Primož Potočnik

Zapiski predavanj iz Algebre in Diskretne Matematike

Ljubljana, marec 2011

Naslov: Zapiski predavanj iz Algebre in Diskretne Matematike
Avtor: Primož Potočnik
1. izdaja
Dostopno na spletnem naslovu `www.fmf.uni-lj.si/~potocnik`

CIP – Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

511.2(0.034.2)
519.172(0.034.2)

POTOČNIK, Primož, 1971 –

Zapiski predavanj iz Algebre in Diskretne matematike [Elektronski vir]

Primož Potočnik. - 1. izd. – El. knjiga. – Ljubljana : samozal., 2011

Način dostopa (URL):
http://www.fmf.uni-lj.si/∼potocnik/Ucbeniki/ADM-Zapiski.pdf

ISBN 978-961-93056-2-1

255520000

Izdano v samozaložbi marca 2011. Avtor si pridržuje vse pravice.

Kazalo

Matematična logika

Za strogo obravnavo matematičnih teorij naravni jeziki niso najprimernejši. Zato smo matematiki zgradili svoje jezike, ki jim pravimo *formalni matematični jeziki*. S formalnimi matematičnimi jeziki se ukvarja veja matematike, ki ji pravimo *matematična logika*. Matematična logika določa poleg slovnice formalnega jezika tudi *pravila sklepanja*, ki nam omogočajo iz že dokazanih trditev izpeljevati nove trditve.

1 Izjave

V logiki razumemo *izjavo* kot tisto kar neki (smiselen) povedni stavek trdi o objektih dane teorije. Poudariti velja, da lahko sicer različni stavki trdijo isto. Izjava je torej tisto, kar je vsem povednim stavkom z enakim "pomenom" skupnega. Vsaka izjava je bodisi pravilna bodisi nepravilna. Pravimo tudi, da vsaka izjava zavzame eno od dveh *logičnih vrednosti*: 1 ali 0. Pri tem simbol 1 predstavlja logično vrednost "pravilno", simbol 0 pa logično vrednost "nepravilno".

Navedimo nekaj stavkov, ki so izjave:

- *Število* 5 *je večje od števila 3.* (pravilna izjava)
- *Vsaka zvezna funkcija je odvedljiva.* (nepravilna izjava)
- *Če je neko število večje ali enako drugemu, drugo pa večje ali enako prvemu, potem sta ti dve števili enaki.* (pravilna izjava)

In še nekaj stavkov, ki niso izjave:

- *Koliko je* 3 *plus* 5*?* (ni povedni stavek)
- *Seštej* 3 *in* 5*!* (ni povedni stavek)
- *Zelena funkcija je šla na dopust.* (nesmiselen stavek)

1.1 Logične operacije

Iz izjav lahko tvorimo nove izjave s pomočjo *logičnih operacij* ali, kot jim tudi pravimo, *logičnih veznikov* oz. *logičnih povezav*. Na tak način dobimo *sestavljene izjave*.

Naj bosta, na primer, A in B izjavi:

$$A \equiv \text{ “Sonce sije.”} \qquad B \equiv \text{ “Pada dež.”}$$

Vsaka od teh dveh izjav je sama po sebi bodisi pravilna bodisi nepravilna; odvisno od dejanskih vremenskih razmer v trenutku, ko sta izrečeni. Iz njiju lahko sestavimo več sestavljenih izjav:

- $A \wedge B \equiv$ “Sonce sije in pada dež.”
- $A \vee B \equiv$ “Sonce sije ali pada dež.”
- $\neg B \equiv$ “Ne pada dež.”
- $A \Rightarrow \neg B \equiv$ “Če sonce sije, potem ne pada dež.”

Prva izjava je pravilna, če in samo če sta pravilni A in B hkrati. Druga je pravilna, če in samo če je vsaj ena od izjav A in B pravilna. Tretja je pravilna, če in samo če je B nepravilna. Za pravilnost četrte izjave se v matematiki domenimo, da je pravilna v vsakem primeru, razen, če je A pravilna, $\neg B$ pa nepravilna, torej, če sonce sije, hkrati pa ni res, da ne bi padal dež.

Za sestavljene izjave je značilno, da je njihova logična vrednost odvisna le od logičnih vrednosti izjav, ki jih sestavljajo. Na kakšen način je logična vrednost sestavljene izjave odvisna od logičnih vrednosti sestavljenih izjav, lahko povemo s pomočjo *pravilnostne tabele*.

V pravilnostni tabeli na levi strani v vrsticah navedemo vse možne nabore logičnih vrednosti sestavljajočih izjav (če je izjav n, je takšnih naborov 2^n), na desni strani pa v vsaki vrstici navedemo pripadajočo logično vrednost sestavljene izjave. Nabor logičnih vrednosti sestavljajočih izjav imenujemo tudi *določilo* sestavljene izjave.

Opišimo nekaj najpomembnejših logičnih operacij in pri vsaki navedimo njeno pravilnostno tabelo.

Negacija (oznaka: $\neg$). *Negacija* je enomestna operacija, ki dano izjavo spremeni v njej nasprotno izjavo. Izjava $\neg A$ je torej pravilna, če in samo če je izjava A nepravilna. Pravilnostna tabela za *negacijo*:

A	$\neg A$
0	1
1	0

Konjunkcija (oznaka: $\wedge$). *Konjunkcija* izjav A in B je pravilna izjava, če in samo če sta pravilni obe izjavi A in B. Označimo jo z $A \wedge B$ in preberemo "A in B". Pravilnostna tabela za *konjunkcijo*:

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

Disjunkcija (oznaka: $\vee$). *Disjunkcija* izjav A in B je pravilna izjava, če in samo če je pravilna vsaj ena od izjav A in B (lahko sta pravilni tudi obe). Označimo jo z $A \vee B$ in preberemo "A ali B". Pravilnostna tabela za *disjunkcijo*:

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

Ekvivalenca (oznaka: $\Leftrightarrow$). *Ekvivalenca* dveh izjav A in B je izjava, ki je pravilna natanko tedaj, ko imata izjavi A in B enaki logični vrednosti. Pravilnostna tabela za *ekvivalenco*:

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

Implikacija (oznaka: $\Rightarrow$). *Implikacija* je zelo pomembna logična operacija, na kateri temelji logično sklepanje. Če sta A in B poljubni izjavi, potem je izjava $A \Rightarrow B$ pravilna v vseh primerih, razen v primeru, ko je A pravilna, B pa nepravilna. Pravilnostna tabela za *implikacijo* je torej:

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

Izjavo $A \Rightarrow B$ preberemo tudi "Iz A sledi B," ali pa "Če A, potem B."

Poleg zgornjih logičnih operacij, ki jih najpogosteje uporabljamo v matematiki, so pomembne še tri, prva zaradi uporabe v računalništvu, drugi dve pa zaradi pomena v logiki.

Ekskluzivna disjunkcija (oznaka: $\veebar$). *Ekskluzivna disjunkcija* dveh izjav A in B je pravilna izjava natanko tedaj, ko imata A in B različni logični vrednosti, torej tedaj, ko je pravilna natanko ena od izjav A in B. V slovenskem jeziku bi ekskluzivno disjunkcijo $A \veebar B$ prebrali "bodisi A bodisi B." Ta logična operacija je pogosto uporabljana v računalništvu, kjer jo označujejo tudi z "Xor". Pravilnostna tabela za *ekskluzivno disjunkcijo*:

A	B	$A \veebar B$
0	0	0
0	1	1
1	0	1
1	1	0

Koliko različnih *dvomestnih* logičnih operacij pa sploh obstaja? Dve logični operaciji sta *različni* natanko tedaj, ko imata različna stolpca logičnih vrednosti. Stolpec vsebuje 4 mesta in na vsakem mestu lahko izbiramo med dvema logičnima vrednostma. Skupaj imamo torej $2^4 = 16$ dvomestnih logičnih operacij. Pravilnostne tabele, oznake in imena dvomestnih logičnih operacij smo združili v naslednji tabeli.

p	0	0	1	1		
q	0	1	0	1		
	0	0	0	0	$p\underline{0}q$	protislovje
	0	0	0	1	$p \wedge q$	konjunkcija
	0	0	1	0	$\neg(p \Rightarrow q)$	negacija implikacije
	0	0	1	1	p	projekcija na prvi faktor
	0	1	0	0	$\neg(q \Rightarrow p)$	negacija obrnjene implikacije
	0	1	0	1	q	projekcija na drugi faktor
	0	1	1	0	$p \veebar q$	ekskluzivna disjunkcija
	0	1	1	1	$p \vee q$	disjunkcija
	1	0	0	0	$p \downarrow q$	Lukasiewicz–Pierceova operacija
	1	0	0	1	$p \Leftrightarrow q$	ekvivalenca
	1	0	1	0	$\neg q$	negacija projekcije na drugi faktor
	1	0	1	1	$q \Rightarrow p$	implikacija
	1	1	0	0	$\neg p$	negacija projekcije na prvi faktor
	1	1	0	1	$p \Rightarrow q$	implikacija
	1	1	1	0	$p \uparrow q$	Shefferjeva operacija
	1	1	1	1	$p\underline{1}q$	tavtologija

1.2 Pravilnostne tabele sestavljenih izjav

Pravilnostne tabele smo v prejšnjem razdelku uporabili za definicijo nekaterih logičnih operacij. Tako definirane logične operacije lahko, skupaj z oklepaji, uporabimo za gradnjo novih sestavljenih izjav. Na primer, iz izjav A, B in C lahko tvorimo sestavljeno izjavo $(A \vee B) \Rightarrow C$.

Pravilnostno tabelo za tako sestavljeno izjavo dobimo s postopnim računanjem logičnih vrednosti sestavljajočih izjav (ob upoštevanju vrstnega reda, ki ga določajo oklepaji).

A	B	C	$(A \vee B)$	$\Rightarrow$	C
1	1	1	1	1	1
1	1	0	1	0	0
1	0	1	1	1	1
1	0	0	1	0	0
0	1	1	1	1	1
0	1	0	1	0	0
0	0	1	0	1	1
0	0	0	0	1	0

Naboru logičnih vrednosti sestavljajočih izjav A, B in C (recimo $A = 1$, $B = 0, C = 1$), rečemo tudi *določilo* sestavljene izjave. Vsaka vrstica zgornje tabele tako predstavlja eno določilo.

Da zmanjšamo število potrebnih oklepajev, podobno kot pri običajnih računskih operacijah ($+$, $-$, $\times$, $:$) uvedemo pravila prednosti logičnih operacij. Najtesneje naj izjave veže operacija $\neg$, nato pa po vrsti: $\wedge$, $\uparrow$, $\downarrow$, $\vee$, $\veebar$, $\Rightarrow$, $\Leftrightarrow$.

Za konec se še dogovorimo, da bomo sestavljene izjave označevali z velikimi tiskanimi črkami: A, B, $C, \ldots$, izjave, ki niso sestavljene, pa z malimi tiskanimi črkami $p, q, r, \ldots$. Če je neka izjava A sestavljena iz nesestavljenih (*atomarnih*) izjav $p, q, r, \ldots$, bomo to poudarili z zapisom $A = A(p, q, r, \ldots)$.

1.3 Tavtologije, protislovja in enakovrednost izjav

Sestavljeni izjavi, ki je pravilna pri vsakem naboru logičnih vrednosti sestavljajočih izjav, pravimo *tavtologija*. Kadar je neka izjava A tavtologija, zapišemo

$$\vDash A.$$

Dve (sestavljeni) izjavi A in B sta enakovredni natanko tedaj, ko je izjava $A \Leftrightarrow B$ tavtologija:

$$(A \sim B) \text{ natanko tedaj, ko } \vDash A \Leftrightarrow B.$$

Ker je izjava $A \Leftrightarrow B$ pravilna natanko tedaj, ko imata A in B isto logično vrednost, je zgornja zahteva ekvivalentna zahtevi, da imata A in B pri vsakem naboru logičnih vrednosti sestavljajočih atomarnih izjav (določilu) isto logično vrednost.

Ali sta dve izjavi enakovredni ali ne, torej lahko ugotovimo iz pravilnostnih tabel obeh izjav.

ZGLED. *Ali sta izjavi $p \Rightarrow q$ in $\neg q \Rightarrow \neg p$ enakovredni?*

Sestavimo njuni pravilnostni tebeli:

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

Vidimo, da sta stolpca z logičnimi vrednostmi pri obeh izjavah enaka, zato lahko zatrdimo, da sta izjavi enakovredni. ∎

Podobno definiramo logično posledico dane izjave. Namreč, izjava B je *logična posledica* izjave A, če in samo če je izjava $A \Rightarrow B$ tavtologija:

$$(A \to B) \text{ natanko tedaj, ko } \vDash A \Rightarrow B.$$

Zapišimo nekaj pomembnih parov enakovrednih izjav:

$\neg(\neg p)$	$\sim$	p	.....	pravilo dvakratne negacije
$p \wedge p$	$\sim$	p	.....	idempotentnost konjunkcije
$p \vee p$	$\sim$	p	.....	idempotentnost disjunkcije
$p \wedge q$	$\sim$	$q \wedge p$	.....	komutativnost konjunkcije
$p \vee q$	$\sim$	$q \vee p$	.....	komutativnost disjunkcije
$(p \wedge q) \wedge r$	$\sim$	$p \wedge (q \wedge r)$	.....	asociativnost konjunkcije
$(p \vee q) \vee r$	$\sim$	$p \vee (q \vee r)$	.....	asociativnost disjunkcije
$(p \vee q) \wedge r$	$\sim$	$(p \wedge r) \vee (q \wedge r)$	.....	distributivnost
$(p \wedge q) \vee r$	$\sim$	$(p \vee r) \wedge (q \vee r)$	.....	distributivnost
$\neg(p \wedge q)$	$\sim$	$\neg p \vee \neg q$	.....	1. de Morganov zakon
$\neg(p \vee q)$	$\sim$	$\neg p \wedge \neg q$	.....	2. de Morganov zakon
$p \Rightarrow q$	$\sim$	$\neg p \vee q$	.....	definicija implikacije
$p \Rightarrow q$	$\sim$	$\neg q \Rightarrow \neg p$	.....	pravilo kontrapozicije
$p \Leftrightarrow q$	$\sim$	$q \Leftrightarrow p$	.....	komutativnost ekvivalence
$p \Leftrightarrow q$	$\sim$	$\neg p \Leftrightarrow \neg q$	.....	neobčutljivost ekvivalence na negacijo
$\neg(p \Leftrightarrow q)$	$\sim$	$p \Leftrightarrow \neg q$	.....	pravilo negacije ekvivalence
$p \vee (p \wedge q)$	$\sim$	p	.....	1. absorbcijsko pravilo
$p \wedge (p \vee q)$	$\sim$	p	.....	2. absorbcijsko pravilo
$p \wedge \underline{0}$	$\sim$	$\underline{0}$	.....	konjunkcija s protislovjem
$p \wedge \underline{1}$	$\sim$	p	.....	konjunkcija s tavtologijo
$p \vee \underline{0}$	$\sim$	p	.....	disjunkcija s protislovjem
$p \vee \underline{1}$	$\sim$	$\underline{1}$	.....	disjunkcija s tavtologijo
$p \vee \neg p$	$\sim$	$\underline{1}$	.....	zakon izključene tretje možnosti
$p \wedge \neg p$	$\sim$	$\underline{0}$	.....	zakon protislovja

S pomočjo osnovnih logičnih enakovrednosti lahko dokazujemo tudi nekoliko zapletenejše enakovrednosti. Spodnji zgled pokaže, kako lahko relativno zapleteno izjavo poenostavimo v preprostejšo, njej enakovredno izjavo.

Zgled. *Dokaži enakovrednost izjave* $(A \Rightarrow B) \Rightarrow (B \Rightarrow C)$ *z izjavo* $B \Rightarrow C$.

Z zaporedno uporabo enakovrednosti iz zgornje tabele dobimo verigo naslednjih enakovrednosti:

$$
\begin{array}{rcl}
(A \Rightarrow B) \Rightarrow (B \Rightarrow C) & \sim & \\
(\neg A \vee B) \Rightarrow (\neg B \vee C) & \sim & \text{definicija implikacije} \\
\neg(\neg A \vee B) \vee (\neg B \vee C) & \sim & \text{definicija implikacije} \\
(A \wedge \neg B) \vee (\neg B \vee C) & \sim & \text{2. de Morganov zakon} \\
((A \wedge \neg B) \vee \neg B) \vee C & \sim & \text{asociativnost disjunkcije} \\
\neg B \vee C & \sim & \text{1. asimilacijsko pravilo} \\
B \Rightarrow C & \sim & \text{definicija implikacije.}
\end{array}
$$

■

1.4 Izbrane oblike izjav

V prejšnjem razdelku smo videli, kako dani izjavi priredimo pravilnostno tabelo. Kaj pa če pravilnostno tabelo imamo, pa bi radi poiskali primerno sestavljeno izjavo? Na primer, radi bi našli izjavo A, sestavljeno iz atomarnih izjav p_1, p_2 in p_3, katere logična vrednost je odvisna od logičnih vrednosti izjav p_1, p_2 in p_3 takole:

p_1	p_2	p_3	A
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1

V nadaljevanju bomo opisali dva postopka za reševanje tovrstnih nalog.

Izbrana disjunktivna oblika izjave

Vzemimo poljubno določilo P (nabor logičnih vrednosti izjav p_1, p_2 in p_3) in sestavimo izjavo

$$q_1 \wedge q_2 \wedge q_3$$

po pravilu:

$$q_i := \begin{cases} p_i & ; \quad \text{če je logična vrednost izjave } p_i \text{ pri določilu } P \text{ enaka 1} \\ \neg p_i & ; \quad \text{če je logična vrednost izjave } p_i \text{ pri določilu } P \text{ enaka 0} \end{cases}$$

Tako dobljena izjava se imenuje *osnovna konjunkcija določila* P. Opazimo, da osnovna konjukcija določila P ni nič odvisna od izjave A, temveč le od določila P.

TRDITEV 1.1 *Osnovna konjunkcija določila P je pravilna pri določilu P in nepravilna pri vseh ostalih določilih.*

DOKAZ: Vzemimo poljubno od zgoraj definiranih izjav q_i in si oglejmo, kakšna je njena logična vrednost pri določilu P. Če je logična vrednost izjave p_i pri tem določilu 1, potem je $q_i = p_i$, in je zato tudi logična vrednost q_i enaka 1. Če pa je logična vrednost izjave p_i pri določilu P enaka 0, potem je $q_i = \neg p_i$, in logična vrednost izjave q_i je zopet 1. Od tod sledi, da ima vsaka od izjav q_i logično vrednost enako 1. Tedaj pa ima tudi osnovna konjukcija $q_1 \wedge q_2 \wedge q_3$ logično vrednost 1.

Sedaj pa vzemimo neko drugo določilo Q, ki se od določila P razlikuje, denimo, pri logični vrednosti izjave p_i. Če je logična vrednost izjave p_i pri določilu P enaka 1, je njena logična vrednost pri določilu Q torej enaka 0. Vendar je v tem primeru $q_i = p_i$, in logična vrednost q_i je enaka 0. Podobno, če je logična vrednost p_i pri določilu P enaka 0, potem je le-ta pri določilu Q enaka 1. Vendar $q_i = \neg p_i$, zato je logična vrednost q_i enaka 0. Od tod sledi, da je pri določilu Q logična vrednost izjave q_i – in se tem tudi osnovne konjukcije $q_1 \wedge q_2 \wedge q_3$ – enaka 0, in to ne glede na to, kakšno je določilo P. ■

Do zapisa izjave, ki je enakovredna izjavi A, pridemo po naslednjem postopku. Najprej sestavimo osnovne konjunkcije pri vseh določilih, pri katerih je izjava A pravilna:

p_1	p_2	p_3	A	osnovna konjunkcija
0	0	0	1	$\neg p_1 \wedge \neg p_2 \wedge \neg p_3$
0	0	1	0	
0	1	0	0	
0	1	1	0	
1	0	0	1	$p_1 \wedge \neg p_2 \wedge \neg p_3$
1	0	1	0	
1	1	0	1	$p_1 \wedge p_2 \wedge \neg p_3$
1	1	1	1	$p_1 \wedge p_2 \wedge p_3$

Dobljene osnovne konjunkcije povežemo z disjunkcijo v sestavljeno izjavo, ki ji rečemo *izbrana disjunktivna oblika izjave* A:

$$(\neg p_1 \wedge \neg p_2 \wedge \neg p_3) \vee (p_1 \wedge \neg p_2 \wedge \neg p_3) \vee (p_1 \wedge p_2 \wedge \neg p_3) \vee (p_1 \wedge p_2 \wedge p_3).$$

Če sestavimo pravilnostno tabelo za zgoraj navedeno izjavo, ugotovimo, da je povsem enaka pravilnostni tabeli izjave A. Izjava A in njena izbrana disjunktivna oblika sta torej enakovredni.

Zgoraj opisani postopek lahko uporabimo pri poljubnem številu osnovnih izjav $p_1, \ldots, p_n$ in poljubni sestavljeni izjavi $A = A(p_1, \ldots, p_n)$. Tudi v tem primeru bi dobili izjavo, ki je enakovredna izjavi A. Velja namreč naslednja trditev.

TRDITEV 1.2 *Izbrana disjunktivna oblika izjave A je enakovredna izjavi A.*

Iz opisanega postopka je razvidno, da lahko izbrano disjunktivno obliko poiščemo prav vsaki izjavi, z izjemo izjavi, katere logična vrednost je 0 prav pri vsakem določilu, torej pri protislovju. Pri takšni izjavi namreč ne bi imeli nobenenih osnovnih konjunkcij, ki naj bi jih v skladu s postopkom povezali med seboj z disjunkcijami. Od tod sledi naslednje.

TRDITEV 1.3 *Vsaka sestavljena izjava A, ki ni protislovje, premore izbrano disjunktivno obliko.*

Izbrana konjunktivna oblika izjave

Poleg izbrane disjunktivne oblike lahko sestavljeni izjavi poiščemo tudi tako imenovano *izbrano konjunktivno obliko*. Naj bo $A = A(p_1, p_2, \ldots, p_n)$ poljubna sestavljena izjava z znano pravilnostno tabelo. Pri poljubnem določilu P izjave A lahko tvorimo izjavo

$$q_1 \vee q_2 \vee \ldots \vee q_n,$$

kjer je

$$q_i := \begin{cases} \neg p_i & ; \quad \text{če je logična vrednost izjave } p_i \text{ pri določilu } P \text{ enaka } 1 \\ p_i & ; \quad \text{če je logična vrednost izjave } p_i \text{ pri določilu } P \text{ enaka } 0 \end{cases},$$

ki mu pravimo *osnovna disjunkcija določila P*. Podobno kot pri osnovni konjunkciji se lahko prepričamo v naslednje.

TRDITEV 1.4 *Osnovna disjunkcija določila P je nepravilna pri določilu P in pravilna pri vseh ostalih določilih.*

Če povežemo osnovne disjunkcije tistih določil, pri katerih je logična izjava A nepravilna, s konjunkcijo, dobimo izjavo, ki ji rečemo *izbrana konjunktivna oblika* izjave A. Podobno kot pri izbrani disjunktivni obliki velja, da je dobljena izjava enakovredna izjavi A, zgradimo pa jo lahko za vsako izjavo A, če le A ni tavtologija.

Trditev 1.5 *Vsaka izjava, ki ni tavtologija, premore izbrano konjunktivno obliko. Izbrana konjunktivna oblika izjave A je enakovredna izjavi A.*

Za zaključek ponazorimo opisani postopek na primeru z začetka razdelka. Za izjavo A najprej poiščemo osnovne disjunkcije pri tistih določilih, kjer je izjava nepravilna.

p_1	p_2	p_3	A	osnovna disjunkcija
0	0	0	1	
0	0	1	0	$p_1 \vee p_2 \vee \neg p_3$
0	1	0	0	$p_1 \vee \neg p_2 \vee p_3$
0	1	1	0	$p_1 \vee \neg p_2 \vee \neg p_3$
1	0	0	1	
1	0	1	0	$\neg p_1 \vee p_2 \vee \neg p_3$
1	1	0	1	
1	1	1	1	

Nato dobljene osnovne disjunkcije povežemo s konjunkcijo:

$$(p_1 \vee p_2 \vee \neg p_3) \wedge (p_1 \vee \neg p_2 \vee p_3) \wedge (p_1 \vee \neg p_2 \vee \neg p_3) \wedge (\neg p_1 \vee p_2 \vee \neg p_3).$$

Omenimo še, da lahko med izbranima oblikama (konjunktivno in disjunktivno) prehajamo tako, da zaporedoma uporabimo zakon dvojne negacije in de Morganov zakon.

1.5 Polni nabori logičnih operacij

V prejšnjem razdelku smo videli, da lahko poljubno sestavljeno izjavo dobimo iz osnovnih zgolj s pomočjo logičnih operacij $\{\vee, \wedge, \neg\}$. Zato rečemo, da je nabor logičnih operacij $\{\vee, \wedge, \neg\}$ *poln*.

Ker je $A \wedge B \sim \neg(\neg A \vee \neg B)$, je poln tudi nabor $\{\neg, \vee\}$. Nadalje, ker je $\neg A \sim A \downarrow A$, je poln tudi nabor $\{\downarrow, \vee\}$. Nazadnje, ker je $A \vee B \sim (A \downarrow B) \downarrow (A \downarrow B)$, je poln tudi nabor $\{\downarrow\}$.

Vse sestavljene izjave lahko torej izrazimo že s pomočjo logične operacije $\downarrow$ (Lukasiewicz–Pierceova operacija) in seveda oklepajev, ki jih potrebujemo za določevanje vrstnega reda operacij v sestavljeni izjavi.

2 Sklepanje in dokazovanje v izjavnem računu

Logika ima dve ključni nalogi: *določiti slovnico formalnega jezika* in *določiti pravila sklepanja*. V tem razdelku se bomo ukvarjali s slednjo nalogo. Poskusili bomo na strog matematični način pojasniti, kdaj je kakšen sklep veljaven. Pojasnili bomo tudi, kako v matematični logiki razumemo pojem *dokaza*.

2.1 Veljavni in neveljavni sklepi

DEFINICIJA 2.1 Naj bo $\mathcal{A} = \{A_1, A_2, \ldots, A_n\}$ množica nekih izjav in B izjava. Izjavi

$$(A_1 \wedge A_2 \wedge \ldots \wedge A_n) \Rightarrow B \tag{I}$$

priredimo izraz

$$A_1, A_2, \ldots, A_n \vDash B, \tag{S}$$

ali krajše

$$\mathcal{A} \vDash B. \tag{S'}$$

Izrazu (S) rečemo *sklep*, izjavam $A_1, A_2, \ldots, A_n$ *predpostavke* (ali *premise*) sklepa, izjavi B pa *zaključek* sklepa. Če je izjava (I) tavtologija, potem rečemo, da je sklep (S) *veljaven*, če pa (I) ni tavtologija, rečemo, da je sklep *neveljaven*. Če je sklep veljaven, rečemo tudi, da je *izjava B logična posledica množice izjav $\mathcal{A}$*.

ZGLED. *Ugotovimo, ali je veljaven naslednji sklep:*

Februarja bom šel smučat v Italijo, poleti pa na morje v Grčijo. Če grem februarja v Italijo, za 1. maja ne morem nikamor. Torej, za 1. maja bom doma.

Če označimo izjave:

$p \equiv$ Februarja grem v Italijo;

$q \equiv$ Poleti grem v Grčijo;

$r \equiv$ Za 1. maja bom doma;

lahko sklep napišemo takole:

$$p \wedge q,\ p \Rightarrow r \ \vDash\ r. \tag{$*$}$$

Sklep $(*)$ je veljaven, če je izjava

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

tavtologija. Če sestavimo njeno pravilnostno tabelo, ugotovimo, da je res tavtologija, torej sklep je veljaven. ∎

Zgled. *Ta človek laže ali pa je naiven. Če ne laže, potem krade. Ampak, ta človek ni naiven. Torej krade.*

Označimo izjave:

$p \equiv$ Ta človek laže.

$q \equiv$ Ta človek je naiven.

$r \equiv$ Ta človek krade.

Sklep ima tedaj naslednjo obliko:

$$p \vee q,\ \neg p \Rightarrow r,\ \neg q \models \neg r. \qquad (*)$$

Sklep $(*)$ je veljaven, če je izjava

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

tavtologija. Sestavimo pravilnostno tabelo in ugotovimo, da zgornja izjava v primeru, ko je izjava p pravilna, izjava q nepravilna in izjava r pravilna, ni pravilna. Sklep $(*)$ zato ni veljaven. (Lahko se namreč zgodi, da človek laže in ni naiven, vendar ne krade. V tem primeru so izpolnjene vse predpostavke sklepa, zaključek sklepa pa je nepravilen.) ∎

Poudarimo še, da je lahko zaključek nekega neveljavnega sklepa v kaki konkretni situaciji (pri kakih konkretnih določilih premis) kljub vsemu pravilen. Po drugi strani je lahko zaključek B logično veljavnega sklepa nepravilen pri tistih določilih, kjer je nepravilna kaka od premis A_i. Pravilnost zaključka sklepa torej ni v neposredni povezavi z veljavnostjo sklepa.

2.2 Dokaz

Veljavnost sklepa lahko vedno preverimo s pomočjo logičnih tabel. Seveda pa to ni vedno najbolj praktično niti najbolj intuitivno prepričljivo. Če želimo sogovornika prepričati v svoja stališča, ponavadi na podlagi bolj ali manj jasno izraženih predpostavk korakoma, z enostavnimi sklepi, privedemo predpostavke do izjave, ki jo zagovarjamo. Takšnemu postopku rečemo *dokaz*.

