.
$\exists x : \neg P(x)$	Vsaj eno naravno število ni praštevilo.
$\neg \forall x : P(x)$	Ni res, da je vsako naravno število praštevilo.

Vprašanje 4 *Katere od zgornjih izjav povedo eno in isto?*

Še nekaj prevodov:

$S(x) \equiv x$ je študent; $U(x) \equiv x$ se uči;

Vsi študentje se učijo	$\forall x : (S(x) \Rightarrow U(x))$
Noben študent se ne uči	$\forall x : (S(x) \Rightarrow \neg U(x))$
Nekateri študentje se učijo	$\exists x : (S(x) \wedge U(x))$
Nekateri študentje se ne učijo	$\exists x : (S(x) \wedge \neg U(x))$

V splošnem si pomagamo z naslednjim obrazcem:

Vsi A so B	$\forall x : (A(x) \Rightarrow B(x))$
Noben A ni B	$\forall x : (A(x) \Rightarrow \neg B(x))$
Nekateri A so B	$\exists x : (A(x) \wedge B(x))$
Nekateri A niso B	$\exists x : (A(x) \wedge \neg B(x))$

Omejeni oz. pogojni kvantifikatorji. Pogosto imamo opraviti z več množicami oz. domenami hkrati. Zato je smiselno vpeljati:

- $\forall x \in A : P(x)$ pomeni $\forall x : (A(x) \Rightarrow P(x))$;
- $\exists x \in A : P(x)$ pomeni $\exists x : (A(x) \wedge P(x))$.

Zgornje prevode lahko zapišemo takole:

Vsi študentje se učijo	$\forall x \in S : U(x)$
Noben študent se ne uči	$\forall x \in S : \neg U(x)$
Nekateri študentje se učijo	$\exists x \in S : U(x)$
Nekateri študentje se ne učijo	$\exists x \in S : \neg U(x)$

Sintaksa predikatnega računa

Izjavni račun ne zadošča za analizo pravilnega sklepanja, zato jezik izjavnega računa razširimo.

Jezik 1. reda je določen z množico simbolov $\mathcal{S}$, množico termov $\mathcal{T}$ in množico izjavnih formul $\mathcal{F}$.

I. Simboli

Množico simbolov $\mathcal{S}$ sestavljajo:

1. **individualne spremenljivke:** $x, y, z, \ldots, x_1, x_2, \ldots$
2. **individualne konstante:** $a, b, c, \ldots, a_1, a_2, \ldots$
3. **predikati:** $P, Q, R, \ldots, P_1, P_2, \ldots$
   So enomestni, dvomestni, itn.
4. **funkcijski simboli:** $f, g, h, \ldots, f_1, f_2, \ldots$
   So tudi enomestni, dvomestni, itn.
5. **izjavni vezniki:** $\neg$, $\wedge$, $\vee$, $\ldots$
6. **kvantifikatorja:** $\forall$ in $\exists$
7. **ločila:** ( ) : ,

II. Termi

Množica termov $\mathcal{T}$ je podana induktivno takole:

1. Vsaka individualna spremenljivka je term.
2. Vsaka individualna konstanta je term.
3. Če je f n-mestni funkcijski simbol in so $t_1, t_2, \ldots, t_n$ termi, potem je $f(t_1, t_2, \ldots, t_n)$ term.

Zgled: x, a, 1, $f(a, x)$, $f(a, b)$, $x + 3$, $g(x, f(b, y))$ so termi.

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

Zgled: V zgornjem zgledu so zaprti termi le a, 1 in $f(a, b)$.

III. Izjavne formule

Množica izjavnih formul $\mathcal{F}$ je definirana induktivno takole:

1. Če je P neki n-mestni predikat in so $t_1, t_2, \ldots, t_n$ termi, potem je $P(t_1, t_2, \ldots, t_n)$ izjavna formula.
2. Če sta Z in Y izjavni formuli, potem so tudi:

   $$\neg(Z),\ (Z) \wedge (Y),\ (Z) \vee (Y),\ (Z) \Rightarrow (Y), \ldots$$

   izjavne formule.
3. Če je Y formula in x individualna spremenljivka, potem sta

   $$(\forall x : Y) \qquad \text{in} \qquad (\exists x : Y)$$

   izjavni formuli.

Zgled: $P(x), P(a), Q(x, y), \forall x : P(x), \forall x : P(x) \wedge \forall y : Q(b, y)$ so izjavne formule.

Dogovor o prednosti in opuščanje ločil:

- Kvantifikatorji vežejo močneje kot izjavni vezniki;
- Dvopičje pred kvantifikatorjem opuščamo.

Zgledi:

- $\forall x\, \exists y : Q(x, y, z) \Rightarrow \exists y : P(y, z, x)$
- $\forall x\, \exists y : (Q(x, y, z) \Rightarrow \exists y : P(y, z, x))$

Doseg kvantifikatorjev

Območje delovanja ali **doseg** kvantifikatorja v izjavni formuli je najkrajše nadaljevanje za kvantifikatorjem, ki je samo zase izjavna formula.

Zgledi: :

$$\forall x : \underline{P(x)} \vee Q(x)$$

$$\forall x : \underline{(P(x, y) \Rightarrow \exists y : \underline{Q(y)})}$$

$$\forall x : \underline{(P(x) \wedge \exists x : \underline{Q(x, z)} \Rightarrow \exists y : \underline{R(x, y)})} \vee Q(x, y)$$

Zaprte izjavne formule oz. izjave

Nastop spremenljivke v izjavni formuli je **vezan**, če

- se nahaja tik za kvantifikatorjem; ali
- je v dosegu kvantifikatorja, ki se nanaša nanjo.

Sicer je nastop **prost**.

Zgledi:

$$\forall x : P(x) \vee Q(x)$$
$$\forall x : (P(x, y) \Rightarrow \exists y : Q(y))$$
$$\forall x : (P(x) \wedge \exists x : Q(x, z) \Rightarrow \exists y : R(x, y))$$

Izjavna formula je **zaprta**, če ne vsebuje prostih nastopov individualnih spremenljivk. Zaprti formuli rečemo **izjava**.

Zgledi: Naslednje izjavne formule so zaprte:

- $P(a)$
- $\exists x : P(x)$
- $\forall x \exists y : (P(x, y) \Rightarrow Q(y))$

Zapiranje izjavnih formul. Odprto izjavno formulo lahko zapremo tako, da:

- proste spremenljivke nadomestimo z individualnimi konstantami; ali
- formulo zapremo s kvantifikatorji.

Zgled: Naj bo $R(x, y)$ predikat "x ima rad y". Kot izjavna formula $R(x, y)$ ima dve prosti spremenljivki x, y in zato ni zaprta. Izjavno formulo zapremo na 8 načinov takole:

$\forall x\, \forall y : R(x, y)$	$\forall x : x$ ima rad vsakogar. Vsi imajo radi vsakogar.
$\forall y\, \forall x : R(x, y)$	$\forall y :$ vsakdo ima rad y. Vsi imajo radi vsakogar.
$\forall x\, \exists y : R(x, y)$	$\forall x : x$ ima nekoga rad. Vsakdo ima koga (vsak svojega) rad.
$\forall y\, \exists x : R(x, y)$	$\forall y :$ nekdo ima rad y. Vsakogar ima nekdo rad.
$\exists x\, \forall y : R(x, y)$	$\exists x : x$ ima rad vse. Nekdo ima rad vse.
$\exists y\, \forall x : R(x, y)$	$\exists y :$ vsi imajo radi y. Vsi imajo radi nekoga (vsi istega).
$\exists x\, \exists y : R(x, y)$	$\exists x : x$ ima nekoga rad. Nekdo ima nekoga rad.
$\exists y\, \exists x : R(x, y)$	$\exists y :$ nekdo ima rad y. Nekdo ima nekoga rad.

Semantika predikatnega računa

Interpretacijo $\mathcal{I}$ jezika 1. reda podamo takole:

1. Izberemo neprazno množico $\mathcal{D}_\mathcal{I}$. To je **domena interpretacije** oz. **področje pogovora**.

2. Za vsako individualno konstanto a izberemo neki element $a_\mathcal{I} \in \mathcal{D}_\mathcal{I}$.

3. Za vsak n-mestni predikat P izberemo neko n-mestno relacijo $P_\mathcal{I} \subseteq {\mathcal{D}_\mathcal{I}}^n$.

4. Za vsak n-mestni funkcijski simbol f izberemo neko n-člen o operacijo $f_\mathcal{I} : {\mathcal{D}_\mathcal{I}}^n \to \mathcal{D}_\mathcal{I}$.

Opomba. V dani interpretaciji

- vsakemu zaprtemu termu ustreza določen element domene;
- vsaki zaprti izjavni formuli pa ustreza določena izjava o elementih domene, ki je lahko resnična oz. neresnična.

Zgled: Vzemimo izjavne formule $P(a)$, $\forall x : P(x)$, $P(f(a,b))$, kjer je P enomesten predikat.

Obravnavajmo naslednjo interpretacijo $\mathcal{I}$:

- $\mathcal{D}_{\mathcal{I}} = \mathbb{N}$
- $a_{\mathcal{I}} = 2$
- $b_{\mathcal{I}} = 3$
- $f_{\mathcal{I}}(x, y) = 2x + y$
- $P_{\mathcal{I}}(x) \equiv x$ je praštevilo.

Potem dobimo:

- $f_{\mathcal{I}}(a_{\mathcal{I}}, b_{\mathcal{I}}) = 2 \cdot 2 + 3 = 7$ je naravno število.
- $P_{\mathcal{I}}(a_{\mathcal{I}})$ je resnična izjava, ker je $a_{\mathcal{I}} = 2$ praštevilo.
- $\forall x : P_{\mathcal{I}}(x)$ je neresnična izjava.
- $P_{\mathcal{I}}(f_{\mathcal{I}}(a_{\mathcal{I}}, b_{\mathcal{I}})) = P_{\mathcal{I}}(7)$ je resnična izjava.

Opomba. Odslej bomo indeks $\mathcal{I}$ opuščali.

Zgled: Vzemimo izjavno formulo $\forall x\, \exists y\, :\, R(x,y)$ v različnih interpretacijah:

$\mathcal{I}_1$: $\mathcal{D} = \mathbb{N}$ in $R(x,y) \equiv x > y$. Potem,

$\forall x\, \exists y : R(x,y) \equiv$ Za vsako naravno število obstaja manjše naravno število. (NI RES)

$\mathcal{I}_2$: $\mathcal{D} = \mathbb{Z}$ in $R(x,y) \equiv x > y$. Potem,

$\forall x\, \exists y : R(x,y) \equiv$ Za vsako celo število obstaja manjše celo število. (RES)

$\mathcal{I}_3$: $\mathcal{D} = \mathbb{N}$ in $R(x,y) \equiv x < y$. Potem,

$\forall x\, \exists y\, :\, R(x,y) \equiv$ Za vsako naravno število obstaja večje naravno število. (RES)

$\mathcal{I}_4$: $\mathcal{D} = \{$ ljudje $\}$ in $R(x,y) \equiv x$ ima rad y-a. Potem,

$\forall x\, \exists y : R(x,y) \equiv$ Vsakdo ima koga rad. (Mogoče je RES, mogoče pa NI RES)

Opomba. Ista izjavna formula je lahko v eni interpretaciji resnična in v drugi neresnična.

Splošno veljavne izjave in enakovrednosti

Zaprta izjavna formula φ je **logično veljavna** (oz. **splošno veljavna**), če je resnična v vsaki interpretaciji. Pišemo $\models \varphi$.

Zgled: Velja

$$\models \forall x : P(x) \Rightarrow \neg\exists x : \neg P(x)\,.$$

Dokaz. Če imajo vsi objekti iz domene interpretacije $\mathcal{D}$ lastnost P, potem gotovo ne obstaja objekt iz $\mathcal{D}$, ki nima lastnosti $\mathcal{D}$. □

Zaprti izjavni formuli φ_1 in φ_2 sta **enakovredni**, če sta v vsaki interpretaciji bodisi obe resnični bodisi obe neresnični. V tem primeru pišemo $\varphi_1 \sim \varphi_2$.

Trditev 16 *Naj bosta φ_1, φ_2 zaprti izjavni formuli. Potem je $\varphi_1 \sim \varphi_2$ natanko tedaj, ko je $\models \varphi_1 \Leftrightarrow \varphi_2$.*

Dokaz. Naj bo najprej $\varphi_1 \sim \varphi_2$. Vzemimo poljubno interpretacijo $\mathcal{I}$. V njej imata φ_1 in φ_2 enako resničnostno vrednost, torej je formula $\varphi_1 \Leftrightarrow \varphi_2$ splošno veljavna.

Naj bo zdaj $\models \varphi_1 \Leftrightarrow \varphi_2$ in $\mathcal{I}$ poljubna interpretacija. V njej je formula $\varphi_1 \Leftrightarrow \varphi_2$ resnična, torej imata φ_1 in φ_2 v $\mathcal{I}$ enako resničnostno vrednost. Ker je bila $\mathcal{I}$ poljubna, je $\varphi_1 \sim \varphi_2$. □

- Kako pokažemo, da neka izjavna formula φ **ni** logično veljavna? – Poiščemo "protiprimer" tj. interpretacijo v kateri φ ni resnična.

- Kako pokažemo, da formuli φ_1 in φ_2 **nista** enakovredni? – Poiščemo "protiprimer" tj. interpretacijo, v kateri je ena resnična, druga pa ne.

Zgled: Pokaži $\forall x \exists y : P(x,y) \not\equiv \exists y \forall x : P(x,y)$!

Protiprimer: Naj bosta $\mathcal{D} = \mathbb{N}$ in $P(x,y) \equiv x \leq y$. Potem:

- $\forall x \exists y : x \leq y$ je resnična izjava (lahko vzamemo kar $y = x$).
- $\exists y \forall x : x \leq y$ trdi, da obstaja naravno število, ki je "največje". Zato je to neresnična izjava.

Zgled: Pokaži $\forall x : (P(x) \vee Q(x)) \not\equiv \forall x : P(x) \vee \forall x : Q(x)$!

Protiprimer: Naj bo $\mathcal{D} = \mathbb{N}$ in $P(x) \equiv x$ je sodo število, $Q(x) \equiv x$ je liho število. Potem:

- $\forall x : (P(x) \vee Q(x))$ trdi, da je vsako naravno število sodo ali liho. To je res!
- $\forall x : P(x) \vee \forall x : Q(x)$ trdi, da so vsa naravna števila soda ali pa so vsa naravna števila liha. To pa ni res!

Zakoni predikatnega računa

V nadaljevanju si oglejmo nekaj tavtologij oz. enakovrednosti (urejenih glede na izjavne povezave):

1. Negacija. Veljata naslednji zvezi:

$$\neg\forall x : P(x) \ \sim \ \exists x : \neg P(x) \quad \text{in} \quad \neg\exists x : P(x) \ \sim \ \forall x : \neg P(x)$$

Tako sta kvantifikatorja $\forall$ in $\exists$ med seboj zamenljiva:

$$\forall x : P(x) \ \sim \ \neg\exists x : \neg P(x) \quad \text{in} \quad \exists x : P(x) \ \sim \ \neg\forall x : \neg P(x)$$

Zgled: Negacija izjave "*Vsi so pošteni*" ni "*Vsi so nepošteni*" ampak je "*Nekdo ni pošten*".

2. Konjunkcija. Tu veljata naslednji zvezi:

$$\begin{aligned} \forall x : (P(x) \wedge Q(x)) \ &\sim \ \forall x : P(x) \wedge \forall x : Q(x) \\ \exists x : (P(x) \wedge Q(x)) \ &\Rightarrow \ \exists x : P(x) \wedge \exists x : Q(x) \end{aligned}$$

Naloga 10 *Pokaži, da naslednja implikacija ne velja:*

$$\exists x : P(x) \wedge \exists x : Q(x) \ \Rightarrow \ \exists x : (P(x) \wedge Q(x)) \,.$$

3. Disjunkcija. Tu veljata naslednji zvezi:

$$\begin{aligned} \exists x : P(x) \vee \exists x : Q(x) &\sim \exists x : (P(x) \vee Q(x)) \\ \forall x : P(x) \vee \forall x : Q(x) &\Rightarrow \forall x : (P(x) \vee Q(x)) \,. \end{aligned}$$

Naloga 11 *Pokaži, da naslednja implikacija ne velja:*

$$\forall x : (P(x) \vee Q(x)) \Rightarrow \forall x : P(x) \vee \forall x : Q(x) \,.$$

4. Implikacija. Tu veljata naslednji zvezi:

$$\begin{aligned} \forall x : (P(x) \Rightarrow Q(x)) &\Rightarrow (\forall x : P(x) \Rightarrow \forall x : Q(x)) \\ \forall x : (P(x) \Rightarrow Q(x)) &\Rightarrow (\exists x : P(x) \Rightarrow \exists x : Q(x)) \,. \end{aligned}$$

5. Ekvivalenca. Splošno veljavna je naslednja izjava:

$$\forall x : (P(x) \Leftrightarrow Q(x)) \Rightarrow (\forall x : P(x) \Leftrightarrow \forall x : Q(x))$$

Naloga 12 *Ugotovi ali sta splošno veljavni naslednji izjavi:*

$$\begin{aligned} \forall x : P(x) \Rightarrow \forall x : Q(x) &\Rightarrow \forall x : (P(x) \Rightarrow Q(x)) \\ \exists x : P(x) \Rightarrow \exists x : Q(x) &\Rightarrow \forall x : (P(x) \Rightarrow Q(x)) \,. \end{aligned}$$

Še nekaj zakonov:

$$\begin{aligned}
\forall x \forall y : P(x,y) &\sim \forall y \forall x : P(x,y) \\
\exists x \exists y : P(x,y) &\sim \exists y \exists x : P(x,y) \\
\exists x \forall y : P(x,y) &\Rightarrow \forall y \exists x : P(x,y)
\end{aligned}$$

Naloga 13 *Ali je veljavna implikacija:*

$$\forall y \exists x : P(x,y) \Rightarrow \exists x \forall y : P(x,y)\,?$$

Splošnejša oblika predikatnih zakonov

Ko smo podali zakone predikatnega računa, smo se omejili na mestnost predikatov P in Q ter privzeli, da spremenljivki x, y nastopata v P in Q. Te omejitve lahko opustimo in dobimo spodnji seznam zakonov.

