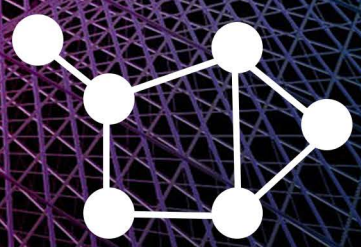
Univerzitetna založba
Univerze v Mariboru

Iztok Peterin

DISKRETNE strukture



Univerza v Mariboru

Fakulteta za elektrotehniko,
računalništvo in informatiko

Diskretne strukture

Avtor
Iztok Peterin

Oktober 2020

Naslov **Diskretne strukture**
Title *Discrete Structures*

Avtor Iztok Peterin
Author (Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko)

Recenzija Aleksandra Tepeh
Review (Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko)

Sandi Klavžar
(Univerza v Ljubljani, Fakulteta za matematiko in fiziko)

Tehnična urednika Iztok Peterin
Technical editors (Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko)

Jan Perša
(Univerza v Mariboru, Univerzitetna založba)

Oblikovanje ovitka Jan Perša
Cover designer (Univerza v Mariboru, Univerzitetna založba)

Grafika na ovitku Fractals avtorja joiom s pixabay.com
Cover graphics (CC0).

Grafične priloge Avtor
Graphic material

Založnik/*Published by*
Univerza v Mariboru
Univerzitetna založba
Slomškov trg 15, 2000 Maribor, Slovenija
https://press.um.si, zalozba@um.si

Izdajatelj/*Co-published by*
Univerza v Mariboru
Fakulteta za elektrotehniko, računalništvo in informatiko
Koroška cesta 46, 2000 Maribor, Slovenija
https://www.feri.um.si, feri@um.si

Izdaja Prva izdaja
Edition

Izdano Maribor, oktober 2020
Published at

Vrsta publikacije E-knjiga
Publication type

Dostopno na https://press.um.si/index.php/ump/catalog/book/512
Available at

CIP - Kataložni zapis o publikaciji
Univerzitetna knjižnica Maribor

510(075.8)

PETERIN, Iztok
Diskretne strukture [Elektronski vir] / avtor Iztok Peterin. - 1. izd. - E-učbenik. - Maribor : Univerzitetna založba Univerze, 2020

Način dostopa (URL):
https://press.um.si/index.php/ump/catalog/book/512
ISBN 978-961-286-400-2
doi: doi.org/10.18690/978-961-286-400-2
COBISS.SI-ID 34068995

ISBN 978-961-286-400-2 (pdf)

DOI https://doi.org/10.18690/978-961-286-400-2

Cena Brezplačni izvod
Price

Odgovorna oseba založnika prof. dr. Zdravko Kačič,
For publisher rektor Univerze v Mariboru

KAZALO

Predgovor

Pred vami je učbenik za predmet Diskretne strukture, ki se izvaja v prvem semestru študijskih smeri RIT-UNI in ITK-UNI na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Za njegovo uporabo ni potrebno globoko predznanje iz matematike. Znanje pridobljeno v srednjih šolah v Sloveniji zadošča.

Diskretne strukture obsegajo širok del matematike in so sestavljene iz veliko področij, prav vsa med njimi igrajo pomembno vlogo v računalništvu. V učbeniku so predstavljena le tista področja, ki jih predelamo tudi na predavanjih. Med njimi ima zagotovo temeljno vlogo logika in z njo tudi njen najpomembnejši igralec, dokaz, brez katerega v matematiki enostavno ne gre. Nato spoznamo matematično indukcijo in njeno razširjeno verzijo, induktivno posplošitev, ki je zelo koristna pri analizi algoritmov. Štetje objektov oziroma kombinatorika je temelj matematike, ne zgolj diskretnih struktur in o tem bomo govorili v tretjem poglavju. Sledi poglavje o rekurzivnih relacijah, s katerimi lahko pogosto preštejemo število potrebnih operacij, da se izvrši kak algoritem. Prav s številom operacij izvršenih v algoritmu lahko vrednotimo algoritme po hitrosti, kar je tema petega poglavja. Sledi poglavje o teoriji števil. Bolje povedano, o uvodu v teorijo števil, ki je osnova za v današnjem računalništvu vseprisotno kriptografijo (kodiranje in dekodiranje). Sedmo poglavje predstavi relacije, ki jih lahko lepo predstavimo v računalniku, čemur je posvečen poseben razdelek. Postavimo tudi temelje za osmo poglavje, ki ga končamo s strukturo Booleovo algebro, ki poraja diskretni ekvivalent krogle. Zaključimo s poglavjem o grafih, ki predstavljajo neverjetno uporaben model za raznovrstne situacije iz realnega sveta.

Učbenik je napisan v tradicionalnem slogu, ki je morda nekoliko zahtevnejši za branje. Ta izbira je namerna, saj je študij najbolj učinkovit, če vanj vložimo dovolj napora. Po drugi strani je razširjen z veliko zgledi in nalogami, ki so pogosto podrobno razloženi in omogočajo lažje razumevanje prej predstavljenih teoretičnih pojmov.

V uvodu vsakega poglavja je tudi notica o literaturi. Ob tem, ko se da veliko reči najti na spletu, je večji poudarek na obstoječi literaturi v slovenščini.

Za konec omenimo nekatere osnovne pojme iz področja teorije množic, ki jih kasneje ne bomo posebej omenjali v tekstu in se pričakuje, da so bralcu že znani. Le-ti so naslednji:

- unija množic $A \cup B = \{x : x \in A \vee x \in B\}$,
- presek množic $A \cap B = \{x : x \in A \wedge x \in B\}$,
- razlika množic $A - B = \{x : x \in A \wedge x \notin B\}$,
- kartezični produkt množic $A \times B = \{(a, b) : a \in A \wedge b \in B\}$,

- moč množice A, ki predstavlja število elementov, ki se nahajajo v množici A in jo označimo z $|A|$ in
- potenčna množica $\mathcal{P}(A)$ množice A, ki vsebuje vse podmnožice množice A.

Omenimo še posebni oznaki dveh podmnožic, ki ju bomo pogosto uporabljali. To sta

- $[n] = \{1, \ldots, n\}$, ki predstavlja vsa naravna števila od 1 do n, in
- $[n]_0 = \{0, 1, \ldots, n\}$, kjer zgornji množici priključimo še število 0.

Zadnjo oznako prilagotimo tudi za vsa naravna števila. Tako $\mathbb{N}_0$ predstavlja množico vseh naravnih števil skupaj s številom nič.

Nekajkrat bomo uporabili pojem injektivne, surjektivne oziroma bijektivne preslikave. Naj bo $f : X \to Y$ preslikava. Potem je preslikava f injektivna, če se v vsak $y \in Y$ preslika največ en $x \in X$. Povedano drugače, če je $x_1 \neq x_2$, potem je $f(x_1) \neq f(x_2)$. Preslikava f je surjektivna, če se v vsak $y \in Y$ preslika vsaj en $x \in X$. Preslikavi, ki je injektivna in surjektivna hkrati, rečemo bijektivna. Torej je f bijektivna, če se v vsak $y \in Y$ preslika natanko en $x \in X$. Ker s predpisom f preslikamo vsak $x \in X$, to že prinese za nas najpomembnejšo lastnost bijekcij: obstoj bijekcije $f : X \to Y$ med končnima množicama X in Y pomeni, da imata X in Y enako moč.

Iz srednješolske matematike bomo nekajkrat uporabili tudi adicijska izreka za kotni funkciji sinus in kosinus, ki sta

- $\sin(x + y) = \sin x \cos y + \sin y \cos x$ in
- $\cos(x + y) = \cos x \cos y - \sin x \sin y$.

1

IZJAVNI RAČUN IN DOKAZOVANJE

V tem poglavju bomo spoznali izjavni račun, ki je pomembna osnova za matematične teorije. Kot vsaka hiša, tudi matematične teorije stojijo na temeljih, ki jim v matematiki rečemo aksiomi. Ko si aksiome določimo, v njihovo resničnost ne dvomimo več, lahko pa iz njih izpeljemo različne rezultate, ki jih v matematiki poimenujemo izreki, trditve, leme, posledice in podobno. Omenjena izpeljava predstavlja osnovo za vso matematiko in ji rečemo dokaz. S pomočjo dokazov gradimo omenjene izreke, trditve in podobno iz aksiomov, iz teh dokazanih izrekov in trditev pa z novimi dokazi utemeljimo resničnost novih izrekov, trditev in podobno. S tem seveda nadaljujemo in če je teorija dovolj bogata—in le-take nas običajno zanimajo—je ta proces neskončen.

Kaj je torej dokaz? Pri odgovoru na to vprašanje moramo biti zelo previdni, saj je eno matematični dokaz, ki ne pušča nobenih dvomov. Pogosto je po drugi strani slišati v politiki, v medijih, na sodiščih, da je nekdo dokazal kakšno tezo. Dovolite, da to dilemo poskusim razložiti s pomočjo angleškega jezika, kjer imajo dva termina za naš dokaz. Matematičnemu dokazu rečejo *proof*, medtem ko "dokazom" iz prej naštetih (in tudi drugih) življenjskih situacij rečejo *evidence*. Ob tem je zanimiva interpretacija Googlovega prevajalnika, ki *proof* prevede v dokaz, *evidence* pa v dokazi, torej množino. Na to ne moremo pristati, saj je lahko več različnih matematičnih dokazov za isti rezultat. Po drugi strani pa je tudi en sam (matematični) dokaz dovolj, da je rezultat, ki je z njim dokazan, resničen.

Tako bi v realnem življenju bilo precej bolj smiselno uporabljati izraz "izpostavili smo en namig, da je omenjena trditev resnična", dokazi pa naj ostanejo v domeni matematikov in matematike. Seveda se bomo v tem delu posvečali matematičnim dokazom, ki pa pogosto, resnici na ljubo, niso preveč priljubljeni med študenti.

Dodatno literaturo v slovenščini iz tega področja je moč najti v [3, 7]. V angleškem jeziku je na voljo precej več primerne literature, tukaj omenimo le [6]. Marsikaj je najti tudi na spletu in pogosto je že Wikipedia (angleška) dober začetni vir informacij. Standardna zbirka nalog za to poglavje je [4]. Veliko izpitnih nalog iz tega poglavja je najti v [12, 13].

1.1 IZJAVE IN IZJAVNE POVEZAVE

Izjava je poved oziroma trditev, ki je resnična ali neresnična, vendar ne oboje hkrati. Za resnične izjave uporabljamo tudi termin pravilna, medtem ko neresničnim izjavam rečemo tudi nepravilne. **Vrednost izjave** je resničnost ali neresničnost izjave. Pogosto vrednost izjave označimo z 1, če je izjava resnična, in z 0, če je izjava neresnična.

Zgled 1.1 *Oglejmo si naslednje povedi s stališča izjav, kot tudi njihove pravilnosti oziroma nepravilnosti.*

(I) *Danes je četrtek.*

(II) *Vsi delitelji števila 9 so 1,3 in 9.*

(III) *Obstaja neskončno mnogo naravnih števil.*

(IV) *Zemlja je edini naseljeni planet v vesolju.*

(V) *Pojdi v trgovino po kruh!*

(VI) *Koliko je ura?*

Povedi od (i)-(iv) predstavljajo izjave, medtem ko povedi (v) in (vi) nista izjavi. Izjava (v) je velelna poved in izjava (vi) je vprašalna poved in takšne povedi niso izjave. Izjava (i) je resnična zgolj ob četrtkih, sicer pa je neresnična in je zato odvisna od dneva v tednu. Izjava (ii) se zdi resnična na prvi pogled, vendar je ponovno odvisna od dodatnega pogoja. Kot bomo videli v poglavju 6 lahko definiramo deljivost na množici celih števil. V tem primeru so delitelji števila 9 tudi $-1, -3$ *in* -9 *in je trditev neresnična. Če pa se omejimo na naravna števila, potem je izjava (ii) resnična. Glede izjave (iii) ni dvomov in je resnična. Za izjavo (iv) še nimamo odgovora ali je resnična ali neresnična, saj do sedaj ne vemo dovolj o vesolju.*

Izjave označujemo z majhnimi in tudi velikimi črkami. Izjava je **enostavna**, če govori le o eni zadevi. Izjave, ki niso enostavne, so **sestavljene**. V slovnici lahko potegnemo vzporednico med enostavnimi izjavami in enostavčnimi povedmi ter med sestavljenimi izjavami in večstavčnimi povedmi. Vendar moramo biti pri tem previdni, saj so lahko tudi enostavne povedi sestavljene izjave, kar pa je pogosto odvisno od konteksta. Tako velja biti previden pri različnih naštevanjih. Oglejmo si nasledno izjavo

V trgovini sem kupil kruh, mleko in sladkor.

Ta izjava je lahko enostavna, če je pomembno zgolj, da je bil opravljen nakup v trgovini. Lahko pa je tudi sestavljena, če je pomembno, kaj je bilo v nakupu.

Sestavljene izjave so sestavljene iz več enostavnih, ki so med seboj povezane z **izjavnimi povezavami** ali **logičnimi operatorji**. Poznamo naslednj izjavne povezave: **negacijo**, **in**, **ali**, **implikacijo**, **ekvivalenco**, **ekskluzivni ali**, **nein** ter **neali**. Definirajmo jih bolj natančno.

- **Negacijo** izjave a označimo z $\neg a$, kar preberemo z ne a. Izjava $\neg a$ je resnična takrat, ko je izjava a neresnična, in obratno, $\neg a$ je neresnična takrat, ko je a resnična.

- **In** ali **konjunkcijo** izjav a in b označimo z $a \wedge b$, kar preberemo z a in b. Izjava $a \wedge b$ je resnična takrat, ko sta obe izjavi a in b resnični, in neresnična sicer.

- **Ali** ali **disjunkcijo** izjav a in b označimo z $a \vee b$, kar preberemo z a ali b. Izjava $a \vee b$ je neresnična takrat, ko sta obe a in b neresnični, in resnična sicer.

- Z $a \Rightarrow b$ označimo **implikacijo** iz izjave a v izjavo b, kar preberemo iz a sledi b, ali celo bolj pogosto, če a, potem b. Izjava $a \Rightarrow b$ je neresnična, če je a resnična izjava in b neresnična izjava, in resnična sicer.

- **Ekvivalenco** izjav a in b označimo z $a \Leftrightarrow b$, kar preberemo izjava a je ekvivalentna izjavi b, ali bolj pogosto, izjava a natanko tedaj, ko izjava b. Izjava $a \Leftrightarrow b$ je resnična, če imata obe izjavi a in b enako vrednost, kar pomeni da sta ali obe resnični ali obe neresnični. Če imata izjavi a in b različni vrednosti, je ekvivalenca neresnična.

- **Ekskluzivni ali** ali **XOR** izjav a in b označimo z $a \veebar b$, kar preberemo ali izjava a ali izjava b. Izjava $a \veebar b$ je resnična, če imata izjavi a in b različno vrednost. Če imata izjavi a in b enaki vrednosti, potem je $a \veebar b$ neresnična.

- **Nein** ali **NAND** izjav a in b označimo z $a \uparrow b$, kar preberemo izjava a ne in izjava b. Izjava $a \uparrow b$ je neresnična, če sta resnični obe a in b, ter resnična sicer.

- **Neali** ali **NOR** izjav a in b označimo z $a \downarrow b$, kar preberemo izjava a ne ali izjava b. Izjava $a \downarrow b$ je resnična, če sta neresnični obe a in b, ter neresnična sicer.

Iz definicij izjavnih povezav lahko hitro razberemo nekatere lastnosti. Tako zlahka uvidimo, da je **nein** negacija od **in**, kot je jasno že iz imena. Podobno je tudi **neali** negacija od **ali** kot tudi **ekskluzivni ali**, ki je negacija od **ekvivalence**. Prav tako se **negacija** razlikuje od preostalih izjavnih povezav, saj deluje na le eni izjavi, preostale izjavne povezave pa delujejo med dvema izjavama. Omenimo še, da imena **XOR**, **NAND** ter **NOR** izhajajo iz angleščine, tukaj jih omenjamo, ker so to kar ukazi v programskih jezikih za te izjavne povezave.

Posebej si oglejmo še implikacijo, ki pogosto predstavlja največje težave pri razumevanju. Iz njene definicije sledi, da je implikacija $a \Rightarrow b$ resnična, če je njen prvi del, torej a, neresničen. To si lahko predstavljamo tako, da če pogoj a ni izpolnjen, potem je celotna implikacija resnična, če pa je pogoj a izpolnjen, potem mora biti tudi drugi del implikacije, torej b, resničen, da je resnična celotna

implikacija $a \Rightarrow b$. To se sklada tudi s pogojnim stavkom (to je IF stavek) iz računalništva, ki je točno opisan z implikacijo.

Pogosto si je definicije izjavnih povezav težko zapomniti, če so zapisane z besedami. Zato si pri izjavah pomagamo s **pravilnostno tabelo**, ki vsebuje vse možne nabore enostavnih izjav, ki nastopajo v izjavi, s katero imamo opravka. Tako prioritetno tabelo za negacijo sestavljata zgolj dve vrstici in je

a	$\neg a$
0	1
1	0

Negacijo sestavlja zgolj ena enostavna izjava in le-ta lahko ima dve različni vrednosti, 0 in 1. Pravilnostna tabela se poveča, če je govora o ostalih izjavnih povezavah. V njih vedno nastopata dve enostavni izjavi, kar pomeni štiri različne možnosti. Pravilnostna tabela zanje je naslednja:

a	b	$a \wedge b$	$a \vee b$	$a \Rightarrow b$	$a \Leftrightarrow b$	$a \veebar b$	$a \uparrow b$	$a \downarrow b$
0	0	0	0	1	1	0	1	1
0	1	0	1	1	0	1	1	0
1	0	0	1	0	0	1	1	0
1	1	1	1	1	1	0	0	0

Z večanjem števila enostavnih izjav, se veča tudi število vrstic pravilnostne tabele. Tako imamo pri treh enostavnih izjavah že osem vrstic pravilnostne tabele, pri štirih enostavnih izjavah 16 vrstic pravilnostne tabele in tako naprej. Ni težko videti, da imamo pri k enostavnih izjavah 2^k vrstic v pravilnostni tabeli (kako preštejemo število vrstic pravilnostne tabele in še več, se bomo naučili v tretjem poglavju o kombinatoriki). Že pri majhnem k je to zelo veliko število. Za $k = 10$ enostavnih izjav tako dobimo 1024 vrstic pravilnostne tabele (takšnemu naraščanju bomo v petem poglavju, kjer bo govora o hitrosti algoritmov, rekli eksponentno). Seveda je to preveč za pisanje na papir in tudi računalniki ne zmorejo tako hitrega naraščanja. Tako lahko ugotovimo, da je pravilnostna tabela uporabna le v majhnih primerih. To pravzaprav ni presenetljivo, saj pravilnostna tabela pregleda vse možnosti, ki so na razpolago in tega je običajno preveč. V nadaljevanju tega poglavja (v tretjem razdelku) bomo spoznali metode, ki se izognejo pravilnostni tabeli.

Kadar je sestavljena izjava povezana z več izjavnimi povezavami, je potrebno paziti na prioriteto izjavnih povezav. To je podobno kot pri računskih operacijah krat in plus, kjer ima krat prednost pred plusom, če imamo račun brez oklepajev. Višja prioriteta izjavnih povezav je razvidna iz višjega položaja v naslednji shemi, ki ji rečemo **prioritetna tabela**:

$$\begin{array}{c}\neg\\ \wedge,\uparrow,\downarrow\\ \vee,\veebar\\ \Rightarrow\\ \Leftrightarrow\end{array}$$

Zgled 1.2 *Oglejmo si uporabo prioritetne tabele na primeru sestavljene izjave* $p \wedge \neg q \Rightarrow r \Leftrightarrow \neg p \vee r$. *Če jo opremimo z oklepaji, da poudarimo prednost operacij, dobimo* $((p \wedge (\neg q)) \Rightarrow r) \Leftrightarrow ((\neg p) \vee r)$. *Ponazorimo to izjavo tudi s pravilnostno tabelo.*

Omenimo, da števila v najvišji vrstici pravilnostne tabele predstavljajo vrstni red glede na prioriteto oziroma oklepaje. Tako je končna vrednost izjave predstavljena v stolpiču, ki je označen s številko 6 in je krepko odtisnjen. Ekvivalenco v stolpiču 6 *gledamo med stolpcem* 3 *na levi in stolpcem* 5 *na desni. To sta najvišje označena stolpca na vsaki strani.*

				2	1	3		6	4	5	
p	q	r	p	$\wedge$	$\neg q$	$\Rightarrow$	r	$\Leftrightarrow$	$\neg p$	$\vee$	r
0	0	0	0	0	1	1	0	**1**	1	1	0
0	0	1	0	0	1	1	1	**1**	1	1	1
0	1	0	0	0	0	1	0	**1**	1	1	0
0	1	1	0	0	0	1	1	**1**	1	1	1
1	0	0	1	1	1	0	0	**1**	0	0	0
1	0	1	1	1	1	1	1	**1**	0	1	1
1	1	0	1	0	0	1	0	**0**	0	0	0
1	1	1	1	0	0	1	1	**1**	0	1	1

.

Zlahka opazimo, da je v recimo drugi vrstici prioritetne tabele več izjavnih povezav. To pomeni, da prioriteta med njimi ni natančno določena. V takem primeru ima prednost tista izjavna povezava, ki je na levi. Tako za izjavo $p \uparrow q \wedge r \downarrow t$ velja vrstni red $((p \uparrow q) \wedge r) \downarrow t$, kjer prioriteto določajo oklepaji.

Posebno vlogo med sestavljenimi izjavami igrajo tiste, ki so resnične ob vsakem naboru enostavnih izjav. Rečemo jim **tavtologije** in jih označimo z 1. Podobno sestavljeno izjavo, ki je neresnična pri vsakem naboru enostavnh izjav, poimenujemo **laž** in jo označimo z 0. Izjava, ki ni ne tavtologija ne laž, je **nevtralna izjava**. Izjava iz zgleda 1.2 je nevtralna, saj ima v sedmih naborih enostavnih izjav vrednost 1, v enem naboru enostavnih izjav pa ima vrednost 0.

Zgled 1.3 *S pravilnostno tabelo pokažimo, da je izjava* $p \wedge (p \Rightarrow q) \Rightarrow q$ *tavtologija. Ponovno števila v zgornji vrstici predstavljajo vrstni red operacij, končni rezultat pa je odtisnjen v krepkem načinu.*

			2		1		3	
p	q	p	$\wedge$	$(p$	$\Rightarrow$	$q)$	$\Rightarrow$	q
0	0	0	0	0	1	0	**1**	0
0	1	0	0	0	1	1	**1**	1
1	0	1	0	1	0	0	**1**	0
1	1	1	1	1	1	1	**1**	1

1.2 ENAKOVREDNOST IZJAV IN IZBRANA OBLIKA

Naj bosta izjavi A in B sestavljeni iz istih enostavnih izjav. Rečemo, da sta A in B **enakovredni**, če imata pri vsakem naboru enostavnih izjav enako vrednost. V tem primeru uporabljamo oznako

$$A \sim B.$$

Enakovrednost izjav lahko pokažemo s pravilnostno tabelo, ki pa je uporabna le, če je število nastopajočih enostavnih izjav dovolj majhno. Kadar je število enostavnih izjav preveliko, poskušamo sestavljeno izjavo poenostaviti ali preoblikovati. Pri tem uporabljamo enakovredne izjave, ki vsebujejo manj enostavnih izjav in jih je moč dokazati s pravilnostno tabelo.

V nadaljevanju bomo predstavili kar nekaj enakovrednih izjav razdeljenih v nekaj sklopov. Začnemo s primeri kako laž in tavtologija vplivata na izjave. Te lastnosti so pogosto uporabne pri računanju z izjavami, kot bomo videli v naslednjem razdelku.

- $\neg 0 \sim 1$,
- $\neg 1 \sim 0$,
- $0 \vee p \sim p$,
- $0 \wedge p \sim 0$,
- $1 \vee p \sim 1$,
- $1 \wedge p \sim p$,
- $p \vee \neg p \sim 1$,
- $p \wedge \neg p \sim 0$.

V naslednji sklop enakovrednih izjav sodijo algebrajske lastnosti izjavnih povezav **in** in **ali**, ki bodo pomembno vlogo igrale v poglavju o Boolovih algebrah.

- $\neg(\neg p) \sim p$ **involucija negacije,**
- $p \wedge p \sim p$ **idempotentnost in,**
- $p \vee p \sim p$ **idempotentnost ali,**
- $p \wedge (p \vee q) \sim p$ **absorpcija,**
- $p \vee (p \wedge q) \sim p$ **absorpcija,**
- $p \wedge q \sim q \wedge p$ **komutativnost in,**
- $p \vee q \sim q \vee p$ **komutativnost ali,**
- $p \wedge (q \wedge r) \sim (p \wedge q) \wedge r$ **asociativnost in,**
- $p \vee (q \vee r) \sim (p \vee q) \vee r$ **asociativnost ali,**
- $p \wedge (q \vee r) \sim (p \wedge q) \vee (p \wedge r)$ **distributivnost,**
- $p \vee (q \wedge r) \sim (p \vee q) \wedge (p \vee r)$ **distributivnost.**

Lahko je opaziti, da zgornje lastnosti, z izjemo involucije, nastopajo v simetričnih parih glede na uporabo **in** in **ali**. V nadaljevanju ne bomo ločevali med eno in drugo lastnostjo v takem paru, saj je le ta razvidna iz uporabljene izjavne povezave. Tako bomo namesto, recimo, komutativnosti **in** oziroma komutativnosti **ali**, govorili zgolj o komutativnosti. Kot že omenjeno lahko vse te enakovrednosti zlahka pokažemo s pravilnostno tabelo. Tukaj si oglejmo le kako je z distributivnostjo, resničnost preostalih pa prepuščamo za vajo.

				2		1				3		5		4	
p	q	r	p	$\wedge$	$(q$	$\vee$	$r)$	$\sim$	$(p$	$\wedge$	$q)$	$\vee$	$(p$	$\wedge$	$r)$
0	0	0	0	**0**	0	0	0		0	0	0	**0**	0	0	0
0	0	1	0	**0**	0	1	1		0	0	0	**0**	0	0	1
0	1	0	0	**0**	1	1	0		0	0	1	**0**	0	0	0
0	1	1	0	**0**	1	1	1		0	0	1	**0**	0	0	1
1	0	0	1	**0**	0	0	0		1	0	0	**0**	1	0	0
1	0	1	1	**1**	0	1	1		1	0	0	**1**	1	1	1
1	1	0	1	**1**	1	1	0		1	1	1	**1**	1	0	0
1	1	1	1	**1**	1	1	1		1	1	1	**1**	1	1	1

Omenimo, da števila v prvi vrstici predstavljajo vrstni red izvedenih operacij glede na prioriteto, določeno z oklepaji. Iz tabele je razvidno, da sta odebeljena stolpca pod številkama 2 in 5, ki predstavljata izjavi na desni oziroma levi, enaka, kar pomeni, da je izjava na levi enakovredna izjavi na desni (in obratno).

Sledita **De Morganova zakona**,[1] ki omogočata prenos **negacije** neposredno pred enostavno izjavo in prav tako nastopata v simetričnem paru.

- $\neg(p \wedge q) \sim \neg p \vee \neg q$,
- $\neg(p \vee q) \sim \neg p \wedge \neg q$.

Zaradi pomembnosti De Morganovih zakonov ju dokažimo s pravilnostno tabelo.

		2		1			3	5	4	7		6			8	10	9
p	q	$\neg($	p	$\wedge$	$q)$	$\sim$	$\neg p$	$\vee$	$\neg q$	$\neg($	p	$\vee$	$q)$	$\sim$	$\neg p$	$\wedge$	$\neg q$
0	0	**1**	0	0	0		1	**1**	1	**1**	0	0	0		1	**1**	1
0	1	**1**	0	0	1		1	**1**	0	**0**	0	1	1		1	**0**	0
1	0	**1**	1	0	0		0	**1**	1	**0**	1	1	0		0	**0**	1
1	1	**0**	1	1	1		0	**0**	0	**0**	1	1	1		0	**0**	0

Iz tabele ponovno razberemo, da sta odebeljena stolpca pod številkama 2 in 5 enaka, kar dokazuje prvi De Morganov zakon. Enaka sta tudi stolpca pod številkama 7 in 10, iz česar sledi drugi De Morganov zakon.

Posebej omenimo naslednjo enakovrednost

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

ki je znana kot **kontrapozicija** in jo bomo kasneje s pridom uporabljali.

Seznam enakovrednih izjav, ki jih omenjamo tukaj, zaključujemo z izražanjem preostalih izjavnih povezav z **negacijo**, **in** in **ali**.

- $p \Rightarrow q \sim \neg p \vee q$,
- $p \uparrow q \sim \neg(p \wedge q)$,
- $p \downarrow q \sim \neg(p \vee q)$,
- $p \Leftrightarrow q \sim (p \Rightarrow q) \wedge (q \Rightarrow p) \sim (\neg p \vee q) \wedge (\neg q \vee p)$,
- $p \veebar q \sim \neg(p \Leftrightarrow q) \sim \neg((\neg p \vee q) \wedge (\neg q \vee p))$.

1 Augustus De Morgan (1806-1871) je bil angleški matematik, ki je znan predvsem po omenjenih zakonih in po formalizaciji matematične indukcije.

Iz zadnjega sklopa je razvidno, da lahko vse izjavne povezave izrazimo zgolj z **negacijo**, **in** in **ali**. Storimo pa lahko še več. S pomočjo De Morganovih zakonov lahko negacijo vedno zapišemo neposredno pred enostavno izjavo. To je že narejeno za **implikacijo** in **ekvivalenco**, pokažimo še za **nein**, **neali** in **ekskluzivni ali**:

- $p \uparrow q \sim \neg p \vee \neg q$,
- $p \downarrow q \sim \neg p \wedge \neg q$,
- $p \veebar q \sim \neg((\neg p \vee q) \wedge (\neg q \vee p)) \sim \neg(\neg p \vee q) \vee \neg(\neg q \vee p) \sim$
  $\sim (p \wedge \neg q) \vee (q \wedge \neg p)$.

Zapisu sestavljene izjave, v katerem nastopajo le **negacija**, **in** in **ali** in ob tem negacije nastopajo le neposredno pred enostavnimi izjavami, rečemo **izbrana oblika** zapisa izjave.

Množica ali nabor izjavnih povezav je **poln**, če lahko vsako izjavo zapišemo kot enakovredno izjavo le z izjavnimi povezavami iz tega nabora. Seveda je nabor $\{\neg, \wedge, \vee\}$ poln, kot smo že videli. Le to nam omogoča krajše preverjanje za ostale nabore, ali so polni. Z izjavami iz nabora moramo izraziti le **negacijo**, **in** in **ali**, z njimi pa lahko izrazimo vse preostale, kot že omenjeno.

Zgled 1.4 *Pokažimo, da je $\{\uparrow\}$ poln nabor. Za to nam zadošča, da izrazimo **negacijo**, **in** in **ali** z **nein**, saj smo že videli, da lahko vse preostale izjavne povezave izrazimo z njimi. Tako je:*

- $\neg p \sim \neg(p \wedge p) \sim p \uparrow p$,
- $p \wedge q \sim \neg(\neg(p \wedge q)) \sim \neg(p \uparrow q) \sim (p \uparrow q) \uparrow (p \uparrow q)$,
- $p \vee q \sim \neg(\neg(p \vee q)) \sim \neg(\neg p \wedge \neg q) \sim \neg((p \uparrow p) \wedge (q \uparrow q)) \sim$
  $\sim (p \uparrow p) \uparrow (q \uparrow q)$.

*Ob tem smo za **negacijo** uporabili idempotentnost ter definicijo **nein**. Za **in** smo najprej uporabili involucijo negacije, nato definicijo **nein** in na koncu izražanje **negacije** z **nein**, ki smo ga pokazali vrstico višje. Končno smo za **ali** uporabili involucijo negacije, De Morganov zakon, izražanje **negacije** z **nein** (dvakrat) in definicijo **nein**.*

Zgled 1.5 *Pokažimo, da $\{\vee, \wedge, \Rightarrow\}$ ni poln nabor. To vidimo iz razmisleka, da je sestavljena izjava, ki vsebuje le **ali**, **in** ter **implikacijo**, vedno resnična, če imajo vse enostavne izjave vrednost 1. Tako z njimi ne moremo izraziti recimo **negacije** ali **nein**.*

1.3 DOKAZOVANJE OZIROMA SKLEPANJE

Izjava B je **logična posledica** izjav $A_1, \ldots, A_k$, če iz resničnosti izjav $A_1, \ldots, A_k$ sledi resničnost izjave B.

Sklep sestavljajo predpostavke $A_1, \ldots, A_k$ in zaključek B, kar lahko shematično predstavimo na naslednji način:

$$\underbrace{A_1, \ldots, A_k}_{\text{predpostavke}} \qquad \underbrace{\vDash B}_{\text{zaključek}} .$$

Pogosto predpostavke označimo kar z množico $\mathcal{A} = \{A_1, \ldots, A_k\}$ in potem sklep zapišemo kot $\mathcal{A} \vDash B$. Sklep $\mathcal{A} \vDash B$ je **resničen** ali **veljaven**, če je zaključek B logična posledica predpostavk $\mathcal{A}$. Iz definicije logične posledice je razvidno, da pri veljavnosti sklepa pomembno vlogo igra implikacija, kar bo še posebej razvidno iz izreka 1.1. Pred tem si oglejmo dva zgleda, v katerih si bomo pomagali s pravilnostno tabelo.

Zgled 1.6 *Oglejmo si sklep, ki ga opisujeta naslednji povedi.*

Če je $2 = 3$, *potem grem plavati z morskimi psi.*

Plaval sem z morskimi psi, zato je $2 = 3$.

V primeru, ko je sklep podan s povedmi oziroma besedami, je najprej potrebno razbrati predpostavke in jih ločiti od zaključka sklepa. Prvo poved sestavlja implikacija, kjer iz enakosti $2 = 3$ *sledi plavanje z morskimi psi. Tako se zdi smiselno, da vpeljemo naslednji oznaki*

$$p \ldots 2 = 3 \text{ in } q \ldots \text{plavanje z morskim psom},$$

iz česar dobimo implikacijo $p \Rightarrow q$, *kar predstavlja prvo predpostavko našega sklepa. Tudi druga poved je sestavljena. V njej igra posebno vlogo beseda* ***zato***, *ki jasno nakazuje, da tisto kar ji sledi, izhaja iz prejšnjega dela povedi. Tako je prvi del druge povedi, ki je z dogovorjenimi oznakami kar* q, *druga predpostavka našega sklepa, medtem ko je* p, *ki sledi besedi zato, zaključek sklepa. Tako imamo*

1.	$p \Rightarrow q$	*predpostavka*
2.	q	*predpostavka*
$\vDash$	p	*zaključek.*

Pomagajmo si s pravilnostno tabelo:

p	q	$p \Rightarrow q$		q		$\vDash p$
0	0	1		0		0
0	1	1		1		0
1	0	0		0		1
1	1	1		1		1

Ker za veljavnost sklepa preverjamo, ali je zaključek p logična posledica prepostavk $p \Rightarrow q$ in q, nas v pravilnostni tabeli zanimajo zgolj tiste vrstice, v katerih sta obe predpostavki resnični. Seveda se to zgodi v drugi in četrti vrstici pravilnostne tabele. V četrti vrstici je tudi zaključek resničen, čemur pa ni tako v drugi vrstici. Tako imamo v drugi vrstici pravilnostne tabele obe predpostavki resnični, zaključek pa neresničen. Zaradi te vrstice zaključek ni logična posledica predpostavk in ta sklep ni resničen.

Zgled 1.7 *Tudi naslednji sklep opisujeta dve povedi.*

Če pingvini živijo na severnem tečaju, potem sonce ne vzhaja na vzhodu.

Sonce vzhaja na vzhodu, zato pingvinov ni na severnem tečaju.

Kot v prejšnjem zgledu zaradi lažjega zapisa vpeljimo naslednji oznaki

$p \ldots$ *pingvini so na severnem tečaju in* $s \ldots$ *sonce vzhaja na vzhodu.*

Prva poved je predpostavka, ki je z vpeljanima oznakama implikacija $p \Rightarrow \neg s$. Druga poved je ponovno sestavljena iz predpostavke (prvi del) in zaključka (drugi del za besedo zato). Tako je druga predpostavka tega sklepa v dogovorjenih oznakah kar s, medtem ko je $\neg p$ zaključek sklepa. Tako imamo

1.	$p \Rightarrow \neg s$	*predpostavka*
2.	s	*predpostavka* .
$\models$	$\neg p$	*zaključek*

Pomagajmo si s pravilnostno tabelo:

p	s	$p \Rightarrow \neg s$		s		$\models \neg p$
0	0	1		0		1
0	1	1		1		1
1	0	1		0		0
1	1	0		1		0

.

Ponovno za veljavnost sklepa preverjamo ali je zaključek $\neg p$ logična posledica prepostavk $p \Rightarrow \neg s$ in s. Zato nas v pravilnostni tabeli zanimajo zgolj tiste vrstice, v katerih sta obe predpostavki resnični. To se zgodi zgolj v drugi vrstici pravilnostne tabele. V tej vrstici je tudi zaključek $\neg p$ resničen, zato je zaključek $\neg p$ logična posledica predpostavk $p \Rightarrow \neg s$ in s in sklep je resničen.

Zgled 1.6 lahko izkoristimo, da ugotovimo, kdaj je sklep neresničen. Kot smo videli v omenjenem zgledu, za to zadošča ena vrstica pravilnostne tabele, za katero so predpostavke resnične, zaključek pa ne. Takemu naboru vrednosti enostavnih izjav rečemo **protiprimer**. Tako za neresničnost sklepa zadošča protiprimer, kar so takšne vrednosti nabora enostavnih izjav, da so vse predpostavke sklepa resnične, sam zaključek sklepa pa je neresničen.

Kot je razvidno iz zgornjih dveh zgledov, lahko pri ugotavljanju resničnosti uporabimo pravilnostno tabelo, vendar nas lahko to hitro privede v težave. Če je sklep zahtevnejši z več enostavnimi izjavami, je pravilnostna tabela enostavno prevelika, kot že omenjeno. Opazimo pa lahko tudi, da je uporaba pravilnostne tabele neekonomična tudi pri manjših primerih, saj pogosto za ugotavljanje resničnosti sklepa sploh ne potrebujemo vse pravilnostne tabele, pač pa zgolj tiste vrstice, za katere so vse predpostavke resnične. Zato se bomo sedaj posvetili metodi, ki se izogne pravilnostni tabeli in ji rečemo dokaz sklepa.

Dokaz izjave B ob predpostavkah $\mathcal{A} = \{A_1, \ldots, A_k\}$ je neko zaporedje izjav $B_1, \ldots, B_m$, kjer je $B_m \sim B$ in za vsak $i \in [m]$ velja ena izmed naslednjih alinej:

- ali je $B_i \sim A_j$, $j \in [k]$ (torej je B_i enakovreden neki predpostavki);
- ali je B_i tavtologija;
- ali je $B_i \sim B_j$ za nek $j < i$ (torej je B_i enakovreden kakšnemu izmed prejšnjih korakov dokaza);
- ali je B_i dobljen iz izjav $B_1, \ldots, B_{i-1}$ s pravilnim sklepom (torej je B_i dobljen iz prejšnjih korakov dokaza s pravilnim sklepom).

Dokaz je temeljni kamen celotne matematike kot jo razumemo danes in pomeni postopek, ki nas pripelje od predpostavk sklepa do zaključka sklepa brez možnosti dvoma. Ob tem sklep pogosto imenujemo kot izrek, ali trditev, ali lema ali kaj podobnega. Običajno je takšno poimenovanje povezano z zahtevnostjo oziroma pomembnostjo sklepa. Tako je za najpomembnejše sklepe rezerviran izraz IZREK. Temu sledijo TRDITVE, ki so po pomembnosti manjvredne od izrekov, a še vedno pomembne. LEMA običajno poimenujemo pomožne trditve, ki jih lahko uporabimo v dokazih pomembnejših izrekov oziroma trditev. Uporabljamo tudi izraz UGOTOVITEV za sklepe s preprostimi dokazi. Preproste dokaze imajo tudi POSLEDICE, ki predstavljajo sklepe, ki jih lahko dokažemo ob upoštevanju kakšnega zahtevnejšega izreka ali trditve.

Nadaljujemo z izrekom, ki nam bo omogočil orodje, s katerim bomo najprej upravičili tri alineje definicije dokaza. Nato bomo predstavili še nekaj lažjih sklepov, ki so uporabni za četrto alinejo iz definicije dokaza.

Izrek 1.1 *Na bo $\mathcal{A} = \{A_1, \ldots, A_k\}$ množica izjav. Sklep $\mathcal{A} \vDash B$ je resničen natanko tedaj, ko je implikacija $A_1 \wedge \cdots \wedge A_k \Rightarrow B$ tavtologija.*

Dokaz. Dokazati moramo ekvivalenco

$$(\mathcal{A} \vDash B) \Leftrightarrow (A_1 \wedge \cdots \wedge A_k \Rightarrow B \sim 1).$$

Ob tem upoštevajmo, da je ta ekvivalenca enakovredna zapisu z dvema implikacijama

$$((\mathcal{A} \vDash B) \Rightarrow (A_1 \wedge \cdots \wedge A_k \Rightarrow B \sim 1)) \wedge ((A_1 \wedge \cdots \wedge A_k \Rightarrow B \sim 1) \Rightarrow (\mathcal{A} \vDash B)).$$

Tako moramo dokazati obe implikaciji, ki ju običajno označimo kar z $(\Rightarrow)$ in $(\Leftarrow)$. Opazimo, da nimamo podanih nobenih predpostavk. Ker je implikacija $p \Rightarrow q$ resnična, če je $p \sim 0$, lahko predpostavimo, da je $p \sim 1$, kar je predpostavka pri dokazovanju implikacije. V tem primeru zadostuje, da pokažemo, da je tudi $q \sim 1$, saj je potem implikacija $p \Rightarrow q$ ponovno resnična. Tej vrsti sklepa bomo kmalu rekli pogojni sklep, glej izrek 1.4.

$(\Rightarrow)$ Torej začnimo z dokazom implikacije $(\mathcal{A} \vDash B) \Rightarrow (A_1 \wedge \cdots \wedge A_k \Rightarrow B \sim 1)$, kjer je predpostavka, da je sklep $\mathcal{A} \vDash B$ resničen. Če je $A_1 \wedge \cdots \wedge A_k \sim 0$, je implikacija $A_1 \wedge \cdots \wedge A_k \Rightarrow B$ avtomatično resnična. Zato naj bo $A_1 \wedge \cdots \wedge A_k \sim 1$. To pomeni, da je vsaka predpostavka A_i resnična, torej $A_i \sim 1$ za vsak $i \in [k]$. Ker je sklep $\mathcal{A} \vDash B$ resničen, to pomeni, da je tudi $B \sim 1$ in je implikacija $A_1 \wedge \cdots \wedge A_k \Rightarrow B$ tudi v tem primeru resnična. Skratka prva implikacija je resnična.

$(\Leftarrow)$ Oglejmo si še nasprotno implikacijo $(A_1 \wedge \cdots \wedge A_k \Rightarrow B \sim 1) \Rightarrow (\mathcal{A} \vDash B)$. Ponovno lahko predpostavimo, da je prvi del implikacije resničen, kar je $A_1 \wedge \cdots \wedge A_k \Rightarrow B \sim 1$. Pokažimo, da iz tega sledi tudi resničnost drugega dela implikacije $\mathcal{A} \vDash B$. Za pravilnost sklepa $\mathcal{A} \vDash B$ lahko predpostavimo, da so vse predpostavke resnične in je $A_i \sim 1$ za vsak $i \in [k]$. Torej je tudi $A_1 \wedge \cdots \wedge A_k \sim 1$. Ker velja tudi $A_1 \wedge \cdots \wedge A_k \Rightarrow B \sim 1$, kar je predpostavka, ugotovimo, da je $B \sim 1$, kar je zaključek sklepa. S tem je sklep resničen in nasprotna implikacija dokazana. ∎

Trditev 1.2 *Za množico izjav $\mathcal{A} = \{A_1, \ldots, A_k\}$ veljajo naslednje trditve.*

(i) *Sklep $\mathcal{A} \vDash A_i$ je resničen za vsak $i \in [k]$.*

(ii) *Za tavtologijo C je sklep $\mathcal{A} \vDash B$ resničen natanko tedaj, ko je resničen sklep $\mathcal{A}, C \vDash B$.*

(iii) *Če velja $B \sim C$, potem je sklep $\mathcal{A} \vDash B$ resničen natanko tedaj, ko je resničen sklep $\mathcal{A} \vDash C$.*

(iv) *Naj veljajo sklepi $\mathcal{A} \vDash B_i$ za vsak $i \in [m]$. Če velja sklep $B_1, \ldots, B_m \vDash C$, potem velja tudi sklep $\mathcal{A} \vDash C$.*

Dokaz. V dokazu bomo s pridom uporabljali izrek 1.1.

Za dokaz točke (i) naj bo $i \in [k]$. Sklep $\mathcal{A} \vDash A_i$ je po izreku 1.1 ekvivalenten temu, da je $A_1 \wedge \cdots \wedge A_k \Rightarrow A_i$ tavtologija. Ker je očitno omenjena implikacija tavtologija, je tudi sklep resničen.

Če je C tavtologija, potem po izreku 1.1 velja

$$\mathcal{A} \vDash B \Leftrightarrow (\mathcal{A} \Rightarrow B \sim 1) \sim ((\mathcal{A} \wedge 1) \Rightarrow B \sim 1) \sim ((\mathcal{A} \wedge C) \Rightarrow B \sim 1) \Leftrightarrow \mathcal{A}, C \vDash B,$$

s čimer je točka (ii) dokazana.

Za dokaz točke (iii) naj bo $B \sim C$. Pokazati moramo ekvivalenco, ki jo pokažemo z dvema implikacijama. Za implikacijo $(\Rightarrow)$ naj velja sklep $\mathcal{A} \vDash B$. Po izreku 1.1 je implikacija $A_1 \wedge \cdots \wedge A_k \Rightarrow B$ tavtologija. Če je $A_1 \wedge \cdots \wedge A_k \sim 0$, potem je tudi implikacija $A_1 \wedge \cdots \wedge A_k \Rightarrow C$ resnična. Zato naj bo $A_1 \wedge \cdots \wedge A_k \sim 1$. Ker je implikacija $A_1 \wedge \cdots \wedge A_k \Rightarrow B$ tavtologija, mora biti v tem primeru $B \sim 1$. Ker velja $B \sim C$, je tudi $C \sim 1$ in implikacija $A_1 \wedge \cdots \wedge A_k \Rightarrow C$ je ponovno resnična. Tako je tudi implikacija $A_1 \wedge \cdots \wedge A_k \Rightarrow C$ tavtologija, kar po izreku 1.1 pomeni, da je sklep $\mathcal{A} \vDash C$ resničen. Za obratno implikacijo $(\Leftarrow)$ zadošča, da v dosedanjem dokazu te točke zamenjamo vlogi B in C.

Za konec naj veljajo sklepi $\mathcal{A} \vDash B_i$ za vsak $i \in [m]$ in naj velja sklep $B_1, \ldots, B_m \vDash C$. Pokažimo, da je implikacija $A_1 \wedge \cdots \wedge A_k \Rightarrow C$ tavtologija, s čimer je dokazan sklep $\mathcal{A} \vDash C$ po izreku 1.1. Če je $A_1 \wedge \cdots \wedge A_k \sim 0$, potem je implikacija $A_1 \wedge \cdots \wedge A_k \Rightarrow C$ resnična. Zato naj bo $A_1 \wedge \cdots \wedge A_k \sim 1$. Ker veljajo sklepi $\mathcal{A} \vDash B_i$ za vsak $i \in [m]$, je $B_i \sim 1$ za vsak $i \in [m]$. Ker velja sklep $B_1, \ldots, B_m \vDash C$, je tudi $C \sim 1$ in implikacija $A_1 \wedge \cdots \wedge A_k \Rightarrow C$ je ponovno resnična in je zato tavtologija, s čimer je tudi točka (iv) dokazana. ∎

Zadnja trditev dejansko podkrepi upravičenost definicije dokaza. Tako točka (i) trditve 1.2 upraviči prvo alinejo iz definicije dokaza, saj lahko iz predpostavk $\mathcal{A}$ sklepamo na resničnost posameznih predpostavk. Podobno točka (ii) trditve 1.2 upraviči drugo alinejo iz definicije dokaza. Točka (iii) trditve 1.2 podkrepi zahtevo, da mora biti zadnja izjava v zaporedju dokaza enakovredna zaključku sklepa, torej $B_m \sim B$. Zadnja alineja iz definicije dokaza sledi iz točke (iv) trditve 1.2. Ob tem še dodajmo, da je tretja alineja iz definicije dokaza kombinacija točke (i) in (iv) trditve 1.2.

Naslednji izrek nam zapolnjuje luknjo, ki jo poraja zadnja alineja definicije dokaza. Do sedaj še nismo spoznali pravilnih sklepov (razen v zgledu 1.7). To vrzel sedaj popravljamo z nekaj enostavnimi sklepi, ki jih običajno uporabljamo.

Izrek 1.3 (Pravila sklepanja) *Naslednji sklepi so resnični.*

(I) *Modus ponens (MP):* $A, A \Rightarrow B \vDash B$.

(II) *Modus tollens (MT):* $\neg B, A \Rightarrow B \vDash \neg A$.

(III) *Disjunktni silogizem (DS):* $\neg A, A \vee B \vDash B$.

(IV) *Hipotetični silogizem (HS):* $A \Rightarrow B, B \Rightarrow C \vDash A \Rightarrow C$.

(V) *Poenostavitev (Po):* $A \wedge B \vDash B$.

(VI) *Pridružitev (Pr):* $A \vDash A \vee B$.

(VII) *Združitev (Zd):* $A, B \vDash A \wedge B$.