DEFINICIJA 2.2 *Dokaz* izjave B iz predpostavk $A_1, A_2, \ldots, A_n$ lahko torej definiramo kot zaporedje izjav $C_1, C_2, \ldots, C_k$, pri čemer je vsaka izjava C_i

i) tavtologija, ali

ii) ena od predpostavk $A_1, A_2, \ldots, A_n$, ali

iii) zaključek veljavnega sklepa, katerega premise so izjave, ki v zaporedju nastopijo pred izjavo C_i.

Čeprav lahko načeloma v točki iii) zgornje definicije uporabljamo katere koli logično veljavne sklepe, se je smiselno omejiti na dovolj majhen nabor še posebej preprostih sklepov. V nadaljevanju bomo navedli nekaj takšnih sklepov, ki so jih poznali že v antiki.

IZREK 2.3 *Naslednji sklepi so logično veljavni:*

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

DOKAZ: Za vsakega od zgornjih sklepov moramo preveriti, ali je ustrezna implikacija tavtologija. Tako moramo pri sklepu modus ponens preveriti, da je izjava $(A \wedge (A \Rightarrow B)) \Rightarrow B$ tavtologija, pri disjunktivnem silogizmu pa moramo preveriti, da je tavtologija izjava $(A \vee B) \wedge \neg A \Rightarrow B$. To lahko storimo s pomočjo pravilnostnih tabel, lahko pa tudi s pomočjo osnovnih logičnih enakovrednosti. Na primer, dokaz veljavnosti sklepa dis-

junktivni silogizem bi lahko potekal takole:

$$\begin{aligned}(A \vee B) \wedge \neg A \Rightarrow B &\sim \neg((A \vee B) \wedge \neg A) \vee B \\ &\sim ((\neg A \wedge \neg B) \vee A) \vee B \\ &\sim ((\neg A \vee A) \wedge (\neg B \vee A)) \vee B \\ &\sim (\underline{1} \wedge (\neg B \vee A)) \vee B \\ &\sim \neg B \vee A \vee B \\ &\sim \neg B \vee B \vee A \\ &\sim \underline{1} \vee A \sim \underline{1}\end{aligned}$$

Podobno lahko dokažemo tudi veljavnost ostalih sklepov. ■

ZGLED. *Sestavimo dokaz sklepa* $p \wedge q,\ p \Rightarrow r \vDash r$.

Predp.	:	$p \wedge q$	...	(1);
(Po)[1]	:	p	...	(2);
Predp.	:	$p \Rightarrow r$	...	(3);
(MP)[2,3]	:	r	...	(4);

V tem dokazu smo uporabili le dva preprosta sklepa: poenostavitev in modus ponens. Seveda to ni edini dokaz, ki ga lahko sestavimo, je pa najkrajši. ■

ZGLED. *Sestavimo dokaz sklepa* $p \Rightarrow q, p \vee s, q \Rightarrow r, s \Rightarrow t, \neg r \vDash t$.

Predp.	:	$q \Rightarrow r$	...	(1);
Predp.	:	$\neg r$	...	(2);
(MT)[1,2]	:	$\neg q$	...	(3);
Predp.	:	$p \Rightarrow q$	...	(4);
(MT)[3,4]	:	$\neg p$	...	(5);
Predp.	:	$p \vee s$	...	(6);
(DS)[5,6]	:	s	...	(7);
Predp.	:	$s \Rightarrow t$	...	(8);
(MP)[7,8]	:	t	...	(9);

■

3 Predikati in kvantifikatorji

Do sedaj so bili osnovni gradniki našega formalnega jezika "osnovne izjave". Zgradbo izjav smo proučevali le na ravni logičnih operacij med posameznimi osnovnimi ali sestavljenimi izjavami. Oglejmo pa si naslednji klasični zgled:

$A \equiv$ Vsi ljudje so smrtni.
$B \equiv$ Sokrat je človek.
$C \equiv$ Sokrat je smrten.

Zdi se nam, da je sklep $A, B \vDash C$ v skladu z logičnimi pravili, čeprav ga ne moremo utemeljiti z dosedaj znanimi sredstvi. Razlog tiči v tem, da veljavnost sklepa sledi iz *notranje zgradbe* izjav A, B in C. Notranjo zgradbo izjave A bi lahko opisali s stavkom

Za vsak x velja: "x je človek" $\Rightarrow$ "x je smrten".

Za opis notranje zgradbe izjave A smo uporabili logično spremenljivko x. S pomočjo spremenljivke smo sestavili *izjavni formuli*:

$P(x) \equiv x$ je smrten,
$Q(x) \equiv x$ je človek.

Formuli $P(x)$ in $Q(x)$ sami zase še nista izjavi. Postaneta pa izjavi, če pred njiju zapišemo: za vsak x (oznaka: $\forall x$), obstaja x (oznaka: $\exists x$), ali pa če x nadomestimo s konkretnim objektom področja pogovora (npr., če spremenljivko x v izjavni formuli $P(x)$ nadomestimo s konkretno osebo z imenom *Sokrat*). Tako lahko izjave A, B in C zapišemo na naslednji način:

$A \equiv \forall x(Q(x) \Rightarrow P(x))$,
$B \equiv Q(\text{Sokrat})$,
$C \equiv P(\text{Sokrat})$.

Sklep, da je Sokrat smrten, zdaj zavzame naslednjo obliko:

$$\forall x(Q(x) \Rightarrow P(x)), Q(\text{Sokrat}) \vDash P(\text{Sokrat}).$$

Znakom P in Q iz zgornjih primerov rečemo tudi *predikati*. Oglejmo si nekaj zgledov predikatov:

- $P(x) \equiv x$ je ženskega spola,
- $Q(x) \equiv x$ je praštevilo,

- $V(x, y) \equiv x \geq y$,
- $R(x, y, z) \equiv$ točka x leži na daljici s krajišči v točkah y in z.

Številu logičnih spremenljivk, ki slediju danemu predikatu, rečemo mestnost predikata. Zgornja predikata P in Q sta tako enomestna, predikat V je dvomesten, predikat R pa celo tromesten.

Izjavne formule lahko s pomočjo logičnih operacij (veznikov) združujemo v nove izjavne formule. Na primer, izjavni formuli "$P(x) \equiv x$ je ženskega spola" in "$T(x) \equiv x$ je lepa" lahko združimo v izjavne formule $P(x) \wedge T(x)$, $P(x) \Rightarrow T(x)$, $\neg P(x)$ in tako dalje.

3.1 Izjavne sheme

Oglejmo si pobliže izjavno formulo

$$\forall x P(\text{Sokrat}, x), \tag{S}$$

V njej nastopa več raznorodnih znakov: predikat P, logična spremenljivka x, konstanta *Sokrat*, kvantifikator $\forall$ in oklepaji ter zaklepaji.

Brž ko se domenimo, katere objekte lahko označujejo logične spremenljivke, kateri konkretni objekt imamo v mislih, ko govorimo o *Sokratu*, in katero konkretno relacijo med objekti označuje predikat P, nam zgornja formula preide v izjavo.

Na primer, če se domenimo, da logične spremenljivke označujejo poljubne antične filozofe, da predikat $P(x, y)$ pomeni "x je pametnejši od y", konstanta *Sokrat* pa označuje dobro znanega filozofa iz Aten, rojenega leta 470 pr. n. št., potem zgornja formula preide v trditev:

Sokrat je pametnejši od vseh antičnih filozofov.

Zgornjemu dogovoru o pomenu posameznih sestavnih delov formule (S) pravimo *interpretacija*, sami formuli pred tem dogovorom pa *izjavna shema*. Izjavna shema je torej zapis, ki ima obliko izjave, pri katerem pa kontekst in pomeni oznak za predikate in konstante še niso določeni.

Preden si ogledamo nekaj zgledov izjavnih shem in njihovih interpretacij, se pomudimo še pri rabi kvantifikatorjev in logičnih spremenljivk. Par oklepajev, ki sledi kvantifikatorju, določa *doseg kvantifikatorja*. Vsak kvantifikator *veže* le tiste pojavitve pripadajoče logične spremenljivke, ki ležijo znotraj dosega kvantifikatorja. Pojavitve logične spremenljivke, ki niso

vezane s kvantifikatorjem, pravimo, da so *proste*. Tako v formuli $(**)$ kvantifikator $\exists$ veže obe pojavitvi spremenljivke x, zato prostih pojavitev spremenljivk ni več. Če pa bi namesto $(**)$ pisali

$$\exists x\big(P(x)\big) \wedge R(x),$$

bi druga pojavitev spremenljivke x ostala prosta. Zato zgornja formula ni izjavna shema, saj prostih pojavitev logičnih spremenljivk v izjavni shemi ne sme biti.

Včasih par oklepajev za kvantifikatorjem v zapisu izjavne sheme tudi izpustimo. V tem primeru za doseg kvantifikatorja vzamemo najkrajši možni niz znakov, ki kvantifikatorju sledijo, za katerega ima izjavna shema še smisel. Na primer, če pišemo $\forall x P(x) \wedge R(x)$, v resnici mislimo $\forall x\big(P(x)\big) \wedge R(x)$.

3.2 Interpretacije izjavnih shem

Vrnimo se sedaj k interpretacijam izjavnih shem. Formalno lahko interpretacijo definiramo kot par (U, φ), kjer je U poljubna množica, ki ji rečemo *področje pogovora*, φ pa preslikava, ki konstante formalnega jezika slika v objekte s področja pogovora, n-mestne predikate pa v n-mestne relacije med objekti področja pogovora. Pri interpretaciji dane sheme moramo torej podati tri stvari:

- področje pogovora, tj. množico objektov, od koder bomo jemali naše logične konstante in vrednosti logični spremenljivk;
- pomen vsakega predikata, ki nastopa v shemi, pri čemer enomestnemu predikatu priredimo lastnost, smiselno za objekte s področja pogovora, dvomestnemu predikatu relacijo med objekti področja pogovora itd.;
- pomene konstant, ki nastopajo v shemi, pri čemer vsaki konstanti priredimo en sam objekt področja pogovora.

Ko je interpretacija izjavne sheme določena, lahko ugotavljamo, ali preide v pravilno ali nepravilno izjavo. Pri tem se držimo pravila, ki pravi, da je izjava $\forall x P(x)$ pravilna, če in samo če je izjava $P(a)$ pravilna za prav vsak objekt $a \in U$, izjava $\exists x P(x)$ pravilna, če in samo če obstaja kak objekt $a \in U$, za katerega je izjava $P(a)$ pravilna.

ZGLED. *Poiščimo nekaj interpretacij izjavne sheme* $\forall y \exists x P(x, y)$.

Pri prvi interpretaciji bomo za področje pogovora vzeli množico vseh realnih števil, predikat P naj preide v relacijo "biti manjši", torej $P(x, y) \equiv x < y$. Pri tej interpretaciji zgornja izjavna shema preide v pravilen stavek, ki trdi, da za vsako realno število obstaja neko drugo realno število, ki je od prvega manjše.

Druga interpretacija naj bo enaka prvi, le da za področje pogovora vzamemo množico naravnih števil namesto množice realnih števil. Pri tej interpretaciji izjavna shema preide v nepravilno izjavo, saj obstaja naravno število (namreč število 1), za katerega ni prav nobenega strogo manjšega naravnega števila.

Tretja dobro znana interpretacija zgornje izjavne sheme se nanaša na neko izbrano funkcijo $f\colon \mathbb{R} \to \mathbb{R}$ in točko $a \in \mathbb{R}$. Področje pogovora naj bo množica pozitivnih realnih števil, predikat $P(\delta, \epsilon)$ pa naj pomeni "Za vsako realno število x, ki je od števila a oddaljeno za manj kot δ, velja, da je vrednost $f(x)$ oddaljena od vrednosti $f(a)$ za manj kot ϵ." Kot vemo, je izjava, ki jo dobimo iz sheme $\forall \epsilon \exists \delta P(\delta, \epsilon)$ pri tej interpretaciji, pravilna, če in samo če je funkcija f zvezna v točki a. ∎

Kot vidimo, lahko posamezna izjavna shema v neki interpretaciji preide v pravilno izjavo, v kaki drugi interpretaciji pa v nepravilno izjavo. Za izjavno shemo S, ki preide v pravilno izjavo pri prav vsaki interpretaciji, rečemo, da je *splošno veljavna*. Pri tem pišemo

$$\vDash S.$$

Če želimo torej dokazati, da kaka izjavna shema ni splošno veljavna, moramo najti interpretacijo, pri kateri preide v nepravilno izjavo. Takšni interpretaciji rečemo *protiprimer* za dano izjavno shemo.

ZGLED. *S protiprimerom dokaži, da izjavna shema* $\forall x \forall y \big(P(x, y) \Rightarrow P(y, x)\big)$ *ni splošno veljavna.*

Podati moramo interpretacijo, pri kateri zgornja shema preide v nepravilno trditev. Za področje pogovora vzemimo, na primer, množico naravnih števil, predikat $P(x, y)$ pa interpretirajmo kot "$x \leq y$", oziroma v slovenščini, "število x je manjše ali enako številu y". Tedaj shema preide v trditev, ki trdi, da za poljubni naravni števili x in y, za kateri je $x \leq y$, velja tudi $y \leq x$. Ta trditev je očitno napačna, saj za $x = 2$ in $y = 3$ velja $x \leq y$, vendar ne velja $y \leq x$. ∎

3.3 Osnovne enakovrednosti izjavnih shem

Če za kaki izjavni shemi S in T velja

$$\models S \Leftrightarrow T,$$

rečemo, da sta *enakovredni*, in pišemo $S \sim T$. Podobno, če velja

$$\models S \Rightarrow T,$$

rečemo, da je shema T logična posledica sheme S, in pišemo $S \to T$. Naštejmo nekaj enakovrednsti in logičnih posledic izjavnih shem.

$$\begin{aligned}
\neg\forall x P(x) &\sim \exists x \neg P(x) && (1)\\
\neg\exists x P(x) &\sim \forall x \neg P(x) && (2)\\
\exists x \exists y P(x,y) &\sim \exists y \exists x P(x,y) && (3)\\
\forall x \forall y P(x,y) &\sim \forall y \forall x P(x,y) && (4)\\
\exists x \forall y P(x,y) &\to \forall y \exists x P(x,y) && (5)\\
\forall x (P(x) \wedge Q(x)) &\sim \forall x P(x) \wedge \forall x Q(x) && (6)\\
\exists x (P(x) \vee Q(x)) &\sim \exists x P(x) \vee \exists x Q(x) && (7)
\end{aligned}$$

Zgornje formule nekoliko pokomentirajmo:

Formuli (1) in (2) nekoliko spominjata na deMorganova zakona in pojasnita, kako znak za negacijo nesemo preko kvantifikatorja. Premislimo, kdaj bo (pri poljubni interpretaciji) izjava $\neg\forall x P(x)$ pravilna. Natanko tedaj, ko bo izjava $\forall x P(x)$ nepravilna. To pa se zgodil, če in samo če najdemo kak objekt a s področja pogovora, za katerega je $P(a)$ nepravilna izjava (saj bi v nasprotnem veljalo $P(a)$ za prav vse objekte, in zato tudi $\forall x P(x)$). To pa pomeni, da je izjava $\neg P(a)$ za takšen objekt a pravilna, kar po drugi strani pomeni, da je pravilna tudi izjava $\exists x \neg P(x)$. Podobno se lahko prepričamo v veljavnost točke (2).

Formuli (3) in (4) nista kdo ve kako zanimivi, saj pravita le, da je vseeno ali rečemo "za vsak x in za vsak y" ali "za vsak y in za vsak x". V sloveščini ti dve besedni zvezi navadno poenostavimo kar v "za vsaka x in y". Tudi simbolni zapis ponavadi poenostavimo in pišemo $\forall x, y : P(x,y)$ (v zapis smo dodali ločilo ":", da nakažemo, kje smo prenehali naštevati logične spremenljivke, ki so "kvantificirane".

Mnogo zanimivejša je formula (5). Poglejmo, kaj (pri poljubni interpretaciji) pravi leva stran formule, $\exists x \forall y P(x,y)$. Če naj bo to pravilna trditev, potem mora na področju pogovora obstajati nek objekt a, za katerega

pri poljubnem drugem objektu y velja $P(a, y)$. To pa med drugim pomeni, da lahko za poljuben objekt y najdemo objekt x (namreč kar objekt $x = a$), za katega velja $P(a, y)$. To pa z znaki lahko zapišemo kot $\forall y \exists x P(x, y)$. Ta premislek pokaže, da pri poljubni interpretaciji iz trditve $\exists x \forall y P(x, y)$ sledi trditev $\forall y \exists x P(x, y)$, kar smo tudi želeli pokazati.

Na tem mestu se pojavi naravno vprašanje, ali velja tudi obratna implikacija: ali pri poljubni interpretaciji iz $\forall y \exists x P(x, y)$ sledi $\exists x \forall y P(x, y)$. Odgovor je negativen, kot smo v resnici videli že v enem od prejšnih zgledov. Namreč, če za področje pogovora vzamemo množico naravnih števil, za predikat $P(x, y)$ pa relacijo $y < x$, tedaj je trditev $\forall y \exists x P(x, y)$ pravilna (saj pravi, da za vsako naravno število obstaja neko drugo, ki je od njega večje), trditev $\exists x \forall y P(x, y)$ pa nepravilna (saj pravi, da obstaja neko naravno število, ki je večje od vsakega drugega naravnega števila).

Nazadnji si oglejmo še formuli (6) in (7). Premislimo, kaj v resnici (pri poljubni interpretaciji) trdi izjava $\forall x(P(x) \wedge Q(x))$. Pravi, da za vsak objekt a s področja pogovora velja tako $P(a) \wedge Q(a)$, in zato, seveda tako $P(a)$ kot $Q(a)$. To pa pomeni, da velja tako $\forall x P(x)$ kot $\forall x Q(x)$, in zato tudi $\forall x P(x) \wedge \forall x Q(x)$. Še lažje se prepričamo, da iz $\forall x P(x) \wedge \forall x Q(x)$ sledi $\forall x(P(x) \wedge Q(x))$, in s tem, da sta ti dve izjavni shemi enakovredni. V pravilnost formule (7) se prepričamo na podoben način.

Pri tem naj poudarimo, da sorodni shemi $\exists x(P(x) \wedge Q(x))$ in $\exists x P(x) \wedge \exists x Q(x)$ nista enakovredni, saj prva trdi, da lahko najdemo objekt a, za katerega velja tako $P(a)$ kot $Q(a)$, medtem ko druga pravi le, da lahko najdemo nek objekt, recimo a, za katerega velja $P(a)$, in morda nek drug objekt, recimo b, za katerega velja $Q(b)$. Ti dve izjavi pa vsaj pri kakšni interpretaciji očitno nista enakovredni (poišči kako tako interpretacijo!). Ni pa težko videti, da velja

$$\exists x(P(x) \wedge Q(x)) \rightarrow \exists x P(x) \wedge \exists x Q(x).$$

Podobno vidimo, da nista enakovredni niti shemi $\forall x(P(x) \vee Q(x))$ in $\forall x P(x) \vee \forall x Q(x)$, da pa velja

$$\forall x P(x) \vee \forall x Q(x) \rightarrow \forall x(P(x) \vee Q(x)).$$

Za konec se domenimo še naslednje: Če je A poljubna množica s področja pogovora in P poljuben predikat, potem smemo zapis $\forall x(x \in A \Rightarrow P(x))$ skrajšati in pisati $(\forall x \in A)P(x)$ in brati: "Za vsak x iz A velja $P(x)$". Podobno skrajšamo zapis $\exists x(x \in A \Rightarrow P(x))$ v $(\exists x \in A)P(x)$ in beremo: "Obstaja x iz A, za katerega velja $P(x)$". Premisli, da v teh skrajšanih

zapisih deMorganova zakona preideta v $\neg(\forall x \in A)P(x) \sim (\exists x \in A)\neg P(x)$ in $(\exists x \in A)P(x) \sim (\forall x \in A)\neg P(x)$.

Množice in relacije

4 Osnovno o množicah

4.1 Relacije vsebovanosti in enakosti

Za naše potrebe *množica* pomeni *skupino* (*zbirko, družino, nabor,...*) nekih *objektov*. Če množica A vsebuje objekt x, pravimo, da je x *element* množice A in zapišemo

$$x \in A.$$

Dve množici sta *enaki* natanko tedaj, ko *vsebujeta* iste elemente. To zapišemo takole:

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

Če množica A vsebuje vse elemente množice B (in morda še kakšnega za povrh), pravimo, da je B *podmnožica* množice A in to zapišemo kot $B \subseteq A$:

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

Množici A in B sta torej enaki natanko tedaj, ko velja tako $A \subseteq B$ kot $B \subseteq A$. S simboli to zapišemo kot

$$\forall A \forall B(A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A).$$

Končno množico lahko določimo tako, da naštejemo vse njene elemente. Na primer,

$$A := \{2, 3, 5, 7\} \text{ ali } X := \{\text{Sonce}, \text{Zemlja}, \text{Mesec}\}.$$

V splošnem množice podamo tako, da podamo *pogoj za pripadnost*. Na primer,

$$\mathbb{P} := \{x \mid x \text{ je naravno število, deljivo le z } 1 \text{ in samim seboj}\}.$$

4.2 Operacije z množicami

Za dani dve množici A in B lahko definiramo njuno *unijo* in *presek*:

$$A \cup B = \{x \mid x \in A \vee x \in B\}, \qquad A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

Če množici A in B nimata nobenega skupnega elementa, je njun presek množica, ki ne vsebuje nobenega elementa. Takšni množici pravimo *prazna množica* in jo označimo s simbolom $\emptyset$.

Za vsako množico A velja

$$\emptyset \subseteq A,\ A \cup \emptyset = A \ \text{ in } \ A \cap \emptyset = \emptyset.$$

Poleg operacij unije in preseka omenimo še operaciji *razlike* in *simetrične razlike* množic

$$A - B = \{x \mid x \in A \wedge x \notin B\}, \qquad A \oplus B = (A \cup B) - (A \cap B).$$

Mnogokrat je udobno vnaprej izbrati množico vseh objektov, o katerih želimo govoriti. Takšni množici rečemo *univerzalna množica* in jo označimo z $\mathcal{U}$. Vse ostale množice so tedaj podmnožice množice $\mathcal{U}$. S pomočjo univerzalne množice definiramo operacijo *komplementa*. Komplement množice A vsebuje natanko tiste elemente univerzalne množice, ki jih A ne vsebuje:

$$\overline{A} = \{x \mid x \notin A\}.$$

Navedimo nekaj zanimivih lastnosti zgoraj definiranih operacij:

$A \cap B = B \cap A$	komutativnost preseka
$A \cup B = B \cup A$	komutativnost unije
$(A \cap B) \cap C = A \cap (B \cap C)$	asociativnost preseka
$(A \cup B) \cup C = A \cup (B \cup C)$	asociativnost unije
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	distributivnost preseka
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	distributivnost unije
$\overline{(A \cap B)} = \overline{A} \cup \overline{B}$	1. de Morganov zakon
$\overline{(A \cup B)} = \overline{A} \cap \overline{B}$	2. de Morganov zakon
$A \cap (A \cup B) = A$	1. absorbcijsko pravilo
$A \cup (A \cap B) = A$	2. absorbcijsko pravilo
$A \cap A = A$	idempotentnost preseka
$A \cup A = A$	idempotentnost unije
$A \cap \emptyset = \emptyset$	presek s prazno množico
$A \cup \emptyset = A$	unija s prazno množico

4.3 Presek in unija družine množic

Poleg preseka in unije dveh množic v matematiki pogosto uporabljamo presek in unijo *družine množic*. Naj bo $\mathcal{D}$ množica, katere elementi so množice (takšni množici ponavadi rečemo *družina množic*. Tedaj *unijo družine* $\mathcal{D}$ definiramo kot množico vseh tistih objektov, ki se pojavijo v vsaj eni od množic iz $\mathcal{D}$:

$$\bigcup \mathcal{D} = \bigcup_{A \in \mathcal{D}} A = \{x \mid \exists A(A \in \mathcal{D} \wedge x \in A)\}.$$

Presek družine $\mathcal{D}$ pa definiramo kot množico vseh tistih objektov, ki so vsebovani v prav vsaki množici iz družine $\mathcal{D}$:

$$\bigcap \mathcal{D} = \bigcap_{A \in \mathcal{D}} A = \{x \mid \forall A(A \in \mathcal{D} \Rightarrow x \in A)\}.$$

Zgled. *Naj bo* $\mathcal{D} = \{\{1,2,3\},\{2,3,4\},\{3,4,5\}\}$. *Tedaj je*

$$\bigcap \mathcal{D} = \{3\} \quad \textit{in} \quad \bigcup \mathcal{D} = \{1,2,3,4,5\}.$$

Dalje, za naravno število n *definirajmo* $A_n = \{x \mid x \in \mathbb{N} \wedge x \geq n\}$. *Tedaj je*

$$\bigcap_{n \in \mathbb{N}} A_n = \emptyset \quad \textit{in} \quad \bigcup_{n \in \mathbb{N}} A_n = \mathbb{N}.$$

■

4.4 Intervali v $\mathbb{R}$

V matematični analizi igrajo pomembno vlogo množice realnih števil, ki ležijo med dvema predpisanima realnima številoma. Takšnim množicam pravimo intervali. Definiramo več vrst intervalov, ki se ločijo glede na to, ali vsebujejo svoja mejna števila ali ne. Naj bosta a in b realni števili in naj bo $a < b$. Tedaj definiramo:

$[a,b] = \{x \mid x \in \mathbb{R} \wedge a \leq x \leq b\}$	zaprti interval
$(a,b) = \{x \mid x \in \mathbb{R} \wedge a < x < b\}$	odprti interval
$(a,b] = \{x \mid x \in \mathbb{R} \wedge a < x \leq b\}$	navzgor polzaprti interval
$[a,b) = \{x \mid x \in \mathbb{R} \wedge a \leq x < b\}$	navzdol polzaprti interval
$[a,\infty) = \{x \mid x \in \mathbb{R} \wedge a \leq x\}$	navzgor neomejeni zaprti interval
$(a,\infty) = \{x \mid x \in \mathbb{R} \wedge a \leq x\}$	navzgor neomejeni odprti interval
$(-\infty,b] = \{x \mid x \in \mathbb{R} \wedge a \leq x\}$	navzdol neomejeni zaprtii interval
$(-\infty,b) = \{x \mid x \in \mathbb{R} \wedge a \leq x\}$	navzdol neomejeni odprtii interval

ZGLED. *Preveri, da velja*

$$\bigcap_{n\in\mathbb{N}} [0, \frac{1}{n}) = \{0\}, \qquad in \qquad \bigcap_{n\in\mathbb{N}} (0, \frac{1}{n}] = \emptyset.$$

■

ZGLED. *Preveri, da velja*

$$\bigcup_{n\in\mathbb{N}} [\frac{1}{n}, 1] = (0, 1].$$

■

4.5 Potenčna množica

Naj bo A dana množica. Množici, katere elementi so natanko vse podmnožice množice A (vključno s podmnožicama A in $\emptyset$) rečemo *potenčna množica množice* A. Označimo jo z oznako $\mathcal{P}A$. Na primer, če je $A = \{1, 2\}$, potem je

$$\mathcal{P}A = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}.$$

Ni se težko prepričati, da potenčna množica množice z n elementi šteje natanko 2^n elementov.

4.6 Urejeni pari in kartezični produkt

Naj bosta a in b dva objekta. Tedaj njun *urejeni par* označimo s simbolom (a, b). Dva urejena para (a, b) in (c, d) sta enaka, če in samo če je $a = c$ in $b = d$. Množico vseh urejenih parov (a, b), kjer a preteče neko množico A, b pa neko množico B, označimo z $A \times B$ in ji rečemo *kartezični produkt* množic A in B.

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

ZGLED. *Naštej elemente kartezičnega produkta $A \times B$, kjer je $A = \{1, 2, 3\}$ in $B = \{3, 4\}$.*

$$A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}.$$

■

Trditev 4.1 *Če množica A šteje n elementov, množica B pa m elementov, tedaj množica $A \times B$ šteje nm elementov.*

Podobno kot kartezični produkt dveh množic lahko definiramo tudi kartezični produkt poljubnega števila množic A_1, $A_2, \ldots, A_n$. Elementi takšnega produkta niso več urejeni pari, temveč urejene n-terice $(a_1, a_2, \ldots, a_n)$:

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

5 Relacije

V matematiki (in tudi zunaj nje) imamo velikokrat opravka s pojmom *relacija*. Na primer, v množici števil lahko vpeljemo relacijo $\leq$, ali pa relacijo $\neq$, ali denimo $\equiv (\bmod 3)$, itd. V geometriji lahko vpeljemo relacije *vzporednosti*, *skladnosti* in podobno. Tudi v vsakdanjem življenju si lahko mislimo relacije kot so: "x je oče y", "x ima rad y", "x je starejši od y", itd. Kako ta intuitiven pojem vpeljati na korekten način?