Za poljubne izjavne formule φ, ψ velja:

$$
\begin{array}{lll}
1. & \neg\forall x : \varphi & \sim \quad \exists x : \neg\varphi \\
2. & \neg\exists x : \varphi & \sim \quad \forall x : \neg\varphi \\
3. & \forall x\, \forall y : \varphi & \sim \quad \forall y\, \forall x : \varphi \\
4. & \exists x\, \exists y : \varphi & \sim \quad \exists y\, \exists x : \varphi \\
5. & \forall x : (\varphi \wedge \psi) & \sim \quad \forall x : \varphi \wedge \forall x : \psi \\
6. & \forall x : (\varphi \vee \psi) & \sim \quad \forall x : \varphi \vee \forall x : \psi\,.
\end{array}
$$

Če x ne nastopa prosto v φ, potem

$$
\begin{array}{lll}
7. & \varphi \vee \forall x : \psi & \sim \quad \forall x : (\varphi \vee \psi) \\
8. & \varphi \vee \exists x : \psi & \sim \quad \exists x : (\varphi \vee \psi)\,.
\end{array}
$$

Podobna zakona lahko zapišemo za $\wedge$.

Če je y nova spremenljivka oz. ne nastopa v $\varphi(x)$, potem

$$
\begin{array}{lll}
9. & \forall x : \varphi(x) & \sim \quad \forall y : \varphi(y) \\
10. & \exists x : \varphi(x) & \sim \quad \exists y : \varphi(y)
\end{array}
$$

Če x ne nastopa prosto v φ (opuščanje nepotrebnih kvantifikatorjev):

$$
11.\quad \forall x : \varphi \sim \varphi \qquad \text{in} \qquad 12.\quad \exists x : \varphi \sim \varphi.
$$

Prenexna normalna oblika

Izjavna formula $\mathcal{F}$ je v **prenexni normalni obliki**, če je oblike

$$\mathcal{F} \;=\; Q_1 x_1 \, Q_2 x_2 \cdots Q_n x_n : \; \mathcal{L},$$

kjer je vsak $Q_i \in \{\forall, \exists\}$ in je $\mathcal{L}$ formula, ki ne vsebuje kvantifikatorjev.

Zgled: Izjavna formula v prenexni normalni obliki:

$$\forall x \, \exists \, y \exists z : (P(x) \Rightarrow Q(x, y) \wedge R(a, z)) \, .$$

Recept za preoblikovanje izjavne formule v prenexno normalno obliko:

1. Vse izjavne veznike nadomestimo z $\neg$, $\wedge$, $\vee$.

2. Vse negacije premaknemo na predikate (uporabimo De Morgana, negacija kvantificirane formule, $\wedge$).

3. Individualne spremenljivke preimenujemo tako, da:
   - nobena spremenljivka ne nastopa hkrati vezano in prosto;
   - nobena spremenljivka ne nastopa v več kot enem kvantifikatorju.

4. Uporabimo distributivnost kvantifikatorjev glede na $\wedge$ in $\vee$: če x ne nastopa prosto v φ, potem

   $\varphi \vee \forall x : \psi \;\sim\; \forall x : (\varphi \vee \psi)$ in $\varphi \vee \exists x : \psi \;\sim\; \exists x : (\varphi \vee \psi) \, .$

   Podobne formule dobimo za $\wedge$.

Zgled: Zapiši izjavno formulo $\mathcal{F}$ v prenexni normalni obliki:

$$R(x,y) \Rightarrow \exists y : (P(y) \Rightarrow (\exists x : P(x) \Rightarrow Q(y)))$$

V 1. koraku $\mathcal{F}$ zapišemo takole:

$$\neg R(x,y) \vee \exists y : (\neg P(y) \vee (\neg \exists x : P(x) \vee Q(y))),$$

po 2. pa takole:

$$\neg R(x,y) \vee \exists y : (\neg P(y) \vee (\forall x : \neg P(x) \vee Q(y))),$$

v 3. koraku vpeljemo zamenjave $x \to u$ in $y \to v$ ter dobimo:

$$\neg R(x,y) \vee \exists v : (\neg P(v) \vee \forall u : \neg P(u) \vee Q(v)) \sim$$

$$\exists v : (\neg R(x,y) \vee \neg P(v) \vee \forall u : \neg P(u) \vee Q(v)) \sim$$

$$\exists v \forall u : (\neg (R(x,y) \wedge P(v) \wedge P(u)) \vee Q(v)).$$

Zaradi preglednosti lahko naredimo en korak več in zapišemo takole:

$$\exists v \forall u : (R(x,y) \wedge P(v) \wedge P(u) \Rightarrow Q(v))$$

Zgled: Zapiši izjave

$$\forall x : P(x) \Rightarrow \forall x : Q(x)$$

in

$$\forall x : (P(x) \Rightarrow \forall y : (Q(x,y) \Rightarrow \neg\forall z : R(y,z)))$$

v prenexni normalni obliki.

Prvo izjavo uredimo takole:

$$\begin{aligned}
\forall x : P(x) \Rightarrow \forall x : Q(x) \quad &\sim \quad \neg\forall x : P(x) \vee \forall x : Q(x) \\
&\sim \quad \exists x : \neg P(x) \vee \forall y : Q(y) \\
&\sim \quad \exists x \forall y : (\neg P(x) \vee Q(y)) \\
&\sim \quad \exists x \forall y : (P(x) \Rightarrow Q(y))
\end{aligned}$$

Drugo izjavo pa takole:

$$\begin{aligned}
&\forall x : (P(x) \Rightarrow \forall y : (Q(x,y) \Rightarrow \neg\forall z : R(y,z))) \quad \sim \\
&\forall x : (\neg P(x) \vee \forall y : (\neg Q(x,y) \vee \exists z : \neg R(y,z))) \quad \sim \\
&\forall x \forall y : (\neg P(x) \vee \exists z : (\neg Q(x,y) \vee \neg R(y,z))) \quad \sim \\
&\forall x \forall y \exists z : (\neg P(x) \vee \neg Q(x,y) \vee \neg R(y,z))) \quad \sim \\
&\forall x \forall y \exists z : (P(x) \wedge Q(x,y) \Rightarrow \neg R(y,z))
\end{aligned}$$

Sklepanje v predikatnem računu

Sklep

$$\varphi_1, \varphi_2, \ldots, \varphi_k \models \varphi$$

je **pravilen** (oz. **logično veljaven** ali **splošno veljaven**), če je v vsaki interpretaciji, v kateri so resnične vse predpostavke, resničen tudi zaključek.

Zgled: Pokaži, da je sklep

$$\begin{array}{ll} \varphi_1. & \forall x : (P(x) \Rightarrow (\exists y : R(x,y) \Rightarrow \exists z : R(z,x))) \\ \varphi_2. & \forall x : (P(x) \wedge \exists z : R(z,x) \Rightarrow R(x,x)) \\ \varphi_3. & \neg\exists x : R(x,x) \\ \hline \varphi. & \forall x : (P(x) \Rightarrow \forall y : \neg R(x,y)) \end{array}$$

pravilen.

Dokaz. Vzemimo $x_0 \in \mathcal{D}$ in predpostavimo, da velja $P(x_0)$. Iz φ_1 dobimo po (MP), da velja

$$\varphi_4. \qquad \exists y : R(x_0, y) \Rightarrow \exists z : R(z, x_0)\,.$$

Če bi veljalo $\exists z : R(z, x_0)$, bi iz φ_2 po (MP) dobili $R(x_0, x_0)$, kar pa je v protislovju s φ_3. Torej velja $\neg\exists z : R(z, x_0)$, kar nam skupaj s φ_4 po (MT) da $\neg\exists y : R(x_0, y)$ oziroma $\forall y : \neg R(x_0, y)$.

Povzemimo: iz predpostavke $P(x_0)$ smo izpeljali $\forall y : \neg R(x_0, y)$ in po (PS) velja

$$P(x_0, y) \Rightarrow \forall y : \neg R(x_0, y).$$

Ker pa je bil x_0 poljuben, velja torej

$$\forall x : (P(x) \Rightarrow \forall y : \neg R(x, y))\,.$$

□

Zgled: Pokaži da spodnji sklep ni splošno veljaven.

φ_1.	Vsi gasilci so močni.
φ_2.	Nekateri gasilci so hrabri.
φ_3.	Nekateri močni ljudje niso gasilci.
φ.	Torej, nekateri močni ljudje niso hrabri

Vpeljemo naslednje oznake:

- $G(x) \equiv x$ je gasilec;
- $M(x) \equiv x$ je močan;
- $H(x) \equiv x$ je hraber;

Sklep zapišemo takole:

$$\begin{array}{ll} \varphi_1. & \forall x : (G(x) \Rightarrow M(x)) \\ \varphi_2. & \exists x : (G(x) \wedge H(x)) \\ \varphi_3. & \exists x : (M(x) \wedge \neg G(x)) \\ \hline \varphi. & \exists x : (M(x) \wedge \neg H(x)) \end{array}$$

Protiprimer:

Množice

Množica je združitev določenih različnih objektov v neko skupino ali zbirko. Te objekte imenujemo **elementi** množice.

Izjavo "*a je element množice A*" zapišemo $a \in A$. Podobno $a \notin A$ pomeni "*a ni element množice A*".

Množica je lahko podana z

- **naštevanjem**, recimo $A = \{a, b, e, f, \ldots\}$
- **izjavno formulo**, recimo $A = \{x\,;\, \phi(x)\}$. Pri tem je $\phi(x)$ izjavna formula, ki ne vsebuje prostih nastopov spremenljivk, razen x.

Zgledi: Obravnavajmo naslednje množice

- $\{x;\, x \neq x\}$;
- $\{x;\, x \in \mathbb{Z} \wedge \exists y : (y \in \mathbb{Z} \wedge x = 2 \cdot y)\}$;
- $\{x;\, x = 0 \vee x = 1 \vee x = 2\}$.

Russellova množica:

$$R = \{x;\, x \notin x\}$$

Enakost, inkluzija in stroga inkluzija

Definirajmo **enakost**, **inkluzijo** ter **strogo inkluzijo** množic:

$$\begin{aligned} A = B \quad &\Leftrightarrow \quad \forall x : (x \in A \Leftrightarrow x \in B) \\ A \subseteq B \quad &\Leftrightarrow \quad \forall x : (x \in A \Rightarrow x \in B) \\ A \subset B \quad &\Leftrightarrow \quad A \subseteq B \ \wedge \ A \neq B \end{aligned}$$

Če velja $A \subseteq B$, rečemo, da je A **podmnožica** množice B. Če pa velja $A \subset B$, rečemo, da je A **prava podmnožica** množice B.

Trditev 17 *Velja*

$$A = B \quad \Leftrightarrow \quad A \subseteq B \ \wedge \ B \subseteq A \, .$$

Dokaz. Izpeljavo naredimo takole:

$$\begin{aligned} A = B \quad &\Leftrightarrow \quad \forall x : (x \in A \Leftrightarrow x \in B) \\ &\Leftrightarrow \quad \forall x : (x \in A \Rightarrow x \in B) \wedge \forall x : (x \in B \Rightarrow x \in A) \\ &\Leftrightarrow \quad A \subseteq B \ \wedge \ B \subseteq A. \end{aligned}$$

□

Osnovne operacije z množicami

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

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

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

Lastnosti osnovnih operacij:

- **idempotentnost:** $A \cup A = A$
  $A \cap A = A$

- **komutativnost:** $A \cup B = B \cup A$
  $A \cap B = B \cap A$

- **asociativnost:** $(A \cup B) \cup C = A \cup (B \cup C)$
  $(A \cap B) \cap C = A \cap (B \cap C)$

- **absorpcija:** $A \cup (A \cap B) = A$
  $A \cap (A \cup B) = A$

- **distributivnost:** $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Lastnosti z inkluzijo:

1. $A \cap B \subseteq A \subseteq A \cup B$
2. $A \subseteq B \quad \Rightarrow \quad A \cup C \subseteq B \cup C$
3. $A \subseteq B \quad \Rightarrow \quad A \cap C \subseteq B \cap C$

Prazna množica in univerzalna množica

Prazna množica je množica, ki ne vsebuje nobenega elementa; označimo jo z $\emptyset$.

Zgledi:

- $\{\emptyset\} \neq \emptyset$
- $\{\{\emptyset\}\} \neq \{\emptyset\}$

Pri uporabah teorije množic nas ponavadi zanimajo elementi ter podmnožice neke izbrane oz. vnaprej določene množice $\mathcal{S}$. Tej množici rečemo **univerzalna množica**.

Lastnosti: Naj bo A poljubna množica. Potem velja

1. $\emptyset \subseteq A \subseteq \mathcal{S}$
2. $\emptyset \cup A = A \quad \text{in} \quad \emptyset \cap A = \emptyset$
3. $\mathcal{S} \cup A = \mathcal{S} \quad \text{in} \quad \mathcal{S} \cap A = A$
4. $A \setminus \emptyset = A \quad \text{in} \quad A \setminus \mathcal{S} = \emptyset$

Množici A, B sta **disjunktni**, če je $A \cap B = \emptyset$.

Zgled: Prazna množica $\emptyset$ je disjunktna z vsako množico. Univerzalna množica $\mathcal{S}$ je disjunktna samo s prazno.

Komplement množic

Komplement množice definiramo kot:

$$A^c \;=\; \mathcal{S} \setminus A$$

Lastnosti:

1. $(A^c)^c = A$
2. $A \cup A^c = \mathcal{S} \quad \text{in} \quad A \cap A^c = \emptyset$
3. De Morganova zakona:

   $$(A \cap B)^c = A^c \cup B^c \quad \text{in} \quad (A \cup B)^c = A^c \cap B^c$$

4. $A \setminus B = A \cap B^c$
5. $\emptyset^c = \mathcal{S} \quad \text{in} \quad \mathcal{S}^c = \emptyset$
6. $A \subseteq B \quad \Leftrightarrow \quad B^c \subseteq A^c$
7. $A \cap B = \emptyset \quad \Leftrightarrow \quad A \subseteq B^c \quad \Leftrightarrow \quad B \subseteq A^c.$

Vsota množic

Vsoto oz. **simetrično razliko** množic definiramo takole:

$$A + B \quad \equiv \quad (A \setminus B) \cup (B \setminus A)$$

Lastnosti:

1. $A + B = (A \cup B) \setminus (A \cap B)$
2. $A + \emptyset = A$
3. $A + A = \emptyset$
4. $A + A^c = \mathcal{S}$
5. $A + B = B + A$
6. $(A + B) + C = A + (B + C)$
7. $A + B = \emptyset \quad \Leftrightarrow \quad A = B$
8. $A \cap B = \emptyset \quad \Leftrightarrow \quad A + B = A \cup B$
9. $(A + B) \cap C \quad = \quad (A \cap C) + (B \cap C)$

Lastnost 6 nam zagotovi, da lahko vsoto posplošimo takole:

$$A_1 + A_2 + \cdots + A_n \;:=\; (\cdots((A_1 + A_2) + A_3) + \cdots + A_n)$$

Vprašanje 5 *Naj bodo $A_1, A_2, \ldots, A_n$ množice. Poišči potreben in zadosten pogoj, da bi bil nek element x vsebovan v vsoti $A_1 + A_2 + \cdots + A_n$?*

Naloga 14 *Dokaži 9. lastnost!*

Enačbe z množicami

Zgled: Kdaj so enačbe rešljive:

1. $X \cup A = B$;
2. $X \cap A = B$;
3. $X + A = B$;

Zgled: Poišči vse rešitve sistema enačb

$$\begin{aligned} X \cup A &= B \\ X \cap A &= C \end{aligned}$$

kjer so A, B, C dane množice. Kdaj je sistem rešljiv?

Postopek za reševanje sistema enačb z neznano množico

Zgled: Poišči vse rešitve sistema enačb

$$\begin{aligned} A \cap X &= B \setminus X \\ C \cup X &= X \setminus A \end{aligned}$$

kjer so A, B, C dane množice. Kdaj je sistem rešljiv?

Korak 1. *Vse člene prenesemo na levo stran enačb z uporabo ekvivalence:*

$$P = Q \qquad \Leftrightarrow \qquad P + Q = \emptyset$$

oz. vsaki enačbi na obeh straneh prištejemo njeno desno stran.

Torej,

$$\begin{aligned} A \cap X \;+\; B \setminus X &= \emptyset \\ C \cup X \;+\; X \setminus A &= \emptyset\,. \end{aligned}$$

Korak 2. *Vse enačbe združimo v eno samo z uporabo ekvivalence*

$$P = \emptyset \quad \text{in} \quad Q = \emptyset \qquad \Leftrightarrow \qquad P \cup Q = \emptyset\,.$$

Pri našem zgledu je to:

$$(A \cap X + B \setminus X) \cup (C \cup X + X \setminus A) = \emptyset\,.$$

Korak 3. *Vse operacije izrazimo z* $\cup$, $\cap$, ^{c}*:*

$$\begin{aligned} P \setminus Q &= P \cap Q^c \\ P + Q &= (P \cap Q^c) \cup (Q \cap P^c) \end{aligned}$$

Z uporabo de Morganovih zakonov in distributivnosti levo stran enačbe zapišemo v obliki unije presekov danih množic, neznane množice ter njihovih komplementov ("DNO").