Dokaz. Naštete sklepe bomo dokazali s pomočjo izreka 1.1 tako, da bomo pokazali, da so ustrezne implikacije tavtologije. Ob računanju bomo pogosto uporabljali enakovrednosti, ki smo jih spoznali v drugem razdelku. Posebej izpostavimo enakovrednost $A \Rightarrow B \sim \neg A \vee B$. Za dokaz Modus ponensa bomo razen omenjene enakovrednosti uporabili tudi De Morganovo pravilo, distributivnost in asociativnost:

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

Podoben račun sledi tudi za Modus tollens. Omenimo še, da smo Modus tollens že dokazali v zgledu 1.7, vendar tukaj podajamo še račun:

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

Nadaljujemo z Disjunktnim silogizmom in podobnim računom:

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

Najdaljši račun nas čaka pri Hipotetičnemu silogizmu:

$$(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C) \sim (\neg A \vee B) \wedge (\neg B \vee C) \Rightarrow (\neg A \vee C) \sim$$
$$\sim \neg[(\neg A \vee B) \wedge (\neg B \vee C)] \vee (\neg A \vee C) \sim$$
$$\sim \neg(\neg A \vee B) \vee \neg(\neg B \vee C) \vee \neg A \vee C \sim (A \wedge \neg B) \vee \neg A \vee (B \wedge \neg C) \vee C \sim$$
$$\sim ((A \vee \neg A) \wedge (\neg B \vee \neg A)) \vee ((B \vee C) \wedge (\neg C \vee C)) \sim$$
$$\sim (1 \wedge (\neg B \vee \neg A)) \vee ((B \vee C) \wedge 1) \sim (\neg B \vee \neg A) \vee (B \vee C) \sim$$
$$\sim \neg B \vee \neg A \vee B \vee C \sim 1 \vee \neg A \vee C \sim 1.$$

Dokaz zadnjih treh sklepov je enostavnejši. Začnimo s Poenostavitvijo

$$A \wedge B \Rightarrow B \sim \neg(A \wedge B) \vee B \sim \neg A \vee \neg B \vee B \sim \neg A \vee 1 \sim 1,$$

nadaljujmo s Pridružitvijo

$$A \Rightarrow (A \vee B) \sim \neg A \vee A \vee B \sim 1 \vee B \sim 1$$

in končajmo z Združitvijo

$$A \wedge B \Rightarrow A \wedge B \sim \neg(A \wedge B) \vee (A \wedge B) \sim 1,$$

s čimer je dokaz zaključen. ∎

Zgled 1.8 *Dokažimo resničnost sklepa s predpostavkama $p \wedge q$ in $p \Rightarrow (q \Rightarrow r)$ ter zaključkom $\vDash r$. Dokaz bomo zapisali kot v definiciji z zaporedjem izjav, kjer bosta na začetku obe predpostavki, sledile pa bodo izjave, ki so dobljene s kakim pravilnim sklepom iz prejšnjih izjav, ki so enakovredne kakšnemu prejšnjemu koraku, ali, ki so tavtologije. Ob tem je zadnja izjava dokaza enakovredna zaključku sklepa, kar je v tem primeru r. Za vsak korak bomo opisali na desni strani, kako smo ga dobili. Tako je dokaz tega sklepa naslednji:*

1.	$p \wedge q$	(predpostavka)
2.	$p \Rightarrow (q \Rightarrow r)$	(predpostavka)
3.	p	(Po točke 1)
4.	$q \Rightarrow r$	(MP točk 2 in 3)
5.	q	(Po točke 1)
6.	r	(MP točk 4 in 5).

Sledi izrek, ki smo ga že s pridom uporabljali, vedno, kadar smo dokazovali implikacijo. Vendar pa sedaj povemo še več in opišemo sklep brez implikacije v zaključku, ki je ekvivalenten sklepu z implikacijo v zaključku.

Izrek 1.4 (Pogojni sklep PS) *Naj bo $\mathcal{A} = \{A_1, \ldots, A_k\}$ množica izjav. Sklep $\mathcal{A} \vDash B \Rightarrow C$ je resničen natanko tedaj, ko je resničen sklep $\mathcal{A}, B \vDash C$.*

Dokaz. Za dokaz ekvivalence ponovno pokažimo resničnost obeh implikacij. Za $(\Rightarrow)$ lahko predpostavimo, da velja $\mathcal{A} \vDash B \Rightarrow C$. Če je $A_1 \wedge \cdots \wedge A_k \wedge B \sim 0$, je seveda $A_1 \wedge \cdots \wedge A_k \wedge B \Rightarrow C \sim 1$. Tako naj bo $A_1 \wedge \cdots \wedge A_k \wedge B \sim 1$. to pomeni, da je $A_i \sim 1$ za vsak $i \in [k]$ in tudi $B \sim 1$. Ker je resničen sklep $\mathcal{A} \vDash B \Rightarrow C$, to pomeni, da je tudi $C \sim 1$ in ponovno je $A_1 \wedge \cdots \wedge A_k \wedge B \Rightarrow C \sim 1$. Torej je zadnja implikacija tavtologija in je po izreku 1.1 sklep $\mathcal{A}, B \vDash C$ resničen.

Pokažimo še obratno implikacijo $(\Leftarrow)$. Sedaj lahko predpostavimo, da je sklep $\mathcal{A}, B \vDash C$ resničen, kar je po izreku 1.1 ekvivalentno, da je implikacija $A_1 \wedge \cdots \wedge A_k \wedge B \Rightarrow C$ tavtologija. Ponovno je implikacija $A_1 \wedge \cdots \wedge A_k \Rightarrow (B \Rightarrow C)$ resnična, če je $A_1 \wedge \cdots \wedge A_k \sim 0$. Zato naj bo $A_1 \wedge \cdots \wedge A_k \sim 1$. Če je $B \sim 0$, je ponovno implikacija $A_1 \wedge \cdots \wedge A_k \Rightarrow (B \Rightarrow C)$ resnična. Zato naj bo tudi $B \sim 1$. Iz resničnosti sklepa $\mathcal{A}, B \vDash C$ sedaj vidimo, da je $C \sim 1$ in implikacija $A_1 \wedge \cdots \wedge A_k \Rightarrow (B \Rightarrow C)$ je resnična tudi v tej zadnji možnosti. Skratka $A_1 \wedge \cdots \wedge A_k \Rightarrow (B \Rightarrow C) \sim 1$ in po izreku 1.1 je sklep $\mathcal{A} \vDash B \Rightarrow C$ resničen. ∎

Zgled 1.9 *Dokažimo resničnost sklepa s predpostavkama $p \Rightarrow r$ in $q \Rightarrow r$ ter zaključkom $\vDash (p \vee q) \Rightarrow r$. Hitro lahko uvidimo, da na obeh predpostavkah ne moremo uporabiti nobenega pravila sklepanja iz izreka 1.3. Tudi če uporabimo Pogojni sklep in dodamo predpostavko $p \vee q$ si ne moremo pomagati z nobenim izmed pravil sklepanja iz izreka 1.3. Lahko pa pogoj iz definicije dokaza, da mora biti zadnji korak dokaza enakovreden*

zaključku ter zaključek sklepa najprej preoblikujemo s kontrapozicijo $(p \vee q) \Rightarrow r \sim \neg r \Rightarrow \neg(p \vee q)$. *Sedaj lahko začnemo s Pogojnim sklepom in preoblikovanim zaključkom. Tako je dokaz tega sklepa naslednji:*

1.	$p \Rightarrow r$	*(predpostavka)*
2.	$q \Rightarrow r$	*(predpostavka)*
3.1.	$\neg r$	*(predpostavka PS)*
3.2.	$\neg p$	*(MT točk 1 in 3.1)*
3.3.	$\neg q$	*(MT točk 2 in 3.1)*
3.4.	$\neg p \wedge \neg q$	*(Zd točk 3.2 in 3.3)*
3.5.	$\neg(p \vee q)$	*(∼ točke 3.4)*
3.	$\neg r \Rightarrow \neg(p \vee q)$	*(PS točk 3.1 in 3.5)*
4.	$(p \vee q) \Rightarrow r$	*(∼ točke 3).*

Opazimo lahko, da smo v zadnjem zgledu uporabili nekoliko drugačen zapis korakov dokaza kot v zgledu 1.8, saj so nekateri koraki zamaknjeni v desno in dodatno številčeni. To je zaradi dodatne predpostavke pogojnega sklepa, ki velja le za trajanje pogojnega sklepa. Tako vseh točk dokaza od 3.1 do 3.5 v nadaljevanju dokaza ne smemo uporabljati (razen, če do njih pridemo na kak drug način). Temu delu dokaza rečemo **podsklep**.

Sledi še en sklep, ki je osnova za zelo uporaben način dokazovanja, ki mu pogosto rečemo kar **dokaz s protislovjem**. Razlog je v tem, da sklep $\mathcal{A} \vDash B$ drži, če ga preoblikujemo tako, da negacijo zaključeka $\neg B$ primaknemo k predpostavkam, iz tega pa dokažemo laž 0. Laž je vedno neresnična in ji zato rečemo tudi nesmisel ali protislovje.

Izrek 1.5 (Redukcija na absurd RA) *Naj bo* $\mathcal{A} = \{A_1, \ldots, A_k\}$ *množica izjav. Sklep* $\mathcal{A} \vDash B$ *je resničen natanko tedaj, ko je resničen sklep* $\mathcal{A}, \neg B \vDash 0$.

Dokaz. Ekvivalenca iz izreka sledi iz spodnje verige ekvivalenc oziroma enakovrednosti. V njih upoštevamo izrek 1.1 in nekatere enakovrednosti iz prejšnjega razdelka (enakovrednost za implikacijo in De Morganovo pravilo). Omenimo še, da zaradi enostavnejšega zapisa namesto $A_1 \wedge \cdots \wedge A_k$ pišemo kar $\mathcal{A}$. Z računom

$$(\mathcal{A} \vDash B) \Leftrightarrow ((\mathcal{A} \Rightarrow B) \sim 1) \Leftrightarrow (\neg\mathcal{A} \vee B \sim 1) \Leftrightarrow (\neg(\mathcal{A} \wedge \neg B) \sim 1) \Leftrightarrow$$
$$\Leftrightarrow (\neg(\mathcal{A} \wedge \neg B) \vee 0 \sim 1) \Leftrightarrow ((\mathcal{A} \wedge \neg B) \Rightarrow 0 \sim 1) \Leftrightarrow (\mathcal{A}, \neg B \vDash 0)$$

je dokaz zaključen. ∎

Kot pri pogojnem sklepu imamo tudi pri redukciji na absurd dodatno predpostavko in sklepov, pridobljenih s to dodatno predpostavko, ne smemo uporabljati zunaj dokaza Redukcije na absurd.

Zgled 1.10 *Dokažimo resničnost sklepa s predpostavkami $p \Rightarrow q$, $r \Rightarrow s$ in $p \vee r$ ter zaključkom $\vDash q \vee s$. Ob podanih predpostavkah ne moremo začeti dokaza z nobenim od enostavnih pravil sklepanja. Tudi Pogojnega sklepa ne moremo uporabiti (vsaj ne direktno), saj v zaključku ni implikacije. V takšnih primerih pogosto uporabimo dokaz s protislovjem oziroma Redukcijo na absurd. Omenimo še, da, tako kot pri uporabi Pogojnega sklepa v zgledu 1.9, sklepov, pridobljenih s predpostavko Redukcije na absurd, ne smemo uporabiti v nadaljevanju dokaza. Zato jih ločimo z dodatnim številčenjem in zamikom.*

1.	$p \Rightarrow q$	*(predpostavka)*
2.	$r \Rightarrow s$	*(predpostavka)*
3.	$p \vee r$	*(predpostavka)*
4.1.	$\neg(q \vee s)$	*(predpostavka RA)*
4.2.	$\neg q \wedge \neg s$	*($\sim$ točki 4.1)*
4.3.	$\neg q$	*(Po točke 4.2)*
4.4.	$\neg p$	*(MT točk 1 in 4.3)*
4.5.	$\neg s$	*(Po točke 4.2)*
4.6.	$\neg r$	*(MT točk 2 in 4.5)*
4.7.	r	*(DS točk 3 in 4.4)*
4.8.	$r \wedge \neg r$	*(Zd točk 4.6 in 4.7)*
4.9.	0	*($\sim$ točki 4.8)*
4.	$q \vee s$	*(RA točk 4.1 in 4.9).*

Ta sklep lahko dokažemo tudi s Pogojnim sklepom, če upoštevamo naslednjo enakovrednost zaključka $q \vee s \sim \neg q \Rightarrow s$. Oglejmo si še ta dokaz, ki je krajši.

1.	$p \Rightarrow q$	*(predpostavka)*
2.	$r \Rightarrow s$	*(predpostavka)*
3.	$p \vee r$	*(predpostavka)*
4.1.	$\neg q$	*(predpostavka PS)*
4.2.	$\neg p$	*(MT točk 1 in 4.1)*
4.3.	r	*(DS točk 3 in 4.2)*
4.4.	s	*(MP točk 2 in 4.3)*
4.	$\neg q \Rightarrow s$	*(PS točk 4.1 in 4.4)*
5.	$q \vee s$	*($\sim$ točki 4).*

1.4 PREDIKATI

Oglejmo si naslednji klasični[2] zgled sklepa.

Vsak človek je umrljiv.
Mark Zuckerberg je človek.
Zato bo Mark Zuckerberg umrl.

V njem imamo dve predpostavki in zaključek sklepa. Ob tem je prva predpostavka nenavadna, saj govori o vseh ljudeh. Nasprotno druga predpostavka, kot tudi zaključek sklepa, govori le o enem predstavniku naše vrste. Zapišimo prvo predpostavko na daljši način:

Če je nekaj človek, potem bo ta nekdo umrl.

Ob tem zapisu se porodijo nova vprašanja. Najprej se lahko vprašamo, od kod izbiramo reči, za katere presojamo, ali so ljudje ali ne. To je lahko poljubna množica, vendar je v tem sklepu primerno, da omenjena množica vsebuje vse ljudi. Tej množici rečemo **območje govora** ali **definicijsko območje**. Tako izbiramo elemente iz definicijskega območja, za katere želimo presoditi, ali imajo neko lastnost ali ne. Elemente iz definicijskega območja pogosto označimo s kakšno črko s konca abecede (x, y, z in podobno). Ker lahko izbiramo različne elemente, govorimo o **spremenljivki**. V preurejeni prvi predpostavki našega primera nam spremenljivko predstavlja beseda nekaj. Sami lastnosti, ki ga izbrani element ima ali pač ne, rečemo **predikat**.

V predikatu lahko nastopa le ena spremenjivka, recimo

$$C(x) \ldots x \text{ je človek ali}$$
$$U(y) \ldots y \text{ je umrljiv.}$$

V tem primeru govorimo o **enostavnem predikatu**. Predikat se lahko izraža z dvema, tremi ali večimi spremenjivkami, recimo

$$H(x, y) \ldots x \text{ je hitrejši od } y \text{ ali}$$
$$V(x, y) \ldots x \text{ je večji od } y \text{ ali}$$
$$M(x, y, z) \ldots y \text{ je med } x \text{ in } z.$$

V takšnih primerih govorimo o **dvomestnih**, **tromestnih** ali **večmestnih** predikatih.

Potrebujemo tudi merilo, ki nas omeji na le določen del definicijskega območja ali, po drugi strani, ne omejuje definicijskega območja. Izkaže se, da za to zadostujeta naslednja kvantifikatorja:

$$\forall \ldots \textbf{univerzalnostni kvantifikator} \text{ (vsak) in}$$
$$\exists \ldots \textbf{eksistenčni kvantifikator} \text{ (obstaja).}$$

2 Običajno namesto Marka Zuckerberga nastopa antični grški filozof Sokrat.

Simbol $\forall$ preberemo enostavno **vsak** in $\exists$ preberemo kot **obstaja**. Tako zapis

$$\forall y : U(y)$$

pomeni: za vsak element y iz definicijskega območja predikata U je res $U(y)$. Ali na kratko, če upoštevamo pomen predikata U: vsak y je umrljiv. Podobno zapis

$$\exists x : C(x)$$

pomeni obstaja element x iz definicijskega območja predikata C, za katerega je $C(x)$ resničen. Seveda uporabljamo krajšo verzijo, ki se glasi: obstaja x, da je x človek.

Sedaj lahko zgled z začetka razdelka končno zapišemo s simboli:

1.	$\forall x : C(x) \Rightarrow U(x)$	(predpostavka)
2.	$C(MZ)$	(predpostavka)
	$\vDash U(MZ)$	(zaključek).

Velja še omeniti, da MZ v $C(MZ)$ pomeni Marka Zuckenberga, kar je v okviru definicijskega območja en fiksen element, torej konstanta.

Za izjave (s predikati ali brez) nas zanima, ali so resnične ali ne. Zato nas zanima, kdaj je resnična izjava $\forall y : U(y)$. Le-ta je resnična tedaj, kadar je predikat U resničen za vse elemente iz definicijskega območja. Ker je govora o predikatu umrljiv, je izjava $\forall y : U(y)$ resnična, če so v definicijskem območju samo živi elementi (saj ti slej kot prej zagotovo umrejo). Po drugi strani ta izjava ni resnična, če v definicijskem območju nastopa kakšen neživ element, recimo kamen ali miza (saj takšni elemetni ne morejo umreti).

Podobno je izjava $\exists x : C(x)$ resnična, če lahko znotraj definicijskega območja najdemo vsaj en element x_0, da je predikat $C(x_0)$ resničen. Tako je za definicijsko območje vseh živih bitij na planetu Zemlja izjava $\exists x : C(x)$ resnična. Za definicijsko območje vseh elementov na Marsu, pa izjava $\exists x : C(x)$ ni resnična, vsaj dokler ne bomo ljudje (živi) prišli na Mars. Ob tem ne vemo, koliko točno je elementov, za katere je $C(x)$ resnična, a nas to tudi ne zanima.

Kako se obnašata kvantifikatorja v primeru negacije, lahko razberemo iz naslednjega izreka.

Izrek 1.6 *Za predikat $P(x)$ veljata naslednji trditvi*

(I) $\neg\forall x : P(x) \sim \exists x : \neg P(x)$.

(II) $\neg\exists x : P(x) \sim \forall x : \neg P(x)$.

Dokaz. Za točko (i) je $\neg\forall x : P(x)$ resnična, kadar za nek element a iz definicijskega območja velja $P(a) \sim 0$. To že pomeni, da obstaja element iz definicijskega območja, to je a, da $P(a)$ ni resnična. Tako (i) velja.

Točko (ii) dobimo s pomočjo točke (i), ki jo negiramo

$$\neg(\neg\forall x : P(x)) \sim \neg(\exists x : \neg P(x)).$$

Seveda se dvojna negacija izniči in dobimo

$$\forall x : P(x) \sim \neg\exists x : \neg P(x),$$

kar je točka (ii) za predikat $\neg P(x)$. ∎

Zgled 1.11 *Za predikat: $M(x,y,z)\ldots y$ je med x in z, si oglejmo resničnost oziroma neresničnost naslednjih trditev glede na definicijsko območje D, ki predstavlja podmnožico realnih števil.*

Trditev $\forall x : M(x,3,7)$ je resnična, če je $D \subseteq (-\infty,3)$ in ni resnična, če je $D \cap [3,\infty) \neq \emptyset$.

Trditev $\forall y : M(7,y,3)$ je resnična, če je $D \subseteq (3,7)$ in ni resnična, če je $D \cap ((-\infty,3] \cup [7,\infty)) \neq \emptyset$, saj predikat M ne zahteva urejenosti, pač pa le, da je druga spremenljivka med prvo in tretjo spremenljivko.

Trditev $\exists z : M(1,3,z)$ je resnična, če je $D \cap (3,\infty) \neq \emptyset$ in ni resnična, če je $D \cap [3,\infty) = \emptyset$.

Trditev $\exists y : M(1,y,1)$ je vedno neresnična, saj med 1 in 1 ni nobenega realnega števila.

Trditev $\forall x, \exists z : M(x,3,z)$ je resnična, če je $D \cap (-\infty,3) \neq \emptyset$ in hkrati $D \cap (3,\infty) \neq \emptyset$ in $3 \notin D$, saj lahko potem za vsak izbran x najdemo ustrezen z (na drugi strani od 3).

Trditev $\exists x, \exists y : M(x,y,5)$ je resnična, če D vsebuje vsaj dve različni števili manjši od 5 ali dve večji od 5, in neresnična sicer.

Zgled 1.12 *Oglejmo si različne pomene vseh možnih kombinacij kvantifikatorjev za predikat $R(x,y)$, ki pomeni, da ima x rad y.*

$\forall x, \forall y : R(x,y)$	...	*vsakdo ima rad vsakogar;*
$\forall x, \exists y : R(x,y)$	...	*vsakdo ima rad nekoga;*
$\exists x, \forall y : R(x,y)$	...	*nekdo ima rad vsakogar;*
$\exists x, \exists y : R(x,y)$	...	*nekdo ima rad nekoga;*
$\forall y, \forall x : R(x,y)$	...	*vsakogar imajo radi vsi;*
$\forall y, \exists x : R(x,y)$	...	*vsakogar ima rad nekdo;*
$\exists y, \forall x : R(x,y)$	...	*nekoga ima rad vsak;*
$\exists y, \exists x : R(x,y)$	...	*nekoga ima rad nekdo.*

Trditev 1.7 *Za vsaka predikata P in Q nad definicijskim območjem D in $a \in D$ veljajo naslednje trditve.*

(I) $\forall x : P(x) \Rightarrow P(a)$.

(II) $P(a) \Rightarrow \exists x : P(x)$.

(III) $\forall x : (P(x) \wedge Q(x)) \Leftrightarrow \forall x : P(x) \wedge \forall x : Q(x)$.

(IV) $\forall x : (P(x) \vee Q(x)) \Leftarrow \forall x : P(x) \vee \forall x : Q(x)$.

(V) $\exists x : (P(x) \vee Q(x)) \Leftrightarrow \exists x : P(x) \vee \exists x : Q(x)$.

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

Dokaz. Točka (i) je očitna, saj če je $P(x)$ resnična za vsak x iz definicijskega območja, potem je resnična tudi za konstanto a iz definicijskega območja. Podobno enostavna je tudi (ii), saj kadar je resničen $P(a)$, potem obstaja nek element iz definicijskega območja, to je ravno a, za katerega je $P(x)$ resničen.

Za (iii) naj velja najprej $\forall x : (P(x) \wedge Q(x))$. Torej je $(P(x) \wedge Q(x))$ resničen za vse elemente definicijskega območja. S tem sta resnična tudi vsak zase $P(x)$ za vse elemente definicijskega območja in $Q(x)$ za vse elemente definicijskega območja. To že pomeni $\forall x : P(x) \wedge \forall x : Q(x)$. Pokažimo še $(\Leftarrow)$ za (iii). Naj torej velja $\forall x : P(x) \wedge \forall x : Q(x)$. Tako je resničen $P(x)$ za vse elemente definicijskega območja in je resničen $Q(x)$ za vse elemente definicijskega območja. Zato je res tudi $P(x) \wedge Q(x)$ za vse elemente definicijskega območja, kar pomeni tudi $\forall x : (P(x) \wedge Q(x))$ in (iii) je dokazana.

Točka (iv) je resnična, če je resničen $\forall x : (P(x) \vee Q(x))$. Zato poglejmo kaj se zgodi, ko $\forall x : (P(x) \vee Q(x))$ ne drži. Tako je

$$0 \sim \forall x : (P(x) \vee Q(x)) \sim \bigwedge_{a \in D} (P(a) \vee Q(a)).$$

Ker je $\wedge$ neresničen takrat, ko je vsaj en člen neresničen, mora obstajati nek element iz D, recimo element a', da je $P(a') \vee Q(a') \sim 0$. Seveda je to res, kadar je $P(a') \sim 0$ in hkrati $Q(a') \sim 0$. Potem je seveda $\forall x : P(x) \sim 0$ in $\forall x : Q(x) \sim 0$, kar pripelje do

$$\forall x : P(x) \vee \forall x : Q(x) \sim 0.$$

Tako vidimo, da če je drugi del implikacije neresničen, potem smo pokazali, da je tudi prvi del implikacije neresničen. To pomeni, da je implikcija v (iv) resnična.

Trditev iz (v) dobimo s pomočjo negacije točke (iii) na naslednji način

$$\neg \forall x : (P(x) \wedge Q(x)) \Leftrightarrow \neg(\forall x : P(x) \wedge \forall x : Q(x)).$$

Sedaj uporabimo (i) iz izreka 1.6 in De Morganovo pravilo ter imamo

$$\exists x : \neg(P(x) \wedge Q(x)) \Leftrightarrow \neg \forall x : P(x) \vee \neg \forall x : Q(x).$$

Ponovimo še enkrat uporabo (i) iz izreka 1.6 in De Morganovo pravilo

$$\exists x : \neg P(x) \vee \neg Q(x) \Leftrightarrow \exists x : \neg P(x) \vee \exists x : \neg Q(x)$$

kar je točka (v) za predikata $\neg P(x)$ in $\neg Q(x)$.

Točko (vi) pokažemo s pomočjo kontrapozicije točke (iv) in imamo

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

kar je točka (vi) za predikata $\neg P(x)$ in $\neg Q(x)$. ∎

Morda je presenetljivo, da v točkah (iv) in (vi) zadnje trditve ni ekvivalence, tako kot v (iii) in (v), a zlahka se najdejo protiprimeri za obratno smer implikacij v (iv) in (vi). Oglejmo si dva zgleda.

Zgled 1.13 *Naj definicijsko območje presikatov $S(n)$ in $L(n)$ tvorijo naravna števila. Predikata sta definirana z*

$$S(n) \ldots n \text{ je sod in } L(n) \ldots n \text{ je lih.}$$

Velja $\forall n : (S(n) \vee L(n))$, saj je vsako naravno število sodo ali liho. Ne velja pa $\forall n : S(n) \vee \forall n : L(n)$, saj vsako naravno število ni sodo in vsako naravno število ni liho. Torej je to protiprimer za implikacijo

$$\forall n : (S(n) \vee L(n)) \Rightarrow \forall n : S(n) \vee \forall n : L(n),$$

ki torej ni resnična.

Zgled 1.14 *Sedaj je definicijsko območje za predikata $P(x)$ in $Q(x)$ enako vsem realnim številom. Predikata sta definrana z*

$$P(x) \ldots x^2 - 3 \leq 0 \text{ in } Q(x) \ldots \ x + 5 < 0.$$

Seveda je $P(x)$ resničen za realna števila iz intervala $[-\sqrt{3}, \sqrt{3}]$ in $Q(x)$ je resničen, če je $x < -5$. Velja $\exists x : P(x) \wedge \exists x : Q(x)$, saj med realnimi števili obstaja tako, ki izpolni $P(x)$ in obstaja takšno, ki izpolni $Q(x)$. Ne velja pa $\exists x : (P(x) \wedge Q(x))$, saj ni realnega števila, ki hkrati izpolni oba $P(x)$ in $Q(x)$. Zato implikacija

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

ni resnična, saj smo pravkar videli protiprimer zanjo.

Tudi v predikatnem zapisu izjav poznamo **izbrano obliko** zapisa. Tudi tokrat zahtevamo, da so vse izjavne povezave izražene le z negacijo $\neg$, in $\wedge$ ter ali $\vee$ in da negacija nastopa le neposredno pred izjavami. Dodatna zahteva za izbrano obliko predikatnega računa je, da vsi kvantifikatorji nastopajo na začetku. Tako dobimo zapis

$$K_1 x_1, K_2 x_2, \ldots, K_n x_n : P(x_1, x_2, \ldots, x_n),$$

kjer so $K_1, K_2, \ldots, K_n$ kvantifikatorji, $P(x_1, x_2, \ldots, x_n)$ pa predikat brez kvantifikatorjev, ki vsebuje le izjavne povezave negacijo $\neg$, in $\wedge$ ter ali $\vee$ in negacija nastopa le neposredno pred predikati.

Zgled 1.15 *Zapišimo naslednjo izjavo s predikati v izbrani obliki:*

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

Na prvem koraku smo uporabili točko (i) izreka 1.6 za negacijo in spremenili smo prvo implikacijo. V drugem koraku je bila spremenjena druga implikacija. V tretjem koraku je sledilo De Morganovo pravilo. Nato smo y s kvantifikatorjem že zapisali naprej, znotraj oklepajev pa smo še enkrat uporabili točko (i) izreka 1.6. V zadnjem koraku smo le še z s kvantifikatorjem zapisali na začetek.

Zgled 1.16 *Kako zapišemo $\exists x : P(x) \wedge \exists x : Q(x)$ v izbrani obliki? Vemo, da*

$$\exists x : P(x) \wedge \exists x : Q(x) \nsim \exists x : (P(x) \wedge Q(x)),$$

saj obratna implikacija točke (vi) ne velja. Trik je preprost, saj moramo le eno spremenljivko nadomestiti z drugo. Tako je

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

1.5 SKLEPANJE S PREDIKATI

Osrednji cilj tega razdelka je pojasniti, kako sklepati v predikatnem računu. Temelje zato smo postavili že s sklepanjem v izjavnem računu. Sedaj moramo ugotoviti, kaj storiti s kvantifikatorji. Z drugačnim zapisom lahko predikat s kvantifikatorjem zapišemo brez le-tega na naslednji način:

$$\begin{aligned}
\forall x \quad &: \quad P(x) \quad \vDash P(c) \quad \forall c \in D \\
\exists x \quad &: \quad P(x) \quad \vDash P(w) \; \exists w \in D,
\end{aligned}$$

kjer je D definicijsko območje. Tako uporabljamo za spremenljivko c izraz **neomejenka**, saj znotraj D ni omejena, medtem ko spremenljivki w rečemo **omejenka**, saj je omejena na le nekatere elemente D. Uporabimo še tretjo oznako in sicer q, ki nam pomeni karkoli: omejenko ali neomejenko. Tako lahko enostavneje zapišemo pravili za odstranjevanje kvantifikatorjev:

- **Univerzalna Specializacija** ali **US**: $\forall x : P(x) \models P(q)$ (q je karkoli),
- **Eksistenčna Specializacija** ali **ES**: $\exists x : P(x) \models P(w)$ (w je nova omejenka).

V Univerzalni specializaciji, ko se znebimo kvantifikatorja $\forall$, lahko imamo v predikatu tako neomejenko kot omejenko. Na koncu uporabimo tisto, ki nam bolj ustreza. Seveda se moramo v eksistenčni specializaciji omejiti na omejenko. Kvantifikatorji lahko nastopajo tudi v zaključku sklepa in takrat je potrebno kvantifikatorje vrniti. To lahko storimo z naslednjima praviloma:

- **Univerzalna Generalizacija** ali **UG**: $P(c) \models \forall x : P(x)$ (c je neomejenka),
- **Eksistenčna Generalizacija** ali **EG**: $P(q) \models \exists x : P(x)$ (q je karkoli).

Tukaj lahko vrnemo kvantifikator $\forall$ v pravilu UG le, če v predikatu nastopa neomejenka, medtem ko lahko kvantifikator $\exists$ vrnemo v pravilu EG ne glede na to, kaj nastopa v predikatu.

S temi dodatnimi pravili odstranjevanja in dodajanja kvantifikatorjev lahko sklepamo tudi v predikatnem računu. Postopek je podoben kot v izjavnem računu, le da vmes po potrebi odstranimo kvantifikatorje in jih na koncu po potrebi spet dodamo. V nadaljevanju razdelka bomo preko zgledov spoznali postopek sklepanja v predikatnem računu in nekatere njegove dodatne zakonitosti.

Zgled 1.17 *Dokažimo najprej enostavni sklep o umrljivosti Marka Zuckenberga iz začetka prejšnjega razdelka.*

1.	$\forall x : C(x) \Rightarrow U(x)$	*(predpostavka)*
2.	$C(MZ)$	*(predpostavka)*
3.	$C(c) \Rightarrow U(c)$	*(US točke 1, c neomejenka)*
4.	$C(MZ) \Rightarrow U(MZ)$	*($\sim$ točki 3, c/MZ)*
5.	$U(MZ)$	*(MP točk 2 in 4).*

Posebej velja omeniti točko 4, kjer smo neomejenko c nadomestili s konstanto MZ, kar smo v utemeljitvi v oklepaju označili s c/MZ. To seveda lahko storimo, saj neomejenka pomeni resničnost predikata na celotnem definicijskem območju, torej tudi za MZ. V tem zgledu tudi ni bilo potrebno vrniti nobenega kvantifikatorja, saj le-tega v zaključku ni.

Zgled 1.18 *Dokažimo še sklep* $\forall x : (P(x) \Rightarrow R(x) \wedge S(x)),\ \exists x : (P(x) \wedge T(x)) \vDash \exists x : (T(x) \wedge S(x))$.

1.	$\forall x : (P(x) \Rightarrow R(x) \wedge S(x))$	*(predpostavka)*
2.	$\exists x : (P(x) \wedge T(x))$	*(predpostavka)*
3.	$P(w) \wedge T(w)$	*(ES točke 2, w omejenka)*
4.	$P(w)$	*(Po točke 3)*
5.	$T(w)$	*(Po točke 3)*
6.	$P(w) \Rightarrow R(w) \wedge S(w)$	*(US točke 1, x/w)*
7.	$R(w) \wedge S(w)$	*(MP točk 4 in 6)*
8.	$S(w)$	*(Po točke 7)*
9.	$T(w) \wedge S(w)$	*(Zd točk 5 in 8)*
10.	$\exists x : (T(x) \wedge S(x))$	*(ES točke 9).*

Tukaj omenimo, da pri US v točki 6 lahko x zamenjamo z omejenko w, saj lahko pri US uporabimo karkoli. Zato je bilo potrebno najprej izpeljati eksistenčno specializacijo in šele nato univerzalnostno specializacijo. Obraten vrstni red v dokazovanju nas privede v težave.

Zgled 1.19 *Zapišimo še 'dokaz' obratne implikacije točke* (vi) *iz trditve 1.7. Beseda dokaz je poudarjena, saj to ne more biti pravi dokaz, ker obratna implikacija omenjene točke* (vi) *ne drži, saj smo v zgledu 1.14 predstavili njen protiprimer. Seveda implikacijo dokazujemo s pogojnim sklepom in imamo le eno predpostavko, ki je kar predpostavka pogojnega sklepa.*

1.	$\exists x : P(x) \wedge \exists x : Q(x)$	*(predpostavka PS)*
2.	$\exists x : P(x)$	*(Po točke 1.)*
3.	$P(w)$	*(ES točke 2., w omejenka)*
4.	$\exists x : Q(x)$	*(Po točke 1.)*
5.	$Q(w)$	*(ES točke 4, w omejenka)*
6.	$P(w) \wedge Q(w)$	*(Zd točk 3. in 5.)*
7.	$\exists x : (P(x) \wedge Q(x))$	*(EG točke 6).*

Kje smo naredili napako? To smo zagotovo storili, saj, kot smo že omenili, ta implikacija ni resnična. Napaka je storjena v točki 5., *kjer smo uporabili enako omejenko kot že prej v točki* 3. *To ni prav, saj omejenka zavzema le nek del definicijskega območja in nova omejenka s tistim delom nima nujno kaj skupnega. Tako je druga omejenka lahko resnična na drugem delu definicijskega območja in sklepa ne moremo zaključiti. Bolj natančno, če bi uporabili različni omejenki* w_1 *in* w_2, *potem imamo* $P(w_1) \wedge Q(w_2)$ *v točki* 6. *in zadnjega koraka ne moremo storiti.*

Odkrili smo pomembno past pri uporabi eksistenčne specializacije.

Pozor! Vedno kadar uporabljamo eksistenčno specializacijo, moramo uporabiti novo omejenko, torej takšno, ki je do tedaj še nismo.

Past se skriva tudi pri kvantifikatorju $\forall$. Kadar želimo uporabiti univerzalnostno generalizacijo, lahko neomejenko, ki jo pri tem uporabimo, uporabljamo le znotraj dela dokaza, kjer delamo korake za dokaz te generalizacije, zunaj pa ne. Tako korake za univerzalnostno generalizacijo pišemo kot podsklep, podobno kot pri pogojnem sklepu in redukciji na absurd. Sam podsklep začnemo s predstavitvijo omejenke, ki se bo uporabljala v tistem delu in jo označimo s $!c$. Tako te **neomejenke, ki jo uporabljamo znotraj podsklepa ne smemo uporabljati zunaj le-tega**. To je podobno kot pri pogojnem sklepu in redukciji na absurd, ko sklepov, dobljenih ob dodatni predpostavki, ne smemo uporabljati zunaj podsklepa. Oglejmo si to na zahtevnejšem sklepu naslednjega zgleda.

Zgled 1.20 *Zaključek sklepa je* $\forall x : (\forall y : (T(y,x) \Rightarrow P(y)) \Rightarrow S(x))$*, njegove predpostavke pa zapiščimo kar na začetek dokaza.*

1.	$\forall x : (P(x) \Rightarrow Q(x))$	*(predpostavka)*
2.	$\forall x : (R(x) \wedge Q(x) \Rightarrow S(x))$	*(predpostavka)*
3.	$\forall x, \exists y : (R(y) \wedge T(y,x))$	*(predpostavka)*
4.	$\forall x, \forall y : (T(y,x) \wedge S(y) \Rightarrow S(x))$	*(predpostavka)*
5.1	$!c$	*(UG, c neomejenka)*
5.2.	$\exists y : (R(y) \wedge T(y,c))$	*(US točke 3, x/c)*
5.3.	$\forall y : (T(y,c) \wedge S(y) \Rightarrow S(c))$	*(US točke 4, x/c)*
5.4.	$R(w) \wedge T(w,c)$	*(ES točke 5.2, y/w omejenka)*
5.5.	$R(w)$	*(Po točke 5.4)*
5.6.	$T(w,c)$	*(Po točke 5.4)*
5.7.1.	$\forall y : (T(y,c) \Rightarrow P(y))$	*(predpostavka PS)*
5.7.2.	$T(w,c) \Rightarrow P(w)$	*(US točke 5.7.1, y/w)*
5.7.3.	$P(w)$	*(MP točk 5.6 in 5.7.2)*
5.7.4.	$P(w) \Rightarrow Q(w)$	*(US točke 1, x/w)*
5.7.5.	$Q(w)$	*(MP točk 5.7.3 in 5.7.4)*
5.7.6.	$R(w) \wedge Q(w)$	*(Zd točk 5.5 in 5.7.5)*
5.7.7.	$R(w) \wedge Q(w) \Rightarrow S(w)$	*(US točke 2, x/w)*
5.7.8.	$S(w)$	*(MP točk 5.7.6 in 5.7.7)*
5.7.9.	$T(w,c) \wedge S(w)$	*(Zd točk 5.6 in 5.7.8)*
5.7.10.	$T(w,c) \wedge S(w) \Rightarrow S(c)$	*(US točke 5.3, y/w)*
5.7.11.	$S(c)$	*(MP točk 5.7.9 in 5.7.10)*
5.7.	$\forall y : (T(y,c) \Rightarrow P(y)) \Rightarrow S(c)$	*(PS točk 5.7.1 in 5.7.11)*
5.	$\forall x : (\forall y : (T(y,x) \Rightarrow P(y)) \Rightarrow S(x))$	*(UG točk 5.1 in 5.7).*

Komentirajmo še pomembnejše točke tega dokaza. V točki 5.1 začnemo z uporabo neomejenke c, s katero nakažemo, da bomo na koncu uporabili univerzalnostno generalizacijo. Od sedaj naprej se lahko ta neomejenka uporablja, dokler UG dejansko ne izvedemo, ne sme se pa uporabljati zunaj tega. Tudi v vseh preostalih univerzalnostnih generalizacijah jo lahko uporabimo, saj je neomejenka. To tudi storimo v točkah 5.2 in 5.3. V točki 5.4

uporabimo novo omejenko, saj je edina v eksistenčni specializaciji. V točki 5.7.1 začnemo s pogojnim sklepom. Opazimo lahko, da je del predpostavke tudi kvantifikator $\forall y$, ki ga v nobenem trenutku ne odstranimo. Če bi ga, potem bi potrebovali novo univerzalnostno generalizacijo in novo neomejenko, recimo $!d$. Kadar kasneje uporabimo US, točke 5.7.2, 5.7.4, 5.7.7 in 5.7.10, vedno izberemo omejenko w, saj ravno to potrebujemo. Tukaj ni težave z uporabo iste omejenke, saj jo uporabimo pri univerzalnostni specializaciji. Omenimo še, da imamo v točki 5.7.8 $S(w)$, a tukaj še ne smemo zaključiti pogojnega sklepa, saj za to potrebujemo $S(c)$, torej neomejenko.

Ostane nam še vprašanje, kako pokazati neveljavnost sklepa v predikatnem računu? Tudi tukaj je potrebno poiskati protiprimer. Torej takšne vrednosti predikatov, da je zaključek neresničen, predpostavke pa resnične. Ob tem so vrednosti predikatov odvisne od definicijskega območja D. Tako se lahko zgodi, da je sklep resničen za dovolj majhno definicijsko območje, ni pa resničen, če je D dovolj velik. Zaključimo z zgledoma dveh neresničnih sklepov.

Zgled 1.21 *Sklep $\forall x : P(x) \Rightarrow \forall x : Q(x) \vDash \forall x : (P(x) \Rightarrow Q(x))$ je neresničen za definicijsko območje $D = \{a, b\}$, če velja*

x	$P(x)$	$Q(x)$
a	0	1
b	1	0

.Ni težko videti, da je $\forall x : P(x) \sim 0$ in $\forall x : Q(x) \sim 0$. Zato je $\forall x : P(x) \Rightarrow \forall x : Q(x) \sim 1$ in predpostavka je resnična. Hkrati je zaključek neresničen, saj je $P(b) \Rightarrow Q(b) \sim 0$ in je zato $\forall x : (P(x) \Rightarrow Q(x)) \sim 0$.

Zgled 1.22 *Sklep $\forall x : (A(x) \Rightarrow B(x)), \exists x : (B(x) \wedge C(x)) \vDash \forall x : (A(x) \Rightarrow C(x))$ je neresničen za definicijsko območje $D = \{a, b\}$, če velja*

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

,saj ni težko videti, da sta predpostavki $\forall x : (A(x) \Rightarrow B(x))$ in $\exists x : (B(x) \wedge C(x))$ resnični, zaključek pa neresničen, saj je $A(a) \Rightarrow C(a) \sim 0$. Po drugi strani je ta sklep resničen, če se omejimo na definicijsko območje z enim samim elementom $D = \{a\}$. V tem primeru se sklep poenostavi, saj pri definicijskem območju z enim samim elementom kvantifikatorja $\forall$ in $\exists$ igrata enako vlogo. Tako imamo sklep $A(a) \Rightarrow B(a), B(a) \wedge C(a) \vDash A(a) \Rightarrow C(a)$, ki ga s pogojnim sklepom zlahka dokažemo.

1.6 NEKATERE (NE)REŠENE NALOGE

Vaja 1.1 *S pomočjo pravilnostne tabele dokažite vse enakovrednosti iz razdelka 1.2.*

Vaja 1.2 *S pravilnostno tabelo preverite, ali sta izjavi* $p \wedge (q \vee r)$ *in* $\neg\,(p \wedge q) \Rightarrow (p \wedge r)$ *enakovredni.*

Vaja 1.3 *Preverite, ali je naslednja izjava tavtologija:*

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

Vaja 1.4 *Pokažite, da so množice* $\{\neg, \wedge\}, \{\neg, \vee\}, \{\downarrow\}, \{\wedge, \vee, \veebar\}$ *polni nabori izjav.*

Vaja 1.5 *Naslednje sklepe dokažite, ali poiščite protiprimer zanje.*

(A) $p \vee r,\ p \Rightarrow q,\ r \Rightarrow s \qquad \models q \wedge s;$

(B) $p \vee q,\ (\neg p \wedge q) \Rightarrow r \qquad \models \neg r \Rightarrow p;$

(C) $p \vee q \Rightarrow r \wedge s,\ s \vee t \Rightarrow u \qquad \models r \wedge s;$

(D) $p \vee q \Rightarrow r \wedge s,\ r \vee t \Rightarrow u \qquad \models p \Rightarrow u;$

(E) $p \vee q \Rightarrow r \wedge s,\ s \vee t \Rightarrow u \qquad \models p \Rightarrow u;$

(F) $p \Rightarrow q \vee r,\ q \Rightarrow \neg p,\ \neg\,(s \wedge r) \qquad \models p \Rightarrow \neg s;$

(G) $p \Rightarrow q,\ r \Rightarrow s,\ p \vee r \qquad \models r \wedge s;$

(H) $p \Rightarrow q \Rightarrow r,\ p \vee s,\ \neg s,\ t \Rightarrow q \qquad \models \neg r \Rightarrow \neg t;$

(I) $p \Leftrightarrow q,\ \neg s \Rightarrow q,\ r \vee \neg s,\ q \Rightarrow r \qquad \models s;$

(J) $p,\ p \Rightarrow r,\ p \Rightarrow (q \vee \neg r),\ s \vee \neg q \qquad \models s;$

(K) $p \Rightarrow q,\ p \Rightarrow \neg q \qquad \models \neg p;$

(L) $p \vee q,\ \neg p \vee r,\ \neg r \qquad \models q;$

(M) $p \vee q,\ \neg q,\ r \Rightarrow \neg p \qquad \models \neg r;$

(N) $p \Leftrightarrow q,\ \neg p,\ \neg(q \Rightarrow r) \vee t,\ s \wedge t \Rightarrow r \qquad \models r \wedge \neg q;$

(O) $p \Leftrightarrow q,\ \neg p,\ \neg(q \Rightarrow r) \vee t,\ s \vee t \Rightarrow r \qquad \models r \wedge \neg q.$

Rešitev. *Sklepi pod točkami* $(a), (c), (g), (h), (i), (n)$ *in* (o) *niso resnični. Za primer* (a) *je tako protiprimer* $p \sim q \sim 1$ *in* $r \sim s \sim 0$. *V primeru* (c) *pa imamo protiprimer, ko imajo vse spremenljivke vrednost* 0. *Podobno poiščemo pri ostalih takšne vrednosti, da je zaključek neresničen, predpostavke pa so resnične. Sklepi v ostalih točkah so resnični. Tako sta dokaza točk* (d) *in* (e) *skoraj identična, saj se razlikujeta le na enem mestu v* r *in* s, *ki pa sicer nastopata simetrično v obeh sklepih. Sicer ju dokažemo s pogojnim sklepom, nato pa Pr, MP, Po, Pr in še enkrat MP. Sklepa* (k) *in* (m) *sta tipična za uporabo redukcije na absurd. Sklep* (l) *dokažemo direktno z dvakratno uporabo DS. Tudi pri sklepu* (j) *gre direktno najprej dvakrat PS in nato dvakrat DS. Tako si natančno oglejmo dokaza sklepov pod* (f) *in* (b). *Začnimo s sklepom* (f)*:*

1.	$p \Rightarrow q \vee r$		*(predpostavka)*
2.	$q \Rightarrow \neg p$		*(predpostavka)*
3.	$\neg (s \wedge r)$		*(predpostavka)*
4.1.		p	*(Predpostavka PS.)*
4.2.		$\neg q$	*(MT točk 4.1 in 2)*
4.3.		$q \vee r$	*(MP točk 1 in 4.1)*
4.4.		r	*(DS točk 4.3 in 4.2)*
4.5.		$\neg s \vee \neg r$	*(∼ točke 3)*
4.6.		$\neg s$	*(DS točk 4.5 in 4.4)*
4.	$p \Rightarrow \neg s$		*(PS točk 4.1 in 4.6).*

Sledi še dokaz sklepa (b)*:*

1.	$p \vee q$			*(predpostavka)*
2.	$(\neg p \wedge q) \Rightarrow r$			*(predpostavka)*
3.1.		$\neg r$		*(predpostavka PS)*
3.2.		$\neg(\neg p \wedge q)$		*(MT točk 3.1 in 2)*
3.3.		$p \vee \neg q$		*(∼ točki 3.2)*
3.4.1.			$\neg p$	*(predpostavka RA)*
3.4.2.			$\neg q$	*(DS točk 3.3 in 3.4.1)*
3.4.3.			q	*(DS točk 1 in 3.4.1)*
3.4.4.			$\neg q \wedge q$	*(Zd točk 3.4.2 in 3.4.3)*
3.4.5.			0	*(∼ točki 3.4.4)*
3.4.		p		*(RA točk 3.4.1 in 3.4.5)*
3.	$\neg r \Rightarrow p$			*(PS točk 3.1 in 3.4).*

Vaja 1.6 *Naslednje sklepe dokažite ali poiščite protiprimer zanje.*

(A) $\forall x:\ (p(x) \vee q(x)),\ \forall x:\ [(\neg p(x) \wedge q(x)) \Rightarrow r(x)]$
$\models \forall x : (\neg r(x) \Rightarrow p(x));$

(B) $\forall x : [p(x) \vee q(x)],\ \exists x : \neg p(x),\ \forall x : [r(x) \vee \neg q(x)],\ \forall x : [s(x) \Rightarrow \neg r(x)]$
$\models \exists x : \neg s(x)$

(C) $\forall x : (p(x) \wedge q(x)), \exists x : (p(x) \Rightarrow (r(x) \wedge q(x))), \forall x : \neg s(x),$
$\forall x : (r(x) \Rightarrow (s(x) \vee t(x)))\qquad \models \exists x : t(x)$

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

(E) $\forall x : (p(x) \Rightarrow (q(x) \wedge r(x)))\ ,\ \forall x : [p(x) \wedge s(x)]\qquad \models \forall x : (r(x) \wedge s(x))$

(F) $\exists x : P(x)\ \vee\ \exists x : Q(x)\ ,\ \forall x : (P(x) \Rightarrow Q(x))\qquad \models \exists x : Q(x)$

(G) $\forall x : (P(x) \Rightarrow \forall y : (Q(x) \Rightarrow R(x,y)))\ ,\ \exists x : (P(x) \wedge \exists y : \neg R(x,y))$
$\models \exists x : \neg Q(x)$

Rešitev. *Vsi sklepi so resnični. Natančno naredimo le (a) in (d). Pri vseh je treba paziti predvsem, da najprej naredimo ES, šele nato US, saj lahko nato uporabimo isto omejenko kot pri ES. Omenimo še, da (f) rešimo enostavno z RA in da je (g) pravzaprav enak sklep kot (d), le da negiramo drugo predpostavko in zaključek. Tudi pri točki (a) uporabimo RA, vendar je najprej smiselno predelati zaključek*

$$\forall x : (\neg r(x) \Rightarrow p(x)) \sim \neg(\neg\forall x : (r(x) \vee p(x))) \sim \neg\exists x : (\neg r(x) \wedge \neg p(x)).$$

Sedaj pa začnemo z RA točke (a).