Denimo, da imamo neko relacijo R med objekti množice A. Ta relacija določa množico

$$\{(x, y) \mid x \text{ je v relaciji } R \text{ z } y\} \subseteq A \times A.$$

Očitno je zgornja množica z relacijo R natanko določena. Velja pa tudi obratno. Vsaka podmnožica $R \subseteq A \times A$ določa neko relacijo, namreč tisto, za katero velja:

$$x \text{ je v relaciji z } y \text{ natanko tedaj, ko je } (x, y) \in R.$$

V tem smislu lahko pojem relacije in podmnožice množice $A \times A$ kar enačimo. V resnici na ta način dobimo tako imenovane dvomestne relacije. Seveda pa poznamo relacije, ki povezujejo več kot dva objekta, na primer, v geometriji lahko vpeljemo "premica x je v relaciji s premicama y in z, če seka y in z pod istim kotom", ali pa v teoriji števil, "x, y in z so v relaciji, če je $x+y = z$", itd. Takšne *trimestne relacije* lahko predstavimo s podmnožicami karteţicnega produkta $A \times A \times A$.

DEFINICIJA 5.1 Naj bo n naravno število. Podmnožici R množice $A^n = A \times A \times \ldots \times A$ pravimo n-mestna relacija na množici A. Če je $(x_1, x_2, \ldots, x_n) \in R$. rečemo, da so elementi $x_1, x_2, \ldots, x_n$ v relaciji R. Če je $n = 2$, dejstvo $(x_1, x_2) \in R$ zapišemo tudi kot $x_1 R x_2$.

Od sedaj dalje se bomo ukvarjali le z dvomestnimi relacijami. Če je množica A, na kateri je relacija definirana, končna (in ne prevelika), si lahko dvomestno relacijo predstavimo tudi s pomočjo *grafa relacije*, ki ga dobimo takole:

Vsak element množice A predstavimo kot točko v ravnini, za vsak par elementov $a, b \in A$, za katera velja aRb, pa narišemo usmerjeno daljico od a do b. Če je $a = b$ (in torej aRa), potem namesto usmerjene daljice narišemo zanko skozi a (ukrivljeno črto, ki se prične in konča v a).

ZGLED. *Nariši graf relacije R na množici $\{2,3,4,5,6,7,8,9\}$ definirani s predpisom $xRy \equiv x$ deli y.*

Narišemo osem točk v ravnini (denimo enakomerno razporejenih na obodu kroga), jih označimo s števili $2,3,\ldots,9$, narišemo usmerjene daljice $\overrightarrow{24}$, $\overrightarrow{26}$, $\overrightarrow{28}$, $\overrightarrow{36}$, $\overrightarrow{39}$, $\overrightarrow{48}$ in dodamo še zanko na vsako od osmih točk. ∎

Naj bo R dvomestna relacija na množici A. Tedaj množici

$$\mathcal{D}_R = \{x \mid \exists y(xRy)\}$$

rečemo *domena realcije* R, množici

$$\mathcal{Z}_R = \{y \mid \exists x(xRy)\}$$

pa *zaloga vrednosti realcije* R. Očitno velja $R \subseteq \mathcal{D}_R \times \mathcal{Z}_R$. Unija $\mathcal{D}_R \cup \mathcal{Z}_R$ se imenuje *polje relacije* R. Na grafu domeno relacije prepoznamo kot množico točk, iz katerih kaže vsaj ena usmerjena daljica (ali zanka), zalogo vrednosti pa kot mnozčio točk, v katero kaže vsaj ena usmerjena daljica (ali zanka).

5.1 Operacije na relacijah

Iz danih relacij R in T na množici A lahko tvorimo nove relacije na množici A. Oglejmo si nekaj načinov:

Komplementarna relacija: Elementa $x, y \in A$ sta v *komplementarni relaciji* $\bar{R}$ natanko tedaj, ko nista v relaciji R:

$$x\,\bar{R}\,y \Leftrightarrow \neg(x\,R\,y).$$

Graf komplementarne relacije narišemo tako, da narišemo usmerjene daljice povsod, kjer jih prej ni bilo, stare pa zbrišemo.

ZGLEDI: Če je R relacija "biti večji ali enak" na množici naravnih števil, je komplementarna relacija $\bar{R}$ relacija "ne biti večji ali enak", kar je na množici naravnih števil isto kot "biti strogo manjši". Komplementarna relacija relacije "biti sin od" je "ne biti sin od". Podobno, če je R relacija "biti vzporeden" na množici vseh premic v ravnini, potem sta dve premici v komplementarni relaciji $\bar{R}$, če in samo če nista vzporedni.

Inverzna relacija: Elementa $x, y \in A$ sta v inverzni relaciji R^{-1}, natanko tedaj, ko sta v obratnem vrstnem redu, y, x, v relaciji R:

$$x\,R^{-1}\,y \Leftrightarrow y\,R\,x.$$

Velja: $\mathcal{D}_{R^{-1}} = \mathcal{Z}_R$ in $\mathcal{Z}_{R^{-1}} = \mathcal{D}_R$. Očitno tudi: $(R^{-1})^{-1} = R$. Graf inverzne relacije dobimo tako, da spremenimo usmeritev vsem usmerjenim daljicam.

ZGLEDI: Inverz relacije $\leq$ na množici $\mathbb{R}$ je relacija $\geq$. Inverz relacije "mož" na množici držaljanov RS je "žena". Inverz relacije "je sosed ali soseda" pa je kar relacija "je sosed ali soseda".

Kompozitum relacij: Elementa x in z sta v sestavljeni relaciji $T \circ R$, če lahko najdemo kak element (recimo y), za katerega velja xRy in yRz. S simboli:

$$x\,(T \circ R)\,z \Leftrightarrow \exists y(x\,R\,y \wedge y\,R\,z).$$

Graf kompozita $T \circ R$ dobimo tako, da na isto sliko narišemo grafa relacij T in R, prvega z modro barvo, drugega z rdečo, nato pa vsak zaporedni par rdeče in modre usmerjene daljice (v tem vrstnem redu) nadomestimo z novo (črno) usmerjeno daljico. Stare (rdeče in modre) daljice seveda zbrišemo.

ZGLED. *Kakšne relacije na množici ljudi predstavljajo naslednji kompoziti: "je brat" ∘ "je sin"; "je sin" ∘ "je brat"; "je sin" ∘ "je oče"; "je oče" ∘ "je sin". Pri tem zaradi enostavnosti predpostavimo, da ima vsaka oseba otroke z največ eno drugo osebo, le-ta pa je nasprotnega spola.*

- x ("je brat" ∘ "je sin") $y \Leftrightarrow x$ "je nečak (po očetovi strani)" y;
- x ("je sin" ∘ "je brat") $y \Leftrightarrow x$ "je sin" $y \wedge x$ ima brata;
- x ("je sin" ∘ "je oče") $y \Leftrightarrow (x = y \wedge x$ ima sina) $\vee (x$ je moški in ima sina z $y)$;
- x ("je oče" ∘ "je sin") $y \Leftrightarrow x = y \vee x$ je brat ali sestra y.

■

Zgornji zgledi kažejo, da v splošnem ne velja komutativnostni zakon $R \circ T = T \circ R$. Velja pa asociativnostni zakon, $R \circ (T \circ S) = (R \circ T) \circ S$, in običajno pravilo za računanje inverza sestavljene relacije, $(R \circ T)^{-1} = T^{-1} \circ R^{-1}$.

Na vsaki množici A z vsaj dvema elementoma imamo vedno vsaj tri relacije: *univerzalno relacijo* $U = A \times A$, prazno relacijo $\emptyset$ in identiteto $I = \{(x, x) \mid x \in A\}$. Očitno za poljubno relacijo R velja:

- $R \circ I = I \circ R = R$,
- $R \circ \emptyset = \emptyset \circ R = \emptyset$,

- $x\, R \circ U\, y \Leftrightarrow (\exists u)(uRy)$,
- $x\, U \circ R\, y \Leftrightarrow (\exists v)(xRv)$.

5.2 Lastnosti relacij

Naj bo R dvomestna relacija na množici A. Tedaj pravimo:

- R je *refleksivna* $\Leftrightarrow (\forall x \in A)(xRx)$;
- R je *irefleksivna* $\Leftrightarrow (\forall x \in A)(x\bar{R}x)$;
- R je *simetrična* $\Leftrightarrow (\forall x \in A)(\forall y \in A)(x\, R\, y \Rightarrow y\, R\, x)$;
- R je *asimetrična* $\Leftrightarrow (\forall x \in A)(\forall y \in A)(x\, R\, y \Rightarrow y\, \bar{R}\, x)$;
- R je *antisimetrična* $\Leftrightarrow (\forall x \in A)(\forall y \in A)(x\, R\, y \wedge y\, R\, x \Rightarrow x = y)$;
- R je *tranzitivna* $\Leftrightarrow (\forall x \in A)(\forall y \in A)(\forall z \in A)(x\, R\, y \wedge y\, R\, z \Rightarrow x\, Rz)$;
- R je *sovisna* $\Leftrightarrow (\forall x \in A)(\forall y \in A)(x \neq y \Rightarrow (x\, R\, y \vee y\, R\, x))$;
- R je *strogo sovisna* $\Leftrightarrow (\forall x \in A)(\forall y \in A)(x\, R\, y \vee y\, R\, x)$.

Zgornje lastnosti relacij se seveda odražajo tudi na grafu relacije. Tako je, na primer, relacija *refleksivna*, če skozi vsako točko poteka zanka, *simetrična*, če graf z vsako usmerjeno daljico vsebuje tudi njej nasprotno usmerjeno daljico (v tem primeru takšen par navadno nadomestimo z eno samo, neusmerjeno daljico), *tranzitivna*, če z vsakim parom zaporednih usmerjenih daljic graf premore tudi usmerjeno daljico od prve do tretje točke v takšnem zaporedju itd.

Za vajo premisli, katere od zgoraj naštetih lastnosti imajo naslednje relacije:

- $<$ na množici $\mathbb{R}$,
- $\leq$ na množici $\mathbb{R}$,
- "kongruenten modulo 5" na $\mathbb{Z}$,
- $\subseteq$ na $\mathcal{P}(\mathbb{N})$.

5.3 Ekvivalenčna relacija in relacije urejenosti

Relacija je *ekvivalenčna*, če je hkrati refleksivna, simetrična in tranzitivna. Najpreprostejši zgled je kar identiteta I. Nadaljni zgledi so kongruenca po modulu m v množici $\mathbb{Z}$, vzporednost v množici premic v ravnini, "biti enako star" na množici ljudi itd.

Lastnost "biti ekvivalenčna relacija" lahko izrazimo tudi v jeziku inverza in kompozita relacij.

TRDITEV 5.2 *Relacija R je ekvivalenčna relacija na množici A natanko tedaj, ko je $\mathcal{D}_R = A$ in velja $R^{-1} \circ R = R$.*

Graf ekvivalenčne relacije razpade na nekaj med seboj nepovezanih grozdov, pri čemer znotraj posameznega grozda najdemo vse možne usmerjene daljico (vključno z vsemi zankami). Tem grozdom pravimo tudi *ekvivalenčni razredi* relacije. Ekvivalenčne razrede natančneje definiramo takole:

DEFINICIJA 5.3 Naj bo R ekvivalenčna relacija na množici A in $a \in A$. Tedaj množici

$$R(a) = \{x \in A \mid aRx\}$$

rečemo ekvivalenčni razred elementa a. Množici

$$A/R = \{R(a) \mid a \in A\}$$

vseh ekvivalenčnih razredov rečemo *faktorska množica* glede na R.

Množici $\mathcal{R} = \{A_1, \ldots, A_n\}$ nepraznih, paroma disjunktnih množic A_i, katerih unija je enaka A, rečemo *razbitje* množice A. Ni se težko prepričati v naslednje:

TRDITEV 5.4 *Faktorska množica A/R ekvivalenčne relacije $R \subseteq A \times A$ tvori razbitje množice A.*

Velja pa tudi obrat zgornje trditve: Denimo, da je $\mathcal{R}$ razbitje množice A. Definirajmo relacijo R na A takole: $xRy \Leftrightarrow$ "x in y ležita v isti množici razbitja $\mathcal{R}$". Ni težko videti, da je tako definirana relacija R ekvivalenčna, faktorska množica A/R pa kar enaka $\mathcal{R}$.

Relacijam, ki so tranzitivne, rečemo tudi *relacije urejenosti*. Relacije urejenosti razvrstimo v različne skupine (in podskupine), glede na to, katere dodatne lastnosti še imajo:

DEFINICIJA 5.5 Naj bo R tranzitivna relacija na množici A. Če je še:

- refleksivna in antisimetrična, ji rečemo *delna urejenost*;
- antisimetrična in strogo sovisna ji rečemo *linearna urejenost*;
- asimetrična, ji rečemo *stroga delna urejenost*;
- asimetrična in sovisna, ji rečemo *stroga linearna urejenost*.

TRDITEV 5.6 *Vsaka strogo sovisna relacija je refleksivna.*

DOKAZ: Naj bo R strogo sovisna relacija na množici S. Tedaj za poljuben par elementov $x, y \in S$ velja xRy ali yRx. Če za y vzamemo kar x, dobimo: xRx ali xRx, kar je isto kot xRx. ■

Neposredno iz definicije skupin urejenosti in zgornje trditve tedaj sledi:

- R je linearna urejenost $\Rightarrow$ R je delna urejenost;
- R je stroga linearna urejenost $\Rightarrow$ R je stroga delna urejenost.

5.4 Funkcije

Kot zanimivost si poglejmo še zvezo med relacijami in funkcijami. Naj bo R relacija na množici S in $A \subseteq S$. S simbolom $R(A)$ (ali tudi s simbolom AR) bomo označevali množico $\{y \in S \mid (\exists x \in A)xRy\}$. Če je $A = \{x\}$ množica z enim samim elementom, pišemo krajše $R(A) = R(x) = xR$.

Množica $R(x)$ je neprazna natanko tedaj, ko je $x \in \mathcal{D}_R$. Načeloma lahko vsebuje več kot en element. Če pa velja, da množica $R(x)$ vsebuje največ element za vsak x, rečemo, da je relacija R enolična. Enoličnim relacijam rečemo tudi *funkcije* (ali *preslikave*). Zapišimo se s simboli:

DEFINICIJA 5.7 Relacija f na množici S je enolična, če zanjo velja:

$$(\forall x)(\forall y)(\forall z)((xfy \wedge xfz) \Rightarrow y = z).$$

Enolični relaciji rečemo tudi funkcija. Pri tem namesto xfy pišemo kar $y = f(x)$, ali pa tudi xf.

Pojem domene in zaloge vrednosti relacije se smiselno prenese tudi na funkcije, saj so le-te poseben primer relacije. Če je torej f enolična relacija na množici S (funkcija), je

$$\mathcal{D}_f = \{x \mid \exists y(y = f(x))\} \quad \text{in} \quad \mathcal{Z}_f = \{y \mid \exists x(y = f(x))\}.$$

Pri funkcijah navadno poudarimo, kaj so njihove domene tako, da pišemo $f\colon A \to S$, kjer je $A = \mathcal{D}_f$, medtem ko je S poljubna množica, ki vsebuje zalogo vrednosti $\mathcal{Z}_f$.

Če pri zapisu $f\colon A \to S$ slučajno velja $S = \mathcal{Z}_f$, rečemo, da je f *surjektivna* funkcija (na množico S).

Inverz funkcije ni nujno enolična relacija. Če pa kljub temu je, rečemo, da je funkcija *injektivna*.

DEFINICIJA 5.8 Funkcija f na množici S je injektivna, če je inverzna relacija f^{-1} enolična:

$$(\forall x)(\forall y)(\forall z)((xfz \wedge yfz) \Rightarrow x = y).$$

Ni težko videti, da za relacijo R na množici S in podmnožici $U, V \subseteq S$ velja naslednje:

- $R(U \cup V) = R(U) \cup R(V)$ in $R(U \cap V) \subseteq R(U) \cap R(V)$ (vsebovanost v obratno smer ne velja nujno – npr. R je konstantna funkcija, U in V pa disjunktni).
- Če je R injektivna, velja tudi $R(U \cap V) = R(U) \cap R(V)$.
- $R^{-1}(U \cup V) = R^{-1}(U) \cup R^{-1}(V)$ in $R^{-1}(U \cap V) \subseteq R^{-1}(U) \cap R^{-1}(V)$.
- Če je R enolična, velja tudi $R^{-1}(U \cap V) = R^{-1}(U) \cap R^{-1}(V)$.
- $U \subseteq R^{-1}(R(U))$.
- Če je R injektivna, velja tudi $U = R^{-1}(R(U))$.
- $R(R^{-1}(U)) \subseteq U$.
- Če je $U \subseteq \mathcal{Z}_R$, velja tudi $R(R^{-1}(U)) = U$.
- $R(R^{-1}(R(U))) = R(U)$.

Teorija grafov

6 Osnovno o grafih

OPOMBA. Ta razdelek v veliki meri sledi prvemu poglavju knjige [3].

6.1 Definicija in osnovni pojmi

Naj bo V (običajno končna) neprazna množica in E poljubna družina dvoelementnih podmnožic množice V. Paru $\Gamma = (V, E)$ pravimo *graf* na *množici točk* (tudi *vozlišč*) $V = V(\Gamma)$ in z *množico povezav* $E = E(\Gamma)$. Če je $\{u, v\}$ povezava grafa Γ, tedaj pravimo, da sta točki u in v *sosednji* in pišemo $u \sim v$. Hkrati pravimo, da sta točki u in v krajišči povezave $\{u, v\}$. Povezavo $\{u, v\}$ včasih pišemo krajše kot uv ali vu.

OPOMBA. Včasih dopuščamo tudi grafe, ki imajo med nekaterimi pari točk več povezav (*vzporedne povezave*) ali pa imajo povezave, ki imajo obe krajišči enaki (*zanke*). Takim grafom bomo rekli *multigrafi*. Če definiramo, da zanka prispeva 2 k stopnji točke, potem lema 6.1 velja tudi za multigrafe. Kadar želimo poudariti, da govorimo o (multi)grafih brez zank in vzporednih povezav, takim grafom rečemo *enostavni grafi*.

Poleg multigrafov je grafom sorodna stuktura *usmerjeni graf*. Neformalno si ga lahko predstavljamo kot graf (ali celo kot multigraf), kjer vsako povezavo usmerimo. Namesto krajišč povezave v tem primeru govorimo kot o začetku in koncu povezave (repu in glavi povezave). Če je u rep in v glava povezave uv, potem napišemo $u \to v$ in rečemo, da je uv usmerjena povezava grafa Γ.

Grafe si radi tudi narišemo. To storimo tako, da vozlišča grafa predstavimo kot točke ravnine, povezavo med sosednjima vozliščema pa kot krivuljo (običajno kar kot daljico) s krajiščema v točkah ravnine, ki ustrezata krajiščema povezave.

Stopnja točke (tudi *valenca točke*) u v grafu Γ, označimo jo z $\deg_\Gamma(u)$, je enaka številu povezav grafa Γ, ki imajo točko u za svoje krajišče. Točkam

stopnje 0 pravimo *izolirane točke*. Graf Γ je *regularen*, če obstaja tako število k, da velja $\deg_\Gamma(u) = k$ za vsak $u \in V(\Gamma)$. V tem primeru rečemo tudi, da je graf Γ k-regularen, oziroma, da je regularen stopnje k.

Stopnje točk in število povezav grafa veže naslednja enakost:

LEMA 6.1 (O rokovanju). *Za vsak graf Γ velja*

$$\sum_{v \in V(\Gamma)} deg(v) = 2 \cdot |E(\Gamma)| \,.$$

DOKAZ: Uporabili bomo tako imenovano računovodsko pravilo. Naj bo $\mathcal{M}$ množica vseh urejenih parov $(u, e) \in V(\Gamma) \times E(\Gamma)$, za katere je u krajišče povezave e. Preštejmo elemente množice $\mathcal{M}$. Po eni strani velja

$$|\mathcal{M}| = \sum_{u \in V(\Gamma)} \deg(u),$$

po drugi strani pa

$$|\mathcal{M}| = \sum_{e \in E(\Gamma)} 2 = 2 \cdot |E(\Gamma)|.$$

S tem je trditev dokazana. ∎

POSLEDICA 6.2 *Vsak graf ima sodo mnogo točk lihe stopnje.*

OPOMBA. V usmerjenih grafih namesto stopnje $\deg(v)$ definiramo *vhodno stopnjo* $\deg^-(v)$ in *izhodno stopnjo* $\deg^+(v)$ točke v, pri čemer prva predstavlja število točk u grafa Γ, za katere je uv usmerjena povezava grafa Γ, druga pa število točk u grafa Γ, za katere je vu usmerjena povezava grafa Γ. V kontekstu grafov lema o rokovanju preide v enakost

$$\sum_{v \in V(\Gamma)} \deg^-(v) = \sum_{v \in V(\Gamma)} \deg^+(v) = |E|.$$

Graf Γ' je *podgraf* grafa Γ, če velja $V(\Gamma') \subseteq V(\Gamma)$ in $E(\Gamma') \subseteq E(\Gamma)$. Podgraf Γ' je *vpet*, če velja $V(\Gamma') = V(\Gamma)$, in je *induciran* z množico točk $U \subseteq V(\Gamma)$, če velja $V(\Gamma') = U$ in $E(\Gamma') = \{uv \in E(\Gamma) \mid u, v \in V(\Gamma')\}$. V tem primeru pišemo tudi $\Gamma' = \Gamma[U]$.

Graf Γ je *dvodelen*, če lahko množico točk $V(\Gamma)$ zapišemo kot disjunktno unijo dveh podmnožic $A, B \subseteq V(\Gamma)$ tako, da je za vsako povezavo $uv \in E(\Gamma)$ ena od točk u, v vsebovana v množici A, druga pa v množici B. Množici A in B imenujemo množici *dvodelnega razbitja* grafa Γ.

6.2 Metrične lastnosti

Zaporedje točk $v_0v_1 \dots v_k$ grafa Γ je *sprehod* dolžine k, če $v_i \sim v_{i+1}$ za $0 \leq i < k$. Sprehod je *enostaven*, če so vse povezave na njem različne. Sprehod je *sklenjen*, če je $v_0 = v_k$. Sprehod, na katerem so vse točke različne, je pot, enostaven sklenjen sprehod z vsaj eno povezavo, na katerem sta enaki le prva in zadnja točka, pa je cikel grafa. Zaradi enostavnosti dopuščamo tudi sprehode dolžine 0, tj. sprehode oblike v_0. Sprehod dolžine 0 je seveda hkrati tudi pot, domenimo pa se, da ga ne bomo imeli za cikel.

LEMA 6.3 *Če med točkama grafa obstaja sprehod dolžine k, potem med njima obstaja tudi pot dolžine največ k.*

DOKAZ: Naj bosta u in v poljubni točki grafa Γ med katerima obstaja sprehod. Če je $u = v$, tedaj med njima obstaja pot dolžine 0 in trditev očitno velja. Predpostavimo torej, da je $u \neq v$. Med vsemi sprehodi med u in v izberimo najkrajšega, denimo $S = v_0v_1 \dots v_m$, $u = v_0$, $v = v_m$. Dovolj je dokazati, da je S pot. Pa denimo, da temu ni tako. Tedaj obstajata v zaporedju $v_0, v_1, \dots, v_m$ kaka točka ponovi, denimo $v_i = v_j$ za $0 \leq i < j \leq m$. Vendar tedaj je tudi $S' = v_0v_1 \dots v_iv_{j+1} \dots v_m$ sprehod med u in v, ki pa je očitno krajši od sprehoda S. To pa nasprotuje naši izbiri sprehoda S in dokazuje, da je S pot. ∎

Za dve točki u in v rečemo, da sta v isti *povezani komponenti*, če med njima obstaja sprehod. Ni težko videti, da je relacija "biti v isti povezani komponenti" ekvivalenčna. Njenim ekvivalenčnim razredom rečemo *povezane komponente grafa*. Graf je *povezan*, če ima eno samo povezano komponento.

Razdaljo $d_\Gamma(u, v)$ med točkama u in v v grafu Γ definiramo kot dolžino najkrajše poti od u do v v Γ. (Če taka pot ne obstaja, za razdaljo vzamemo vrednost ∞.) Kot pove lema 6.3, bi lahko razdaljo ekvivalentno definirali tudi kot dolžino najkrajšega sprehoda med danima točkama.

S tako definirano razdaljo postane množica točk povezanega grafa metrični prostor. Največji razdalji med parom točk grafa pravimo *premer* (tudi *diameter*) grafa,

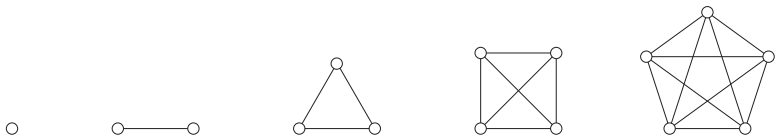
$$\operatorname{diam}(\Gamma) = \max\{d_\Gamma(u, v) \mid u, v \in V(\Gamma)\}\,.$$

Dolžini najkrajšega cikla v grafu pravimo tudi *notranji obseg* (ali *ožina*) grafa.

6.3 Nekatere družine grafov

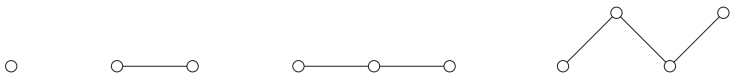
V tem razdelku si bomo ogledali nekaj družin grafov, ki jih pogosto srečujemo v zgledih in nalogah.

Polni grafi K_n: $V(K_n) = \mathbb{Z}_n$, $E(K_n) = \{uv \mid u, v \in \mathbb{Z}_n, u \neq v\}$. Polni graf K_n ima n točk in $\binom{n}{2} = \frac{n(n-1)}{2}$ povezav. Je $(n-1)$-regularen graf in je dvodelen le za $n = 1$ in 2.



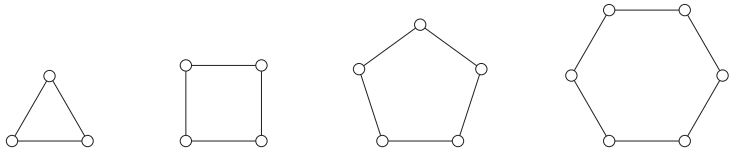
Slika 1: Polni grafi K_1, K_2, K_3, K_4 in K_5.

Poti P_n: $V(P_n) = \mathbb{Z}_n$, $E(P_n) = \{u(u+1) \mid u = 0, 1, \ldots, n-2\}$. Pot P_n ima n točk in $n-1$ povezav (njena *dolžina* je $n-1$). Za $n = 1$ in $n = 2$ je enaka grafu K_n. Vse poti so dvodelni grafi.



Slika 2: Poti P_1, P_2, P_3 in P_4.

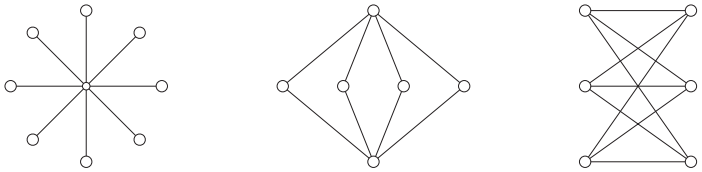
Cikli C_n $(n \geq 3)$: $V(C_n) = \mathbb{Z}_n$, $E(C_n) = \{u(u+1) \mid u \in \mathbb{Z}_n\}$. Kadar dopuščamo tudi multigrafe, sta definirana še cikla C_1 (zanka) in C_2 (par vzporednih povezav). Cikel C_n ima n točk in n povezav. Je 2-regularen graf in je dvodelen natanko tedaj, ko je n sodo število. Vsak 2-regularen graf je disjunktna unija enega ali več ciklov. Cikel C_3 imenujemo tudi *trikotnik*.



Slika 3: Cikli C_3, C_4, C_5 in C_6.

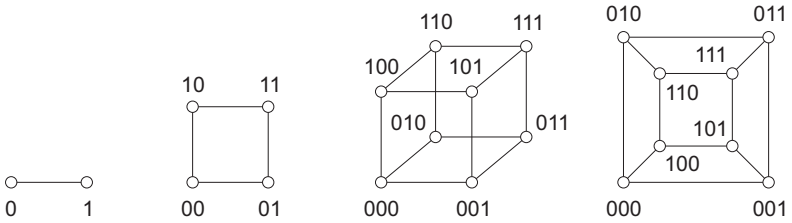
Polni dvodelni grafi $K_{m,n}$: $V(K_{m,n}) = A \cup B$, kjer velja $|A| = m$, $|B| = n$ in $A \cap B = \emptyset$, $E(K_{m,n}) = \{uv \mid u \in A, v \in B\}$. Polni dvodelni graf $K_{m,n}$

ima $m + n$ točk in mn povezav. Graf $K_{m,n}$ je regularen natanko tedaj, ko je $m = n$. Vsi grafi $K_{m,n}$ so dvodelni. Grafom $K_{1,n}$ pravimo tudi *zvezde*.



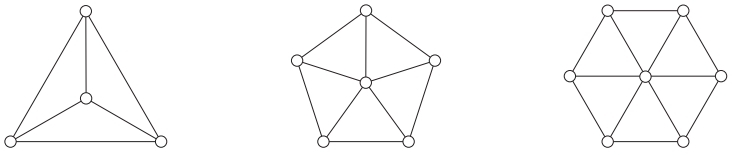
Slika 4: Polni dvodelni grafi $K_{1,8}$, $K_{2,4}$ in $K_{3,3}$.