Pri našem zgledu dobimo,

$$\begin{gathered} (A \cap X \cap (B \cap X^c)^c) \cup (B \cap X^c \cap (A \cap X)^c) \cup \\ ((C \cup X) \cap (X \cap A^c)^c) \cup (X \cap A^c \cap (C \cup X)^c) = \emptyset \end{gathered}$$

in od tukaj

$$\begin{gathered} (A \cap X \cap (B^c \cup X)) \cup (B \cap X^c \cap (A^c \cup X^c)) \cup \\ ((C \cup X) \cap (X^c \cup A)) \cup (X \cap A^c \cap C^c \cap X^c) = \emptyset\,. \end{gathered}$$

Uporabimo absorpcijo ter druge zakone, da poenostavimo takole:

$$(A \cap X) \cup (B \cap X^c) \cup (C \cap X^c) \cup (C \cap A) = \emptyset\,.$$

Korak 4. *Vsak presek oblike* $P_1 \cap P_2 \cap \cdots P_n$, *kjer so* P_i *znane množice ali njihovi komplementi, nadomestimo s*

$$(P_1 \cap P_2 \cap \cdots P_n \cap X) \cup (P_1 \cap P_2 \cap \cdots P_n \cap X^c)\,.$$

S tem dosežemo, da v vsakem preseku nastopa bodisi X *bodisi* X^c.

V našem primeru dobimo

$$(A \cap X) \cup (B \cap X^c) \cup (C \cap X^c) \cup (C \cap A \cap X) \cup (C \cap A \cap X^c) = \emptyset,$$

s pomočjo absorpcije pa poenostavimo

$$(A \cap X) \cup (B \cap X^c) \cup (C \cap X^c) = \emptyset.$$

Korak 5. *Izpostavimo* X *in* X^c *in s tem enačbo prevedemo v obliko:*

$$(P \cap X) \cup (Q \cap X^c) = \emptyset\,.$$

Od tod hitro dobimo:

$$\begin{aligned} (P \cap X) \cup (Q \cap X^c) = \emptyset \quad &\Leftrightarrow \quad P \cap X = \emptyset \;\; \textit{in} \;\; Q \cap X^c = \emptyset \\ &= \quad Q \subseteq X \subseteq P^c\,. \end{aligned}$$

Torej rešitev obstaja le, če je $Q \subseteq P^c$ *oziroma* $Q \cap P = \emptyset$.

V našem primeru dobimo

$$(A \cap X) \cup ((B \cup C) \cap X^c) = \emptyset.$$

Odgovor: Naš sistem ima rešitev natanko tedaj, ko je $A \cap (B \cup C) = \emptyset$. Tedaj je rešitev vsaka množica X, za katero velja:

$$B \cup C \;\subseteq\; X \;\subseteq\; A^c.$$

Potenčna množica

Potenčna množica dane množice A je

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

Zgledi:

- $\mathcal{P}(\{a,b,c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$
- $\mathcal{P}(\emptyset) = \{\emptyset\}$
- $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$

Naloga 15 *Izračunaj $\mathcal{P}^3(\emptyset)$. Koliko elementov ima množica $\mathcal{P}^5(\emptyset)$?*

Za potenčno množico velja:

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

Družine množic

Naj bo $\mathcal{M} = \{A, B, C, \ldots\}$ družina množic. Pojem **unija** in **presek** lahko razširimo na družine množic takole:

Unija družine $\mathcal{M}$ je

$$\bigcup_{Y \in \mathcal{M}} Y = \{x\,;\, \exists Y \in \mathcal{M} : x \in Y\}$$

Presek družine $\mathcal{M}$ je

$$\bigcap_{Y \in \mathcal{M}} Y = \{x\,;\, \forall Y \in \mathcal{M} : x \in Y\}$$

Včasih uporabimo okrajšavo

$$\cup\,\mathcal{M} = \bigcup_{Y \in \mathcal{M}} Y \quad \text{in} \quad \cap\,\mathcal{M} = \bigcap_{Y \in \mathcal{M}} Y$$

Pogosto uporabljamo **indeksno obliko**. Naj bo $\mathcal{I}$ indeksna množica ter

$$\mathcal{M} = \{A_i\,;\, i \in \mathcal{I}\}\,.$$

Potem je

$$\cup\,\mathcal{M} = \bigcup_{i \in \mathcal{I}} A_i \quad \text{in} \quad \cap\,\mathcal{M} = \bigcap_{i \in \mathcal{I}} A_i\,.$$

Zgled:

$$\bigcup_{i\in\mathbb{N}} \left[\frac{1}{n}, 1\right] = (0, 1] \qquad \text{in} \qquad \bigcap_{i\in\mathbb{N}} \left[\frac{1}{n}, 1\right] = \{1\}$$

Veljata posplošeni distributivnosti:

$$B \cap \left(\bigcup_{i\in\mathcal{I}} A_i\right) \quad = \quad \bigcup_{i\in\mathcal{I}} (B \cap A_i)$$

in

$$B \cup \left(\bigcap_{i\in\mathcal{I}} A_i\right) \quad = \quad \bigcap_{i\in\mathcal{I}} (B \cup A_i)\,.$$

Pokritja in razbitja

Družina podmnožic $\mathcal{M} = \{A_i\,;\, i \in \mathcal{I}\}$ množice A je **pokritje množice** A, če je

$$A \quad = \quad \bigcup_{i \in \mathcal{I}} A_i\,.$$

Družina podmnožic $\mathcal{M} = \{A_i\,;\, i \in \mathcal{I}\}$ množice A je **razbitje** oz. **particija** množice A, če velja:

1. $\mathcal{M}$ je pokritje množice A;
2. elementi iz $\mathcal{M}$ so neprazni;
3. elementi iz $\mathcal{M}$ so paroma disjunktni, tj. $A_i \cap A_j = \emptyset$ za poljubna dva indeksa $i, j \in \mathcal{I}$.

Urejeni pari in n-terice

Vemo, da je 2-elementna množica $\{x, y\}$ neurejen par, tj. $\{x, y\} = \{y, x\}$.

Urejeni par s 1. komponento x ter 2. komponento y definiramo takole:

$$(x, y) \;=\; \{\{x, y\}, \{x\}\}$$

Trditev 18 (Osnovna lastnost urejenih parov) *Velja:*

$$(x, y) = (u, v) \quad \Leftrightarrow \quad x = u \wedge y = v$$

Dokaz.

Urejeno n-terico definiramo takole

$$(a_1, a_2, a_3, \ldots, a_n) = (\cdots((a_1, a_2), a_3), \ldots, a_n)$$

Kartezični produkt

Kartezični produkt dveh množic podamo na naslednji način:

$$A \times B = \{(a, b)\,;\, a \in A \text{ in } b \in B\}$$

Zgled:

Lastnosti:

1. Kartezični produkt z unijo:

$$\begin{aligned} A \times (B \cup C) &= (A \times B) \cup (A \times C) \\ (B \cup C) \times A &= (B \times A) \cup (C \times A) \end{aligned}$$

2. Kartezični produkt s presekom:

$$\begin{aligned} A \times (B \cap C) &= (A \times B) \cap (A \times C) \\ (B \cap C) \times A &= (B \times A) \cap (C \times A) \end{aligned}$$

3. $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$

4. $A = \emptyset \ \vee \ B = \emptyset \quad \Leftrightarrow \quad A \times B = \emptyset$

5. $A \subseteq C \ \wedge \ B \subseteq D \quad \Rightarrow \quad A \times B \subseteq C \times D$

6. $A \times B \ \subseteq \ C \times D \ \wedge \ A \times B \neq \emptyset \quad \Rightarrow \quad A \subseteq C \ \wedge \ B \subseteq D$

7. Naj bo A končna množica z n elementi in B končna množica z m elementi, potem je $A \times B$ končna množica z $n \cdot m$ elementi .

Kartezični produkt n množic podamo takole:

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \, ; \, a_i \in A_i\}$$

Funkcije

Funkcija je enolična relacija $f \in \mathrm{Rel}(A, B)$ tj.

$$\forall x \in A, y_1, y_2 \in B : (x\, f\, y_1 \ \wedge \ x\, f\, y_2 \ \Rightarrow \ y_1 = y_2)$$

Funkcija f je **preslikava iz A v B**, če je $\mathcal{D}_f = A$. Pišemo $f : A \to B$.

Pisava

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

Za preslikavo $f : A \to B$ velja:

- $A = \mathcal{D}_f$ je **domena** oz. **definicijsko območje**
- B je **kodomena**
- **Slika** oz. **zaloga vrednosti** je

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

$B^A = \{f\ ;\ f : A \to B\}$ je množica vseh preslikav iz A v B.

Nekateri tipi funkcij

- **prazna funkcija** $\emptyset_B : \emptyset \to B$. Velja
  1. $B^\emptyset = \{\emptyset_B\}$
  2. $\emptyset^A = \emptyset$, če $A \neq \emptyset$.
- **identiteta** $\mathrm{id}_A : A \to A$, $\forall x \in A : \mathrm{id}_A(x) = x$. Identiteta je bijektivna funkcija.
- **vložitev** $i : A \to B$ če je $A \subseteq B$ ter $i(x) = x$ za vse $x \in A$. Funkcija i je injektivna.
- **projekcija na i-to komponento** je $p_i : A_1 \times \cdots \times A_n \to A_i$, če $p_i(a_1, a_2, \ldots, a_n) = a_i$. Ta funkcija je surjektivna.
- **naravna (kanonska) projekcija** je $p : A \to A/R$, kjer je R ekvivalenčna relacija na A ter $p(x) = R[x]$ za vse $x \in A$. To je surjektivna funkcija.
- **karakteristična funkcija podmnožice A množice B**

$$\chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \in B \setminus A\,. \end{cases}$$

- **zožitev funkcije $f : A \to B$ na $A_1 \subseteq A$** je funkcija $g : A_1 \to B$, če $g(x) = f(x)$ za vsak $x \in A_1$. Pišemo $g = f|_{A_1}$.

Lastnosti preslikav

Naj bo $f : A \to B$ preslikava. Definiramo

- f je **injektivna**, če $\forall x, y \in A : (f(x) = f(y)) \Rightarrow x = y$);
- f je **surjektivna**, če $\mathcal{Z}_f = B$;
- f je **bijektivna**, če je injektivna in surjektivna.

Naloga 16 *Katere od zgornjih lastnosti imajo funkcije*

- $f : \mathbb{Z} \to \mathbb{Z}$ *kjer je* $f(x) = 2x$
- $\mathrm{id}_{\mathbb{N}}$
- $f : \mathbb{R} \to \mathbb{R}^+ \cup \{0\}$ *kjer je* $f(x) = x^2$*?*

Inverzna funkcija oz. preslikava

Za vsako funkcijo f obstaja inverzna relacija f^{-1}. Kdaj je relacija f^{-1} funkcija oz. preslikava?

Trditev 19 *Naj bo f funkcija iz A v B. Potem*

(a) Relacija f^{-1} je funkcija natanko tedaj, ko je f injektivna;

(b) Relacija f^{-1} je preslikava natanko tedaj, ko je f bijektivna.

Dokaz. Dokažimo najprej trditev (a) takole:

$$\begin{aligned} f^{-1} \text{ je funkcija} &\Leftrightarrow \forall x, y, z : (x\, f^{-1}\, y \ \wedge\ x\, f^{-1}\, z \ \Rightarrow\ y = z) \\ &\Leftrightarrow \forall x, y, z : (y\, f\, x \ \wedge\ z\, f\, x \ \Rightarrow\ y = z) \\ &\Leftrightarrow \forall x, y, z : (x = f(y) \ \wedge\ x = f(z) \ \Rightarrow\ y = z) \\ &\Leftrightarrow \forall y, z : (f(y) = f(z) \ \Rightarrow\ y = z) \\ &\Leftrightarrow f \text{ je injekcija.} \end{aligned}$$

Sledi dokaz točke (b): f^{-1} je preslikava natanko takrat, kadar je f^{-1} funkcija za katero velja $D_{f^{-1}} = B$. Po trditvi (a) je f^{-1} funkcija natanko takrat, ko je f injektivna. Torej, funkcija f^{-1} je preslikava natanko takrat, ko je f surjekcija. Od tod pa sledi trditev. □

Kompozitum funkcij

Naj bosta $f \subseteq A \times B$ in $g \subseteq B \times C$. Definirajmo **kompozitum** $g \circ f \subseteq A \times C$ takole

$$\forall x \in \mathcal{D}_f : g \circ f(x) = g(f(x)).$$

Trditev 20 *Za poljubni funkciji $f \subseteq A \times B$ in $g \subseteq B \times C$ velja*

$$g \circ f = f * g,$$

kjer je operacija $*$ relacijski produkt.

Dokaz. Pokažimo, da je $y = g \circ f(x)$ natanko takrat, kadar sta x in y v relaciji $f * g$:

$$\begin{aligned} x(f * g)y &\Leftrightarrow \exists z \in B : (x\, f\, z \wedge z\, g\, y) \\ &\Leftrightarrow \exists z \in B : (f(x) = z \wedge g(z) = y) \\ &\Leftrightarrow y = g(f(x)) \end{aligned}$$

□

Lastnosti kompozituma

Trditev 21 *Velja*

- *Naj bosta f, g funkciji. Potem je $g \circ f$ funkcija.*
- *Naj bosta $f : A \to B$ in $g : B \to C$ preslikavi. Potem je $g \circ f$ tudi preslikava.*

Dokaz.

Problem 1 *Naj bo $f : A \to B$ preslikava. Pokaži, da velja:*

- $f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$
- *f je injektivna* $\Leftrightarrow f^{-1} \circ f = \mathrm{id}_A$
- *f je surjektivna* $\Leftrightarrow f \circ f^{-1} = \mathrm{id}_B$.

Dokaz.

Trditev 22 *Naj bosta* $f : A \to B$ *in* $g : B \to C$ *preslikavi. Potem velja*

- f *in* g *injekciji* $\Rightarrow$ $g \circ f$ *injekcija;*
- f *in* g *surjekciji* $\Rightarrow$ $g \circ f$ *surjekcija;*
- $g \circ f$ *injekcija* $\Rightarrow$ f *injekcija;*
- $g \circ f$ *surjekcija* $\Rightarrow$ g *surjekcija.*

Dokaz.

Trditev 23 *Naj za preslikavi* $f : A \to B$ *in* $g : B \to A$ *velja* $g \circ f = \mathrm{id}_A$ *ter* $f \circ g = \mathrm{id}_B$*. Potem sta* f *in* g *bijektivni ter* $g = f^{-1}$*.*

Dokaz. Iz $f \circ g = \mathrm{id}_B$ sledi, da je g injektivna ter f surjektivna. Podobno iz $g \circ f = \mathrm{id}_A$ sklepamo, da je f injektivna ter g surjektivna. Torej sta funkciji g in f bijekciji. Pokažimo, da je prva inverzna drugi:

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

□

Slike in praslike

Naj bo $f \subseteq A \times B$ funkcija ter $A_1 \subseteq A$ in $B_1 \subseteq B$.

- **Slika** množice A_1 je

$$f(A_1) = \{y \in B; \exists x \in A_1 : y = f(x)\}$$

- **Praslika** množice B_1 je

$$f^{-1}(B_1) = \{x \in A; f(x) \in B_1\}$$

Lastnosti: Za funkcijo $f \in A \times B$ ter $A_1, A_2 \subseteq A$ in $B_1, B_2 \subseteq B$ velja:

- $f^{-1}(f(A_1)) \supseteq A_1$ (če je f injektivna, velja enačaj)
- $f(f^{-1}(B_1)) \supseteq B_1$ (če je f surjektivna, velja enačaj)
- $f(\emptyset) = \emptyset$
- $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
- $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$
- $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$
- $f^{-1}(B_1 \cap B_2) \subseteq f^{-1}(B_1) \cap f^{-1}(B_2)$

Permutacije

Naj bo A končna množica. **Permutacija** na A je poljubna bijektivna funkcija.

$S(A)$ - množica vseh permutacij na A;

Množico vseh permutacij na $\{1, 2, \ldots, n\}$ označimo s S_n.

Za vsako permutacijo iz S_n rečemo, da je **dolžine** n ter jo ponavadi podamo s tabelo takole:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \end{pmatrix},$$

kjer so vsi a_i paroma različni elementi množice $\{1, 2, \ldots, n\}$.

Zgledi:

- $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ je permutacija reda 2 ;
- $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ je permutacija reda 4 ;

Vprašanje 6 *Koliko je različnih permutacij reda n?*

Produkt permutacij

Ker so permutacije funkcije oz. relacije, lahko uporabljamo produkte $\circ$ oz. $*$.

Torej za poljubni permutaciji α in β iz S_n velja

$$\alpha \circ \beta \quad = \quad \beta * \alpha$$

Zgled: Naj bo

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \text{ter} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

Potem je

$$\beta \circ \alpha = \alpha * \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

in

$$\alpha \circ \beta = \beta * \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

Naloga 17 *Ali je $*$ oz. $\circ$ komutativna operacija?*

Opomba: Med $*$ in $\circ$ za "default" izberemo $*$. Torej, $\alpha\,\beta$ pomeni $\alpha * \beta$!

Identiteta in fiksne točke

Identiteta reda n je

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & 2 & 3 & \cdots & n-1 & n \end{pmatrix}$$

Za vsako drugo permutacijo $\pi \in S_n$ velja $\mathrm{id} * \pi = \pi * \mathrm{id} = \pi$.

Trditev 24 *Za vsako permutacijo π obstaja "inverzna" permutacija π^{-1} in tako velja*

$$\pi * \pi^{-1} = \pi^{-1} * \pi = \mathrm{id}.$$

Število k je **fiksna točka** permutacije π, če je $\pi(k) = k$. Rečemo tudi, da π **pribije** k.

Velja:

- id pribije vsa števila;
- π in π^{-1} pribijeta ista števila.

Cikli

Permutacija π je **cikel** natanko takrat, ko obstaja neprazno zaporedje različnih števil

$$a_0, a_1, a_2, \ldots, a_{r-1}$$

iz množice $\{1, 2, \ldots, n\}$ ter velja:

- π pribije vsa števila, ki niso v zaporedju;
- za števila iz zaporedja velja $\pi(a_k) = a_{k+1 \mod r}$

V takem primeru zapišemo $\pi = (a_0\, a_1\, a_2 \cdots a_{r-1})$. Število r je **dolžina** cikla.