1.	$\forall x:\ (p(x) \vee q(x))$	*(predpostavka)*
2.	$\forall x:\ [(\neg p(x) \wedge q(x)) \Rightarrow r(x)]$	*(predpostavka)*
3.1.	$\exists x : (\neg r(x) \wedge \neg p(x))$	*(predpostavka RA)*
3.2.	$\neg r(w) \wedge \neg p(w)$	*(ES točke 3.1, x/w omejenka)*
3.3	$\neg r(w)$	*(Po točke 3.2)*
3.4.	$\neg p(w)$	*(Po točke 3.2)*
3.5.	$p(w) \vee q(w)$	*(US točke 1. x/w)*
3.6.	$q(w)$	*(DS točk 3.4 in 3.5)*
3.7.	$\neg p(w) \wedge q(w)$	*(Zd točk 3.4 in 3.6)*
3.8.	$(\neg p(w) \wedge q(w)) \Rightarrow r(w)$	*(US točke 2 x/w)*
3.9.	$r(w)$	*(MP točk 3.8 in 3.7)*
3.10.	$r(w) \wedge \neg r(w) \sim 0$	*(Zd točk 3.9 in 3.3)*
3.	$\neg\exists x : (\neg r(x) \wedge \neg p(x))$	*(RA točk 3.1 in 3.10).*

Ker je zadnja vrstica enakovredna zaključku, smo sklep (a) dokazali. Nadaljujemo s sklepom (d).

1.	$\forall x : (P(x) \Rightarrow \forall y : (Q(y) \Rightarrow R(x,y)))$	*(predpostavka)*
2.	$\neg\forall x : (P(x) \Rightarrow \forall y : R(x,y))$	*(predpostavka)*
3.	$\exists x : \neg(\neg P(x) \vee \forall y : R(x,y))$	*($\sim$ točki 2)*
4.	$\exists x : (P(x) \wedge \exists y : \neg R(x,y))$	*($\sim$ točki 3)*
5.	$P(w) \wedge \exists y : \neg R(w,y)$	*(ES točke 4, x/w omejenka)*
6.	$P(w)$	*(Po točke 5)*
7.	$\exists y : \neg R(w,y)$	*(Po točke 5)*
8.	$P(w) \Rightarrow \forall y : (Q(y) \Rightarrow R(w,y))$	*(US točke 1, x/w)*
9.	$\forall y : (Q(y) \Rightarrow R(w,y))$	*(MP točk 6 in 8)*
10.1.	$\forall x : Q(x)$	*(predpostavka RA)*
10.2.	$Q(c)$	*(US točke 10.1, x/c neomejenka)*
10.3.	$Q(c) \Rightarrow R(w,c)$	*(US točke 9, x/c)*
10.4.	$\neg R(w,w')$	*(ES točke 7, y/w' nova omejenka)*
10.5.	$R(w,c)$	*(MP točk 10.2 in 10.3)*
10.6	$R(w,w')$	*(prilagoditev točke 10.5 c/w')*
10.7	$\neg R(w,w') \wedge R(w,w') \sim 0$	*(Zd točk 10.4 in 10.6)*
10	$\neg\forall x : Q(x)$	*(RA točk 10.1 in 10.7).*

Vaja 1.7 *Naslednje sklepe prevedite v izjavni račun ter jih dokažite, ali poiščite protiprimer zanje.*

(A) *Danes se potim in mi je vroče. Če se potim, delam in mi je vroče. Če delam, dobim denar, ali naredim komu uslugo. Nimam denarja. Sklepam, da sem naredil komu uslugo.*

(B) *Študent, ki ima naslednji dan izpit, si reče: če bo jutri dež, bom naredil. Naslednji dan je lepo vreme. Ali to pomeni, da je študent padel na izpitu?*

(C) *Računalničar, ki dobro obvlada teorijo, vedno naredi dober program. Dober program je lahko prodati. Torej: računalničar, ki ne proda svojega programa, ne obvlada dobro teorije.*

(D) *Zmagal bo ali Popaj ali Silak. Če zmaga Popaj, bo Oliva vesela. Torej: če zmaga Silak, Oliva ne bo vesela.*

(E) *Samo pripravljeni študentje naredijo izpit. Nekateri študentje niso naredili izpita. Torej nekateri študentje niso bili pripravljeni.*

(F) *Barona je umoril nekdo izmed njegovega osebja: kuharica, strežnik ali šofer. Če je morila kuharica, je bil zastrupljen s hrano. Če je kriv šofer, je bil vzrok smrti bomba. Hrana ni zastrupljena in strežnik ni morilec. Torej: morilec je šofer!*

(G) *V trgovino grem natanko tedaj, ko mi naroči mama. Če mi mama naroči, tudi pokosim travo. Ali bom pokosil travo, ali šel v kino. Če grem v kino, bom povedal mami. To pomeni: Ne grem v kino!*

(H) *Vsi telovadci so gibčni. Peter je okoren. Torej Peter ni telovadec!*

(I) *Če delam, imam denar. Če lenarim, sem zadovoljen. Če lenarim, nimam denarja. Če delam, nisem zadovoljen. Lahko ali delam, ali lenarim. Ali je res, da sem zadovoljen samo, če nimam denarja.*

(J) *Šel bom na tekmo. Zvečer bom napisal nalogo. Če grem na tekmo in nato še v kino, ne bom utegnil napisati naloge. Ali lahko sklepamo, da ne morem iti v kino?*

(K) *Ta žival ali ni ptič, ali pa ima krila. Če je ta žival ptič, potem leže jajca. Ta žival nima kril, zato ne leže jajc!*

Rešitev. *Resnični so sklepi (a), (c), (e), (f), (g), (h), (i) in (j). Preostali so neresnični. Zapišimo jih v izjavnem računu (imena za izjave so določena po začetnicah ali splošnih simbolih) in nekatere izmed njih tudi komentirajmo. Predpostavke za (a) so $p \wedge v$, $p \Rightarrow d \wedge v$, $d \Rightarrow \$ \vee u$ in $\neg\$$, ob tem ko je u zaključek. Sklep (b) sestavljata dve predpostavki $d \Rightarrow i$ in $\neg d$, zaključek pa je $\neg i$. Njegov protiprimer je $d \sim 0$ in $i \sim 1$. Sklep (c) ima predpostavki $T \Rightarrow DP$ in $DP \Rightarrow PR$, zaključek pa je $\neg PR \Rightarrow \neg T$. Dokažemo ga s pogojnim sklepom. Protiprimer za sklep (d) je $P \sim 0$, $S \sim 1$ in $Ol \sim 1$, medtem ko je sklep $P \veebar S$, $P \Rightarrow Ol \vDash S \Rightarrow \neg Ol$. Predpostavki sklepa (e) sta $\forall x : P(x) \Rightarrow I(x)$ in $\exists x : \neg I(x)$, zaključek $\exists x : \neg P(x)$ zlahka dokažemo. Tudi dokaz zaključka $\vDash$ š sklepa (f) ni težko dokazati iz predpostavk $k \vee s \vee$ š, $k \Rightarrow h$, š $\Rightarrow b$, $\neg h$ in $\neg s$. Sklep (g) je zahtevnejši in ga pokažimo v celoti:*

1.	$m \Rightarrow t$	*(predpostavka)*
2.	$t \veebar k$	*(predpostavka)*
3.	$k \Rightarrow m$	*(predpostavka)*
4.	$(t \wedge \neg k) \vee (\neg t \wedge k)$	*($\sim$ 2)*
5.1.	k	*(predpostavka RA)*
5.2.	m	*(MP točk 3 in 5.1)*
5.3.	t	*(MP točk 1 in 5.2)*
5.4.	$\neg t \vee k$	*(Pr točki 5.1)*
5.5.	$\neg(t \wedge \neg k)$	*($\sim$ 5.4)*
5.6.	$\neg t \wedge k$	*(DS točke 4 in 5.5)*
5.7.	$\neg t$	*(Po točke 5.6)*
5.8.	$t \wedge \neg t \sim 0$	*(Zd točk 5.3 in 5.7)*
5.	$\neg k$	*(RA točk 5.1 in 5.8).*

Sklep $\forall x : T(x) \Rightarrow G(x)$, $\neg G(P) \vDash \neg T(P)$ iz (h) zlahka dokažemo. V sklepu (i), ki se glasi $D \Rightarrow \$$, $L \Rightarrow Z$, $L \Rightarrow \neg\$$, $D \Rightarrow \neg Z$, $D \veebar L \vDash \neg\$ \Rightarrow Z$, uporabimo podoben trik v zvezi z ekskluzivnim ali, kot v primeru (g). Sklep (j) je ponovno preprost in sklep (k) ni resničen.

Vaja 1.8 *Prevedi v izjavni račun naslednji pogovor, ki je (menda) potekal med očetom in sinom v antični Grčiji, in preveri ali sta sklepa pravilna.*

Oče: "Če boš pošten, ti bodo nasprotovali bogati in močni. Če boš lagal, ti bodo nasprotovali preprosti ljudje. Lahko si le ali poštenjak, ali lažnivec. Torej: ali ti bodo nasprotovali bogati in močni, ali pa preprosti ljudje."

Sin: "Če bom poštenjak, me bo podpiralo ljudstvo. Če bom lažnivec, me bodo podpirali bogati in močni. Ker sem lahko ali lažnivec, ali poštenjak, me bodo podpirali ali bogati in močni, ali pa preprosto ljudstvo."

Rešitev. *Oba sklepa sta napačna.*

2

TEORIJE

V tem poglavju bomo spoznali in postavili temelje za matematične modele, ki so zgrajeni na aksiomih. Aksiomi so (preproste) trditve, ki jih proglasimo za resnične in bi jih lahko primerjali s temelji hiše. S pomočjo aksiomov potem izpeljemo, ugotavljamo, dokazujemo in podobno, katere izjave imajo poseben status—rečemo, da so izreki.

Začeli bomo s še enim zelo pomembnim načinom dokazovanja in sicer z matematično indukcijo. To je metoda, s katero lahko dokazujemo izreke, ki vsebujejo naravna števila.

Ta postopek bomo nato posplošili in model iz naravnih števil prenesli na razrede objektov, ki jih dobimo tako, da iz nekaterih podanih elementov zgradimo celoten razred elementov s pomočjo podanih pravil. Takšnim razredom bomo rekli induktivni razredi.

Ker so induktivni razredi sestavni del deduktivnih teorij, to je splošnih matematičnih teorij, ki jih lahko zgradimo iz množice aksiomov, bomo pridobljeno znanje izkoristili, da si ogledamo še osnovne lastnosti teorij.

Zapisano je smiselno, ker lahko tudi računalniške algoritme predstavimo kot teorije. Tako teorije predstavljajo teoretični model za preučevanje algoritmov is so zanimive tudi v računalništvu.

Dodatno literaturo v slovenščini iz tega področja je moč najti v [3] in [11]. Standardna zbirka nalog za to poglavje je [4]. Veliko izpitnih nalog iz tega poglavja je najti v [12, 13].

2.1 MATEMATIČNA INDUKCIJA

V osnovni šoli se običajno naravna števila, ki jih označimo z $\mathbb{N}$, definirajo kot tista števila, s katerimi štejemo. Lahko štejemo samo s sodimi števili, da smo hitrejši (recimo otroke v vrtcu, ki se morajo postaviti po parih). Štejemo lahko tudi dele celote (pojedel je tri kose torte, pico so razrezali na osem kosov in podobno), kar pomeni, da lahko posredno preštevamo tudi z ulomki. Tako nam takšna definicija ne more zadoščati. Matematično natančno definiramo naravna števila s Peanovimi[3] aksiomi, ki sledijo.

P_1. 1 je naravno število ($1 \in \mathbb{N}$).

P_2. Vsako naravno število n ima svojega naslednika $n+1$ med naravnimi števili ($\forall n \in \mathbb{N} : n \in \mathbb{N} \Rightarrow n+1 \in \mathbb{N}$).

P_3. Različni naravni števili imata različna naslednika ($\forall n, m \in \mathbb{N} : n \neq m \Rightarrow n+1 \neq m+1$).

P_4. 1 ni naslednik naravnega števila ($\forall n \in \mathbb{N} : 1 \neq n+1$).

P_5. Vsaka množica, ki vsebuje 1 in z vsakim naravnim številom n tudi njegovega naslednika, vsebuje vsa naravna števila ($\forall S, \forall n \in \mathbb{N} : (1 \in S \wedge (n \in S \Rightarrow n+1 \in S) \Rightarrow \mathbb{N} \subseteq S)$).

O aksiomu P_1 ni vredno izgubljati besed, saj je bolj naraven aksiom težko najti. Aksiom P_2 zagotavlja naslednika vsakemu naravnemu številu. Tako je smiselna naslednja funkcija $f : \mathbb{N} \to \mathbb{N}$, ki je definirana s predpisom $f(n) = n+1$. V luči pravkar definirane funkcije f nam aksiom P_3 pove, da je f injektivna funkcija, saj sta sliki različnih elementov različni. Po drugi strani aksiom P_4 zagotavlja, da f ni surjektivna, saj 1 ni slika elementa iz $\mathbb{N}$.

Posebno mesto med Peanovimi aksiomi zavzema aksiom P_5, ki je na prvi pogled zahtevnejši od preostalih štirih. Potreben je, ker aksiomi P_1, P_2, P_3 in P_4 sicer zagotavljajo, da smo dobili vsa naravna števila, kot smo jih navajeni, vendar ne garantirajo, da ni zraven še česa. Seveda ne želimo nobenega dodatka k številu 1 in vsem naslednikom, ki jih dobimo, če začnemo z 1.

Opazimo lahko, da prve štiri Peanove aksiome lahko zapišemo s predikatnim računom, kot smo to storili. Pozoren bralec bo tudi opazil, da se simbolni zapis aksioma P_5 razlikuje od predikatnega računa, kot smo ga spoznali. Razlog za to je v prvem kvantifikatorju $\forall$, ki se nahaja pred množico in ne pred spremenljivko. Tako zapisane trditve spadajo v logiko drugega reda, ki ni predmet tega učbenika.

3 Giuseppe Peano (1858-1932) je bil italijanski matematik, ki se je ukvarjal z matematično logiko. Najbolj znan je ravno po aksiomih za naravna števila. Vpeljal pa je tudi moderna simbola za presek in unijo, ki sta v veljavi še danes.

Dodatna pozitivna lastnost aksioma P_5 je, da nam omogoča dokazovanje trditev, ki vsebujejo naravna števila, da so resnične za vsa naravna števila. Temu postopku rečemo **matematična indukcija** in je sestavljen iz dveh korakov: **baze indukcije** in **indukcijskega koraka**. Naj bo T trditev, ki vsebuje naravna števila in naj množica S vsebuje vsa števila, za katera je T resnična. Trditev T dokažemo za vsa naravna števila z matematično indukcijo na naslednji način.

1. Pokažemo, da je T resnična za 1 ($1 \in S$).
2. Pokažemo, da je za vsako naravno število n resnična implikacija: če je T resnična za naravno število n, potem je T resnična tudi za $n+1$ ($\forall n \in \mathbb{N} : n \in S \Rightarrow n+1 \in S$).

Točka 1 je baza matematične indukcije in točki 2 rečemo indukcijski korak. Če smo uspeli pokazati resničnost baze in indukcijskega koraka za T, potem po P_5 velja, da je $\mathbb{N} \subseteq S$ in trditev T velja za vsa naravna števila. Omenimo še, da v indukcijskem koraku dokazujemo implikacijo, kar seveda naredimo s pogojnim sklepom, kjer predpostavimo resničnost prvega dela implikacije: T je resnična za naravno število n, oziroma $n \in S$. Zato ta del poimenujemo tudi **indukcijska predpostavka**. Če v postopku dokazovanja indukcijske predpostavke ne uporabimo, potem smo ali naredili napako, ali pa lahko trditev T dokažemo tudi brez uporabe matematične indukcije.

Omenimo še **popolno indukcijo**, ki se od matematične indukcije razlikuje v indukcijski predpostavki in da je baza posredno vključena v indukcijski korak. Tako jo lahko zapišemo le z enim predpisom:

$$\text{če je } T \text{ resnična za vsa naravna števila } \leq n, \text{ potem je } T \text{ resnična tudi za } n+1$$
$$(\forall n \in \mathbb{N} : [n] \subseteq S \Rightarrow n+1 \in S).$$

Oba postopka indukcije sta med seboj enakovredna, kar je razvidno iz naslednjega izreka.

Izrek 2.1 *Trditev T lahko dokažemo z matematično indukcijo natanko tedaj, ko lahko T dokažemo s popolno indukcijo.*

Dokaz. Za dokaz ekvivalence bomo dokazali obe implikaciji. Predpostavimo najprej, da trditev T lahko dokažemo z matematično indukcijo in naj bo $n \in \mathbb{N}$. Ker lahko T dokažemo z matematično indukcijo, je resnična za vsa naravna števila $\leq n$, s čimer je resničen prvi del implikacije, ki predstavlja popolno indukcijo. Po matematični indukciji je trditev T resnična tudi za $n+1$, s čimer je resničen tudi drugi del popolne indukcije. Torej lahko T dokažemo tudi s popolno indukcijo.

Obratno recimo, da lahko T dokažemo s popolno indukcijo in naj bo $n \in \mathbb{N}$. Ker lahko T dokažemo s popolno indukcijo, je T resnična za vsa naravna števila in s tem tudi za 1 ter za n, kar pomeni, da sta baza in indukcijska predpostavka resnični. Po popolni indukciji je trditev T resnična tudi za $n+1$, s čimer je resničen tudi drugi del matematične indukcije in T lahko dokažemo tudi z matematično indukcijo. ∎

Zgled 2.1 *Z matematično indukcijo pokažimo resničnost zveze*

$$1+2+\cdots+n=\frac{n(n+1)}{2}.$$

Vpeljimo oznaki $L(n)=1+2+\cdots+n$ *in* $D(n)=\frac{n(n+1)}{2}$*, ki predstavljata levo in desno stran enačaja. Za bazo naj bo* $n=1$ *in imamo* $L(1)=1$ *in* $D(1)=\frac{1(1+1)}{2}=1$*. Torej je baza resnična. Naj bo sedaj izpolnjena indukcijska predpostavka za* $n\in\mathbb{N}$*, torej* $L(n)=D(n)$ *in računajmo*

$$\begin{aligned}L(n+1)&=1+2+\cdots+n+(n+1)=(1+2+\cdots+n)+(n+1)=\\&=L(n)+(n+1)=D(n)+(n+1)=\tfrac{n(n+1)}{2}+(n+1)=\\&=(n+1)\left(\tfrac{n}{2}+1\right)=\tfrac{(n+1)(n+2)}{2}=D(n+1).\end{aligned}$$

Zato velja indukcijski korak in trditev je resnična za vsako naravno število. Omenimo še, da je dobro vidna uporaba indukcijske predpostavke $L(n)=D(n)$*.*

Zgled 2.2 *Z matematično indukcijo pokažimo resničnost zveze*

$$1^2+2^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

Ponovno vpeljimo oznaki $L(n)=1^2+2^2+\cdots+n^2$ *in* $D(n)=\frac{n(n+1)(2n+1)}{6}$*. Za bazo naj bo* $n=1$ *in imamo* $L(1)=1^2=1$ *in* $D(1)=\frac{1(1+1)(2+1)}{6}=\frac{6}{6}=1$*. Baza je ponovno resnična. Naj bo sedaj izpolnjena indukcijska predpostavka za* $n\in\mathbb{N}$*, torej* $L(n)=D(n)$ *in računajmo*

$$\begin{aligned}L(n+1)&=1^2+2^2+\cdots+n^2+(n+1)^2=(1^2+2^2+\cdots+n^2)+(n+1)^2=\\&=L(n)+(n+1)^2=D(n)+(n+1)^2=\tfrac{n(n+1)(2n+1)}{6}+(n+1)^2=\\&=(n+1)\left(\tfrac{n(2n+1)}{6}+(n+1)\right)=(n+1)\tfrac{(2n^2+n)+6(n+1)}{6}=\\&=\tfrac{(n+1)(2n^2+7n+6)}{6}=\tfrac{(n+1)(n+2)(2n+3)}{6}=D(n+1).\end{aligned}$$

Zato velja indukcijski korak in trditev je resnična za vsako naravno število. Ponovno smo uporabili indukcijsko predpostavko $L(n)=D(n)$*, kar je lepo vidno v drugi vrstici izračuna.*

Zgled 2.3 *Pokažimo, da število* 3 *deli vsak izraz oblike* 5^n+2^{n+1} *za* $n\in\mathbb{N}$*. Če želimo pokazati deljivost števila* 5^n+2^{n+1} *s* 3*, to pomeni, da je večkratnik števila tri. Torej želimo pokazati, da je* $5^n+2^{n+1}=3k$ *za nek* $k\in\mathbb{N}$*. Vpeljimo oznako* $P(n)=5^n+2^{n+1}$*. Za bazo naj bo* $n=1$ *in imamo* $P(1)=5^1+2^{1+1}=9=3\cdot 3$*, s čimer je baza izpolnjena. Naj sedaj velja indukcijska predpostavka* $P(n)=5^n+2^{n+1}=3k$ *za nek* $k\in\mathbb{N}$*. Računajmo*

$$\begin{aligned}P(n+1)&=5^{n+1}+2^{n+1+1}=5\cdot 5^n+2\cdot 2^{n+1}=(3+2)\cdot 5^n+2\cdot 2^{n+1}=\\&=3\cdot 5^n+2\cdot 5^n+2\cdot 2^{n+1}=3\cdot 5^n+2\cdot(5^n+2^{n+1})=\\&=3\cdot 5^n+2P(n)=3\cdot 5^n+2\cdot 3k=3(5^n+2k).\end{aligned}$$

Ker je $k \in \mathbb{N}$, je tudi $5^n + 2k \in \mathbb{N}$ in $P(n+1)$ je večkratnik števila 3. S tem je indukcijski korak dokazan in 3 deli vsa števila oblike $5^n + 2^{n+1}$ za $n \in \mathbb{N}$.

Zgled 2.4 *Pokažimo, da za vsako naravno število $n \geq 2$ in za vsako realno število x, kjer je $0 < x < 1$, velja $(1-x)^n > 1 - nx$. Omenimo takoj, da pogoj $n \geq 2$, ne pomeni, da lahko izpustimo bazo indukcije. Pravzaprav niti matematične indukcije ne bi smeli uporabiti, saj je to orodje za vsa naravna števila, ta trditev pa ne velja za ena. Tej težavi se formalno izognemo z vpeljavo nove spremenljivke $m = n - 1$, kjer je sedaj m poljubno naravno število in lahko delamo indukcijo za m. Ob tem je v bazi $m = 1$, kar prevedeno pomeni, da je $n = 2$. Običajno se v podobnih primerih vpeljavi nove spremenljivke kar izognemo in naredimo bazo indukcije za $n = 2$. Preden se lotimo računanja, vpeljimo ponovno oznaki $L(n) = (1-x)^n$ in $D(n) = 1 - nx$. Za $n = 2$ imamo*

$$L(2) = (1-x)^2 = 1 - 2x + x^2 > 1 - 2x = D(2),$$

saj je $x^2 > 0$ zaradi pogoja $x > 0$. Tako je baza izpolnjena. Za indukcijski korak predpostavimo resničnost indukcijske predpostavke $L(n) > D(n)$. Ponovno računajmo

$$\begin{aligned} L(n+1) = (1-x)^{n+1} = (1-x)(1-x)^n = (1-x)L(n) > (1-x)D(n) = \\ = (1-x)(1-nx) = 1 - (n+1)x + nx^2 > 1 - (n+1)x = D(n+1), \end{aligned}$$

kjer prva neenakost drži zaradi indukcijske predpostavke, druga pa, ker je $nx^2 > 0$, saj je $n \geq 2$ in $x > 0$. S tem je trditev dokazana. Z nekaj znanja o neenačbah lahko opazimo, da ta izračun ne drži v primeru, ko je $x > 1$, saj za lih $n+1$ velja $L(n+1) < 0$, medtem ko je člen iz izračuna $(1-x)(1-nx)$ pozitiven. Po drugi strani ni težko opaziti, da je trditev resnična tudi, če je $x = 1$ (direktno brez matematične indukcije), ali $x < 0$ (z matematično indukcijo).

Zgled 2.5 *Z $f_{n+2} = f_{n+1} + f_n$, $f_1 = f_2 = 1$, je definirano Fibonaccijevo zaporedje $(1, 1, 2, 3, 5, 8, 13, \ldots)$. Pokažimo, da za vsak $n \geq 4$, $n \in \mathbb{N}$, velja*

$$\left(\frac{3}{2}\right)^{n+1} < f_{n+2}. \tag{1}$$

Tokrat bomo uporabili popolno indukcijo. Kot običajno označimo desno in levo stran neenačbe z $L(n) = \left(\frac{3}{2}\right)^{n+1}$ in $D(n) = f_{n+2}$. Začnimo z bazo, ki jo moramo sedaj narediti za $n = 4$ in $n = 5$. Velja

$$\begin{aligned} L(4) &= \left(\frac{3}{2}\right)^5 = \frac{243}{32} < 8 = f_6 = D(4), \\ L(5) &= \left(\frac{3}{2}\right)^6 = \frac{729}{64} < 13 = f_7 = D(5), \end{aligned}$$

s čimer je baza zaključena. Vprašanje, zakaj smo bazo naredili za dve vrednosti, bo odgovorjeno z indukcijskim korakom, kjer bomo morali uporabiti dve prejšnji vrednosti. Slednje je tudi razlog, da moramo uporabiti popolno namesto matematične indukcije.

Predpostavimo torej, da je pogoj (1) resničen za vsa naravna števila med štiri in $n \geq 5$. Še posebej potrebujemo resničnost (1) za n in $n-1$: torej $L(n) = \left(\frac{3}{2}\right)^{n+1} < f_{n+2} = D(n)$, oziroma $L(n-1) = \left(\frac{3}{2}\right)^{n} < f_{n+1} = D(n-1)$. Računajmo

$$\begin{aligned} L(n+1) = \left(\tfrac{3}{2}\right)^{n+2} = \tfrac{3}{2}\left(\tfrac{3}{2}\right)^{n+1} = \left(\tfrac{3}{2}\right)^{n+1} + \tfrac{1}{2}\left(\tfrac{3}{2}\right)^{n+1} = \\ = \left(\tfrac{3}{2}\right)^{n+1} + \tfrac{3}{4}\left(\tfrac{3}{2}\right)^{n} = L(n) + \tfrac{3}{4}L(n-1) < L(n) + L(n-1) < \\ < D(n) + D(n-1) = f_{n+2} + f_{n+1} = f_{n+3} = D(n+1). \end{aligned}$$

Kot vidimo, smo v računu uporabili indukcijsko predpostavko za n in tudi za $n-1$, zaradi česar smo tudi bazo morali narediti za najmanjši dve števili 4 in 5.

2.2 INDUKTIVNA POSPLOŠITEV

V tem razdelku bomo matematično indukcijo posplošili, da bo uporabna na množicah, ki so strukturno pogosto bolj bogate od naravnih števil. Oglejmo si najprej množice, o katerih je govora. Zgled zanje nam lahko predstavljajo kar naravna števila, saj lahko vsako naravno število n dobimo iz prvega naravnega števila 1, če le dovolj krat, to je $n-1$-krat, izvedemo operacijo naslednika. Tako dobimo 5 iz 1 tako, da je naslednik od 1 število 2, njegov naslednik je 3, le-temu sledi 4 in naslednik od 4 je 5. Tako lahko naravna števila predstavimo v dveh korakih: z bazo $1 \in \mathbb{N}$ in pravilom $n \in \mathbb{N} \Rightarrow n+1 \in \mathbb{N}$, ki predstavlja notranjost operacije naslednik.

Če omenjena koraka sprostimo do te mere, da dovolimo več elementov v bazi ter tudi več pravil, govorimo o induktivnih razredih. Tako **induktivni razred** $\mathcal{I}_n(\mathcal{B}, \mathcal{P})$ sestavljata **baza** $\mathcal{B}$, ki je neka množica elementov, in **pravila** $\mathcal{P}$, ki povedo, kako iz že obstoječih elementov iz $\mathcal{I}_n$ zgradimo nove elemente v $\mathcal{I}_n$. Če je množica K enaka induktivnemu razredu $\mathcal{I}_n(\mathcal{B}, \mathcal{P})$, potem rečemo tudi, da je K **definirana induktivno**. Dogovorimo se, da bomo za neko pravilo $P_i \in \mathcal{P}$ in elemet $x \in \mathcal{I}_n(\mathcal{B}, \mathcal{P})$ s $P_i(x)$ označili element, ki ga dobimo iz x, če na njem uporabimo pravilo P_i. Oglejmo si nekaj zgledov.

Zgled 2.6 *Kot že omenjeno, so naravna števila induktiven razred, ki ga lahko pišemo kot $\mathbb{N} = \mathcal{I}_n(\mathcal{B}, \mathcal{P})$, kjer je $\mathcal{B} = \{1\}$ in v $\mathcal{P}$ je zgolj eno pravilo $n \in \mathbb{N} \Rightarrow n+1 \in \mathbb{N}$.*

Zgled 2.7 *Naj bo Σ množica simbolov, ki ji rečemo abeceda. Nad abecedo Σ lahko sestavljamo besede, ki predstavljajo poljubna (končna) zaporedja simbolov iz Σ. Tako lahko sestavimo induktivni razred tako, da nekatere besede proglasimo za bazne (baza je lahko tudi prazna), zraven pa še določimo pravila, ki bodo določala, kaj lahko zgradimo iz baznih elementov. Če je recimo $\Sigma = \{x, y, w\}$, potem so nekatere besede nad Σ naslednje*

$$xxxxyyywxyyxw, xywyxwxywyxw, xxx, wywywwyy, yyyxxwxxyyy$$

in tako naprej. Če je v besedi več zaporednih znakov enakih, jih zaradi preglednosti običajno pišemo kot potenco, kar pomeni

$$xxxxyyywxyyxw = x^4y^3wxy^2xw, xxx = x^3, yyyxxwxxyyy = y^3x^2wx^2y^3.$$

Definirajmo še bazo $\mathcal{B} : w \in \mathcal{I}_n$ in pravila $\mathcal{P}$, ki jih v tem primeru sestavljata dve pravili $P_1 : z \in \mathcal{I}_n \Rightarrow zy \in \mathcal{I}_n$ in $P_2 : z \in \mathcal{I}_n \Rightarrow xzy^2 \in \mathcal{I}_n$. Ob tem omenimo, da je z, ki nastopa v obeh pravilih, katerikoli element iz induktivnega razreda $\mathcal{I}_n$. Oglejmo si, kaj dobimo iz baze, z nekajkratno uporabo pravila P_1:

$$w \xrightarrow{P_1} wy \xrightarrow{P_1} wyy = wy^2 \xrightarrow{P_1} wy^3 \underbrace{\xrightarrow{P_1} \cdots \xrightarrow{P_1}}_{k-3\text{-krat}} wy^k.$$

Podobno lahko nekajkrat uporabimo pravilo P_2 in dobimo

$$w \xrightarrow{P_2} xwy^2 \xrightarrow{P_2} x^2wy^4 \xrightarrow{P_2} x^3wy^6 \underbrace{\xrightarrow{P_2} \cdots \xrightarrow{P_2}}_{\ell-3\text{-krat}} x^\ell wy^{2\ell}.$$

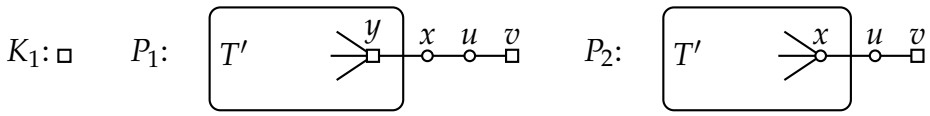
Seveda lahko obe pravili izvajamo tudi izmenično in ni težko videti, da v zaporedju, kjer izvršimo pravilo P_1 k-krat in pravilo P_2 ℓ-krat (ne nujno v tem vrstnem redu), dobimo element $x^\ell wy^{k+2\ell}$ za poljubna $k, \ell \in \mathbb{N}_0$. Tako so vsi elementi množice

$$K_1 = \{x^\ell wy^{k+2\ell} : k, \ell \in \mathbb{N}_0\}$$

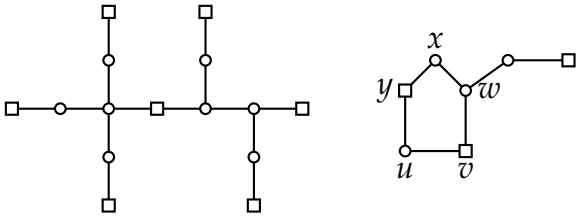
pripadajo našemu induktivnemu razredu $\mathcal{I}_n$ in velja $K_1 \subseteq \mathcal{I}_n$. Kasneje bomo pokazali enakost med K_1 in $\mathcal{I}_n$. Oglejmo si še besedi xw ter $x^2w^3y^6$, ki nista iz $\mathcal{I}_n$. Pravilo P_2 je edino, ki doda x levo od w, vendar hkrati prinese še y^2 desno od w. Ker pa ni pravila, ki bi odvzemalo y iz desne strani w, lahko sklenemo, da $xw \notin \mathcal{I}_n$. Podobno $x^2w^3y^6$ ni iz $\mathcal{I}_n$, saj nobeno pravilo ne doda w (čeprav bi x^2 na levi in y^6 na desno od w lahko dobili, če dvakrat uporabimo P_1 in dvakrat P_2).

Zgled 2.8 *Model, ki prav tako lahko predstavlja induktivni razred so grafi, o katerih bomo podrobneje govorili v zadnjem poglavju. Graf G je sestavljen iz množice vozlišč $V(G)$ in množice povezav $E(G)$, kjer je $E(G)$ množica nekaterih neurejenih parov vozlišč. Običajno si poenostavimo zapis in namesto $\{u, v\} \in E(G)$ pišemo kar $uv \in E(G)$. Vozlišča najpogosteje predstavimo s točkami v ravnini, povezavo $uv \in E(G)$, kjer sta $u, v \in V(G)$, pa predstavimo s črto (ravno ali krivo) med vozliščema u in v. Oglejmo si primer induktivnega razreda $\mathcal{G}_n(\mathcal{B}, \mathcal{P})$ na grafih, kjer so vozlišča nadalje ločena na kvadratna in okrogla. V bazi $\mathcal{B}$ je graf, ki vsebuje le eno kvadratno vozlišče. Običajno ga označimo s K_1. V $\mathcal{P}$ sta dve pravili P_1 in P_2. Za pravilo P_1 naj bo graf G' iz induktivnega razreda $\mathcal{I}_n$ in y kvadratno vozlišče iz G'. Potem je v $\mathcal{G}_n$ tudi graf G, ki mu dodamo dve okrogli vozlišči x in u in eno kvadratno vozlišče v ter povezave yx, xu in uv. Pravilo P_2 nam iz grafa $G' \in \mathcal{G}_n$ in okroglega vozlišča $x \in V(G')$ naredi graf $G \in \mathcal{G}_n$ tako, da dodamo okroglo vozlišče u in kvadratno vozlišče v ter povezavi uv in xu. Baza $\mathcal{B}$ ter pravili P_1 in P_2 sta predstavljeni na sliki 1. Ni težko videti, da lahko na baznem*

elementu uporabimo le pravilo P_1, saj graf iz baze K_1 ne vsebuje okroglega vozlišča. Levi graf s slike 2 lahko dobimo iz baznega elementa, če zapored uporabimo dvakrat pravilo P_1 in nato štirikrat pravilo P_2 (za ustrezna okrogla vozlišča) ali pravilo P_1, nato dvakrat pravilo P_2, spet pravilo P_1 in še dvakrat pravilo P_2. Desni graf s slike 2 ni predstavnik induktivnega razreda $\mathcal{G}_n$, saj vsebuje cikel $xyuvw$ (to je zaporedje različnih vozlišč, kjer obstaja povezava med dvema zaporednima vozliščema in tudi med prvim in zadnjim vozliščem, ki ga ne moremo dobiti iz baznega grafa K_1 z zaporedno uporabo pravil P_1 in P_2.



Slika 1: Pravili P_1 in P_2 iz zgleda 2.8.



Slika 2: Grafa za zgled 2.8.

Naj bo $\mathcal{I}_n(\mathcal{B},\mathcal{P})$ induktivni razred in $x \in \mathcal{I}_n$. Zaporedju pravil, s katerim iz baznih elementov dobimo element x, rečemo **konstrukcijsko zaporedje** elementa x. Če ima vsak element iz $\mathcal{I}_n(\mathcal{B},\mathcal{P})$ natanko eno konstrukcijsko zaporedje, rečemo, da je induktivni razred $\mathcal{I}_n(\mathcal{B},\mathcal{P})$ **enoumen**. Sicer, v primeru da imajo nekateri elementi dva ali več različnih konstrukcijskih zaporedij, govorimo o **dvoumnih**, oziroma **večumnih** induktivnih razredih. Naravna števila predstavljajo primer enoumnega indukcijskega razreda, medtem ko je induktivni razred iz zgleda 2.7 večumen, saj lahko pravili P_1 in P_2 pri uporabi poljubno premešamo. Tudi induktivni razred $\mathcal{G}_n(\mathcal{B},\mathcal{P})$ iz zgleda 2.8 je večumen, kot je razvidno že iz levega grafa s slike 2.

Osnovno vprašanje, ki govori o razmerju med elementi, ki so na razpolago in indukcijskem razredu, je sledeče.

$$\text{Ali element } x \text{ pripada induktivnemu razredu } \mathcal{I}_n(\mathcal{B},\mathcal{P}) \text{ ali ne?} \qquad (2)$$

Seveda sta možna odgovora le DA ali NE. Z DA odgovorimo, če lahko najdemo konstrukcijsko zaporedje elementa x v induktivnem razredu $\mathcal{I}_n(\mathcal{B},\mathcal{P})$. Če pa najdemo kako lastnost, ki jo x ima, elementi iz $\mathcal{I}_n(\mathcal{B},\mathcal{P})$ pa ne, je odgovor na zgornje vprašanje NE.

Ob tem se poraja vprašanje, kako preveriti, ali ima induktivni $\mathcal{I}_n(\mathcal{B}, \mathcal{P})$ razred neko lastnost Q? Ta problem lahko rešimo z **induktivno posplošitvijo**, ki je, kot pove že ime samo, posplošitev matematične indukcije. Kot matematična indukcija, je tudi induktivna posplošitev sestavljena iz dveh korakov.

1. Pokažemo, da imajo vsi elementi iz baze $\mathcal{B}$ lastnost Q.
2. Pokažemo, da vsa pravila iz $\mathcal{P}$ ohranjajo lastnost Q.

V prvem koraku postopamo podobno kot pri bazi matematične indukcije, le da tukaj pokažemo lastnost Q za vse elemente iz baze. V drugem koraku moramo za vsako pravilo $P_i \in \mathcal{P}$ pokazati, da, če ima element x iz induktivnega razreda $\mathcal{I}_n(\mathcal{B}, \mathcal{P})$ lastnost Q, potem ima lastnost Q tudi element $P_i(x)$. Povedano drugače, želimo resničnost implikacije

$$x \in \mathcal{I}_n(\mathcal{B}, \mathcal{P}) \text{ ima lastnost } Q \Rightarrow P_i(x) \text{ ima lastnost } Q$$

za vsako pravilo $P_i \in \mathcal{P}$. Implikacijo seveda dokazujemo s Pogojnim sklepom, kar pomeni, da predpostavimo resničnost prvega dela implikacije $x \in \mathcal{I}_n(\mathcal{B}, \mathcal{P})$. Tej predpostavki rečemo **predpostavka induktivne posplošitve** ali pogosto kar **indukcijska predpostavka** kot pri matematični indukciji.

Zgled 2.9 *Z induktivno posplošitvijo pokažimo, da ima induktivni razred $\mathcal{G}_n(\mathcal{B}, \mathcal{P})$ iz zgleda 2.8 naslednje lastnosti:*

Q_1 *: če je $G \in \mathcal{G}_n(\mathcal{B}, \mathcal{P})$, potem G sestavlja le en del;*

Q_2 *: če je $G \in \mathcal{G}_n(\mathcal{B}, \mathcal{P})$, potem G nima ciklov*[4]*;*

Q_3 *: če je $G \in \mathcal{G}_n(\mathcal{B}, \mathcal{P})$, potem ima vsako okroglo vozlišče iz G natanko enega kvadratnega soseda v G;*

Q_4 *: če je $G \in \mathcal{G}_n(\mathcal{B}, \mathcal{P})$, potem sta med poljubnima kvadratnima vozliščema iz G vsaj dve okrogli vozlišči.*

*V naslednjih obrazložitvah si je smiselno pomagati s sliko 2. Grafu z lastnostjo Q_1 bomo kasneje rekli, da je **povezan**. Seveda je kvadratno vozlišče K_1 iz baze sestavljeno iz le enega dela. Naj bo sedaj $G' \in \mathcal{G}_n(\mathcal{B}, \mathcal{P})$. Naša indukcijska predpostavka je, da je G' sestavljen iz le enega dela. Pravilo P_1 nam h grafu G' in (kvadratnemu) vozlišču y doda vozlišča x, u in v ter povezave yx, xu in uv. Tako vozlišča x, u in v tvorijo en del zaradi povezav xu in uv. Hkrati je ta del preko povezave yx povezan z grafom G'. Ker je G' sestavljen iz enega dela, je tudi nov graf G dobljen iz G' s pravilom P_1 sestavljen iz le enega dela. Podobno nam pravilo P_2 h grafu G' in (okroglemu) vozlišču x doda vozlišču u in v ter povezavi uv in xu. Ker je G' sestavljen iz enega dela, nam povezavi xu in uv zagotavljata, da je tudi graf G, dobljen iz G' s pravilom P_2, sestavljen iz le enega dela.*

4 Za natančno definicijo cikla glejte razdelek 9.1.

Tako obe pravili ohranjata lastnost Q_1, s čimer je induktivna posplošitev končana. Tako imajo vsi elementi induktivnega razreda $\mathcal{G}_n(\mathcal{B},\mathcal{P})$ lastnost Q_1, oziroma so sestavljeni iz enega dela.

Za Q_2 je cikel v grafu zaporedje različnih vozlišč, kjer obstaja povezava med zaporednimi vozlišči kot tudi med prvim in zadnjim. Seveda element baze nima cikla, s čimer je baza induktivne posplošitve zaključena. Naj bo sedaj $G' \in \mathcal{G}_n(\mathcal{B},\mathcal{P})$. Naša indukcijska predpostavka je, da je G' brez cikla. Obe pravili P_1 in P_2 ne dodata povezave, ki bi bila sestavljena iz dveh vozlišč, ki pripadata grafu G'. Če bi graf G, ki ga dobimo iz grafa G' s pravilom P_1 ali s pravilom P_2, vseboval nek cikel, potem bi moral ta cikel vsebovati kakšno vozlišče, ki ga ni v G', saj bi v nasprotnem ta cikel imeli že v G', kar je v nasprotju z indukcijsko predpostavko. Nova vozlišča ne morejo tvoriti cikla, saj le eno izmed njih tvori skupno povezavo z vozliščem iz G', vozlišča iz cikla pa morajo biti različna. Zato tudi graf G ne vsebuje cikla in lastnost Q_2 velja za vse predstavnike iz $\mathcal{G}_n(\mathcal{B},\mathcal{P})$.

*Baza je za lastnost Q_3 izpolnjena sama po sebi, saj graf iz baze K_1 ne vsebuje okroglega vozlišča. Predpostavimo lahko, da je $G' \in \mathcal{G}_n(\mathcal{B},\mathcal{P})$ in da ima vsako okroglo vozlišče iz G' natanko enega kvadratnega soseda. Pravilo P_1 ohranja lastnost Q_3, saj ima novo okroglo vozlišče x natanko enega kvadratnega soseda y in novo okroglo vozlišče u ima natanko enega kvadratnega soseda v. Podobno lastnost Q_3 ohranja tudi pravilo P_2, saj ima edino novo okroglo vozlišče u natanko enega kvadratnega soseda v. Torej imajo elementi iz $\mathcal{G}_n(\mathcal{B},\mathcal{P})$ tudi lastnost Q_3. (Množici kvadratnih vozlišč rečemo da je **dominantna** množica zaradi lastnosti Q_3, saj ima vsako vozlišče, ki ni kvadratno, vsaj enega kvadratnega soseda.)*

*Tudi za lastnost Q_4 je baza očitno izpolnjena, saj bazni element K_1 ne vsebuje dveh kvadratnih vozlišč. Naj bo $G' \in \mathcal{G}_n(\mathcal{B},\mathcal{P})$ in zanj velja indukcijska predpostavka, da sta med poljubnima kvadratnima vozliščema vsaj dve okrogli vozlišči. Pravilo P_1 ohranja lastnost Q_4, saj sta med novim kvadratnim vozliščem v in vsakim kvadratnim vozliščem v G' vsaj dve okrogli vozlišči, ki sta v tem primeru x in u. Prav tako ohranja lastnost Q_4 tudi pravilo P_2, saj sta med novim kvadratnim vozliščem v in vsakim kvadratnim vozliščem v G' vsaj dve okrogli vozlišči, ki sta ponovno x in u. Tako je tudi lastnost Q_4 resnična za vse grafe iz induktivnega razreda $\mathcal{G}_n(\mathcal{B},\mathcal{P})$. (Rečemo, da množica kvadratnih vozlišč, ki ima lastnost Q_4, tvori **pakiranje** grafa G. Ker je množica kvadratnih vozlišč hkrati dominantna in tudi tvori pakiranje, nam graf G tudi **učinkovito dominira**.)*

Oglejmo si še drug razred elementov, ki so definirani s pomočjo kake lastnosti. **Konceptualen razred** je množica, ki vsebuje vse elemente, ki imajo neko lastnost Q.

Zgled 2.10 *Primeri konceptualnih razredov so*

$$\begin{aligned} K_1 &= \{x^\ell w y^{k+2\ell} : k,\ell \in \mathbb{N}_0\},\\ K_2 &= \{(x,y) \in \mathbb{R}^2 : y = x^2 - 3x + 2\},\\ K_3 &= \{x \in \mathbb{R} : \sin x < \cos x\},\\ K_4 &= \{(4k-\ell, 3\ell - 2k) : k,\ell \in \mathbb{N}\}. \end{aligned}$$

Konceptualen razred je **odločljiv**, če je enak kakšnemu induktivnemu razredu. Sicer konceptualen razred **ni odločljiv**. V zgornjem zgledu sta K_1 in K_4 odločljiva konceptualna razreda, kar bomo videli kasneje, medtem ko K_2 in K_3 nista odločljiva.

Pogosto želimo induktivni razred opisati s konceptualnim ali obratno. Prednost konceptualnega razreda je pogosto v preverjanju, ali nek element pripada razredu ali ne. Pri induktivnem razredu moramo za odgovor na to vprašanje zgraditi konstrukcijsko zaporedje, medtem ko pri konceptualnem razredu preverimo, ali element ustreza pogoju. Tako lahko včasih pogoj zlahka preverimo, konstrukcijsko zaporedje pa je težko izgradljivo. Lahko je tudi drugače in pogoja iz konceptualnega razreda ne moremo preveriti hitro. Ne glede na vse, želimo odgovoriti na naslednje vprašanje.

Ali je induktivni razred $\mathcal{I}_n(\mathcal{B},\mathcal{P})$ enak konceptualnemu razredu K? (3)

Če je odgovor na vprašanje (3) negativen, ga ni težko obrazložiti. Ker sta oba razreda, tako induktivni kot konceptualni, pravzaprav množici, sta dve množici različni, če obstaja element, ki ga najdemo v eni, medtem ko ga ni v drugi množici. Torej moramo za negativni odgovor na (3) poiskati element, ki je v K, vendar ga ne moremo skonstruirati v $\mathcal{I}_n(\mathcal{B},\mathcal{P})$ ali skonstruiramo element v $\mathcal{I}_n(\mathcal{B},\mathcal{P})$, ki ne ustreza pogoju za K.

Pozabavajmo se še z možnostjo pozitivnega odgovora na vprašanje (3). V tem primeru je potrebno pokazati obe inkluziji $\mathcal{I}_n(\mathcal{B},\mathcal{P}) \subseteq K$ in $K \subseteq \mathcal{I}_n(\mathcal{B},\mathcal{P})$. Prvo inkluzijo $\mathcal{I}_n(\mathcal{B},\mathcal{P}) \subseteq K$ pokažemo z induktivno posplošitvijo tako, da najprej pokažemo, da imajo vsi elementi iz baze lastnost Q, ki je značilna za konceptualni razred K, nato pokažemo še, da vsa pravila iz $\mathcal{P}$ ohranjajo lastnost Q. Za dokaz inkluzije $K \subseteq \mathcal{I}_n(\mathcal{B},\mathcal{P})$ moramo za splošen element (ali splošne elemente) iz K zgraditi konstrukcijsko zaporedje v induktivnem razredu $\mathcal{I}_n(\mathcal{B},\mathcal{P})$.

Zgled 2.11 *Pokažimo, da je konceptualni razred $K_1 = \{x^\ell w y^{k+2\ell} : k,\ell \in \mathbb{N}_0\}$ iz zgledov 2.7 in 2.10 enak induktivnemu razredu $\mathcal{I}_n(\mathcal{B},\mathcal{P})$ iz zgleda 2.7. V zgledu 2.7 smo že pokazali, da lahko vsak element iz K_1 zgradimo iz baznega elementa $w \in \mathcal{B}$. Torej velja $K_1 \subseteq \mathcal{I}_n(\mathcal{B},\mathcal{P})$. Pokažimo še obratno inkluzijo $\mathcal{I}_n(\mathcal{B},\mathcal{P}) \subseteq K_1$ z induktivno posplošitvijo. Bazni element lahko zapišemo kot $w = x^0 w y^0$, ki se nahaja v K_1, s čimer je baza izpolnjena. Izberimo sedaj poljuben element $x^\ell w y^{k+2\ell}, k,\ell \in \mathbb{N}_0$, iz K_1 in pokažimo, da pravili P_1 in P_2 ohranjata lastnost vsebovanosti v K_1. Tako imamo*

$$x^\ell w y^{k+2\ell} \xrightarrow{P_1} x^\ell w y^{(k+1)+2\ell} \text{ in } x^\ell w y^{k+2\ell} \xrightarrow{P_2} x^{\ell+1} w y^{k+2\ell+2} = x^{\ell+1} w y^{k+2(\ell+1)}.$$

Seveda sta $\ell+1, k+1 \in \mathbb{N}_0$, saj sta $k,\ell \in \mathbb{N}_0$. Torej sta tudi $x^\ell w y^{k+1+2\ell}$ in $x^{\ell+1} w y^{k+2(\ell+1)}$ elementa iz K_1 in obe pravili ohranjata lastnost biti iz K_1. Tako velja tudi obratna inkluzija $\mathcal{I}_n(\mathcal{B},\mathcal{P}) \subseteq K_1$, s čimer smo dobili enakost med induktivnim razredom $\mathcal{I}_n(\mathcal{B},\mathcal{P})$ in konceptualnim razredom K_1.