Hiperkocke Q_d: $V(Q_d) = \{(u_1, u_2, \ldots, u_d) \mid u_i \in \{0, 1\}\}$, $E(Q_n) = \{uv \mid u, v \in V(Q_d) : \sum_{i=1}^{d} |u_i - v_i| = 1\}$. Običajno med hiperkocke štejemo tudi 0-razsežno kocko $Q_0 = K_1$. Hiperkocka Q_d (skelet d-razsežne kocke) ima 2^d točk in $d \cdot 2^{d-1}$ povezav. Je d-regularen graf. Vse hiperkocke so dvodelni grafi (za množici dvodelnega razbitja vzamemo množico točk, ki imajo sodo mnogo komponent enakih 0, in množico točk, ki imajo liho mnogo komponent enakih 0).



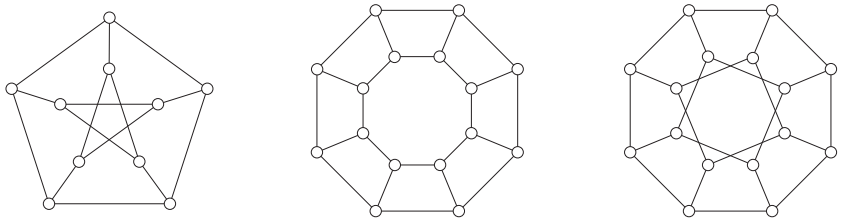
Slika 5: Hiperkocki Q_1 in Q_2 ter dve sliki hiperkocke Q_3.

Kolesa W_n ($n \geq 3$): $V(W_n) = \mathbb{Z}_n \cup \{\infty\}$, $E(W_n) = \{u(u+1), u\infty \mid u \in \mathbb{Z}_n\}$. Graf W_n ima $n + 1$ točk in $2n$ povezav. Za kolesa velja $\delta(W_n) = 3$ in $\Delta(W_n) = n$. Edino regularno kolo je $W_3 \simeq K_4$. Nobeno kolo ni dvodelen graf.



Slika 6: Kolesa W_3, W_5 in W_6.

Posplošeni Petersenovi grafi $P_{n,k}$ ($n \geq 3$ in $0 < k < n$): $V(P_{n,k}) = \{u_i, v_i \mid i \in \mathbb{Z}_n\}$, $E(P_{n,k}) = \{u_iu_{i+1}, u_iv_i, v_iv_{i+k} \mid i \in \mathbb{Z}_n\}$. Posplošeni Petersenov graf $P_{n,k}$ ima $2n$ točk. Če je $n \neq 2k$, ima $3n$ povezav in je kubičen graf, za $n = 2k$ pa ima $\frac{5n}{2}$ povezav. Graf $P_{n,k}$ je dvodelen natanko tedaj, ko je število n sodo in število k liho. Družina ima ime po *Petersenovem grafu* $P_{5,2}$.



Slika 7: Petersenov graf in posplošena Petersenova grafa $P_{8,1}$ in $P_{8,2}$.

7 Drevesa

V povezanem grafu med poljubnima dvema točkama obstaja vsaj ena pot. Grafu, v katerem med poljubnima dvema točkama obstaja natanko ena pot, rečemo *drevo*.

TRDITEV 7.1 *Za graf* Γ *so ekvivalentne naslednje trditve:*

(1) Γ *je drevo;*

(2) Γ *je povezan, ampak z odstranitvijo poljubne povezave postane nepovezan;*

(3) Γ *je povezan in* $|E(\Gamma)| = |V(\Gamma)| - 1$.

(4) Γ *ne vsebuje cikla in* $|E(\Gamma)| = |V(\Gamma)| - 1$.

(5) Γ *je povezan in ne vsebuje cikla.*

DOKAZ: Dokaz poteka z indukcijo na število točk. Trditev očitno drži za vse grafe na dveh točkah (takšna grafa sta samo dva, K_2 in njegov komplement). Denimo, da trditev drži za vse grafe na manj kot n točkah. Dokažimo, da tedaj velja tudi za graf Γ na n točkah.

(1) $\Rightarrow$ (2): Denimo, da je Γ drevo. Tedaj je povezan po deficiji. Naj bo $e = uv$ poljubna povezava grafa Γ. Tedaj je (u, v) **edina** pot med u in v. To pa pomeni, da v grafu $\Gamma - e$ ni nobene poti, kar pomeni, da Γ ni povezan.

(2) $\Rightarrow$ (3): Predpostavimo, da je Γ povezan, odstranitev poljubne povezave pa ga razbije. Dokazujemo enakost $|E(\Gamma)| = |V(\Gamma)| - 1$. Izberi povezavo e. Tedaj je $\Gamma - e$ unija povezanih komponent X in Y (premisli, da sta povezani komponenti dve in ne morda tri ali več). Grafa X in Y sta povezana, če pa odstanimo kakšno povezavo, razpadeta (saj če ne bi razpadla, ne bi ob odstranitvi te iste povezave razpadel niti graf Γ). Uporabimo indukcijo in dobimo $|E(X)| = |V(X)| - 1$ and $|E(Y)| = |V(Y)| - 1$. Tedaj

$$|E(\Gamma)| = |E(X)| + |E(Y)| + 1 = (|V(X)| - 1) + (|V(Y)| - 1) + 1 = |V(\Gamma)| - 1.$$

(3) $\Rightarrow$ (4): Predpostavljamo, da je Γ povezan in da zadošča pogoju $|E(\Gamma) = |V(\Gamma)| - 1$. Dokazujemo, da Γ nima ciklov. Pa recimo, da obstaja cikel C. Za vsak $v \in V(\Gamma)$ poiščemo prvo povezavo e_v na kaki najkrajši poti med v in C. Premislek pokaže, da je $e_v \neq e_u$ za poljubni različni točki $u, v \in V(\Gamma) \setminus V(C)$. Zato je

$$|E(\Gamma) \geq |E(C)| \cup |\{e_v : v \in V(\Gamma) \setminus V(C)\}| = V(\Gamma),$$

kar je protislovje.

(4) $\Rightarrow$ (5): Predpostavljamo, da je Γ brez ciklov in da velja$|E(\Gamma)| = |V(\Gamma)| - 1$. Dokazati moramo, da je Γ povezan. Naj bodo $X_1, \ldots, X_k$ komponente za povezanost in denimo, da je $k \geq 2$. Vsak izmed grafov X_i zadošča (5), zato po indukcijski predpostavki X_i zadošča tudi (4). Tedaj pa je $|E(X_i)| = |V(X_i)| - 1$. Po drugi strani:

$$|E(\Gamma)| = \sum_{i=1}^{k} |E(X_i)| = \sum_{i=1}^{k} |V(X_i)| - k.$$

Ker je $|E(\Gamma)| = |V(\Gamma)| - 1$, sledi $k = 1$, in Γ je povezan.

(5) $\Rightarrow$ (1): Predpostavljamo, da je Γ povezan in brez ciklov. Dokazujemo, da obstaja med poljubnima točkama natanko ena pot. Zaradi povezanoti obstaja vsaj ena pot. Če bi bili dve, bi dobili cikel – protislovje. ∎

POSLEDICA 7.2 *Drevo z vsaj dvema točkama vsebuje dve točki stopnje* 1.

DOKAZ: Naj bo Γ graf, v katerem ima vsaj $|V(\Gamma)| - 1$ točk stopnjo vsaj 2 (označimo množico teh točk z U). Preostala točka ima stopnjo vsaj 1, saj bi sicer tvorila komponentno za povezanost. Tedaj je

$$|E(\Gamma)| = \frac{1}{2}(\sum_{v \in U} \deg(v) + 1) \geq \frac{1}{2}(|V(\Gamma)| \cdot 2 + 1) = |V(\Gamma)| + \frac{1}{2}.$$

Pri tem smo pri prvi neenakosti uporabili lemo o rokovanju. Sedaj pa iz trditve 7.1 sledi, da Γ ni drevo, kar je protislovje ∎

OPOMBA. Točki stopnje 1 rečemo tudi *list* grafa. Zgornja posledica torej pravi, da ima drevo vsaj dva lista. Če ima drevo natanko dva lista, potem se neenakost v dokazu zgornje trditve izide le, če ima vsaka druga točka stopno natanko 2. Ni se težko prepričati, da je povezan graf, ki ima dva lista, ostale točke pa imajo stopnjo 2, izomorfen poti.

7.1 Vpeta drevesa

Vpet podgraf grafa Γ, ki je drevo, se imenuje *vpeto drevo* grafa Γ.

TRDITEV 7.3 *Graf je povezan, če in samo če vsebuje vpeto drevo.*

DOKAZ: Če graf Γ vsebuje vpeto drevo, obstaja pot med poljubnima dvema točkama že v drevesu. Zato je Γ povezan. Naj bo sedaj Γ povezan graf. Če je Γ drevo, je trditev dokazana. Sicer obstaja povezava e, za katero je $\Gamma - e$ povezan. Odstranimo e iz Γ in postopek nadaljujemo, dokler ne dobimo (vpetega) drevesa. ∎

Povezan graf, ki ni drevo, ima več kot eno vpeto drevo. *Število vpetih dreves* v grafu Γ označimo s $\tau(\Gamma)$.

Pri računanju števila $\tau(\Gamma)$ je priročno razširiti naš horizont na družino multigrafov. Za povezavo e multigrafa Γ na $\Gamma - e$ označuje multigraf, ki ga dobimo iz Γ z odstranitvijo povezave e, Γ/e pa multigraf, ki ga dobimo iz Γ, če povezavo e *skrčimo*, tj. identificiramo njeni krajišči, zanko, ki nastane iz e ob tako nastali novi točki, pa odstranimo. Nasploh lahko v naslednjem izreku v multigrafih, ki nastopajo, brišemo vse zanke, ki se morebiti pojavijo.

TRDITEV 7.4 *Naj bo e poljubna povezana multigrafa Γ. Tedaj velja*

$$\tau(\Gamma) = \tau(\Gamma - e) + \tau(G/e).$$

DOKAZ: Vpetih dreves multigrafa Γ, ki povezave e ne vsebujejo, je natanko toliko kot vpetih dreves multigrafa $\Gamma - e$. Po drugi strani pa iz vpetega drevesa multigrafa Γ, ki vsebuje povezavo e, s skrčitvijo te povezave dobimo vpeto drevo multigrafa Γ/e. Ta postopek nam očitno da bijekcijo med vpetimi drevesi multigrafa Γ, ki vsebujejo povezavo e, z vpetimi drevesi multigrafa Γ/e. ∎

OPOMBA. Število vpetih dreves pa lahko izračunamo tudi s pomočjo linearne algebre, natančneje, s pomočjo Laplaceove matrike grafa.

DEFINICIJA 7.5 *Laplacova matrika $L(\Gamma)$* (multi)grafa Γ je kvadratna matrika, katere stoplci in vrstice so indeksirane s točkami grafa, v presečišču vrstice u in stoplca v leži negativno število povezav med u in v, diagonalni element točke v pa je enak stopnji točke v.

TRDITEV 7.6 *Število vpetih dreves (multi)grafa Γ je enako absolutni vrednosti determinante matrike, ki jo dobimo iz $L(\Gamma)$ tako, da odstanimo poljubno vrstico in poljuben stolpec.*

S pomočjo te trditve (in nekaj spretnosti pri računanju determinant) lahko dokažemo tako imenovano Cayleyjevo formulo za število vpetih dreves polnega grafa, ki pravi $\tau(K_n) = n^{n-2}$.

8 Eulerjevi in hamiltonovi grafi

OPOMBA. Ta razdelek v veliki meri sledi četrtemu poglavju knjige [3].

8.1 Eulerjevi grafi

Sprehod v grafu (ali multigrafu) je enostaven, če vsebuje vsako povezavo grafa največ enkrat. Enostaven sprehod, je *eulerjev*, če vsebuje vse povezave grafa (vsako natanko enkrat). Multigraf je *eulerjev*, če vsebuje eulerjev obhod, torej sklenjen sprehod, ki vsebuje vsako povezavo multigrafa natanko enkrat. Eulerjevih multigrafov ni težko prepoznati.

IZREK 8.1 *Multigraf* Γ *brez izoliranih točk je eulerjev, če in samo če je povezan in so vse njegove točke sode stopnje.*

DOKAZ: Naj bo Γ graf brez izoliranih točk. Denimo, da je Γ eulerjev. Tedaj je očitno povezan, saj vsaka točka leži na eulerjevem sprehodu. (Tu smo uporabili dejstvo, da Γ nima izoliranih točk.) Vsakič, ko eulerjev sprehod obišče kako točko, porabi dve povezavi – eno za vstop v točko, drugo za izhod iz nje. Ker eulerjev obhod pri vsaki točki porabi vse povezave, mora biti stopnja vsake točke soda.

Denimo sedaj, da je Γ povezan, vsaka njegova točka pa ima sodo stopnjo. Naj bo W najdaljši med enostavnimi obhodi v Γ in naj bo Γ' multigraf, ki ga dobimo iz Γ, če odstranimo vse povezave obhoda W. Če Γ ni eulerjev, potem Γ' premore kakšno povezavo. Po drugi strani ima vsaka točka multigrafa Γ' sodo stopnjo, saj smo stopnjo točke z odstranjevanjem povezavav iz W zmanjšali za sodo število. Še več, ker je Γ povezan, ima vsaj ena točka na sprehodu W v grafu Γ' stopnjo večjo ali enako 2. V takšni točki lahko torej začnemo sprehod v grafu Γ', ki ga nadaljujemo poljubno ter končamo šele, ko se vrnemo v začetno točko (ker ima v grafu Γ' vsaka točka sodo stopnjo, takšen sprehod resnično slej ko prej zopet vrne v začetno točko). Če ta novi sklenjeni sprehod vrinemo v sprehod W, dobimo sklenjeni sprehod v Γ, ki je daljši od W. To pa je protislovje. ■

8.2 Hamiltonovi grafi

Pot P v grafu Γ je *hamiltonova*, če velja $V(P) = V(\Gamma)$. Cikel C v grafu Γ je *hamiltonov*, če velja $V(C) = V(\Gamma)$. Hamiltonova pot in cikel sta torej vpeta pot oziroma vpet cikel. Graf je *hamiltonov*, če ima hamiltonov cikel.

Znan ni noben preprost, hitro preverljiv potreben in hkrati zadosten pogoj za hamiltonost grafa. Preprost potreben pogoj je podan v naslednji trditvi. Pri njej je uporabljena oznaka $\Omega(\Delta)$ za število povezanih komponent grafa Δ.

TRDITEV 8.2 *Naj bo $S \subset V(\Gamma)$ neprazna množica točk grafa Γ. Če je $\Omega(\Gamma - S) > |S|$, potem Γ nima hamiltonovega cikla.*

DOKAZ: Naj bodo $\Gamma_1, \ldots, \Gamma_k$ povezane komponente grafa $\Gamma - S$ in naj bo $C = v_0 v_2 \ldots v_{n-1} v_0$ hamiltonov cikel grafa Γ. Dokazati moramo, da je $|S| \geq k$. Brez škode za splošnost lahko privzamemo, da $v_{n-1} \in S$.

Za $i = 1, \ldots, k$ naj bo n_i največji indeks, za katerega je $v_{n_i} \in V(\Gamma_i)$. Točka v_{n_i} je torej zadnja točka na ciklu C, ki še leži v komponenti Γ_i. Naslednja točka, v_{i+1}, je element množice S. Točke $v_{n_1+1}, v_{n_2+1}, \ldots, v_{n_k+1}$ so torej (paroma različni) elementi množice S, in zato $|S| \geq k$. ∎

Zgornji potrebni pogoj za hamiltonost grafa žal ni tudi zadostni, kot kaže primer Petersenovega grafa. V Petersenovem grafu Pet za vsako neprazno množico $S \subseteq V(\text{Pet})$ velja $\Omega(\Gamma - S) \leq |S|$, vendar graf vseeno ni hamiltonov.

Dobrih zadostnih pogojev za hamiltonost grafa ni enostavno najti. Navedimo jih nekaj.

TRDITEV 8.3 *Naj bosta u in v takšni nesosednji točki grafa Γ, da velja $deg(u) + deg(v) \geq |V(\Gamma)|$. Če je graf $\Gamma + uv$ hamiltonov, potem je hamiltonov tudi graf Γ.*

DOKAZ: Naj bo $n = |V(\Gamma)|$. Denimo, da je graf $\Gamma + uv$ hamiltonov. Potem obstaja hamiltonova pot $uv_1v_2 \ldots v_{n-2}v$ v grafu Γ. Naj bo U množica indeksov sosed točke u ter V množica indeksov sosed točke v v grafu Γ. Če je za kak $i \in U$ velja $i - 1 \in V$, tedaj je $v_0 v_1 \ldots v_{i-1} v_{n-1} v_{n-2} \ldots v_i v_0$ hamiltonov cikel v grafu Γ. Predpostavimo torej lahko, da takšnega indeksa i ni. Z drugimi besedami, $V \subseteq \{0, 1, \ldots, n-2\} \setminus (U - 1)$, kjer smo z $U - 1$ označili množico $\{i - 1 : i \in U\}$. Od tod sledi neenakost $\deg(v) = |V| \leq n - 1 - |U| = n - 1 - \deg(u)$, kar je v prostislovju z našo predpostavko o vsoti stopenj točk u in v. ∎

Od tod z lahkoto izpeljemo naslednji posledici.

IZREK 8.4 (Ore). *Če za vsak par nesosednjih točk u, v grafa Γ velja $deg(u) + deg(v) \geq |V(\Gamma)|$, potem je graf Γ hamiltonov.*

IZREK 8.5 (Dirac). *Če ima graf* Γ *vsaj* 3 *točke in velja* $\delta(\Gamma) \geq \frac{|V(\Gamma)|}{2}$, *potem je graf* G *hamiltonov.*

9 Ravninski grafi in Eulerjeva formula

Kot smo že omenili v uvodu, grafe radi rišemo v ravnini tako, da vozlišče grafa predstavimo kot točko ravnine, povezo med vozliščema pa kot ravno (ali pa tudi krivo) črto s krajišči v točkah, ki ustrezata krajiščema povezave. Pri tem pazimo, da povezava (oziroma, natančneje, črta, ki ponazarja povezavo) ne seka same sebe in ne poteka skozi nobeno drugo vozlišče kot le svoje krajišče. Seveda ima lahko dani graf več različnih risb.

Če obstaja risba grafa, pri kateri se nobeni dve povezavi med seboj ne sekata (razen morda v svojih krajiščih), rečemo, da je graf *ravninski*, takšni risbi pa *ravniska risba grafa*. Tako so, na primer, ravninski vsi cikli C_n, vse poti P_n, vsa drevesa, pa tudi polni grafi K_3 in K_4 ter polni dvodelni grafa $K_{2,n}$, $n \in \mathbb{N}$. Kasneje pa bomo videli, da polni grafi K_n za $n \geq 5$ in polni dvodelni grafi $K_{m,n}$ za $m, n \geq 3$ niso ravninski.

Opomba. Formalno definicijo risbe in ravninskosti grafa lahko opišemo takole: *Vložitev* multigrafa Γ v metrični prostor Σ je določena z injektivno preslikavo $\varphi\colon V(\Gamma) \to \Sigma$, ki vsaki točki multigrafa priredi točko prostora Σ, in tako družino zveznih preslikav $\varphi_e\colon [0,1] \to \Sigma$ (tu smo povezavo e predstavili z zaprtim intervalom $[0,1]$), da velja: $\varphi_e(0)$ je slika enega, $\varphi_e(1)$ pa slika drugega krajišča povezave e, $\varphi_e|_{(0,1)}$ je injektivna in njena slika ne vsebuje nobene točke, ki bi bila slika točke grafa ali pa del slike kake druge povezave grafa. Graf, ki premore vložitev v ravnino, se imenuje *ravninski graf*.

Dokazati, da je neki graf ravninski, je načeloma enostavno – najti moramo njegovo ravninsko risbo. Precej težje pa je dokazati, da graf ni ravninski, saj bi morali pregledati vse možne njegove risbe in preveriti, da nobena ni ravninska. Ker je to seveda nemogoče, je za dokazovanje neravninskosti grafov potrebno razviti kakšne drugačne prijeme. Eden takšnih je *Eulerjeva formula*.

9.1 Eulerjeva formula

Zamislimo si ravninsko risbo ravninskega grafa Γ. Če iz ravnine izrežemo vse črte in točke, ki predstavljajo povezave in vozlišča grafa, dobimo nekaj med seboj ločenih povezanih območij, ki jih imenujemo *lica*. Eno od teh območij je neomejeno in obdaja celotno risbo grafa, ostala območja pa so omejena. Množico vsej lic tako narisanega grafa Γ označimo z $F(\Gamma)$.

Na prvi pogled ni videti nobenega razloga, zakaj bi število lic grafa ne bilo odvisno od konkretne ravniske risbe le-tega. Zato je toliko presenetljivejša

naslednja trditev, iz katere med drugim sledi, da je število lic ravninskega grafa neodvisno od konkretne ravninske risbe.

IZREK 9.1 (Eulerjeva formula) *Naj bo* Γ *ravninski graf z množico vozlišč* V *in množico povezav* E. *Naj bo* F *množica lic kake ravninske slike grafa* Γ *in* Ω *množica komponent za povezanost grafa* Γ. *Tedaj velja naslednja enakost:*

$$|V| - |E| + |F| = 1 + |\Omega|.$$

Zgornji izrek navadno dokazujemo z indukcijo na število povezav grafa. Pri tem si pomagamo tudi s formulo o številu povezav v drevesu z n točkami. Podrobnosti dokaza bomo izpustili. Namesto tega raje izpeljimo naslednjo pomembno posledico Eulerjeve formule.

TRDITEV 9.2 *Naj bo* Γ *povezan ravninski graf z vsaj tremi točkami. Tedaj je*

$$|E(\Gamma)| \leq 3|V(\Gamma)| - 6.$$

DOKAZ: Izberimo kako ravninsko sliko grafa Γ in z F označimo množico pripadajočih lic, z $\vec{E}$ pa množico vseh usmerjenih povezav grafa Γ (tj. množico vseh parov (u, v), $u, v \in V(\Gamma)$, za katere je $u \sim v$).

Če rob lica prehodimo v smeri urinega kazalca, dobimo sklenjen sprehod v grafu, ki ga bomo imenovali kar *usmerjeni rob lica*. Za razliko od omejenih lic se domenimo, da je usmerjeni rob neomejenega lica obhod, ki ga dobimo, če robne povezave zunanjega lica prehodimo v smeri, ki je nasprotna urinemu kazalcu. Opazimo, da vsaka usmerjena povezava leži na natanko enem robu lica (namreč na robu tistega lica, ki leži desno od nje, če gledamo v smeri usmeritve povezave). Hkrati pa vsak rob lica vsebuje vsako usmerjeno povezavo največ enkrat.

Število usmerjenih povezav, ki jih vsebuje rob lica $f \in F$, označimo z $\deg(f)$. Enostaven premislek pokaže, da iz $\deg(f) \leq 2$ sledi, da je graf Γ izomorfen K_1 ali K_2, kar pa je v protislovju s predpostavko, da je $|V(\Gamma)| \geq 3$. Zato je $\deg(f) \geq 3$ za vsak $f \in F$.

Oglejmo si množico parov $\mathcal{M} = \{(e, f) : e \in \vec{E}, f \in F, e \text{ leži na robu } f\}$. Elemente množice $\mathcal{M}$ preštejmo na dva načina:

$$|\mathcal{M}| = \sum_{e \in \vec{E}} 1 = |\vec{E}| = 2|E|.$$

Po drugi strani:

$$|\mathcal{M}| = \sum_{f \in F} \deg(f) \geq \sum_{f \in F} 3 = 3|F|.$$

Od tod sledi $|F| \leq \frac{2}{3}|E|$. Vstavimo to v enakost $|F| = 2 - |V| + |E|$, ki sledi iz Eulerjeve fornule. Dobimo $2 - |V| + |E| \leq \frac{2}{3}|E|$, od koder dobimo $\frac{1}{3}|E| \leq |V| - 2$. To neenakost še pomnožimo s 3 in dobimo, kar smo trdili. ∎

Podobno kot zgornjo trditev lahko dokažemo tudi naslednje.

TRDITEV 9.3 *Naj bo* Γ *povezan ravninski graf z vsaj štirimi točkami. Če* Γ *ne vsebuje cikla dolžine* 3*, tedaj je*

$$|E(\Gamma)| \leq 2|V(\Gamma)| - 4.$$

Iz zgornjih dveh rezultatov neposredno sledi naslednje.

TRDITEV 9.4 *Grafa* K_5 *in* $K_{3,3}$ *nista ravninska.*

DOKAZ: Graf K_5 ima 5 vozlišč in 10 povezav. Če bi bil ravninski, bi veljalo $10 \leq 3 \cdot 5 - 6$, kar pa očitno ni res. Zato graf K_5 ni ravninski. Podobno, graf $K_{3,3}$ ima 6 vozlišč in 9 povezav ter ne vsebuje ciklov dolžine 3. Če bi bil ravninski, bi veljalo $9 \leq 2 \cdot 6 - 4$. Ker to ni res, graf $K_{3,3}$ ni ravninski.

9.2 Izreka Wagnerja in Kuratowskega

V tem razdelku si bomo ogledali nekaj operacij na grafih, ki ohranjajo lastnost "biti ravninski". Prva od takih operacij je operacija "podgraf". Očitno namreč velja naslednje:

TRDITEV 9.5 *Če je graf* Γ *ravninski, tedaj je ravniski tudi vsak njegov podgraf* Γ'*.*

Naslednja operacija, ki ohranja ravninskost, je operacija *subdivizije*, ki jo bomo sedaj opisali. Naj bo $e = u_0v_0$ poljubna povezava grafa Γ. Z Γ' označimo graf, ki ga dobimo iz Γ tako, da na sredi povezave e dodamo novo točko (stopnje 2). (Formalno bi lahko Γ' definirali kot graf z množico točk $V(\Gamma) \cup \{e\}$, kjer sta dve točki $u, v \in V(\Gamma)$, $uv \neq e$, sosednji v Γ', če sta bili sosednji v Γ, "nova točka" e je sosednja svojima krajiščema u_0 in v_0 v grafu Γ, točki u_0 in v_0 pa v grafu Γ' nista sosednji.) Grafu Γ' tedaj rečemo *graf, dobljen iz* Γ *s subdivizijo povezave* e. Vsakemu grafu, ki ga dobimo iz Γ z zaporednim subdividiranjem povezav, rečemo *subdivizija grafa* Γ. Ni se težko prepričati, da velja naslednje.

TRDITEV 9.6 *Naj bo Γ' poljubna subdivizija grafa Γ. Tedaj je Γ ravninski, če in samo če je ravninski Γ'.*

Če združimo zgornji dve trditvi s Trdtivijo 9.4, ugotovimo, da Γ, ki vsebuje kak podgraf Γ', ki je subdivizija grafa K_5 ali pa grafa $K_{3,3}$, ni ravninski. Presenetljivo pa je, da je ta potrebni pogoj za ravninskost hkrati tudi zadostni. Velja namreč naslednji globok in netrivialen izrek, ki nosi ime poljskega matematika Kazimierza Kuratowskega.

IZREK 9.7 *(Kuratowski) Graf Γ je ravninski, če in samo če noben od njegovih podgrafov ni subdivizija niti grafa K_5 niti grafa $K_{3,3}$.*

Za konec definirajmo še tretjo operacijo, ki ohranja ravninskost. Naj bo Γ' graf, dobljen iz kakega podgrafa grafa Γ z odstranjevanjem in krčenjem povezav (na vsakem koraku lahko odstranimo dobljene zanke, vzporedne povezave pa združimo v eno samo povezavo – tako ves čas ostajamo v razredu enostavnih grafov). Tedaj grafu Γ' rečemo *minor* grafa Γ. Ni se težko prepričati, da velja naslednje.

TRDITEV 9.8 *Če je graf Γ ravninski, tedaj je ravninski tudi vsak njegov minor Γ'.*

S pomočjo Trditve 9.4 lahko zato sklenemo, da graf, ki premore kak minor, izomorfen grafu K_5 ali grafu $K_{3,3}$, ni ravninski. Podobno kot v primeru subdivizij, pa velja ta implikacija tudi v obratni smeri. Karakterizaciji ravninskih grafov, ki jo tako dobimo, rečemo *Wagnerjev izrek*.

IZREK 9.9 *(Wagner) Graf Γ je ravninski, če in samo če ne premore minorja, izomorfnega K_5 ali $K_{3,3}$.*

10 Barvanja grafov

Opomba. Ta razdelek v veliki meri sledi sedmemu poglavju knjige [3].

Preslikavi $c\colon V(\Gamma) \to \{1, 2, \ldots, k\}$ pravimo *k-barvanje* točk grafa Γ. Barvanje točk c je *dobro* (tudi *pravilno*), če so sosednje točke obarvane z različnimi barvami, tj. $u \sim v \Rightarrow c(u) \neq c(v)$. Najmanjše število k, za katero obstaja dobro k-barvanje točk grafa Γ, imenujemo *kromatično število* (tudi *barvnost*) grafa G; oznaka $\chi(\Gamma)$.

Podobno preslikavi $c'\colon E(\Gamma) \to \{1, 2, \ldots, k\}$ pravimo *k-barvanje povezav* multigrafa brez zank Γ. Barvanje povezav c' je *dobro* (tudi *pravilno*), če so povezave, ki imajo kako skupno krajišče, obarvane z različnimi barvami. Najmanjše število k, za katero obstaja dobro k-barvanje povezav multigrafa brez zank Γ, imenujemo *kromatični indeks* multigrafa Γ; oznaka $\chi'(G)$.