Vaja:

- Zapiši cikel $(3\,6\,2\,4)$ kot permutacijo dolžine 6!
- Zmnoži cikla $(1\,2\,3)$ in $(3\,1\,6)$.

Velja:

- Če je $C = (a_1\, a_2 \cdots a_n)$, potem je $C^{-1} = (a_n\, a_{n-1} \cdots a_1)$.
- Če sta C_1 in C_2 disjunktna cikla, potem $C_1 * C_2 = C_2 * C_1$.

Orbite

Trditev 25 *Vsaka permutacija se da (enoličnо) razcepiti na produkt disjunktnih ciklov. Razcep je enoličen do vrstnega reda ciklov.*

Elementi vsakega cikla razbitja tvorijo **orbite**.

Zgled: Permutacija

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 & 10 \end{pmatrix}$$

se zapiše kot produkt disjunktnih ciklov takole:

$$\alpha \quad = \quad (1\,6)\,(2\,4)\,(3\,7\,8\,9)\,(10).$$

Orbite te permutacije so $\{1, 6\}$, $\{2, 4\}$, $\{3, 7, 8, 9\}$ ter $\{10\}$.

Velja:

- Če je $\pi = C_1 * C_2 * \cdots * C_k$ disjunktni razcep, potem je $\pi^{-1} = C_1^{-1} * C_2^{-1} * \cdots * C_k^{-1}$.

Sode in lihe permutacije

Cikel dolžine 2 imenujemo **transpozicija**. Vsak cikel daljši od 2, lahko zapišemo kot produkt transpozicij takole:

$$(a_1\, a_2\, \cdots\, a_k) \;=\; (a_1\, a_2)\,(a_1\, a_3)\,\cdots\,(a_1\, a_k)$$

Trditev 26 *Vsaka permutacija se da zapisati kot produkt transpozicij. Zapis ni enoličen, ohrani pa se parnost števila transpozicij.*

Permutacija je **soda**, če je sodo mnogo transpozicij v produktu, sicer pa je **liha**.

Zgledi: $(123)(45)$ je liha permutacija, $(125)(34)(6789)$ pa je soda permutacija.

$S_3 = \{\mathrm{id}, (123), (132), (1)(23), (2)(13), (12)(3)\}$

$A_3 = \{\mathrm{id}, (123), (132)\}$ sode permutacije iz S_3.

Velja:

- id je soda permutacija,
- π in π^{-1} sta enake parnosti.

Ciklična struktura

Naj ima permutacija $\pi \in S_n$ v zapisu k_i ciklov dolžine i, za $i = 1, \ldots, n$.

Potem pravimo, da ima π **ciklično strukturo**

$$(k_1, k_2, \ldots, k_n).$$

Velja

$$1 \cdot k_1 + 2 \cdot k_2 + 3 \cdot k_3 + \cdots + n \cdot k_n = n.$$

Zgledi:

- Permutacija $(123)(45)(6\,10)(7)(89)$ ima ciklično strukturo

$$(1, 3, 1, 0, 0, 0, 0, 0, 0, 0)$$

- Ciklična struktura permutacije id dolžine n je

$$(n, 0, \ldots, 0)$$

Naloga 18 *Pokaži, da imata π in π^{-1} enako ciklično strukturo.*

Red permutacije

Red $\mathrm{red}(\pi)$ permutacije π je najmanjše pozitivno naravno število k, za katerega velja $\pi^k = \mathrm{id}$.

Zgled: Poiščimo red permutacije

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 & 10 \end{pmatrix}$$

Trditev 27 *Red permutacije ima naslednje lastnosti:*

- *Če je C cikel dolžine m, potem je* $\mathrm{red}(C) = m$.
- *Če je π produkt tujih ciklov dolžine $m_1, m_2, \ldots, m_k$, potem je* $\mathrm{red}(\pi) = \mathrm{lcm}(m_1, m_2, \ldots, m_k)$.
- *Za poljubno permutacijo π velja* $\mathrm{red}(\pi) = \mathrm{red}(\pi^{-1})$.

Dokaz.

Vaja:

Relacijo **konjugiranost** $\approx$ na $S(A)$ definiramo takole:

$$\pi_1 \approx \pi_2, \qquad \text{če} \quad \exists \tau \in G : \pi_2 = \tau \circ \pi_1 \circ \tau^{-1}$$

Izrek 28 *Permutaciji π in σ sta konjugirani natanko takrat, ko imata enako ciklično strukturo.*

Dokaz. ($\Rightarrow$). Če je $C = (i_1\, i_2\, \cdots\, i_k)$ cikel, potem je

$$\tau \circ C \circ \tau^{-1} = (\tau(i_1)\, \tau(i_2)\, \cdots\, \tau(i_k)).$$

Pri produktu disjunktnih ciklov pa tako učinkuje posebej na vsakem ciklu. Naj bo

$$\pi = (a_1\, a_2\, \cdots\, a_k) \circ (b_1\, b_2\, \cdots\, b_l) \circ \cdots \circ (c_1\, c_2\, \cdots\, c_m).$$

Potem je

$$\begin{aligned}
\tau \circ \pi \circ \tau^{-1} &= \tau \circ (a_1\, a_2\, \cdots\, a_k) \circ (b_1\, b_2\, \cdots\, b_l) \circ \cdots (c_1\, c_2\, \cdots\, c_m) \circ \tau^{-1} \\
&= \tau \circ (a_1\, a_2\, \cdots\, a_k) \circ [\tau^{-1} \circ \tau] \circ (b_1\, b_2\, \cdots\, b_l) \circ [\tau^{-1} \circ \tau] \circ \cdots (c_1\, c_2\, \cdots\, c_m) \circ \tau^{-1} \\
&= [\tau \circ (a_1\, a_2\, \cdots\, a_k) \circ \tau^{-1}] \circ [\tau \circ (b_1\, b_2\, \cdots\, b_l) \circ \tau^{-1}] \circ \cdots [\tau \circ (c_1\, c_2\, \cdots\, c_m) \circ \tau^{-1}] \\
&= \big(\tau(a_1)\, \tau(a_2)\, \cdots\, \tau(a_k)\big) \circ \big(\tau(b_1)\, \tau(b_2)\, \cdots\, \tau(b_l)\big) \circ \cdots \big(\tau(c_1)\, \tau(c_2)\, \cdots\, \tau(c_m)\big).
\end{aligned}$$

($\Leftarrow$) Recimo:

$$\pi = (a_1\, a_2\, \cdots\, a_k) \circ (b_1\, b_2\, \cdots\, b_l) \circ \cdots \circ (c_1\, c_2\, \cdots\, c_m)$$

in

$$\sigma = (a'_1\, a'_2\, \cdots\, a'_k) \circ (b'_1\, b'_2\, \cdots\, b'_l) \circ \cdots \circ (c'_1\, c'_2\, \cdots\, c'_m).$$

Definirajmo funkcijo $\tau : x \mapsto x'$. Očitno, da je τ permutacija iz $S(A)$. Velja pa $\tau \circ \pi \circ \tau^{-1} = \sigma$. To vidimo takole:

$$\tau \circ \pi \circ \tau^{-1}(x'_i) = \tau \circ \pi(x_i) = \tau(x_{i+1}) = x'_{i+1} = \sigma(x'_i).$$

□

Naslednja trditev je hitra posledica prejšnjega izreka.

Posledica 29 *Konjugiranost $\approx$ je ekvivalenčna relacija.*

Moč množic

Končne množice

Naj bo A končna množica. Potem z $|A|$ označimo število elementov oz. **moč** množice A.

Končni množici A in B sta **enako močni**, če je $|A| = |B|$. V tem primeru pišemo $A \sim B$.

Zgledi:

- $|\emptyset| = 0$
- $|\{0, 1\}| = 2$
- $|\{\{0, 1\}\}| = 1$
- $|\{\emptyset\}| = 1$

Trditev 30 *Naj bosta A, B končni množici. Potem je $A \sim B$ natanko takrat, kadar obstaja bijektivna preslikava $f : A \to B$.*

Dokaz.

Lastnosti: Naj bodo A, B, C končne množice. Potem velja:

- $|A \times B| = |A| \cdot |B|$
- $|\mathcal{P}(A)| = 2^{|A|}$
- $|B^A| = |\{f\,;\, f : A \to B\}| = |B|^{|A|}$
- $|A \setminus B| = |A| - |A \cap B|$
- Če je $B \subseteq A$, potem $|A \setminus B| = |A| - |B|$
- $|A \cup B| = |A| + |B| - |A \cap B|$
- Če je $A \cap B = \emptyset$, potem je $|A \cup B| = |A| + |B|$
- $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$.

Naloga 19 *Koliko je števil na intervalu* $[1, 100]$, *ki so deljiva s* 3, *a niso deljiva s* 5*?*

Rešitev:

Princip vključitve & izključitve

Naj bodo $A_1, A_2, \ldots, A_n$ končne množice. Potem velja

$$\begin{aligned}
|A_1 \cup A_2 \cup \cdots \cup A_n| \quad &= \; |A_1| + |A_2| + \cdots + |A_n| \\
&- \; |A_1 \cap A_2| - |A_1 \cap A_3| - \cdots - |A_{n-1} \cap A_n| \\
&+ \; |A_1 \cap A_2 \cap A_3| + \cdots + |A_{n-2} \cap A_{n-1} \cap A_n| \\
&- \; |A_1 \cap A_2 \cap A_3 \cap A_4| - \cdots \\
&\quad \ldots \\
(-1)^{n+1} \; &|A_1 \cap A_2 \cap \cdots \cap A_n|.
\end{aligned}$$

Kompakten zapis principa: Naj bo

$$S_k = \sum_{\substack{\mathcal{I} \subseteq \{1,2,\ldots,n\} \\ |\mathcal{I}|=k}} |\bigcap A_i|$$

potem

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^{n} (-1)^{i-1} S_i \,.$$

Komplementarna vključitev & izključitev

Naj bo A končna množica in $A_1, A_2, \ldots, A_n$ podmnožice A. Definiramo $A_i^c = A \setminus A_i$. Potem velja

$$\begin{aligned}
|A_1^c \cap A_2^c \cap \cdots \cap A_n^c| \quad &= |A| - |A_1| - |A_2| - \cdots - |A_n| \\
&+ |A_1 \cap A_2| + |A_1 \cap A_3| + \cdots + |A_{n-1} \cap A_n| \\
&- |A_1 \cap A_2 \cap A_3| - \cdots - |A_{n-2} \cap A_{n-1} \cap A_n| \\
&+ |A_1 \cap A_2 \cap A_3 \cap A_4| + \cdots \\
&\cdots \\
(-1)^n \ &|A_1 \cap A_2 \cap \cdots \cap A_n|.
\end{aligned}$$

Kompaktnejši zapis: Postavimo $S_0 = |A|$. Potem je

$$|A_1^c \cap A_2^c \cap \cdots \cap A_n^c| = \sum_{i=0}^{n} (-1)^i S_i \,.$$

Neskončne množice

Množici A in B sta **enakomočni**, kadar med njima obstaja bijektivna funkcija $f : A \to B$. Pišemo $A \sim B$.

Zgled: Funkcija $f : \mathbb{Z} \to \mathbb{N}$

$$f(z) = \begin{cases} 2z, & z \geq 0 \\ -2z - 1, & z < 0 \end{cases}$$

je bijekcija med $\mathbb{Z}$ in $\mathbb{N}$. Torej, $\mathbb{Z} \sim \mathbb{N}$.

Trditev 31 *Relacija $\sim$ je enakovrednost.*

Dokaz.

Ekvivalenčnim razredom enakovrednosti $\sim$ rečemo **kardinalna števila**. Poljubni množici A ustrezno kardinalno število označimo z $|A|$ oz. $\mathrm{card}(A)$.

Dedekindova definicija. Množica A je **neskončna** natanko tedaj, ko obstaja neka prava podmnožica $B \subset A$ tako, da $A \sim B$. Množica A je **končna** natanko tedaj, ko ni neskončna.

Krajše zapišemo:

$$A \text{ neskončna} \quad \Leftrightarrow \quad \exists B \subset A : A \sim B$$

Zgled: Funkcija $g(x) = x + 1$ je bijekcija med $\mathbb{N}$ in $\mathbb{N} \setminus \{0\}$. Torej, množica naravnih števil $\mathbb{N}$ je neskončna.

Trditev 32 *Naj bo $A \subset B$. Če je A neskončna, potem je tudi B neskončna.*

Dokaz. Ker je množica A neskončna, obstajata $A' \subset A$ in bijekcija $f : A \to A'$. Naj bo $D = A' \cup (B \setminus A)$. Tedaj je $D \subseteq B$ in je preslikava

$$g(x) = \begin{cases} f(x) & x \in A' \\ x & x \in B \setminus A, \end{cases}$$

bijekcija med B in D. Torej je B neskončna. □

Posledica 33 *Vsaka podmnožica končne množice je končna.*

Posledica 34 *Naj bo $f : A \to B$ injektivna preslikava ter A neskončna. Potem je B neskončna.*

Zgledi: Naslednje množice so neskončne:

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$
- $\mathbb{N} \cup \{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}\}$
- $\mathcal{P}(\mathbb{N})$, $\mathbb{R} \times \mathbb{R}$.

Števna neskončnost

Množica A je **števno neskončna**, kadar je $A \sim \mathbb{N}$. Množica A je **števna**, kadar je končna ali števno neskončna.

Razred števno neskončnih množic označimo z $\aleph_0$ (beri: alef 0)

Zgled: Funkcija $f(m,n) = \binom{n+m+1}{2} + n$ je bijekcija med $\mathbb{N} \times \mathbb{N}$ in $\mathbb{N}$. Torej, množica $\mathbb{N} \times \mathbb{N}$ je števno neskončna.

Problem 2 *Naj bo Σ končna abeceda ter naj bo Σ^* množica vseh končnih besed na abecedo Σ. Ali velja $\Sigma \sim \mathbb{N}$?*

Problem 3 *Ali je $\mathbb{Q} \sim \mathbb{N}$?*

Moč kontinuuma

Izrek 35 (Cantor) *Množica vseh realnih števil na intervalu* $(0,1)$ *ni števno neskončna.*

Dokaz. Preslikava $f : n \mapsto \frac{1}{n+2}$ je injekcija iz $\mathbb{N}$ v $(0,1)$. Torej je $(0,1)$ neskončna množica.

Vsako število $x \in (0,1)$ lahko (enolično) zapišemo kot neskončno decimalno število

$$x = 0\,.\,x_1x_2x_3x_4\ldots$$

Torej, za število $\frac{1}{2}$ izberemo zapis $0.499999\ldots$ in ne zapis $0.50000\ldots$.

Predpostavimo, da je množica $(0,1)$ števna. Potem obstaja bijekcija $f : \mathbb{N} \to (0,1)$. Torej

$$\begin{aligned} f(0) &= 0.a_0^0a_1^0a_2^0a_3^0a_4^0a_5^0\ldots \\ f(1) &= 0.a_0^1a_1^1a_2^1a_3^1a_4^1a_5^1\ldots \\ f(2) &= 0.a_0^2a_1^2a_2^2a_3^2a_4^2a_5^2\ldots \\ f(3) &= 0.a_0^3a_1^3a_2^3a_3^3a_4^3a_5^3\ldots \\ &\ldots \end{aligned}$$

Obravnavajmo število

$$b = 0.b_0b_1b_2b_3b_4\ldots,$$

za katerega velja, da je

$$b_i = \begin{cases} 1, & a_i^i \neq 1 \\ 2, & a_i^i = 1\,. \end{cases}$$

Ker je $b \in (0,1)$, obstaja $k \in \mathbb{N}$ za katerega velja, da je $f(k) = b$. Obravnavajmo $b_k \in \{1,2\}$: premisli ali je $b_k = 1$ oz. $b_k = 2$!

□

Zadnji izrek nam implicira naslednjo posledico:

Posledica 36 *Velja*

$$(0,1) \not\sim \mathbb{N}\,.$$

Za množice, ki so enakomočne množici $(0,1)$, rečemo, da imajo moč **kontinuuma**. Ustrezno kardinalno število označimo s **c**.

Zgledi: Naslednje množice imajo moč kontinuuma:

- (a,b) za $a<b$: $f(x)=a+(b-a)x$ je ustrezna bijekcija med $(0,1)$ in (a,b);

- $\mathbb{R}^+$: ustrezna bijekcija je $f(x)=\frac{x}{1-x}$;

- $\mathbb{R}$: ustrezna bijekcija je $f(x)=\frac{1-2x}{x(1-x)}$.

Relacija $\preceq$

Množica A ima **manjšo ali enako moč** kot B, če obstaja kakšna injekcija $f : A \to B$. Pišemo $A \preceq B$.

Velja:

$$A \subseteq B \;\Rightarrow\; A \preceq B\,.$$

Definiramo lahko še **strogo manjšo moč**:

$$A \prec B \quad \equiv \quad A \preceq B \;\text{ in }\; A \not\sim B.$$

Izrek 37 (Shröder-Bernsteinov izrek) *Če $A \preceq B$ in $B \preceq A$, potem $A \sim B$.*

Izrek 38 (Izrek o trihotomiji) *Poljubni množici A in B sta primerljivi glede na njuno moč in velja natanko ena izmed možnosti: $A \prec B$ ali $B \prec A$ ali $A \sim B$.*

Trditev 39 *Relacija $\preceq$ je sovisna.*

Dokaz.

Izrek 40 (Izrek o surjekciji) *Za poljubni množici $A \neq \emptyset$ in B velja $A \preceq B$ natanko takrat, ko obstaja surjekcija $g : B \to A$.*

Za dve množici A, B pokažemo, da je $A \sim B$ na naslednje načine:

- poiščemo bijekcijo med njima;
- poiščemo injekcijo v obeh smereh;
- poiščemo surjekcijo v obeh smereh;
- poiščemo injekcijo in surjekcijo v isti smeri;
- pokažemo $A \sim C$ in $B \sim C$.