Zgled 2.12 *Induktivni razred $\mathcal{G}_n(\mathcal{B},\mathcal{P})$ iz zgleda 2.8 je enak konceptualnemu razredu K, ki vsebuje vse grafe, ki izpolnjujejo lastnosti Q_1, Q_2, Q_3 in Q_4 iz zgleda 2.9. V zgledu 2.9 smo z induktivno posplošitvijo že pokazali, da imajo vsi elementi induktivnega razreda $\mathcal{G}_n(\mathcal{B},\mathcal{P})$ lastnosti Q_1, Q_2, Q_3 in Q_4, kar pomeni, da je $\mathcal{G}_n(\mathcal{B},\mathcal{P}) \subseteq K$. Dokaz obratne inkluzije $K \subseteq \mathcal{G}_n(\mathcal{B},\mathcal{P})$ presega nivo tega dela in ga tukaj opuščamo. Omenimo le, da konstrukcijsko zaporedje zgradimo s pomočjo popolne indukcije, tako da odrežemo ustrezen del grafa z lastnostmi Q_1, Q_2, Q_3 in Q_4, nato pa pokažemo, da lahko manjkajoči del v nekaj korakih zgradimo nazaj do G s pravili iz $\mathcal{P}$. V primerih, ko to ni mogoče, pa poiščemo protislovje, s katero izmed lastnosti Q_1, Q_2, Q_3 in Q_4.*

Kot že omenjeno, lahko pogosto algoritme predstavimo z induktivnimi razredi. Ker obstaja več algoritmov za nek problem, lahko imamo več induktivnih razredov, ki opisujejo algoritme za enak problem. Seveda nas zanima, ali so enaki, saj smo potem lahko prepričani v pravilnost algoritmov. Tako se zastavlja naslednje vprašanje.

$$\text{Ali sta induktivna razreda } \mathcal{I}_n(\mathcal{B},\mathcal{P}) \text{ in } \mathcal{I}'_n(\mathcal{B}',\mathcal{P}') \text{ enaka?} \tag{4}$$

Ponovno lahko njuno različnost pokažemo tako, da najdemo element, ki je v enem in ga hkrati ni v drugem indukcijskem razredu. Pri preverjanju njune enakosti imamo na razpolago dve orodji. Prva možnost je, da poiščemo konceptualen razred K, za katerega velja $\mathcal{I}_n(\mathcal{B},\mathcal{P}) = K = \mathcal{I}'_n(\mathcal{B}',\mathcal{P}')$. Seveda oba enačaja pokažemo kot opisano po vprašanju (3). Druga možnost predstavlja direktni pristop, kjer ponovno pokažemo obe inkluziji $\mathcal{I}_n(\mathcal{B},\mathcal{P}) \subseteq \mathcal{I}'_n(\mathcal{B}',\mathcal{P}')$ in $\mathcal{I}'_n(\mathcal{B}',\mathcal{P}') \subseteq \mathcal{I}_n(\mathcal{B},\mathcal{P})$ s pomočjo induktivne posplošitve.

Zgled 2.13 *Induktivni razred $\mathcal{C}_n(\mathcal{B},\mathcal{P})$ je podmnožica $\mathbb{Z}\times\mathbb{Z}$ in je definiran z bazo $\mathcal{B}$ in pravili $P_1, P_2 \in \mathcal{P}$ na naslednji način:*

$$\begin{aligned} \mathcal{B} &: (0,0) \in \mathcal{C}_n, \\ P_1 &: (i,j) \in \mathcal{C}_n \Rightarrow (i+3, j-2) \in \mathcal{C}_n, \\ P_2 &: (i,j) \in \mathcal{C}_n \Rightarrow (i-2, j+3) \in \mathcal{C}_n. \end{aligned}$$

Pokažimo, da je $(n,n) \in \mathcal{C}_n$ za vsak $n \in \mathbb{N}$ in poiščimo konceptualen razred K, ki je enak $\mathcal{C}_n(\mathcal{B},\mathcal{P})$. Če večkrat zapored uporabimo pravilo P_1, oziroma pravilo P_2, recimo k-krat P_1, oziroma ℓ-krat P_2, dobimo

$$(0,0) \xrightarrow{k\times P_1} (3k,-2k) \in \mathcal{C}_n \text{ oziroma } (0,0) \xrightarrow{\ell\times P_2} (-2\ell,3\ell) \in \mathcal{C}_n.$$

Tako po k-kratni uporabi P_1 in ℓ-kratni uporabi P_2 (ne nujno v tem vrstnem redu) dobimo $(3k-2\ell, 3\ell-2k) \in \mathcal{C}_n$. Če je $k = n = \ell$, potem vidimo, da je $(n,n) \in \mathcal{C}_n$. Po drugi strani nimamo druge možnosti, kot da nekajkrat (recimo k-krat, $k \in \mathbb{N}_0$) uporabimo pravilo P_1 in nekajkrat (recimo ℓ-krat, $\ell \in \mathbb{N}_0$) pravilo P_2 (ne nujno v tem vrstnem redu) na baznem elementu $(0,0)$. Tako lahko upamo, da je

$$K = \{(3k-2\ell, 3\ell-2k) : k, \ell \in \mathbb{N}_0\}$$

iskani konceptualni razred. Ker smo za elemente iz K že zgradili konstrukcijska zaporedja, je $K \subseteq \mathcal{C}_n(\mathcal{B},\mathcal{P})$. Z induktivno posplošitvijo pokažimo še obratno inkluzijo $\mathcal{C}_n(\mathcal{B},\mathcal{P}) \subseteq K$. Za $k = \ell = 0$ bazni element $(0,0)$ pripada K in baza je izpolnjena. Naj bosta $k,\ell \in \mathbb{N}_0$ in s tem $(3k-2\ell, 3\ell-2k) \in K$. Potem je

$$P_1((3k-2\ell,3\ell-2k)) = (3k-2\ell+3, 3\ell-2k-2) = (3(k+1)-2\ell, 3\ell-2(k+1))$$
$$P_2((3k-2\ell,3\ell-2k)) = (3k-2\ell-2, 3\ell-2k+3) = (3k-2(\ell+1), 3(\ell+1)-2k).$$

Ker sta tudi $k+1$ in $\ell+1$ iz množice $\mathbb{N}_0$, sta tudi elementa $P_1((3k-2\ell,3\ell-2k))$ in $P_2((3k-2\ell,3\ell-2k))$ iz K. To pomeni, da pravili P_1 in P_2 ohranjata pripadnost h K in velja $\mathcal{C}_n(\mathcal{B},\mathcal{P}) \subseteq K$. Obe inkluziji nam porajata željeno enakost.

Zgled 2.14 *Induktivni razred $\mathcal{C}'_n(\mathcal{B}',\mathcal{P})$ je podmnožica $\mathbb{Z}\times\mathbb{Z}$ in je definiran z bazo $\mathcal{B}'$ in pravili $P_1, P_2 \in \mathcal{P}$ na naslednji način:*

$$\begin{aligned} \mathcal{B}' &: (3,-2) \in \mathcal{C}_n, \\ P_1 &: (i,j) \in \mathcal{C}_n \Rightarrow (i+3, j-2) \in \mathcal{C}_n, \\ P_2 &: (i,j) \in \mathcal{C}_n \Rightarrow (i-2, j+3) \in \mathcal{C}_n. \end{aligned}$$

Seveda lahko opazimo, da se induktivni razred $\mathcal{C}'_n(\mathcal{B}',\mathcal{P})$ razlikuje od induktivnega razreda $\mathcal{C}_n(\mathcal{B},\mathcal{P})$ iz zgleda 2.13 le v bazi. Zanima nas, ali sta dejansko enaka. Zadoščalo bi pokazati, da je tudi $\mathcal{C}'_n(\mathcal{B}',\mathcal{P})$ enak konceptualnemu razredu K iz zgleda 2.13, kar lahko vsak bralec poskusi sam. Tukaj poskusimo direktno z dokazom obeh inkluzij $\mathcal{C}'_n(\mathcal{B}',\mathcal{P}) \subseteq \mathcal{C}_n(\mathcal{B},\mathcal{P})$ in $\mathcal{C}_n(\mathcal{B},\mathcal{P}) \subseteq \mathcal{C}'_n(\mathcal{B}',\mathcal{P})$. Pravzaprav moramo pokazati le, da s pravili iz $\mathcal{P}$ lahko iz baznega elementa baze $\mathcal{B}$ dobimo bazni element baze $\mathcal{B}'$ in obratno, saj sta pravili enaki v obeh induktivnih razredih. Zlahka vidimo, da je $P_1((0,0)) = (3,-2)$, kar poraja inkluzijo $\mathcal{C}'_n(\mathcal{B}',\mathcal{P}) \subseteq \mathcal{C}_n(\mathcal{B},\mathcal{P})$. Pri obratni inkluziji se zaplete, saj sprva ni videti, da lahko iz baznega elementa $\mathcal{B}'$ pridemo do baznega elementa $(0,0) \in \mathcal{B}$. Pokažimo, da to dejansko ne gre. Kot v zgledu 2.13 lahko z nekajkratno (recimo $k \in \mathbb{N}_0$-kratno) uporabo pravila P_1 in nekajkratno (recimo $\ell \in \mathbb{N}_0$-kratno) uporabo pravila P_2 iz baznega elementa $(3,-2)$ dobimo

$$(3,-2) \xrightarrow{k\times P_1} (3k+3, -2k-2) \xrightarrow{\ell\times P_2} (3k+3-2\ell, 3\ell-2k-2) \in \mathcal{C}'_n.$$

Če želimo, da je $(3k+3-2\ell, 3\ell-2k-2) = (0,0)$, potem imamo $3k+3-2\ell = 0$ in $3\ell-2k-2 = 0$. Rešitev tega sistema je $k=-1$ in $\ell = 0$, kar je nemogoče, saj je $k \in \mathbb{N}_0$. Tako baznega elementa $(0,0) \in \mathcal{B}$ ne moremo izraziti v induktivnem razredu $\mathcal{C}'_n(\mathcal{B}',\mathcal{P})$ in induktivna razreda $\mathcal{C}'_n(\mathcal{B}',\mathcal{P})$ in $\mathcal{C}_n(\mathcal{B},\mathcal{P})$ nista enaka.

2.3 DEDUKTIVNE TEORIJE

Teorija $\mathcal{T}$ je sestavljena iz razreda **izjav** E in razreda **izrekov** I in pišemo $\mathcal{T} = (E, \mathcal{I})$. Izjave nam povedo območje govora, izreki pa povedo, katere izmed izjav iz E imajo poseben status. Tako velja $\mathcal{I} \subseteq E$, kjer izjave E tvorijo odločljiv konceptualni razred. Teorija je **deduktivna**, če je razred izrekov induktivni razred, to je $\mathcal{I} = \mathcal{C}_n(\mathcal{A}, \mathcal{P})$, kjer elementom baze $\mathcal{A}$ rečemo **aksiomi**. V deduktivnih teorijah vse izreke izpeljemo iz aksiomov, zato imajo le-ti posebno vlogo. Zato morajo biti aksiomi po eni strani dovolj preprosti, da jim lahko zaupamo, po drugi strani pa jih mora biti dovolj, da dobimo dovolj bogato teorijo.

Zgled 2.15 *Spomnimo se Dedekindovega*[5] *aksioma, ki je osnoven aksiom realnih števil. Pravi, da ima vsaka neprazna navzgor omejena množica realnih števil natančno zgornjo mejo med realnimi števili.*

Aksiomi so **odvisni**, če lahko enega (ali več) izmed njih izrazimo s preostalimi aksiomi. Odvisnim aksiomom se poskušamo izogniti, saj to pomeni le, da lahko aksiom, ki ga lahko izrazimo s preostalimi, izbrišemo izmed aksiomov in teorija ostane enaka, saj ta aksiom lahko izrazimo iz preostalih in je med izreki. Če aksiomi niso odvisni, so **neodvisni**, kar pomeni, da nobenega izmed aksiomov ne moremo izpeljati iz preostalih aksiomov. V teorijah težimo k neodvisnim množicam aksiomov.

Zgled 2.16 *Spomnimo se Peanovih aksiomov, ki nam opišejo naravna števila in pokažimo, da so neodvisni. Aksioma P_1 ne moremo izpustiti, saj potem tudi prazna množica $\emptyset$ kot tudi recimo množica $\mathbb{N} - \{1\}$ izpolnjujeta vse preostale Peanove aksiome, a vemo, da niso naravna števila. Če opustimo aksiom P_2, potem množica $\{1\}$ izpolnjuje preostale štiri aksiome, kar ponovno ni v redu. Vsaka končna množica $[n]$ izpolnjuje aksiome P_1, P_2, P_4 in P_5, če le definiramo, da je naslednik od n kar n sam (preostali nasledniki so definirani kot običajno). Torej je tudi aksiom P_3 neodvisen od preostalih. Tudi za dokaz neodvisnosti aksioma P_4 lahko uporabimo množico $[n]$, le da je tokrat 1 naslednik od n. Brez aksioma P_5 nam preostali aksiomi $P_1 - P_4$ zagotovijo vsa naravna števila, vendar lahko tudi kaj dodamo. Recimo množica $\left\{\frac{1}{2}\right\} \cup \mathbb{N}$ zadošča aksiomom $P_1 - P_4$, če le definiramo, da je naslednik od $\frac{1}{2}$ kar $\frac{1}{2}$. (Seveda lahko $\frac{1}{2}$ nadomestimo s katerimkoli številom, ki ni naravno.) Tako je aksiom P_5 potreben, da ne dobimo preveč in je prav tako neodvisen od preostalih.*

Zgled 2.17 *Omenimo še, da se več kot 2000 let ni vedelo, ali je aksiom o ne sekanju vzporednih premic iz Evklidske geometrije neodvisen od preostalih. Z opustitvijo tega aksioma se dobi nova teorija, ki se imenuje projektivna geometrija,*[6] *za katero velja, da se tudi vzporedni premici sekata (v točki neskončno). To je pravzaprav geometrija, po kateri deluje naš vid, saj s prostim očesom vidimo, da se dovolj dolgi vzporedni liniji v daljavi sečeta (recimo ravni železniški tiri).*

5 Julius Wilhelm Richard Dedekind (1831-1916) je bil nemški matematik, ki se je med drugim ukvarjal s teorijo kolobarjev in definicijo realnih števil, kamor sodi tudi tale aksiom.

6 Za začetnika projektivne geometrije veljata nemški astronom in matematik Johannes Kepler (1571–1630) in francoski matematik Girard Desargues (1591–1661).

Zgled 2.18 *Simetrična verzija Dedekindovega aksioma pravi, da ima vsaka neprazna navzdol omejena množica realnih števil natančno spodnjo mejo med realnimi števili. Vendar to ni aksiom, saj to trditev zlahka izpeljemo iz Dedekindovega aksioma. Samo izpeljavo tukaj opuščamo, saj ne sodi na področje diskretne matematike.*

Teorija $\mathcal{T} = (E, \mathcal{I})$, ki vsebuje izjavni račun, je **protislovna**, če obstaja taka izjava $e \in E$, da sta oba e in $\neg e$ izreka. V nasprotnem primeru, torej, če je za vsako izjavo $e \in E$ največ ena izmed e in $\neg e$ izrek, rečemo, da je teorija **neprotislovna**. Protislovne teorije so dolgočasne, kot je razvidno iz naslednje trditve.

Trditev 2.2 *Če je teorija $\mathcal{T} = (E, \mathcal{I})$, opremljena z izjavnim računom, protislovna, potem je $E = \mathcal{I}$.*

Dokaz. Naj bo teorija $\mathcal{T} = (E, \mathcal{I})$ protislovna in naj bo $e \in E$ taka izjava, da sta oba e in $\neg e$ izreka. Na e in $\neg e$ uporabimo združitev (imamo izjavni račun) in dobimo, da je izrek tudi laž $e \wedge \neg e \sim 0$. Če pa je laž izrek, potem je izrek vsaka izjava $a \in E$, saj lahko uporabimo pridružitev in je $0 \vee a \sim a$ izrek. ∎

Ali lahko o protislovnosti govorimo tudi v teorijah brez izjavnega računa? V takem primeru potrebujemo preslikavo $f : E \to E$. Teorija $\mathcal{T} = (E, \mathcal{I})$ je **protislovna glede na preslikavo** f, če obstaja izjava $e \in E$, da sta oba e in $f(e)$ izreka. Obratno, če je za vsako izjavo $e \in E$ največ ena izmed izjav e in $f(e)$ izrek, potem je teorija $\mathcal{T} = (E, \mathcal{I})$ **neprotislovna glede na** f. Teorija $\mathcal{T} = (E, \mathcal{I})$ je **absolutno neprotislovna**, če je $E \neq \mathcal{I}$. Seveda se absolutna neprotislovnost ujema z neprotislovnostjo v primeru teorij opremljenih z izjavnim računom.

Zadnja lastnost teorij, ki jo omenjamo tukaj, je polnost. Teorija $\mathcal{T} = (E, \mathcal{I})$, opremljena z izjavnim računom, je **polna**, če je za vsako izjavo $e \in E$ natanko ena izmed izjav e in $\neg e$ izrek. Dovolj bogate teorije običajno niso polne.

Zgled 2.19 *Oglejmo si naslednje izjave in skušajmo pojasniti kaj je narobe z njimi.*

- *Brivec iz vasi brije vse v vasi, ki se ne brijejo sami.*
- *Krečan je izrekel: "Vsak Krečan vedno laže."*
- *Stavek, ki ga ravnokar izrekam, je laž.*

Težava prve povedi je sam brivec, saj nastopa v dveh vlogah: kot brivec in kot samostojni brivec. Če se brije sam, ga on, brivec, ne brije. Če se ne brije sam, pa ga brije brivec, torej on sam. Ker je v drugi povedi trditev izjavil Krečan, naj bi po trditvi iz te povedi, lagal tudi s to trditvijo samo. To pomeni, da je trditev iz povedi lažna in nekateri Krečni ne lažejo vedno. Tretjo poved, oziroma njen ekvivalent, bomo pravzaprav bolj natančno analizirali v nadaljevanju.

Paradoks lažnivca je resnična izjava e, pri kateri niti e niti $\neg e$ nista izreka. Pokažimo, da lahko z izjavnim računom izrazimo paradoks lažnivca. Oglejmo si naslednjo izjavo.

Izjava e govori sama o sebi: "Izjava e ni izrek." (5)

Privzamemo lahko, da je teorija neprotislovna, kar pomeni, da

lažne izjave niso izreki. (6)

Pokažimo najprej s protislovjem, da je izjava e resnična. Če e ni resnična, potem je izrek po (5). Ker e ni resnična, po (6) ni izrek. Torej e je izrek in ni izrek hkrati, kar je protislovje.

Pokažimo še, da oba e in $\neg e$ nista izreka. Ker je e resnična, e ni izrek po (5). Podobno, ker je e resnična, $\neg e$ ni resnična in ni izrek po (6). Torej obstajajo izjave, ki so resnične, a tako izjava kot njena negacija nista izreka. Omenimo še znamenit izrek Gödla[7] iz leta 1931, ki ga navajamo brez dokaza, saj le-ta bistveno presega nivo tega dela.

Izrek 2.3 *Paradoks lažnivca je izrazljiv v rekurzivni aritmetiki (to je vsak aksiomatski sistem, ki poraja tudi naravna števila, recimo Peanovi aksiomi).*

Kadar teorija ni opremljena z izjavnim računom, si lahko ponovno pomagamo s preslikavami. Teorija je **polna glede na preslikavo** $f : E \to E$, če je za vsako izjavo $e \in E$ natanko ena izmed izjav e in $f(e)$ izrek.

Teorija $\mathcal{T} = (E, \mathcal{I})$ je **absolutno polna**, če je $E \neq \mathcal{I}$ in za vsako izjavo $e \in E$, ki ni izrek, velja, da je induktivni razred, ki ga porodijo izreki $\mathcal{I}$ skupaj z izjavo e, enak vsem izjavam E. Ponovno se absolutna polnost ujema s polnostjo v primeru teorij opremljenih z izjavnim računom. Če je namreč teorija polna in opremljena z izjavnim računom, potem $e \in E$ in $e \notin \mathcal{I}$ pomeni, da je $\neg e$ izrek. Sedaj nadaljujemo, kot v dokazu trditve 2.2 in dobimo, da je induktivni razred porojen iz $\mathcal{I} \cup \{e\}$ enak vsem izjavam E.

Zgled 2.20 *Nad abecedo $\Sigma = \{a, b\}$ je definirana množica izjav z $E = \{a^n b a^m : n, m \in \mathbb{N}\}$. Izreki deduktivne teorije $\mathcal{T} = (E, \mathcal{I})$ predstavljajo induktivni razred $\mathcal{I} = \mathcal{C}_n(\mathcal{A}, \mathcal{P})$, kjer sta v $\mathcal{A}$ dva aksioma $A_1 : aba \in \mathcal{I}$ in $A_2 : a^3ba \in \mathcal{I}$. Nove elemente v $\mathcal{I}$ tvorimo iz aksiomov s pomočjo treh pravil iz $\mathcal{P}$ in sicer*

$$\begin{aligned} P_1 &: xby \in \mathcal{I} \Rightarrow ybx \in \mathcal{I}, \\ P_2 &: xby \in \mathcal{I} \Rightarrow xabya \in \mathcal{I}, \\ P_3 &: xby, ybz \in \mathcal{I} \Rightarrow xbz \in \mathcal{I}. \end{aligned}$$

Pokažimo najprej, da je A_1 odvisen od A_2, da lahko torej A_1 zgradimo iz A_2 s pravili iz $\mathcal{P}$. Na a^3ba najprej uporabimo pravilo P_1 in dobimo $aba^3 \in \mathcal{I}$. Sedaj imamo $aba^3, a^3ba \in \mathcal{I}$

7 Kurt Friedrich Gödel (1906-1978) je bil avstrijski matematik, ki se je ukvarjal z logiko in teorijami.

in po uporabi P_3 dobimo $aba \in I$. Tako smo zgradili konstrukcijsko zaporedje za aba iz a^3ba, kar pomeni, da je A_1 odvisen od A_2.

Pokažimo, da je razred izrekov $\mathcal{I}$ enak konceptualnemu razredu $\mathcal{K} = \{a^nba^m : n + m = 2k, n, m, k \in \mathbb{N}\}$. Za dokaz inkluzije $\mathcal{I} \subseteq \mathcal{K}$ uporabimo induktivno posplošitev. Za bazo zadostuje, da je $A_2 \in \mathcal{K}$, saj je A_1 odvisen od A_2. Seveda je $3 + 1 = 4 = 2 \cdot 2$ za a^3ba in je $A_2 \in \mathcal{K}$. Predpostavimo sedaj, da sta $a^nba^m, a^mba^r \in \mathcal{K}$, torej velja $n + m = 2k$ in $m + r = 2\ell$. Velja $P_1(a^nba^m) = a^mba^n$, $P_2(a^nba^m) = a^{m+1}ba^{n+1}$ in $P_3(a^nba^m, a^mba^r) = a^nba^r$. Seveda je $m + n = 2k$ in $n + 1 + m + 1 = 2k + 2 = 2(k + 1)$ in sta zato tudi $P_1(a^nba^m)$ in $P_2(a^nba^m)$ iz $\mathcal{K}$. Velja tudi $n + r = 2k + 2\ell - 2m = 2(k + \ell - m)$, kjer je $k + \ell - m \in \mathbb{N}$, kar pomeni tudi $P_3(a^nba^m, a^mba^r) \in \mathcal{K}$. Torej vsa tri pravila ohranjajo lastnost biti element $\mathcal{K}$ in inkluzija $\mathcal{I} \subseteq \mathcal{K}$ velja.

Za obratno inkluzijo $\mathcal{K} \subseteq \mathcal{I}$ moramo za splošen element a^nba^m iz $\mathcal{K}$, kjer je $n + m = 2k$ in $m, n, k \in \mathbb{N}$, zgraditi konstrukcijsko zaporedje iz A_2 s pravili iz $\mathcal{P}$. Pokažimo najprej s pomočjo matematične indukcije, da je $a^{2s-1}ba \in \mathcal{I}$ za vsak $s \in \mathbb{N}$. Za $s = 1$ smo že videli, da lahko element aba zgradimo iz A_3, s čimer je baza izpolnjena. Naj bo sedaj trditev resnična za $s \in \mathbb{N}$, kar pomeni, da lahko $a^{2s-1}ba$ zgradimo iz A_2 s pravili $\mathcal{P}$. Na $a^{2s-1}ba$ dvakrat uporabimo pravilo P_2 in dobimo $a^{2s+1}ba^3 \in \mathcal{I}$. Sedaj izvedemo pravilo P_3 na besedah $a^{2s+1}ba^3$ in a^3ba ter dobimo $a^{2s+1}ba = a^{2(s+1)-1}ba \in \mathcal{I}$, s čimer je indukcija zaključena.

Do sedaj smo pokazali, da je $a^{2s-1}ba \in \mathcal{I}$ za vsak $s \in \mathbb{N}$. Zlahka vidimo, da velja tudi $aba^{2s-1} \in \mathcal{I}$, za vsak $s \in \mathbb{N}$, saj je $P_1(a^{2s-1}ba) = aba^{2s-1}$. Pred nadaljevanjem dodajmo še tole, da je $m + n = 2k$ le v primeru, ko sta ali oba m in n liha ali oba m in n soda. Če sta oba m in n liha, potem sta $a^nba, aba^m \in \mathcal{I}$ kot smo že videli. Velja tudi $P_3(a^nba, aba^m) = a^nba^m \in \mathcal{I}$. Naj bosta m in n še sodi števili. Tedaj sta $m - 1$ in $n - 1$ lihi števili in potemtakem $a^{n-1}ba, aba^{m-1} \in \mathcal{I}$. Na teh dveh izrekih uporabimo pravilo P_2 in dobimo $P_2(a^{n-1}ba) = a^nba^2 \in \mathcal{I}$ in $P_2(aba^{m-1}) = a^2ba^m \in \mathcal{I}$. Sedaj s pravilom P_3 dobimo $P_3(a^nba^2, a^2ba^m) = a^nba^m \in \mathcal{I}$. Torej smo našli konstruksijsko zaporedje za a^nba^m v vseh primerih, ko je $n + m$ sodo število in velja $\mathcal{K} \subseteq \mathcal{I}$ in s tem tudi enakost med $\mathcal{I}$ in $\mathcal{K}$.

S predpisom $f(e) = ea$ je definirana preslikava $f : E \to E$. Tako velja $f(a^nba^m) = a^nba^{m+1}$ za poljubno izjavo $a^nba^m \in E$. Če je $n + m$ sodo število, potem je $n + m + 1$ liho in če je $n + m$ liho, potem je $n + m + 1$ sodo. S pomočjo enakosti med $\mathcal{I}$ in $\mathcal{K}$ zlahka opazimo, da, če je $e \in \mathcal{I}$, potem $f(e) \notin \mathcal{I}$ in obratno, če $e \notin \mathcal{I}$, potem je $f(e) \in \mathcal{I}$. Povedano drugače, za vsako izjavo e je natanko ena izmed izjav e in $f(e)$ izrek. Torej je teorija $\mathcal{T} = (E, \mathcal{I})$ polna glede na f. Ker je polna glede na f, se seveda ne zgodi, da sta oba e in $f(e)$ izreka in je zato tudi neprotislovna glede na f. Slednje zagotavlja tudi neenakost $E \neq \mathcal{I}$, s čimer je $\mathcal{T} = (E, \mathcal{I})$ absolutno neprotislovna.

2.4 NEKATERE (NE)REŠENE NALOGE

Vaja 2.1 *Naslednje trditve dokažite z matematično indukcijo*

(A) $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$ *za vsak* $n \in \mathbb{N}$;

(B) $(13^{2n} + 6)$ *je deljivo s* 7 *za vsak* $n \in \mathbb{N}$;

(C) $(4^n + 15n - 1)$ *je deljivo z* 9 *za vsak* $n \in \mathbb{N}$;

(D) $n! \geq 2^n$ *za vsako naravno število* $n \geq 2$;

(E) $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} \geq \sqrt{n}$ *za vsak* $n \in \mathbb{N}$.

Rešitev. *Vse trditve so resnične. Natančneje si oglejmo* (a), (c) *in* (e). *Pri* (a) *naj bo* $L(n) = 1^3 + 2^3 + 3^3 + \cdots + n^3$ *in* $D(n) = \left(\frac{n(n+1)}{2}\right)^2$. *Za dokaz baze izračunamo* $L(1) = 1 = D(1)$. *V indukcijskem koraku imamo*

$$\begin{aligned} L(n+1) &= 1^3 + 2^3 + \cdots + n^3 + (n+1)^3 = L(n) + (n+1)^3 = \\ &= D(n) + (n+1)^3 = \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 = \\ &= (n+1)^2 \left(\frac{n^2}{4} + n + 1\right) = (n+1)^2 \frac{n^2 + 4n + 4}{4} = \\ &= (n+1)^2 \frac{(n+2)^2}{4} = D(n+1) \end{aligned}$$

in trditev (a) *je resnična.*

V (c) *želimo pokazati, da je* $4^n + 15n - 1 = 9k$ *za nek* $k \in \mathbb{Z}$ *za vsak* $n \in \mathbb{N}$. *Označimo* $A(n) = 4^n + 15n - 1$. *Baza pri* $n = 1$ *je izpolnjena, saj je* $A(1) = 4 + 15 - 1 = 18 = 2 \cdot 9$. *Pokažimo še induktivni korak za* $n + 1$, *ob resničnosti indukcijske predpostavke* $A(n) = 9k$. *Računajmo*

$$\begin{aligned} A(n+1) &= 4^{n+1} + 15(n+1) - 1 = 4 \cdot 4^n + 15n + 14 = \\ &= 4 \cdot 4^n + 4 \cdot 15n - 4 - 45n + 18 = \\ &= 4(4^n + 15n - 1) - 45n + 18 = 4 \cdot 9k - 9(5n - 2). \end{aligned}$$

Torej 9 *deli tudi* $A(n)$ *za vsako naravno število* n.

Za nalogo (e) *vpeljimo oznaki* $L(n) = \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}}$ *in* $D(n) = \sqrt{n}$. *Za* $n = 1$ *velja* $L(1) = \frac{1}{\sqrt{1}} = 1 \geq \sqrt{1} = D(1)$ *in baza je izpolnjena. Naj velja sedaj indukcijska predpostavka* $L(n) \geq D(n)$ *in računajmo za* $n + 1$

$$\begin{aligned} L(n+1) &= \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n+1}} = L(n) + \frac{1}{\sqrt{n+1}} \geq \\ &\geq D(n) + \frac{1}{\sqrt{n+1}} = \sqrt{n} + \frac{1}{\sqrt{n+1}}. \end{aligned}$$

Za dokončanje dokaza moramo pokazati še

$$\sqrt{n} + \frac{1}{\sqrt{n+1}} \geq D(n+1) = \sqrt{n+1}.$$

Če pomnožimo zadnji izraz z $\sqrt{n+1}$*, dobimo*

$$\sqrt{n}\sqrt{n+1} + 1 \geq n + 1,$$

oziroma $\sqrt{n^2+n} \geq n^2$*. Če tole še kvadriramo, potem dobimo* $n^2 + n \geq n$*, oziroma* $n \geq 0$*, kar je seveda res za vsa naravna števila. S tem je tudi dokončan dokaz za* (e)*.*

Vaja 2.2 *Izračunajte najprej induktivni korak za enakost* $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! = (n+1)!$ *za* $n \geq 2$ *in šele nato bazo za* $n = 1$*.*
Rešitev. *V indukcijskem koraku predpostavimo, da velja zgornja enakost. Označimo* $L(n) = 1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n!$ *ter* $D(n) = (n+1)!$ *in računajmo*

$$\begin{aligned} L(n+1) &= 1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! + (n+1)(n+1)! = \\ &= L(n) + (n+1)(n+1)! = D(n) + (n+1)(n+1)! = \\ &= (n+1)! + (n+1)(n+1)! = (n+2)(n+1)! = (n+2)! = D(n+2). \end{aligned}$$

Torej velja induktivni korak. A enačaj ne velja, saj nismo preverili baze za $n = 1$*, ki ne drži, saj je*

$$L(1) = 1 \neq 2 = D(1).$$

Tako smo v indukcijskem koraku narobe uporabili predpostavko $L(n) = D(n)$*, ki ni resnična.*

Vaja 2.3 *Pokažite, da število* 17 *deli vsa števila oblike* $8^n + 9^n$ *za vsa liha števila* n*.*
Rešitev. *Poljubno liho število* n *laho zapišemo kot* $n = 2k - 1$ *za nek* $k \in \mathbb{N}$*. Tako moramo pokazati, da* 17 *deli vsa števila oblike* $8^{2k-1} + 9^{2k-1}$ *za vsak* $k \in \mathbb{N}$*. Označimo* $F(k) = 8^{2k-1} + 9^{2k-1}$ *in pokažimo, da je* $F(k) = 17\ell$ *za nek* $\ell \in \mathbb{Z}$*. Za* $k = 1$ *imamo* $F(1) = 8 + 9 = 17 \cdot 1$*, s čimer je baza pokazana. Naj sedaj velja indukcijska predpostavka* $F(k) = 17\ell$ *in računajmo*

$$\begin{aligned} F(k+1) &= 8^{2(k+1)-1} + 9^{2(k+1)-1} = 8^{2k+1} + 9^{2k+1} = 64 \cdot 8^{2k-1} + 81 \cdot 9^{2k-1} = \\ &= (13 + 51) \cdot 8^{2k-1} + (13 + 68) \cdot 9^{2k-1} = \\ &= 13(8^{2k-1} + 9^{2k-1}) + 51 \cdot 8^{2k-1} + 68 \cdot 9^{2k-1} = \\ &= 13F(k) + 17(3 \cdot 8^{2k-1} + 4 \cdot 9^{2k-1}) = 13 \cdot 17\ell + 17m = 17n. \end{aligned}$$

Seveda je n *naravno število in indukcija je zaključena.*

Vaja 2.4 *Izjave teorije $\mathcal{T} = (\mathcal{E}, \mathcal{I})$ imajo obliko $a^n b^m a^p$ za $m, n, p \geq 0$. Razred izrekov $\mathcal{I}$ je določen z:*

$$\begin{aligned} A.&\quad \vdash b,\\ P1.&\quad Xb \vdash Xb^4,\\ P2.&\quad X \vdash a^3X,\\ P3.&\quad aXb \vdash X,\\ P4.&\quad X \vdash Xa. \end{aligned}$$

(A) *Podaj induktivno definicijo razreda izjav $\mathcal{E}$.*

(B) *Katere od izjav $a^2b^8a^2$, a^5b^3 in $a^{2020}b^2a^{2020}$ so izreki?*

(C) *Pokaži, da če je $a^m b^n a^p \in \mathcal{I}$, potem je $a^p b^n a^m \in \mathcal{I}$ natanko takrat, ko je $p \equiv m \pmod 3$.*

(D) *Ali je teorija $\mathcal{T}$ neprotislovna ali polna glede na $f : X \mapsto aX$?*

Rešitev. *Induktivna definicija razreda izjav je*

$$\begin{aligned} B.&\quad \vdash \lambda, b,\\ E1.&\quad Xb \vdash Xbb,\\ E2.&\quad X \vdash aX,\\ E3.&\quad X \vdash Xa. \end{aligned}$$

Izreka sta a^5b^3 (konstrukcijsko zaporedje je P_1, $2P_2$ in P_3) in $a^{2020}b^2a^{2020}$ (konstrukcijsko zaporedje je P_1, $674P_2$, $2P_3$ in $2020P_4$). Za dokaz trditve (c) je potrebno uvideti, da je $a^m b^n a^p \in \mathcal{I}$ natanko takrat, ko je $m \equiv n - 1 \pmod 3$. Teorija ni polna (a in $f(a)$ nista izreka) in je neprotislovna glede na f.

Vaja 2.5 *Induktivni razred C_n nad abecedo $\Sigma = \{a, b\}$ je definiran z*

$$\begin{aligned} B.&\quad \lambda \in C_n,\\ P_1.&\quad x \in C_n \Rightarrow a^3x \in C_n,\\ P_2.&\quad x \in C_n \Rightarrow xb^3 \in C_n,\\ P_3.&\quad axb \in C_n \Rightarrow x \in C_n. \end{aligned}$$

(A) *Ali so nizi a^4b^7, $a^{2020}b$, b^{2020} iz razreda C_n?*

(B) *Pokaži: če je $a^n b^m \in C_n$, je tudi $a^m b^n \in C_n$.*

Rešitev. *Pomagamo si lahko s konceptualnim razredom*

$$K = \{a^k b^\ell : k \equiv \ell \pmod 3\},$$

ki je enak podanemu induktivnemu razredu. Pokažite to enakost! Sedaj ni težko videti, da sta a^4b^7, $a^{2020}b \in C_n$ in $b^{2020} \notin C_n$. Točka (b) sedaj sledi iz simetričnosti kongruence, glej (ii) trditve 6.18.

Vaja 2.6 *Naj bo K konceptualen razred nad abecedo $\Sigma = \{a, b, c\}$, v katerem nastopa c natanko* 2020*-krat. Poišči induktivni razred C_n, ki je enak K in to tudi dokaži.*
Rešitev. *Induktivni razred je*

$$\begin{aligned} B.&\quad c^{2020} \in C_n,\\ P_1.&\quad xy \in C_n \Rightarrow xay \in C_n,\\ P_2.&\quad xy \in C_n \Rightarrow xby \in C_n, \end{aligned}$$

kjer je potrebno omeniti, da sta x ali y v pravilih P_1 in P_2 lahko tudi prazni besedi. Seveda v bazi c nastopa 2020*-krat. To lastnost ohranjata tudi obe pravili in tako je $C_n \subseteq K$. Konstrukcijsko zaporedje poljubnega elementa iz K zgradimo tako, da začnemo na levi in vedno, ko naletimo na skupek a-jev ali b-jev, recimo a^k, oziroma b^ℓ, uporabimo k-krat obrat pravila P_1, oziroma ℓ-krat obrat pravila P_2. Tako se na levi strani znebimo a-jev in b-jev. S tem postopkom se pomikamo proti desni in povsod se znebimo a-jev in b-jev. Na koncu nam ostane* 2020 *c-jev, kar je bazni element.*

Vaja 2.7 *Induktivni razred C_n je podan z bazo in pravili:*

$$\begin{aligned} B.&\quad aba \in C_n,\\ P_1.&\quad xby \in C_n \Rightarrow xabya \in C_n,\\ P_2.&\quad xby \in C_n \Rightarrow xbya \in C_n,\\ P_3.&\quad xby, ybz \in C_n \Rightarrow xbz \in C_n,\\ P_4.&\quad xaabyaa \in C_n \Rightarrow xabya \in C_n,\\ P_5.&\quad xby, ybx \in C_n \Rightarrow xcy \in C_n. \end{aligned}$$

(A) *Katere izmed besed a^2ba^4, a^3ba^2, aca in a^2ca^3 so iz C_n?*

(B) *Pokaži, da je pravilo P_3 izpeljano iz ostalih pravil.*

Rešitev. *Najlaže je pokazati, da je induktivni razred C_n enak konceptualnemu razredu*

$$K = \{a^k ba^{k+\ell}, a^k ca^k : k, \ell \in \mathbb{N}_0\}.$$

Pokažite to enakost! Sedaj vidimo, da sta a^2ba^4 in aca iz C_n, a^3ba^2 in a^2ca^3 pa ne. Prav tako vidimo, da lahko vse elemente iz K izpeljemo brez pravila P_3, ki je zato nepotrebno in ga lahko izpeljemo iz preostalih. Ali velja enak razmislek tudi za pravilo P_4?

Vaja 2.8 *Nad abecedo $\Sigma = \{a, b, c\}$ sestavi induktivno definicijo za naslednji razred izjav: vsi nizi vsebujejo* 2020 *a-jev in če niz vsebuje n c-jev, vsebuje $2n$ b-jev.*
Rešitev. *Induktivna definicija je sledeča*

$$\begin{aligned} B.&\quad a^{2020} \in C_n,\\ P_1.&\quad xyz \in C_n \Rightarrow xcyb^2z \in C_n,\\ P_2.&\quad xyz \in C_n \Rightarrow xb^2ycz \in C_n,\\ P_3.&\quad xyzw \in C_n \Rightarrow xbyczbw \in C_n. \end{aligned}$$

Spet so besede x, y, z in w lahko prazne. Razmisliti je še potrebno, da sta konceptualni in induktivni razred res enaka.

3

KOMBINATORIKA OZIROMA PREŠTEVANJE

Kombinatorika je pravzaprav drugačno ime za štetje ali preštevanje. Seveda je smiselno takoj podvomiti v smiselnost učenja štetja na univerzitetnem nivoju, ko pa so števila in štetje z nami že od zgodnjih let našega življenja. Tako obstaja veliko raziskav, ki govorijo o tem, da je otrokom v vrtcu in prvih letih osnovne šole matematika precej bližja kot recimo pisana beseda. Zakaj bi potemtakem znova začeli preštevati?

Odgovor je zelo preprost in kot pogosto v tem poglavju ga bomo ponazorili s primerom. Seveda je že vsak štel do sto, čeprav se marsikdo tega sploh ne spomni. Zelo malo ljudi pa si vzame čas in šteje do tisoč. Vendar je tisoč zelo malo število, sploh v današnjem svetu digitalnih sistemov. Tako bi ob hipotetični predpostavki, da preštejemo eno število na sekundo (kar je nemogoče za velika števila), do miljona prešteli v približno enajstih dnevih in pol. Seveda brez spanja in počitka ter vseh ostalih za življenje potrebnih reči.

Zgornji razmislek nas hitro pripelje do ugotovitve, da je zelo smiselno razviti metode in tehnike štetja, ki nas privedejo do velikih števil na relativno eleganten in enostaven način. To je možno za skupine objektov, ki imajo kakšno skupno lastnost. Nekatere izmed teh lastnosti si bomo ogledali v tem poglavju.

Dogovorimo se še za oznako. S simbolom # bomo označevali število, ki ga bomo tedaj iskali.

Dodatno literaturo v slovenščini iz tega področja je moč najti v [10] in [11]. V angleškem jeziku je na voljo precej več primerne literature, tukaj omenimo le [1, 6]. Marsikaj je najti tudi na spletu in pogosto je že Wikipedia (angleška) dober začetni vir informacij. Standardna zbirka nalog za to poglavje je [9]. Veliko izpitnih nalog iz tega poglavja je najti v [12, 13].

3.1 ENOSTAVNA ŠTETJA

V tem razdelku si bomo pogledali dve enostavni pravili štetja: pravilo seštevanja in pravilo množenja. Kot že omenjeno, si bomo pomagali vsebino najprej podkrepiti s primerom.

V neki osnovni šoli imajo tri prve razrede. V 1a hodi 22 učencev, 1b obiskuje 21 učencev in v 1c greje šolske klopi 19 učencev. Zlahka odgovorimo na vprašanje, koliko prvošolcev je na tej šoli v aktualnem šolskem letu. Seveda je odgovor 62, kjer smo rezultat dobili s seštevanjem števila učencev po razredih. Malce težje postane, če želimo model, ki smo ga uporabili, predstaviti z matematičnimi pojmi.

Na učence, ki obiskujejo 1x razred, $x \in \{a, b, c\}$, lahko pogledamo kot na elemente množice X, $X \in \{A, B, C\}$. Ob tem števila 22, 21 in 19 predstavljajo število elementov v množici A, B oziroma C. Spomnimo se, da število elementov množice X poimenujemo moč množice X, kar označimo z $|X|$. Tako imamo v našem primeru $|A| = 22$, $|B| = 21$ in $|C| = 19$. Ker nas zanima število vseh prvošolcev, nas v matematičnem smislu zanima moč unije $|A \cup B \cup C|$. Do rezultata, ki je vsota, je sedaj le še en korak. Moči posameznih množic lahko seštejemo, ker vsak prvošolec hodi v natanko en razred. Povedano z množicami, poljubni dve množici sta disjunktni (to je, da imata prazen presek). Tako imamo

$$|A \cup B \cup C| = |A| + |B| + |C| = 22 + 21 + 19 = 62.$$

Ta razmislek je univerzalen in ga lahko uporabimo na poljubnem številu množic, če so le paroma disjunktne. Tako smo dokazali naslednji rezultat.

Izrek 3.1 (Pravilo seštevanja) *Če so $A_1, A_2, \ldots, A_k$ paroma disjunktne množice, potem velja*

$$|A_1 \cup A_2 \cup \cdots \cup A_k| = |A_1| + |A_2| + \cdots + |A_k|.$$

Kako določiti število elementov unije množic v primeru, ko preseki niso paroma disjunktni, si bomo ogledali kasneje v razdelku o vključitvah in izključitvah.

Za boljše razumevanje pravila množenja si oglejmo primer restavracije s hitro prehrano, v kateri je možno dobiti glavno jed (GJ), prilogo (PR) in pijačo (PI). Med glavnimi jedmi so na razpolago hamburger (H), kebab (K) in hotdog (D), med prilogami sta na razpolago solata (S) in ocvrt krompirček (O), odžejamo pa se lahko s pivom (P), cockto (C), radensko (R) ali vodo (V). Zanima nas, koliko različnih naročil je možnih, če izberemo eno glavno jed, eno prilogo in eno pijačo. Na tem majhnem primeru se lahko preštevanja lotimo tudi direktno. Tako zlahka vidimo, da lahko k vsaki glavni jedi dodamo dve prilogi, kar je skupaj šest različnih možnosti

$$(H, O), (H, S), (K, O), (K, S), (D, O), (D, S).$$

K vsaki izmed omenjenih možnosti sedaj dodamo še eno izmed štirih pijač in dobimo

$$\begin{aligned}
&(H,O,P),(H,O,C),(H,O,R),(H,O,V),\\
&(H,S,P),(H,S,C),(H,S,R),(H,S,V),\\
&(K,O,P),(K,O,C),(K,O,R),(K,O,V),\\
&(K,S,P),(K,S,C),(K,S,R),(K,S,V),\\
&(D,O,P),(D,O,C),(D,O,R),(D,O,V),\\
&(D,S,P),(D,S,C),(D,S,R),(D,S,V).
\end{aligned}$$

Zlahka preštejemo, da je skupaj 24 različnih možnosti. Ob tem lahko uvidimo, da se da uporabiti tudi množenje in velja $\# = 3 \cdot 2 \cdot 4 = 24$. Tudi tukaj uporabimo moč posameznih množic $GJ = \{H, K, D\}$, $PR = \{O, S\}$ in $PI = \{P, C, R, V\}$, ki so $|GJ| = 3$, $|PR| = 2$ in $|PI| = 4$. Ni pa tako očitno, kaj predstavlja število 24. Povedano drugače: moč katere množice je 24? Namig za to je podan že v zapisu vseh možnosti, kjer smo vsako možnost zapisali kot urejeno trojico. Urejene trojice pa predstavljajo elemente kartezičnega produkta treh množic. Tako imamo

$$|GJ \times PR \times PI| = |GR| \cdot |PR| \cdot |PI| = 3 \cdot 2 \cdot 4 = 24.$$

Ponovno velja zgornji razmislek za poljubno število množic, če so le neprazne, s čimer je dokazan naslednji izrek.

Izrek 3.2 (Pravilo množenja) *Če so $A_1, A_2, \ldots, A_k$ neprazne množice, potem velja*

$$|A_1 \times A_2 \times \cdots \times A_k| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_k|.$$

V pravilu množenja nastopa operacija množenja in pogosto se zgodi, da velja $|A_i| = k - i + 1$ za vsak $i \in [k]$. V tem primeru dobimo rezultat

$$|A_1 \times A_2 \times \cdots \times A_k| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_k| = k \cdot (k-1) \cdot \ldots \cdot 2 \cdot 1.$$

Tako je smiselno vpeljati novo oznako za ta produkt in pišemo

$$k! = k \cdot (k-1) \cdot \ldots \cdot 1.$$

Številu $k!$ rečemo k **fakulteta** ali k **faktoriela** in je definirano za vsa naravna števila. V računalništvu je morda bolj primerna rekurzivna[8] definicija za $k!$, ki je naslednja:

(A) za $k = 1$ velja $k! = 1$ (začetni pogoj);

(B) za $k > 1$ velja $k! = k \cdot (k-1)!$ (rekurzija).

8 Bolj podrobno bomo o rekurzivnih relacijah govorili v naslednjem poglavju.

To definicijo lahko uporabimo tudi za opis induktivnega razreda, kjer je točka (a) baza, točka (b) pa je edino pravilo. Tak induktivni razred je enak konceptualnemu razredu $K = \{k! : k \in \mathbb{N}\}$.

Kasneje bomo opazili, da je smiselno vpeljati tudi 0 fakulteta. Tukaj 0! ni v skladu z zgornjo definicijo in se dogovorimo, da velja

$$0! = 1.$$

Ta oznaka bo precej poenostavila nekatere zapise in nam olajšala delo.

Omenimo še, da se obe pravili pogosto kombinirata in nastopata skupaj, kot bo razvidno (tudi) iz naslednjih primerov.