10.1 Barvanje točk

Če je $\Gamma' \subseteq \Gamma$, potem je $\chi(\Gamma') \leq \chi(\Gamma)$. Naj bo $\omega(\Gamma)$ velikost največjega polnega podgrafa grafa Γ (velikost *maksimalne klike*) in $\Delta(\Gamma)$ maksimalna stopnja kakega vozlišča v Γ. Tedaj velja $\omega(\Gamma) \leq \chi(\Gamma) \leq \Delta(\Gamma) + 1$. Spodnja meja je očitna, saj za pravilno barvanje točk polnega grafa na n točkah potrebujemo n barv, zgornjo mejo pa z lahkoto dokažemo, če poskusimo točke pobarvati kar po požrešni metodi.

Nekoliko težje pa je dokazati, da je ta zgornja meja dosežena le pri lihih ciklih in polnih grafih. Prav to pravi Brooksov izrek.

Izrek 10.1 (Brooks). *Naj bo Γ povezan graf. Če Γ ni lih cikel in ni poln graf, potem je $\chi(\Gamma) \leq \Delta(\Gamma)$.*

Določanje kromatičnega števila konkretnega grafa je običajno sestavljeno iz dveh delov: iskanja spodnje meje (pri preprostih nalogah najdemo podgraf, za katerega poznamo kromatično število, npr. $\chi(K_n) = n$, $\chi(C_n) = 2$ za sode n in 3 za lihe n, $\chi(\Gamma) \leq 2$ natanko tedaj, ko je Γ dvodelen graf, itn.) in konstrukcije barvanja, ki dokaže, da je spodnjo mejo res moč doseči (večkrat si lahko pomagamo tudi z Brooksovim izrekom).

Včasih si delo lahko poenostavimo z naslednjim znamenitim izrekom:

Izrek 10.2 (Izrek štirih barv). *Za vsak ravninski graf Γ je $\chi(\Gamma) \leq 4$.*

ZGLED. *Poišči kromatično število Petersenovega grafa Pet.*

Ker Pet vsebuje cikel dolžine 5, je $\chi(\text{Pet}) \geq \chi(C_5) = 3$. Ker je Pet kubičen graf, iz Brooksovega izreka dobimo $\chi(\text{Pet}) \leq 3$. Torej $\chi(\text{Pet}) = 3$. ∎

10.2 Barvanje povezav

Tudi za barvanja povezav velja, da iz $\Gamma' \subseteq \Gamma$ sledi $\chi'(\Gamma) \leq \chi'(\Gamma)$. Najpomembnejši izrek o barvanju povezav grafov je:

IZREK 10.3 (Vizing). *Za vsak graf G velja $\Delta(\Gamma) \leq \chi'(\Gamma) \leq \Delta(\Gamma) + 1$.*

Graf Γ je *razreda* 1, če je $\chi'(\Gamma) = \Delta(\Gamma)$, sicer je *razreda* 2. Če je n sod, sta grafa C_n in K_n razreda 1, za lihe n-je pa sta razreda 2. Pomembna družina grafov razreda 1 so dvodelni grafi. Natančneje:

IZREK 10.4 (König). *Za dvodelni multigraf Γ velja $\chi'(\Gamma) = \Delta(\Gamma)$.*

Za multigrafe je kromatični indeks lahko večji od maksimalne stopnje točk plus ena.

IZREK 10.5 (Vizing; Shannon). *Naj bo Γ multigraf brez zank, v katerem ne obstaja več kot μ paroma vzporednih povezav (za grafe vzamemo $\mu = 1$). Potem je $\Delta(\Gamma) \leq \chi'(\Gamma) \leq \min\{\Delta(\Gamma) + \mu, \frac{3}{2}\Delta(\Gamma)\}$.*

Algebra in teorija števil

11 Algebrske strukture

Pod pojmom *algebrska struktura* v matematiki navadno razumemo poljubno množico skupaj z eno ali več operacijami na njej. Nekate algebrske strukture, pri katerih operacije zadoščajo kakim dodatnim tipičnim lastnostim, poimenujemo s posebnimi imeni, kot so *polgrupa*, *grupa*, *kolobar*, *obseg*, *vektorski prostor* itd. V tem poglavjuu si bomo na hitro ogledali nekatere od teh algebrskih struktur.

11.1 Operacije

Naj bo M poljubna množica. *Operacija na množici* M je poljubno pravilo, ki (urejenemu) paru elementov $a, b \in M$ priredi tretji element iz M. Če operacijo označimo s $\circ$, tedaj element, ki ga ta operacija priredi paru $a, b \in M$, označimo z

$$a \circ b.$$

Med dobro znane zglede operacij sodijo množenje na množici naravnih (ali pa racionalnih, realnih, kompleksnih) števil, odštevanje na množici celih (racionalnih, realnih, kompleksnih) števil, deljenje na množici neničelnih kompleknih (realnih, racionalnih) števil, matrično množenje na množici kvadratnih matrik fiksne velikosti ipd.

Če je $\circ$ poljubna operacija na množici M, podmnožica $N \subseteq M$ pa takšna, da je za vsak par elementov $a, b \in N$ tudi $a \circ b$ element množice N, pravimo, da je N *zaprta za operacijo* $\circ$. V tem primeru lahko operacijo $\circ$ razumemo tudi kot operacijo na množici N.

Vpeljimo sedaj dve lastnosti operacij.

Definicija 11.1 Naj bo $\circ$ poljubna operacija na množici M. Če za vsako

trojico elementov $a, b, c \in M$ velja

$$(a \circ b) \circ c = a \circ (b \circ c),$$

tedaj rečemo, da je operacija *asociativna*.

Večina operacij, ki smo jih spoznali v osnovni in srednji šoli, je asociativnih. Tako sta, na primer, asociativni operaciji seštevanja in množenja na množici kompleksnih števil (in posledično na vsaki podmnožici kompleksnih števil, zaprti za ti dve operaciji). Pač pa ni asociativna operacija odštevanja, saj število $(a - b) - c$ ni (nujno) enako številu $a - (b - c)$. Podobno ni asociativno niti deljenje na množici neničelnih racionalnih števil. Pri asociativnih operacijah lahko pri večkratni uporabi te operacije oklepaje v zapisu izpuščamo, saj je končni rezultat odvisen le od vrstnega reda elementov, ki jih združujemo, nič pa od tega, kako jih združujemo med seboj. Tako, na primer, namesto

$$\big(a \circ (b \circ c)\big) \circ d \qquad (*)$$

pišemo kar

$$a \circ b \circ c \circ d, \qquad (+)$$

saj je rezultat izraza $(*)$ enak rezultatu, ki ga dobimo, če v $(+)$ vstavimo oklepaje na kakršen koli način.

DEFINICIJA 11.2 Naj bo $\circ$ poljubna operacija na množici M. Če za vsak par elementov $a, b \in M$ velja

$$a \circ b = b \circ a,$$

tedaj rečemo, da je operacija *komutativna*.

Med komutativne operacije sodijo množenje in seštevanje na množici kompleksnih številih, ne pa tudi odštevanje in deljenje. Tudi množenje matrik, kot vemo, ni komutativna operacija.

Včasih se primeri, da v množici M obstaja element, denimo e, za katerega pri vsakem $a \in M$ velja pravilo

$$a \circ e = e \circ a = a.$$

Takšnemu elementu pravimo *nedelavni element* ali tudi *enota za operacijo* $\circ$. Hitro se prepričamo v naslednje:

LEMA 11.3 *V množici M, na kateri je definirana operacija $\circ$, obstaja največ ena enota za operacijo $\circ$.*

DOKAZ: Naj bosta $e, e' \in M$ poljubni enoti za $\circ$. Oglejmo si element $e \circ e'$. Ker je e enota, je ta element enak e'. Ker pa je tudi e' enota, je hkrati enak tudi e. Zato $e = e'$. ∎

Naj bo sedaj $\circ$ operacija na množici M, za katero obstaja enota e, in naj bo a poljuben element množice M. Če v množici M najdemo element b, za katerega velja

$$a \circ b = b \circ a = e,$$

tedaj pravimo, da je element a *obrnljiv* in da je b *inverzni element* elementa a glede na operacijo $\circ$. Če je iz konteksta razvidno, katero operacijo imamo v mislih, tedaj takšen element b označimo tudi z a^{-1}, v posebnem primeru, ko operacijo $\circ$ označujemo z znakom $+$ ali pa $\oplus$, pa tudi z $-a$. Element množice M, ki premore inverz za operacijo $\circ$, je *obrnljiv glede na operacijo* $\circ$.

LEMA 11.4 *Naj bo $\circ$ asociativna operacija na množici M. Tedaj za dani element a obstaja največ en inverzni element.*

DOKAZ: Naj bosta b in c dva inverzna elementa elementa a. Označimo enoto z e. Tedaj je $a \circ b = e = a \circ c$. Pomnožimo levo in desno stran enakosti z b, da dobimo $b \circ (a \circ b) = b \circ (a \circ c)$. Če upoštevamo asociativnost operacije $\circ$ in dejstvo, da je $b \circ a = e$, dobimo $e \circ b = e \circ c$, in zato $b = c$. ∎

Naslednja lema med drugim pove, da je množica obrnljivih elementov zaprta za operacijo.

LEMA 11.5 *Naj bosta a in b obrnljiva elementa množice M z asociativno operacijo $\circ$. Tedaj je tudi $a \circ b$ obrnljiv element in $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.*

DOKAZ: Preveriti moramo, da je

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = e = (b^{-1} \circ a^{-1}) \circ (a \circ b).$$

V to pa se zlahka prepričamo, če upoštevamo asociativnost operacije in definicijo inverza ter enote. ∎

11.2 Algebrske strukture z eno operacijo

Polgrupa

DEFINICIJA 11.6 Množici M skupaj z asociativno operacijo $\circ$ rečemo *polgrupa*. Če v množici M obstaja tudi enota za operacijo $\circ$, polgrupi M rečemo *monoid* ali *polgrupa z enoto*. Če je operacija $\circ$ komutativna, govorimo o *komutativni polgrupi*.

Preprost zgled polgrupe je množica naravnih števil $\mathbb{N} = \{1, 2, 3, \ldots\}$ skupaj z operacijo seštevanja. Če množici dodamo še element 0, dobimo monoid. V tem monoidu je edini obrnljiv element ravno enota 0.

Nadalje, množica $\mathbb{Z}$ vseh celih števil tvori skupaj z operacijo množenja monoid. Enota v tem monoidu je element 1, obrnljiva elementa pa sta 1 in -1.

Vsi zgornji zgledi polgrup so komutativni. Za zgled nekomutativnega monoida lahko vzamemo množico vseh 2×2 matrik z realnimi koeficienti skupaj z operacijo običajnega matričnega množenja. Obrnljivi elementi v tem monoidu so natanko matrike z neničelno determinanto.

Grupa

DEFINICIJA 11.7 Monoidu M z operacijo $\circ$, v katerem je vsak element obrnljiv glede na $\circ$, rečemo *grupa*. Če je operacija $\circ$ komutativna, govorimo o *abelovi grupi*.

Najosnovnejši vir grup predstavljajo množice obrnljivih elementov v monoidu. Velja namreč naslednje.

LEMA 11.8 *Naj bo M monoid z operacijo $\circ$. Tedaj je množica M^* vseh obrnljivih elementov monoida zaprta za operacijo $\circ$ in tvori skupaj s to operacijo grupo.*

Nadaljni viri grup so množica celih števil z operacijo seštevanja, množica neničelnih kompleksnih števil z operacijo množenja in množica obrnljivih $n \times n$ matrik z operacijo matričnega množenja.

Posebej pomemben zgled grupe tvori množica permutacij dane množice Ω (bijektivnih preslikav iz Ω v Ω) skupaj z operacijo kompozita.

11.3 Algebrske strukture z dvema operacijama

Kolobar

Algebrske strukture iz prejšnjih razdelkov so premogle eno samo operacijo. Struktura, ki jo bomo obravnavali v tem razdelku, pa bo premogla dve operaciji, ki jih običajno imenujemo *množenje* in *seštevanje* in označujemo bodisi s pikico "$\cdot$" in plusom "+" bodisi s simboloma $\odot$ in $\oplus$. Ti dve operaciji bosta zadoščali tako imenovanemu *distributivnostnemu zakonu*, ki ga bomo sedaj definirali.

DEFINICIJA 11.9 Naj bosta $\oplus$ in $\odot$ dve operaciji na množici M. Če za vsako trojico $a, b, c \in M$ velja

$$(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c) \text{ in } c \odot (a \oplus b) = (c \odot a) \oplus (c \odot b),$$

potem rečemo, da je operacija $\odot$ distributivna proti operaciji $\oplus$.

Tako je, na primer, običajno množenje števil (kompleksnih, realnih, racionalnih itd.) distributivno proti običajnemu seštevanju. Podobno je običajno matrično množenje kvadratnih matrik distributivno proti seštevanju matrik po komponentah. Zelo zanimiv zgled pa tvorita operaciji preseka ($\cap$) in unije ($\cup$) množic. Vsaka od teh dveh operacij je namreč distributivna proti drugi.

Oboroženi z definicijo distributivnosti lahko definiramo tudi pojem *kolobarja*.

DEFINICIJA 11.10 Množci M skupaj z operacijama *seštevanja* $\oplus$ in *množenja* $\odot$ rečemo *kolobar*, če velja naslednje:

(i) Množica M skupaj z operacijo $\oplus$ tvori abelovo grupo;

(ii) Množica M skupaj z operacijo $\odot$ tvori polgrupo;

(iii) Operacija $\odot$ je distributivna proti operaciji $\oplus$.

Če je operacija $\odot$ komutativna, govorimo o komutativnem kolobarju, če pa obstaja enota za operacijo $\odot$, pa govorimo o *kolobarju z enoto*. Množico elementov kolobarja M, ki so obrnljivi glede na operacijo množenja, označimo z M^*.

Iz definicije kolobarja sledi, da kolobar vedno premore enoto za operacijo $\oplus$, ki jo navadno označimo z 0. Če premore tudi enoto za operacijo $\odot$, jo označimo z 1.

Zgledi kolobarjev so, na primer, številske množice $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ in $\mathbb{C}$ skupaj z običajnima operacijama seštevanja in množenja. Vsi ti kolobarji so komutativni in imajo enoto. Za zgled nekomutativnega kolobarja lahko vzamemo množico vseh $n \times n$ matrik s kompleksnimi (ali realnimi) koeficienti, skupaj z običajnima operacijama seštevanja in množenja matrik.

TRDITEV 11.11 *Za poljuben element a poljubnega kolobarja M velja enakost*

$$a \cdot 0 = 0 \cdot a = 0.$$

DOKAZ: Z upoštevanjem definicije ničle in distributivnosti množenja proti seštevanju dobimo enakost

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a.$$

Če prištejemo na levi in desni inverz elementa $0 \cdot a$ glede na seštevanje (takšen inverz navadno označimo z $-0 \cdot a$) in upoštevamo definicijo inverza, dobimo enakost $0 = 0 \cdot a$. Analogno dokažemo tudi enakost $a \cdot 0 = 0$. ■

Obseg

DEFINICIJA 11.12 Kolobarju z enoto in vsaj dvema elementoma, v katerem je vsak neničelni element obrnljiv glede na operacijo množenja, pravimo *obseg*. Obseg, v katerem je operacija množenja komutativna, je *polje*.

Na primer, množica kompleksnih (realni ali racionalnih) števil, skupaj z običajnima operacijama množenje in seštevanja je polje.

12 Teorija števil

Teorija števil se ukvarja s *celimi števili*. Množico celih števil zapišemo kot

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$$

in jo razdelimo na množico naravnih števil

$$\mathbb{N} = \{1, 2, 3, \ldots, \},$$

množico negativnih celih števil

$$\mathbb{N}^- = \{-1, -2, -3, \ldots\}$$

in množico, ki vsebuje le število 0.

12.1 Delitelji in večkratniki

Med najosnovnejše pojme teorije števil sodi pojem deljivosti.

Definicija 12.1 Celo število m deli celo število n, če in samo če obstaja takšno celo število k, da je $n = km$. V tem primeru pišemo $m \mid n$ in rečemo, da je m delitelj števila n, da je n deljiv s številom m in da je n večkratnik števila m.

Opazimo, da je 0 večkratnik vsakega celega števila (saj je $0 = 0 \cdot m$ za vsak $m \in \mathbb{Z}$) in da je edino število, ki ga 0 deli, število 0 (saj je $k \cdot 0 = 0$ za vsak $k \in \mathbb{Z}$). Po drugi stran pa števili 1 in -1 delita prav vsa cela števila (saj je $n = n \cdot 1$ in $n = (-n) \cdot (-1)$ za vsak $n \in \mathbb{Z}$) in poleg števil 1 in -1 nimata prav nobenih drugih deliteljev.

Naj bosta m in n poljubni števili. Tedaj največje naravno število, ki deli tako m kot n označimo z $\gcd(m, n)$ in ga imenujemo *največji skupni delitelj* števil m in n. (Oznaka gcd izvira iz angleškega poimenovanja *greatest common divisor*). Najmanjše naravno število, ki je deljivo tako z m kot z n, pa imenujemo *najmanjši skupni večkratnik* števil m in n in ga označimo z $\mathrm{lcm}(m, n)$ (angl. *least common multiple*). Celi števili m in n sta *tuji*, če velja $\gcd(m, n) = 1$.

Omenimo še, da je relacija deljivosti tranzitivna relacije. Natančneje, velja naslednje:

Trditev 12.2 *Če $r \mid m$ in $m \mid n$, tedaj $r \mid n$.*

Dokaz: Iz definicije deljivosti sledi, da obstajata celi števili k in ℓ, za kateri je $m = kr$ in $n = \ell m$. Tedaj pa je $n = \ell kr$, od koder sledi, da je n deljiv z r. ∎

Funkciji div in mod

Naj bo n poljubno celo število in m poljubno neničelno celo število. Kot smo že opazili, kvocient n/m tedaj ni nujno celo število, kar pomeni, da v množici celih števil običajna operacija deljenje ni dobro definirana. Namesto običajnega deljenja zato vpeljemo operacijo celoštevilskega deljenja, ki številoma n in m priredi *celoštevilski količnik* $k = n \operatorname{div} m$ ter *ostanek* $r = n \bmod m$. Celoštevilski količnik k in ostanek r sta natanko določena s pogojem:

$$n = km + r; \quad k, r \in \mathbb{Z},\ 0 \leq r \leq |m| - 1.$$

12.2 Praštevila

DEFINICIJA 12.3 Od 1 različno naravno število je praštevilo, če poleg samega sebe in 1 ne premore nobenega drugega naravnega delitelja.

TRDITEV 12.4 *Vsako od* 1 *različno naravno število je deljivo z vsaj enim praštevilom.*

DOKAZ: Dokaz bo potekal z indukcijo na naravno število n. Za $n = 1$ trditev ne trdi ničesar, za $n = 2$ pa je pravilna, saj je 2 res deljiv s praštevilom, namreč kar z 2. Privzemimo torej, da je $n \geq 3$ in da je vsako naravno število, ki je manjše od n, deljivo s kakim praštevilom. Dokazati moramo, da tedaj isto velja tudi za število n.

Če je n praštevilo, tedaj je deljivo s praštevilom n. Če n ni praštevilo, tedaj je deljivo s kakim naravnim številom m, $2 \leq m \leq n-1$. Po indukcijski predpostavki je m deljiv z nekim praštevilom p. Tedaj pa iz Trditve 12.2 sledi, da p deli n. ∎

TRDITEV 12.5 *Praštevil je neskončno mnogo.*

DOKAZ: Pa recimo, da jih je le končno mnogo; označimo jih s p_1, $p_2, \ldots, p_n$. Oglejmo si število $m = p_1 p_2 \ldots p_m + 1$. Očitno je m večji od vsakega od praštevil p_i, zato ni praštevilo. Iz Trditve 12.4 tedaj sledi, da je p deljiv s kakim praštevilom; denimo s p_i. Tedaj je

$$m = p_1 \ldots p_{i-1} p_i p_{i+1} \ldots p_m + 1 = kp_i$$

za kak $k \in \mathbb{Z}$, in zato $1 = p_i(k - p_1 \ldots p_{i-1} p_{i+1} \ldots p_m)$. To pa je nemogoče, saj 1 ni deljiv z nobenim praštevilom, torej tudi ne s p_i. ∎

DEFINICIJA 12.6 Naj bodo $p_1, p_2, \ldots, p_k$ poljubna, paroma različna praštevila in $\alpha_1, \ldots, \alpha_k$ poljubna naravna števila. Tedaj zapisu

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

pravimo razcep števila n na prafaktorje.

TRDITEV 12.7 *Vsako od* 1 *različno naravno število premore razcep na prafaktorje. Razcep je do vrstnega reda faktorjev en sam.*

Včasih je priročno v razcep naravnega števila n vrini še kako praštevilo, s katerim n ni deljiv; tako praštevilo mora seveda v razcepu nastopati z eksponentom 0. Na ta način omogočimo, da poljubni dve naravni števili $a, b \in \mathbb{N}$ zapišemo z naborom istih praštevil: $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, $\alpha_i, \beta_i \geq 0$. S pomočjo razcepa na prafaktorje lahko dokažemo več zanimivih trditev:

TRDITEV 12.8 *Naravno število m deli naravno število n, če in samo če za njuna razcepa na prafaktorje velja naslednje:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},\ m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},\ b_i \leq a_i \text{ za vsak } i \in \{1, \ldots, k\}.$$

TRDITEV 12.9 *Naj bodo a, b in c poljubna cela števila. Če sta a in b tuji števili in če a deli bc, tedaj a deli c.*

TRDITEV 12.10 *Naj bosta a in b poljubni celi števili in c njun skupni delitelj. Tedaj je* $\gcd(\frac{a}{c}, \frac{b}{c}) = \frac{\gcd(a,b)}{c}$.

Iz zgornje trditeve neposredno sledi, da sta za poljubni celi števili a in b števili $\frac{a}{\gcd(a,b)}$ in $\frac{b}{\gcd(a,b)}$ tuji.

Računanje gcd in lcm s pomočjo razcepa na prafaktorje

Vzemimo naravni števili m in n. Če je katero od njih enako 1 (denimo $n = 1$), potem je očitno

$$\gcd(m, 1) = 1 \quad \text{in} \quad \operatorname{lcm}(m, 1) = m.$$

Predpostavimo sedaj, da je $m, n \geq 2$. Naj bodo $p_1, \ldots, p_n$ tista praštevila, ki delijo tako m kot n. Tedaj imata razcepa števili m in n na prafaktorje obliko

$$\begin{aligned} m &= p_1^{\alpha_1} \cdots p_n^{\alpha_n} \cdot q_1^{\delta_1} \cdots q_k^{\delta_k}, \\ n &= p_1^{\beta_1} \cdots p_n^{\beta_n} \cdot r_1^{\gamma_1} \cdots r_\ell^{\gamma_\ell}, \end{aligned}$$

pri čemer je $q_i \neq r_j$ za vsak par indeksov i, j. V tem primeru velja:

$$\begin{aligned} \gcd(m,n) &= p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_n^{\min\{\alpha_n,\beta_n\}} \\ \operatorname{lcm}(m,n) &= p_1^{\max\{\alpha_1,\beta_1\}} \cdots p_n^{\max\{\alpha_n,\beta_n\}} \cdot q_1^{\delta_1} \cdots q_k^{\delta_k} \cdot r_1^{\gamma_1} \cdots r_\ell^{\gamma_\ell} \end{aligned}$$

Od tod neposredno sledi naslednje:

TRDITEV 12.11 *Za poljubni naravni števili m in n velja enakost*

$$\gcd(m,n) \cdot \operatorname{lcm}(m,n) = mn.$$

12.3 Diofantske enačbe

Enačbe, pri katerih iščemo zgolj celoštevilske rešitve, se imenujejo *diofantske enačbe*. Oglejmo si nekoliko podrobneje linearne diofantske enačbe, torej enačbe oblike

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c, \qquad (*)$$

kjer so a_i, $i = 1, \ldots, n$, in c poljubna cela števila, x_i, $i = 1, \ldots, n$, pa neznanke. Rešitev enačbe $(*)$ je vsaka n-terica $(x_1, \ldots, x_n)$ celih števil, ki zadošča $(*)$.

Oglejmo si najprej primer, ko imamo eno samo neznanko:

$$ax = c, \;\; a \neq 0. \qquad (+)$$

Če bi dopuščali tudi racionalne rešitve, bi zgornja enačba imela natanko eno rešitev, namreč $x = c/a$. Ker pa nas pri diofantskih enačbah zanimajo le celoštevilske rešitve, bo imela diofantska enačba $(+)$ rešitev tedaj in le tedaj, ko bo a delil c (in bo zato c/a celo število).

Nekoliko bolj zanimiva je linearna diofantska enačba z dvema neznankama:

$$ax + by = c, \;\; a, b \neq 0. \qquad (\times).$$

Premislimo najprej, kako je z racionalnimi rešitvami. Ker je $a \neq 0$, lahko zgornjo enakost preoblikujemo v $x = (c - by)/a$. To pomeni, da lahko za poljuben y najdemo ustrezen x, tako da bo par (x, y) rešil enačbo $(\times)$. Racionalnih rešitev enačbe $(\times)$ je torej neskončno mnogo pri poljubnih koeficientih a, b in c.

Če pa zahtevamo, da so rešitve celoštevilske, pa se pojavi težava, saj število $x = (c - by)/a$ niti pri celoštevilskih y ni nujno celo. Velja pa naslednje:

IZREK 12.12 *Diofantska enačba*

$$ax + by = c, \;\; a, b \neq 0, \qquad (\times)$$

je rešljiva, če in samo če je število c deljivo z največjim skupnim deliteljem števil a in b. V tem primeru je rešitev neskončno mnogo. Če je (x_0, y_0) neka rešitev enačbe $(\times)$, so ostale rešitve enačbe $(\times)$ oblike

$$x = x_0 - kb', \;\; y = y_0 + ka', \qquad k \in \mathbb{Z},$$

kjer je $a' = a/\gcd(a, b)$ in $b' = b/\gcd(a, b)$.

DOKAZ: Obstoj rešitve, v primeru, da $\gcd(a, b)$ deli c, bomo pokazali v nadaljevanju, ko bomo predstavili postopek za iskanje rešitve. Osredotočimo se torej na preostale trditve iz izreka.

Denimo, da je enačba $(\times)$ rešljiva. Tedaj obstajata takšni števili $x_0, y_0 \in \mathbb{Z}$, da je $ax_0 + bx_0 = c$. Če je m poljuben skupni delitelj števil a in b, tedaj je $a = rm$ in $b = tm$ za neki celi števili r in t, in zato

$$c \;=\; ax_0 + by_0 \;=\; rmx_0 + tmy_0 \;=\; (rx_0 + ty_0)m.$$

Od tod sledi, da vsak skupni delitelj števil a in b (tudi $\gcd(a, b)$) deli c.

Naj bo (x_0, y_0) poljubna rešitev enačbe $(\times)$ in $x = x_0 - kb'$, $y = y_0 + ka'$ za neko celo število k. Tedaj je

$$ax + by = a(x_0 - kb') + b(y_0 + ka') = ax_0 + by_0 = c,$$

kar dokazuje, da je tudi (x, y) rešitev enačbe.

Dokazati moramo le še, da je res vsaka rešitev enačbe $(\times)$ oblike $x = x_0 + kb'$, $y = y_0 - ka'$. Pa naj bo (x_1, y_1) še neka rešitev enačbe $(\times)$. Tedaj je $(ax_0 + by_0) - (ax_1 + by_1) = 0$, in zato $a(x_0 - x_1) = b(y_1 - y_0)$. Če iz slednje enakosti pokrajšamo največji skupni večkratnik števil a in b, dobimo

$$a'(x_0 - x_1) = b'(y_1 - y_0).$$

Iz trditve 12.10 sledi, da sta števili a' in b' tuji. Tedaj pa iz trditve 12.9 sledi, da je $k = (y_1 - y_0)/a'$ celo število. Pri tem velja

$$x_0 - kb' = x_0 - \frac{(y_1 - y_0)b'}{a'} = x_0 - (x_0 - x_1) = x_1, \quad y_0 + ka' = y_0 + (y_1 - y_0) = y_1,$$

in rešitev (x_1, y_1) je res zahtevane oblike. ∎

12.4 Razširjeni Evklidov algoritem

Razširjeni Evklidov algoritem uporabljamo za računanje največjega skupnega delitelja danih celih števil in za reševanje linearnih diofantskih enačb z dvema neznankama. Sam postopek lahko opišemo takole:

VHODNI PODATEK: Par (a, b) neničelnih celih števil.

$(r_0, x_0, y_0) := (a, 1, 0)$;
$(r_1, x_1, y_1) := (b, 0, 1)$;
$i := 1$;
dokler $r_i \neq 0$ izvajaj
    $i := i + 1$;
    $k_i := r_{i-2}$ div r_{i-1};
    $(r_i, x_i, y_i) := (r_{i-2}, x_{i-2}, y_{i-2}) - k_i(r_{i-1}, x_{i-1}, y_{i-1})$;
konec zanke

VRNI: $(r_{i-1}, x_{i-1}, y_{i-i})$.