Naslednji izrek nam pove, da je števna neskončnost najmanjša neskončnost. Na vprašanje: *Ali sta $\aleph_0$ in $\mathbf{c}$ edini neskočnosti?* - bomo odgovorili v naslednjem razdelku.

Izrek 41 *Vsaka neskončna množica vsebuje števno neskončno podmnožico.*

Moč potenčne množice

Izrek 42 (Cantor) *Za poljubno množico A velja*

$$A \prec \mathcal{P}(A)$$

Dokaz. Najprej pokažimo, da je $A \preceq \mathcal{P}(A)$. Obravnavajmo preslikavo $g : \mathcal{P}(A) \to A$

$$g(X) = \begin{cases} x & X = \{x\} \\ \\ a & \text{sicer,} \end{cases}$$

kjer je a vnaprej izbran element iz A. Ker za vsak $x \in A$ velja $\{x\} \in \mathcal{P}(A)$, sklepamo, da je g surjekcija. Torej po izreku 40 sledi $A \preceq \mathcal{P}(A)$.

Zdaj pa pokažemo, da je $A \not\sim \mathcal{P}(A)$. Predpostavimo nasprotno. Potem obstaja bijekcija $f : A \to \mathcal{P}(A)$. Za nekatere elemente $x \in A$ velja $x \in f(x)$, za nekatere pa $x \notin f(x)$. Združimo slednje v množico:

$$B = \{x \in A; x \notin f(x)\}.$$

Ker je f bijekcija, obstaja $b \in A$ tako, da je $f(b) = B$. Če poskusimo odgovoriti na vprašanje: Ali je $b \in B$? - pridemo v protislovje, ker

- če $b \in B$, potem $b \notin f(b) = B$;
- če $b \notin B$, potem $b \in f(b) = B$.

□

Zadnji izrek nam takoj implicira naslednjo posledico. Ta nam pove, da obstaja neomejeno mnogo neskončnih množic, ki so vse različnih kardinalnosti.

Posledica 43 *Velja*

$$\mathbb{N} \prec \mathcal{P}(\mathbb{N}) \prec \mathcal{P}(\mathcal{P}(\mathbb{N})) \prec \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) \cdots$$

Hipoteza kontinuuma. *Ali je med* $\aleph_0$ *in* $\mathbf{c}$ *še kakšno kardinalno število?*

Nekaj uporabnih trditev in zgledov

Trditev 44 *Če je A neskončna in B števna je $A \cup B \sim A$.*

Trditev 45 *Če je A neskončna in B končna, potem je $A \setminus B \sim A$.*

Zgledi: Veljajo naslednje zveze:

- $(0,1) \sim (0,1] \sim [0,1) \sim [0,1]$.
- $\mathcal{P}(\mathbb{N}) \sim [0,1]$ in $[0,1] \sim \mathbb{R}$. Od tod, $\mathcal{P}(\mathbb{N}) \sim \mathbb{R}$.
- $\mathbb{N}^{\mathbb{N}} \sim \mathbb{R}^{\mathbb{N}} \sim \mathbb{R}$.
- $\mathbb{N} \sim \mathbb{N}^2 \sim \mathbb{N}^3 \ldots$
- Družina vseh *končnih* množic naravnih števil je števno neskončna.
- Družina sintaktično pravilnih programov v `Javi` je števno neskončna.

Relacije

Naj bodo $A_1, A_2, \ldots, A_n$ neprazne množice ter naj bo $R \subseteq A_1 \times A_2 \times \cdots \times A_n$. Potem rečemo, da je R **n-mestna relacija**.

Če $(x_1, x_2, \ldots, x_n) \in R$, potem rečemo, da so elementi $x_1, x_2, \ldots, x_n$ **v relaciji** R.

Lahko definiramo ter uporabljamo **relacijo-predikat**

$$R(x_1, x_2, \ldots, x_n) \quad \equiv \quad (x_1, x_2, \ldots, x_n) \in R$$

Zgledi:

1. Naj bo $A = \{a, b, c, d\}$ ter $R = \{(a, b), (b, c), (c, a), (c, d)\}$. Potem je $R \subseteq A \times A$ 2-mestna relacija.
2. 3-mestna relacija-predikat:

   $$S(x, y, z) \equiv x \text{ je otrok matere } y \text{ in očeta } z$$

3. Relaciji $<$ "manjši" ter $\leq$ "manjši ali enak" v $\mathbb{R}$

   $$(<) = \{(x, y)\,;\, x, y \in \mathbb{R} \text{ ter } x < y\}$$

   in

   $$(\leq) = \{(x, y)\,;\, x, y \in \mathbb{R} \text{ ter } x \leq y\}$$

4. Relacija deli $\mid$ v $\mathbb{N}^+$, definirana kot:

   $$a \mid b \quad \equiv \quad \exists k \in \mathbb{N}^+ : b = k \cdot a$$

5. Relacija vsebovanost $\subseteq$ v $\mathcal{P}(A)$.

Dvomestne oz. binarne relacije

Naj bo $R \subseteq A \times B$ dvomestna relacija. Rečemo, da je R relacija **iz** množice A **v** množico B. Uporabljamo tudi pisavo $a\,R\,b$, če $(a, b) \in R$.

Za $A = B$ rečemo, da je R relacija **na** množici A.

Domena oz. **definicijsko območje** relacije R je

$$\mathcal{D}_R = \{x \in A\,;\, \exists y \in B : x\,R\,y\}$$

Zaloga vrednosti relacije R je

$$\mathcal{R}_R = \{y \in B\,;\, \exists x \in A : x\,R\,y\}$$

Nekatere znane relacije:

- **polna** relacija $T_{A,B} = A \times B$
- **ničelna** relacija $\emptyset$
- **identitetna** relacija $I_A = \{(x, x) : x \in A\}$.

Graf relacije G_R

Naj bo A končna množica ter R relacija na A. Relacijo R grafično predstavimo tako, da:

1. za vsak element $a \in A$ izberemo točko v $\mathbb{R}^2$, to točko kar poimenujemo a;
2. za vsak par $(a, b) \in R$ narišemo usmerjeno povezavo iz točke a do točke b.

Tako risbo imenujemo **graf** relacije R ter ga označimo z G_R.

Zgled: Naj bo $A = \{a, b, c, d\}$ ter $R = \{(a, b), (a, c), (b, c), (c, a), (c, c), (c, d)\} \subseteq A \times A$. Graf G_R relacije R je:

Relacijska matrika M_R

Naj bo A končna množica ter R relacija na A. Vsakemu elementu iz A priredimo eno vrstico ter en stolpec matrike M_R tako, da v presečišču vrstice $a \in A$ ter stolpca $b \in A$ zapišemo 1, če je $a\,R\,b$, v nasprotnem primeru pa zapišemo 0, tj.

$$M_R[a,b] \;=\; \begin{cases} 1 & a\,R\,b; \\ 0 & \text{sicer.} \end{cases}$$

Matriko M_R imenujemo **relacijska matrika** relacije R.

Zgled: Naj bo $A = \{a,b,c,d\}$ ter $R = \{(a,b),(a,c),(b,c),(c,a),(c,c),(c,d)\} \subseteq A \times A$. Matrika M_R relacije R je:

Osnovne lastnosti binarnih relacij

1. R je **refleksivna**, če

$$\forall a \in A : a \, R \, a$$

2. R je **simetrična**, če:

$$\forall a, b \in A : (a \, R \, b \Rightarrow b \, R \, a)$$

3. R je **antisimetrična**, če:

$$\forall a, b \in A : (a \, R \, b \ \wedge \ b \, R \, a \ \Rightarrow \ a = b)$$

4. R je **tranzitivna**, če:

$$\forall a, b, c \in A : (a \, R \, b \ \wedge \ b \, R \, c \ \Rightarrow a \, R \, c)$$

Naloga 20 *Naj bo A neprazna množica. Ugotovi, katere od zgornjih lastnosti imata naslednji relaciji:*

- *relacija I_A;*
- *relacija $\subseteq$ na $\mathcal{P}(A)$.*

Druge lastnosti binarnih relacij

1. R je **irefleksivna**, če

$$\forall a \in A : \neg a \, R \, a$$

2. R je **asimetrična**, če:

$$\forall a, b \in A : (a \, R \, b \Rightarrow \neg b \, R \, a)$$

3. R je **itranzitivna**, če:

$$\forall a, b, c \in A : (a \, R \, b \text{ in } b \, R \, c \Rightarrow \neg a \, R \, c)$$

4. R je **sovisna**, če

$$\forall a, b \in A : (a \neq b \Rightarrow a \, R \, b \vee b \, R \, a)$$

5. R je **strogo sovisna**, če

$$\forall a, b \in A : (a \, R \, b \vee b \, R \, a)$$

6. R je **enolična**, če

$$\forall a, b, c \in A : (a \, R \, b \wedge a \, R \, c \Rightarrow b = c)$$

Naloga 21 *Za relaciji $<$ ter $\leq$ na $\mathbb{R}$ ugotovi, katere od zgornjih lastnosti veljajo.*

Operacije na relacijah

Naj bosta R, S relaciji iz A v B. Ker $R, S \subseteq A \times B$, lahko naravno definiramo **unijo**, **presek**, **razliko** in **simetrično razliko** na relacijah R in S:

$$R \cup S \qquad R \cap S \qquad R \setminus S \qquad R + S$$

Velja:

$$\begin{aligned} x\, R \cup S\, y &\quad\Leftrightarrow\quad x\, R\, y \vee x\, S\, y \\ x\, R \cap S\, y &\quad\Leftrightarrow\quad x\, R\, y \wedge x\, S\, y \\ x\, R \setminus S\, y &\quad\Leftrightarrow\quad x\, R\, y \wedge \neg x\, S\, y \\ x\, R + S\, y &\quad\Leftrightarrow\quad x\, R\, y \oplus x\, S\, y \end{aligned}$$

Komplement oz. **dopolnitev**:

$$R^c \;=\; (A \times B) \setminus R$$

Velja:

$$(R^c)^c \;=\; R\,.$$

Obratna oz. **inverzna** relacija $R^{-1} \subseteq B \times A$:

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

Produkt relacij $R, S \subseteq A \times A$:

$$R * S = \{(x, y); \exists z \in A : (x, z) \in R \text{ in } (z, y) \in S\}$$

Velja:

$$\begin{aligned} x\,R\,y &\Leftrightarrow \neg x\,R^c\,y \\ x\,R\,y &\Leftrightarrow y\,R^{-1}\,x \\ x\,R * S\,y &\Leftrightarrow \exists z : (x\,R\,z \wedge z\,S\,y) \end{aligned}$$

Lastnosti operacij z relacijami

Naj bodo R, S, T relacije na A. Potem veljajo naslednje lastnosti:

1. $(R^{-1})^{-1} = R$
2. $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$
3. $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$
4. $(R * S)^{-1} = S^{-1} * R^{-1}$
5. $R * (S \cup T) = R * S \cup R * T$
   $(S \cup T) * R = S * R \cup T * R$
6. $(R * S) * T = R * (S * T)$
7. $R * I_A = I_A * R = R$
8. $R \subseteq S \quad \Rightarrow \quad R * T \subseteq S * T \quad \text{in} \quad T * R \subseteq T * S$

Algebraična karakterizacija lastnosti operacij

Naj bo R relacija na A. Potem velja:

1. R je refleksivna $\Leftrightarrow$ $I_A \subseteq R$
2. R je irefleksivna $\Leftrightarrow$ $R \cap I_A = \emptyset$
3. R je simetrična $\Leftrightarrow$ $R = R^{-1}$
4. R je antisimetrična $\Leftrightarrow$ $R \cap R^{-1} \subseteq I_A$
5. R je asimetrična $\Leftrightarrow$ $R \cap R^{-1} = \emptyset$
6. R je tranzitivna $\Leftrightarrow$ $R * R \subseteq R$
7. R je itranzitivna $\Leftrightarrow$ $R * R \cap R = \emptyset$
8. R je sovisna $\Leftrightarrow$ $R \cup R^{-1} \cup I_A = A \times A$
9. R je strogo sovisna $\Leftrightarrow$ $R \cup R^{-1} = A \times A$
10. R je enolična $\Leftrightarrow$ $R^{-1} * R \subseteq I_A$

Potence relacije

Potence relacije $R \subseteq A \times A$ definiramo takole:

- $R^0 = I_A$
- $R^{n+1} = R^n * R$

Velja:

$$\begin{aligned} R^n * R^m &= R^{n+m} \\ (R^n)^m &= R^{n\,m} \\ Q \subseteq R &\Rightarrow Q^n \subseteq R^n \end{aligned}$$

Grafovski pomen potence

Trditev 46 *Velja $a\, R^k\, b$ natanko takrat, ko v grafu G_R obstaja sprehod dolžine k iz točke a v točko b.*

Dokaz.

Negativne potence definiramo takole:

$$R^{-n} \equiv (R^{-1})^n, \quad \text{za } n > 0.$$

Opomba: Če sta m in n celi števili različnega predznaka, potem $R^n * R^m$ ni nujno enako R^{n+m}.

Zgled: Naj bo $A = \{a, b, c\}$ in $R = \{(a, c), (b, c)\} \subseteq A \times A$. Tedaj je $R^{-1} = \{(c, a), (c, b)\}$. Dobimo pa

$$R * R^{-1} = \{(a, a), (a, b), (b, a), (b, b)\} \neq I_A\,.$$

Relaciji R^+ in R^*

Definiramo relaciji:

$$R^+ = R \cup R^2 \cup R^3 \cup \cdots$$

ter

$$R^* = I_A \cup R \cup R^2 \cup R^3 \cup \cdots$$

Velja:

$$\begin{aligned} x\, R^+\, y &\sim \exists n \geq 1 : x\, R^n\, y \\ x\, R^*\, y &\sim \exists n \geq 0 : x\, R^n\, y \\ R^* &= I_A \cup R^+ \\ R^+ &= R * R^* \\ R^* &= R^* * R^* \end{aligned}$$

Zgled: Naj bo $A = \{a, b, c, d\}$ ter $R = \{(a, b), (a, c), (b, c), (c, a), (c, c), (c, d)\} \subseteq A \times A$. Poišči R^+ in R^*.

Vprašanje 7 *Kako iz G_R konstruiramo grafa G_{R^+} in G_{R^*}?*

Zgled: Za relacijo R iz prejšnjega zgleda nariši G_{R^+} in G_{R^*}.

Naloga 22 *Pokaži:*

1. *Če je R tranzitivna relacija, potem $R = R^+$;*
2. *Če je R tranzitivna in refleksivna relacija, potem $R = R^*$.*

Ovojnice relacij

Naj bo $R \subseteq A \times A$ ter naj bo $\mathcal{L}$ neka relacijska lastnost. Relacija $R^{\mathcal{L}}$ je **ovojnica** relacije R **glede na** lastnost $\mathcal{L}$, če velja:

(O1). $R \subseteq R^{\mathcal{L}}$

(O2). $R^{\mathcal{L}}$ ima lastnost $\mathcal{L}$

(O3). Če ima relacija $S \subseteq A \times A$ lastnost $\mathcal{L}$ ter $R \subseteq S$, potem $R^{\mathcal{L}} \subseteq S$.

Izrek 47 *Relacija* $R^{\text{ref}} := I \cup R$ *je refleksivna ovojnica relacije* R.

Dokaz. Očitno $R \subseteq R^{\text{ref}}$ in $I \subseteq R^{\text{ref}}$, tj. veljata (O1) in (O2).

Pokažimo še lastnost (O3). Naj bo S refleksivna relacija, ki vsebuje R, tj. $I \subseteq S$ in $R \subseteq S$. Pokazati moramo, da je $R^{\text{ref}} \subseteq S$. To pa je očitno, ker $R^{\text{ref}} = I \cup R$ in $I \cup R \subseteq S$. □

Izrek 48 *Relacija* $R^{\text{sim}} := R \cup R^{-1}$ *je simetrična ovojnica relacije* R*.*

Dokaz. Očitno $R \subseteq R^{\text{sim}}$, tj. velja (O1). Pokažimo lastnost (O2):

$$(R^{\text{sim}})^{-1} = (R \cup R^{-1})^{-1} = R^{-1} \cup (R^{-1})^{-1} = R^{-1} \cup R = R^{\text{sim}}.$$

Zdaj pa pokažimo še lastnost (O3). Naj bo S simetrična relacija, ki vsebuje R, tj. $S = S^{-1}$ in $R \subseteq S$. Pokazati moramo, da je $R^{\text{sim}} \subseteq S$. Velja $R^{-1} \subseteq S^{-1} = S$. Torej $R \cup R^{-1} \subseteq S$ od tod pa $R^{\text{sim}} \subseteq S$, kar je bilo treba dokazati. □

Izrek 49 *Dokaži, da je* R^+ *tranzitivna ovojnica relacije* R*.*

Dokaz. Ker je $R \subseteq R^+$, velja (O1). Pokažimo (O2), tj. da je R^+ tranzitivna:

$$R^+ \cup R^+ * R^+ = R^+ * (I \cup R^+) = R^+ * R^* = R * R^* * R^* = R * R^* = R^+$$

iz česar sledi, da je $R^+ * R^+ \subseteq R^+$, to pa je pogoj tranzitivnosti.

Preostane nam še lastnost $(O3)$. Recimo $Q \supseteq R$ in, da je Q tranzitivna. Torej $Q = Q^+$ (to smo že dokazali). Od tod pa

$$Q = Q^+ = (R \cup Q)^+ \supseteq R^+$$

iz česar sledi, da je $R^+ \subseteq Q$. □

Izrek 50 *Dokaži, da je R^* tranzitivna in refleksivna ovojnica relacije R.*

Dokaz. Ker je $R \subseteq R^*$, velja (O1). Pokažimo (O2), tj. da je R^* refleksivna in tranzitivna. Refleksivnost sledi iz $I \subseteq R$, tranzitivnost pa sledi iz $R^* * R^* = R^*$.