Zgled 3.1 *Kako se spremeni rezultat, če v zgornjem primeru o restavraciji s hitro hrano dovolimo, da naročnik ne rabi naročiti pijače? Še vedno ostane šest različnih možnosti glede hrane. Kar se tiče napitkov, imamo sedaj na razpolago enake pijače kot prej in še dodatno možnost, da pijače ne naročimo. Tako je rezultat*

$$\# = 3 \cdot 2 \cdot 5 = 30.$$

Zgled 3.2 *Ana, Boris, Cveto, Črt, Darja in Erika se potegujejo za mesta predsednika, tajnika in blagajnika novo ustanovljene slovenske stranke. Na koliko različnih načinov lahko zasedejo ta mesta, če funkcije niso združljive in velja naslednji pogoj.*

(A) *Ni omejitev.*

(B) *Predsednik mora postati Ana ali Boris.*

(C) *Erika mora dobiti eno funkcijo.*

(D) *Črt in Cveto morata dobiti funkcijo.*

Če označimo vsakega kandidata z začetno črko njegovega imena, lahko postavimo $P = \{A, B, C, \check{C}, D, E\}$ *in iz te množice izberemo predsednika* pr*. Sedaj naj bo* $T = P - \{pr\}$ *in iz te množice izbiramo tajnika* taj*. Ko je le ta izbran, nam preostane množica* $BL = P - \{pr, taj\}$*, iz katere izbiramo blagajnika. Po pravilu množenja imamo*

$$\#_a = |P| \cdot |T| \cdot |BL| = 6 \cdot 5 \cdot 4 = 120.$$

Omenimo, da običajno pravila množenja ne uporabljamo tako strogo, da bi si zapisovali in natančno definirali vse množice. To bomo tudi upoštevali v vseh preostalih primerih. Tako sta v drugem primeru le dva kandidata za predsednika, preostali množici pa imata enako moč, saj lahko neizvoljen predsedniški kandidat zasede kakšno od preostalih funkcij. Tako je

$$\#_b = 2 \cdot 5 \cdot 4 = 40.$$

Ko mora Erika dobiti eno funkcijo, lahko opazimo, da je izračun simetričen ne glede na to, katero funkcijo zasede. Tako lahko te tri primere opazujemo ločeno in uporabimo pravilo seštevanja. Za preostali funkciji tako kandidira enkrat pet in drugič štirje kandidati. Tako imamo

$$\#_c = 1 \cdot 5 \cdot 4 + 5 \cdot 1 \cdot 4 + 5 \cdot 4 \cdot 1 = 60.$$

V zadnjem primeru obrnemo gledišče in določimo, na koliko načinov lahko priredimo funkcijo Cvetu in Črtu. Prvi ima na razpolago tri, medtem ko za drugega preostaneta še dve. Za zadnjo funkcijo so nato seveda še štirje preostali kandidati in velja

$$\#_d = 3 \cdot 2 \cdot 4 = 24.$$

Zgled 3.3 *Poiščimo število urejenih trojic X_1, X_2 in X_3, da velja $X_1 \cup X_2 \cup X_3 = \{1,2,3,4,5,6,7,8,9\}$ in $X_1 \cap X_2 \cap X_3 = \emptyset$. Iz danih pogojev lahko razberemo, da mora biti vsako število iz unije vsebovano v vsaj eni izmed množic X_1, X_2 in X_3, vendar ne v vseh treh hkrati, zaradi drugega pogoja. Če označimo z A^C komplement množice A, je lahko vsako število iz unije v eni izmed naslednjih množic:*

$$X_1 \cap X_2 \cap X_3^C, X_1 \cap X_2^C \cap X_3, X_1^C \cap X_2 \cap X_3,$$
$$X_1 \cap X_2^C \cap X_3^C, X_1^C \cap X_2 \cap X_3^C, X_1^C \cap X_2^C \cap X_3.$$

Tako imamo za vsako izmed devetih števil šest različnih možnosti, kje se lahko nahaja in velja

$$\# = 6 \cdot 6 \cdot 6 \cdot 6 \cdot 6 \cdot 6 \cdot 6 \cdot 6 \cdot 6 = 6^9 = 10\,077\,696.$$

3.2 UREJENE IZBIRE

Na razpolago imamo $n \in \mathbb{N}$ različnih elementov. Izmed njih izberemo k elementov, kjer je seveda $k \in [n]_0$. Na koncu izbranim k elementom določimo vrstni red: prvi element, drugi element in tako naprej vse do k-tega elementa. Tej konstrukciji rečemo **urejena** (n,k)**-izbira**. Običajno obstaja veliko različnih urejenih (n,k)-izbir in naša naloga je, da preštejemo vse različne urejene (n,k)-izbire. Tako bomo s $P(n,k)$ označili število vseh različnih urejenih (n,k)-izbir. Ker je začetnih n elementov različnih, je jasno, da bo to število vedno enako, ne glede na tip začetnih elementov. S tem je mišljeno, da je $P(n,k)$ enak, če urejeno izbiramo k elementov iz množice z n različnimi krompirji, kot tudi, če urejeno izbiramo k elementov iz množice z n različnimi knjigami. Poudarimo še, da je $P(n,k)$ število in da je ena urejena (n,k)-izbira zaporedje k različnih elementov. Seveda ju tako ne moremo primerjati ali celo enačiti.

Izrek 3.3 (Urejene izbire) *Za števili $n \in \mathbb{N}$ in $k \in [n]_0$ velja*

$$P(n,k) = \frac{n!}{(n-k)!}.$$

Dokaz. Naj množica A_1 vsebuje n različnih elementov. Induktivno bomo definirali množice A_i, $2 \leq i \leq k$, kjer A_i dobimo iz A_{i-1} tako, da iz A_{i-1} odvzamemo en element x_{i-1}, $2 \leq i \leq k$. Tako je $A_i = A_{i-1} - \{x_{i-1}\}$. Opazimo lahko, da je $|A_1| = n$, $|A_2| = n-1$, $|A_3| = n-2$ vse do $|A_k| = n-k+1$. Po pravilu množenja imamo

$$\begin{aligned} P(n,k) &= |A_1 \times A_2 \times \cdots \times A_k| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_k| = \\ &= n(n-1)(n-2)\ldots(n-k+1) = \\ &= n(n-1)(n-2)\ldots(n-k+1)\frac{(n-k)!}{(n-k)!} = \\ &= \frac{n!}{(n-k)!}, \end{aligned}$$

s čimer je dokaz končan. ∎

Opazimo lahko, da za $n = 0$ v izreku dobimo $P(0,0) = \frac{0!}{0!} = 1$. Tudi to bomo v nadaljevanju upoštevali kot dogovor.

Omenimo, da se v srednji šoli namesto urejenih izbir pogosto uporabljata dva termina in sicer **variacije**, ko je $k < n$, in **permutacije**, ko je $k = n$. V skladu z dogovorom o oznaki $0! = 1$ vidimo, da je govora pravzaprav o isti stvari in da je smiselno oboje združiti. Še bolj je to razvidno iz samega dokaza zgornjega izreka, kjer je zadnji oklepaj v drugi vrstici izračuna enak $(n-k+1) = 1$ v primeru, ko je $k = n$. Tako velja naslednja posledica.

Posledica 3.4 *Za naravno število n velja $P(n,n) = n!$.*

Zgled 3.4 *Tipičen primer urejenih izbir je zgled 3.2 (a) izbiranja predsednika, tajnika in blagajnika, kjer imamo*

$$\# = 6 \cdot 5 \cdot 4 = \frac{6!}{3!} = P(6,3).$$

Zgled 3.5 *Sestavljamo besede iz vseh črk množice $\{A, B, C, D, E, F, G\}$. (Beseda tukaj pomeni nize črk, ki ne potrebujejo nujno kakšnega smisla v slovenskem jeziku.) Koliko je različnih besed, če*

(A) *ni omejitev?*

(B) *zahtevamo podniz DEF?*

(C) *zahtevamo, da so črke D, E in F postavljene skupaj, vendar ne nujno v tem vrstnem redu?*

Če ni nobenih omejitev, je s podobnim razmislekom kot dokazu izreka 3.3 rezultat

$$\#_a = P(7,7) = 7! = 5040.$$

Ko je zahtevan podniz DEF, lahko nanj pogledamo kot na eno samo črko sestavljeno iz treh in nato sestavljamo besede iz petih črk A, B, C, DEF in G. Tako imamo

$$\#_b = P(5,5) = 5! = 120.$$

Če zahtevamo, da so črke D, E in F skupaj, vendar ne nujno v tem vrstnem redu, nanje še vedno gledamo kot na eno črko in dobimo $P(5,5)$ možnosti. Ob tem upoštevamo, da jih lahko medsebojno premešamo na $P(3,3)$ različnih načinov. Oboje seveda združimo s pravilom množenja in imamo

$$\#_c = P(5,5)P(3,3) = 5!3! = 720.$$

Zgled 3.6 *Na koliko različnih načinov lahko posedemo šest ljudi za okroglo mizo? Najprej moramo ugotoviti, kaj pomeni fraza 'različni način' pri okrogli mizi. Označimo šest oseb z $A, B, C, Č, D$ in E ter jih v tem vrstnem redu posadimo za mizo v smeri urinega kazalca. Ali je ta postavitev enaka kot, če se vsak premakne za eno mesto v levo? Če izločimo zunanje vplive, kot so recimo bližina okna ali vrat glede na določen sedež, v matematiki opisanih dveh postavitev ne ločimo, saj ima vsak ista soseda na enakih straneh. Tako je rezultat, ki ga iščemo, različen od $P(6,6)$, kot bi morebiti kdo pomislil. Da se dokopljemo do željenega števila, najprej izberemo eno osebo, nato pa sedeže drugih vrednotimo glede na izbrano osebo. Ker je ostalo še pet prostih stolov, urejenih glede na izbrano osebo, in pet oseb, je iskan rezultat*

$$\# = P(5,5) = 5! = 120.$$

Zgled 3.7 *Sedem študentov in pet dijakov piše test IQ za dolgo ravno mizo. Na koliko načinov jih lahko posedemo v ravni vrsti, če dijaki ne smejo sedeti skupaj? Najprej poskrbimo za študente, ki jih lahko uredimo na $P(7,7)$ načinov. Med poljubna študenta kot tudi na začetek ali konec lahko vrinemo točno enega dijaka. Tako imamo za pet dijakov osem možnih pozicij. Ko prvemu dijaku dodelimo fiksno pozicijo, jih ostane še sedem za štiri dijake. Če s tem nadaljujemo, opazimo, da dobimo $P(8,5)$ različnih možnosti. Oboje seveda združimo po pravilu množenja in imamo*

$$\# = P(7,7)P(8,5) = 7!\frac{8!}{3!} = 33\ 868\ 800.$$

3.3 NEUREJENE IZBIRE

Kot že ime pove, bomo tudi v tem razdelku izbirali, vendar bo tokrat izbiranje neurejeno. Tudi tukaj so lahko osnovni parametri enaki: na razpolago imamo $n \in \mathbb{N}$ različnih elementov izmed katerih jih izberemo $k \in [n]_0$. Za razliko od urejenih izbir, tokrat izbranim k elementom ne določamo vrstnega reda. Tako je **neurejena** (n,k)**-izbira** poljubna izbira $k \in [n]_0$ elementov izmed $n \in \mathbb{N}$ različnih elementov.

Neurejeno (n,k)-izbiro zlahka predstavimo v jeziku množic. Če je X množica moči $n \in \mathbb{N}$, potem je neurejena (n,k)-izbira poljubna podmnožica moči $k \in [n]_0$ množice X. (Omenimo, da so vsi elementi v množici vedno tudi različni. Če pa se elementi ponavljajo, potem govorimo o multi-množici.)

Kot pri urejenih izbirah, nas zanima število vseh različnih neurejenih (n,k)-izbir, ki ga označimo s

$$C(n,k).$$

Z drugimi besedami, število $C(n,k)$ prestavlja, koliko je različnih podmnožic moči k množice X z močjo n. Seveda je ponovno potrebno ločiti med $C(n,k)$, ki je število, in med eno neurejeno (n,k)-izbiro, ki je (pod)množica.

Ni težko opaziti, da lahko iz ene neurejene (n,k)-izbire dobimo urejeno (n,k)-izbiro tako, da izbranih k elementov naknadno še uredimo. Kadar urejamo k elemetov izmed izbranih k elementov, lahko to storimo, po posledici 3.4, na $P(k,k) = k!$ različnih načinov. Ker je vseh neurejenih izbir $C(n,k)$, lahko po pravilu množenja dobimo število vseh urejenih (n,k)-izbir, kjer vsako neurejeno izbiro še uredimo na $P(k,k)$ različnih načinov:

$$P(n,k) = C(n,k)P(k,k).$$

Ker obe vrednosti $P(n,k)$ in $P(k,k)$ že poznamo, lahko iz zgornje enakosti izrazimo $C(n,k)$:

$$C(n,k) = \frac{P(n,k)}{P(k,k)} = \frac{n!}{(n-k)!k!}.$$

S tem smo dokazali naslednji izrek.

Izrek 3.5 (Neurejene izbire) *Za števili $n \in \mathbb{N}$ in $k \in [n]_0$, velja*

$$C(n,k) = \frac{n!}{(n-k)!k!}.$$

Kot pri urejenih izbirah, se lahko tudi tukaj vprašamo, kako je v primeru, ko je $n = 0$. Tukaj je pričakovan odgovor 1, saj lahko prazno množico ($k = 0$) izberemo na en način iz prazne množice ($n = 0$). Zaradi dogovora $0! = 1$ to dobimo tudi v zgornjem izreku in imamo

$$C(0,0) = \frac{0!}{0!0!} = 1.$$

Za neurejene izbire se v srednji šoli običajno uporablja ime **kombinacije**. Tokrat pa ima posebno ime kot tudi oznako število $C(n,k)$. Pogosto mu rečemo **binomski simbol** in uporabljamo oznako

$$\binom{n}{k} = C(n,k) = \frac{n!}{(n-k)!k!}.$$

Razlog za to je v povezavi teh števil s potenco binoma, o čemer bo govora v izreku 3.9.

Zgled 3.8 *Na koliko različnih načinov lahko izberemo tričlansko delovno predsedstvo občnega zbora Prostovoljnega gasilskega društva izmed desetih kandidatov? Ker zadolžitve predsedstva med seboj niso ločene, iščemo število različnih podmnožic moči tri množice z desetimi elementi. To je po izreku 3.5*

$$\# = C(10,3) = \frac{10!}{7!3!} = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2 \cdot 1} = 120.$$

Zgled 3.9 *Karte za poker sestavljajo štiri barve (srce, kara, pik in križ) in vsaka barva ima 13 različnih likov (števila od ena do deset, kjer številu ena rečemo tudi as, ter fanta, damo in kralja). Vsak igralec dobi v roko pet kart.*

(A) *Koliko je različnih možnosti, ki jih lahko dobi nek igralec?*

(B) *Koliko je različnih možnosti, da je vseh pet kart enake barve (flush)?*

(C) *Koliko je možnosti, da dobi 'full house' (to so tri karte enakega lika in še preostali dve enakega, recimo tri petke in dva fanta)?*

Točka (a) je neposredna uporaba izreka 3.5 in velja

$$\#_a = C(52,5) = \frac{52!}{47!5!} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 2\,598\,960.$$

Za enako barvo imamo na razpolago štiri barve in med njimi lahko določimo eno na $C(4,1) = 4$ različne načine. Ko je barva fiksirana, lahko izbiramo pet kart izmed trinajstih, kar lahko opravimo na $C(13,5)$ različnih načinov. Po pravilu množenja imamo

$$\#_b = C(4,1)C(13,5) = 5148.$$

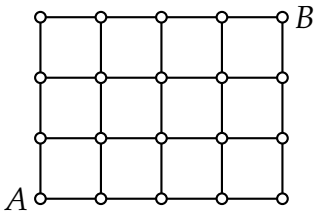
Za 'full house' najprej določimo na koliko načinov lahko imamo tri predstavnike istega lika. Izmed 13. likov izberemo enega in to storimo na $C(13,1) = 13$ različnih načinov. Ko je ta lik določen, izmed štirih kart z istim likom izberemo tri in to lahko storimo na $C(4,3)$ načine. Sedaj ponovimo razmisek še za par, ki ga lahko izbiramo izmed 12 preostalih likov, torej na $C(12,1) = 12$ načinov. Na razpolago so spet štiri karte, izmed katerih izbiramo dve: $C(4,2)$. Ponovno vse združimo s pravilom množenja in imamo

$$\#_c = C(13,1)C(4,3)C(12,1)C(4,2) = 3744.$$

Zgled 3.10 *Na koliko različnih načinov se lahko sprehodimo po najkrajši poti od točke A do točke B na zemljevidu na sliki 3? Ker želimo med A in B po najkrajši poti, lahko v vsaki točki, ki predstavlja križišče, zavijemo le navzgor ali desno. Še več, glede na zemljevid, se natanko trikrat odpravimo navzgor, v vseh preostalih možnostih moramo izbrati desno. Ker je križišč, v katerih potrebujemo odločitev, na najkrajši poti med A in B sedem, izbiramo tri križišča, v katerih gremo navzgor. To lahko storimo na*

$$\# = C(7,3) = \frac{7!}{4!3!} = 35.$$

Opazimo lahko, da nam enak razmislek, le da izbiramo tista križišča, v katerih gremo na desno, da enak rezultat $\# = C(7,4) = 35$.



Slika 3: Zemljevid poti za zgled 3.10.

3.4 IZBIRE S PONAVLJANJEM

Do sedaj smo si ogledali, kako preštevati objekte z določenimi lastnostmi, ki so povezani z množico n različnih elementov. Kako se zadeve spremenijo, če opustimo zahtevo o različnosti elementov? V tem primeru govorimo o **multimnožicah**. Za njih je značilno, da se lahko elementi, med katerimi ne ločimo, oziroma so enaki, pojavijo večkrat. Pri tem ločimo dva principa.

Lahko imamo na razpolago n elementov, kjer se nekateri lahko ponovijo, ali pa imamo na razpolago n različnih elementov, kjer se vsi lahko ponovijo poljubno mnogokrat. Prvo možnost lahko ponazorimo z vrečko bonbonov, v kateri je pet različnih tipov bonbonov (z okusom jagode, karamele, limone, jabolka in breskve). Seveda je teh bonbonov končno mnogo. Drug primer najlažje ilustriramo s črkami, iz katerih tvorimo besede. Seveda lahko poljubno črko uporabimo poljubno mnogokrat in nismo omejeni s številom uporabe kakšne črke, pač pa z dolžino besede, torej mest, ki jih izbiramo. Posamezen princip bomo razložili s pomočjo primerov.

Opica je dobila v roke listke s črkami besede KROKODIL. Vprašajmo se, na koliko različnih načinov jih lahko sestavi v besedo? V tem primeru uporabimo vse elemente, ki so na razpolago, vendar se dva med njimi, K in O, ponovita dvakrat. Tako lahko recimo oba O-ja v vsaki postavitvi zamenjamo med sabo in dobimo enako besedo. Skratka, pričakujemo lahko, da je možnosti manj kot vseh urejenih izbir $P(8,8)$. Na razpolago imamo 8 različnih pozicij za črke in vprašamo se lahko, na koliko različnih načinov lahko postavimo oba O-ja. Ker izbiramo dve mesti med osmimi, je odgovor seveda $C(8,2)$. S tem razmislekom nadaljujemo na šestih še prostih mestih in dobimo $C(6,2)$ različnih možnosti za pozicije K-ja. Ostala so še štiri mesta za črke R, D, I in L. Mesto za R lahko izberemo na $C(4,1)$ načinov, pozicijo za D na $C(3,1)$ načinov, za I ostane $C(2,1)$ možnosti in na koncu imamo za L le $C(1,1) = 1$ možnost. Vse omenjene delne rezultate seveda združimo po pravilu množenja in imamo

$$\begin{aligned} \# &= C(8,2)C(6,2)C(4,1)C(3,1)C(2,1)C(1,1) \\ &= \frac{8!}{2!6!}\frac{6!}{2!4!}\frac{4!}{1!3!}\frac{3!}{1!2!}\frac{2!}{1!1!}\frac{1!}{1!0!} \\ &= \frac{8!}{2!2!1!1!1!1!} = 10\,080. \end{aligned}$$

Tukaj je potrebno opozoriti na vzorec krajšanja v drugi vrstici izračuna, kjer se druga fakulteta v imenovalcu ulomka vedno pokrajša s fakulteto v števcu naslednjega ulomka (z izjemo zadnjega ulomka, kjer je $0! = 1$). Prav tako ni potrebno pisati vseh $1!$ v zadnji vrstici, a so ostala, da se lažje prepozna vzorec.

Izrek 3.6 *Naj bodo $n, n_1, n_2, \ldots, n_k \in \mathbb{N}$, da velja $n = n_1 + n_2 + \cdots + n_k$. Če multimnožica vsebuje n_i elementov tipa i, za vsak $i \in [k]$, potem lahko vse elemente uredimo na*

$$\# = \frac{n!}{n_1! n_2! \cdots n_k!}$$

različnih načinov.

Dokaz. Razmislek je podoben razmisleku v primeru pred izrekom. Na razpolago imamo n mest in elementom posameznega tipa prirejamo prosta mesta, ob tem pa preštevamo vse možne načine. Tako za elemente tipa 1 izberemo n_1 mest izmed n mest, ki so na razpolago. To je $C(n, n_1)$ različnih možnosti. Za elemnte tipa 2 izberemo n_2 mest izmed preostalih $n - n_1$ mest, kar znese $C(n - n_1, n_2)$ različnih možnosti. Elemente tipa 3 razporedimo na n_3 mest izmed preostalih $n - n_1 - n_2$ mest. To je $C(n - n_1 - n_2, n_3)$ različnih možnosti. S tem nadaljujemo do zadnjega, k-tega tipa, kjer izbiramo n_k mest izmed preostalih $n_k = n - n_1 - n_2 - \cdots - n_{k-1}$ mest, kar storimo na $C(n - n_1 - n_2 - \cdots - n_{k-1}, n_k)$ načinov. S pravilom množenja imamo

$$\begin{aligned}
\# &= C(n, n_1) C(n - n_1, n_2) C(n - n_1 - n_2, n_3) \cdots C(n - n_1 - n_2 - \cdots - n_{k-1}, n_k) \\
&= \frac{n!}{n_1!(n - n_1)!} \frac{(n - n_1)!}{n_2!(n - n_1 - n_2)!} \cdots \frac{(n - n_1 - n_2 - \cdots - n_{k-1})!}{n_k! 0!} \\
&= \frac{n!}{n_1! n_2! n_3! \cdots n_k!},
\end{aligned}$$

kar je iskan rezultat. ∎

Zgled 3.11 *Na koliko različnih načinov lahko razdelimo osem različnih knjig med tri študente, če Lojze dobi štiri knjige, Janko in Metka pa vsak po dve knjigi? Če si pripravimo štiri etikete s črko L in po dve s črkama J in M in knjigam dodeljujemo te etikete, potem lahko po izreku 3.6 to storimo na*

$$\# = \frac{8!}{4!2!2!} = \frac{8 \cdot 7 \cdot 6 \cdot 5}{2 \cdot 2} = 420$$

različnih načinov.

Preklopimo sedaj na primer, ko imamo na razpolago poljubno mnogo simbolov in jih izbiramo najprej na urejen način. Recimo, koliko besed dolžine šest lahko sestavimo s črkami slovenske abecede? Za vsako mesto imamo na razpolago 25 različnih črk in imamo po pravilu množenja

$$\# = 25 \cdot 25 \cdot 25 \cdot 25 \cdot 25 \cdot 25 = 25^6 = 244\,140\,625.$$

Kadar izmed multimnožice z n različnimi elementi–vsak element se ponovi vsaj k-krat–izbiramo k elementov in jim določimo vrstni red, rečemo temu **urejena** (n,k)**-izbira s ponavljanjem**. Število vseh urejenih (n,k)-izbir s ponavljanjem označimo s

$$P_p(n,k).$$

Ponovno opozorimo, da je $P_p(n,k)$ število, medtem ko je ena urejena (n,k)-izbira s ponavljanjem zaporedje simbolov dolžine k. Omenimo še, da pogoj $k \leq n$, ki je veljal pri izbirah brez ponavljanja, tukaj ne velja več, saj se lahko simboli poljubno (vsaj k-krat) ponovijo. Naslednji izrek je neposredna posledica pravila množenja in ga zato navajamo brez dokaza.

Izrek 3.7 (Urejene izbire s ponavljanjem) *Za števili $n,k \in \mathbb{N}$ velja*

$$P_p(n,k) = n^k.$$

Zgled 3.12 *Spomnimo se zgleda 3.3, kjer smo iskali različne trojice množic X_1, X_2 in X_3, da je veljalo $X_1 \cup X_2 \cup X_3 = \{1,2,3,4,5,6,7,8,9\}$ in $X_1 \cap X_2 \cap X_3 = \emptyset$, ki predstavlja tipično uporabo izreka 3.7, če si nalogo pravilno interpretiramo.*

Kadar izmed multi-množice z n različnimi elementi–vsak element se ponovi vsaj k-krat–izbiramo k elementov, rečemo temu **neurejena** (n,k)**-izbira s ponavljanjem**. Število vseh neurejenih (n,k)-izbir s ponavljanjem označimo s

$$C_p(n,k).$$

Podobno kot pri neurejenih izbirah brez ponavljanja, lahko tudi neurejeno (n,k)-izbiro s ponavljanjem predstavimo kot podstrukturo, tokrat kot podmultimnožico moči k. Seveda se vsaka neurejena (n,k)-izbira s ponavljanjem zato razlikuje od $C_p(n,k)$, ki je število. Tudi pogoj $k \leq n$, ki je veljal pri izbirah brez ponavljanja, ponovno ne velja več, saj se lahko simboli poljubno (vsaj k-krat) ponovijo. Preden si ogledamo splošen rezultat za $C_p(n,k)$, naredimo razmislek s sledečim primerom.

V knjižnici izbiramo šest knjig med knjigami za Diskretne strukture (DS), za Programiranje (P) in za Osnove elektrotehnike (OE). Na koliko različnih načinov jih lahko izberemo, če med knjigami za posamezni predmet ne ločimo in imamo na razpolago vsaj šest knjig za vsak predmet? Za vsako izbrano knjigo uporabimo simbol x, kar znese šest x-ov. Ker jih je potrebno še razlikovati glede na predmet, jih razvrstimo tako, da bodo na začetku knjige za DS, nato knjige za P in na koncu knjige za OE. Tako obstajata dve meji med knjigami različnih predmetov: ena med DS in P ter druga med P in OE. Označimo ti meji s simboloma y. Tako nam razporeditvi

$$xxyxxxyx \text{ in } xyxxxxxy$$

predstavljata dve možni izbiri. V prvi imamo dve knjigi za DS, tri za P in eno za OE, v dugi pa eno knjigo za DS, pet knjig za P in nobene za OE. Uvidimo lahko,

da vsaka taka razporeditev šestih simbolov x in dveh simbolov y pomeni eno našo iskano izbiro. Po izreku 3.6 lahko tole zapišemo kot

$$C_p(3,6) = \frac{8!}{6!2!} = C(8,2) = C(8,6),$$

saj smo razvrstili osem simbolov, kjer jih je šest enega tipa (x-si) in dva drugega tipa (y-a). Omenimo še, da velja $8 = 3+6-1$ in $2 = 3-1$, kar je pomembno zaradi posplošitve v naslednjem izreku.

Izrek 3.8 (Neurejene izbire s ponavljanjem) *Za števili $n, k \in \mathbb{N}$ velja*

$$C_p(n,k) = C(n+k-1, n-1) = C(n+k-1, k).$$

Dokaz. Izbiramo k elementov, kjer so nekateri lahko enaki, oziroma se ponavljajo. Označimo jih s simboli x in imamo k simbolov x. Ker imamo n različnih tipov elementov, z $n-1$ simboli y razmejimo elemente istega tipa, ko jih razvrstimo. Vsaka taka razvrstitev pomeni natanko eno našo neurejeno (n,k)-izbiro s ponavljanjem. Po izreku 3.6 velja

$$C_p(n,k) = \frac{(k+n-1)!}{k!(n-1)!} = C(n+k-1, n-1) = C(n+k-1, k)$$

in dokaz je končan. ∎

Zgled 3.13 *Na koliko različnih načinov lahko razdelimo* 12 *identičnih knjig med štiri študente?*

Če za vsakega študenta napišemo 12 *listkov z njihovimi imeni, ki nam tvorijo množico, potem so študentje tisti, ki se ponavljajo. Tako z neposredno uporabo izreka 3.8 dobimo*

$$C_p(4,12) = C(15,3) = \frac{15!}{3!12!} = 455.$$

Zgled 3.14 *Koliko rešitev ima enačba $x_1 + x_2 + x_3 = 26$, če velja*

(A) $x_1, x_2, x_3 \in \mathbb{N}$;

(B) $x_1 \geq 2$, $x_2 \geq 4$ *in* $x_3 \geq 5$ *za* $x_1, x_2, x_3 \in \mathbb{N}$.

Ker iščemo le rešitve v okviru naravnih števil, lahko število 26 *razdelimo na* 26 *enic. K vsaki enici pripišemo ali x_1 ali x_2 ali x_3, ki se tako ponavljajo. Ob tem moramo zagotoviti v primeru (a), da imamo vsaj eno enico dodeljeno k vsaki spremenljivki, da bodo rešitve res iz naravnih števil. To pomeni, da pravzaprav delimo le še* 23 *enic in velja po izreku 3.8*

$$\#_a = C_p(3,23) = C(25,2) = \frac{25!}{23!2!} = 300.$$

Podobno je v primeru (b), ko moramo na začetku v x_1 pripisati k dvema enkama, x_2 k štirim enkam in x_3 k petim enkam, da izpolnimo dane pogoje. Tako ostane le še 15 enic za razporejanje in velja

$$\#_b = C_p(3,15) = C(17,2) = \frac{17!}{15!2!} = 136.$$

Zgled 3.15 *V prvi košari so rdeče žoge, v drugi košari najdemo zelene žoge, bele žoge so v tretji košari in v zadnji se nahajajo črne žoge. Na koliko različnih načinov lahko izberemo osem žog iz omenjenih košar, če žog iste barve ne razlikujemo med sabo in je v vsaki košari vsaj osem žog? To nalogo lahko prevedemo na reševanje enačbe* $x_1 + x_2 + x_3 + x_4 = 8$ *za* $x_1, x_2, x_3, x_4 \in \mathbb{N}_0$*, kjer* x_i *pomeni število žog iz i-te košare za vsak* $i \in [4]$*. Dodajmo še, da v rešitvi lahko nastopa tudi nič, saj se lahko zgodi, da med izbranimi osmimi žogami ni kakšne barve. Kot v prejšnjem zgledu je potem*

$$\# = C_p(4,8) = C(11,3) = \frac{11!}{8!3!} = 165.$$

3.5 OSNOVNO O BINOMSKEM SIMBOLU

V tem razdelku si bomo ogledali nekatere lastnosti binomskega koeficienta $\binom{n}{k} = C(n,k) = \frac{n!}{(n-k)!k!}$. Osnovne lastnosti zlahka izpeljemo iz same definicije in so

- $\binom{n}{0} = \binom{n}{n} = 1$;
- $\binom{n}{1} = \binom{n}{n-1} = n$;
- $\binom{n}{k} = \binom{n}{n-k}$.

Ime binomski koeficient, kot že na kratko omenjeno, izhaja iz povezave s potenco binoma, o čemer govori naslednji rezultat.

Izrek 3.9 (Binomski izrek) *Za števili* $a, b \in \mathbb{R}$ *in za* $n \in \mathbb{N}$ *velja*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Dokaz. Predstavljajmo si

$$(a+b)^n = (a+b)(a+b)\cdots(a+b),$$

kjer množimo n enakih binomov. Ko množimo te binome, v vsakem oklepaju izberemo, ali bomo množili z a ali z b. Naj bo $k \in [n]_0$ neko izbrano število. Izmed n oklepajev v $(a+b)^n$ izberemo natanko k tistih, kjer bomo množili z b. Seveda moramo pri vseh ostalih $n-k$ oklepajih množiti z a. Tako izmed n oklepajev izbiramo k oklepajev in to lahko storimo na $\binom{n}{k}$ različnih načinov. Prav tako imamo pri tem faktorju potenco $a^{n-k}b^k$, saj smo z b množili k-krat in z a v vseh preostalih $n-k$ možnostih. Ker je k omejen navzdol z 0 in navzgor z n, smo končali z dokazom. ∎

Zgled 3.16 *Izračunajmo* $(2x-3y)^4$. *Po izreku 3.9 je*

$$\begin{aligned}(2x-3y)^4 &= \binom{4}{0}(2x)^4(-3y)^0+\binom{4}{1}(2x)^3(-3y)^1+\\ &\quad+\binom{4}{2}(2x)^2(-3y)^2+\binom{4}{3}(2x)^1(-3y)^3+\binom{4}{4}(2x)^0(-3y)^4=\\ &= 16x^4-96x^3y+216x^2y^2-216xy^3+81y^4.\end{aligned}$$

Zgled 3.17 *Določimo koeficient pri* a^6b^9 *v binomu* $(3a-2b)^{15}$. *Ob upoštevanju koeficienta* 3 *pri* a *in* -2 *pri* b *je po izreku 3.9*

$$\# = \binom{15}{9}3^6(-2)^9 = -4\,269\,957\,120.$$

Zgled 3.18 *Določimo koeficient pri* $x^3y^4z^5$ *v trinomu* $(x+y+z)^{12}$. *Uporabimo podoben razmislek kot v dokazu izreka 3.9. Tako med 12. oklepaji* $(x+y+z)$ *izbiramo tri, kjer bomo množili z* x. *To lahko storimo na* $\binom{12}{3}$ *različnih načinov. Izmed preostalih 9 oklepajev izberemo štiri tiste, kjer bomo množili z* y, *kar storimo na* $\binom{9}{4}$ *različnih načinov. Na koncu nam ostane pet oklepajev, kjer množimo z* z *in to lahko storimo na* $\binom{5}{5}=1$ *način. Vse zdužimo po pravilu množenja in imamo*

$$\# = \binom{12}{3}\binom{9}{4}\binom{5}{5} = 27\,720.$$

Vse binomske koeficiente lahko po vrsticah zložimo v shemo na naslednji način:

n													
0						1							
1					1		1						
2				1		2		1					
3			1		3		3		1				
4		1		4		6		4		1			
5	1		5		10		10		5		1		
6		1		6		15		20		15		6		1
7	1		7		21		35		35		21		7		1
⋮			⋮				⋮				⋮		

Tej shemi rečemo tudi Pascalov[9] trikotnik. Pascalov trikotnik je ena bolj znanih kombinatoričnih shem in vsebuje veliko lepih lastnosti. Oglejmo si rekurzivno relacijo, ki se skriva v njem in nam omogoča, da zlahka izračunamo naslednjo vrstico, če le poznamo prejšnjo vrstico.

9 Blaise Pascal (1623-1662) je bil francoski matematik, ki je najbolj znan po delu v projektivni geometriji in verjetnosti, velja pa tudi za izumitelja kalkulatorja.

Izrek 3.10 *Za števili $n \in \mathbb{N}$ in $k \in [n]$ velja*

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

Dokaz. Naj bo X množica, ki vsebuje n elementov in med njimi ni elementa a. Tako množica $Y = X \cup \{a\}$ vsebuje $n+1$ elementov. Iz nje lahko izberemo k elementov na dva načina.

(A) med k izbranimi elementi ni elementa a. To pomeni, da so vsi izbrani elementi iz množice X in jih lahko izberemo na $\binom{n}{k}$ različnih načinov.

(B) med k izbranimi elementi je a. To pomeni, da je med izbranimi elementi $k-1$ elementov iz X in njih lahko izberemo na $\binom{n}{k-1}$ različnih načinov.

Ker imata oba načina prazen presek, ju lahko združimo po pravilu seštevanja in dobimo končen rezultat. ∎

Zgled 3.19 *Pokažimo, da za vsak $n \in \mathbb{N}$ velja*

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^{n-1}\binom{n}{n-1} + (-1)^n\binom{n}{n} = 0.$$

Če uporabimo lastnost $\binom{n}{0} = \binom{n}{n} = 1$ in izrek 3.10, potem je leva stran prejšnjega izraza enaka

$$1 - \left[\binom{n-1}{0} + \binom{n-1}{1}\right] + \left[\binom{n-1}{1} + \binom{n-1}{2}\right] - \cdots$$
$$\cdots + (-1)^{n-1}\left[\binom{n-1}{n-2} + \binom{n-1}{n-1}\right] + (-1)^n.$$

Seveda se v tem izrazu večina vrednosti odšteje, ostane le

$$1 - \binom{n-1}{0} + (-1)^{n-1}\binom{n-1}{n-1} + (-1)^n = 1 - 1 + (-1)^{n-1} + (-1)^n = 0,$$

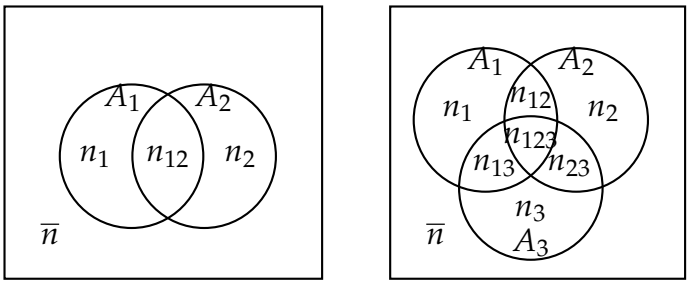
s čimer smo pokazali željeno.

3.6 VKLJUČITVE IN IZKLJUČITVE

V tem razdelku bomo podali odgovor na vprašanje, koliko elementov vsebuje $A_1 \cup A_2 \cup \cdots \cup A_k$, če preseki med poljubnimi množicami niso prazni. Spomnimo se, da v primeru paroma disjunktnih množic $A_1, A_2, \ldots, A_k$ lahko uporabimo pravilo seštevanja. Zlahka lahko vidimo, recimo na primeru dveh množic A_1 in A_2, da to pravilo ne velja, če je $A_1 \cap A_2 \neq \emptyset$ (glej desni diagram slike 4).

Najprej vpeljimo oznake, ki nas bodo spremljale skozi ta razdelek. Naj bo M univerzalna množica z močjo $|M| = n$. Naj bodo $A_1, A_2, \ldots, A_k \subseteq M$ z močjo $n_i = |A_i|$ za vsak $i \in [k]$. S tem nadaljujemo za poljubni presek dveh množic. Tako označimo $n_{ij} = |A_i \cap A_j|$, kjer sta $i, j \in [k]$ in je $i < j$. Naslednja oznaka je $n_{ij\ell} = |A_i \cap A_j \cap A_\ell|$ za $i, j, \ell \in [k]$ in $i < j < \ell$. Nadaljujemo z enakim vzorcem vse do $n_{12\ldots k} = |A_1 \cap A_2 \cap \cdots \cap A_k|$. Dodajmo še oznako za moč komplementa unije, ki je $\overline{n} = |M - (A_1 \cup A_2 \cup \cdots \cup A_k)|$. Unija $A_1 \cup A_2 \cup \cdots \cup A_k$ in njen komplement imata seveda prazen presek in zanju lahko uporabimo pravilo seštevanja. Tako velja

$$n = \overline{n} + |A_1 \cup A_2 \cup \cdots \cup A_k|. \tag{7}$$



Slika 4: Vključitve in izključitve v primeru dveh, oziroma treh množic.

Zaradi lažjega razumevanja si najprej oglejmo primer, ko je $k = 3$, saj lahko ta primer lepo predstavimo s sliko (glej desni diagram slike 4). V tem primeru imamo $n_1, n_2, n_3, n_{12}, n_{13}, n_{23}$ in n_{123}, ob n in $\overline{n}$ seveda. Za začetno oceno $|A_1 \cup A_2 \cup A_3|$ lahko uporabimo pravilo seštevanja, vendar se je potrebno zavedati, da v tem primeru preseke dveh množic štejemo dvakrat, presek vseh treh množic pa celo trikrat. Tako lahko zapišemo

$$|A_1 \cup A_2 \cup A_3| \leq n_1 + n_2 + n_3.$$

Seveda velja enačaj natanko takrat, ko so preseki paroma prazni, saj je to potem pravilo seštevanja. To oceno lahko izboljšamo tako, da moči presekov dveh množic enostavno odštejemo, saj smo jih šteli dvakrat. Ob tem lahko opazimo, da moč preseka $A_1 \cap A_2 \cap A_3$, ki smo ga prej šteli trikrat, sedaj tudi trikrat odštejemo. Tako dobimo

$$n_1 + n_2 + n_3 - n_{12} - n_{13} - n_{23} \leq |A_1 \cup A_2 \cup A_3| \leq n_1 + n_2 + n_3.$$

Na levi strani imamo enačaj natanko takrat, ko je $n_{123} = 0$, saj smo do sedaj elemente iz $A_1 \cap A_2 \cap A_3$ trikrat prišteli in trikrat odšteli. Tako do enačaja v vseh primerih potrebujemo še moč preseka $A_1 \cap A_2 \cap A_3$ in dokazali smo naslednjo trditev.

Trditev 3.11 *Naj bodo $A_1, A_2, A_3 \subseteq M$. Ob dogovorjenih oznakah velja*

$$|A_1 \cup A_2 \cup A_3| = n_1 + n_2 + n_3 - n_{12} - n_{13} - n_{23} + n_{123} \quad \textit{in}$$

$$\overline{n} = n - n_1 - n_2 - n_3 + n_{12} + n_{13} + n_{23} - n_{123}.$$

Preden ilustriramo ti dve formuli na dveh primerih, omenimo še, da druga formula sledi neposredno iz (7).

Zgled 3.20 *Koliko naravnih števil $n \in [1000]$ je deljivo s 5, s 7, ali z 11? Označimo z A_1 vsa naravna števila iz $[1000]$, ki so deljiva s 5, z A_2 vsa naravna števila iz $[1000]$, ki so deljiva s 7 in z A_3 vsa naravna števila iz $[1000]$, ki so deljiva z 11. Tako imamo*

$$n_1 = \left\lfloor \frac{1000}{5} \right\rfloor = 200,\ n_2 = \left\lfloor \frac{1000}{7} \right\rfloor = 142,\ n_3 = \left\lfloor \frac{1000}{11} \right\rfloor = 90,$$

$$n_{12} = \left\lfloor \frac{1000}{35} \right\rfloor = 28,\ n_{13} = \left\lfloor \frac{1000}{55} \right\rfloor = 18,\ n_{23} = \left\lfloor \frac{1000}{77} \right\rfloor = 12$$

$$\textit{in}\ \ n_{123} = \left\lfloor \frac{1000}{385} \right\rfloor = 2.$$

Tukaj simbol $\lfloor x \rfloor$ pomeni največje celo število, ki je manjše ali enako (realnemu) številu x. Po trditvi 3.11 imamo

$$\# = 200 + 142 + 90 - 28 - 18 - 12 + 2 = 376.$$

Zgled 3.21 *Spomnimo se zgleda 3.14, kjer smo reševali enačbo $x_1 + x_2 + x_3 = 26$, $x_1, x_2, x_3 \in \mathbb{N}$. Koliko različnih rešitev ima ta enačba ob dodatnih pogojih $x_1 \leq 12$, $x_2 \leq 11$ in $x_3 \leq 10$? Če so bili pogoji za spodnje meje, nismo imeli težav, glej zgled 3.14, sedaj pa so spremenljivke omejene navzgor. Določimo množice, da bomo lahko uporabili trditev 3.11. V množici M so vse rešitve enačbe, v množico A_1 damo vse rešitve enačbe, za katere velja $x_1 > 12$, podobno so v A_2 vse rešitve enačbe z $x_2 > 11$ in v A_3 vse rešitve enačbe s pogojem $x_3 > 10$. Seveda je jasen pomen presekov teh množic. Sedaj lahko razmišljamo na enak način kot v zgledu 3.14 in imamo*

$$n = C_p(3,23) = \binom{25}{2} = 300,\ n_1 = C_p(3,11) = \binom{13}{2} = 78,$$

$$n_2 = C_p(3,12) = \binom{14}{2} = 91, n_3 = C_p(3,13) = \binom{15}{2} = 105,$$

$$n_{12} = C_p(3,0) = \binom{2}{2} = 1,\ n_{13} = C_p(3,1) = \binom{3}{2} = 3,$$

$$n_{23} = C_p(3,2) = \binom{4}{2} = 6\ \textit{in}\ n_{123} = 0.$$

Po trditvi 3.11 imamo

$$\# = 300 - 78 - 91 - 105 + 1 + 3 + 6 - 0 = 36.$$

Sedaj se lahko lotimo tudi splošnega primera.

Izrek 3.12 (Vključitve in izključitve) *Naj bodo $A_1, A_2, \ldots, A_k \subseteq M$. Ob dogovorjenih oznakah velja*

$$|A_1 \cup A_2 \cup \cdots \cup A_k| = \sum_{1\le i\le k} n_i - \sum_{1\le i<j\le k} n_{ij} + \sum_{1\le i<j<\ell\le k} n_{ij\ell} - \cdots + (-1)^{k-1} n_{12\ldots k}$$

$$\text{in } \overline{n} = n - |A_1 \cup A_2 \cup \cdots \cup A_k|.$$

Dokaz. Opazimo lahko, da je zaradi (7) drugi enačaj neposredna posledica prvega enačaja v izreku. Tako bomo dokazali le prvi enačaj. Tukaj bomo pokazali, da element $x \in A_1 \cup A_2 \cup \cdots \cup A_k$ prispeva natanko 1 k desni strani enačaja. Predpostavimo, da se x nahaja točno v ℓ množicah A_i, $i \in [k]$, v preostalih $k - \ell$ množicah ga pa ni. Tako prispeva ℓ k vsoti $\sum_{1\le i\le k} n_i$. Po drugi strani obstaja natanko $\binom{\ell}{2}$ različnih parov množic, ki vsebujejo x. Zato x prispeva $\binom{\ell}{2}$ k drugi vsoti $\sum_{1\le i<j\le k} n_{ij}$. V tretji vsoti ga lahko najdemo natanko v $\binom{\ell}{3}$ različnih trojicah, kar je tudi prispevek k tretji vsoti $\sum_{1\le i<j<\ell\le k} n_{ij\ell}$. Z nadaljevanjem tega razmisleka in ob upoštevanju alterniranja predznaka v izrazu dobimo, da je x prisoten

$$\binom{\ell}{1} - \binom{\ell}{2} + \binom{\ell}{3} - \cdots + (-1)^{\ell-1}\binom{\ell}{\ell}$$

krat na desni strani enačaja. Iz zgleda 3.19 lahko vidimo, da je zgornja vsota enaka $\binom{\ell}{0} = 1$, s čimer je izrek dokazan. ∎

Zgled 3.22 *Naj bo $|X| = s \ge t = |Y|$. Preštejmo, koliko je vseh različnih surjektivnih funkcij $f : X \to Y$. Očitno je vseh funkcij t^s po izreku 3.7. Vendar vse niso surjektivne in jih moramo nekaj odšteti. Tako označimo z A_i, $i \in [t]$, množico, ki vsebuje vse tiste funkcije, kjer ne obstaja $x \in X$, ki se preslika v element $y_i \in Y$. Takšne funkcije niso surjektivne in jih moramo odšteti od števila vseh funkcij. Element y_i lahko določimo na $\binom{t}{1}$ različnih načinov. Ob tem se vsi elementi iz X lahko preslikajo na poljuben način v $Y - \{y_i\}$, ki vsebuje $t - 1$ elementov. Različnih takih funkcij obstaja $(t-1)^s$ po izreku 3.7. Z uporabo pravila množenja dobimo*

$$\sum_{1\le i\le k} n_i = \binom{t}{1}(t-1)^s.$$

S podobnim razmislekom opazimo tudi, da velja

$$\sum_{1\le i<j\le k} n_{ij} = \binom{t}{2}(t-2)^s,$$

saj lahko dva elementa iz Y, v katera se ne preslika noben element, izberemo na $\binom{t}{2}$ različnih načinov, preostali pa se lahko slikajo v kateregakoli iz preostalih $t - 2$ elementov.

S tem nadaljujemo vse do $\binom{t}{t-1}(t-(t-1))^s = \binom{t}{t-1} = t$, *saj je zadnji člen enak* 0. *Po drugi enakosti izreka 3.12 imamo*

$$\begin{aligned} \# &= t^s - \binom{t}{1}(t-1)^s + \binom{t}{2}(t-2)^s - \cdots + (-1)^t \binom{t}{t-1}(t-(t-1))^s = \\ &= \sum_{k=0}^{t-1} (-1)^k \binom{t}{k}(t-k)^s. \end{aligned}$$

Zgled 3.23 *V konjski dirki tekmuje deset konjev (z jezdeci), ki so rangirani od* 1 *do* 10 *glede na stavniške kvote. John sklene 10 stav in sicer za konja, ki je rangiran na i-to,* $i \in [10]$, *mesto, tudi stavi, da bo dosegel i-to mesto v končni razvrstitvi. Razmislimo, na koliko različnih načinov se lahko konča dirka, da bo John izgubil vseh 10 stav. Ekvivalentno vprašanje temu je, na koliko različnih načinov lahko razvrstimo 10 števil tako, da i-to število,* $i \in [10]$, *ne bo na i-tem mestu. Označimo z* A_i *množico vseh tistih razvrstitev, da je število i na i-tem mestu. Vseh razvrstitev je* 10!. *Če je eno število na pravem mestu, potem lahko le-tega izberemo na* $\binom{10}{1}$ *različnih načinov, vse preostale pa razvrstimo na* 9! *različnih načinov. Tako je*

$$\sum_{1 \le i \le 10} n_i = \binom{10}{1} 9!.$$

S podobnim razmislekom pridemo do

$$\sum_{1 \le i < j \le 10} n_{ij} = \binom{10}{2} 8!,$$

saj dve števili, ki sta na pravem mestu, izberemo na $\binom{10}{2}$ *različnih načinov, preostale pa razvrstimo poljubno na* 8! *različnih načinov. Tako postopoma določimo še preostale vsote in imamo po drugi enakosti izreka 3.12*

$$\begin{aligned} \# &= 10! - \binom{10}{1} 9! + \binom{10}{2} 8! - \cdots + \binom{10}{10} 0! = \\ &= \sum_{k=0}^{10} (-1)^k \binom{t}{k} (10-k)!. \end{aligned}$$

Izpeljimo zgornjo vsoto bolj podrobno

$$\begin{aligned} \# &= 10! - \frac{10!}{1!9!} 9! + \frac{10!}{2!8!} 8! - \cdots + \frac{10!}{10!0!} 0! = \\ &= 10! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{1}{10!}\right). \end{aligned}$$

Bralec s poglobljenim znanjem iz analize funkcij bo v zadnjem oklepaju prepoznal Taylorjev polinom desete stopnje za $f(x) = e^x$ *pri vrednosti* $x = -1$. *Tako velja*

$$\# \approx 10! e^{-1}.$$

Razvrstitve v zadnjem zgledu nosijo posebno ime in sicer **deranžacije**. Za poljuben $n \in \mathbb{N}$ je razmislek pri iskanju deranžacij dolžine n enak in rezultat, ki ga tokrat označimo z d_n, je potem

$$d_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right). \tag{8}$$

Ponovno lahko približno vrednost za d_n izračunamo s pomočjo Taylorjevega polinoma in imamo $d_n \approx n!e^{-1}$. Ta približek je bolj natančen pri velikih številih.