TRDITEV 12.13 *Naj bosta a in b neničelni celi števili. Tedaj trojica (d, x, y), ki jo vrne razširjeni Evklidov algoritem z vhodnim podatkom (a, b), zadošča pogoju*

$$ax + by = d, \quad d = \gcd(a, b).$$

DOKAZ: Za števila r_i, a_i in b_i iz opisa razširjenega evklidovega algoritma za vsak $i \geq 0$ z indukcijo dokažimo enakost

$$ax_i + by_i = r_i. \tag{$*$}$$

Ta enakost očitno velja za $i = 0$ in $i = 1$, saj je $ax_0+by_0 = a\cdot 1+b\cdot 0 = a = r_0$ in $ax_1+by_1 = a\cdot 0+b\cdot 1 = b = r_1$. Denimo sedaj, da je $i \geq 2$, in privzemimo, da enakost $(*)$ velja za vse indekse manjše od izbranega i. Tedaj

$$ax_i+by_i = a(x_{i-2}-k_ix_{i-1})+b(y_{i-2}-k_iy_{i-1}) = ax_{i-2}+by_{i-2}-k(ax_{i-1}+by_{i-1}).$$

Po indukcijski predpostavki je slednje enako $r_{i-2} - kr_{i-1} = r_i$. S tem smo dokazali enakost $(*)$, in zato tudi $ax + by = d$.

Dokazati moramo še, da je $\gcd(a, b) = d$. V izreku 12.12 smo že dokazali, da iz enakosti $ax + by = d$ sledi, da $\gcd(a, b)$ deli d. Dokazati moramo še, da d deli tako a kot b (in zato tudi $\gcd(a, b)$).

Razširjeni Evklidov algoritem se ustavi takrat, ko vrednost ostanka r_i pade na nič, število d, ki ga algoritem vrne, pa je zadnji neničelni ostanek

(označimo njegov indeks z n). Ker je $0 = r_{n+1} = r_{n-1} - kr_n = r_{n-1} - kd$, vidimo, da d deli r_{n-1}. Dokažimo, da d deli r_i za vsak $i \in \{0, \ldots, n\}$. Pa denimo, da temu ni tako, in vzemimo največji indeks j, za katerega r_n ne deli r_j (seveda $j \leq n-2$). Ker je $r_{j+2} = r_j - kr_{j+1}$, je $r_j = r_{j+2} + kr_{j+1}$. Iz definicije indeksa j sledi, da sta števili r_{j+1} in r_{j+2} deljivi z d, in zato tudi število r_j. To pa je v protislovju z našo predpostavko. S tem smo dokazali, da d res deli r_i za vsak $i \geq 0$, torej tudi $r_0 = a$ in $r_1 = b$. S tem je izrek dokazan. ∎

Trditev 12.13 nam pove, kako poiskati rešitev diofantske enačbe $ax + by = c$ kadar je $c = \gcd(a, b)$. Kaj pa, če je c nek pravi večkratnik števila $\gcd(a, b)$, na primer $c = t \gcd(a, b)$. Tedaj najprej z razširjenim evklidovim algoritmom poiščemo rešitev (x', y') enačbe $ax' + by' = \gcd(a, b)$. Če to enakost pomnožimo s številom t, vidimo, da je $x_0 = tx'$, $y_0 = ty'$ res rešitev prvotne diofantske enačbe.

Zgled. *Poišči vse rešitve diofantske enačbe*

$$4333x + 623y = 21. \qquad (*)$$

Izvedimo razširjeni Evklidov algoritem z vhodnim podatkom $(a, b) = (4333, 623)$.

i	r_i	x_i	y_i	k_i
0	4333	1	0	
1	623	0	1	
2	595	1	−6	6
3	28	−1	7	1
4	7	22	−153	21
5	0	−89	619	4

Algoritem torej vrne trojico $(7, 22, -153)$. Trditev 12.13 tedaj pravi, da je $\gcd(4333, 623) = 7$ in

$$4333 \cdot 22 + 623 \cdot (-153) = 7.$$

Enakost pomnožimo s 3 in dobimo:

$$4333 \cdot 66 + 623 \cdot (-459) = 21.$$

Od tod razberemo, da je $x_0 = 66$ in $y_0 = -459$ rešitev enačbe $(*)$. Iz Izreka 12.12 sledi, da je poljubna rešitev enačbe $(*)$ enaka $x_k = 66 - \frac{623}{7}k = 66 + 89k$, $y_k = -459 + \frac{4333}{7}k = -459 + 619k$, za kak $k \in \mathbb{Z}$. ∎

12.5 Modularna aritmetika

DEFINICIJA 12.14 Naj bo m poljubno naravno število. Pravimo, da sta celi števili x in y *kongruentni po modulu* m, če in samo če m deli $y - x$. Pri tem pišemo

$$x \equiv y \pmod{m} \text{ ali tudi } x \equiv_m y.$$

Relacija kongruence je v tesni zvezi z operacijo celoštevilskega ostanka mod . Velja namreč naslednje:

TRDITEV 12.15 *Za poljubna števila* $x, y \in \mathbb{Z}$ *in* $m \in \mathbb{N}$ *velja*

$$x \equiv y \pmod{m} \;\Leftrightarrow\; x \bmod m = y \bmod m.$$

DOKAZ: Zapišimo $x = km + r$ in $y = \ell m + s$, kjer je $r = x \bmod m$ in $s = y \bmod m$. Če je $r = s$, tedaj očitno m deli število $y - x = m(\ell - k)$.

Denimo sedaj, da je $x \equiv y \pmod{m}$. Dokazati moramo, da od tod sledi $r = s$. Ker m deli število $y - x = (\ell - k)m + s - r$, je $(\ell - k) + s - r = tm$ za neki $t \in \mathbb{Z}$, in zato $s - r = m(t + k - \ell)$. Vendar števili s in r obe ležita na intervalu med 0 in $m - 1$, zato tudi njuna razlika po absolutni vrednosti ne presega števila $m - 1$. Iz zgornje enakosti tedaj sledi, da je $t + k - \ell = 0$, in zato $s = r$, kot je bilo potrebno dokazati. ∎

Kot kaže naslednji izrek, je relacija kongruence lepo uglašena z operacijama seštevanja in množenja.

IZREK 12.16 *Naj velja* $x_1 \equiv y_1 \pmod{m}$ *in* $x_2 \equiv y_2 \pmod{m}$. *Tedaj velja tudi*

$$x_1 + x_2 \equiv y_1 + y_2 \pmod{m} \text{ in } x_1 x_2 \equiv y_1 y_2 \pmod{m}.$$

DOKAZ: Pišimo $y_1 - x_1 = k_1 m$ in $y_2 - x_2 = k_2 m$. Tedaj je $(y_1 + y_2) - (x_1 + x_2) = (k_1 + k_2)m$, in zato $x_1 + x_2 \equiv y_1 + y_2 \pmod{m}$.

Pri dokazu druge kongruence moramo biti nekoli zviti. Računajmo:

$$y_1 y_2 - x_1 x_2 = y_1(y_2 - x_2) + (y_1 - x_1)x_2 = (y_1 k_2 + k_1 x_2)m.$$

Torej m deli razliko $y_1 y_2 - x_1 x_2$, in zato $x_1 x_2 \equiv y_1 y_2 \pmod{m}$. ∎

Od tod lahko z uporabo indukcije izpeljemo naslednji sklep.

TRDITEV 12.17 *Če je* $x \equiv y \pmod{m}$ *in* $r \in \mathbb{N}$, *tedaj je tudi* $x^r \equiv y^r \pmod{m}$.

Naslednji izrek pa nam pove, na kakšen način lahko iz kongruence krajšamo multiplikativne faktorje.

IZREK 12.18 *Naj bodo a, x, y poljubna cela števila, $a \neq 0$, in m poljubno naravno število. Tedaj velja naslednji sklep:*

$$ax \equiv ay \pmod{m} \;\Rightarrow\; x \equiv y \pmod{\frac{m}{\gcd(a,m)}}.$$

DOKAZ: Naj velja $ax \equiv ay \pmod{m}$. Tedaj obstaja $k \in \mathbb{Z}$, tako da je $ay - ax = km$. Na levi izpostavimo a in enakost delimo z $\gcd(a,m)$. Dobimo:

$$\frac{a}{\gcd(a,m)}(y-x) = k\frac{m}{\gcd(a,m)}.$$

Iz trditve 12.9 sledi, da sta števili $\frac{a}{\gcd(a,m)}$ in $\frac{m}{\gcd(a,m)}$ tuji. Trditev 12.10 pa tedaj pravi, da $\frac{m}{\gcd(a,m)}$ deli $y - x$, kot smo želeli pokazati. ∎

Zgornjo trditev največkrat uporabimo v dveh skrajnih primerih: ko je a tuj m in ko a deli m. Sklepa, ki ju dobimo v teh dveh primerih, zapišimo posebej:

POSLEDICA 12.19 *Naj velja $ax \equiv ay \pmod{m}$.*

(i) *Če je $\gcd(a,m) = 1$, tedaj je $x \equiv y \pmod{m}$.*

(ii) *Če a deli m, tedaj je $x \equiv y \pmod{\frac{m}{a}}$.*

12.6 Kolobar ostankov

Skozi ves razdelek naj m predstavlja poljubno fiksno naravno število, večje ali enako 2. Množico vseh možnih ostankov pri deljenju s številom m označimo takole:

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}.$$

Na množici ostankov $\mathbb{Z}_m$ definirajmo operaciji, ki ju bomo imenovali *seštevanje in množenje po modulu m* in označevali z $\oplus$ in $\odot$. Za $a, b \in \mathbb{Z}_m$ naj bo

$$a \oplus b = (a+b) \bmod m \;\text{ in }\; a \odot b = (ab) \bmod m.$$

Kot bomo videli, se ti dve operaciji v mnogočem obnašata podobno kot navadno seštevanje in množenje, zato bomo, kadar ne bo nevarnosti za pomoto, krožec okoli znakov + in · izpuščali. Z nekaj dela se lahko prepričamo v naslednj trditev.

TRDITEV 12.20 *Množica $\mathbb{Z}_m$ skupaj z operacijama seštevanja in množenja po modulu m tvori komutativni kolobar z enoto.*

V kolobarju $\mathbb{Z}_m$ se lahko nekateri elementi obnašajo nekoliko nenavadno. Oglejmo si na primer elementa 6 in 4 v $\mathbb{Z}_8$. Njun običajni produkt je enak 24, kar je deljivo z 8. Zato v $\mathbb{Z}_8$ velja enakost $6 \odot 4 = 0$. V kolobarju ostankov je torej produkt dveh neničelni Števil lahko enak 0. Takšna števila si zaslužijo ime: imenujemo jih *delitelji niča*. Ni težko razmisliti, da je neničelni element x kolobarja $\mathbb{Z}_m$ delitelj niča, če in samo če x ni tuj m.

12.7 Obrnljivi elementi v $\mathbb{Z}_n$

Naj bo n poljubno naravno število, večje ali enako 2. Zaradi enostavnejšega zapisa bomo v tem razdelku operaciji $\oplus$ in $\odot$ v kolobarju $\mathbb{Z}_n$ pisali kar kot običajna "plus" in "krat". Kadar bo obstajala nevarnosti za nesporazum, bomo posebej poudarili, ali imamo v mislih običajne operacije v $\mathbb{Z}$ ali pa gre za operacije v $\mathbb{Z}_n$.

DEFINICIJA 12.21 Naj bo x poljuben element kolobarja ostankov $\mathbb{Z}_n$. Če v $\mathbb{Z}_n$ obstaja element $\bar{x}$, za katerega v kolobarju $\mathbb{Z}_n$ velja $x\bar{x} = 1$, rečemo, da je element x obrnljiv v $\mathbb{Z}_n$, element $\bar{x}$ pa imenujemo *inverz* elementa x in ga označimo z x^{-1}.

Za zgled si oglejmo element 2 v $\mathbb{Z}_7$. Ker je $2 \cdot 4 = 8 \equiv 1 \pmod 7$, je 2 obrnljiv element v $\mathbb{Z}_7$ in $2^{-1} = 4$. Če si ogledamo spodnjo tabelico množenja v kolobarju $\mathbb{Z}_7$, se hitro prepričamo, da je v $\mathbb{Z}_7$ obrnljiv prav vsak neničelni element.

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Inverze lahko prečitamo iz spodnje tabele.

x	1	2	3	4	5	6
x^{-1}	1	4	5	2	3	6

Precej drugačna je situacija v kolobarju $\mathbb{Z}_6$. Oglejmo si tabelico množenja.

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Vidimo, da sta edina obrnljiva elementa kolobarja $\mathbb{Z}_6$ števili 1 in 5. Pri tem, kot vedno, velja $1^{-1} = 1$. Nekoliko nenavadna pa je enakost $5^{-1} = 5$.

Vprašajmo se torej, ali znamo za dano naravno število n ugotoviti, kateri elementi kolobarja $\mathbb{Z}_n$ so obrnljivi, ne da bi izračunali celotno tabelico množenja. Odgovor se skriva v naslednjem izreku.

IZREK 12.22 *Neničelni element a kolobrja $\mathbb{Z}_n$ je obrnljiv, če in samo če je tuj proti številu n.*

DOKAZ: Problem prevedimo na običajne operacije med celimi števili. Element $a \in \mathbb{Z}_n$ je obrnljiv v $\mathbb{Z}_n$, če in samo če obstaja število x, za katerega je $ax \equiv 1 \,(\mathrm{mod}\, n)$, oziroma, če in samo če obstajata celi števili x in y, za kateri je $ax - 1 = ny$. Takšni števili pa obstajata, če in samo če je rešljiva naslednja diofantska enačba

$$ax - ny = 1. \qquad (*)$$

Kot vemo, pa ima zgornja enačba rešitev, če in samo če sta števili a in n tuji. S tem je izrek dokazan. ■

Dokaz pa nam je povedal tudi, kako inverz danega elementa dejansko izračunati. Potrebno je rešiti diofantsko enačbo $(*)$ in po potrebi poiskati tisto rešitev, za katero je x na intervalu med 0 in $n - 1$. (Premisli, da lahko takšno rešitev vedno najdemo.)

ZGLED. *Izračunaj* 31^{-1} *v* $\mathbb{Z}_{365}$

Rešiti moramo difantsko enačbo $31x - 365y = 1$. To lahko storimo z razširjenim Evklidovim algoritmom. ■

Koliko obrnljivih elementov pa premore kolobar $\mathbb{Z}_n$? Kot pravi izrek 12.22, natanko toliko, kot je naravnih števil med 1 in $n - 1$, ki so tuja številu n. Število takšnih števil je tako pomembno, da nosi svoje ime.

12.8 Eulerjeva funkcija

DEFINICIJA 12.23 Naj bo n poljubno naravno število, večje ali enako 2. Število tistih naravnih števil med 1 in $n-1$, ki so tuja n, označimo z $\varphi(n)$. Dodatno definiramo še $\varphi(1) = 1$. Tako definirani funkciji $\varphi\colon \mathbb{N} \to \mathbb{N}$ rečemo *Eulerjeva funkcija.*

TRDITEV 12.24 *Če je p praštevilo in r poljubno naravno število, je*

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1) = p^r(1 - \frac{1}{p}).$$

Če sta a in b tuji naravni števili, je

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Zgornja trditev nam omogoča, da izračunamo Eulerjevo funkcijo $\varphi(n)$ za vsako naravno število n, če ga le znamo razcepiti na prafaktorje. Namreč, če je

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

razcep števila n na prafaktorje, tedaj je

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) = p_1^{\alpha_1}(1 - \frac{1}{p_1})p_2^{\alpha_2}(1 - \frac{1}{p_2}) \cdots p_k^{\alpha_k}(1 - \frac{1}{p_k}) =$$

$$= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

12.9 Mali Fermatov izrek in Eulerjev izrek

IZREK 12.25 (**Fermat**) *Naj bo p praštevilo in a naravno število, tuje p. Tedaj je $a^{p-1} \equiv 1 \bmod p$.*

Opomba. Zgornji izrek lahko povemo tudi v jeziku kolobarjev ostankov. Izrek namreč pravi, da za vsako praštevilo p in element $a \in \mathbb{Z}_p \setminus \{0\}$ velja $a^{p-1} = 1$.

DOKAZ: Oglejmo si elemente $a, 2a, 3a, \ldots, (p-1)a$ of $\mathbb{Z}_p$. Če sta dva izmed njih enaka, denimo $ia = ja$, potem z množenjem z a^{-1} v $\mathbb{Z}_p$ dobimo $i = j$ (spomni se, da je element a v $\mathbb{Z}_p$ obrnljiv, če je tuj proti p. S tem smo dokazali, da so zgoraj našteti elementi paroma različni, in ker jih je ravno $p-1$, tvorijo množico vseh neničelnih elementov v $\mathbb{Z}_p$:

$$\{a, 2a, 3a, \ldots, (p-1)a\} = \{1, 2, 3, \ldots, p-1\}.$$

Če zmnožimo vse elemente množic na levi in desni strani enakosti, dobimo naslednjo enakost v $\mathbb{Z}_p$:

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1) = a \cdot 2a \cdot 3a \cdots (p-1)a = (p-1)!a^{p-1}.$$

Vendar $(p-1)!$ je tuj proti p, zato ga smemo iz leve in desne strani enakosti v $\mathbb{Z}_p$ pokrajšati. Od to dobimo enakost $a^{p-1} = 1$ v $\mathbb{Z}_p$. ∎

Zgornji izrek pa lahko nekoliko posplošimo. Najprej opazimo, da je $\varphi(p) = p-1$ za vsako praštevilo p. Zato lahko izraz a^{p-1} interpretiramo tudi kot $a^{\varphi(p)}$. Ob tej interpretaciji se izkaže, da lahko pogoj, da je p praštevilo, izpustimo. Velja namreč naslednji izrek.

Izrek 12.26 (**Euler**) *Naj bo n poljubno naravno število in a število, ki je tuje n. Tedaj je $a^{\varphi(n)} \equiv 1 \bmod n$.*

Opomba. V jeziku kolobarjev ostankov zgornji izrek pravi, da je $a^{\varphi(n)} = 1$ za vsak obrnljiv element $a \in \mathbb{Z}_n^*$.

Dokaz Eulerjevega izreka je na las podoben dokazu malega Fermatovega izreka, le da namesto s števili $a, 2a, \ldots, (p-1)a$ pričnemo z elementi za, kjer z preteče vse obrnljive elemente iz $\mathbb{Z}_n^*$. Podrobnosti dokaza lahko izdela bralec sam.

Zgled. *S pomočjo Eulerjevega izreka izračunaj* $1840^{1995} \bmod 26$

Najprej izračunamo $1840 \bmod 26 = 20$. Zato $1840^{1995} \equiv 20^{1995} \bmod 26$. Ker 20 ni tuje 26, Eulerjevega izreka ne moremo uporabiti takoj. Zato 20^{1995} pišemo kot $4^{1995} \cdot 5^{1995}$. Za razcep $20 = 4 \cdot 5$ smo se odložili zato, ker je 5 med delitelji števila 20 največji, ki je tuj 26.

Ker je $\gcd(5, 26) = 1$, lahko število $5^{1995} \bmod 26$ izračunamo neposredno s pomočjo Eulerjevega izreka. Ker je $\varphi(26) = 12$, najprej zapišemo $1995 = 12 \cdot 166 + 3$ in od tod dobimo

$$5^{1995} \equiv (5^{12})^{166} \cdot 5^3 \equiv 5^3 \equiv 21 \,(\bmod 26).$$

Pri računanju ostanka $4^{1995} \bmod 26$ moramo biti nekoliko iznajdljivejši. Najprej zapišemo $4^{1995} = 2^{3990}$ in označimo $x = 2^{3990} \bmod 26$. Tedaj je $x = 2^{3990} - 26q$, kjer $q = 2^{3990} \operatorname{div} 26$, in zato $x = 2y$ za neko naravno število y. Od tod dobimo $2y \equiv 2^{3990} \,(\bmod 26)$, od koder sledi $y \equiv 2^{3989} \,(\bmod 13)$, in zato $y = 2^{3989} \bmod 13$. Slednji ostanek pa lahko izračunamo s pomočjo

Eulerjevega izreka (oziroma celo s pomočjo Fermatovega malega izreka). Ker je $\varphi(13) = 12$ in $3989 = 332 \cdot 12 + 5$, je

$$2^{3989} \equiv 2^5 \equiv 6 \bmod 13,$$

in torej $y = 6$ in $x = 12$. S tem smo dokazali kongruenco

$$4^{1995} \equiv 12 \,(\bmod 26).$$

Račun zaključimo takole:

$$1840^{1995} \equiv 20^{1995} \equiv 4^{1995} \cdot 5^{1995} \equiv 12 \cdot 5^3 \equiv 60 \cdot 25 \equiv 8 \cdot (-1) \equiv 18 \,(\bmod 26).$$

■

12.10 Kriptografski sistem RSA

Za zgled uporabe modularne aritmetike si oglejmo kriptografsko metodo, imenovano RSA, ki omogoča pošiljanje tajnih sporočil med več udeleženci, pri čemer vsebino tajnega sporočila lahko razbere le tisti, ki mu je bilo sporočilo poslano.

Sistem RSA sodi med kriptografke sisteme z javnim ključem. Posebnost teh sistemov je, da vsak udeleženec komunikacije, ki želi prejemati tajna sporočila od ostalih udeležencev, javno objavi svoj *javni ključ* (geslo), ki ga ostali uporabijo za šifriranje njemu namenjenih sporočil, v tajnosti pa ohrani svoj *privatni ključ*, ki je potreben za dešifriranje sporočil, ki so bila zašifrirana z njegovim javnim ključem. Varnost metode sledi na dejstvu, da je iz posameznikovega javnega ključa zelo težko (praktično neizvedljivo) izračunati njegov privatni ključ.

Opišimo na kratko, kaj mora storiti oseba A, ki bi od osebe B želela prejeti tajno sporočilo.

- Najprej naključno izbere dve praštevili, p in q, ter izračuna

  $$n = pq, \quad \varphi = \varphi(n) = (p-1)(q-1).$$

  Za varnost sistema je zelo pomembno, da sta praštevili p in q tako veliki, da števila n nihče, razen osebe A, ne zna razcepiti na produkt praštevil. Danes se v praksi uporabljajo vsaj 100 mestna praštevila, kjer pa je potrebna večja varnost, pa še večja praštevila.

- Izbere poljubno število $e \in \mathbb{Z}_\varphi^*$ (število med 1 in $\varphi - 1$, ki je tuje φ) in s pomočjo razširjenega Evklidovega algoritma izračuna inverz

$$d = e^{-1} \in \mathbb{Z}_\varphi^*.$$

  V praksi število e izbremo tako, da naključno izberemo število med 1 in $\varphi - 1$, nato pa z razširjenim Evklidovim algoritmom testiramo, ali je število e res tuje številu φ; če ni, postopek izbire števila e ponovimo. Kot bomo videli kasneje, nekatere vrednosti števila e niso najbojše (na primer, $e = 1$), zato zavrnemo tudi morebitne takšne naključne izbire.

- Javno objavi števili n in e (javni ključ), sam pa varno shrani število d (privatni ključ). Ostale podatke "pozabi".

Zdaj pa si oglejmo, kaj mora storiti oseba B, ki želi osebi A poslati tajno sporočilo.

- Svoje tekstovno sporočilo najprej pretvori v število $m \in \mathbb{Z}_n$. To stori na javno znan način in tako, da bo vsak, ki bo poznal število m, brez težav rekonstruiral začetno tekstovno sporočilo. Če je tekstovno sporočilo predolgo, ga najprej razbije na manjše dele, jih pretvori v zaporedje števil v $\mathbb{Z}_n$, in izvede spodaj opisani postopek za vsak člen tega zaporedja.

- Prebere javni ključ (n, e) osebe A, izračuna število

$$c = m^e \bmod n$$

  in ga pošlje osebi A.

Ko oseba A prejme število c, uporabi svoj privatni ključ d in izračuna število

$$m' = c^d \bmod n.$$

Izkaže se, da je število m' kar enako originalnemu številu m. Nazadnje oseba A iz števila $m' = m$ rekonstruira tekstovno sporočilo osebe B.

Vidimo, da celotna metoda temelji na naslednji trditvi.

Trditev 12.27 *Naj bosta p in q različni praštevili in naj bo $n = pq$ ter $\varphi = (p-1)(q-1)$. Nadalje, naj bo e poljuben obrnljiv element kolobarja $\mathbb{Z}_\varphi$ in $d = e^{-1} \in \mathbb{Z}_\varphi^*$ njegov inverz. Tedaj za vsako celo število m, $1 \leq m \leq n-1$, iz enakosti $c = m^e \bmod n$ sledi enakost $c^d \bmod n = m$.*

DOKAZ: Ker je d inverz elementa e v $\mathbb{Z}_\varphi$, obstaja celo število x, za katerega je $ed - x\varphi = 1$. Tedaj

$$c^d \equiv m^{ed} = m^{1+x\varphi} = m \cdot (m^\varphi)^x \bmod n.$$

Če je $\gcd(m, n) = 1$, potem iz Eulerjevega izreka sledi $m^\varphi \equiv 1 \bmod n$, in zato $c^d \equiv m \bmod n$.

Predpostavimo torej lahko, da m ni tuj n. To se zgodi le, če bodisi p bodisi q deli število m. Brez izgube splošnoti lahko predpostavimo, da je m večkratnik števila p. Tedaj je tudi število $c^d = m^{ed}$ deljivo s p, in zato

$$c^d \equiv m \equiv 0 \bmod p.$$

Ker m ni hkrati deljiv tudi s q (saj bi sicer ne bil manjši od n), smemo uporabiti Fermatov izrek in ugotoviti, da je $m^{q-1} \equiv 1 \bmod q$. Zato velja

$$c^d = m^{ed} = m^{1+x\varphi} = m \cdot \left(m^{(q-1)}\right)^{(p-1)x} \equiv m \bmod q.$$

Od tod sledi, da imata števili $c^d \bmod n$ in m enaka ostanka pri deljenju s p kot tudi pri deljenju s q. Ni težko videti, da imata tedaj enaka ostanka tudi pri deljenju z $n = pq$. Ker sta obe števili manjši ali enaki n, sta zato enaki. ∎

Kombinatorika

Kombinatorika je široko področje, ki se ukvarja predvsem s končnimi matematičnimi objekti. Osrednji vprašanji, ki si jih zastavlja kombinatorika, sta obstoj in generiranje objektov s predpisanimi lastnostmi in pa število takšnih objektov. V našem hitrem pregledu kombinatorike se bomo osredotočili predvsem na slednje vprašanje.

V prvem razdelku bomo obravnavali vprašanja tipa "Na koliko načinov lahko izberemo k kroglic iz škatle z n kroglicami". Obravnavali bomo več različicah tega vprašanja.

13 Izbori

Razdelek pričnimo z naslednjim zgledom. Pri igri loto se v bobnu nahaja 39 kroglic, oštevilčenih s števili $1, 2, \ldots, 39$. Organizator igre iz bobna zaporedoma sedemkrat izvleče po eno kroglico. Na koliko načinov lahko to stori?

Odgovor je odvisen od tega, kako razumemo besedo "način". Osnovni dilemi pri razumevanju naloge sta naslednji: Prva dilema je, ali kroglico, ki smo jo v posameznem koraku izvlekli, vrnemo v boben – od tega je namreč odvisno, ali lahko posamično kroglico izvlečemo večkrat ali morda največ enkrat. Druga dilema pa je, ali je za nas vrstni red izvlečenih kroglic pomemben – konkretneje, ali naj razlikujemo med izboroma sicer iste množice kroglic, na primer $\{2, 6, 7, 13, 19, 21, 35\}$, kjer v prvem primeru kroglice izvlečemo v vrstnem redu $2, 13, 35, 7, 6, 21, 19$, v drugem pa v drugačnem vrstnem redu, denimo, $35, 13, 7, 6, 21, 19, 2$? Ti dve dilemi mora seveda razrešiti tisti, ki nam je nalogo zastavil. Od njegovega odgovora je odvisno, kako bomo nalogo reševali.

Kadar je za zastavljalca naloge vrstni red pomemben, bomo preštevali *urejene izbore* (tudi *variacije*) izvlečenih kroglic – bodisi s ponavljanjem (če kroglice vračamo) bodisi brez ponavljanja (če kroglic ne vračamo). Če

pa vrstni red ni pomemben, bomo šteli *neurejene izbore* (tudi *kombinacije*) kroglic – spet bodisi s ponavljanjem bodisi brez ponavljanja.

V nadaljevanju si bomo ogledali vsako od štirih možnih interpretacij naloge nekoliko podrobneje. Za lažjo izražavo bomo rezultat vlečenja kroglic imenovali *žreb*. Množico 39 kroglic označimo z $\mathcal{N} = \{1, 2, \ldots, 39\}$.

13.1 Urejeni izbori s ponavljanjem

Denimo, da izvlečene kroglice v boben **vračamo**, vrstni red izvlečenih kroglic pa je **pomemben**. Tedaj lahko rezultat žreba enolično predstavimo z **urejeno sedmerico** elementov množice kroglic $\mathcal{N}$, pri čemer urejeno sedmerico $(a_1, \ldots, a_7)$ razumemo kot tisti žreb, pri katerem v i-tem poskusu izvlečemo kroglico $a_i \in \mathcal{N}$. To nas napelje na idejo, da urejen izbor s ponavljanjem definiramo na naslednji način.

DEFINICIJA 13.1 Naj bo $\mathcal{N}$ poljubna množica z n elementi in r poljubno naravno število. Urejeni r-terici $(a_1, a_2, \ldots, a_r)$ elementov množice $\mathcal{N}$ rečemo *urejeni izbor elementov množice $\mathcal{N}$ dolžine r*. Če želimo poudariti, da so lahko nekateri izmed elementov a_i med seboj tudi enaki, dodamo, da gre za urejeni izbor *s ponavljanjem*. Množico vseh takšnih izborov označimo s simbolom $\overline{\mathcal{V}}(\mathcal{N}, r)$.