Preostane nam še lastnost $(O3)$. Recimo $Q \supseteq R$ in Q refleksivna ter tranzitivna. Torej $Q = Q^*$ (to smo že dokazali). Od tod pa

$$Q = Q^* = (R \cup Q)^* \supseteq R^*$$

iz česar sledi, da je $R^* \subseteq Q$. □

Iz prejšnjih štirih izrekov velja:

- $R^{\text{refl}} = R \cup I_A$
- $R^{\text{sim}} = R \cup R^{-1}$
- $R^{\text{tranz}} = R^+ = R \cup R^2 \cup R^3 \cup \cdots$
- $R^{\text{refl+tranz}} = R^* = I_A \cup R \cup R^2 \cup R^3 \cup \cdots$

Ekvivalenčne relacije

Relacija $R \subseteq A \times A$ je **ekvivalenčna** oz. **enakovrednost**, če je

- refleksivna,
- simetrična in
- tranzitivna.

Naj bo R ekvivalenčna relacija na A ter naj bo $x \in A$

- $R[x] = \{y \in A; x\, R\, y\}$ je **ekvivalenčni razred** x-a;
- $A/R = \{R[x]; x \in A\}$ je **faktorska** oz. **kvocientna množica**.

Naloga 23 *Pokaži, da je* $\equiv \pmod{12}$ *ekvivalenčna relacija v* $\mathbb{Z}$. *Kateri so ekvivalenčni razredi?*

Izrek 51 *Relacija R na A je enakovrednost natanko takrat, ko velja*

$$\mathcal{D}_R = A \quad in \quad R^{-1} * R = R\,.$$

Dokaz. Recimo, da je R enakovrednost. Potem nam pogoj refleksivnosti $I_A \subseteq R$ zagotovi, da je $\mathcal{D}_R = A$. Iz simetričnosti ter tranzitivosti velja

$$R = R^{-1} \quad \text{in} \quad R^2 \subseteq R\,.$$

Od tod pa dobimo

$$R^{-1} * R = R * R = R * (I \cup R) = R * I \cup R^2 = R^2 \cup R = R\,.$$

Zdaj pa pokažimo v drugo smer. Obravnavajmo vse tri lastnosti posebej.

simetričnost: Lastnost pokažemo takole

$$R^{-1} = (R^{-1} * R)^{-1} = R^{-1} * (R^{-1})^{-1} = R^{-1} * R = R\,.$$

tranzitivnost: Iz pogoja simetričnosti $R^{-1} = R$ dobimo, da je $R^2 = R^{-1} * R = R$, kar nam zagotovi pogoj tranzitivnosti $R^2 \subseteq R$.

refleksivnost: Iz $\mathcal{D}_R = A$ sledi, da za vsak $x \in A$, obstaja $y \in A$ tako, da je $x\,R\,y$. Potem pa iz simetričnosti dobimo $y\,R\,x$. Od tu pa naprej po tranzitivnosti $x\,R\,x$, kar je lastnost refleksivnosti.

□

Trditev 52 *Naj bo R ekvivalenčna relacija na A ter naj bosta $x, y \in A$. Potem velja*

$$R[x] = R[y] \;\Leftrightarrow\; x\,R\,y$$

Dokaz. Iz $a\,R\,a$ sledi, da je $a \in R[a]$ za vsak $a \in A$. Torej, iz $R[x] = R[y]$ sledi, da je $y \in R[x]$ in od tod $x\,R\,y$.

Pokažimo obratno smer. Recimo $x\,R\,y$. Za poljuben element $a \in R[x]$ iz $y\,R\,x$ in $x\,R\,a$ po tranzitivnosti dobimo $y\,R\,a$, tj. $a \in R[y]$. To pa nam zagotovi $R[x] \subseteq R[y]$. Podobno lahko pokažemo, da je $R[y] \subseteq R[x]$. Od tod pa dobimo $R[x] = R[y]$. □

Trditev 53 *Naj bo R ekvivalenčna relacija na A ter naj bosta $x, y \in A$, za katera velja $(x, y) \notin R$. Potem $R[x] \cap R[y] = \emptyset$.*

Dokaz. Recimo da $a \in R[x] \cap R[y]$. Potem nam $x\,R\,a$ in $a\,R\,y$ po tranzitivnosti zagotovita, da je $x\,R\,y$, kar je narobe. □

Spomnimo se:

$\mathcal{B} = \{B_1, B_2, \ldots, B_k\}$ je **razbitje** oz. **particija** množice A, če velja:

1. $\emptyset \subset B_i \subseteq A$
2. $B_i \cap B_j = \emptyset$ za $i \neq j$
3. $A = B_1 \cup B_2 \cup \cdots \cup B_k$.

Izrek 54 *Naj bo R ekvivalenčna relacija na A. Potem je faktorska množica R/A razbitje množice A.*

Dokaz. Očitno za vsak $a \in A$ velja $R[a] \subseteq A$, kar je prva lastnost razbitja. Iz refleksivnosti za vsak $a \in A$ velja $a\,R\,a$ in od tod $a \in R[a]$. Tako dobimo tretjo lastnost razbitja

$$\bigcup_{X \in A/R} = A\,.$$

Preostane nam pokazati še drugo lastnost, tj., da za poljubna različna $R[a]$ in $R[b]$ velja $R[a] \cap R[b] = \emptyset$. Iz $R[a] \neq R[b]$ po trditvi 52 sledi, da je $(a, b) \notin R$. Od tod pa po trditvi 53 sledi, da je $R[a] \cap R[b] = \emptyset$. □

Izrek 55 *Naj bo* $\mathcal{B} = \{A_1, A_2, \ldots, A_k\}$ *razbitje množice* A*, potem je relacija:*

$$R = \{(a, b)\,;\, \exists i : a \in A_i \wedge b \in A_i\} = \bigcup_{i \in I} A_i \times A_i$$

enakovrednost.

Dokaz. Preverimo posebej vsako od lastnosti enakovrednosti.

refleksivnost:

simetričnost:

tranzitivnost:

Urejenosti

Relacija $(M, \preceq)$ je **delna urejenost**, če veljajo naslednje tri lastnosti:

- **refleksivnost:** $\forall a \in M : a \preceq a$
- **antisimetričnost:** $\forall a, b \in M : a \preceq b \text{ in } b \preceq a \Rightarrow a = b$
- **tranzitivnost:** $\forall a, b, c \in M : a \preceq b \text{ in } b \preceq c \Rightarrow a \preceq c$

Linearna urejenost je sovisna delna urejenost.

Zgled: Relacija $\leq$ na množicah $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ je linearna urejenost.

Naloga 24 *Naj bo A neprazna množica. Pokaži, da je $(\mathcal{P}(A), \subseteq)$ delna urejenost.*

Naloga 25 *Pokaži, da je množica deliteljev $D(n)$ naravnega števila n z relacijo deljivosti $\mid$ delna urejenost.*

Elementa $x, y \in M$ sta **primerljiva**, če je $x \preceq y$ ali $y \preceq x$, sicer sta **neprimerljiva**.

Če $x \preceq y$ ter $x \neq y$, potem pišemo tudi $x \prec y$.

Element x je **neposredni predhodnik** y oz. y je **neposredni naslednik** x, če

- $x \prec y$,
- ne obstaja "vmesni" element, tj. ne obstaja element $z \in M$ tako, da je $x \prec z \prec y$.

Element $a \in M$ je **minimalen**, če

$$\forall x \in M : (x \preceq a \ \Rightarrow \ x = a) .$$

Element $a \in M$ je **maksimalen**, če

$$\forall x \in M : (a \preceq x \ \Rightarrow \ x = a) .$$

Element $a \in M$ je **prvi** oz. **najmanjši**, če

$$\forall x \in M : a \preceq x .$$

Element $a \in M$ je **zadnji** oz. **največji**, če

$$\forall x \in M : x \preceq a .$$

Trditev 56 *V delni urejenosti* $(M, \preceq)$ *velja:*

1. *Če je* $a \in M$ *prvi, potem je minimalen;*
2. *Če je* $a \in M$ *zadnji, potem je maksimalen;*
3. *Če sta* $a_1, a_2 \in M$ *prva, potem* $a_1 = a_2$*;*
4. *Če sta* $a_1, a_2 \in M$ *zadnja, potem* $a_1 = a_2$*.*

Dokaz.

Trditev 57 *V linearni urejenosti* $(M, \preceq)$ *velja:*

1. *Če je* $a \in M$ *minimalen, potem je prvi;*
2. *Če je* $a \in M$ *maksimalen, potem je zadnji.*

Dokaz.

Hassejev diagram

Hassejev diagram delne urejenosti $(M, \preceq)$ je risba, pri kateri elemente množice A predstavimo s točkami v ravnini tako, da za poljubne $a, b \in M$ velja

- če $a \preceq b$, potem b leži "nad" a;
- a in b povežemo, če je a neposredni predhodnik b-ja.

Naloga 26 *Nariši Hassejev diagram delne urejenosti* $(\mathcal{P}(\{a, b, c\}), \subseteq)$.

Naloga 27 *Nariši Hassejev diagram delne urejenosti* $(D(60), |)$
.

Inverzna urejenost

Inverz urejenosti $\preceq$ označimo z $\succeq$, tj.

$$\succeq := \preceq^{-1}$$

Trditev 58 *Če je* $(M, \preceq)$ *delna urejenost, potem je tudi* $(M, \succeq)$ *delna urejenost. Velja še:*

1. *če je* x *minimalen za* $\preceq$*, potem je* x *maksimalen v* $\succeq$*;*

2. *če je* x *prvi za* $\preceq$*, potem je* x *zadnji v* $\succeq$*.*

Vprašanje 8 *Če je* $(M, \preceq)$ *linearna urejenost, ali je potem tudi* $(M, \succeq)$ *linearna urejenost?*

Produkt urejenosti

Za delni urejenosti $(M_1, \preceq_1)$ in $(M_2, \preceq_2)$ lahko definiramo urejenost $(M_1, \preceq_1) \times (M_2, \preceq_2)$ z množico $M_1 \times M_2$ ter relacijo

$$(x_1, x_2) \preceq (y_1, y_2) \quad \equiv \quad x_1 \preceq_1 y_1 \text{ in } x_2 \preceq_2 y_2$$

Zgled: $(\mathbb{N}, \leq) \times (\mathbb{N}, \leq)$

Trditev 59 *Če sta* $(M_1, \preceq_1)$ *in* $(M_2, \preceq_2)$ *delni urejenosti, potem je tudi* $(M_1, \preceq_1) \times (M_2, \preceq_2)$ *delna urejenost.*

Leksikografska urejenost

Naj bo $(M, \preceq)$ linearna urejenost. **Leksikografsko** urejenost $\leq_{\text{lex}}$ na množici $M \times M$ definiramo takole:

$$(m_1, n_1) \preceq_{\text{lex}} (m_2, n_2) \;\equiv\; m_1 \prec m_2 \;\vee\; (m_1 = m_2 \wedge n_1 \preceq n_2)$$

Zgled: $(\mathbb{N} \times \mathbb{N}, \leq_{\text{lex}})$

Trditev 60 $(M \times M, \preceq_{\text{lex}})$ *je linearna urejenost.*

Zgled: Slovarček

Druge urejenosti

Med tranzitivnimi relacijami, poleg linearne ter delne urejenosti, nas običajno zanimajo še:

1. **navidezna urejenost:** tranzitivnost + refleksivnost;
2. **šibka urejenost:** tranzitivnost + stroga sovisnost;
3. **polurejenost:** tranzitivnost + antisimetričnost;
4. **stroga delna urejenost:** tranzitivnost + irefleksivnost;
5. **stroga linearna urejenost:** tranzitivnost + irefleksivnost + sovisnost;

Lastnosti:

1. Če je R nekakšna urejenost, potem je R^{-1} urejenost istega tipa.

2. Naj bo R nekakšna urejenost na A ter naj bo $B \subseteq A$. **Zožitev** $R_{|B} := R \cap B \times B$ je urejenost iste vrste.

3. Če je relacija R polurejenost, je $R \cup I$ delna urejenost in $R \setminus I$ stroga delna urejenost.

4. Naj bo R navidezna urejenost, potem je $R \cap R^{-1}$ enakovrednost.

Topološko urejanje

Naj bo $(M, \preceq)$ polurejenost, kjer je M končna. **Pravilno oštevilčenje** je preslikava $i : M \to \{1, \ldots, |M|\}$, za katero velja:

$$x \neq y \;\Rightarrow\; i(x) \neq i(y) \quad \text{in} \quad x \prec y \;\Rightarrow\; i(x) < i(y)$$

Izrek 61 *Vsako končno polurejeno množico lahko pravilno oštevilčimo.*

Dokaz. Pravilno oštevilčenje dobimo z naslednjim postopkom:

$S := M; j := 0;$
while $S \neq \emptyset$ **do**
    izberi: x je minimalni element S;
    $j := j + 1;$
    $i(x) := j;$
    $S := S \setminus \{x\};$
end

□

Pravilnemu oštevilčenju ustreza urejanje oz. sortiranje elementov v vrsto

$$a_1,\ a_2,\ a_3, \ldots,\ a_{|M|}$$

tako, da mora za $a_i \prec a_j$ veljati $i < j$. Takemu sortiranju rečemo **topološko urejanje**.

Supremum in Infimum

Najmanjša zgornja meja $\sup(a, b)$ elementov a ter b je element $\gamma \in M$, za katerega velja:

- $a \preceq \gamma$ in $b \preceq \gamma$;
- če za poljuben $x \in M$ velja $a \preceq x$ in $b \preceq x$, potem $\gamma \preceq x$.

Največja spodnja meja $\inf(a, b)$ elementov a ter b je element $\lambda \in M$, za katerega velja:

- $\lambda \preceq a$ in $\lambda \preceq b$;
- če za poljuben $x \in M$ velja $x \preceq a$ in $x \preceq b$, potem $x \preceq \lambda$.

Trditev 62 *V delni urejenosti so naslednje trditve enakovredne:*

$$a \preceq b \quad \Leftrightarrow \quad a = \inf(a, b) \quad \Leftrightarrow \quad b = \sup(a, b)$$

Mreže

Relacijska definicija

Definicija R. Delna urejenost $(M, \preceq)$ je **mreža**, če za vsak par $a, b \in M$ obstajata elementa:

- $\sup\{a, b\}$
- $\inf\{a, b\}$.

Zgled: Delna urejenost $(D(n), |)$ je mreža in za vsak $a, b \in D(n)$ velja

$$\inf(a, b) = \gcd(a, b) \quad \text{in} \quad \sup(a, b) = \operatorname{lcm}(a, b).$$

Zgled: Delna urejenost $(\mathcal{P}(A), \subseteq)$ je mreža, za vsak $X, Y \subseteq A$ pa velja:

$$\inf(X, Y) = X \cap Y \quad \text{in} \quad \sup(X, Y) = X \cup Y.$$

Algebrska definicija

Definicija A. Algebrajska struktura $(M, \vee, \wedge)$ je **mreža**, če veljajo naslednje lastnosti:

- **idempotentnost:** $a \vee a = a$
  $a \wedge a = a$

- **komutativnost:** $a \vee b = b \vee a$
  $a \wedge b = b \wedge a$

- **asociativnost:** $(a \vee b) \vee c = a \vee (b \vee c)$
  $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

- **absorpcija:** $a \vee (a \wedge b) = a$
  $a \wedge (a \vee b) = a$

Zgled: Izjavni račun $(\{0, 1\}, \wedge, \vee)$ je mreža.

Zveza med algebrajsko ter relacijsko definicijo mreže

Velja naslednje:

$$a \preceq b \quad \Leftrightarrow \quad a \vee b = b \quad (\Leftrightarrow \quad a \wedge b = a)$$

ter

$$\sup\{a, b\} = a \vee b \quad \text{in} \quad \inf\{a, b\} = a \wedge b.$$

Podmreže

Naj bo $(M, \vee, \wedge)$ mreža ter N neprazna podmnožica v M tako, da velja pogoj

$$\forall a, b \in N : a \vee b \in N \ \text{ in } \ a \wedge b \in N.$$

Potem rečemo, da je $(N, \vee, \wedge)$ **podmreža** v $(M, \vee, \wedge)$.

Interval med $a, b \in M$ je

$$[a, b] = \{x : a \preceq x \preceq b\}.$$

Omejenost in komplementarnost

Mreža je **omejena**, ko v njej obstaja največji element 1 in najmanjši element 0:

$$\forall a : 0 \preceq a \preceq 1,$$

oz. ekvivalentno:

$$0 \vee a = a \quad \text{in} \quad 0 \wedge a = 0$$

$$1 \vee a = 1 \quad \text{in} \quad 1 \wedge a = a.$$

Trditev 63 *Vsaka končna mreža je omejena.*

Dokaz.

□

V omejeni mreži je element b **komplement** elementa a, če velja

$$a \vee b = 1 \quad \text{in} \quad a \wedge b = 0.$$

Mreža je **komplementarna**, če ima vsak element komplement.

Opomba 1 *V splošnem ima element lahko več komplementov.*

Homomorfizem mrež

Naj bosta $(M, \vee, \wedge)$ ter $(N, \sqcup, \sqcap)$ mreži. Preslikava $h : M \to N$ je **homomorfizem mrež**, če $\forall x, y \in M$ velja

$$h(x \vee y) = h(x) \sqcup h(y) \quad \text{in} \quad h(x \wedge y) = h(x) \sqcap h(y).$$

Kadar je h bijekcija, imamo **izomorfizem mrež**.