3.7 DIRICHLETOV PRINCIP ALI PRINCIP GOLOBNJAKA

V tem kratkem razdelku bomo spoznali Dirichletov[10] princip ali princip golobnjaka, kot se zadnja leta popularno imenuje. Najprej bomo dokazali rezultat, ki je osnova za omenjeni princip. Pred tem se spomnimo, da je funkcija $f : A \to B$ injektivna, če iz $x \neq y$ sledi, da velja $f(x) \neq f(y)$ za vsaka $x, y \in A$. Ta pogoj se pogosto uporablja kot kontrapozicija in se glasi: $f : A \to B$ je injektivna, če iz $f(x) = f(y)$ sledi, da je $x = y$.

Izrek 3.13 *Naj bosta $m, n \in \mathbb{N}$. Če obstaja injektivna funkcija $f : [n] \to [m]$, potem je $n \leq m$.*

Dokaz. Dokažimo ta izrek s pomočjo indukcije za n. Če je $n = 1$, je trditev resnična za vsak m, saj je $m \in \mathbb{N}$ in zato velja $1 \leq m$, s čimer je baza dokazana.

Naj bo sedaj $n \geq 1$ in predpostavimo, da je izrek resničen za vsa naravna števila iz množice $[n]$. Pokažimo, da je resnična tudi za $n+1$. Naj bo $f : [n+1] \to [m]$ injektivna. Ker je $n + 1 \geq 2$, mora biti tudi $m > 1$ zaradi injektivnosti f. Torej je m naslednik nekega naravnega števila k in velja $m = k + 1$. Skonstruirali bomo injektivno funkcijo $f^* : [n] \to [k]$, iz katere bo sledilo, da je $n \leq k$ po indukcijski predpostavki.

Predpostavimo najprej, da je $f(x) \neq k + 1 = m$ za vsak $x \in [n]$. Potem definiramo $f^*(x) = f(x)$ in je f^* injektivna, saj je taka tudi f.

Predpostavimo še, da obstaja $x \in [n]$, za katerega velja $f(x) = k + 1 = m$. Potem je $f(n+1) = y$, kjer je $y \neq k + 1$, saj je f injektivna. V tem primeru definiramo

$$f^*(x) = y \text{ in } f^*(t) = f(t) \text{ za vsak } t \in [n] - \{x\}.$$

Ponovno je f^* injektivna zaradi injektivnosti f. Ker je f^* injektivna v obeh primerih, velja $n \leq k$ po indukcijski predpostavki. Potem pa je tudi $n + 1 \leq m = k + 1$ in dokaz je zaključen. ∎

10 Peter Gustav Lejeune Dirichlet (1805-1859) je bil nemški matematik, ki je prispeval k razvoju teorije števil, teoriji Fourierjeve vrste in funkcijam nasploh.

Kontrapozicija tega izreka se sedaj glasi

$$\text{če je } n > m, \text{ potem ne obstaja injekcija } f : [n] \to [m].$$

V običajnem jeziku se zaradi enostavnosti skušamo izogniti besedi injekcija. Če injektivnost nadomestimo z definicijo, potem dobimo naslednje.

Izrek 3.14 (Dirichletov princip) *Naj bo $f : A \to B$ funkcija in naj bo $|A| = n$ ter $|B| = m$ za neka $n, m \in \mathbb{N}$. Če je $n > m$, potem obstajata različna $x, x' \in A$, da velja $f(x) = f(x')$.*

Terminologija se še sprosti z naslednjo živalsko primerjavo (pomen ostaja enak).

Izrek 3.15 (Princip golobnjaka) *Če se n golobov namesti v m golobjih lukenj golobnjaka, kjer je $n > m$ in $n, m \in \mathbb{N}$, potem bosta vsaj v eni luknji vsaj dva goloba.*

Princip se lahko tudi posploši v naslednji obliki. Dokaz opustimo, saj je očiten. Omenimo le, da sam pogoj $n > m$ sedaj več ni potreben.

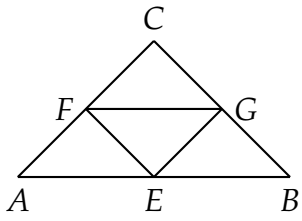
Izrek 3.16 (Posplošen Dirichletov princip) *Naj bo $f : A \to B$ funkcija in je $|A| = n$ ter $|B| = m$ in $n, m \in \mathbb{N}$. Za $k = \lceil \frac{n}{m} \rceil$ obstajajo različni $a_1, a_2, \ldots, a_k \in A$, da velja $f(a_1) = f(a_2) = \cdots = f(a_k)$.*

Izrek 3.17 (Posplošen princip golobnjaka) *Če se n golobov namesti v m golobjih lukenj golobnjaka za $n, m \in \mathbb{N}$, potem je vsaj v eni golobnji luknji vsaj $k = \lceil \frac{n}{m} \rceil$ golobov.*

Na (posplošen) princip golobnjaka je potrebno gledati kot na orodje, ki se pogosto izkaže za uporabno. Tako ga bomo recimo uporabili v dokazu izreka 9.9. Njegova moč je uporabnost na veliko področjih. Težava je le v tem, da se je v danem trenutku, ko so izpolnjeni pogoji, potrebno spomniti nanj.

Zgled 3.24 *Pokažimo, da imata med trinajstimi ljudmi vsaj dva rojstni dan v istem mesecu. Seveda je dvanajst različnih mesecev (ki predstavljajo luknje v golobnjaku) in trinajst ljudi (ki predstavljajo golobe). Po principu golobnjaka imata vsaj dva posameznika rojstni dan v istem mesecu.*

Zgled 3.25 *V enakostraničnem trikotniku s stranico dolžine 1 izberemo 5 točk v notranjosti trikotnika. Pokažimo, da obstajata med njimi dve točki na razdalji manj kot $\frac{1}{2}$. Naj bodo točke E, F in G razpolovišča stranic AB, AC, oziroma BC. Te dodatne točke tvorijo z začetnimi oglišči štiri enakostranične trikotnike s stranico dolžine $\frac{1}{2}$ in sicer AEF, EFG, EBG in GFC, glej sliko 5. Če izberemo 5 točk v notranjosti trikotnika ABC, bosta po principu golobnjaka vsaj dve v enem od manjših trikotnikov AEF, EFG, EBG ali GFC. Ker so dodatno izbrane točke v notranjosti, so različne od točk A, B, C, D, E in F. Tisti dve, ki sta v istem malem trikotniku sta sedaj na razdalji, ki je manjša od $\frac{1}{2}$.*



Slika 5: Situacija iz zgleda 3.25.

Zgled 3.26 *Poslanec Tone bo v* 28 *dneh dopusta odigral vsaj en set tenisa na dan, vendar ne več kot* 40 *setov skupaj. Pokažimo, da obstaja nekaj zaporednih dni, v katerih bo skupaj odigral* 15 *setov. Z* x_i, $i \in [28]$, *označimo število setov, ki jih odigra do konca i-tega dne. Naj bo* $y_i = x_i + 15$ *za* $i \in [28]$. *Ker vsak dan odigra vsaj en set, velja*

$$1 \leq x_1 < x_2 < \cdots < x_{28} \leq 40 \text{ in } 16 \leq y_1 < y_2 < \cdots < y_{28} \leq 55.$$

Tako imamo 56 *števil* $x_1, x_2, \ldots, x_{28}, y_1, y_2, \ldots, y_{28}$, *za katera imamo na razpolago* 55 *različnih vrednosti. Po principu golobnjaka morata biti dve izmed njih enaki. Ker so vsi x-si med seboj različni in vsi y-ni med seboj različni, obstajata* x_i *in* y_j *da velja* $x_i = y_j$. *Toda* $x_i = y_j = x_j + 15$, *zato je od dneva* $i + 1$ *do konca j-tega dneva odigral ravno* 15 *setov.*

3.8 NEKATERE (NE)REŠENE NALOGE

Vaja 3.1 *Prvi igralec ima* 3 *karte in drugi* 9 *kart. Na koliko načinov lahko zamenjata karte (eno ali več), da bosta po zamenjavi imela enako število kart kot na začetku?*

Rešitev. *Zamenjata lahko ali* 0 *ali* 1 *ali* 2 *ali* 3 *karte. Tako je* $\# = 1 + \binom{3}{1}\binom{9}{1} + \binom{3}{2}\binom{9}{2} + \binom{3}{3}\binom{9}{3} = 220$.

Vaja 3.2 *Na koliko načinov lahko sestaviš ogrlico iz 5 rdečih, 3 modrih, 2 zelenih in 1 črne kroglice?*

Rešitev. *Za ogrlico postavljamo kroglice v krog, zato je potrebno eno kroglico fiksirati- najbolje črno (ker je samo ena). Ostale postavimo v vrsto na* $\frac{10!}{5!3!2!}$ *načinov. To število še delimo z 2 za končen rezultat* $\# = 1260$, *saj lahko verižico obračamo.*

Vaja 3.3 *Koliko zaporedij s šestimi črkami imamo v slovenski abecedi, če*

(A) *zaporedje vsebuje natanko en vokal?*

(B) *zaporedje vsebuje vsaj en vokal?*

Rešitev. *Vokal se lahko pojavi na enem izmed šestih mest, imamo* 5 *vokalov in* 20 *soglasnikov, zato je* $\#_a = 6 \cdot 5 \cdot 20^5$. *Za* (b) *od vseh možnosti odštejemo vse besede brez vokalov in je* $\#_b = 25^5 - 20^5$.

Vaja 3.4 *Na koliko načinov lahko razporedimo v vrsto* 5 *študentov,* 4 *študentke,* 3 *dijake in* 3 *dijakinje, če*

(A) *naj predstavniki posameznih skupin stojijo skupaj?*

(B) *so poljubno premešani?*

(C) *morajo študentje stati skupaj, ostali pa poljubno?*

Rešitev. *Imamo* 4 *skupine, ki so poljubno premešane in tudi znotraj posameznih skupin so poljubno premešani, zato je* $\#_a = 4!5!4!3!3!$. *Skupaj jih je* 15, *kar pomeni* $\#_b = 15!$. *Na študente gledamo kot na eno osebo, znotraj katere so poljubno premešani na* 5! *načinov, zato je* $\#_c = 5!11!$.

Vaja 3.5 *Koliko je pravih 5-mestnih števil, ki imajo*

(A) *vse števke različne;*

(B) *vse števke različne in naraščajo (na primer 13789);*

(C) *vse števke različne in padajo;*

(D) *vsaj dve števki enaki;*

(E) *vsaj dve zaporedni števki enaki.*

Rešitev. *Seveda je* $\#_a = 9 \cdot 9 \cdot 8 \cdot 7 \cdot 6 = 27216$, *saj na prvem mestu ne moremo imeti* 0. *Ker nam ena izbira petih števk da natančno eno število (zaradi naraščanja števk), je* $\#_b = \binom{9}{5} = 126$, *saj med števkami ni* 0, *ponovno zaradi naraščanja števk. Za* (c) *lahko k številkam dodamo tudi* 0 *in imamo* $\#_c = \binom{10}{5} = 252$. *Od vseh možnosti* $(9 \cdot 10^4)$ *odštejemo tiste, ki imajo vse števke različne* $(\#_a)$ *in dobimo* $\#_d = 62784$. *Nazadnje je*

$$\#_e = 4 \cdot 9 \cdot 10^3 - 3 \cdot 9 \cdot 10^2 + 2 \cdot 9 \cdot 10 - 1 \cdot 9 = 33471$$

po formuli vključitev in izključitev. Dve zaporedni števki sta lahko enaki na štirih mestih v $9 \cdot 10^3$ *primerih, kjer pa smo nekatere možnosti šteli prevečkrat. Zato odštejemo tiste, ko so tri zaporedne števke enake in tako naprej.*

Vaja 3.6 *Izračunajte katerih je več:*

(A) *štirimestnih števil z lastnostjo, da je vsaka naslednja števka večja ali enaka prejšnji, ali petmestnih števil z isto lastnostjo;*

(B) *štirimestnih števil z lastnostjo, da je vsaka naslednja števka manjša ali enaka prejšnji, ali petmestnih števil z isto lastnostjo.*

Rešitev. *Kot v prejšnji nalogi je* $\#_a(4) = \binom{9}{4} = \binom{9}{5} = \#_a(5)$ *in je obojih enako. Po drugi strani je* $\#_b(4) = \binom{10}{4} < \binom{10}{5} = \#_b(5)$, *saj lahko sedaj vsebujejo ničlo.*

Vaja 3.7 *Na zboru aktiva kmečkih žena spodnje Šajerske je 5 okroglih miz za 10 oseb. Na koliko načinov se lahko posede 50 žena, če*

(A) *ni pogojev;*

(B) *za vsako mizo je natanko ena izmed petih prepirljivk;*

(C) *predsedstvo 10 žena sedi skupaj za najboljšo mizo.*

Rešitev. *Rešitev v prvem primeru je* $\#_a = \frac{50!}{10!10!10!10!10!}10!10!10!10!10!5! = 50!5!$, *saj lahko* 50 *žena razdelimo na* 5 *skupin po* 10 *žena na* $\frac{50!}{10!10!10!10!10!}$ *načinov, mize lahko izbiramo na* 5! *različnih načinov za izbrane desetke, nato za vsako mizo določimo vrstni red na* 10! *načinov (POZOR: tukaj je vrstni red odvisen od pozicije za mizo, saj je pomembno kam si usmerjen). Podobno je* $\#_b = 5!\frac{45!}{9!9!9!9!9!}10!10!10!10!10!5!$ *in* $\#_c = \frac{40!}{10!10!10!10!}10!10!10!10!10!4! = 40!10!4!$.

Vaja 3.8 *Podani sta množici* X *s* s *elementi in* Y *s* t *elementi ter funkcija* $f : X \to Y$.

(A) *Koliko različnih bijektivnih funkcij* f *obstaja, ko je* $s = t$*?*

(B) *Koliko različnih injektivnih funkcij* f *obstaja, ko je* $s \leq t$*?*

Rešitev. *Seveda je* $\#_a = P(n,n) = n!$ *in* $\#_b = P(t,s) = \frac{t!}{(t-s)!}$. *(Spomnimo se, da smo število surjektivnih funkcij določili v zgledu 3.22.)*

Vaja 3.9 *Vsak uporabnik računalniškega sistema ima uporabniško ime, ki je sestavljeno iz petih, šestih, ali sedemih znakov, ki so lahko velike tiskane črke slovenske abecede ali števila. Vsako uporabniško ime se začne s črko in vsebuje vsaj eno cifro. Koliko je vseh uporabniških imen?*

Rešitev. *Rešitev lahko izrazimo z dvojno vsoto, kjer seštevamo glede na dolžino uporabniškega imena (*$k \in \{5,6,7\}$*) in nato pri vsakem k-ju ločimo še glede na število cifer (*$i \in \{1,\ldots,k-1\}$*) kjer i mest s števkami izberemo na* $\binom{k-1}{i}$ *različnih načinov. Tako je* $\# = \sum_{k=5}^{7}\sum_{i=1}^{k-1}\binom{k-1}{i}25^{k-1}10^i$.

Vaja 3.10 *Štirje dečki in osem deklic se posede v krog in igra gnilo jajce (torej en izmed njih ne sedi). Na koliko različnih načinov se lahko posedejo, če jih razlikujemo le po spolu?*

Rešitev. *Njihovo skupno število zmanjšamo za* 2, *ker so razporejeni v krog, enega fiksiramo, in ker eden teka okrog. Ločiti moramo štiri primera, glede na spol tistega, ki je fiksiran in tistega, ki teka okrog. Tako je* $\# = \frac{(12-2)!}{(4-2)!8!} + 2\frac{(12-2)!}{(4-1)!(8-1)!} + \frac{(12-2)!}{4!(8-2)!} = 495$.

Vaja 3.11 *Na neki osnovni šoli je vpisanih 57 prvošolcev. Na koliko načinov jih lahko razporedijo v razrede A, B in C, če mora biti v vsakem razredu*

(A) *enako število učencev?*

(B) *vsaj 18 otrok?*

Rešitev. *Če je v vsakem razredu* 19 *učencev, jih lahko razporedimo na* $\#_a = \frac{57!3!}{(19!)^3}$ *načinov, kjer* 3! *predstavlja določanje razredov* A, B *in* C *izbranim skupinam po* 19 *učencev. Če je v vsakem razredu vsaj* 18 *otrok, potem imamo tri možnosti: enako otrok v vseh razredih,* 18 *otrok v dveh razredih in* 21 *v enem razredu ter po* 18, 19 *in* 20 *otrok v razredih. Tako je* $\#_b = \frac{57!3!}{(19!)^3} + \frac{57!3!}{(18!)^2 21!} + \frac{57!3!}{18!19!20!}$.

Vaja 3.12 *Na koliko načinov lahko razdelimo* 12 *različnih predmetov med* 3 *ljudi, če vsak dobi* 4 *predmete?*

Rešitev. *Seveda je* $\# = \frac{12!}{4!4!4!}$.

Vaja 3.13 *Koliko rešitev ima enačba* $x_1 + x_2 + x_3 = 19$, $x_i \in \mathbb{N}$, *če*

(A) *ni omejitev?*

(B) *velja* $x_1 \geq 3$, $x_2 \geq 4$ *in* $x_3 \geq 5$*?*

(C) *velja* $x_1 \leq 8$, $x_2 \leq 8$ *in* $x_3 \leq 5$*?*

Rešitev. *Za razlago te naloge si lahko ogledamo zgleda 3.14 in 3.20 in rešitev je* $\#_a = C_p(3,16) = 153$, $\#_b = C_p(3,7) = 36$ *in* $\#_c = 6$ *(vključitve in izključitve).*

Vaja 3.14 *Na koliko načinov lahko sosedovim otrokom Katarini, Reneju in Maticu razdeliš 13 bonbonov, če*

(A) *ni omejitev;*

(B) *vsak dobi vsaj dva bonbona;*

(C) *vsak dobi največ šest bonbonov.*

Rešitev. *Ta naloga je enakega tipa kot prejšnja. Rešujemo enačbo* $x_k + x_r + x_m = 13$, *le da so tukaj* $x_k, x_r, x_m \in \mathbb{N}_0$. *Tako je* $\#_a = C_p(3,13) = 105$, $\#_b = C_p(3,7) = 36$ *in* $\#_c = 21$ *(vključitve in izključitve).*

Vaja 3.15 *Štiri najstniške ninja mutantske želve Donatelo, Leonardo, Michelangelo in Rafaelo se ob neki priliki spopadejo z 20 enakovrednimi nasprotniki. Na koliko načinov si lahko razdelijo to dvajseterico, če*

(A) *ni omejitev.*

(B) *vsak pospravi vsaj tri.*

(C) *Donatelo zmore največ štiri zaradi prejšnjih poškodb, Rafaelo pa največ dva, saj ima močan glavobol.*

Rešitev. *Tudi to je naloga enakega tipa kot prejšnji dve, le da imamo štiri spremenljivke. Tako je* $\#_a = C_p(4,20) = 1772$, $\#_b = C_p(4,8) = 165$ *in* $\#_c = \#_a - C_p(4,15) - C_p(4,17) + C_p(4,12) = 270$.

Vaja 3.16 *Štirje igralci igrajo poker (4 barve po 13 kart), pri katerem dobi vsak igralec dve karti, preostale tri pa so skupne vsem štirim. Na koliko načinov lahko prvi igralec dobi:*

(A) *križevo kraljevo barvo (križ asa, kralja, damo, fanta in desetko)?*

(B) *križevo barvo (vseh pet je križev)?*

(C) *poker iz asov (vsi štirje asi, peta karta poljubna)?*

Rešitev. *Najprej je potrebno ugotoviti, da to, kako se karte delijo, ne vpliva na rezultat. Sedaj imamo pet kart, ki so pomembne za prvega igralca in pri kraljevi križevi barvi mora teh pet mest zasesti pet izbranih kart v poljubnem vrstnemo redu. Preostalih 47 kart je razdeljenih poljubno. Tako je* $\#_a = 47!5!$. *Podobno je* $\#_b = \binom{13}{5}47!5!$, *kjer pet križev izberemo na* $\binom{13}{5}$ *različnih načinov in* $\#_c = 5 \cdot 48!4!$, *kjer je peta karta poljubna in je njeno mesto poljubno med petimi za prvega igralca.*

Vaja 3.17 *Tarok je igra s 54 kartami, kjer na začetku deljenja kart izločimo 6 prvih kart, ki jim rečemo talon. Posebno vlogo igrajo pri taroku tri karte škis, mond in pagat, ki jim rečemo trula.*

(A) *Koliko je različnih talonov, kjer je celotna trula v talonu?*

(B) *Koliko je različnih talonov, kjer so škis, mond in pagat zaporedoma v talonu? (Ne nujno v tem vrstnem redu.)*

(C) *Koliko je različnih talonov, kjer so škis, mond in pagat prve tri ali zadnje tri karte v talonu? (Ne nujno v tem vrstnem redu.)*

Rešitev. *Tri karte iz talona so fiksne, izberemo še preostale tri na* $\binom{51}{3}$ *načinov. Karte v talonu so lahko poljubno premešane in imamo* $\#_a = \binom{51}{3}6!$. *Ker je trula v* (b) *in* (c) *skupaj, nanjo gledamo kot na en element, ki je lahko poljubno premešan. Zato je* $\#_b = \binom{51}{3}3!4!$ *in* $\#_c = 2!3!3!\binom{51}{3}$. *Opomnimo še, da nas karte izven talona ne zanimajo.*

Vaja 3.18 *Pri nedavnem odprtju nove trgovine so imeli na zalogi 10 televizorjev in 15 pralnih strojev. V trgovino so spustili 40 kupcev. Na koliko načinov so lahko pokupili te televizorje in pralne stroje, če*

(A) *vsak kupi največ en aparat in*

  (I) *vsi bi imeli raje pralni stroj;*

  (II) *ne delamo razlik med televizorjem in pralnim strojem.*

(A) *trije uspejo kupiti televizor in pralni stroj hkrati in*

  (I) *vsi bi imeli raje pralni stroj;*

  (II) *ne delamo razlik med televizorjem in pralnim strojem.*

Rešitev. *Rešitve so naslednje* $\#_{a_i} = \binom{40}{15}\binom{25}{10}$, $\#_{a_{ii}} = \binom{40}{25}$, $\#_{b_i} = \binom{40}{3}\binom{37}{12}\binom{25}{7}$ *in* $\#_{b_{ii}} = \binom{40}{3}\binom{37}{19}$.

Vaja 3.19 *Študenta imata* 6 *bankovcev po* 50 *EUR in* 4 *bankovce po* 100 *EUR. Bankovcev z isto vrednostjo ne ločimo med sabo.*

(A) *Na koliko načinov si jih lahko razdelita?*

(B) *Na koliko načinov si jih lahko razdelita tako, da dobi vsak enako število bankovcev?*

(C) *Na koliko načinov si jih lahko razdelita tako, da dobita vsak enako vrednost denarja?*

(D) *Na koliko načinov si jih lahko razdelita, če bankovce ločimo med sabo?*

Rešitev. *Ugotoviti je potrebno, da je dovolj opazovati le enega študenta, saj preostanek pripade drugemu študentu. Ko določimo število bankovcev, ki jih prejme prvi, je potem potrebno še ločiti, koliko ima pedesetakov in koliko stotakov. Tako je* $\#_a = 35$, $\#_b = 5$ *in* $\#_c = 3$. *Po drugi strani je* $\#_d = 2^{10}$, *saj imamo za vsak bankovec dve možnosti.*

Vaja 3.20 *V ravnini je* n *točk, od katerih nobena trojica ne leži na isti premici, določajo pa natanko* n *trikotnikov. Izračunaj* n.

Rešitev. *Ker vsaka trojica ni na isti premici, vsaka trojica določa natanko en trikotnik. Tako imamo zvezo* $\binom{n}{3} = n$, *oziroma* $\frac{n!}{3!(n-3)!} = n$. *Ko pokrajšamo in pomnožimo s* 6, *dobimo* $(n-1)(n-2) = 6$, *oziroma* $n^2 - 3n - 4 = 0$, *ki ima rešitvi* $n_1 = 4$ *in* $n_2 = -1$. *Seveda je iskana rešitev* $n = 4$.

Vaja 3.21 *Kakšen je koeficient pri* x^8y^9 *v* $(3x - 2y)^{17}$*?*

Rešitev. *Koeficient je* $\# = 3^8(-2)^9\binom{17}{8}$.

Vaja 3.22 *Dokaži naslednji enakosti:*

(A) $\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}$, $k \leq r \leq n$;

(B) $\binom{2n}{2} = 2\left(\binom{n}{2} + n^2\right)$.

Rešitev. *Obe enakosti zlahka dokažemo, če le upoštevamo definicijo binomskega koeficienta in krajšamo ulomke.*

Vaja 3.23 *Od* 100 *učencev se jih* 28 *ukvarja s košarko,* 30 *z rokometom in* 42 *z nogometom. Med njimi* 8 *s košarko in rokometom,* 10 *s košarko in nogometom ter* 5 *z rokometom in nogometom. Trije učenci se ukvarjajo z vsemi športi hkrati. Koliko učencev se ne ukvarja z nobenim športom?*

Rešitev. *Uporabimo vključitve in izključitve ter dobimo* $\# = 100 - 28 - 30 - 42 + 8 + 10 + 5 - 3 = 20$.

Vaja 3.24 *Po Sahari gre karavana sestavljena iz n kamel. Na koliko načinov se lahko po počitku v oazi razporedijo tako, da nobena kamela ne hodi za isto kamelo, kot je hodila pred počitkom? Naredite še poseben primer za $n = 4$.*

Rešitev. *Vseh razvrstitev je $n!$. Razvrstitev, kjer vsaj ena kamela hodi za isto kot prej, je $\binom{n-1}{1}(n-1)!$, kjer nam binomski simbol pove, na koliko načinov lahko izberemo to eno kamelo izmed $n-1$ kamel (prva od prej ne more hoditi za isto kot prej!!!), $(n-1)!$ pa nam pove, na koliko načinov jih lahko razporedimo v vrsto. Podobno nadaljujemo: za vsaj dve kameli za istimi kot prej je $\binom{n-1}{2}(n-2)!$ načinov in tako naprej. Po načelu vključitev in izključitev dobimo*

$$\# = n! - \binom{n-1}{1}(n-1)! + \binom{n-1}{2}(n-2)! - \cdots + (-1)^{n-1}\binom{n-1}{n-1}1! =$$

$$= \sum_{k=0}^{n-1}(-1)^k\binom{n-1}{k}(n-k)!.$$

V primeru, ko je $n = 4$, je $\# = 11$.

Vaja 3.25 *Poslati moramo n različnih pisem na n različnih naslovov. Pomešamo naslove. Na koliko načinov lahko izberemo naslove tako, da*

(A) *natanko dve pismi ne bosta prispeli na pravi naslov?*

(B) *natanko tri pisma ne bodo prispela na pravi naslov?*

(C) *nobeno pismo ne bo prišlo na pravi naslov?*

Za vse tri točke izračunaj primer, ko je $n = 4$.

Rešitev. *Velja $\#_a = \binom{n}{2}1$–na koliko načinov lahko izberemo dve pismi, ki bosta zgrešili naslov, krat 1, saj lahko dve pismi pošljemo narobe le na en način; za $n = 4$ imamo $\#_a(4) = 6$. Podobno je $\#_b = \binom{n}{3}2$–na koliko načinov lahko izberemo tri pisma, ki bodo zgrešila naslov, krat 2, saj lahko tri pisma pošljemo narobe na dva načina; za $n = 4$ imamo $\#_b(4) = 8$. Zadnjo nalogo rešimo s pomočjo vključitev in izključitev in imamo $\#_c = \sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)!$, kjer člen $\binom{n}{i}(n-i)!$ pomeni, da vsaj i pisem gre na pravi naslov; tokrat je $\#_c(4) = 9$.*

Vaja 3.26 *Točke ravnine pobarvamo z dvema barvama. Pokaži, da vedno obstaja enako pobarvan par točk na razdalji ena.*

Rešitev. *Izberimo enakostranični trikotnik v ravnini. Ima tri oglišča, ki so paroma na razdalji ena. Ker so pobarvana z dvema barvama, sta vsaj dve izmed njih po principu golobnjaka enake barve in ti dve predstavljata iskani par.*

Vaja 3.27 *Naj bo $a_1, a_2, \ldots, a_n$ končno zaporedje celih števil. Pokaži, da vsebuje strnjeno podzaporedje, katerega vsota je deljiva z n. Pomagaj si z delnimi vsotami in ostanki pri deljenju.*

Rešitev. *Definirajmo delno vsoto prvih i členov z $s_i = a_1 + a_2 + \cdots + a_i$ za vsak $i \in [n]$. Če n deli nek s_i, $i \in [n]$, potem n deli vsoto prvih i števil tega zaporedja in smo končali. Sicer imamo največ $n-1$ različnih ostankov pri deljenju delnih vsot z n, saj 0 ni med njimi. Po principu golobnjaka imata vsaj dva med njimi, recimo s_i in s_j, $i < j$, enak ostanek r pri deljenju z n, kjer je $0 < r < n$. Tako je $s_i - r = kn$ in $s_j - r = \ell n$. Če ju odštejemo, dobimo $s_j - s_i = (\ell - k)n$ in n deli $s_j - s_i$. Po drugi strani je $s_j - s_i = a_{i+1} + a_{i+2} + \cdots + a_j$, kar je vsota členov strnjenega podzaporedja.*

Vaja 3.28 *Naj bo množica S podmnožica množice $A = [2n]$ z $n+1$ elementi. Pokaži, da obstajata dve različni števili $x, y \in S$, da x deli y. Pomagaj si z zapisom $x = 2^r a$, kjer je a liho število in mu pravimo lihi del števila x.*

Rešitev. *Naj bo $S = \{x_1, x_2, \ldots, x_{n+1}\} = \{2^{r_1}a_1, 2^{r_2}a_2, \ldots, 2^{r_{n+1}}a_{n+1}\}$. Števila iz A imajo največ n različnih lihih delov. Tako sta v S po principu golobnjaka vsaj dva enaka liha dela a_i in a_j za različna $i, j \in [n+1]$. Če je $r_i > r_j$, potem x_j deli x_i, sicer je $r_i < r_j$ in x_i deli x_j. Tako smo našli različni števili iz S, kjer eno deli drugo.*

4

REKURZIVNE RELACIJE

Ponavljajočim se procesom se ni moč izmakniti. Že samo izmenjavanje dneva in noči je primer takšnega procesa. (Ob tem zanemarimo, da dolžina enega in drugega nekoliho niha preko leta.) Podobno si lahko za enoto vzamemo kakšno drugo časovno obdobje, recimo teden, mesec ali leto. Seveda ni pričakovati, da bodo recimo dnevi v tednu enaki. Tako je sreda v enem tednu lahko podobna sredi v naslednjem tednu, saj je urnik na fakulteti enak (znotraj enega semestra), vendar lahko imamo različen zajtrk. Tako lahko zaporednim dogodkom pripišemo nek opis (glede na katero izmed prej omenjenih časovnih enot ali kaj popolnoma drugega).

Nekateri dogodki so predvidljivi, kot recimo omenjeni urnik, ki ga poznamo vnaprej za cel semester, druge dogodke težko predvidimo vnaprej. To je lahko že dobra in dolga zabava na ŠTUKu, zaradi katere se zjutraj ne moremo vstati in zamudimo prva predavanja.

Matematično nas zanima napoved naslednjega dogodka. Tako lahko datum določimo iz prvega dneva v letu, če le poznamo število dni, ki so pretekli od omenjenega prvega dneva. Po drugi strani pogosto potrebujemo nedavne informacije, kot je recimo tista z zabavo na ŠTUKu. Zaporednim dogodkom v matematiki rečemo zaporedja. Če lahko nek element iz zaporedja dobimo s poznavanjem nekaj prvih členov tega zaporedja, potem je zaporedje podano s splošnim členom. Kadar pa naslednji element zaporedja določimo iz nekaj njegovih predhodnikov, potem rečemo, da je zaporedje podano rekurzivno.

Oba omenjena načina sta koristna in zaželeno je, da znamo preiti iz ene možnosti v drugo. To se bomo naučili v tem poglavju za nekatera rekurzivno podana zaporedja. To je uporabno v računalništvu, kjer imamo stavke, ki se večkrat ponovijo. Zlasti to velja za FOR stavek, pa tudi v primeru WHILE in UNTIL stavkov pride prav, le da je potem potrebno še oceniti, največ kolikokrat se izvedeta. S tem pristopom lahko pogosto preštejemo, koliko operacij je potrebnih (v najslabšem primeru), da se algoritem izvede. Tako lahko primerjamo algoritme med seboj po učinkovitosti, kar bo tema naslednjega poglavja.

Dodatna literatura v slovenščini je dostopna v [11]. V angleškem jeziku je na voljo precej več primerne literature, tukaj omenimo le [6] in nekoliko drugačen pristop v [1]. Marsikaj je najti tudi na spletu in pogosto je že Wikipedia (angleška) dober začetni vir informacij. Standardna zbirka nalog za to poglavje je [9]. Veliko izpitnih nalog iz tega poglavja je najti v [12, 13].

4.1 DEFINICIJA

Funkciji $a : \mathbb{N} \to Y$ rečemo **zaporedje**. Pogosto množico $\mathbb{N}$ nadomestimo z $\mathbb{N}_0$, kar pa je običajno razvidno že iz predpisa. Če je $Y = \mathbb{R}$, potem govorimo o **realnih zaporedjih**. V primeru, ko je $Y = \mathbb{C}$, govorimo o **kompleksnih zaporednjih**. Namesto $a(n)$ pogosto pišemo kar a_n. Tukaj je a_n funkcijska vrednost, v katero se preslika element n. Če želimo označiti celotno zaporedje, to storimo s simbolom (a_n) ali $(a_n)_{n\in\mathbb{N}}$. Kadar je podan funkcijski predpis za zaporedje a_n, rečemo, da je zaporedje podano s **splošnim členom**. Zaporedja pogosto zapišemo tudi z nekaj začetnimi členi $(a_n) = (a_1, a_2, a_3, \ldots)$. Tako se lahko spomnimo dveh tipov zaporedij, ki so natančno obravnavana v srednji šoli.

Zaporedju podanemu s splošnim členom oblike

$$a_n = a_0 + nd, d \in \mathbb{R}, n \in \mathbb{N}_0,$$

rečemo **aritmetično zaporedje**. Vrednost a_0 je **začetna vrednost** zaporedja in imamo $(a_n) = (a_0, a_0 + d, a_0 + 2d, a_0 + 3d, \ldots)$.

Kadar je zaporedje podano s splošnim členom oblike

$$a_n = q^n a_0, q \in \mathbb{R}, n \in \mathbb{N}_0,$$

govorimo o **geometrijskem zaporedju**. Ponovno je a_0 začetna vrednost in velja $(a_n) = (a_0, qa_0, q^2a_0, q^3a_0, \ldots)$.

V prejšnjem poglavju smo s preštevanji že dobili veliko zaporedij, ki so podani s splošnim členom. Tako lahko gledamo na recimo $p_n = P(n, n) = n!$ kot na zaporedje, medtem ko $P(n, k)$ ni zaporedje, če le n in k prosto izbiramo, saj imamo tukaj dve spremenljivki n in k, ki sta sicer obe naravni števili. Če rečemo, da je k fiksno število, ki se ne spreminja, recimo $k = k_0$, potem postane $p_n^{k_0} = P(n, k_0) = \frac{n!}{(n-k_0)!}$ zaporedje. Podobno lahko fiksiramo tudi $n = n_0$ in imamo $p_k^{n_0} = P(n_0, k) = \frac{n_0!}{(n_0-k)!}$. Strogo gledano $p_k^{n_0}$ ni zaporedje, saj je definiran le za $k \in [n_0]_0$, ne pa tudi ko je $k > n_0$. Vendar lahko proglasimo $p_k^{n_0} = 0$ za vsak $k > n_0$ in s tem dobimo zaporedje, ki mu rečemo **končno zaporedje.** Na podoben način se lahko poigramo tudi s $C(n, k)$, $P_p(n, k)$ in s $C_p(n, k)$.

Podrobneje si oglejmo primer deranžacij (8), ki smo jih obravnavali na koncu razdelka o vključitvah in izključitvah v zgledu 3.23. Spomnimo se

$$d_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right),$$

kar je seveda zaporedje. Opravimo naslednji izračun

$$\begin{aligned} nd_{n-1} &= n(n-1)!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^{n-1}\frac{1}{(n-1)!}\right) \\ &= n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^{n-1}\frac{1}{(n-1)!}\right) + (-1)^n - (-1)^n \\ &= n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^{n-1}\frac{1}{(n-1)!} + (-1)^n\frac{1}{n!}\right) - (-1)^n \\ &= d_n - (-1)^n. \end{aligned}$$

Izrazimo lahko d_n in dobimo

$$d_n = nd_{n-1} + (-1)^n, n \geq 2, d_1 = 0, \tag{9}$$

kjer je očitno začetna vrednost $d_1 = 0$, saj ne obstaja deranžacija na enem elementu.

Ta zapis se razlikuje od zapisa s splošnim členom, saj lahko naslednji člen izračunamo iz prejšnjega člena. Zapisu zaporedja, kjer lahko naslednji člen izračunamo iz nekaj prejšnjih, bomo rekli **rekurzivna relacija**, oziroma **rekurzija**. Drugo ime za rekurzivno relacijo je **differenčna enačba**, ki ga bomo tudi uporabljali.

Opravimo še dodaten izračun z deranžacijami

$$\begin{aligned} d_{n+1} &= (n+1)!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n\frac{1}{n!} + (-1)^{n+1}\frac{1}{(n+1)!}\right) \\ &= (n+1)n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n\frac{1}{n!}\right) + (-1)^{n+1} \\ &= (n+1)d_n + (-1)^{n+1} \\ &= nd_n + d_n - (-1)^n \\ &= nd_n + nd_{n-1}, \end{aligned}$$

kjer smo zadnjo vrstico dobili iz (9). Če v tem izračunu prestavimo indeks iz $n+1$ v n, dobimo že drugo rekurzivno relacijo za deranžacije in sicer

$$d_n = (n-1)(d_{n-1} + d_{n-2}), n \geq 3, d_1 = 0, d_2 = 1, \tag{10}$$

kjer ni težko videti, da obstaja točno ena deranžacija na dveh elementih.

Kadar so zaporedja podana s splošnim členom, lahko pogosto, z nekaj dela, izrazimo rekurzivno relacijo, kot smo to storili v primeru deranžacij. To je smiselno, če nam to olajša računanje naslednjih členov. To vedno ni očitno, saj moramo za d_{100} ob uporabi (9) ali (10) izračunati vse predhodnike od d_1 do d_{99}. Vendar je to v tem primeru bolje kot računanje d_{100} z (8), kjer moramo prav tako sešteti 100 členov, ki jih je težje izračunati. Več o hitrosti računanja bomo spoznali v naslednjem poglavju.

Zgled 4.1 *Rekurzivna relacija aritmetičnega zaporedja je*

$$a_n = a_{n-1} + d, n \in \mathbb{N}, d, a_0 \in \mathbb{R}.$$

Dobimo jo iz splošnega člena tako, da od $a_n = a_0 + nd$ odštejemo $a_{n-1} = a_0 + (n-1)d$.

Zgled 4.2 *Rekurzivna relacija geometrijskega zaporedja je*

$$a_n = qa_{n-1}, n \in \mathbb{N}, q, a_0 \in \mathbb{R}.$$

Dobimo jo iz splošnega člena tako, da $a_{n-1} = q^{n-1}a_0$ vstavimo v splošni člen $a_n = q^n a_0 = q(q^{n-1}a_0) = qa_{n-1}$.

Do takšne zagate ne pride vedno, saj je, recimo, splošni člen aritmetičnega ali geometrijskega zaporedja precej lažje izračunljiv, kar je vidno iz zgornjih dveh zgledov, kot da bi računali vse dotedanje člene z rekurzivno relacijo. Tako je pogosto lažje zapisati rekurzivno relacijo podanega problema in nato iz podane rekurzije določiti splošni člen. Do tega lahko pogosto pridemo z manipulacijo vhodnih podatkov tako, da izrazimo a_n iz nekaj prejšnjih členov s pomočjo operacij, ki pripeljejo do a_n. To je še posebaj uporabno v analizi algoritmov, kjer lahko dobimo rekurzivno relacijo tako, da zmanjšamo število vhodnih podatkov iz recimo n na $n-1$ in ocenimo ali preštejemo število operacij, ki so dodatno potrebne, ko dodamo opuščene vhodne podatke.

Zgled 4.3 *Zelo znano je Fibonaccijevo zaporedje, ki je podano z rekurzivno relacijo*

$$f_n = f_{n-1} + f_{n-2}, n \geq 3, f_1 = f_2 = 1.$$

Dobljena je iz hipotetičnega razplojevanja zajcev, kjer začnemo z enim parom mladih zajcev. Le ta par v prvem obdobju odraste do spolne zrelosti in se spari. Tako imamo v času brejosti, to je drugo obdobje, še vedno en par zajcev. Ko zajkla skoti, dobimo nov par zajcev, star par pa se ponovno spari. Tako imamo v tretjem obdobju dva para zajcev. Na začetku četrtega obdobja starejša zajkla skoti in imamo zato tri pare zajcev, oba starejša para pa se ponovno sparita. Če s to razlago nadaljujemo, lahko uvidimo, da zgornja rekurzija ustreza temu modelu. (Model je hipotetičen, ker ne predvideva smrti zajcev, tako kot ne upošteva parjenja med sorodniki. Seveda je lahko v leglu tudi več malih zajčkov.) Z enostavnim računanjem dobimo

$$(f_n) = (1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots).$$

Opazimo lahko, da s spremembo začetnih pogojev dobimo drugačno zaporedje. Tako je, recimo, za isto rekurzijo in začetna pogoja $f'_1 = -1$ in $f' = 2$, zaporedje naslednje

$$(f'_n) = (-1, 2, 1, 3, 4, 7, 11, 18, 29, 47, \ldots).$$

Zgled 4.4 *Problem Hanoiskega stolpa je uganka, v kateri imamo tri nosilce označene z* 1, 2 *in* 3 *in n okroglih diskov različnih velikosti. Diski imajo na sredini dovolj veliko luknjo, da jih lahko poveznemo na nosilce. Na začetku so vsi diski zloženi po velikosti na nosilcu 1, pri čemer je največji disk na dnu. Naloga je, da premaknemo vse diske na nosilec* 3*, pri čemer je v vsakem trenutku dovoljeno premikati le en disk iz nosilca na nosilec in manjši disk ne sme biti pod večjim diskom na istem nosilcu. Označimo najmanjše število potrebnih premikov n diskov s h_n. Ni težko videti, da lahko največji disk premaknemo na nosilec* 3 *le, če ni na tem nosilcu nobenega diska. To pomeni, da so vsi preostali diski na nosilcu* 2 *in da so na tem nosilcu zloženi po velikosti. Da premaknemo $n-1$ diskov na nosilec* 2*, potrebujemo h_{n-1} premikov, nato premaknemo največji disk na nosilec* 3 *in zaključimo s ponovnim premikom vseh $n-1$ diskov iz nosilca* 2 *na nosilec* 3*, za kar ponovno porabimo h_{n-1} potez. Skupaj imamo tako rekurzivno relacijo*

$$h_n = 2h_{n-1} + 1, h_1 = 1,$$

ki opiše problem Hanoiskega stolpa za 3 nosilce.

Zgled 4.5 *Algoritem 'Bubble sort' je algoritem, ki uredi n števil $a_1, a_2, \ldots, a_n$ od najmanjšega do največjega (ali obratno). Predpostavimo, da v najslabšem primeru potrebujemo b_n operacij, da razvrstimo n števil. Njegovo delovanje lahko opišemo induktivno. Če je $n = 1$, je eno samo število že tudi urejeno in je $b_1 = 0$. Recimo, da smo že uredili n števil z b_n operacijami v najslabšem primeru in da je na vrsti število a_{n+1}. Če je a_{n+1} manjše od vseh predhodnikov, potrebujemo n zamenjav: najprej s številom na zadnjem n-tem mestu, nato s številom na $(n-1)$-mestu in tako naprej vse do števila, ki je na prvem mestu. To je tudi najslabši možni primer. Iz zapisanega je jasno, da je*

$$b_{n+1} = b_n + n, n \in \mathbb{N}, b_1 = 0$$

rekurzivna relacija, ki opiše število operacij algoritma v najslabšem primeru.

V nadaljevanju bomo preučili nekatere rekurzivne relacije in se naučili, kako iz njih poiskati splošni člen zaporedja. Tega še zdaleč ne znamo narediti za vse rekurzije. Rekurzivni relaciji

$$c_n a_n + c_{n-1} a_{n-1} + \cdots + c_{n-k} a_{n-k} = f(n), c_n, c_{n-1}, \ldots, c_{n-k} \in \mathbb{R}, \qquad (11)$$

rečemo **linearna rekurzivna relacija s konstantnimi koeficienti reda** k. Če je $f(n) = 0$, potem je (11) **homogena linearna rekurzivna relacija s konstantnimi koeficienti reda** k, sicer, ko je $f(n) \neq 0$, ji rečemo **nehomogena linearna rekurzivna relacija s konstantnimi koeficienti reda** k.

Razložimo poimenovanje bolj natančno. Najprej poudarimo, da velja $c_n, c_{n-1}, \ldots, c_{n-k} \in \mathbb{R}$, kar pomeni, da so to fiksna števila. Zato je v imenu zveza konstantni koeficienti. Če si ogledamo obe izpeljani rekurziji (9) in (10) za deranžacije, lahko opazimo, da nista linearni, saj koeficient pred recimo d_{n-1} ni konstanten (to je fiksno število), pač pa je odvisen od n in se spreminja s spreminjanjem n-ja. Vse ostale rekurzije, ki smo jih spoznali, imajo konstantne koeficiente.

Termin linearna nastopa, ker vsi členi iskanega zaporedja nastopajo sami in ne v kakšni funkciji, ki ne bi bila linearna. Vse do sedaj zapisane rekurzije so linearne. Navedimo še dva primera nelinearnih rekurzivnih relacij:

$$a_n = 2a_{n-1}a_{n-2} + 3n \text{ in } b_n = \sqrt{5b_{n-1}} - b_{n-2}^2.$$

V prvi imamo produkt $a_{n-1}a_{n-2}$, ki pokvari linearnost, v drugi pa oba člena $\sqrt{5b_{n-1}}$ in b_{n-2}^2 kvarita linearnost, saj to niso primeri linearnih funkcij.

Nazadnje je v imenu tudi red k. Le-to pomeni, da lahko največji člen v rekurziji izrazimo s k preostalimi členi zaporedja:

$$a_n = \frac{1}{c_n} f(n) - \frac{1}{c_n}(c_{n-1}a_{n-1} + \cdots + c_{n-k}a_{n-k}), c_n, c_{n-1}, \ldots, c_{n-k} \in \mathbb{R}.$$

4.2 HOMOGENE LINEARNE REKURZIVNE RELACIJE

V tem razdelku bomo predstavili postopek reševanja za vse homogene linearne rekurzivne relacije s konstantnimi koeficienti reda k

$$c_n a_n + c_{n-1}a_{n-1} + \cdots + c_{n-k}a_{n-k} = 0, c_n, c_{n-1}, \ldots, c_{n-k} \in \mathbb{R}. \tag{12}$$

Žal je potrebno povedati, da to znamo narediti zgolj, kadar znamo poiskati vse ničle dotičnega z (12) povezanega polinoma. Ker točnih ničel polinoma za polinome dovolj velike stopnje ($k \geq 5$) ne znamo vedno poiskati, nam predstavljena metoda včasih ne pomaga. (Kadar ničel polinoma ne znamo poiskati analitično, še vedno lahko uporabimo numerične metode in z njimi dobimo dobre približke za ničle in s tem tudi za rešitev dane homogene rekurzivne relacije.)

Oglejmo si najprej osnovni izrek o različnih rešitvah (12), ki generirajo novo rešitev. Povedano drugače, vsota dveh rešitev (12) je tudi sama rešitev (12).

Izrek 4.1 *Če sta S_n in T_n rešitvi rekurzivne relacije (12), potem je tudi $U_n = K_1S_n + K_2T_n$ rešitev rekurzivne relacije (12) za poljubni realni števili K_1 in K_2.*

Dokaz. Ker sta S_n in T_n rešitvi rekurzije (12), velja

$$\begin{aligned} c_n S_n + c_{n-1} S_{n-1} + \cdots + c_{n-k} S_{n-k} &= 0 \\ c_n T_n + c_{n-1} T_{n-1} + \cdots + c_{n-k} T_{n-k} &= 0. \end{aligned}$$

Če prvo vrstico pomnožimo s K_1 in drugo s K_2 ter ju nato seštejemo, dobimo

$$c_n(K_1 S_n + K_2 T_n) + c_{n-1}(K_1 S_{n-1} + K_2 T_{n-1}) + \cdots + c_{n-k}(K_1 S_{n-k} + K_2 T_{n-k}) = 0.$$

Torej je $U_n = K_1 S_n + K_2 T_n$ rešitev rekurzije (12). ∎

Če je $a_n = r^n$, potem iz rekurzivne relacije (12) dobimo

$$c_n r^n + c_{n-1} r^{n-1} + \cdots + c_{n-k} r^{n-k} = 0.$$

Seveda lahko zadnjo vrstico delimo z r^{n-k} in dobimo

$$c_n r^k + c_{n-1} r^{k-1} + \cdots + c_{n-k} = 0. \tag{13}$$

To lahko predstavimo kot iskanje ničel polinoma k-te stopnje spremenljivke r. Iz te kratke izpeljave je razvidno, da je vsaka ničla tega polinoma povezana s kako rešitvijo rekuzivne relacije (12). Tako naj bo recimo r_1 rešitev (13) in velja

$$c_n r_1^k + c_{n-1} r_1^{k-1} + \cdots + c_{n-k} = 0.$$

Kar lahko pomnožimo nazaj z r_1^{n-k} in dobimo

$$c_n r_1^n + c_{n-1} r_1^{n-1} + \cdots + c_{n-k} r_1^{n-k} = 0$$

in je $S_n = r_1^n$ rešitev (12). Po izreku 4.1 je rešitev tudi $U_n = K_1 r_1^n$, če recimo izberemo $K_2 = 0$.

Zgornja izpeljava upravičuje vpeljavo naslednje terminologije. Polinomu

$$p_k(r) = c_n r^k + c_{n-1} r^{k-1} + \cdots + c_{n-k}$$

rečemo **karakteristični polinom** rekurzivne relacije (12). Kot smo videli, so ničle karakterističnega polinoma tesno povezane z rešitvami rekurzije (12). Tako zaradi izreka 4.1 velja naslednji rezultat.