TRDITEV 13.2 *Naj bo $\mathcal{N}$ poljubna množica z n elementi in r poljubno naravno število. Tedaj množica $\overline{\mathcal{V}}(\mathcal{N}, r)$ premore n^r izborov.*

DOKAZ: V to se najlažje prepričamo z indukcijo na dolžino izbora r. Če je $r = 1$, je tipični izbor oblike (a), kjer je a element množice $\mathcal{N}$. Ker je elementov množice $\mathcal{N}$ ravno n, je toliko tudi izborov. Formula torej drži za $r = 1$.

Pa denimo, da za neki k formula drži za vse $r \leq k$. Dokažimo, da velja tudi za $r = k + 1$. Res! Označimo elemente množice $\mathcal{N}$ s simboli $a_1, \ldots, a_n$. Izbore iz $\overline{\mathcal{V}}(\mathcal{N}, k + 1)$ razvrstimo v n skupin, $\mathcal{R}_1, \ldots, \mathcal{R}_n$, pri čemer v skupino $\mathcal{R}_i$ razvrstimo vse izbore, ki imajo na prvem mestu element a_i. Če izboru $(a_i, x_1, \ldots, x_k)$ iz množice $\mathcal{R}_i$ odrežemo prvo komponento, dobimo "ostanek" $(x_1, \ldots, x_k)$, ki je izbor iz $\overline{\mathcal{V}}(\mathcal{N}, k)$. Pri tem se vsak izbor iz $\overline{\mathcal{V}}(\mathcal{N}, k)$ pojavi natanko enkrat kot "ostanek" izbora iz skupine $\mathcal{R}_i$. Zato je v vsaki skupini $\mathcal{R}_i$ natanko toliko izborov, kot je izborov v množici $\overline{\mathcal{V}}(\mathcal{N}, k)$; teh pa je, kot zagotavlja indukcijska predpostavka, n^k. Skupaj imamo torej $n^k n = n^{k+1} = n^r$ izborov. S tem je indukcijski korak dokazan. ∎

OPOMBA. Če so $A_1, \ldots, A_r$ poljubne množice, tedaj množici vseh urejenih r-teric oblike $(x_1, \ldots, x_r)$, $x_i \in A_i$, rečemo *kartezični produkt množic* $A_1, \ldots, A_r$ in jo označimo s simbolom $A_1 \times \ldots \times A_r$. Če so vse množice A_i enake neki fiksni množici A, tedaj govorimo o *kartezični potenci*, ki jo označimo z A^r. Množica $\overline{\mathcal{V}}(A, r)$ ni tako nič drugega kot kartezična potenca A^r. Trditev, ki smo jo dokazali zgoraj, se posploši do dejstva, da je moč kartezičnega produkta množic enaka produktu moči množic, ki nastopajo v produktu.

13.2 Urejeni izbori brez ponavljanja

Še naprej si mislimo, da je vrstni red izvlečenih kroglic **pomemben**, le da tokrat izbranih kroglic v boben **ne vračamo**. Tako kot prej si žreb, v katerem v i-tem koraku izberemo kroglico a_i, predstavimo z **urejeno sedmerico** $(a_1, \ldots, a_7)$ elementov $a_i \in \mathcal{N}$. Ker kroglic ne vračamo, so elementi a_i **paroma različni**. Po drugi strani pa vsaka sedmerica paroma različnih elementov množice $\mathcal{N}$ predstavlja kak žreb. Možnih žrebov je torej toliko, kot je različnih sedmeric paroma različnih kroglic v bobnu. Povedano povzemimo v naslednjo formalno definicijo *urejenega izbora brez ponavljanja*.

DEFINICIJA 13.3 Urejeni r-terici paroma različnih elementov množice $\mathcal{N}$ rečemo *urejeni izbor elementov množice* $\mathcal{N}$ *dolžine* r *brez ponavljanja*. Množico vseh takšnih izborov označimo s simbolom $\mathcal{V}(\mathcal{N}, r)$.

Urejenih izborov brez ponavljanja je seveda nekoliko manj kot vseh urejenih izborov. Preden jih preštejemo, vpeljimo naslednji funkciji nravnih števil n in r:

$$n^{\underline{r}} \;=\; n(n-1)\cdots(n-r+1), \quad n! \;=\; n^{\underline{n}} \;=\; n(n-1)\cdots 1$$

in dodatno definirajmo še $n^{\underline{0}} = 0! = 1$ za vsak $n \in \mathbb{N}_0$. Simbolu $n^{\underline{r}}$ rečemo *padajoča potenca* števila n, simbolu $n!$ pa n *fakulteta* (tudi *faktoriela*).

TRDITEV 13.4 *Naj bo* $\mathcal{N}$ *poljubna množica z* n *elementi in* r *poljubno naravno število. Tedaj množica* $\mathcal{V}(\mathcal{N}, r)$ *premore* $n^{\underline{r}}$ *izborov.*

DOKAZ: Razmišljamo lahko povsem enako kot pri dokazu trditve 13.2. Za $r = 1$ trditev očitno velja. V indukcijskem koraku definiramo množice $\mathcal{R}_i$ enako kot prej, le da v njih razporedimo le izbore brez ponavljanja. Opazimo, da je ostanek $(x_1, \ldots, x_n)$ tipičnega elementa $(a_i, x_1, \ldots, x_k) \in \mathcal{R}_i$ izbor elementov množice $\mathcal{N} \setminus \{a_i\}$ brez ponavljanja. Kot v dokazu

trditve 13.2 uporabimo indukcijsko predpostavko in ugotovimo, da $\mathcal{R}_i$ premore $n^{\underline{k}}$ izborov. Vseh iskanih izborov je tako $n(n-1)^{\underline{k}} = n^{\underline{k+1}} = n^{\underline{r}}$. ∎

Če je $|\mathcal{N}| = r$, se v urejenem izboru elementov množice $\mathcal{N}$ dolžine r brez ponavljanja vsak element množice $\mathcal{N}$ pojavi natanko enkrat. Takšnemu izboru rečemo *permutacija* množice $\mathcal{N}$. Iz trditve 13.4 neposredno sledi naslednje:

TRDITEV 13.5 *Število vseh permutacij n-elementne množice je enako*

$$n^{\underline{n}} = n!.$$

OPOMBA. Permutacijo $(a_1, \ldots, a_n)$ množice $\mathcal{N}$ lahko razumemo tudi kot linearno ureditev elementov množice $\mathcal{N}$, pri kateri je a_1 "prvi" element, ki mu "sledi" element a_2 in tako dalje, vse do "zadnjega" elementa a_n. Če pa so elementi množice $\mathcal{N}$ že vnaprej podani z nekim vrstnim redom (npr. če je $\mathcal{N} = \{1, 2, \ldots, n\}$) pa lahko na permutacijo $(a_1, \ldots, a_n)$ pogledamo tudi kot na bijektivno preslikavo iz množice $\mathcal{N}$ vase, ki i-temu elementu množice $\mathcal{N}$ priredi element a_i.

13.3 Neurejeni izbori brez ponavljanja

Mislimo si sedaj, da vrstni red izbranih kroglic **ni pomemben**, izbranih kroglic pa **ne vračamo** v boben. V tem primeru lahko izid žreba enolično podamo z **množico** sedmih izžrebanih kroglic. Možnih izidov žreba je torej toliko, kot je vseh sedemelemntnih podmnožic množice kroglic $\mathcal{N}$. To nas napelje na naslednjo definicijo.

DEFINICIJA 13.6 Naj bo $\mathcal{N}$ poljubna množica z n elementi in r poljubno nenegativno celo število. Tedaj r-elementni podmnožici množice $\mathcal{N}$ rečemo *neurejeni izbor elementov množice $\mathcal{N}$ brez ponavljanja dolžine r*. Množico vseh takšnih izborov označimo s simbolom $\mathcal{K}(\mathcal{N}, r)$ njihovo število pa s simbolom

$$\binom{n}{r} = |\mathcal{K}(\mathcal{N}, r)|,$$

ki mu pravimo *binomski simbol* (tudi *binomski koeficient*) in ga preberemo "n nad r".

TRDITEV 13.7 *Za poljubni nenegativni celi števili n in r velja enakost*

$$\binom{n}{r} = \frac{n^{\underline{r}}}{r!}.$$

Dokaz: Naj bo $\mathcal{N}$ poljubna n-elementna množica in r poljubno nenegativno celo število. Za $r = 0$, trditev preide v stavek, da poljubna množica premore natanko eno podmnožico z 0 elementi. Ker je prazna množica edina 0-elementna množica, je slednje očitno pravilno. Predpostavimo torej lahko, da je $r \geq 1$.

Trditev bomo dokazali tako, da bomo ponovno prešteli vse urejene izbore brez ponavljanja iz množice $\mathcal{V}(\mathcal{N}, r)$. Za $A \in \binom{\mathcal{N}}{r}$ definirajmo naslednjo množico urejenih izborov:

$$\mathcal{R}_A = \{(a_1, \ldots, a_r) : \{a_1, \ldots, a_r\} = A\}.$$

Opazimo, da je $\mathcal{R}_A$ natanko množica vseh permutacij množice A, zato je $|\mathcal{R}_A| = r!$. Ker se vsak izbor iz $\mathcal{V}(\mathcal{N}, r)$ pojavi v natanko eni od množic $\mathcal{R}_A$ (namreč tisti, za katere je množica njegovih komponent enaka A), je število vseh takšnih izborov enako $\binom{n}{r} r!$. Iz trditve 13.4 tedaj sledi enakost

$$\binom{n}{r} r! = n^{\underline{r}}.$$

Delimo še z $r!$ in dobimo formulo iz trditve. ∎

13.4 Neurejeni izbori s ponavljanjem

Nazadnje se lotimo še različice naloge, kjer vrstni red izbranih kroglic **ni pomemben**, izžrebane kroglice pa **vračamo** v boben. V tem primeru izida žreba žal ne moremo podati z množico izžrebanih kroglic, saj množica ne dopušča večkratnih pojavitev svojih elementov. Zato za opis žreba potrebujemo matematično strukturo, ki ima podobne lastnosti kot *množica*, dopušča pa večkratno pripadnost kakega elementa. Takšnemu objektu pravimo *multimnožica*. Formalno je multimnožico najlažje opisati kot preslikavo, ki vsakemu potencialnemu elementu priredi njegovo kratnost v multimnožici. Pri tem za elemente, ki jih v multimnožici ni, rečemo, da v njej nastopajo s kratnostjo 0.

Definicija 13.8 *Multimnožica z elementi v množici A* je poljubna preslikava

$$\mu \colon A \to \mathbb{N}_0.$$

Pri tem številu $\mu(a)$, $a \in A$, rečemo *kratnost* elementa a v multimnožici μ, vsoti

$$\sum_{a \in A} \mu(a)$$

pa moč multimnožice μ.

Neformalno pa lahko multimnožice podajamo tudi kot množice, pri čemer dopuščamo, da se nekateri elementi multimnožice pojavijo več kot enkrat. Pri tem red elementov, tako kot pri množicah, ni pomemben. Na primer, multimnožico $\mu\colon \{a, b, c, d\} \to \mathbb{N}_0$

$$\mu(a) = 1,\ \mu(b) = 2,\ \mu(c) = 0,\ \mu(c) = 3$$

lahko podamo tudi z naštevanjem elementov

$$\mu = [b, c, c, a, c, b] = [c, b, c, b, a, c] = \ldots \quad \text{ali} \quad \mu = [a^1, b^2, c^3]$$

Moč multimnožice μ je 6.

Neurejene izbore s ponavljanjem lahko sedaj opišemo v jeziku multimnožic.

DEFINICIJA 13.9 Naj bo A množica moči n. Multimnožici moči r z elementi v množici A rečemo *neurejeni izbor elementov množice A dolžine r s ponavljanjem.* Množico vseh takšnih multimnožic označimo s simbolom

$$\overline{\mathcal{K}}(A, r),$$

njihovo število pa s

$$\overline{\mathcal{K}}(n, r).$$

TRDITEV 13.10 *Za poljubni nenegativni števili n in r velja*

$$\overline{\mathcal{K}}(n, r) = \binom{n + r - 1}{n - 1} = \binom{n + r - 1}{r}.$$

DOKAZ: Vzemimo n-elementno množico $A = \{a_1, \ldots, a_n\}$. Trditev dokažemo na strog matematičen način tako, da najdemo bijektivno preslikavo iz množice $\overline{\mathcal{K}}(A, r)$ v množico $\mathcal{K}(NN_{n+r-1}, n-1)$[1] Ker so množice, med katerimi obstajajo bijektivne preslikave, enako močne, to res zadošča za dokaz prve enakosti v zgornji formulu. Drugi enačaj sledi neposredno iz lastnosti binomskih simbolov (glej razdelek 13.6).

Naj bo $\mu\colon A \to \mathbb{N}_0$ multimnožica moči r. Za $k \in \{1, \ldots, n-1\}$ definirajmo

$$b_k = \mu(a_1) + \ldots + \mu(a_k) + k$$

[1] Glej opombo, ki sledi trditvi 13.12.

in jih združimo v množico $B_\mu = \{b_1, b_2, \ldots, b_{n-1}\}$. Dokažimo najprej, da je B_μ elementna podmnožica množice $\mathbb{N}_{n+r-1}$ in da premore $n-1$ elementov. Ker je

$$b_{k+1} = b_k + \mu(a_{k+1}) + 1$$

za vsak $k \geq 1$, je zaporedje števil b_k strogo naraščajoče. Ker je $b_1 = \mu(a_1) + 1 \geq 1$, so števila b_k pozitivna. Po drugi strani pa je

$$b_{n-1} = \mu(a_1) + \ldots + \mu(a_{n-1}) + n - 1 \leq \sum_{k=1}^{n} \mu(a_k) + n - 1 = r + n - 1. \quad (*)$$

Zato je res B_μ element množice $\mathcal{K}(\mathbb{N}_{n+r-1}, n-1)$. Dokažimo zdaj, da je preslikava

$$\Phi\colon \overline{\mathcal{K}}(A, r) \to \mathcal{K}(\mathbb{N}_{n+r-1}, n-1), \quad \Phi(\mu) = B_\mu,$$

bijekcija. Surjektivnost dokažemo tako, da vzamemo poljubno $(n-1)$-elementno podmnožico $B \subseteq \mathbb{N}_{n+r-1}$, uredimo njene elemente b_k po velikosti, $b_1 < b_2 < \ldots < b_{n-1}$, in rešimo sistem enačb izhajajoč iz prvega enačaja formule $(*)$ na neznanke $\mu(a_k)$. Dobimo:

$$\mu(a_1) = b_1 - 1, \quad \mu(a_k) = b_k - b_{k-1} - 1 \ \text{ za } \ k \geq 2.$$

Za tako določeno multimnožico $\mu \in \overline{\mathcal{K}}(A, r)$ očitno velja $B_\mu = B$. S tem je surjektivnost preslikave Φ dokazana. Injektivnost sledi iz dejstva, da so števila b_k v formuli $(*)$ natanko določajo vrednosti $\mu(a_k)$. ■

Na koncu poglavja se vrnimo k naši začetni nalogi o številu možnih žrebov sedmih kroglic. Pri vseh štirih različicah naloge preštevamo izbore elementov množice z $n = 39$ elementi dolžine $r = 7$.

Če je vrstni red izvlečenih kroglic pomemben, kroglice pa vračamo v boben, štejemo urejene izbore s ponavljanjem. Teh je – v skladu s trditvijo 13.2 – natanko

$$39^{\overline{7}} = 137\,231\,006\,679.$$

Če je vrstni red izvlečenih kroglic pomemben, kroglic pa ne vračamo v boben, štejemo urejene izbore brez ponavljanja. Teh je – v skladu s trditvijo 13.4 – natanko

$$39^{\underline{7}} = 77\,519\,922\,480.$$

Če vrstni red izvlečenih kroglic ni pomemben, kroglice pa vračamo v boben, štejemo neurejene izbore s ponavljanjem. Teh je – v skladu s trditvijo

13.10 – natanko

$$\binom{39+7-1}{7} = \binom{45}{7} = 45\,379\,620.$$

Nazadnje si oglejmo še interpretacijo naloge, ki ustreza dejanskim pravilom igre loto, torej, ko vrstni red izvlečenih kroglic ni pomemben in kroglic ne vračamo v boben. Tedaj štejemo neurejene izbore brez ponavljanja, ki jih je – v skladu s trditvijo 13.7 – natanko

$$\binom{39}{7} = \frac{39^{\underline{7}}}{7!} = 15\,380\,937.$$

13.5 Permutacije multimnožic

Naj bo $\mu\colon A \to \mathbb{N}_0$ multimnožica moči n. Urejeni n-terici $(x_1, \ldots, x_n)$, v kateri se vsak element $a \in A$ pojavi natanko $\mu(a)$-krat, rečemo *permutacija multimnožice* μ.

TRDITEV 13.11 *Naj bo μ multimnožica moči n z elementi $x_1, \ldots, x_k$ in kratnostmi $\mu(x_i) = n_i$. Tedaj je število permutacij multimnožice μ enako*

$$\binom{n}{n_1, \ldots, n_k} = \frac{n!}{n_1! \cdots n_k!}$$

DOKAZ: Za vsak $i\{1, \ldots, k\}$ definirajmo množico $X_i = \{x_i\} \times \mathbb{N}_{n_i}$ ter množice X_i združimo v množico $X = \cup_{i=1}^{k} X_i$. Na elemente množice X lahko pogledamo kot na elemente multimnožice μ, pri čemer pojavitve istega elementa med seboj razlikujemo.

Iz permutacije množice X lahko dobimo permutacijo multimnožice μ tako, da pri vsakem elementu množice X odmislimo njegovo drugo komponento.

Na primer, če je $\mu = \{x_1^1, x_2^3, x_3^2\}$, potem iz permutacije

$$((x_2, 3), (x_1, 1), (x_2, 1), (x_2, 2), (x_3, 2), (x_3, 1))$$

množice X dobimo permutacijo $(x_2, x_1, x_2, x_2, x_3, x_3)$ multimnožice μ

Vsako permutacijo multimnožice μ lahko na takšen način dobimo iz natanko $n_1! \cdots n_k!$ različnih permutacij množice X. Ker je permutacij množice X natanko $n!$, je permutacij množice μ $n!/n_1! \cdots n_k!$. ∎

13.6 Binomski simboli in Pascalov trikotnik

Oglejmo si nekaj zanimivih lastnosti binomskih simbolov, ki smo jih vpeljali v razdelku 13.3. Najprej opazimo, da lahko formulo iz trditve 13.7 podamo v naslednji "neokrajšani" obliki:

$$\binom{n}{r} = \frac{n^{\underline{r}}}{r!} = \frac{n!}{r!(n-r)!}.$$

Če za r v zgornji formuli vstavimo $n-r$ dobimo naslednjo enakost:

$$\binom{n}{n-r} = \frac{n!}{(n-r)!(n-(n-r))!} = \frac{n!}{(n-r)!r!} = \binom{n}{r}.$$

Z računskim postopkom smo tako prišli do enakosti med števili, ki pa imajo, kot sledi iz definicije 13.6 in trdtive 13.7, tudi kombinatorično interpretacijo:

Trditev 13.12 *Naj bo $\mathcal{N}$ poljubna n-elementna množica. Tedaj je r-elementnih podmnožic množice $\mathcal{N}$ enako mnogo kot $(n-r)$-elementnih podmnožic množice $\mathcal{N}$.*

Zgornje dejstvo niti ni tako presenetljivo, saj bi do njega lahko prišli tudi z naslednjim neposrednim premislekom: Vsaki r-elementni podmnožici $A \subseteq \mathcal{N}$ priredimo njen komplement $A^C \subseteq \mathcal{N}$. Komplement A^C tedaj šteje $n-r$ elementov. Na ta način vsaki r-elementni podmnožici priredimo neko $(n-r)$-elementno podmnožico množice $\mathcal{N}$. Ker sta komplementa A^C, B^C dveh različnih podmnožic $A \neq B$ tudi sama različna, in ker je vsaka $(n-r)$-elementna podmnožica množice $\mathcal{N}$ komplement kake r-elementne podmnožice (saj je enaka komplementu svojega komplementa), je s tem zgornja trditev dokazana.

Opomba. Načelo, ki ga uporabili na koncu zgornjega premisleka, je zelo pomembno kombinatorično načelo in ga lahko povzamemo takole: Če med množicama $\mathcal{A}$ in $\mathcal{B}$ najdemo bijektivno preslikavo, tedaj množici $\mathcal{A}$ in $\mathcal{B}$ premoreta enako mnogo elementov. Temu preprostemu načelu rečemo tudi *načelo enakosti*. Vlogo množic $\mathcal{A}$ in $\mathcal{B}$ v zgornjem premisleki igrata množici $\mathcal{A} = \mathcal{K}(\mathcal{N}, r)$ in $\mathcal{B} = \mathcal{K}(\mathcal{N}, n-r)$, vlogo bijekcije med $\mathcal{A}$ in $\mathcal{B}$ pa preslikava, ki množico $A \in \mathcal{A}$ preslika v njen komplement A^C.

Trditev 13.13 *Za poljubni števili $n, r \in \mathbb{N}_0$, $r \leq n$, velja:*

$$\binom{n+1}{r+1} = \binom{n}{r} + \binom{n}{r+1}.$$

DOKAZ: Navedimo dva dokaza te trditve. Prvi je povsem računski in temelji na formuli iz trditve 13.7. Računajmo:

$$\binom{n}{r} + \binom{n}{r+1} = \frac{n^{\underline{r}}}{r!} + \frac{n^{\underline{r+1}}}{(r+1)!} = \frac{(r+1)n^{\underline{r}} + n^{\underline{r+1}}}{(r+1)!} =$$

$$= \frac{(r+1)n^{\underline{r}} + (n-r)n^{\underline{r}}}{(r+1)!} = \frac{(n+1)n^{\underline{r}}}{(r+1)!} = \frac{n+1^{\underline{r+1}}}{(r+1)!} = \binom{n+1}{r+1}.$$

Drugi dokaz trditve pa je povsem kombinatoričen in upošteva le dejstvo, da je $\binom{n}{r}$ enako številu r-elementnih podmnožic n-elementne množice.

Naj bo $\mathcal{N}$ poljubna $(n+1)$-elementna množica. Brez izgube splošnosti lahko predpostavimo, da je $\mathcal{N} = \{1, 2, \ldots, n, n+1\}$. Množico $(r+1)$-elementnih podmnožic razdelimo v dve skupini: V prvi naj bodo tiste podmnožice, ki vsebujejo element $n+1$, v drugi pa preostale. V drugi skupini so tako pristale ravne vse $(r+1)$-elementne podmnožice množice $\mathcal{N} \setminus \{n+1\}$ – teh je natanko $\binom{n}{r+1}$.

Preštejmo še one iz prve skupine: vsaki podmnožici A iz prve skupine priredimo množico $A' = A \setminus \{n+1\}$. Ker A po predpostavki vsebuje element $n+1$, je A' r-elementna podmnožica množice $\mathcal{N} \setminus \{n+1\}$. Če sta A in B dve različni množici iz prve skupine, sta tudi množici A' in B' različni. Po drugi strani pa je vsaka r-elementna podmnožica množice $\mathcal{N} \setminus \{n+1\}$ enaka A' za neko množico A iz prve skupine (namreč kar za $A = A' \cup \{n+1\}$). S tem smo dokazali, da je preslikava, ki množici A priredi $A' = A \setminus \{n+1\}$ bijektivna preslikava med prvo skupino množic in množico vseh r-elementnih podmnožic množice $\mathcal{N} \setminus \{n+1\}$. Ker je slednjih $\binom{n}{r}$, je toliko tudi podmnožic iz prve skupine.

V obeh skupinah skupaj je torej $\binom{n}{r} + \binom{n}{r+1}$ podmnožic. Po drugi strani pa obe skupini podmnožic skupaj tvorita množico vseh $(r+1)$-elementnih podmnožic $(n+1)$-elementne množice $\mathcal{N}$, za katere pa vemo, da jih je $\binom{n+1}{r+1}$. Enakost je s tem dokazana. ∎

Formula iz trditve 13.13 nosi ime *Pascalova identiteta*. Omogoča nam računati binomske koeficiente rekurzivno s pomočjo sheme, ki ji rečemo *Pascalov trikotnik*. Shema ima obliko enakokrakega trikotnika, ki ga gradimo iz "gornjega" oglišča "navzdol" tako, da na skrajni mesti vsake vrstice najprej vpišemo število 1, "notranjost" vrstice pa zapolnimo tako, v vsako prazno mesto vpišemo vsoto števili, ki stojita levo in desno diagonalno nad praznim mestom. Pri tem prvo vrstico, v kateri stoji le ena številka, namreč 1, imenujemo 0-to vrstico, naslednje pa prva, druga, tretja itd. Podobno

skrajno levemu mestu v vsaki vrstici rečemo 0-to mesto, naslednja pa prvo, drugo, tretje itd. Iz Pascalove identitete tedaj sledi, da se na r-tem mestu n-te vrstice nahaja število $\binom{n}{r}$.

Naslednja zanimiva lastnost binomskih koeficinetov sledi iz dobro znane binomske formule, ki pravi, da za poljubni realni števili x in y ter poljubno naravno število n velja enakost

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r.$$

TRDITEV 13.14

$$\begin{aligned} \sum_{r=0}^{n} \binom{n}{r} &= 2^n; \\ \sum_{r=0}^{n} (-1)^r \binom{n}{r} &= 0. \end{aligned}$$

DOKAZ: Prvo trditev dobimo, če v binomsko formulo vstavimo $x = y = 1$, druga pa, če vstavimo $x = 1$ in $y = -1$. ∎

Od tod z lahkoto izpeljemo naslednji rezultat.

TRDITEV 13.15 *Naj bo $\mathcal{N}$ poljubna n-elementna množica in $P\mathcal{N}$ množica vseh njenih podmnožic. Tedaj je*

$$|P\mathcal{N}| = 2^n.$$

DOKAZ: Seveda je $P\mathcal{N} = \cup_{r=0}^{n} \mathcal{K}(\mathcal{N}, r)$, saj se vsaka pomnožica A množice $\mathcal{N}$ pojavi v kaki (natanko eni) množici iz $\mathcal{K}(\mathcal{N}, r)$, namreč tisti, pri kateri je $r = |A|$. Ker so si množice v uniji desno od enačaja paroma tuje, je moč množice na levi enaka vsoti moči množic na desni. ∎

ZGLED. *S pomočjo izpeljanih trditev rešimo nekaj preprostih preštevalnih nalog.*

1. *Koliko besed dolžine* 3 *lahko sestavimo iz* 25 *črk slovenske abecede. Koliko od teh je takšnih, da se nobena črka ne ponovi.*

2. *Koliko* 8*-mestnih varnostnih gesel lahko sestavimo iz nabora številk* $0, 1, \ldots, 9$ *ter velikih in malih črk angleške abecede, če mora geslo vsebovati vsaj eno številko?*

3. *Varnostno geslo je sestavljeno iz sedem ali osem znakov, ki jih izbiramo med 25 črkami in 10 števkami. Geslo mora vsebovati vsaj pet črk in vsaj eno števko. Koliko takšnih varnostnih gesel obstaja?*

4. *Koliko besed lahko dobimo s premetavanjem črk besede "čmrlj"?*

REŠITVE:

1. Besedo dolžine 3 si predstavimo kot urejeni izbor črk slovenske abecede dolžine 3. Če se črke smejo ponavljati, uporabimo trditev 13.2 in zaključimo, da je iskanih besed natanko $25^3 = 15\,625$. Če se črke ne smejo ponavljati, pa uporabimo trditev 13.4 in dobimo rezultat $25^{\underline{3}} = 13\,800$.

2. Preštejmo najprej vsa gesla, vključno s tistimi, ki ne vsebujejo nobene številke. Takšno geslo lahko predstavimo kot poljuben urejen izbor s ponavljanjem dolžine 8, pri čemer elemente izbiramo iz množice številk in velikih ter malih črk angleške abecede. Ker angleška abeceda šteje 26 znakov, je vseh razpoložljivih simbolov $10+2\cdot 26 = 62$. Vseh gesel je zato 62^8. Da dobimo število dopustnih gesel (torej tistih, ki vsebujejo vsaj eno številko), moramo od tega odšteti število "slabih" gesel, torej tistih, ki so sestavljena zgolj iz črk. Teh je po enakem premisleku 52^8. Odgovor na zastavljeno nalogo je torej $62^8 - 52^8 = 164\,880377\,053440$.

3. Naj $A_{m,n}$ označuje množico gesel, sestavljenih iz m črk in n števk. Geslo zadošča pogojem naloge natanko tedaj, ko pripada kaki od množic $A_{5,2}$, $A_{6,1}$, $A_{5,3}$, $A_{6,2}$ in $A_{7,1}$. Ker so te množice paroma disjunktne, je iskano število enako vsoti njihovih moči. Izračunajmo zdaj moč množice $A_{m,n}$ za poljubni par m, n.