Če sta M ter N omejeni mreži, potem surjektivni homomorfizem h ohranja "mejne" elemente:

$$h(0_M) = 0_N \quad \text{in} \quad h(1_M) = 1_N.$$

Distributivne mreže

Mreža je **distributivna**, če veljata oba distributivnostna zakona:

(D1) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

(D2) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Trditev 64 *Če v mreži* $(M, \vee, \wedge)$ *velja eden od zakonov* $(D1)$ *in* $(D2)$*, potem velja tudi drugi.*

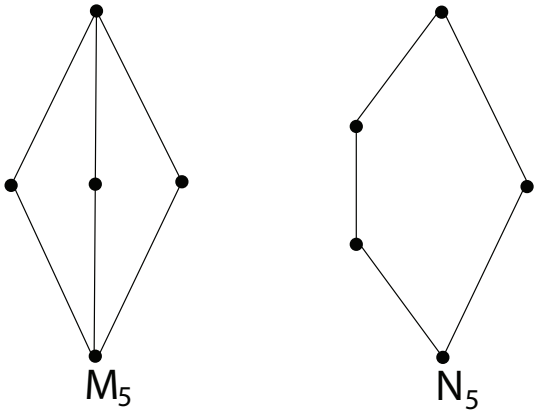
Dokaz. Predpostavimo, da velja $(D1)$ ter izpeljimo $(D2)$:

$$\begin{aligned} a \vee (b \wedge c) &= (a \vee (a \wedge c)) \vee (b \wedge c) \\ &= a \vee ((a \wedge c) \vee (b \wedge c)) \\ &= a \vee ((c \wedge a) \vee (c \wedge b)) \\ &= a \vee (c \wedge (a \vee b)) \\ &= a \vee ((a \vee b) \wedge c) \\ &= (a \wedge (a \vee b)) \vee ((a \vee b) \wedge c) \\ &= ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) \\ &= (a \vee b) \wedge (a \vee c) \end{aligned}$$

Podobno pokažemo, da iz $(D2)$ sledi $(D1)$. □

Opis distributivnih mrež

Naloga 28 *Pokaži, da mreži M_5 in N_5 nista distributivni.*



Izrek 65 (Birkhoff) *Mreža je distributivna natanko takrat, ko ne vsebuje M_5 in N_5 kot podmreže.*

Booleova algebra

Komplementarni distributivni mreži rečemo **Booleova algebra**.

Trditev 66 *V Booleovi algebri ima vsak element natanko en komplement.*

Dokaz. Recimo, da sta b in c komplementa elementa a. Tedaj velja

$$\begin{aligned} b &= b \wedge 1 \\ &= b \wedge (a \vee c) \\ &= (b \wedge a) \vee (b \wedge c) \\ &= 0 \vee (b \wedge c) \\ &= (a \wedge c) \vee (b \wedge c) \\ &= (a \vee b) \wedge c \\ &= 1 \wedge c \\ &= c \end{aligned}$$

□

Komplement elementa a označimo z $\neg a$.

Booleovo algebro označimo z $\mathcal{B} = (B, \vee, \wedge, \neg)$.

Trditev 67 *Naj bo $h : B_1 \to B_2$ izomomorfizem Booleovih algeber. Potem velja*

$$\forall x \in B_1 : h(\neg x) = \neg h(x).$$

De Morganova zakona

Trditev 68 *V Booleovi algebri veljata De Morganova zakona:*

$$\neg(a \wedge b) = \neg a \vee \neg b \quad \textit{in} \quad \neg(a \vee b) = \neg a \wedge \neg b$$

Dokaz. Pokažimo le prvi zakon, dokaz drugega je analogen. Za dokaz bo dovolj, če preverimo naslednji zvezi:

$$(a \wedge b) \wedge (\neg a \vee \neg b) = 0$$

ter

$$(a \wedge b) \vee (\neg a \vee \neg b) = 1$$

Prvo zvezo izpeljemo takole:

$$\begin{aligned}(a \wedge b) \wedge (\neg a \vee \neg b) &= a \wedge (b \wedge (\neg a \vee \neg b)) \\ &= a \wedge [(b \wedge \neg a) \vee (b \wedge \neg b)] \\ &= a \wedge b \wedge \neg a \\ &= b \wedge 0 \\ &= 0.\end{aligned}$$

Zdaj pa še drugo zvezo, pa bo konec dokaza:

$$\begin{aligned}(a \wedge b) \vee (\neg a \vee \neg b) &= ((a \vee \neg a) \wedge (b \vee \neg a)) \vee \neg b \\ &= (1 \wedge (b \vee \neg a)) \vee \neg b \\ &= b \vee \neg b \vee a \\ &= 1 \vee a \\ &= 1.\end{aligned}$$

□

Dualnost

Naj bo $\mathcal{B} = (B, \vee, \wedge, \neg)$ Booleova algebra.

Lahko priredimo novo algebro $\mathcal{B}^* = (B, \wedge, \vee, \neg)$.

Velja:

- 0 v $\mathcal{B}$ je 1 v $\mathcal{B}^*$;
- 1 v $\mathcal{B}$ je 0 v $\mathcal{B}^*$;
- $\vee$ v $\mathcal{B}$ je $\wedge$ v $\mathcal{B}^*$;
- $\wedge$ v $\mathcal{B}$ je $\vee$ v $\mathcal{B}^*$;

Vprašanje 9 *Kako dobimo Hassejev diagram algebre $\mathcal{B}^*$ iz diagrama algebre $\mathcal{B}$?*

Opomba 2 *Za vsako trditev $\mathcal{T}$ obstaja dualna trditev $\mathcal{T}^*$, ki jo dobimo iz $\mathcal{T}$ tako, da zamenjamo $\vee$ and $\wedge$. Opazimo, da je $(D_1)^* = (D_2)$ oz. $(D_2)^* = (D_1)$.*

Opis Booleovih algeber

Naloga 29 *Naj bo A množica. Preveri, da je $(\mathcal{P}(A), \cup, \cap)$ Booleova algebra. Kako je definiran komplement $\neg X$ za poljubno množico $X \in \mathcal{P}(A)$?*

Izrek 69 (Stone) *Vsaka Booleova algebra je izomorfna Booleovi algebri $(\mathcal{P}(A), \cup, \cap)$ za neko množico A.*

Vprašanje 10 *Ali obstaja Booleova algebra z 10 elementi?*

Teorija števil

Vsebina:

1. Zgornji in spodnji celi del

2. Deljivost in Evklidov algoritem

3. Linearna diofantska enačba z dvema neznankama

4. Praštevila

5. Kongruenca

6. Eulerjeva funkcija

7. Uporaba v kriptografiji

Zgornji in spodnji celi del

Spodnji celi del

$$\lfloor x \rfloor = \max\{k \in \mathbb{Z};\, k \leq x\}$$

Zgornji celi del

$$\lceil x \rceil = \min\{k \in \mathbb{Z};\, k \geq x\}$$

Zgledi:

Lastnosti:

1. $x \in \mathbb{Z} \;\Leftrightarrow\; x = \lfloor x \rfloor \;\Leftrightarrow\; x = \lceil x \rceil$
2. $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \quad \text{in} \quad x - 1 < \lfloor x \rfloor \leq x$
3. $\lceil x \rceil - 1 < x \leq \lceil x \rceil \quad \text{in} \quad x \leq \lceil x \rceil < x + 1$
4. Za poljuben $k \in \mathbb{Z}$ imamo
$$\begin{aligned} \lfloor x + k \rfloor &= \lfloor x \rfloor + k \\ \lceil x + k \rceil &= \lceil x \rceil + k \end{aligned}$$
5. $\lceil x \rceil = -\lfloor -x \rfloor \quad \text{in} \quad \lfloor x \rfloor = -\lceil -x \rceil$
6. $\lceil x \rceil = \begin{cases} \lfloor x \rfloor & x \in \mathbb{Z} \\ \lfloor x \rfloor + 1 & \text{sicer} \end{cases} \quad \text{ter} \quad \lfloor x \rfloor = \begin{cases} \lceil x \rceil & x \in \mathbb{Z} \\ \lceil x \rceil - 1 & \text{sicer.} \end{cases}$

Problem 4 *Za $m, n \in \mathbb{N}$ izračunaj, koliko je naravnih števil med 1 in n deljivih z m.*

Rešitev: To so števila $m, 2m, 3m, \ldots, k\,m$, kjer je $k\,m \leq n$ in $(k+1)\,m > n$. Tako je k iskano število. Velja

$$k \leq \frac{n}{m} \quad \text{in} \quad k+1 > \frac{n}{m},$$

od tod pa dobimo, da je $k = \lfloor \frac{n}{m} \rfloor$.

Problem 5 *Za $n \in \mathbb{N}$ in p praštevilo poišči eksponent praštevila p v razcepu števila $n!$ na prafaktorje.*

Rešitev: Ker je $n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$ iz prejšnje naloge sledi, da je število faktorjev deljivih s p $\lfloor \frac{n}{p} \rfloor$. Število faktorjev deljivih s p^2 je $\lfloor \frac{n}{p^2} \rfloor$. Število faktorjev deljivih s p^3 je $\lfloor \frac{n}{p^3} \rfloor$, itd.

Tako sklepamo, da je iskano število enako vsoti:

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^k} \right\rfloor,$$

kjer je $k \in \mathbb{N}$ število, za katerega velja $p^k \leq n < p^{k+1}$ tj. $k = \lfloor \lg_p n \rfloor$.

Naloga 30 *Poišči eksponent praštevila 5 v razcepu števila 2007! na prafaktorje.*

Deljivost celih števil

Za števila $m, n \in \mathbb{Z}$ pravimo, da m **deli** n ter pišemo $m \mid n$, če obstaja število $k \in \mathbb{Z}$ tako, da je $n = k \cdot m$.

Rečemo tudi:

- n **je deljiv z** m
- m **je delitelj** n
- n **je večkratnik** m

Če m ni delitelj n, potem pišemo $m \nmid n$.

Zgledi:

- $3 \mid 2007$, ker je $2007 = 669 \cdot 3$;
- $5 \nmid 2007$, ker je $401 \cdot 5 < 2007 < 402 \cdot 5$.

Naj bo n celo število. Potem velja:

- $1 \mid n$, ker je $n = n \cdot 1$;
- $n \mid n$, ker je $n = 1 \cdot n$;
- $n \mid 0$, ker je $0 = n \cdot 0$;
- $n \mid -n$, ker je $-n = (-1) \cdot n$.

Lastnosti relacije $\mid$

1. *refleksivnost*: $n \mid n$

2. *tranzitivnost*:
$$\begin{aligned} k \mid m \wedge m \mid n &\Rightarrow \exists p \in \mathbb{Z} : m = p \cdot k \wedge \exists q \in \mathbb{Z} : n = q \cdot m \\ &\Rightarrow \exists p, q \in \mathbb{Z} : n = (p \cdot q) \cdot k \\ &\Rightarrow \exists r \in \mathbb{Z} : n = r \cdot k \\ &\Rightarrow k \mid n \end{aligned}$$

3. *antisimetričnost na* $\mathbb{N}$:
$$\begin{aligned} n \mid m \wedge m \mid n &\Rightarrow \exists p \in \mathbb{N} : m = n \cdot p \wedge \exists q \in \mathbb{N} : n = m \cdot q \\ &\Rightarrow \exists p, q \in \mathbb{N} : n = (p \cdot q) \cdot m \\ &\Rightarrow p = q = 1 \\ &\Rightarrow m = n \end{aligned}$$

4. *delna urejenost na* $\mathbb{N}$: sledi iz lastnosti 1.-3.

5. *Če* $m \mid a$ *in* $m \mid b$, *potem* $m \mid a + b$:
$$\begin{aligned} m \mid a \wedge m \mid b &\Rightarrow \exists p \in \mathbb{Z} : a = p \cdot m \wedge \exists q \in \mathbb{Z} : b = q \cdot m \\ &\Rightarrow \exists p, q \in \mathbb{Z} : a + b = (p + q) \cdot m \\ &\Rightarrow \exists r \in \mathbb{Z} : a + b = r \cdot m \\ &\Rightarrow m \mid a + b \end{aligned}$$

6. *Če* $m \mid a$, *potem za vsak* $n \in \mathbb{Z}$ *velja* $m \mid n \cdot a$:
$$\begin{aligned} m \mid a \wedge n \in \mathbb{Z} &\Rightarrow \exists p \in \mathbb{Z} : a = p \cdot m \\ &\Rightarrow \exists p \in \mathbb{Z} : n \cdot a = (p \cdot n) \cdot m \\ &\Rightarrow \exists r \in \mathbb{Z} : n \cdot a = r \cdot m \\ &\Rightarrow m \mid n \cdot a \end{aligned}$$

Izrek o deljenju (ID)

Izrek 70 *Naj bosta $n, m \in \mathbb{Z}$ ter $m > 0$. Potem obstajata enoličnо določena $k, r \in \mathbb{Z}$ tako, da je*

$$n = k \cdot m + r \quad \text{in} \quad 0 \leq r < m. \tag{1}$$

Rečemo ter pišemo:

- k je **kvocient** oz. **količnik** števil n in m;
- r je **ostanek** pri deljenju števila n z m.
- $r = n \bmod m$.

Dokaz. Naj bo $k = \lfloor \frac{n}{m} \rfloor$ in $r = n - k \cdot m$. Potem:

$$\begin{array}{rcccl}
\frac{n}{m} - 1 & < & \lfloor \frac{n}{m} \rfloor & \leq & \frac{n}{m} \\
\frac{n}{m} - 1 & < & k & \leq & \frac{n}{m} \\
n - m & < & k \cdot m & \leq & n \\
m - n & > & -k \cdot m & \geq & -n \\
m & > & n - k \cdot m & \geq & 0 \\
m & > & r & \geq & 0.
\end{array}$$

Pokažimo še enoličnost. Recimo, da (1) velja tudi za par k_1, r_1. Tako imamo

$$n = k \cdot m + r = k_1 \cdot m + r_1.$$

Od tod $(k - k_1) \cdot m = r_1 - r$. Torej $m \mid r_1 - r$. Ker je $-m < r_1 - r < m$, sledi da je $r_1 - r = 0$, tj. $r_1 = r$. Iz tega pa tudi sledi, da je $k_1 = k$. $\square$

Zgledi:

- $17 \bmod 3 = 2$, ker je $17 = 5 \cdot 3 + 2$ in $0 \leq 2 < 3$;
- $(-17) \bmod 3 = 1$, ker je $-17 = (-6) \cdot 3 + 1$ in $0 \leq 1 < 3$.

Največji skupni delitelj. Če $m, n \in \mathbb{Z}$ nista 0, potem ga definiramo takole:

$$\gcd(m, n) = \max\{d \in \mathbb{N};\ d \mid m \text{ in } d \mid n\},$$

sicer $\gcd(0, n) = n$.

Najmanjši skupni večkratnik. Če $m, n \in \mathbb{Z}$ nista oba 0, potem ga definiramo takole:

$$\operatorname{lcm}(m, n) = \min\{v \in \mathbb{N};\ m \mid v \text{ in } n \mid v \text{ in } v > 0\},$$

sicer $\operatorname{lcm}(0, n) = 0$.

Zgled: $\gcd(20, 30) =$ $\operatorname{lcm}(20, 30) =$

$\gcd(0, 5) =$ $\operatorname{lcm}(0, 5) =$

Trditev 71 *Naj bo n skupni večkratnik števil a in b. Potem* $\operatorname{lcm}(a, b) \mid n$.

Dokaz. Po izreku o deljenju naj bo $n = k \cdot \operatorname{lcm}(a, b) + r$ in $0 \leq r < \operatorname{lcm}(a, b)$. Potem je $r = k \cdot \operatorname{lcm}(a, b) - n$ skupni večkratnik števil a in b. Zato iz $0 \leq r < \operatorname{lcm}(a, b)$ sledi, da je $r = 0$.

Evklidov algoritem

Trditev 72 *Naj bo* $a = k\,b + r$ *ter* $0 \leq r < b$. *Potem*

$$\gcd(a, b) = \gcd(b, r).$$

Dokaz. Velja naslednje

$$\begin{aligned} m \mid a \text{ in } m \mid b &\Rightarrow m \mid a - k\,b \Rightarrow m \mid r \\ m \mid b \text{ in } m \mid r &\Rightarrow m \mid k\,b + r \Rightarrow m \mid a \end{aligned}$$

Zgornja izpeljava nam zagotovi, da je poljubno število m delitelj števil a in b natanko takrat, ko je delitelj števil b in r, tj.

$$\begin{aligned} \{m \in \mathbb{N};\, m \mid a \text{ in } m \mid b\} &= \{m \in \mathbb{N};\, m \mid b \text{ in } m \mid r\} \\ \max\{m \in \mathbb{N};\, m \mid a \text{ in } m \mid b\} &= \max\{m \in \mathbb{N};\, m \mid b \text{ in } m \mid r\} \\ \gcd(a, b) &= \gcd(b, r). \end{aligned}$$

□

Zgled: Izračunajmo $\gcd(899, 812)$!

Velja

$$\begin{aligned} 899 &= 1 \cdot 812 + 87 \\ 812 &= 9 \cdot 87 + 29 \\ 87 &= 3 \cdot 29 + 0. \end{aligned}$$

Torej

$$\gcd(899, 812) = \gcd(812, 87) = \gcd(87, 29) = \gcd(29, 0) = 29.$$

Razširjeni Evklidov algoritem (REA)

REA poišče ne le $\gcd(a, b)$, ampak tudi $s, t \in \mathbb{Z}$ tako, da velja

$$a \cdot s + b \cdot t = \gcd(a, b)\,.$$

Zgled: $a = 899$, $b = 812$, $\gcd(a, b) = 29$!

Velja

$$\begin{aligned} 29 &= 1 \cdot 812 - 9 \cdot 87 \\ &= 812 - 9 \cdot (899 - 1 \cdot 812) \\ &= 812 \cdot 10 + 899 \cdot (-9) \end{aligned}$$

Torej, $s = 10$ in $t = -9$.

REA postopek

- Začetne vrednosti:

$$\begin{array}{lll} r_{-1} = a & s_{-1} = 1 & t_{-1} = 0 \\ r_0 = b & s_0 = 0 & t_0 = 1 \end{array}$$

- Iteracija: za $i = 1, 2, \ldots, n+1$ izračunaj

$$\begin{aligned} k_i &= \lfloor \tfrac{r_{i-2}}{r_{i-1}} \rfloor \\ r_i &= r_{i-2} - k_i \cdot r_{i-1} \\ s_i &= s_{i-2} - k_i \cdot s_{i-1} \\ t_i &= t_{i-2} - k_i \cdot t_{i-1}, \end{aligned}$$

  kjer je $n+1$ najmanjši indeks, za katerega je $r_{n+1} = 0$.