Izrek 4.2 *Če so $r_1, r_2, \ldots, r_\ell$ različne ničle karakterističnega polinoma rekurzivne relacije (12), potem je*

$$a_n = K_1 r_1^n + K_2 r_2^n + \cdots + K_\ell r_\ell^n$$

rešitev rekurzivne relacije (12) za poljubne $K_1, K_2, \ldots, K_\ell \in \mathbb{R}$.

Zgled 4.6 *Poiščimo splošni člen rekurzivno podanega geometrijskega zaporedja $a_n = \frac{1}{2} a_{n-1}$ z začetno nalogo $a_0 = 1$. Najprej ga preoblikujemo in dobimo $a_n - \frac{1}{2} a_{n-1} = 0$. Tako je karakteristični polinom enak $p_1(r) = r - \frac{1}{2}$ in njegova edina ničla je $r_1 = \frac{1}{2}$. Splošna rešitev je tako $a_n = K_1 \left(\frac{1}{2}\right)^n = K_1 2^{-n}$. Ob upoštevanju začetne naloge dobimo $1 = K_1 2^{-0}$, iz česar takoj sledi, da je $K_1 = 1$. Rešitev začetne naloge je torej $a_n = 2^{-n}$.*

Zgled 4.7 *Poiščimo splošni člen Fibonaccijevega zaporedja iz zgleda 4.3, ki je podano z rekurzivno relacijo*

$$f_n - f_{n-1} - f_{n-2} = 0,\ n \geq 3,\ f_1 = f_2 = 1.$$

Ponovno poiščemo ničle karakterističnega polinoma, ki je $p_2(r) = r^2 - r - 1$. *Ničli sta*

$$r_1 = \frac{1+\sqrt{5}}{2} \text{ in } r_2 = \frac{1-\sqrt{5}}{2}.$$

Po izreku 4.2 velja

$$f_n = K_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + K_2 \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Določiti moramo še konstanti K_1 *in* K_2. *Ob upoštevanju začetnih pogojev* $f_1 = f_2 = 1$ *dobimo*

$$\begin{aligned} K_1 \left(\frac{1+\sqrt{5}}{2}\right) + K_2 \left(\frac{1-\sqrt{5}}{2}\right) &= 1 \\ K_1 \left(\frac{1+\sqrt{5}}{2}\right)^2 + K_2 \left(\frac{1-\sqrt{5}}{2}\right)^2 &= 1. \end{aligned}$$

Če drugo vrstico kvadriramo in nato obe pomnožimo z dva, dobimo

$$\begin{aligned} (1+\sqrt{5})K_1 + (1-\sqrt{5})K_2 &= 2 \\ (3+\sqrt{5})K_1 + (3-\sqrt{5})K_2 &= 2. \end{aligned}$$

Sedaj od druge vrstice odštejemo prvo in dobimo $2K_1 + 2K_2 = 0$, *oziroma* $K_1 = -K_2$. *To vstavimo v eno od zgornjih vrstic, recimo v prvo, in dobimo* $(1+\sqrt{5}-1+\sqrt{5})K_1 = 2$, *oziroma* $K_1 = \frac{1}{\sqrt{5}} = \frac{\sqrt{5}}{5}$. *Seveda je* $K_2 = -\frac{\sqrt{5}}{5}$ *in rešitev začetne naloge je*

$$f_n = \frac{\sqrt{5}}{5} \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{\sqrt{5}}{5} \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Omenimo še, da kljub večkratni pojavi $\sqrt{5}$ *v rešitvi, le ta vedno poraja naravno število pri vsakem* $n \in \mathbb{N}$, *ker je to Fibonaccijevo zaporedje.*

Med ničlami polinoma so lahko tudi kompleksna števila in rešitev predstavljena v izreku 4.2 velja tudi zanje. Ker pa nas zanimajo predvsem realne rekurzivne relacije, nas čudi kompleksna rešitev le-te. Tako je na mestu vprašanje, ali se lahko kompleksnim številom, ki nastopajo v rešitvi, kako izognemo? Odgovor je pozitiven, vendar se je potrebno spomniti nekaj dejstev o kompleksnih številih.

Naj bo $r_1 = x + iy$ kompleksna ničla karakterističnega polinoma rekurzivne relacije (12). Seveda je tudi $r_2 = x - iy$ ničla istega karakterističnega polinoma, saj kompleksne ničle vedno nastopajo v konjungiranih parih. Zaradi izpeljave pred izrekom 4.2, lahko pričakujemo v rešitvi tudi

$$K_1 r_1^n + K_2 r_2^n.$$

Torej rešitev vsebuje binoma $(x + iy)^n$ in $(x - iy)^n$. Iz izreka 3.9 vemo, da potenca binoma nima elegantnega zapisa. Temu se lahko izognemo, saj lahko kompleksna števila predstavimo tudi drugače in sicer v polarni obliki. Polarni koordinati kompleksnega števila r_1 sta r in φ, kjer r predstavlja razdaljo med r_1 in številom $z = 0$ v kompleksni ravnini, φ pa je kot (v radianih!) od pozitivnega dela realne osi do poltraka od $z = 0$ skozi r_1. Ob tem je kot pozitiven, če vrtimo v nasprotni smeri urnega kazalca, in negativen, če vrtimo v smeri urnega kazalca. Glej sliko 6 za lažje razumevanje. Iz pravokotnega trikotnika s slike 6 ni težko videti, da lahko realno in imaginarno koordinato izrazimo s polarnima na naslednji način

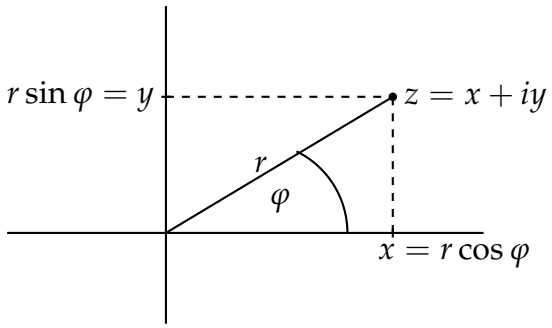
$$x = r\cos\varphi \text{ in } y = r\sin\varphi.$$

Obratno lahko tudi polarni koordinati izrazimo z realno in imaginarno koordinato in velja

$$r = \sqrt{x^2 + y^2} \text{ in } \tan\varphi = \frac{y}{x}.$$

Tako lahko predstavimo kompleksni števili r_1 in r_2 v polarni obliki

$$r_1 = r(\cos\varphi + i\sin\varphi) \text{ in } r_2 = r(\cos\varphi - i\sin\varphi).$$



Slika 6: Kartezične in polarne koordinate kompleksnega števila z.

Ob tem dodajmo, da če je kot od r_1 enak φ, potem je kot od r_2 enak $-\varphi$. Potenciranje kompleksnih števil v polarni obliki je v nasprotju s kartezično obliko razmeroma elegantno z uporabo Moivrovega[11] obrazca

$$r_1^n = (r(\cos\varphi + i\sin\varphi))^n = r^n(\cos(n\varphi) + i\sin(n\varphi)).$$

11 Abraham de Moivre (1667-1754) je bil francoski matematik, ki je najbolj znan po omenjenem obrazcu in po delu v verjetnostni teoriji.

Podobno je

$$r_2^n = (r(\cos\varphi - i\sin\varphi))^n = r^n(\cos(n\varphi) - i\sin(n\varphi)).$$

V rešitvi rekurzije (12) lahko sedaj zapišemo

$$\begin{aligned} K_1 r_1^n + K_2 r_2^n &= K_1 r^n(\cos(n\varphi) + i\sin(n\varphi)) + K_2 r^n(\cos(n\varphi) - i\sin(n\varphi)) \\ &= r^n((K_1 + K_2)\cos(n\varphi) + i(K_1 - K_2)\sin(n\varphi)) \\ &= r^n(C_1\cos(n\varphi) + C_2\sin(n\varphi)), \end{aligned}$$

kjer velja zveza $C_1 = K + K_2$ in $C_2 = i(K_1 - K_2)$. Opazimo lahko tudi, da v tem zapisu ni kompleksnih števil, saj bomo iz realne začetne naloge dobili tudi realni števili C_1 in C_2. Povzamimo to razpravo v izreku.

Izrek 4.3 *Če sta $r_1 = r(\cos\varphi + i\sin\varphi)$ in $r_2 = r(\cos\varphi - i\sin\varphi)$ kompleksni ničli karakterističnega polinoma rekurzivne relacije (12), potem lahko del rešitve rekurzivne relacije (12) zapišemo kot*

$$a_n = r^n(C_1\cos(n\varphi) + C_2\sin(n\varphi))$$

za poljubna $C_1, C_2 \in \mathbb{R}$.

Zgled 4.8 *Poiščimo splošni člen rekurzivne relacije $a_n - 2a_{n-1} - 2a_{n-2} = 0$ z začetno nalogo $a_1 = 1$ in $a_2 = 2$. Najprej zapišemo karakteristični polinom, ki je $p_2(r) = r^2 - 2r - 2$ in določimo njegovi ničli $r_1 = 1 + i$ in $r_2 = 1 - i$. Tako lahko določimo $r = \sqrt{2}$ in $\tan\varphi = 1$, oziroma $\varphi = \frac{\pi}{4}$. Po izreku 4.3 je splošna rešitev $a_n = \left(\sqrt{2}\right)^n (C_1\cos\frac{\pi n}{4} + C_2\sin\frac{\pi n}{4})$. S pomočjo začetne naloge določimo še konstanti C_2 in C_2:*

$$\begin{aligned} 1 &= \sqrt{2}(C_1\cos\frac{\pi}{4} + C_2\sin\frac{\pi}{4}), \\ 2 &= \left(\sqrt{2}\right)^2(C_1\cos\frac{2\pi}{4} + C_2\sin\frac{2\pi}{4}). \end{aligned}$$

Iz druge vrstice takoj sledi, da je $C_2 = 1$. Ko to upoštevamo v prvi vrstici, dobimo $C_1 = 0$. Tako je rešitev začetne naloge

$$a_n = 2^{n/2}\sin\frac{\pi n}{4}.$$

Zgled 4.9 *Poiščimo splošni člen rekurzivne relacije $D_n - bD_{n-1} + b^2D_{n-2} = 0$, $b \in \mathbb{R}$, z začetno nalogo $D_1 = b$ in $D_2 = 0$. Ponovno začnemo s karakterističnim polinomom, ki je $p_2(r) = r^2 - br + b^2$ in določimo njegovi ničli $r_1 = \frac{b}{2}(1 + i\sqrt{3})$ in $r_2 = \frac{b}{2}(1 - i\sqrt{3})$. Določimo polarni koordinati za r_1, ki sta $r = b$ in $\tan\varphi = \sqrt{3}$, oziroma $\varphi = \frac{\pi}{3}$. Po izreku 4.3 je splošna rešitev $D_n = b^n(C_1\cos\frac{\pi n}{3} + C_2\sin\frac{\pi n}{3})$. S pomočjo začetne naloge določimo še konstanti C_2 in C_2:*

$$\begin{aligned} b &= b(C_1\cos\frac{\pi}{3} + C_2\sin\frac{\pi}{3}), \\ 0 &= b^2(C_1\cos\frac{2\pi}{3} + C_2\sin\frac{2\pi}{3}). \end{aligned}$$

Prvo vrstico delimo z b, drugo pa z b^2, nakar ju seštejemo in dobimo $C_2 = \frac{1}{\sqrt{3}}$. *Če ju odštejemo, potem dobimo* $C_1 = 1$. *Tako je rešitev začetne naloge*

$$a_n = b^n(\cos\frac{\pi n}{3} + \frac{1}{\sqrt{3}}\sin\frac{\pi n}{3}).$$

V izreku 4.2 imamo predstavljeno celotno rešitev le, ko so vse ničle karakterističnega polinoma enostavne, oziroma prve stopnje. Seveda se je potrebno vprašati, kaj se zgodi, če je r_1 ničla stopnje $\ell > 1$ karakterističnega polinoma rekurzivne relacije (12). Karakteristični polinom lahko potem zapišemo v obliki

$$p_k(r) = (r - r_1)^\ell q_{k-\ell}(r), \tag{14}$$

kjer je $q_{k-\ell}(r)$ polinom stopnje $k - \ell$. Ker je r_1 ničla ℓ-te stopnje karakterističnega polinoma, lahko uporabimo Binomski izrek in dobimo naslednjo zvezo

$$(r - r_1)^\ell = \sum_{i=0}^{\ell} \binom{\ell}{i} r^{\ell-i} r_1^i = 0. \tag{15}$$

Preden si ogledamo splošen primer, se najprej omejimo na rekurzivno relacijo

$$a_{n+2} - 2r_1 a_{n+1} + r_1^2 a_n = 0, \tag{16}$$

s karakterističnim polinomom

$$p_k(r) = (r - r_1)^2.$$

Po izreku 4.2 je $a_n = K_1 r_1^n$ del rešitve rekurzije (16). Pokažimo, da je tudi $a_n = n r_1^n$ del rešitve rekurzivne relacije (16), ki jo zapišemo v obliki $a_{n+2} = 2r_1 a_{n+1} - r_1^2 a_n$. To storimo z matematično indukcijo na n. Za bazo naj bo $n = 1$ in velja

$$\begin{aligned} a_{1+2} &= 2r_1 a_{1+1} - r_1^2 a_1 \\ &= 2r_1 \cdot 2r_1^2 - r_1^2 \cdot 1 r_1 \\ &= 3r_1^3 = (1+2) r_1^{(1+2)}. \end{aligned}$$

Tako je baza izpolnjena in predpostavimo, da je $n > 1$. Sedaj imamo $a_n = n r_1^n$ in $a_{n+1} = (n+1) r_1^{n+1}$ in računamo

$$\begin{aligned} a_{n+2} &= 2r_1 a_{n+1} - r_1^2 a_n \\ &= 2r_1 (n+1) r_1^{n+1} - r_1^2 n r_1^n \\ &= r_1^{n+2}(2n + 2 - n) \\ &= (n+2) r_1^{n+2}, \end{aligned}$$

s čimer je pokazan tudi indukcijski korak. Pokazali smo, da je $a_n = n r_1^n$ ena rešitev. Vemo že, da je tudi $a_n = K_1 r_1^n$ rešitev po izreku 4.2. Oboje lahko združimo po izreku 4.1 in dobimo splošno rešitev

$$a_n = K_1 r_1^n + K_2 n r_1^n = r_1^n (K_1 + K_2 n).$$

Ne glede na to kakšen je $q_{k-2}(r)$, lahko s preprosto manipulacijo rekurzivne relacije (12) uvidimo, da se lahko omejimo zgolj na del karakterističnega polinoma, ki zadeva našo ničlo r_1:

$$(r - r_1)^2 = r^2 - 2r_1 r + r_1^2.$$

Kadar je r_1 ničla karakterističnega polinoma reda ℓ, velja naslednji izrek, ki ga navajamo brez dokaza, saj le-ta presega nivo tega učbenika.

Izrek 4.4 *Če je $r_1 = r_2 = \cdots = r_\ell$ ničla karakterističnega polinoma ℓ-te stopnje rekurzivne relacije (12), potem lahko del splošne rešiteve rekurzivne relacije (12) zapišemo kot*

$$a_n = r_1^n(C_1 + C_2 n + \cdots + C_\ell n^{\ell-1}).$$

Zgled 4.10 *Poiščimo splošni člen rekurzivne relacije $a_{n+2} - 4a_{n+1} + 4a_n = 0$ z začetno nalogo $a_0 = 3$ in $a_1 = 5$. Najprej zapišemo karakteristični polinom, ki je $p_2(r) = r^2 - 4r + 4 = (r-2)^2$. Kot vidimo je $r_1 = r_2 = 2$, kar je ničla druge stopnje. Po izreku 4.4 je splošna rešitev $a_n = 2^n(C_1 + C_2 n)$. S pomočjo začetne naloge določimo še konstanti C_1 in C_2:*

$$\begin{aligned} 3 &= C_1 + C_2 \cdot 0, \\ 5 &= 2(C_1 + C_2 \cdot 1). \end{aligned}$$

Prva vrstica nam pove, da je $C_1 = 3$, medtem ko iz druge dobimo $C_2 = -\frac{1}{2}$. Ko to upoštevamo v splošni rešitvi, dobimo rešitev začetne naloge

$$a_n = 2^n(3 - \frac{n}{2}).$$

Zgled 4.11 *Rešimo začetno nalogo $b_0 = 0$ in $b_1 = 1$ rekurzivne relacije $b_n - b_{n-1} + \frac{1}{4}b_{n-2} = 0$. Kot običajno začnemo s karakterističnim polinom, ki je $p_2(r) = r^2 - r + \frac{1}{4} = (r - \frac{1}{2})^2$. Seveda sta njegovi ničli enaki $r_1 = r_2 = \frac{1}{2}$ in zato druge stopnje. Po izreku 4.4 je splošna rešitev $b_n = \left(\frac{1}{2}\right)^n (C_1 + C_2 n) = 2^{-n}(C_1 + C_2 n)$. S pomočjo začetne naloge določimo še konstanti C_1 in C_2:*

$$\begin{aligned} 0 &= C_1 + C_2 \cdot 0, \\ 1 &= 2^{-1}(C_1 + C_2 \cdot 1). \end{aligned}$$

Prva vrstica nam določi $C_1 = 0$, druga vrstica pa zagotovi $C_2 = 2$. Tako je rešitev začetne naloge

$$b_n = 2^{-n} \cdot 2n = \frac{n}{2^{n-1}}.$$

4.3 NEHOMOGENE LINEARNE REKURZIVNE RELACIJE

Naj bo

$$c_n a_n + c_{n-1} a_{n-1} + \cdots + c_{n-k} a_{n-k} = f(n), c_n, c_{n-1}, \ldots, c_{n-k} \in \mathbb{R}, \qquad (17)$$

nehomogena linearna rekurzivna relacija reda k s konstantnimi koeficienti. To seveda pomeni, da je $f(n) \neq 0$. Kot bomo videli v nadaljevanju, bomo znali poiskati rešitev rekurzije (17) le v primeru, ko je funkcija $f(n)$ dovolj lepa. Bolj natančno, če je $f(n)$ polinom, ali eksponentna funkcija a^n, ali sinusna funkcija $\sin(\varphi n)$, ali kosinusna funkcija $\cos(\varphi n)$, ali vsote, oziroma produkti omenjenih funkcij. Z $a_n^{(p)}$ bomo označili rešitev rekurzije (17), ki ji rečemo **partikularna** ali **delna** rešitev.

Homogeni rekurzivni relaciji reda k s konstantnimi koeficienti

$$c_n a_n + c_{n-1} a_{n-1} + \cdots + c_{n-k} a_{n-k} = 0$$

rečemo **pripadajoča homogena rekurzivna relacija** rekurzije (17). Njeno rešitev označimo z $a_n^{(h)}$ in ji rečemo **rešitev pripadajoče homogene rekurzivne relacije** ali kar **homogena rešitev**. Kot smo videli v prejšnjem razdelku, znamo $a_n^{(h)}$ vedno poiskati, če le znamo določiti ničle karakterističnega polinoma. Pokažimo najprej, da je tudi vsota homogene in partikularne rešitve rešitev za (17).

Izrek 4.5 *Rešitev (17) je* $a_n = a_n^{(h)} + a_n^{(p)}$.

Dokaz. Vstavimo $a_n^{(h)} + a_n^{(p)}$ v (17) in računajmo:

$$\begin{aligned} c_n(a_n^{(h)} + a_n^{(p)}) + c_{n-1}(a_{n-1}^{(h)} + a_{n-1}^{(p)}) + \cdots + c_{n-k}(a_{n-k}^{(h)} + a_{n-k}^{(p)}) = \\ = (c_n a_n^{(h)} + c_{n-1} a_{n-1}^{(h)} + \cdots + c_{n-k} a_{n-k}^{(h)}) + \\ + (c_n a_n^{(p)} + c_{n-1} a_{n-1}^{(p)} + \cdots + c_{n-k} a_{n-k}^{(p)} = \\ = 0 + f(n) = f(n). \end{aligned}$$

Tako vidimo, da je $a_n^{(h)} + a_n^{(p)}$ rešitev (17). ∎

Rešitvi $a_n = a_n^{(h)} + a_n^{(p)}$ rečemo **splošna rešitev**, ki vsebuje še nekaj konstant v homogeni rešitvi $a_n^{(h)}$. Le-te lahko določimo, če je podana začetna naloga, ki jo sestavljajo vrednosti k začetnih členov zaporedja a_n. Tako splošna rešitev predstavlja družino zaporedij, medtem ko je rešitev začetne naloge eno samo zaporedje.

Torej moramo poiskati partikularno rešitev $a_n^{(p)}$, saj $a_n^{(h)}$ že znamo izračunati. Ni težko videti, da mora biti $a_n^{(p)}$ podobne oblike kot $f(n)$, saj moramo na levi strani (17) dobiti enako funkcijo kot na desni strani (17), ki je enaka $f(n)$. Zato $a_n^{(p)}$ iščemo s pomočjo nastavka, ki je zelo podoben $f(n)$. Pravzaprav uporabimo v $a_n^{(p)}$ funkcijo enakega tipa kot je $f(n)$, le da koeficiente polinoma iz $f(n)$ pustimo še nedoločene. Zaradi tega rečemo tej metodi **metoda nedoločenih koeficientov**. Omenimo še, da v vsaki funkciji $f(n)$ nastopa polinom. Tudi če ga ne prepoznamo takoj, lahko rečemo, da je funkcija $f(n)$ pomnožena z 1, kar je polinom stopnje nič.

Kadar je funkcija $f(n) = f_1(n) + f_2(n) + \cdots + f_k(n)$, kjer so $f_1(n), f_2(n), \ldots, f_k(n)$ funkcije različnih tipov, potem lahko poiščemo nastavke $a_n^{(p_1)}, a_n^{(p_2)}, \ldots, a_n^{(p_k)}$ ločeno. To pomeni, da je $a_n^{(p_i)}$, za vsak $i \in [k]$, funkcija enakega tipa kot $f_i(n)$, le da so koeficienti iz polinoma, ki nastopa v $a_n^{(p_i)}$, še nedoločeni koeficienti. Razjasnimo si kaj mislimo s funkcijo različnega tipa na naslednjem zgledu.

Zgled 4.12 *Podane so funkcije*

$$\begin{aligned} f(n) &= n^2 + 1 - n \cdot 2^n + \sin\frac{\pi n}{2} - n\cos\frac{\pi n}{2} + n^2 \sin\frac{\pi n}{3}, \\ g(n) &= n^2 \cdot 2^n + 5 \cdot 3^n + 3^n \sin\frac{\pi n}{2} - \cos\frac{\pi n}{2}, \\ h(n) &= 3n + n \cdot 2^n - \sin\frac{\pi n}{4} + 2^n(\sin\frac{\pi n}{6} - n\cos\frac{\pi n}{3}). \end{aligned}$$

Funkcijo $f(n)$ lahko razbijemo na naslednji način

$$\begin{aligned} f(n) &= (n^2+1) + (-n \cdot 2^n) + (\sin\frac{\pi n}{2} - n\cos\frac{\pi n}{2}) + (n^2 \sin\frac{\pi n}{3}) \\ &= f_1(n) + f_2(n) + f_3(n) + f_4(n), \end{aligned}$$

kjer velja $f_1(n) = n^2 + 1$, $f_2(n) = -n \cdot 2^n$, $f_3(n) = \sin\frac{\pi n}{2} - n\cos\frac{\pi n}{2}$ in $f_4(n) = n^2 \sin\frac{\pi n}{3}$. Vidimo lahko, da je $f_1(n)$ kvadratni polinom iz $f(n)$ in $f_2(n)$ je linearni polinom pomnožen z eksponentno funkcijo. V $f_3(n)$ sta oba, tako $\sin\frac{\pi n}{2}$ kot tudi $\cos\frac{\pi n}{2}$, ki je povrhu še pomnožen z linearnim polinomom. Oba sta istega tipa, ker imata enak kot $\varphi = \frac{\pi}{2}$, saj moramo za izračun recimo a_{n-1} uporabiti adicijski izrek, v njem pa sinus (oziroma kosinus) prehaja v oba, tako sinus kot kosinus. Od $f_3(n)$ pa moramo ločiti $\sin\frac{\pi n}{3}$ (pomnožen s kvadratnim polinomom), saj je kot sedaj $\frac{\pi}{3}$, kar je različno od $\frac{\pi}{2}$.

Podobno naredimo s funkcijo $g(n)$:

$$\begin{aligned} g(n) &= (n^2 \cdot 2^n) + (5 \cdot 3^n) + (3^n \sin\frac{\pi n}{2}) + (-\cos\frac{\pi n}{2}) \\ &= g_1(n) + g_2(n) + g_3(n) + g_4(n), \end{aligned}$$

kjer velja $g_1(n) = n^2 \cdot 2^n$, $g_2(n) = 5 \cdot 3^n$, $g_3(n) = 3^n \sin\frac{\pi n}{2}$ in $g_4(n) = -\cos\frac{\pi n}{2}$. Ob tem sta $g_1(n)$ in $g_2(n)$ različnega tipa, saj imata v eksponentnih funkcijah različno

osnovo. Omenimo, da polinom različne stopnje pri $g_1(n)$ in $g_2(n)$ ni razlog za različni tip funkcije. Funkciji $g_3(n)$ in $g_4(n)$ imata sedaj v sinusu in v kosinusu enak kot $\varphi = \frac{\pi}{2}$, vendar sta različnega tipa, ker imamo pri $g_3(n)$ še eksponentno funkcijo 3^n, ki je v $g_4(n)$ ni.

Za konec zgleda razbijmo še funkcijo $h(n)$, kar poteka takole

$$\begin{aligned} h(n) &= (3n) + (n \cdot 2^n) + (-\sin\frac{\pi n}{4}) + (2^n \sin\frac{\pi n}{6}) + (-n2^n \cos\frac{\pi n}{3}) \\ &= h_1(n) + h_2(n) + h_3(n) + h_4(n) + h_5(n). \end{aligned}$$

Ob tem velja $h_1(n) = 3n$, $h_2(n) = n \cdot 2^n$, $h_3(n) = -\sin\frac{\pi n}{4}$, $h_4(n) = 2^n \sin\frac{\pi n}{6}$ in $h_5(n) = -n2^n \cos\frac{\pi n}{3}$. Ob tem sta $h_1(n)$ in $h_2(n)$ različnega tipa, četudi imata obe linearni polinom, vendar ima $h_2(n)$ eksponentno funkcijo, ki je $h_1(n)$ nima. Funkcije $h_3(n)$, $h_4(n)$ in $h_5(n)$ so različnega tipa, saj imajo različne kote, čeprav imata ob tem $h_4(n)$ in $h_5(n)$ enako eksponentno funkcijo.

Ko imamo nastavek $a_n^{(p)}$, lahko zapišemo tudi ostale člene $a_{n-1}, \ldots, a_{n-k}$ in vse vstavimo v (17). Nato z nekaj enostavnega računanja določimo neznane koeficiente s primerjanjem koeficientov na levi in desni strani rekurzije (17). Oglejmo si kako omenjena metoda deluje na primeru Hanoiskega stolpa in na primeru algoritma Bubble sort.

Zgled 4.13 *V zgledu 4.4 smo predstavili problem Hanoiskega stolpa in zanj izpeljali rekurzijo*

$$h_n - 2h_{n-1} = 1, h_1 = 1. \tag{18}$$

Poiskati moramo $h_n^{(h)}$ in $h_n^{(p)}$. Lotimo se najprej pripadajoče homogene rekurzije

$$h_n - 2h_{n-1} = 0.$$

Njen karakteristični polinom je $p_1(r) = r - 2$ in edina njegova ničla je $r = 2$. Tako je homogena rešitev $h_n^{(h)} = K \cdot 2^n$.

Partikularno rešitev iščemo z nastavkom, ki je, kot omenjeno, enakega tipa kot $f(n) = 1$. Tokrat je funkcija polinom stopnje nič in tudi nastavek bo zato polinom stopnje nič s še neznanim koeficientom. Skratka, $h_n^{(p)} = A$, kjer je A konstanta. Seveda je potem $h_{n-1}^{(p)} = A$ in oboje vstavimo v (18) in dobimo

$$A - 2A = 1.$$

Seveda velja $A = -1$ in partikularna rešitev je tako $h_n^{(p)} = -1$.

Skupna rešitev je vsota homogene in partikularne rešitve in je

$$h_n = K \cdot 2^n - 1.$$

Rešimo še začetno nalogo $h_1 = 1$ *in dobimo*

$$1 = K \cdot 2^1 - 1,$$

oziroma $K = 1$. *Tako je rešitev začetne naloge Hanoiskega stolpa*

$$h_n = 2^n - 1.$$

Zgled 4.14 *Poiščimo sedaj rešitev za število potrebnih operacij, da se izvede algoritem Bubble sort, ki smo ga uspeli opisati v zgledu 4.5 z rekurzijo*

$$b_{n+1} - b_n = n, b_1 = 0. \tag{19}$$

Ponovno se lotimo pripadajoče homogene rekurzije

$$b_{n+1} - b_n = 0,$$

ki ima karakteristični polinom $p_1(r) = r - 1$ *in je* $r = 1$ *njegova edina ničla. Tako je* $b_n^{(h)} = K \cdot 1^n = K$.

Nadaljujmo z iskanjem partikularne rešitve. Tokrat je $f(n) = n$ *polinom prve stopnje in pričakujemo lahko, da bo tudi* $b_n^{(p)}$ *polinom prve stopnje, torej* $b_n^{(p)} = An + B$. *Seveda je*

$$b_{n+1}^{(p)} = A(n+1) + B = An + A + B.$$

Vstavimo $b_{n+1}^{(p)}$ *in* $b_n^{(p)}$ *v (19) in dobimo*

$$An + A + B - An - B = n.$$

Ko uredimo, dobimo $A = n$, *kar je protislovje, saj konstanta* A *ne more biti enaka* $n \in \mathbb{N}$, *ki je neodvisna spremenljivka. Kaj je šlo narobe?*

Če primerjamo $b_n^{(h)}$ *in nastavek za* $b_n^{(p)}$, *opazimo, da v obeh nastopa konstanta. Torej smo v nastavek za* $b_n^{(p)}$ *(nehote) vključili homogeno rešitev. Seveda je rezultat konstante iz partikularne rešitve enak* 0, *saj je le-ta konstanta tudi homogena rešitev. V tem primeru nastavek za partikularno rešitev pomnožimo še z* n, *da se izognemo homogeni rešitvi v nastavku za partikularno rešitev. Tako je pravi nastavek sedaj*

$$b_n^{(p)} = (An + B)n = An^2 + Bn$$

in

$$b_{n+1}^{(p)} = A(n+1)^2 + B(n+1) = An^2 + 2An + A + Bn + B.$$

Oba vstavimo v (19) in dobimo

$$An^2 + 2An + A + Bn + B - An^2 - Bn = n.$$

Uredimo in dobimo

$$2An + A + B = n.$$

Tako imamo enačaj med polinomoma prve stopnje in če želimo, da je enačaj izpolnjen, morata biti istoležna koeficienta enaka. Torej enačimo koeficiente iz desne in leve strani pri n^1 in pri n^0 in dobimo sistem:

$$\begin{aligned} n^1 = n &\ : \ 2A = 1, \\ n^0 = 1 &\ : \ A + B = 0. \end{aligned}$$

Seveda je rešitev tega sistema $A = \frac{1}{2}$ in $B = -A = -\frac{1}{2}$. Tako je $b_n^{(p)} = \frac{1}{2}n^2 - \frac{1}{2}n$. Sedaj lahko zapišemo splošno rešitev

$$b_n = b_n^{(h)} + b_n^{(p)} = K + \frac{1}{2}n^2 - \frac{1}{2}n.$$

Poiščimo še začetno nalogo za $b_1 = 0$:

$$0 = b_1 = K + \frac{1}{2} \cdot 1 - \frac{1}{2} \cdot 1 = K.$$

Tako je rešitev začetne naloge kar

$$b_n = \frac{1}{2}(n^2 - n).$$

Povzemimo zaplet iz zadnjega zgleda. Funkcija $f(n)$ je linearni polinom in splošni linearni polinom, to je nastavek za partikularno rešitev, vsebuje tudi konstanto. Hkrati je konstanta homogena rešitev. V takšnem primeru nastavek dodatno pomnožimo z najmanjšo potenco n^k, tako da nastavek za partikularno rešitev več ne vsebuje homogene rešitve ali kakšnega njenega dela.

Omenimo še kako postopamo s kotnima funkcijama $\sin(\varphi n)$, oziroma $\cos(\varphi n)$. Vedno kadar v $f(n)$ nastopa le ena izmed njiju, postavimo v partikularni nastavek obe na simetrični način. Razlog za to je v računanju $a_{n+i}^{(p)}$ za nek fiksen i. Oba $\sin(\varphi(n+i))$, oziroma $\cos(\varphi(n+i))$, vedno problikujemo z adicijskima izrekoma, v katerih se vsak $\sin(\varphi(n+i))$ kot tudi $\cos(\varphi(n+i))$ izražata z obema $\sin(\varphi n)$ in $\cos(\varphi n)$. Zato morata biti tudi v nastavku zastopana oba.

Ločimo dva tipa nastavkov, ki jih lahko uspešno rešimo z metodo nedoločenih koeficientov: s kotnimi funkcijami in brez njih. Oglejmo si najprej slednje, saj so enostavnejši. Naj bo $f(n) = p_\ell(n)a^n$, kjer je $p_\ell(n)$ nek podan polinom ℓ-te stopnje in a^n eksponentna funkcija za nek fiksen $a \in \mathbb{R} - \{0\}$. Za to funkcijo je nastavek $a_n^{(p)}$ sestavljen iz eksponentne funkcije a^n in polinoma $t_\ell(n) = A_\ell n^\ell + A_{\ell-1}n^{\ell-1} + \cdots + A_1 n + A_0$ stopnje ℓ, v katerem še ne poznamo njegovih koeficientov $A_\ell, A_{\ell-1}, \ldots, A_1, A_0$. Vprašajmo se še, kdaj je tak nastavek lahko tudi del homogene rešitve $a_n^{(h)}$? To se zgodi, če je a ničla karakterističnega polinoma. V tem primeru nastopa A_0a^n v $a_n^{(p)}$ in C_1a^n v $a_n^{(h)}$, kar je enak tip funkcije, ki se razlikujeta le v konstantah A_0 in C_1. Zato moramo $a_n^{(p)}$ pomnožiti

z ustrezno, to je najmanjšo, potenco n^k, da v $a_n^{(p)}$ ne najdemo več homogene rešitve ali njenega dela. Še več, če je a ničla stopnje k karakterističnega polinoma, potem moramo pomnožiti $a_n^{(p)}$ vsaj z n^k, da dobimo $a^n A_0 n^k$ in konstanten člen polinoma $t_\ell(n)$ več ne nastopa v homogeni rešitvi $a_n^{(h)}$, ki vsebuje del $a^n(C_1 + C_2 n + \cdots + C_\ell n^{k-1})$. Seveda je potenca n^k tudi dovolj in dobili smo merilo, s kakšno potenco n^k je potrebno pomnožiti partikularni nastavek, da se izognemo homogeni rešitvi. Tu je $k \in \mathbb{N}_0$ število ničel karakterističnega polinoma, ki so enake a. Najpogosteje je $k = 0$, kar pomeni, da a ni ničla karakterističnega polinoma. Tako imamo

$$f(n) = p_m(n)a^n \Rightarrow a_n^{(p)} = n^k t_m(n)a^n, \tag{20}$$

kjer je $t_m(n)$ polinom stopnje m z neznanimi koeficienti in k je število ničel karakterističnega polinoma, ki so enaka a.

Preden se lotimo zgleda, si poglejmo še, kakšne možnosti nam nudi (20). Če je $a = 1$, potem imamo $f(n) = p_\ell(n)1^n = p_\ell(n)$, kar je polinom ℓ-te stopnje. Nastavek je sedaj $a_n^{(p)} = n^k t_\ell(n)$, kjer je k število ničel karakterističnega polinoma enakih 1.

Naslednji poseben primer je $\ell = 0$ in je $p_\ell(n)$ polinom 0-te stopnje, oziroma konstanta A_0. V tem primeru je $f(n) = A_0 a^n$ kar eksponentna funkcija pomnožena s konstanto. Nastavek je sedaj v skladu z (20) kar $a_n^{(p)} = n^k B_0 a^n$, kjer je B_0 še neznana konstanta in je k število ničel karakterističnega polinoma enakih a. Zgodi se lahko tudi, da je $A_0 = 1$ in imamo $f(n) = a^n$. Nastavek je sedaj enak kot prej $a_n^{(p)} = n^k B_0 a^n$, saj je tudi $A_0 = 1$ polinom 0-te stopnje.

Zgled 4.15 *Rekurziji $a_{n+2} - 10a_{n+1} + 21a_n = f(n)$ določimo nastavke, glede na različne funkcije $f(n)$ iz spodnje tabele. Najprej določimo njeno pripadajočo homogeno rešitev, saj bomo z njeno pomočjo lažje določali potenco n^k, s katero je potrebno pomnožiti nastavek. Ničli karakterističnega polinoma sta $r_1 = 3$ in $r_2 = 7$, kar je razvidno iz*

$$r^2 - 10r + 21 = (r-3)(r-7) = 0.$$

Tako je $a_n^{(h)} = C_1 3^n + C_2 7^n$. Oglejmo si funkcije in nastavke v naslednji tabeli

$f(n)$	$a_n^{(p)}$
5	A_0
$n^2 - 8$	$A_1 n^2 + A_2 n + A_3$
$5 \cdot 2^n$	$A_4 2^n$
$4 \cdot 7^n$	$A_5 n 7^n$
$n3^n$	$(A_6 n + A_7) n 3^n$
$5 \cdot 3^n - 2^n$	$A_8 n 3^n + A_9 2^n$
$\sin \frac{\pi n}{2}$	$A_{10} \sin \frac{\pi n}{2} + A_{11} \cos \frac{\pi n}{2}$
$3^n \sin \frac{\pi n}{2}$	$3^n \left(A_{12} \sin \frac{\pi n}{2} + A_{13} \cos \frac{\pi n}{2} \right)$.

V prvi vrstici imamo v $f(n)$ polinom 0-te stopnje pomnožen z eksponentno funkcijo 1^n. Ker 1 ni ničla karakterističnega polinoma, je sedaj $n^k = n^0 = 1$ in nastavek je neznan polinom 0-te stopnje, ki smo ga označili z A_0. V drugi vrstici imamo kvadratni polinom v $f(n)$. Podobno kot v prvi vrstici je nastavek kar kvadratni polinom z neznanimi koeficienti. Omenimo še, da četudi v $f(n)$ ni linearnega člena, le-ta nastopa v nastavku $a_n^{(p)}$.

Naslednje tri vrstice prinašajo eksponentne funkcije pomnožene s polinomom. Tako je tudi nastavek enaka eksponentna funkcija pomnožena s polinomom iste stopnje s še neznanimi koeficienti. Posebej poudarimo, da je v četrti vrstici $a = 7$ enojna ničla karakterističnega polinoma, zato moramo nastavek pomnožiti z $n^k = n^1 = n$. Podobno nastavek pomnožimo z n tudi v peti vrstici, saj je tudi $a = 3$ enojna ničla karakterističnega polinoma.

Funkcija iz šeste vrstice prinaša vsoto dveh eksponentnih funkcij pomnoženih s konstantnima polinomoma. V takšnem primeru lahko zapišemo nastavek za vsako posebej in nastavka nato seštejemo. Za $a = 3$ moramo ponovno dodatno pomnožiti z $n^k = n^1 = n$, saj je 3 enojna ničla karakterističnega polinoma.

Zadnji dve vrstici prinašata kotni funkciji. Kot omenjeno, moramo k $\sin(\varphi n)$ v funkciji v nastavku dodati tudi $\cos(\varphi n)$. Dodajmo še, da imamo v zadnji vrstici v $f(n)$ tudi $a^n = 3^n$, kjer je 3 ničla karakterističnega polinoma. Tukaj nastavka ne množimo dodatno z n, saj je v $f(n)$ eksponentna funkcija 3^n pomnožena s $\sin(\varphi n)$, kar ne nastopa v homogeni rešitvi.

Zgled 4.16 *Rekurziji $a_{n+2} - 4a_{n+1} + 4a_n = f(n)$ določimo nastavke, glede na različne funkcije $f(n)$ iz spodnje tabele. Ponovno določimo njeno pripadajočo homogeno rešitev. Tokrat je $r_1 = r_2 = 2$ dvojna ničla karakterističnega polinoma, saj je*

$$r^2 - 4r + 4 = (r-2)^2 = 0.$$

Tako je $a_n^{(h)} = 2^n(C_1 + C_2 n)$. Oglejmo si funkcije in nastavke v spodnji tabeli

$f(n)$	$a_n^{(p)}$
$3n^2 - 6$	$B_0n^2 + B_1n + B_2$
$n7^n$	$(B_3n + B_4)7^n$
$3 \cdot (-2)^n$	$B_5(-2)^n$
$3 \cdot 2^n$	$n^2B_6 2^n$
$(n+2)2^n$	$n^2(B_7n + B_8)2^n$
$n^2 2^n$	$n^2(B_9n^2 + B_{10}n + B_{11})2^n$
$n \sin \frac{\pi n}{2} + 3 \cos \frac{\pi n}{2}$	$(B_{12}n + B_{13}) \sin \frac{\pi n}{2} + (B_{14}n + B_{15}) \cos \frac{\pi n}{2}$
$2^n \sin \frac{\pi n}{3}$	$2^n \left(B_{16} \sin \frac{\pi n}{3} + B_{17} \cos \frac{\pi n}{3}\right)$.

Najprej omenimo, da kadar bomo sedaj dodatno množili s potenco n^k, bomo množili z n^2, saj je 2 dvojna ničla karakterističnega polinoma. V prvi vrstici imamo v $f(n)$ kvadratni polinom pomnožen z $a^n = 1^n = 1$, ki je tudi v nastavku, le da z neznanimi koeficienti. Seveda ga ne množimo z n^2, saj $a = 1$ ni ničla karakterističnega polinoma.

V naslednjih petih vrsticah imamo eksponentne funkcije pomnožene s polinomom. Tako je tudi nastavek ista eksponentna funkcija pomnožena s polinomom enake stopnje s še neznanimi koeficienti. Razlika je, da v drugi in tretji vrstici ne množimo z n^2, saj $a = 7$, oziroma $a = -2$ nista ničli karakterističnega polinoma. Temu ni tako v sledečih treh vrsticah, kjer je $a = 2$ hkrati tudi dvojna ničla karakterističnega polinoma in zato nastavek množimo z n^2.

Funkciji v zadnjih dveh vrsticah prinašata funkciji $\sin \frac{\pi n}{2}$, *oziroma* $\cos \frac{\pi n}{2}$. *V predzadnji vrstici je tako* $\sin \frac{\pi n}{2}$ *pomnožen z linearnim polinomom,* $\cos \frac{\pi n}{2}$ *pa s kontantnim polinomom. Ne glede na to imamo v nastaku obakrat linearen polinom, to je polinom večje stopnje iz funkcije $f(n)$. Omenimo še, da v zadnji vrstici ponovno ne množimo z n^2, saj $2^n \sin \frac{\pi n}{3}$ ni del homogene rešitve, četudi je 2 (dvojna) ničla karakterističnega polinoma.*

Razmislimo sedaj, kako je, ko v funkciji $f(n)$ najdemo funkciji sinus, oziroma kosinus in je

$$f(n) = a^n(p_m(n)\sin(\varphi n) + q_\ell(n)\cos(\varphi n)).$$

Seveda nas polinoma v zgornjem zapisu ne zanimata, saj ju nadomestimo s polinomoma s še neznanimi koeficienti. Tako se lahko posvetimo le delu $f_1(n) = a^n(\sin(\varphi n) + \cos(\varphi n))$. Funkciji sinus in kosinus najdemo v homogeni rešitvi le, če imamo kompleksne ničle v karakterističnem polinomu. Spomnimo se, da po izreku 4.3 za konjungirani kompleksni ničli karakterističnega polinoma $r_1 = x + iy$ in $r_2 = x - iy$, dobimo del homogene rešitve v obliki $a_n^{(h)} = r^n(C_1\cos(\varphi_1 n) + C_2\sin(\varphi_1 n))$, kjer velja povezava $r = \sqrt{x^2+y^2}$ in $\tan\varphi_1 = \frac{y}{x}$. Če torej želimo enake funkcije v $f_1(n)$ in v $a_n^{(h)}$, potem mora veljati $a = r$ in $\varphi = \varphi_1$. Tako partikularni nastavek množimo s potenco n^k le v primeru, ko je $r_1 = x_1 + iy_1$ za $x_1 = a\cos\varphi$ in $y_1 = a\sin\varphi$ ničla karakterističnega polinoma k-te stopnje. (Seveda je potem tudi $r_1 = x_1 - iy_1$ ničla karakterističnega polinoma k-te stopnje, saj kompleksne ničle vedno nastopajo v konjungiranih parih.) Tako imamo

$$f(n) = a^n(p_m(n)\sin(\varphi n) + q_\ell(n)\cos(\varphi n)) \Rightarrow$$

$$\Rightarrow a_n^{(p)} = n^k a^n(s_M(n)\sin(\varphi n) + t_M(n)\cos(\varphi n)), \tag{21}$$

kjer je $r = x + iy$ za $x = a\cos\varphi$ in $y = a\sin\varphi$ ničla karakterističnega polinoma k-te stopnje. Razen tega sta $s_M(n)$ in $t_M(n)$ polinoma z neznanimi koeficienti stopnje $M = \max\{m, \ell\}$. Opazimo lahko, da tudi (20) sledi iz (21), če je le $\varphi = 0$ ali $\varphi = \pi$.

Posebni primeri v (21) nastopijo, če je $a = 1$ ali $p_m(n) = 0$ ali $q_\ell(n) = 0$. V teh primerih nimamo eksponentne funkcije, oziroma $\sin(\varphi n)$, oziroma $\cos(\varphi n)$. Posebej poudarimo, da v primeru $p_m(n) = 0$ v funkciji $f(n)$ ni sinusa, le-ta pa nastopi v nastavku a_n^p in podobno, če v $f(n)$ ni $\cos(\varphi n)$, kar pomeni $q_\ell(n) = 0$, le-ta kasneje nastopi v nastavku a_n^p. Seveda nima smisla, da sta oba $p_m(n)$ in $q_\ell(n)$ enaka 0, saj je v tem primeru $f(n) = 0$ in imamo homogeno rekurzivno relacijo.

Zgled 4.17 *Določimo nastavke za rekurzijo $a_{n+2} + a_n = f(n)$ glede na funkcije $f(n)$, ki jih najdemo v sledeči tabeli. Najprej homogena rašitev. Tokrat je imamo*

$$r^2 + 1 = (r - i)(r + i) = 0$$

in ničli karakterističnega polinoma sta tokrat kompleksni števili $r_1 = i$ in $r_2 = -i$. Seveda je njuna oddaljenost od števila 0 enaka $r = 1$, medtem ko je kot $\varphi = \frac{\pi}{2}$. Tako je $a_n^{(h)} = 1^n(C_1 \cos \frac{\pi n}{2} + C_2 \sin \frac{\pi n}{2}) = C_1 \cos \frac{\pi n}{2} + C_2 \sin \frac{\pi n}{2}$. Oglejmo si funkcije in nastavke v spodnji tabeli

$f(n)$	$a_n^{(p)}$
$n - 3$	$D_0 n + D_1$
$n2^n$	$(D_2 n + D_3)2^n$
$3 \cdot (-2)^n + n$	$D_4(-2)^n + D_5 n + D_6$
$\sin \frac{\pi n}{3}$	$D_7 \sin \frac{\pi n}{3} + D_8 \cos \frac{\pi n}{3}$
$\sin \frac{\pi n}{3} + \cos \frac{\pi n}{2}$	$D_9 \sin \frac{\pi n}{3} + D_{10} \cos \frac{\pi n}{3} + n \left(D_{11} \sin \frac{\pi n}{2} + D_{12} \cos \frac{\pi n}{2} \right)$
$2^n \cos \frac{\pi n}{2}$	$2^n \left(D_{13} \sin \frac{\pi n}{2} + D_{14} \cos \frac{\pi n}{2} \right)$.

V prvi vrstici imamo v $f(n)$ linearni polinom pomnožen z $a^n = 1^n = 1$, ki je tudi v nastavku, le da z neznanimi koeficienti. V drugi vrstici je linearni polinom pomnožen z eksponentno funkcijo, česar tudi ne najdemo v homogeni rešitvi. Zato je tudi nastavek enak linearnemu polinomu $(D_2 n + D_3)$ (z neznanimi koeficienti) pomnoženemu z enako eksponentno funkcijo 2^n.

V tretji vrstici imamo vsoto dveh funkcij (eksponentne in linearnega polinoma), ki ju ponovno ni najti v homogeni rešitvi. Tako je tudi nastavek sestavljen iz vsote eksponentne funkcije $(-2)^n$ pomnožene s konstanto D_4, ki predstavlja polinom 0-te stopnje (z neznanim koeficientom) in linearne funkcije $D_5 n + D_6$.

V zadnjih treh vrsticah nastopajo razne variante povezane s funkcijama sinus in kosinus. Ob tem lahko opazimo, da funkciji $\sin \frac{\pi n}{3}$ in $2^n \cos \frac{\pi n}{2}$ ne nastopata v homogeni rešitvi in zato v tem primeru ni potrebno množiti s potenco $n^k = n$. To moramo storiti zgolj v delu predzadnje vrstice za del funkcije $\cos \frac{\pi n}{2}$. Tako je v četrti vrstici nastavek kar $a_n^{(p)} = D_7 \sin \frac{\pi n}{3} + D_8 \cos \frac{\pi n}{3}$, saj moramo sinus in kosinus pomnožiti s polinomoma 0-te stopnje. V predzadnji vrstici imamo vsoto dveh funkcij $\sin \frac{\pi n}{3}$ in $\cos \frac{\pi n}{2}$, ki se razlikujeta, saj je kot $\frac{\pi}{3}$ različen od kota $\frac{\pi}{2}$. Tako je nastavek sestavljen iz dveh delov. Prvi $D_9 \sin \frac{\pi n}{3} + D_{10} \cos \frac{\pi n}{3}$ pripada $\sin \frac{\pi n}{3}$, medtem ko $\cos \frac{\pi n}{2}$ nastopa tudi v homogenem

delu in moramo množiti tudi z n in imamo $n\left(D_{11}\sin\frac{\pi n}{2}+D_{12}\cos\frac{\pi n}{2}\right)$. V zadnji vrstici nastavka ne množimo z n, saj $2^n\sin\frac{\pi n}{2}$ ni del homogene rešitve, četudi $\sin\frac{\pi n}{2}$ najdemo v homogeni rešitvi, a tam ni pomnožen z 2^n in sta to različni funkciji.