   Elemente množice $A_{m,n}$ bomo razvrstili v nekaj podmnožic glede na to, na katerih mestih v geslu se nahajajo števke. Natančneje, za vsako n-elementno množico $\mathcal{J} \subseteq \mathbb{N}_{m+n}$ naj bo $M_{\mathcal{J}}$ množica vseh tistih gesel iz $A_{m,n}$, ki ima na k-tem mestu števko natanko tedaj, ko je $k \in \mathcal{J}$. Množico $M_{\mathcal{J}}$ si lahko sedaj predstavljmo kot kartezični produkt množic $C_1 \times \ldots \times C_{m+n}$, kjer je C_k množica števk, če je $k \in M_{\mathcal{J}}$, in je C_k množica črk sicer. Sledi, da je $|M_{\mathcal{J}}| = 25^m 10^n$. S pomočjo načela vsote dobimo:

$$|A_{m,n}| = \sum_{\mathcal{J} \in \binom{\mathbb{N}_{m+n}}{n}} |M_{\mathcal{J}}| = \binom{m+n}{n} 25^m 10^n.$$

Iskano število gesel je torej enako

$$|A_{5,2}| + |A_{6,1}| + |A_{5,3}| + |A_{6,2}| + |A_{7,1}| =$$

$$\binom{7}{2}\cdot 25^5\cdot 10^2+\binom{7}{1}\cdot 25^6\cdot 10+\binom{8}{3}\cdot 25^5\cdot 10^3+\binom{8}{2}\cdot 25^6\cdot 10^2+\binom{8}{1}\cdot 25^7\cdot 10$$

$$\approx 1{,}7 \cdot 10^{12}.$$

4. Ker se nobena črka v besedi "čmrlj" ne ponovi, je premetank te besede ravno toliko, kot je permutacij množice črk č, m, r, l, j, torej $5! = 120$.

■

14 Razbitja množic in razčlenitve števil

14.1 Stirlingova števila druge vrste

Množici paroma disjunktnih nepraznih množic $A_1, \ldots, A_k$, katerih unija je enaka množici A, rečemo *razbitje množice* A. Številu vseh razbitij n-elementne množice A na k nepraznih podmnožic rečemo *Stirlingovo število druge vrste* in ga označimo z $S(n,k)$. Očitno velja

$$S(n,k) = 0 \text{ za } k > n\ , \quad S(n,n) = 1 \text{ in } S(n,1) = 1.$$

Dodatno definiramo še $S(n,0) = 0$ za vsak $n \geq 1$ in $S(0,0) = 1$.

TRDITEV 14.1 *Za vsak par naravnih števil n, k, $1 \leq k \leq n$ velja*

$$S(n,k) = S(n-1,k-1) + kS(n-1,k).$$

DOKAZ: Naj bo $\mathcal{N} = \{x_1, \ldots, x_n\}$ poljubna množica, $\mathcal{R}$ množica vseh razbitij množice A na k nepraznih podmnožic, $\mathcal{R}_0$ množica tistih razbitij iz $\mathcal{R}$, v katerih nastopa podmnožica $\{x_n\}$ in $\mathcal{R}_1 = \mathcal{R} \setminus \mathcal{R}_0$.

Vzemimo poljubno razbitje $R = \{A_1, \ldots, A_k\} \in \mathcal{R}$. Mislimo si, da element a_x iz množice $\mathcal{N}$ izrežemo. Tedaj razbitje R preide v razbitje $R' = \{A_1 \setminus \{x_n\}, \ldots, A_k \setminus \{x_n\}\}$ množice $\mathcal{N} \setminus \{x_n\}$.

Če razbitje R sodi v skupino $\mathcal{R}_0$, tedaj je ena od množic razbitja R' prazna in mislimo si lahko, da jo iz R' odstanimo. Tako dobimo razbitje množice $(n-1)$-elementne množice $\mathcal{N} \setminus \{x_n\}$ na $k-1$ nepraznih podmnožic. Obratno, vsako razbitje $T = \{A'_1, \ldots, A'_{k-1}\}$ množice $\mathcal{N} \setminus \{x_n\}$ na $k-1$ nepraznih podmnožic lahko z vključitvijo množice $\{x_n\}$ dopolnimo do razbitja $R = \{\{x_n\}, A'_1 \ldots, A'_{k-1}\}$ množice $\mathcal{N}$. Ni težko videti, da je R edino razbitje iz $\mathcal{R}_0$, za katero je $R' = T$. Zato je razbitij iz skupine R_0 natanko toliko kot razbitij množice $\mathcal{N} \setminus \{n\}$ na $k-1$ nepraznih podmnožic, torej $S(n-1,k-1)$.

Če pa razbitje R sodi v skupino $\mathcal{R}_1$, tedaj nobena od množic rabitja R' ni prazna, kar pomeni, da je R' razbitje mnozčie $\mathcal{N} \setminus \{x_n\}$ na k nepraznih podmnožic. Če vzamemo poljubno razbitje $T = \{A'_1, \ldots, A'_k\}$ množice $\mathcal{N} \setminus \{x_n\}$ na k nepraznih podmnožic, lahko z vključitvijo elementa $\{x_n\}$ va katero koli od k množic A'_i dobimo razbitje R iz skupine R_1, za katerega je $R' = T$. Tako dobljena razbitja R so hkrati edina, za katere je $R' = T$, kar pomeni, da je vseh razbitij iz skupine R_1 natanko k-krat toliko, kot je razbitij $(n-1)$-elementne množice $\mathcal{N} \setminus \{x_n\}$ na k-nepraznih podmnožic, torej $kS(n-1,k)$.

Trditev sedaj z lahkoto sledi, saj je $|\mathcal{R}| = |\mathcal{R}_0| + |\mathcal{R}_1| = S(n-1,k-1) + kS(n-1,k)$. ∎

Rekurzivna formula nam omogoča, da Stirlingova števila 2. vrste računamo podobno kot binomske koeficiente. Sestavimo tabelo, v kateri na presečišču n-te vrstice in k-tega stolpca stoji število $S(n,k)$:

$n\|k$	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0
3	0	1	3	1	0	0	0	0
4	0	1	7	6	1	0	0	0
5	0	1	15	25	10	1	0	0
6	0	1	31	90	65	15	1	0
7	0	1	63	301	350	140	21	1

Iz začetnih pogojev sledi, da so nad glavno diagonalo same ničle, po diagonali same enke, v prvem stolpcu pa, razen pri prvem elementu, zopet same ničle. Število $S(n,k)$ v tabeli dobimo tako, da seštejemo število, ki stoji diagonalno levo nad njim in k-kratnik števila neposredno nad njim. Število 65, ki leži v vrstici 6 in stolpcu 4, smo torej dobili tako, da smo sešteli 25 (levo zgoraj) in $4 \cdot 10$ (smo v stolpcu 4, nad iskanim številom pa stoji 10).

14.2 Lahova števila

Lahovo število $L(n,k)$ je definirano kot število *linearno urejenih razbitij* n-elementne množice na k nepraznih podmnožic. Neformalno lahko linearno urejeno razbitje množice $A = \{a_1, \ldots, a_n\}$ opišemo kot običajno razbitje, pri čemer vsako množico razbitja linearno uredimo. Dve razbitji na iste množice se pri tem razlikujeta, če se razlikujeta vrstna reda elementov v kateri od množic razbitja.

Razliko med običajnimi in linearno urejenimi razbitji si oglejmo na naslednjem primeru. Naj bo $A = \{a,b,c,d\}$ in poiščimo vsa (običajna) razbitjana množice A na dve podmnožici. Le-ta so

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

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

Razbitje $\{\{a,b\},\{c,d\}\}$ porodi štiri različna linearno urejena razbitja:

$$\{[a,b],[c,d]\},\ \{[b,a],[c,d]\},\ \{[a,b],[d,c]\},\ \{[b,a],[d,c]\}.$$

Podobno velja za ostala razbitja na dve enako možni množici. Po drugi strani pa razbitje $\{\{a\},\{b,c,d\}\}$ porodi $3! = 6$ porodi različnih linearno urejenih razbitij – za vsako linearno ureditev elementov $\{b,c,d\}$ po eno. Zato je

$$L(4,2) = 4 \cdot 3 + 6 \cdot 4 = 36.$$

Za skrajne vrednosti Lahovih števil očitno velja naslednje

$$L(n,k) = 0 \text{ za } k > n\ , \quad L(n,n) = 1 \ \text{ in } \ L(n,1) = n!.$$

Dodatno definiramo še $L(n,0) = 0$ za vsak $n \geq 1$ in $L(0,0) = 1$.

Podobno kot pri Stirlingovih številih 2. vrste lahko tudi za Lahova števila izpeljemo rekurzivno zvezo. Izpeljava se razlikuje zgolj v tem, da tu pri štetju razbitij iz skupine $\mathcal{R}_1$ iz danega razbitja $T = \{A'_1, \ldots, A'_k$ množice $\mathcal{N} \setminus \{x_n\}$ lahko najdemo $n - 1 + k$ razbitij R iz skupine $\mathcal{R}_1$, za katera je $R' = T$; izbrisani element x_n lahko namreč vrinemo v katero koli množico A'_i na eno od $|A'_i| + 1$ razpoložljivih mest (za vse elemente množice A'_i ali pa pred kakega od $|A'_i|$ elementov množice A). Element x_n lahko torej vrinemo v razbitje na $(|A_1| + 1) + (|A_2| + 1) + \ldots + (|A_k| + 1)$ načinov, kar znese $n - 1 + k$. Od tod seldi naslednja trditev.

TRDITEV 14.2 *Za $1 \leq k \leq n$ velja*

$$L(n,k) = L(n-1,k-1) + (n+k-1)L(n-1,k).$$

Z indukcijo na število n in z uporabo rekurzivne formule iz trditve 14.2 lahko izpeljemo tudi eksplicitno formulo, ki Lahova števila izrazi s pomočjo binomskih simbolov.

TRDITEV 14.3 *Za $1 \leq k \leq n$ velja*

$$L(n,k) = \binom{n-1}{k-1}\frac{n!}{k!} = \binom{n}{k}\frac{(n-1)!}{(k-1)!}.$$

Podobno kot pri binomskih simbolih in Strilingovih številih 2. vrste, lahko tudi Lahova števila računamo s pomočjo sheme, ki izhaja iz rekurzivne zveze. V spodnji tabeli na presečišču n-te vrstice in k-tega stolpca stoji število $L(n,k)$, ki ga dobimo tako, da seštejemo število, ki stoji diagonalno levo nad njim in $(n+k-1)$-kratnik števila neposredno nad njim. Število 240, ki leži v vrstici 5 in stolpcu 2, smo torej dobili tako, da smo sešteli 24 (levo zgoraj) in $6 \cdot 36$.

$n\|k$	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0
2	0	2	1	0	0	0	0	0
3	0	6	6	1	0	0	0	0
4	0	24	36	12	1	0	0	0
5	0	120	240	120	20	1	0	0
6	0	720	1800	1200	300	30	1	0
7	0	5040	15120	12600	4200	630	42	1

Poleg običajnih Lahovih števila se v literaturi pojavljajo tudi *predznačena Lahova števila*, definirana s formulo

$$L'(n,k) = (-1)^n L(n,k).$$

14.3 Stirlingova števila prve vrste

Stirlingovo število prve vrste $s(n,k)$ štejeje razbitja n-elementne množice na k nepraznih *ciklično urejenih* množic. Pri tem pojem "ciklično urejena množica" pomeni množico, denimo $A = \{a,b,c,d\}$, skupaj s cikličnim vrstnim redom elementov, denimo

$$[a,b,c,d] = [b,c,d,a] = [c,d,a,b] = [d,a,b,c].$$

Hiter premislek pokaže, da lahko vsako m-elementno množico ciklično uredimo na $(m-1)!$ načinov, saj si lahko ciklično ureditev predstavljamo kot linearno ureditev množice, pri čemer m linearnih ureditev, ki se razlikujejo zgolj za ciklični pomik, štejemo kot isto ciklično ureditev. Ker je linearnih ureditev m-elemente množice $m!$, je zato cikličnih ureditev $\frac{m!}{m} = (m-1)!$.

Stirligova števila za mejne pare števil n in k zadoščajo enakostim

$$s(n,k) = 0 \text{ za } k > n\ , \quad s(n,n) = 1 \text{ in } L(n,1) = (n-1)!.$$

Dodatno definiramo še $s(n,0) = 0$ za vsak $n \geq 1$ in $s(0,0) = 1$.

Na zelo podoben način kot pri Stirlingovih številih druge vrste in Lahovih številih, lahko tudi tu izpeljemo naslednjo rekurzivno formulo.

$$s(n,k) = s(n-1,k-1) + (n-1)s(n-1,k).$$

V tabeli Stirlingovih števil 1. vrste, v kateri na presečišču n-te vrstice in k-tega stolpca stoji število $s(n,k)$, ležijo nad glavno diagonalo same ničle, po diagonali same enke, v prvem stolpcu pa, razen prvega elementa, spet same

ničle. V skladu z rekurzivno formulo izračunamo število $s(n,k)$ v tabeli dobimo tako, da seštejemo število, ki stoji levo zgoraj nad njim, in $(n-1)$-kratnik števila, ki stoji neposredno nad njim. Na primer, na presečišču vrstice 5 in stolpca 3 dobimo vsoto števila 11 (levo zgoraj) in števila $(5-1)\cdot 6 = 24$, torej 35.

$n\|k$	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0
3	0	2	3	1	0	0	0	0
4	0	6	11	6	1	0	0	0
5	0	24	50	35	10	1	0	0
6	0	120	274	225	85	15	1	0
7	0	720	1764	1624	735	175	21	1

V literaturi srečamo tudi *predznačena Stirlingova števila prve vrste*, ki so definirana s formulo

$$s'(n,k) = (-1)^{n-k} s(n,k).$$

14.4 Število razbitij naravnega števila

Zaporedju (neničelnih) naravnih števil $m_1 \le m_2 \le \ldots \le m_k$, katerih vsota je enaka n, rečemo *razčlenitev naravnega števila n na k členov*. Število vseh takšnih razčlenitev označimo s $p_k(n)$. Očitno je

$$p_k(n) = 0 \text{ za } k > n.$$

Dodatno definiramo $p_0(0) = 1$ in $p_0(n) = 0$ za $n > 0$.

TRDITEV 14.4 *Za vsak par naravnih števil n, k velja*

$$p_k(n) = p_{k-1}(n-1) + p_k(n-k).$$

DOKAZ: Združimo tiste razčlenitve $(m_1, \ldots, m_k)$, za katera je $m_1 = 1$ v množico $\mathcal{R}_0$, tiste, za katera pa je $m_1 > 1$, pa v množico $\mathcal{R}_1$. Če razčlenitvi iz množice $\mathcal{R}_0$ odvzamemo prvi element $m_1 = 1$, dobimo razčlenitev števila $n-1$ na $k-1$ sumandov. Obratno, če razčlenitvi števila $n-1$ na $k-1$ sumandov dodamo na začetek enico, dobimo razčlenitev iz $\mathcal{R}_0$. Zato je $|R_0| = p_{k-1}(n-1)$.

Razčlenitev $(m_1, \ldots, m_k) \in \mathcal{R}_1$ lahko spremenimo v razčlenitev števila $n-k$ na k sumandov, če vsak m_i zmanjšamo za 1. Ker vsako razčlenitev

števila $n-k$ na k sumandov dobimo na takšen način natanko enkrat, je $|\mathcal{R}_1| = p_k(n-k)$. Od tod dobimo $p_k(n) = |\mathcal{R}_0| + |\mathcal{R}_1| = p_{k-1}(n-1) + p_k(n-k)$. ∎

Računanje števil $p_k(n)$ si olajšamo, če sestavimo tabelo, v kateri na presečišču n-te vrstice in k-tega stolpca stoji število $p_k(n)$. Začetni pogoji in rekurzivna formula pravijo, da so nad glavno diagonalo same ničle, po diagonali same enke, v prvem stolpcu pa, razen prvega elementa, spet same ničle. Število $p_k(n)$ v tabeli dobimo tako, da seštejemo število, ki stoji levo zgoraj nad njim, in število, ki stoji k vrstic nad iskanim številom. Na primer, na presečišču vrstice 7 in stolpca 3 dobimo vsoto števila 3 (levo zgoraj) in števila 1 (tri vrstice višje).

$n\|k$	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0
3	0	1	1	1	0	0	0	0
4	0	1	2	1	1	0	0	0
5	0	1	2	2	1	1	0	0
6	0	1	3	3	2	1	1	0
7	0	1	3	4	3	2	1	1

15 Načelo vključitev in izključitev

Načelo vsote nam pove, da je moč unije paroma disjunktnih množic enaka vsoti njihovih moči. Kaj pa, če množice niso paroma disjunktne. Tedaj je moč unije seveda strogo manjša od vsote moči posameznih množic, saj pri seštevanju moči množic elemente, ki nastopajo v presekih dveh ali več množic štejemo več kot enkrat. Načelo vključitev in izključitev podaja zvezo med močjo unije ter močmi posameznih množic ter njihovih presekov.

15.1 Unija dveh množic

Pričnimo s preprostim zgledom unije dveh množic A in B. Če preštejemo najprej elemente množice A, nato pa Še elemente množice B, smo prešteli vsak element unije $A \cup B$, pri čemer smo elemente v preseku $A \cap B$ prešteli dvakrat. Zato velja dobro znana formula:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

15.2 Unija poljubno mnogo množic

Če je množic več, moč njihove unije računamo s pomočjo naslednje trditve.

TRDITEV 15.1 *Naj bodo $A_1, \ldots, A_n$ poljubne množice. Za $k \in \{1, \ldots, n\}$ naj*

$$S_k = \sum_{\mathcal{J} \in \binom{\mathbb{N}_n}{k}} |\bigcap_{i \in \mathcal{J}} A_i|$$

označuje vsoto moči presekov vseh k-teric množic A_i. Tedaj je

$$|\bigcup_{i=1}^{n} A_i| = \sum_{k=1}^{n} (-1)^{k-1} S_k. \qquad (*)$$

DOKAZ: Naj bo x element unije $\cup_{i=1}^{n} A_i$. Tedaj je x vsebvan v vsaj eni od množic A_i. Pa denimo, da je x vsebovan v natanko m množicah A_i. Tedaj se za vsak $k \in \{1, \ldots, n\}$ element x pojavi v natanko $\binom{m}{k}$ presekih $\cap_{i \in \mathcal{J}} A_i$ za katere je $|\mathcal{J}| = k$. To pa pomeni, da x za vsak k prispeva k desni strani enakosti $(*)$ natanko $(-1)^{k-1}\binom{m}{k}$, skupaj torej

$$\sum_{k=1}^{n} (-1)^{k-1} \binom{m}{k} = 1 + \sum_{k=0}^{m} (-1)^{k-1} \binom{m}{k} = 1,$$

kjer smo pri zadnji enakosti uporabili trditev 13.13. S tem je trditev dokazana. ∎

Zgled. *V krčmo na Divjem zahodu vstopi druščina n revolverašev. Ker je v salonu prepovedano nositi orožje, pri vratih vsak odda svoj revolver. Zaradi objektivnih okoliščin so v nekem trenutku krčmo prisiljeni na hitro zapustiti, pri čemer vsak na slepo zagrabi enega od n oddanih revolverjev. Kolikšna je verjetnost, da nihče od revolverašev ni zagrabil svojega revolverja.*

Označimo revolveraše z naravnimi števili med 1 in n. Situacijo po odhodu iz salona lahko opišemo z n-terico $(a_1, \ldots, a_n)$, kjer je a_i zaporedna številka lastnika revolverja, ki ga je ob odhodu zagrabil i-ti revolveraš. Ta n-terica je očitno permutacija množice $\mathbb{N}_n$. Vseh možnih situacij po odhodu iz salona je torej $n!$.

Koliko situacij pa je takih, da noben revolveraš ne zagrabi svojega revolverja? Za $i = 1, \ldots, n$ naj bo A_i množica tistih permutacij $(a_1, \ldots, a_n)$ za katere je $a_i = i$. Permutacije v A_i predstavljajo natanko tiste situacije, kjer je i-ti revolveraš zagrabil svojo pištolo. Unija $\cup_{i=1}^{n} A_i$ tedaj predstavlja množico tistih situacij, kjer vsaj eden revolveraš zagrabi svojo pištolo. Nas zanima število $n! - |\cup_{i=1}^{n} A_i|$.

Opazimo, da je $|\cap_{i\in\mathcal{J}} A_i| = (n-k)!$, za vsako indeksno množico $\mathcal{J} \in \binom{\mathbb{N}_n}{k}$. Število S_k iz načela o vključitvah in izključitvah je tako enako

$$S_k = \sum_{\mathcal{J}\in\binom{\mathbb{N}_n}{k}} |\bigcap_{i\in\mathcal{J}} A_i| = \binom{n}{k}(n-k)! = \frac{n!}{k!}.$$

Zato je

$$n! - |\bigcup_{i=1}^{n} A_i| = n! - \sum_{k=1}^{n}(-1)^{k-1}\frac{n!}{k!} = n!\sum_{k=0}^{n}(-1)^k\frac{1}{k!}.$$

Iskana verjetnost je tako enaka alternirajoči vsoti

$$\sum_{k=0}^{n}(-1)^k\frac{1}{k!},$$

kar je za dovolj velike n približno enako $e^{-1} \approx 0{,}37$. ∎

16 Dirichletovo načelo in sorodni izreki

16.1 Dirichletovo načelo

Če razvrstimo n predmetov v več kot n škatel, bo vsaj ena od škatel vsebovala vsaj dva predmeta. To preprosto dejstvo imenujemo *Dirichletovo načelo*[2] Navedimo ga v nekoliko splošnejši obliki.

IZREK 16.1 *Če več kot kn objektov razporedimo v n škatel, potem bo v vsaj eni škatli več kot k objektov.*

Oglejmo si nekaj zgledov uporab Diricheltovega načela.

ZGLED. *Vsak človek ima na glavi največ sto tisoč las. V Sloveniji gotovo živi več kot milijon petsto tisoč ljudi. Dokažite, da v Sloveniji obstaja skupina desetih ljudi, ki imajo na glavi enako število las.*

V mislih razdelimo prebivalce Slovenije v 100.001 škatlo, pri čemer v i-to škatlo ($i = 0, 1, \ldots, 100.000$) uvrstimo vse tiste ljudi, ki imajo natanko i las na glavi. Ker je vseh prebivalcev Slovenije več kot $10 \cdot 100.001$, nam osnovna oblika Dirichletovega načela pravi, da obstaja škatla, v kateri je več kot 10 ljudi (vstavi $k = 10$, $n = 100.001$). Seveda imajo vsi ljudje v tej škatli enako število las na glavi. ∎

Veliko nalog o deljivosti razlik celih števil lahko prevedemo na Dirichletovo načelo, če upoštevamo dejstvo, da je razlika dveh celih števil deljiva z danim naravnim številom m, če in samo če dasta pri deljenju z m enak *ostanek*. Če se zavedamo, da je ostanek pri deljenju z m lahko le eno od m števil $0, 1, \ldots, m-1$, zlahka rešimo naslednjo nalogo:

ZGLED. *Med* 101 *celim številom vedno lahko najdemo dve, katerih razlika je deljiva s* 100.

Mislimo si, da imamo na razpolago 100 škatel, ki jih označimo s števili $0, 1, \ldots, 99$. Danih 101 števil razporedimo v teh 100 škatel, pri čemer število x razvrstimo v škatlo i, če in samo če je ostanek števila x pri deljenju s 100 enak i. Ker je števil, ki jih razvrščamo, več, kot je škatel, nam Dirichletovo načelo pravi, da obstaja škatla z vsaj dvemi števili. Razlika teh dveh števil je seveda deljiva s 100. ∎

[2]Johann Dirichlet (1805–1859), nemški matematik, utemeljitelj modernega koncepta funkcije. V angleško govorečih deželah tukaj opisano Diricheltovo načelo imenujejo tudi *načelo golobnjaka* (ang. *pigeonhole principle*). S tem se izognejo zamenjavi s pomembnim izrekom iz analize, ki prav tako nosi ime Dirichletovo načelo.

ZGLED. *Pobarvajmo vsak kvadratek neskončnega karirastega lista papirja z eno od desetih barv. Dokaži, da obstajajo štirje enako pobarvani kvadratki, katerih središča so oglišča pravokotnika s stranicami, ki so vzporedne črtam karirastega papirja.*

Oglejmo si pas karirastega papirja višine 11 kvadratkov. Po Dirichletovem principu morata biti v vsakem stolpcu pasu vsaj dve polji pobarvani enako. Stolpec je lahko pobarvan na 10^{11} načinov. Če pogledamo znotraj pasu poljubnih $10^{11} + 1$ stolpcev, morata biti vsaj dva pobarvana popolnoma enako. V teh dveh stolpcih vzemimo po dva enako pobarvana kvadratka. Dobili smo zahtevane 4 enako pobarvane kvadratke. ∎

16.2 Ramseyev izrek

Dirichletovemu načelu soroden izrek je tako imenovani *Ramseyjev izrek*. Za motivacijo navedimo naslednje zanimivo dejstvo.

TRDITEV 16.2 *Če se neke zabave udeleži vsaj šest ljudi, tedaj bomo med njemi lahko našli bodisi skupino treh, ki se med seboj vzajemno poznajo (vsak iz trojice pozna vsakega drugega iz trojice) bodisi vzajemno ne poznajo (nihče iz trojice ne pozna nikogar drugega iz trojice).*

Preden trditev dokažemo, jo prevedimo v jeziku grafov. Naj bo G graf in $K \subseteq V(G)$. Če sta poljubni dve točki množice K v grafu G sosednji, pravimo, da je K *klika* grafa G. Množica K je *antiklika* (tudi *neodvisna množica*) grafa G, če nobeni dve točki iz K v grafu G nista sosednji. Zgornjo trditev sedaj lahko povemo takole:

TRDITEV 16.3 *Vsak graf z vsaj šestimi točkami premore vsebuje kliko moči* 3 *ali pa antikliko moči* 3.

DOKAZ: Naj ima graf G vsaj 6 točk. Denimo, da graf G ne premore niti klike niti antiklike velikosti 3. Potem seveda niti komplementarni graf G^C ne premore niti klike niti antiklike velikosti 3. Naj bo u poljubna točka grafa G in $G(u)$ soseščina točke u. Če bi v $G(u)$ obstajali dve sosednji točki, bi le-ti skupaj z u tvorile kliko velikosti 3. To pa pomeni, da točke v množici $G(u)$ tvorijo antikliko. Ker graf ne premore antiklik moči 3, vsebuje soseščina poljubne točke grafa G največ dve točki. Z drugimi besedami, stopnja vsake točke grafa G je največ 2. Ker pa ima graf G vsaj 6 točk, je stopnja vsake točke v komplementarnem grafu G^C vsaj 3. To pa ravno

dokazanem pomeni, da vsebuje graf G^C bodisi kliko bodisi antikliko velikosti 3, kar je protislovje z začetno predpostavko. ■

Pravkar dokazno trditev posploši naslednji znameniti *Ramseyjev izrek*.

IZREK 16.4 *Za poljubni naravni števili k in l obstaja najmanjše takšno naravno število $n = r(k,l)$, za katerega velja naslednje: Vsak graf z vsaj n točkami premore bodisi kliko velikosti k bodisi antikliko velikosti l.*

Števila $r(k,l)$ imenujemo *Ramseyjeva števila*. Ramseyjev izrek nam sicer zagotavlja obstoj takšnih števil, na daje pa nam nobenega praktičnega napotka, kako jih računati. Problem računanja Ramseyjevih števil zelo težak že pri majhnih vrednostih števil k in l. Če želimo dokazati, da je Ramseyjevo število $r(k,l)$ enako n, moramo v resnici dva problema. Najprej moramo dokazati, da vsak graf z vsaj n točkami premore bodisi kliko velikosti k bodisi antikliko velikosti l. S tem dokažemo neenakost $n \geq r(k,l)$. Nato pa moramo najti graf na $n-1$ točkah, ki ne premore niti klike velikosti k niti antiklike velikosti l. S tem dokažemo še $n \leq r(k,l)$.

Brez dokaza navedimo naslednje enakosti in neenakosti:

$$\begin{aligned}
r(k,l) &= r(l,k) \\
r(1,l) &= r(k,1) = 1 \\
r(k,2) &= k \\
r(k,l) &\leq r(k-1,l) + r(k,l-1)\,, \\
r(k,l) &\leq \binom{k+l-2}{k-1}\,, \\
r(k,k) &\geq 2^{\frac{k}{2}} \text{ za } k > 1\,.
\end{aligned}$$

ZGLED. *Dokaži, da je $r(3,3) = 6$.*

Neenakost $r(3,3) \leq 6$ sledi iz Trditve 16.3. Za dokaz neenakosti $r(3,3) \geq 6$ moramo poiskati graf na petih točkah, ki ne premore niti klike niti antiklike moči 3. Tak graf je, na primer, cikel dolžine 5. ■

Omenimo še, da lahko Ramseyjev izrek izrazimo tudi z barvanjem povezav polnega grafa. Če namreč povezave polnega grafa na $r(k,l)$ točkah pobarvamo z dvema barvama, denimo rdečo in modro, bomo gotovo našli bodisi polni graf moči k s samimi rdečimi povezavami bodisi polni podgraf moči l s samimi modrimi povezavami.

Literatura

[1] V. Batagelj: *Kombinatorika*, samozaložba, Ljubljana, 1997.

[2] V. Batagelj, S. Klavžar: *DS2, algebra in teorija grafov, naloge*, DMFAS, Ljubljana, 1992.

[3] M. Juvan, P. Potočnik: *Kombinatorika s teorijo grafov: primeri in rešene naloge*, DMFAS, Ljubljana, 2000.

vir6 D. Veljan: Kombinatorika s teorijom grafova Školska knjiga, Zagreb, 1989

[4] R. J. Wilson, J. J. Watkins: *Uvod v teorijo grafov*, DMFAS, Ljubljana, 1997.