Velja. $r_n = \gcd(a, b)$.

Prikaz postopka s tabelo:

	a	1	0
k_1	b	0	1
k_2	r_1	s_1	t_1
k_3	r_2	s_2	t_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
k_{n+1}	$r_n \neq 0$	s_n	t_n
	$r_{n+1} = 0$	s_{n+1}	t_{n+1}

Trditev 73 *Velja:*

- $a \cdot s_i + b \cdot t_i = r_i \ za \ i = -1, 0, \ldots n+1;$
- $r_n | r_i \ za \ i = n, n-1, \ldots, 0, -1;$
- $\gcd(a, b) = r_n.$

Dokaz. Prvo trditev pokažimo z indukcijo po i:

$$\begin{aligned}
i = -1: \quad a \cdot 1 + b \cdot 0 &= a \\
i = 0: \quad a \cdot 0 + b \cdot 1 &= b \\
i > 0: \quad a \cdot s_i + b \cdot t_i &= a\,(s_{i-2} - k_i s_{i-1}) + b\,(t_{i-2} - k_i \cdot t_{i-1}) \\
&= (a\,s_{i-2} + b\,t_{i-2}) - k_i\,(a\,s_{i-1} + b\,t_{i-1}) \\
&= r_{i-2} - k_i\,r_{i-1} \\
&= r_i\,.
\end{aligned}$$

Drugo trditev pokažemo z indukcijo po i nazaj:

$$\begin{aligned}
i = n: \quad & r_n \mid r_n \\
i = n-1: \quad & 0 = r_{n+1} = r_{n-1} - k_{n+1} \cdot r_n \text{ od tod } r_{n-1} = k_{n+1} \cdot r_n\,. \\
& \text{Torej } r_n \mid r_{n-1} \\
i \leq n-2: \quad & r_{i+2} = r_i - k_{i+2} \cdot r_{i+1} \text{ oziroma } r_i = k_{i+2} \cdot r_{i+1} + r_{i+2}. \\
& \text{Ker } r_n \mid r_{i+1} \text{ in } r_n \mid r_{i+2}, \text{ dobimo } r_n \mid r_i.
\end{aligned}$$

Pokažimo zadnjo trditev. Po drugi trditvi, $r_n \mid r_{-1} = a$ in $r_n \mid r_0 = b$, kar sledi, da je r_n skupni delitelj a in b. Če je d skupni delitelj a, b potem $d \mid a$ in $d \mid b$ in od tod $d \mid a \cdot s_n + b \cdot t_n = r_n$. Torej, $r_n = \gcd(a, b)$. □

Prikaz postopka s tabelo:

	899	1	0
1	812	0	1
9	87	1	−1
3	29	−9	10
	0	28	−31

Tuji števili

Če je $\gcd(a,b) = 1$ za števili $a, b \in \mathbb{N}$, potem rečemo, da sta **tuji** ter pišemo $a \perp b$.

Zgled: $3 \perp 8,\ 12 \perp 35,\ 6 \not\perp 15\,.$

Trditev 74 *Za števila* $a, b, c \in \mathbb{N}$ *velja*

$$a \mid b\,c \quad \wedge \quad a \perp b \quad \Rightarrow \quad a \mid c.$$

Dokaz. Ker $a \mid b\,c$, obstaja $k \in \mathbb{Z}$ tako, da je $b\,c = k\,a$. Po (REA) iz $\gcd(a,b) = 1$ sledi

$$\exists s, t \in \mathbb{Z} : a\,s + b\,t = 1.$$

Zmnožimo s c zadnjo enačbo:

$$a\,s\,c + b\,t\,c = c,$$

zdaj vstavimo $b\,c = k\,a$ ter izpostavimo a

$$a\,(s\,c + t\,k) = c$$

in od tod sklepamo, da $a \mid c$. □

Trditev 75 *Za števili* $a, m \in \mathbb{N}$ *velja*

$$m \perp a \quad \Leftrightarrow \quad m \perp (a \bmod m).$$

Dokaz. Po (ID) naj bo $a = k\,m + r$ tj. $r = a \bmod m$. Potem iz (EA) sledi, da je $\gcd(a,r) = \gcd(a,m) = 1$. Torej je $m \perp r$ natanko takrat, ko je $m \perp (a \bmod m)$. □

Zveza med gcd in lcm

Izrek 76 *Za poljubni naravni števili a in b velja*

$$\gcd(a,b)\cdot\operatorname{lcm}(a,b) = a\cdot b\,.$$

Dokaz. Naj bo $d=\gcd(a,b)$ ter $a=a_1\,d$ in $b=b_1\,d$ za neka $a_1,b_1\in\mathbb{N}$. Potem velja $a_1\perp b_1$. Iz zveze

$$\frac{a\,b}{d} = a_1\,b_1\,d = a_1\,b = b_1\,a$$

sledi, da je $\frac{a\,b}{d}$ skupni večkratnik števil a in b.

Zdaj naj bo $v=\operatorname{lcm}(a,b)$ ter $v=a\,p$ in $v=b\,q$ za neka $p,q\in\mathbb{N}$. Potem

$$v \;=\; p\,a_1\,d \;=\; q\,b_1\,d \quad\Rightarrow\quad p\,a_1 \;=\; q\,b_1 \quad\Rightarrow\quad b_1 \mid p\,a_1.$$

Iz $a_1\perp b_1$ sledi, da $b_1\mid p$, tj. $p=k\,b_1$ za nek $k\in\mathbb{N}$. Torej

$$v \;=\; k\,a\,b_1 \;=\; k\,a_1\,b_1\,d \;\Rightarrow\; a_1\,b_1\,d \mid v$$

Ker pa je $a_1\,b_1\,d$ večkratnik od a in b, sklepamo, da je $v=a_1\,b_1\,d$, tj. $\frac{a\,b}{d}=v$. To pa je iskana zveza. □

Zgled: Preveri zgornji izrek za $a=12$ ter $b=15$.

Praštevila

Naravno število $n \geq 2$ je **praštevilo**, če ima natanko dva delitelja, 1 in n. Sicer je n **sestavljeno število**.

Zgled: Praštevila do 100 so 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Par praštevil oblike $(p, p+2)$ imenujemo **praštevilska dvojčka**.

Naloga 31 *Koliko je parov praštevilskih dvojčkov med* 1 *in* 100*?*

Trditev 77 *Naj bosta a, b naravni števili. Potem velja:*

1. *Če je p praštevilo, potem $p \perp a$ ali $p \mid a$;*
2. *Če je p praštevilo ter $p \mid a \cdot b$, potem $p \mid a$ ali $p \mid b$;*
3. *Za $a \geq 2$ obstaja praštevilo p tako, da $p \mid a$.*

Dokaz.

Izrek 78 (Evklid) *Praštevil je neskončno.*

Dokaz. Predpostavimo obratno, naj bodo $p_1, p_2, p_3 \ldots, p_{k-1}, p_k$ vsa praštevila. Obravnavajmo število

$$P = p_1\, p_2\, p_3 \cdots p_{k-1}\, p_k + 1$$

Velja $P \geq 2$ ter $P \bmod p_i = 1$ za $i = 1, 2, \ldots, k$. To pa je v protislovju s prejšnjo trditvijo.

Hipteza 1 (Goldenberg) *Praštevilskih dvojčkov je neskončno mnogo.*

Kongruenca po modulu m

Naj bosta $a, b \in \mathbb{Z}$ ter $m \in \mathbb{N}$. Če $m \mid a - b$ potem rečemo, da sta a in b **kongruentna po modulu** m ter pišemo $a \equiv b \pmod{m}$.

Zgledi:

- $17 \equiv 26 \pmod{3}$
- $25 \not\equiv 18 \pmod{3}$
- $a \equiv b \pmod{2} \quad \Leftrightarrow \quad a$ in b sta enake parnosti.

Velja

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad a \bmod m = b \bmod m\,,$$

od tod pa sledi, da je $\equiv \pmod{n}$ ekvivalenčna relacija na $\mathbb{Z}$ ter je število razredov m – za vsak ostanek en razred.

Zgled:

Lastnosti kongruence:

1. Če $a \equiv b \pmod{m}$ ter $c \in \mathbb{Z}$, potem

$$\begin{aligned} a + c &\equiv b + c \pmod{m} \\ a - c &\equiv b - c \pmod{m} \\ a \cdot c &\equiv b \cdot c \pmod{m} \end{aligned}$$

2. Če $a \equiv b \pmod{m}$ ter $c \equiv d \pmod{m}$, potem

$$\begin{aligned} a + c &\equiv b + d \pmod{m} \\ a - c &\equiv b - d \pmod{m} \\ a \cdot c &\equiv b \cdot d \pmod{m} \end{aligned}$$

3. Če $a \equiv b \pmod{m}$ ter $n \in \mathbb{N}$, potem $a^n \equiv b^n \pmod{m}$.
4. Če $a \cdot c \equiv b \cdot c \pmod{m}$ ter $c \perp m$, potem $a \equiv b \pmod{m}$.

Naloga 32 *Izračunaj* $3^{2007} \bmod 13$.

Naloga 33 *Naj bosta* p *in* q *različni praštevili tako, da* $a \equiv b \pmod{p}$ *in* $a \equiv b \pmod{q}$. *Pokaži, da* $a \equiv b \pmod{p\,q}$.

Eulerjeva funkcija $\varphi(n)$

Za $n \in \mathbb{N}$ je **Eulerjeva funkcija** $\varphi(n)$ število naravnih števil med 1 in n, ki so tuja n, tj.

$$\varphi(n) = |\{k \in \mathbb{N};\, 1 \leq k \leq n \,\wedge\, k \perp n\}|.$$

Zgledi:

$$\begin{aligned} &\varphi(4) = 2 && 1, 2, 3, 4 \\ &\varphi(5) = 4 && 1, 2, 3, 4, 5 \\ &\varphi(8) = 4 && 1, 2, 3, 4, 5, 6, 7, 8 \end{aligned}$$

Trditev 79 *Za vsako praštevilo p velja $\varphi(p) = p - 1$.*

Dokaz. Trditev velja, ker je vsako izmed števil $1, 2, \ldots, p-1$ tuje s p.

Trditev 80 *Za praštevilo p velja $\varphi(p^n) = p^n - p^{n-1}$.*

Dokaz. Če poljubno število ni tuje s p, potem je to število deljivo s p. Torej, p, $2\,p$, $3\,p, \ldots, p^{n-1}\,p^n$ so natanko števila na intervalu $[1, p^n]$, ki niso tuja s p. Takih števil je p^{n-1}. Ostalih $p^n - p^{n-1}$ pa je tujih s p.

Izrek 81 *Za poljubni tuji števili $a, b \in \mathbb{N}$ velja $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$!*

Dokaz. Zapišimo števila od 1 do ab v tabeli:

$$\begin{array}{rrrcr} 1 & 2 & 3 & \cdots & a \\ a+1 & a+2 & a+3 & \cdots & 2a \\ 2a+1 & 2a+2 & 2a+3 & \cdots & 3a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (b-1)a+1 & (b-1)a+2 & (b-1)a+3 & \cdots & ba \end{array}$$

Števila, ki so tuja ab, morajo biti tuja a in tudi b. Oglejmo si po stolpcih, koliko je tujih z a in koliko z b.

Števila v k-tem stolpcu so oblike $i \cdot a + k$, kjer je $i = 0, \ldots, b-1$. Torej imajo vsa ta števila ostanek k pri deljenju z a. Zato sklepamo, da so bodisi vsa števila v nekem stolpcu tuja a bodisi nobeno ni tuje a. Stolpcev, ki vsebujejo števila, ki so tuja a, je $\varphi(a)$.....

Naloga 34 *Preveri zgornji izrek za $\varphi(15) = \varphi(3) \cdot \varphi(5)$.*

Posledica 82 *Naj bo* $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ *praštevilski razcep števila* n*, kjer so* $p_1, p_2, \ldots, p_r$ *različna praštevila. Potem:*

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Dokaz. Iz prejšnjega izreka sledi:

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{k_1})\, \varphi(p_2^{k_2}) \cdots \varphi(p_r^{k_r}) \\
&= (p_1^{k_1} - p_1^{k_1-1})\, (p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) \\
&= p_1^{k_1} (1 - \tfrac{1}{p_1})\; p_2^{k_2} (1 - \tfrac{1}{p_2}) \;\cdots\; p_r^{k_r} (1 - \tfrac{1}{p_r}) \\
&= n\, (1 - \tfrac{1}{p_1})\, (1 - \tfrac{1}{p_2}) \cdots (1 - \tfrac{1}{p_r}).
\end{aligned}$$

□

Zgled:

$$\begin{aligned}
\varphi(720) &= \varphi(9 \cdot 8 \cdot 10) \\
&= \varphi(2^4)\varphi(3^2)\varphi(5) \\
&= (2^4 - 2^3) \cdot (3^2 - 3) \cdot (5 - 1) \\
&= 8 \cdot 6 \cdot 4 \\
&= 192
\end{aligned}$$

Izrek 83 *Za vsako naravno število* n *velja:*

$$\sum_{d \in D(n)} \varphi(d) = n\,.$$

Dokaz. Obravnavajmo množico

$$A = \left\{ \frac{k}{n};\, 0 \leq k < n \right\}$$

Očitno je $|A| = n$. Zdaj okrajšamo vse ulomke iz A. Imenovalci dobljenih ulomkov so delitelji n. Števci ulomkov z imenovalcem d so števila tuja z d, takih ulomkov pa je $\varphi(d)$. Vseh ulomkov je torej

$$|A| = \left\{ \frac{k}{n} \,;\, 0 \leq k < n \right\} = \sum_{d \in D(n)} \varphi(d).$$

□

Zgled: Naj bo $n = 12$. Potem

$$\begin{aligned} A &= \{\tfrac{0}{12}, \tfrac{1}{12}, \tfrac{2}{12}, \tfrac{3}{12}, \tfrac{4}{12}, \tfrac{5}{12}, \tfrac{6}{12}, \tfrac{7}{12}, \tfrac{8}{12}, \tfrac{9}{12}, \tfrac{10}{12}, \tfrac{11}{12}\} \\ &= \{\tfrac{0}{1}, \tfrac{1}{12}, \tfrac{1}{6}, \tfrac{1}{4}, \tfrac{1}{3}, \tfrac{5}{12}, \tfrac{1}{2}, \tfrac{7}{12}, \tfrac{2}{3}, \tfrac{3}{4}, \tfrac{5}{6}, \tfrac{11}{12}\} \\ &= \{\tfrac{0}{1}, \tfrac{1}{2}, \tfrac{1}{3}, \tfrac{2}{3}, \tfrac{1}{4}, \tfrac{3}{4}, \tfrac{1}{6}, \tfrac{5}{6}, \tfrac{1}{12}, \tfrac{5}{12}, \tfrac{7}{12}, \tfrac{11}{12}\}. \end{aligned}$$

Sistemi s tajnim ključem

K je tajni ključ, ki ga poznata le pošiljatelj in prejemnik.

Imamo dva postopka, **kodiranje** $\mathcal{E}$ in **dekodiranje** $\mathcal{D}$, za katera velja:

- $\mathcal{E}(M, K) = C$;
- $\mathcal{D}(C, K) = M$;

kjer je M neko sporočilo in C ustrezni **kriptogram**.

Opomba. Pomanjkljivost je, da morata tajni ključ K poznati oba, tako pošiljatelj kot prejemnik!

Sistemi z javnim ključem

Pri sistemih z javnim ključem ima vsaka oseba X dva ključa:

- J_X je **javni ključ**, ki je znan vsem;
- T_X je **tajni ključ**, ki je znan samo lastniku.

Problem avtentikacije oz. digitalni podpis

Recimo, da oseba A želi poslati osebi B sporočilo M. Vprašanje je: kako bo B vedel, da je sporočilo zares poslal A! Uporabimo naslednji postopek:

1. Oseba A kodira sporočilo M s svojim tajnim ključem T_A ter tako dobi sporočilo $T_A(M)$. Potem kodira $T_A(M)$ z javnim ključem J_B ter dobi sporočilo $J_B(T_A(M))$.
2. Oseba B dekodira sporočilo $J_B(T_A(M))$ s tajnim ključem T_B ter dobi sporočilo $T_A(M)$. Potem dekodira $T_A(M)$ z javnim ključem J_A ter dobi začetno sporočilo M.

Kriptografska shema RSA

Ključa J_X in T_X dobimo takole:

1. izberimo različni veliki praštevili p in q;
2. izračunajmo: $n = p \cdot q$ in $m = (p-1) \cdot (q-1)$;
3. izberimo $1 < e < m$ tako, da je $e \perp m$;
4. z REA izračunajmo $1 < d < m$ tako, da je $d \cdot e \equiv 1 \pmod{m}$;
5. ključa sta $J_X = (n, e)$ in $T_X = d$.

Kodiramo in dekodiramo takole:

- **Kodiranje:** $C := M^e \pmod{n}$
- **Dekodiranje:** $M := C^d \pmod{n}$.

Da sta postopka kodiranja in dekodiranja usklajena, sledi iz naslednjega izreka:

Izrek 84 *Velja* $M^{de} \equiv M \pmod{n}$.

Dokaz. Za neko število k velja

$$de = km + 1 = k(p-1)(q-1) + 1.$$

Trdimo, da $M^{de} \equiv M \pmod{p}$. Če $p \mid M$, potem trditev očitno velja. Če pa $p \perp M$, potem $M \equiv 1 \pmod{p}$ in po Malem Fermatovem izreku sklepamo, da je $M^{p-1} \equiv 1 \pmod{p}$. Če potenciramo, dobimo $M^{k(p-1)(q-1)} \equiv 1 \pmod{p}$. Zdaj pa takoj sledi trditev.

Podobno dokažemo, da $M^{de} \equiv M \pmod{q}$.

Iz $p \mid M^{de} - M$ in $q \mid M^{de} - M$ sledi, da $pq \mid M^{de} - M$, kar je enako trditvi $M^{de} \equiv M \pmod{n}$. □