Strnimo formalen zapis iz (20) in (21) v naslednji tabeli.

$f(n)$	$a_n^{(p)}$
$p_m(n)a^n$	$n^k t_m(n)a^n$
$a^n(p_m(n)\sin(\varphi n)+q_\ell(n)\cos(\varphi n))$	$n^k a^n(s_M(n)\sin(\varphi n)+t_M(n)\cos(\varphi n))$.

(22)

V prvem stolpcu imamo funkcijo iz rekurzivne relacije, medtem ko je v drugem stolpcu zapisan nastavek. V drugem stolpcu nastopajo nekateri simboli, ki potrebujejo dodatno razlago.

V drugi vrstici je k število ničel karakterističnega polinoma enakih a, ki je najpogosteje kar nič. Po drugi strani je $t_m(n)$ polinom stopnje m, ki vsebuje še nezane koeficiente $A, B, \ldots$ (metoda se imenuje metoda neznanih koeficientov).

Tudi v zadnji vrstici sta $s_M(n)$ in $t_M(n)$ polinoma stopnje $M=\max\{m,\ell\}$ s še neznanimi koeficienti $A, B, \ldots$ (metoda se imenuje metoda neznanih koeficientov). Ob tem je k tokrat število ničel karakterističnega polinoma enakih $x+iy$, kjer sta $x=a\cos\varphi$ in $y=a\sin\varphi$.

Omenimo še posebne primere zgornje tabele. Če je $a=1$, potem imamo v srednji vrstici $f(n)=p_m(n)$. Tako nam srednja vrstica pokriva tudi primer, ko je $f(n)$ polinom m-te stopnje. V tem primeru je nastavek kar $n^k t_m(n)$, torej neznan polinom m-te stopnje pomnožen z n^k, kjer število k predstavlja kolikokratna ničla karakterističnega polinoma je 1 (najpogosteje je kar $k=0$).

Lahko se zgodi tudi, da je $m=0$ in je $p_0(n)$ polinom 0-te stopnje, kar je konstanta. V tem primeru je tudi $t_m(n)=t_0(n)$ kar neznana konstanta, recimo A. Če je povrh vsega omenjena konstanta 1, potem je $f(n)=a^n$. Nastavek je v tem primeru še vedno enak $a_n^{(p)}=An^k a^n$, kjer je A neznan polinom $t_0(n)$ 0-te stopnje in k je število ničel karakterističnega polinoma enakih a.

Oglejmo si še posebne primere zadnje vrstice. Eden izmed polinomov $p_m(n)$ in $q_\ell(n)$ je lahko enak nič. V tem primeru v funkciji $f(n)$ nastopa ali zgolj sinus ali zgolj kosinus. Ne glede na to imamo v nastavku $a_n^{(p)}$ oba, tako sinus kot tudi kosinus, saj je pred njima neznani polinom stopnje $M=\max\{m,\ell\}$. Podobno kot za srednjo vrstico je lahko kateri izmed polinomov $p_m(n)$ in $q_\ell(n)$ kar konstanta, v najbolj izpostavljenem primeru celo 1. Tedaj je ustrezna stopnja $m=0$ ali $\ell=0$ in stopnja polinomov v nastavku M je definirana kot maksimum.

Če je $a = 1$, potem je tudi $a^n = 1^n = 1$, ki je v izrazu seveda ne pišemo. Tedaj je $f(n) = p_m(n)\sin(\varphi n) + q_\ell(n)\cos(\varphi n)$ in nadaljujemo z nastavkom kjer je $a = 1$.

Opazimo lahko tudi, da v primeru $\varphi = 0$ dobimo

$$f(n) = a^n(p_m(n)\sin 0 + q_\ell(n)\cos 0) = q_\ell(n)a^n,$$

kar predstavlja funkcijo iz srednje vrstice.

Če je funkcija $f(n) = f_1(n) + f_2(n)$ vsota dveh različnih funkcij $f_1(n)$ in $f_2(n)$, kjer sta obe $f_1(n)$ in $f_2(n)$ iz tabele, potem lahko določimo dva različna nastavka $a_n^{(p1)}$ za $f_1(n)$ in $a_n^{(p2)}$ za $f_2(n)$ in nadaljujemo z vsakim nastavkom posebej.

Za konec omenimo še, da če pomnožimo dve različni funkciji iz tabele, potem z nekaj računske spretnosti[12] ponovno dobimo funkcijo iz tabele.

Ko je nastavek $a_n^{(p)}$ določen, potem lahko zapišemo tudi $a_{n-1}^{(p)}, a_{n-2}^{(p)}, \ldots, a_{n-k}^{(p)}$ iz (17). Vse te člene nato vstavimo v (17) in zapis uredimo. Na levi in na desni strani dobimo polinome pomnožene s funkcijami istega tipa, recimo a^n ali $a^n\sin(\varphi n)$ ali $a^n\cos(\varphi n)$. Če želimo, da enačaj velja, potem morajo biti polinom ob neki funkciji na levi enak polinomu ob tej isti funkciji na desni in ju zato enačimo. (Včasih je polinom ob funkciji na desni preprosto enak 0.) Nadalje so polinomi enaki, kadar so koeficienti ob istih potencah enaki. Ko enačimo le-te, dobimo sistem linearnih enačb, v katerih nastopajo še neznani koeficienti polinomov iz nastavka. Z rešitvijo omenjenega linearnega sistema, dobimo rešitev $a_n^{(p)}$ in splošna rešitev (17) je po izreku 4.5 enaka

$$a_n = a_n^{(h)} + a_n^{(p)}.$$

Splošna rešitev (17) vsebuje k konstant, ki nastopajo v $a_n^{(h)}$. To pomeni, da imamo neskončno mnogo rešitev za (17). Kadar je podanih k začetnih členov zaporedja $a_1, a_2, \ldots, a_n$, jim rečemo **začetna naloga** za (17). Z njimi lahko določimo konstante v splošni rešitvi a_n in dobimo eno samo rešitev za (17), ki ji rečemo rešitev podane začetne naloge. Poudarimo posebej, da začetne naloge v primeru nehomogene rekurzije ne rešujemo le na homogeni rešitvi $a_n^{(h)}$, ampak moramo poiskati najprej splošno rešitev in šele nato iščemo rešitev začetne naloge. Oglejmo si celoten postopek na nekaterih zgledih.

Zgled 4.18 *Poiščimo splošno rešitev nehomogene rekurzije*

$$a_{n+2} + 3a_{n+1} + 2a_n = 3^n + n. \tag{23}$$

Najprej poiščemo homogeno rešitev $a_n^{(h)}$ za

$$a_{n+2} + 3a_{n+1} + 2a_n = 0.$$

12 Množenje polinomov, množenje eksponentnih funkcij ter množenje sinusov in kosinusov. Slednje lahko prevedemo na vsoto sinusov in kosinusov.

Za to potrebujemo karakteristični polinom

$$r^2 + 3r + 2 = 0,$$

oziroma njegove ničle, ki ju razberemo iz

$$(r+2)(r+1) = 0.$$

Imamo dve realni ničli $r_1 = -2$ *in* $r_2 = -1$ *prve stopnje, zato po izreku 4.2 velja*

$$a_n^h = C_1(-2)^n + C_2(-1)^n, C_1, C_2 \in \mathbb{R}.$$

Za partikularno rešitev potrebujemo nastavek $a_n^{(p)}$ *za funkcijo* $f(n) = 3^n + n$. *To funkcijo lahko razdelimo na dva dela in sicer* $f_1(n) = 3^n$ *in* $f_2(n) = n$. *Za vsako izmed njiju poiščemo nastavek iz tabele (22). Nastavek za* $f_1(n)$ *je*

$$a_n^{(p1)} = A \cdot 3^n,$$

saj je $a = 3$, $p_m(n) = 1$ *in* $k = 0$, *saj 3 ni ničla karakterističnega polinoma. Zapišimo še* $a_{n+1}^{(p1)}$ *in* $a_{n+2}^{(p1)}$:

$$\begin{aligned} a_{n+1}^{(p1)} &= A \cdot 3^{n+1} = 3A \cdot 3^n, \\ a_{n+2}^{(p1)} &= A \cdot 3^{n+2} = 9A \cdot 3^n. \end{aligned}$$

Vstavimo vse tri v (23) in uredimo

$$\begin{aligned} 9A \cdot 3^n + 3 \cdot 3A \cdot 3^n + 2A \cdot 3^n &= 3^n = f_1(n) \\ (9A + 9A + 2A)3^n &= 3^n \\ 20A \cdot 3^n &= 1 \cdot 3^n. \end{aligned}$$

Seveda je $20A = 1$, *oziroma* $A = \frac{1}{20}$. *Tako je* $a_n^{(p1)} = \frac{1}{20}3^n$.

Nastavek za $f_2(n)$ *je*

$$a_n^{(p2)} = Bn + C,$$

saj je $a = 1$, $p_m(n) = n$ *in* $k = 0$, *saj 1 ni ničla karakterističnega polinoma. Zapišimo še* $a_{n+1}^{(p2)}$ *in* $a_{n+2}^{(p2)}$:

$$\begin{aligned} a_{n+1}^{(p2)} &= B(n+1) + C = Bn + B + C, \\ a_{n+2}^{(p2)} &= B(n+2) + C = Bn + 2B + C. \end{aligned}$$

Vstavimo vse tri v (23) in uredimo

$$\begin{aligned} (Bn + 2B + C) + 3(Bn + B + C) + 2(Bn + C) &= n = f_2(n) \\ 6Bn + (5B + 6C) \cdot 1 &= n + 0 \cdot 1 \\ 6Bn + (5B + 6C) \cdot n^0 &= n + 0 \cdot n^0. \end{aligned}$$

Dobili smo enakost med dvema linearnima polinomoma, zato morajo biti enaki koeficientih ob enakih potencah. Tako je

$$\begin{aligned} n &: 6B = 1, \\ n^0 &: 5B + 6C = 0. \end{aligned}$$

Po prvi enačbi je $B = \frac{1}{6}$ *in iz druge dobimo* $C = -\frac{5}{6}B = -\frac{5}{36}$. *Tako je* $a_n^{(p2)} = \frac{n}{6} - \frac{5}{36}$ *in splošna rešitev je*

$$\begin{aligned} a_n &= a_n^{(h)} + a_n^{(p1)} + a_n^{(p2)}, \\ a_n &= C_1(-2)^n + C_2(-1)^n + \frac{1}{20}3^n + \frac{n}{6} - \frac{5}{36},\ C_1, C_2 \in \mathbb{R}. \end{aligned}$$

Zgled 4.19 *Poiščimo začetno nalogo* $a_0 = a_1 = 1$ *nehomogene rekurzije*

$$a_{n+2} - 2a_{n+1} + a_n = \sin\frac{\pi n}{2}.$$

Najprej poiščemo homogeno rešitev $a_n^{(h)}$ *za*

$$a_{n+2} - 2a_{n+1} + a_n = 0.$$

Za to potrebujemo karakteristični polinom

$$r^2 - 2r + 1 = 0,$$

oziroma njegove ničle, ki ju razberemo iz

$$(r-1)^2 = 0.$$

Imamo eno realno ničlo $r_1 = 1$ *druge stopnje, zato po izreku 4.4 velja*

$$a_n^{(h)} = 1^n(C_1 + C_2 n) = C_1 + C_2 n, C_1, C_2 \in \mathbb{R}.$$

Za partikularno rešitev potrebujemo nastavek $a_n^{(p)}$ *za funkcijo* $f(n) = \sin\frac{\pi n}{2}$. *Nastavek zanjo je*

$$a_n^{(p)} = A \cdot \sin\frac{\pi n}{2} + B\cos\frac{\pi n}{2},$$

saj je $a = 1$, $p_m(n) = 1$, $q_\ell(n) = 0$, $M = 1$, $\varphi = \frac{\pi}{2}$, $x = a\cos\varphi = 0$, $y = a\sin\varphi = 1$ *in* $k = 0$, *saj* $i = x + iy$ *ni ničla karakterističnega polinoma. Zapišimo še* $a_{n+1}^{(p1)}$ *in* $a_{n+2}^{(p1)}$:

$$\begin{aligned} a_{n+1}^{(p)} &= A\sin\frac{\pi(n+1)}{2} + B\cos\frac{\pi(n+1)}{2} = A\sin\left(\frac{\pi n}{2} + \frac{\pi}{2}\right) + B\cos\left(\frac{\pi n}{2} + \frac{\pi}{2}\right), \\ a_{n+2}^{(p)} &= A\sin\frac{\pi(n+2)}{2} + B\cos\frac{\pi(n+2)}{2} = A\sin\left(\frac{\pi n}{2} + \pi\right) + B\cos\left(\frac{\pi n}{2} + \pi\right). \end{aligned}$$

Uporabimo najprej adicijska izreka za sinus in kosinus in uredimo za

$$\begin{aligned} a_{n+1}^{(p)} &= A\left(\sin\frac{\pi n}{2}\cos\frac{\pi}{2}+\sin\frac{\pi}{2}\cos\frac{\pi n}{2}\right)+B\left(\cos\frac{\pi n}{2}\cos\frac{\pi}{2}-\sin\frac{\pi n}{2}\sin\frac{\pi}{2}\right)= \\ &= A\cos\frac{\pi n}{2}-B\sin\frac{\pi n}{2} \\ a_{n+2}^{(p)} &= A\left(\sin\frac{\pi n}{2}\cos\pi+\sin\pi\cos\frac{\pi n}{2}\right)+B\left(\cos\frac{\pi n}{2}\cos\pi-\sin\frac{\pi n}{2}\sin\pi\right)= \\ &= -A\sin\frac{\pi n}{2}-B\cos\frac{\pi n}{2}. \end{aligned}$$

Vstavimo $a_{n+2}^{(p)}$, $a_{n+1}^{(p)}$ *in* $a_n^{(p)}$ *v (4.19) in uredimo, tako da izpostavimo* $\sin\frac{\pi n}{2}$ *ter* $\cos\frac{\pi n}{2}$ *kjer je mogoče:*

$$\begin{aligned} -A\sin\frac{\pi n}{2}-B\cos\frac{\pi n}{2}-2\left(A\cos\frac{\pi n}{2}-B\sin\frac{\pi n}{2}\right)+A\cdot\sin\frac{\pi n}{2}+B\cos\frac{\pi n}{2} & \\ =\sin\frac{\pi n}{2}=f(n) & \\ (-A+2B+A)\sin\frac{\pi n}{2}+(-B-2A+B)\cos\frac{\pi n}{2}=\sin\frac{\pi n}{2} & \\ 2B\sin\frac{\pi n}{2}-2A\cos\frac{\pi n}{2}=1\cdot\sin\frac{\pi n}{2}+0\cdot\cos\frac{\pi n}{2}. & \end{aligned}$$

V zadnji vrstici je enačaj izpolnjen natanko tedaj, ko je polinom na levi pri sinusu enak polinomu na desni pri sinusu in podobno mora biti polinom na levi pri kosinusu enak polinomu na desni pri kosinusu. Tako imamo

$$2B=1 \text{ in } 2A=0,$$

iz česar sledi $B=\frac{1}{2}$ *in* $A=0$. *Torej je*

$$a_n^{(p)}=\frac{1}{2}\cos\frac{\pi n}{2},$$

kar porodi splošno rešitev

$$a_n=a_n^{(h)}+a_n^{(p)}=C_1+C_2n+\frac{1}{2}\cos\frac{\pi n}{2}.$$

Rešiti moramo začetno nalogo $a_0=a_1=1$, *za katero dobimo linearen sistem*

$$\begin{aligned} 1 &= a_0=C_1+C_2\cdot 0+\frac{1}{2}\cos\frac{\pi\cdot 0}{2}=C_1+\frac{1}{2}, \\ 1 &= a_1=C_1+C_2\cdot 1+\frac{1}{2}\cos\frac{\pi\cdot 1}{2}=C_1+C_2. \end{aligned}$$

Zlahka uvidimo, da je njegova rešitev $C_1=C_2=\frac{1}{2}$, *s čimer je rešitev začetne naloge zaporedje*

$$a_n=\frac{1}{2}+\frac{1}{2}n+\frac{1}{2}\cos\frac{\pi n}{2}.$$

4.4 NEKATERE (NE)REŠENE NALOGE

Vaja 4.1 *Poiščite rešitve podanih homogenih rekurzivnih relacij.*

(A) $a_{n+2} - 2a_{n+1} + 2a_n = 0$, $a_0 = 0$, $a_1 = 1$.

(B) $b_n - 6b_{n-1} + 9b_{n-2} = 0$, $b_0 = -2$, $b_1 = 3$.

(C) $c_{n+1} - 9c_n - 10c_{n-1} = 0$, $c_0 = \frac{1}{2}$, $c_1 = -\frac{1}{2}$.

(D) $d_{n+2} - 8d_{n-1} = 0$, $d_0 = 3, d_1 = 2$, $d_2 = 4$.

(E) $e_{n+3} - 8e_{n+1} - 9e_{n-1} = 0$.

Rešitev. *Homogeno rešitev $a_n^{(h)}$ dobimo tako, da zapišemo karakteristični polinom, poiščemo njegove ničle in nato zapišemo rešitev glede na izreke 4.1, 4.2, 4.3 in 4.4.*

Ničle karakterističnega polinoma prve rekurzije dobimo iz $r^2 - 2r + 2 = 0$ in nista realni. Enaki sta $r_1 = 1 + i$ in $r_2 = 1 - i$. Zapišimo r_1 v polarni obliki. Seveda je $r = \sqrt{1^2 + 1^2} = \sqrt{2}$ in $\tan\varphi = 1$, kar pomeni, da je $\varphi = \frac{\pi}{4}$, saj se kompleksno število nahaja v prvem kvadrantu. Tako imamo v polarni obliki $r_1 = \sqrt{2}(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})$ in $r_2 = \sqrt{2}(\cos\frac{\pi}{4} - i\sin\frac{\pi}{4})$. Splošna rešitev pa je po izreku 4.3

$$a_n = \left(\sqrt{2}\right)^n \left(K_1 \cos\frac{\pi n}{4} + K_2 \sin\frac{\pi n}{4}\right).$$

Z začetno nalogo $a_0 = 0$, $a_1 = 1$ določimo še K_1 in K_2. Iz $a_0 = 0$ dobimo $K_1 = 0$ in iz $a_1 = 1$ dobimo $\sqrt{2}\left(\frac{\sqrt{2}}{2}K_1 + \frac{\sqrt{2}}{2}K_2\right) = 1$, oziroma $K_2 = 1$. Tako je rešitev začetne naloge prve rekurzije $a_n = \left(\sqrt{2}\right)^n \sin\frac{\pi n}{4}$.

Ničle karakterističnega polinoma druge rekurzije dobimo iz $r^2 - 6r + 9 = (r-3)^2 = 0$ in imamo dvojno ničlo $r_1 = r_2 = 3$. Po izreku 4.4 je splošna rešitev $b_n = (K_1 + K_2 n)3^n$. Iz začetne naloge $b_0 = -2$ in $b_1 = 3$ dobimo $K_1 = -2$ in $(K_1 + K_2)3 = 3$. Tako je še $K_2 = 3$, s čimer je rešitev začetne naloge $b_n = (-2 + 3n)3^n$.

Ničle karakterističnega polinoma zadnje rekurzije dobimo iz

$$r^4 - 8r^2 - 9 = (r^2 - 9)(r^2 + 1) = (r-3)(r+3)(r-i)(r+i) = 0.$$

Torej imamo štiri enojne ničle $r_1 = 3$, $r_2 = -3$, $r_3 = i$ in $r_4 = -i$. Za $r_3 = i$ je oddaljenost od koordinatnega izhodišča enak $r = 1$, medtem ko je kot $\varphi = \frac{\pi}{2}$. Z uporabo izrekov 4.1, 4.2, 4.3 zapišemo iskano splošno rešitev

$$e_n = K_1 3^n + K_2(-3)^n + K_3 \cos\frac{\pi n}{2} + K_4 \sin\frac{\pi n}{2}.$$

Preostali rešitvi sta $c_n = \frac{1}{2}(-1)^n$ in $d_n = 2^n\left(\frac{4}{3} + \frac{\sqrt{3}}{3}\sin\frac{2\pi n}{3} + \frac{5}{3}\cos\frac{2\pi n}{3}\right)$.

Vaja 4.2 *Poiščite splošne rešitve podanih rekurzivnih relacij.*

(A) $a_{n+2} + 4a_{n+1} + 3a_n = 2n - 3\sin\frac{\pi n}{2}$.

(B) $b_{n+2} - 7b_{n+1} + 10b_n = 3\sin\frac{\pi n}{3} - 2\cos\frac{\pi n}{3}$.

(C) $c_{n+1} - 2c_n - 3c_{n-1} = \cos\frac{\pi n}{4} + 5 \cdot 3^n$.

(D) $d_{n+1} - 3d_n + 2d_{n-1} = n^2 + 4 \cdot 2^n$.

Rešitev. *Splošno rešitev vedno poiščemo tako, da najprej poiščemo homogeno rešitev in nato še partikularno rešitev. Homogeno rešitev $a_n^{(h)}$ dobimo tako, da zapišemo karakteristični polinom, poiščemo njegove ničle in nato zapišemo rešitev glede na izreke 4.1, 4.2, 4.3 in 4.4. Partikularno rešitev $a_n^{(p)}$ iščamo z nastavkom, ki je odvisen od funkcije $f(n)$ in homogene rešitve. Splošna rešitev je nato $a_n = a_n^{(h)} + a_n^{(p)}$.*

V primeru (a) poiščemo ničli karakterističnega polinoma $r^2 + 4r + 3 = (r+3)(r+1) = 0$, ki sta $r_1 = -3$ in $r_2 = -1$. Tako je $a_n^{(h)} = C_1(-3)^n + C_2(-1)^n$ po izreku 4.2. Funkcijo $f(n) = 2n - 3\sin\frac{\pi n}{2}$ je smiselno razdeliti na dva dela $f_1(n) = 2n$ ter $f_2(n) = -3\sin\frac{\pi n}{2}$. Tako je nastavek $a_n^{(p_1)} = An + B$, saj je $f_1(n)$ tudi linearna funkcija in $a = 1$ ni ničla karakterističnega polinoma. Seveda sta

$$\begin{aligned} a_{n+1}^{(p_1)} &= A(n+1) + B = An + A + B, \\ a_{n+2}^{(p_1)} &= A(n+2) + B = An + 2A + B. \end{aligned}$$

Vse tri vstavimo v začetno diferenčno enačbo in enačimo s $f_1(n)$:

$$An + 2A + B + 4(An + A + B) + 3(An + B) = 2n.$$

Uredimo levo stran in dobimo

$$8An + 6A + 8B = 2n,$$

kar lahko zapišemo tudi kot

$$8An^1 + (6A + 8B)n^0 = 2n^1 + 0n^0.$$

Linearna polinoma sta enaka, kadar so enaki istoležni koeficienti, to je $8A = 2$ in $6A + 8B = 0$. Tako je $A = \frac{1}{4}$ in $B = -\frac{3}{16}$ in posledično $a_n^{(p_1)} = \frac{1}{4}n + -\frac{3}{16}$.

Po drugi strani je nastavek $a_n^{(p_2)} = D\sin\frac{\pi n}{2} + E\cos\frac{\pi n}{2}$, saj karakteristični polinom nima kompleksnih ničel. Določimo še $a_{n+1}^{(p_2)}$ in $a_{n+2}^{(p_2)}$, kjer si pomagamo z adicijskima izrekoma za sinus in kosinus:

$$\begin{aligned} a_{n+1}^{(p_2)} &= D\sin\frac{\pi(n+1)}{2} + E\cos\frac{\pi(n+1)}{2} = D\sin\left(\frac{\pi n}{2} + \frac{\pi}{2}\right) + E\cos\left(\frac{\pi n}{2} + \frac{\pi}{2}\right) \\ &= D\sin\frac{\pi n}{2}\cos\frac{\pi}{2} + D\sin\frac{\pi}{2}\cos\frac{\pi n}{2} + E\cos\frac{\pi n}{2}\cos\frac{\pi}{2} - E\sin\frac{\pi n}{2}\sin\frac{\pi}{2} \\ &= D\cos\frac{\pi n}{2} - E\sin\frac{\pi n}{2} \end{aligned}$$

$$\begin{aligned} a_{n+2}^{(p_2)} &= D\sin\frac{\pi(n+2)}{2} + E\cos\frac{\pi(n+2)}{2} = D\sin\left(\frac{\pi n}{2}+\pi\right) + E\cos\left(\frac{\pi n}{2}+\pi\right) \\ &= D\sin\frac{\pi n}{2}\cos\pi + D\sin\pi\cos\frac{\pi n}{2} + E\cos\frac{\pi n}{2}\cos\pi - E\sin\frac{\pi n}{2}\sin\pi \\ &= -D\sin\frac{\pi n}{2} - E\cos\frac{\pi n}{2}. \end{aligned}$$

Ponovno vstavimo vse tri $a_n^{(p_2)}$, $a_{n+1}^{(p_2)}$ in $a_{n+2}^{(p_2)}$ v začetno diferenčno enačbo in enačimo s $f_2(n)$:

$$-D\sin\frac{\pi n}{2} - E\cos\frac{\pi n}{2} + 4\left(D\cos\frac{\pi n}{2} - E\sin\frac{\pi n}{2}\right) + 3\left(D\sin\frac{\pi n}{2} + E\cos\frac{\pi n}{2}\right) = \\ = -3\sin\frac{\pi n}{2}.$$

Levo stran razdelimo na dva dela, v prvem so vsi členi pri sinusu in v drugem vsi členi pri kosinusu:

$$(-D-4E+3D)\sin\frac{\pi n}{2} + (-E+4D+3E)\cos\frac{\pi n}{2} = -3\sin\frac{\pi n}{2} + 0\cos\frac{\pi n}{2}.$$

Opazimo lahko, da smo na desni dodali člen $0\cos\frac{\pi n}{2} = 0$, ki ničesar ne spremeni. Zgornji izraz je enak tedaj, ko so členi pri sinusu in kosinusu enaki na obeh straneh. Tako je $2D - 4E = 3$ in $2E + 4D = 0$, iz česar sledi $D = \frac{3}{10}$ in $E = -\frac{3}{5}$ in $a_n^{(p_2)} = \frac{3}{10}\sin\frac{\pi n}{2} - \frac{3}{5}\cos\frac{\pi n}{2}$. Splošna rešitev je sedaj

$$a_n = C_1(-3)^n + C_2(-1)^n + \frac{n}{4} - \frac{3}{16} + \frac{3}{10}\sin\frac{\pi n}{2} - \frac{3}{5}\cos\frac{\pi n}{2}.$$

Podrobneje si oglejmo še primer (d). Ničli karakterističnega polinoma dobimo iz $r^2 - 3r + 2 = (r-1)(r-2) = 0$ in sta $r_1 = 1$ ter $r_2 = 2$. Tako je $d_n^{(h)} = C_1 1^n + C_2 2^n = C_1 + C_2 2^n$. Ponovno lahko $f(n) = n^2 + 4\cdot 2^n$ razdelimo na dva dela in sicer $f_1(n) = n^2$ in $f_2(n) = 4\cdot 2^n$. Nastavek za prvi del je $d_n^{(p_1)} = n(An^2 + Bn + C) = An^3 + Bn^2 + Cn$, saj je $a = 1$ za $f_1(n)$, ki je hkrati tudi enkratna ničla karakterističnega polinoma. Zapišimo še $d_{n+1}^{(p_1)}$ in $d_{n-1}^{(p_1)}$:

$$\begin{aligned} d_{n+1}^{(p_1)} &= A(n+1)^3 + B(n+1)^2 + C(n+1) = \\ &= An^3 + 3An^2 + 3An + A + Bn^2 + 2Bn + B + Cn + C \\ d_{n-1}^{(p_1)} &= A(n-1)^3 + B(n-1)^2 + C(n-1) = \\ &= An^3 - 3An^2 + 3An - A + Bn^2 - 2Bn + B + Cn - C \end{aligned}$$

in vse vstavimo v začetno diferenčno enačbo s $f_1(n)$ na desni strani

$$\begin{aligned} n^2 = {} & An^3 + 3An^2 + 3An + A + Bn^2 + 2Bn + B + Cn + C - 3(An^3 + Bn^2 + Cn) \\ & +2(An^3 - 3An^2 + 3An - A + Bn^2 - 2Bn + B + Cn - C). \end{aligned}$$

Izraz uredimo in dobimo

$$1n^2 + 0n + 0n^0 = -3An^2 + (9A - 2B)n + (-A + 3B - C)n^0.$$

Enačaj velja, ko so istoležni koeficienti enaki, kar pomeni $-3A = 1$, $9A - 2B = 0$ *in* $-A + 3B - C = 0$. *Zlahka izračunamo* $A = -\frac{1}{3}$, $B = -\frac{3}{2}$ *in* $C = -\frac{25}{6}$ *ter dobimo*

$$d_{n+1}^{(p_1)} = -\frac{1}{3}n^3 - \frac{3}{2}n^2 - \frac{25}{6}n.$$

Za $f_2(n) = 4 \cdot 2^n$ *imamo nastavek* $d_n^{(p_2)} = nD2^n$, *saj je tudi tokrat* $a = 2$ *enkratna ničla karakterističnega polinoma. Tokrat je* $d_{n+1}^{(p_2)} = (n+1)D2^{n+1}$ *in* $d_{n-1}^{(p_2)} = (n-1)D2^{n-1}$. *Ko vstavimo nastavke v začetno diferenčno enačbo dobimo*

$$(n+1)D2^{n+1} - 3nD2^n + 2(n-1)D2^{n-1} = 4 \cdot 2^n.$$

Celoten izraz delimo z 2^n *in dobimo* $2nD + 2D - 3nD + nD - D = 4$, *oziroma* $D = 4$. *Tako je* $d_n^{(p_2)} = 4n2^n$. *Splošna rešitev je tako*

$$d_n = C_1 + C_2 2^n - \frac{1}{3}n^3 - \frac{3}{2}n^2 - \frac{25}{6}n + 4n2^n = C_1 - \frac{25}{6}n - \frac{3}{2}n^3 - \frac{1}{3}n^3 + (C_2 + 4n)2^n.$$

Za primera (b) *in* (c) *zapišimo le glavne korake brez podrobnosti. Za* (b) *poiščemo ničle karakterističnega polinoma iz* $r^2 - 7r + 10 = (r-2)(r-5) = 0$ *in imamo* $r_1 = 2$ *ter* $r_2 = 5$. *Tako je* $b_n^{(h)} = C_1 2^n + C_2 5^n$. *Nastavek za partikularno rešitev je* $b_n^{(p)} = A \sin \frac{\pi n}{3} + B \cos \frac{\pi n}{3}$. *Zapišemo* $b_{n+1}^{(p)}$, $b_{n+2}^{(p)}$, *ju uredimo z adicijskima izrekoma, vse nastavke vstavimo v začetno diferenčno enačbo in z nekaj računanja dobimo* $A = \frac{6+2\sqrt{3}}{21}$ *in* $B = \frac{3\sqrt{3}-4}{21}$. *Tako je splošna rešitev*

$$b_n = C_1 2^n + C_2 5^n + \frac{6+2\sqrt{3}}{21} \sin \frac{\pi n}{3} + \frac{3\sqrt{3}-4}{21} \cos \frac{\pi n}{3}.$$

Za (c) *poiščemo ničle karakterističnega polinoma iz* $r^2 - 2r - 3 = (r-3)(r+1) = 0$ *in imamo* $r_1 = 3$ *ter* $r_2 = -1$. *Tako je* $c_n^{(h)} = C_1 3^n + C_2(-1)^n$. *Za partikularno rešitev ponovno uporabimo dva nastavka* $c_n^{(p_1)} = A \sin \frac{\pi n}{4} + B \cos \frac{\pi n}{4}$ *in* $c_n^{(p_2)} = nD3^n$ *(tukaj je* $a = 3$ *enojna ničla karakterističnega polinoma). Zapišemo* $c_{n+1}^{(p_1)}$, $c_{n-1}^{(p_1)}$, *ju uredimo z adicijskima izrekoma, vse nastavke vstavimo v začetno diferenčno enačbo in z nekaj računanja dobimo* $A = \frac{2}{4+7\sqrt{2}}$ *in* $B = -\frac{2+\sqrt{2}}{14+4\sqrt{2}}$. *Zgodbo ponovimo s* $c_{n+1}^{(p2)}$ *in* $c_{n-1}^{(p2)}$ *(tokrat brez adicijskih izrekov) in dobimo* $D = \frac{5}{4}$. *Tako je splošna rešitev*

$$b_n = \left(C_1 + \frac{5}{4}n\right) 3^n + C_2(-1)^n + \frac{2}{4+7\sqrt{2}} \sin \frac{\pi n}{4} - \frac{2+\sqrt{2}}{14+4\sqrt{2}} \cos \frac{\pi n}{4}.$$

Vaja 4.3 *Rešite začetne naloge podanih rekurzivnih relacij.*

(A) $a_{n+2} - 6a_{n+1} + 9a_n = 3 \cdot 2^n + 7 \cdot 3^n$, $a_0 = 1$, $a_1 = 3$.

(B) $b_n + 5b_{n-1} - 6b_{n-2} = 5n + 3^n$, $b_0 = 6$, $b_1 = \frac{65}{49}$.

(C) $c_{n+2} - 8c_{n+1} + 15c_n = 3^n \sin \frac{\pi n}{2}$, $c_0 = 0$, $c_1 = 2$.

(D) $d_{n+2} + d_n = 5\cos\frac{\pi n}{2} + 2^n$, $d_0 = d_1 = 0$.

(E) $e_{n+2} - 4e_{n+1} + e_n = 3n + 2^n$, $e_0 = e_1 = 0$.

(F) $2f_{n+2} + f_{n+1} - f_n = 3n^2 + 2n + 4\sin\frac{\pi n}{3}$, $f_0 = 1$, $f_1 = -1$.

(G) $g_{n+2} + g_{n+1} - 4g_n - 4g_{n-1} = 2^n + \cos\frac{\pi n}{3}$, $g_0 = 0$, $g_1 = 1$, $g_2 = 2$.

(H) $h_{n+3} - 8h_n = 2^{n+1}n^2 + 2^n$, $h_0 = h_2 = h_4 = 0$.

(I) $i_{n+2} - 4i_n = 2 - 8n + 3^n$, $i_0 = 0$, $i_1 = 5$.

(J) $j_{n+2} + 4j_{n+1} + 4j_n = 7n^2 2^n$, $j_0 = 1$, $j_1 = 2$.

(K) $k_{n+2} - k_n = \cos\frac{\pi n}{2} + n2^n$, $k_0 = 1$, $k_1 = 1$.

Rešitev. *Podrobno bomo opisali le rešitvi za (a) in (d), krajši opis postopka bo podan za točki (b) in (c), medtem ko bomo za preostale zapisali zgolj rešitev. Za rešitev začetne naloge najprej potrebujemo splošno rešitev, v katero nato vstavimo dodatne podatke za začetno nalogo.*

V primeru (a) poiščemo ničli karakterističnega polinoma $r^2 - 6r + 9 = (r-3)^2 = 0$, ki sta $r_1 = r_2 = 3$. Tako je $a_n^{(h)} = (C_1 + C_2 n)3^n$ po izreku 4.4. Funkcijo $f(n) = 3 \cdot 2^n + 7 \cdot 3^n$ razdelimo na dva dela $f_1(n) = 3 \cdot 2^n$ ter $f_2(n) = 7 \cdot 3^n$. Tako je nastavek $a_n^{(p_1)} = A2^n$, saj $a = 2$ ni ničla karakterističnega polinoma. Seveda sta

$$\begin{aligned} a_{n+1}^{(p_1)} &= A2^{n+1} = 2A2^n, \\ a_{n+2}^{(p_1)} &= A2^{n+2} = 4A2^n. \end{aligned}$$

Vse tri vstavimo v začetno diferenčno enačbo in enačimo s $f_1(n)$:

$$4A2^n - 12A2^n + 9A2^n = 3 \cdot 2^n.$$

Uredimo levo stran, delimo z 2^n in dobimo $A = 3$. Tako je $a_n^{(p_1)} = 3 \cdot 2^n$.

Po drugi strani je nastavek $a_n^{(p_2)} = n^2 B \cdot 3^n$, saj je $a = 3$ dvojna ničla karakterističnega polinoma. Določimo še $a_{n+1}^{(p_2)}$ in $a_{n+2}^{(p_2)}$:

$$a_{n+1}^{(p_2)} = (n+1)^2 B3^{n+1} = 3^n(3Bn^2 + 6Bn + B),$$

$$a_{n+2}^{(p_2)} = (n+2)^2 B3^{n+2} = 3^n(9Bn^2 + 36Bn + 36B).$$

Ponovno vstavimo vse tri $a_n^{(p_2)}$, $a_{n+1}^{(p_2)}$ in $a_{n+2}^{(p_2)}$ v začetno diferenčno enačbo in enačimo s $f_2(n)$:

$$3^n(9Bn^2 + 36Bn + 36B) - 6 \cdot 3^n(3Bn^2 + 6Bn + B) + 9Bn^2 3^n = 7 \cdot 3^n.$$

Uredimo levo stran, delimo s 3^n *in dobimo* $30B = 7$, *oziroma* $B = \frac{7}{30}$. *Tako je* $a_n^{(p_2)} = \frac{7}{30}n^2 3^n$. *Splošna rešitev je sedaj*

$$a_n = \left(C_1 + C_2 n + \frac{7}{30}n^2\right) 3^n + 3 \cdot 2^n.$$

Sedaj uporabimo še začetno nalogo $a_0 = 1$ *in* $a_1 = 3$. *Iz* $a_0 = 1$ *dobimo* $C_1 + 3 = 1$, *oziroma* $C_1 = -2$. *Iz* $a_1 = 3$ *in ob upoštevanju* $C_1 = -2$ *dobimo* $\left(-2 + C_2 + \frac{7}{30}\right) 3 + 6 = 3$, *oziroma* $C_2 = \frac{23}{30}$. *Dobljeni konstanti* C_1 *in* C_2 *še vstavimo v splošno rešitev in rešitev začetne naloge je*

$$a_n = \left(-2 + \frac{23}{30}n + \frac{7}{30}n^2\right) 3^n + 3 \cdot 2^n.$$

Podrobneje si oglejmo še primer (d). *Ničli karakterističnega polinoma dobimo iz* $r^2 + 1 = (r - i)(r + i) = 0$ *in sta* $r_1 = i$ *ter* $r_2 = -i$. *Kompleksno število* i *ima razdaljo* $r = 1$ *od koordinatnega izhodišča in kot* $\varphi = \frac{\pi}{2}$. *Po izreku 4.3 je* $d_n^{(h)} = C_1 \sin\frac{\pi n}{2} + C_2 \cos\frac{\pi n}{2}$. *Ponovno lahko* $f(n) = 5\cos\frac{\pi n}{2} + 2^n$ *razdelimo na dva dela in sicer* $f_1(n) = 5\cos\frac{\pi n}{2}$ *in* $f_2(n) = 2^n$. *Nastavek za prvi del je* $d_n^{(p_1)} = n\left(A\sin\frac{\pi n}{2} + B\cos\frac{\pi n}{2}\right)$, *saj je* $a = i$ *enkratna ničla karakterističnega polinoma. Zapišimo še* $d_{n+2}^{(p_1)}$ *in ga uredimo:*

$$\begin{aligned}
d_{n+2}^{(p_1)} &= (n+2)\left(A\sin\frac{\pi(n+2)}{2} + B\cos\frac{\pi(n+2)}{2}\right) = \\
&= (n+2)\left(A\sin\left(\frac{\pi n}{2} + \pi\right) + B\cos\left(\frac{\pi n}{2} + \pi\right)\right) = \\
&= (n+2)\left(A\sin\frac{\pi n}{2}\cos\pi + A\sin\pi\cos\frac{\pi n}{2} + \right. \\
&\qquad \left. + B\cos\frac{\pi n}{2}\cos\pi - B\sin\frac{\pi n}{2}\sin\pi\right) = \\
&= (n+2)\left(-A\sin\frac{\pi n}{2} - B\cos\frac{\pi n}{2}\right).
\end{aligned}$$

Vstavimo še $d_{n+2}^{(p_1)}$*in* $d_n^{(p_1)}$ *v začetno diferenčno enačbo s* $f_1(n)$ *na desni strani*

$$(n+2)\left(-A\sin\frac{\pi n}{2} - B\cos\frac{\pi n}{2}\right) + n\left(A\sin\frac{\pi n}{2} + B\cos\frac{\pi n}{2}\right) = 5\cos\frac{\pi n}{2}.$$

Izraz uredimo in dobimo

$$-2A\sin\frac{\pi n}{2} - 2B\cos\frac{\pi n}{2} = 0\sin\frac{\pi n}{2} + 5\cos\frac{\pi n}{2}.$$

Enačaj velja, ko so istoležni koeficienti enaki, kar pomeni $-2A = 0$ *in* $-2B = 5$, *oziroma* $A = 0$ *in* $B = -\frac{5}{2}$. *Torej je*

$$d_{n+1}^{(p_1)} = -\frac{5}{2}n\cos\frac{\pi n}{2}.$$

Za $f_2(n) = 2^n$ *imamo nastavek* $d_n^{(p_2)} = D2^n$, *saj* $a = 2$ *ni ničla karakterističnega polinoma. Tokrat je* $d_{n+2}^{(p_2)} = D2^{n+2} = 4D2^n$. *Ko vstavimo nastavka v začetno rekurzijo dobimo*

$$4D2^n + D2^n = 2^n.$$

Celoten izraz delimo z 2^n *in dobimo* $5D = 1$, *oziroma* $D = \frac{1}{5}$. *Tako je* $d_n^{(p_2)} = \frac{1}{5} \cdot 2^n$. *Splošna rešitev je tako*

$$d_n = C_1 \sin \frac{\pi n}{2} + \left(C_2 - \frac{5}{2} n \right) \cos \frac{\pi n}{2} + \frac{1}{5} \cdot 2^n.$$

Upoštevajmo še začetno nalogo $d_0 = d_1 = 0$. *Pri* d_0 *dobimo* $C_2 + \frac{1}{5} = 0$, *oziroma* $C_2 = -\frac{1}{5}$. *Podobno pri* d_1 *dobimo* $C_1 + \frac{2}{5} = 0$ *in je* $C_1 = -\frac{2}{5}$. *Tako je rešitev začetne naloge*

$$d_n = -\frac{2}{5} \sin \frac{\pi n}{2} + \left(-\frac{1}{5} - \frac{5}{2} n \right) \cos \frac{\pi n}{2} + \frac{1}{5} \cdot 2^n.$$

Za primera (b) *in* (c) *zapišimo le glavne korake brez podrobnosti. Za* (b) *poiščemo ničle karakterističnega polinoma iz* $r^2 + 5r - 6 = (r-1)(r+6) = 0$ *in imamo* $r_1 = 1$ *ter* $r_2 = -6$. *Tako je* $b_n^{(h)} = C_1 1^n + C_2(-6)^n = C_1 + C_2(-6)^n$. *Za partikularno rešitev uporabimo dva nastavka* $b_n^{(p_1)} = n(An + B)$ *(tukaj je* $a = 1$ *enojna ničla karakterističnega polinoma) in* $b_n^{(p_2)} = D3^n$. *Zapišemo* $b_{n-1}^{(p_1)}$, $b_{n-2}^{(p_1)}$, *ju uredimo, vse nastavke vstavimo v začetno rekurzijo in z nekaj računanja dobimo* $A = \frac{5}{14}$ *in* $B = \frac{95}{98}$. *Zgodbo ponovimo z* $b_{n-1}^{(p2)}$ *in* $b_{n-2}^{(p2)}$ *in dobimo* $D = \frac{1}{2}$. *Tako je splošna rešitev*

$$b_n = C_1 + \frac{95}{98} n + \frac{5}{14} n^2 + C_2(-6)^n + \frac{1}{2} \cdot 3^n.$$

Rešiti moramo še začetno nalogo $b_0 = 6$, $b_1 = \frac{65}{49}$. *Tako dobimo sistem* $6 = C_1 + C_2 + \frac{1}{2}$ *in* $\frac{65}{49} = C_1 + \frac{95}{98} + \frac{5}{14} - 6C_2 + \frac{3}{2}$, *oziroma v urejeni verziji* $C_1 + C_2 = \frac{11}{2}$ *in* $C_1 - 6C_2 = -\frac{3}{2}$. *Sistem ima rešitev* $C_2 = 1$ *in* $C_1 = \frac{9}{2}$. *Tako je rešitev začetne naloge*

$$b_n = \frac{9}{2} + \frac{95}{98} n + \frac{5}{14} n^2 + (-6)^n + \frac{1}{2} \cdot 3^n.$$

Za (c) *poiščemo ničle karakterističnega polinoma iz* $r^2 - 8r + 15 = (r-3)(r-5) = 0$ *in imamo* $r_1 = 3$ *ter* $r_2 = 5$. *Tako je* $c_n^{(h)} = C_1 3^n + C_2 5^n$. *Za partikularno rešitev uporabimo nastavek* $c_n^{(p)} = 3^n \left(A \sin \frac{\pi n}{2} + B \cos \frac{\pi n}{2} \right)$. *Zapišemo* $c_{n+1}^{(p)}$, $c_{n+2}^{(p)}$, *ju uredimo z adicijskima izrekoma, vse nastavke vstavimo v začetno rekurzijo in z nekaj računanje dobimo* $A = \frac{1}{102}$ *in* $B = \frac{2}{51}$. *Tako je splošna rešitev*

$$c_n = C_1 3^n + C_2 5^n + 3^n \left(\frac{1}{102} \sin \frac{\pi n}{2} + \frac{2}{51} \cos \frac{\pi n}{2} \right).$$

Rešimo še začetno nalogo $c_0 = 0$, $c_1 = 2$. *Tako dobimo sistem* $0 = C_1 + C_2 + \frac{2}{51}$ *in* $2 = 3C_1 + 5C_2 + \frac{1}{34}$. *Sistem ima rešitev* $C_2 = \frac{77}{68}$ *in* $C_1 = -\frac{239}{204}$. *Tako je rešitev začetne naloge*

$$c_n = \frac{77}{68} 5^n + 3^n \left(-\frac{239}{204} + \frac{1}{102} \sin \frac{\pi n}{2} + \frac{2}{51} \cos \frac{\pi n}{2} \right).$$

Zapišimo še rešitve za preostale rekurzivne relacije:

(E) $e_n = \frac{-7+6\sqrt{3}}{12}(2+\sqrt{3})^n - \frac{7+6\sqrt{3}}{12}(2-\sqrt{3})^n - \frac{3}{2}n + \frac{3}{2} - \frac{1}{3}2^n$,

(F) $f_n = \left(\frac{5}{6} - \frac{\sqrt{3}}{72}\right)(-1)^n + \left(\frac{\sqrt{3}}{18} - \frac{28}{3}\right)2^{-n} + \frac{3}{2}n^2 - \frac{13}{2}n + \frac{19}{2} - \frac{1}{24}\sin\frac{\pi n}{3} - \frac{\sqrt{3}}{24}\cos\frac{\pi n}{3}$,

(G) $g_n = \left(\frac{17}{72} + \frac{1}{12}n\right)2^n - \frac{5}{18}(-1)^n - \frac{11}{56}(-2)^n + \frac{\sqrt{3}}{21}\sin\frac{\pi n}{3} - \frac{2}{21}\cos\frac{\pi n}{3}$,

(H) $h_n = 2^n\left(\frac{1}{12}n^3 - \frac{1}{24}n^2 - \frac{5}{8}n - \frac{17}{36} - \frac{35\sqrt{3}}{36}\sin\frac{2\pi n}{3} + \frac{17}{36}\cos\frac{2\pi n}{3}\right)$,

(I) $i_n = \frac{43}{90}\cdot 2^n - \frac{5}{18}(-2)^n + \frac{8}{3}n + \frac{10}{9} + \frac{1}{3}\cdot 3^n$,

(J) $j_n = \left(\frac{25}{32} - 2n\right)(-2)^n + \left(\frac{7}{36} - \frac{7}{8}n + \frac{7}{16}n^2\right)2^n$,

(K) $k_n = \frac{9}{4} + \frac{5}{36}(-1)^n - \frac{1}{2}\cos\frac{\pi n}{2} + \left(\frac{1}{3}n - \frac{8}{9}\right)2^n$.

Vaja 4.4 *Podano je zaporedje $a_n = 5\cdot 2^n + 4(-3)^n + 8$. Poiščite vse linearne rekurzivne relacije s konstantnimi koeficienti, katerih rešitev ustrezne začetne naloge je zaporedje a_n.*

Rešitev. *Različne rekurzije, ki imajo za rešitev zaporedje a_n, lahko dobimo tako, da različne dele zaporedja a_n proglasimo za homogeno rešitev, medtem ko je preostanek partikularna rešitev. V vseh primerih je a_n rešitev začetne naloge in potrebovali bomo začetne člene, torej $a_0 = 17$, $a_1 = 6$ in $a_2 = 64$.*

Naj najprej celotno zaporedje izhaja iz homogene rekurzije, oziroma $a_n^{(p)} = 0$. Tako ima karakteristični polinom tri različne ničle $r_1 = 2$, $r_2 = -3$ in $r_3 = 1$. S tem dobimo karakteristični polinom

$$p_3(r) = (r-2)(r+3)(r-1) = r^3 - 7r + 6$$

in posledično začetno nalogo homogene rekurzije z rešitvijo a_n, ki je

$$a_{n+3} - 7a_{n+1} + 6a_n = 0, a_0 = 17, a_1 = 6, a_2 = 64.$$

Naslednja možnost je, da po en člen iz zaporedja a_n proglasimo za partikularno rešitev. Tako dobimo tri različne možnosti. Naj bo najprej $a_n^{(p)} = 8$. Karakteristični polinom ima sedaj dve različni ničli $r_1 = 2$ in $r_2 = -3$ in je enak $p_2(r) = (r-2)(r+3) = r^2 + r - 6$. V tem primeru je rekurzija enaka

$$a_{n+2} + a_{n+1} - 6a_n = x,$$

kjer števila x še ne poznamo. Dobimo ga iz partikularne rešitve, ki je $a_n^{(p)} = 8$. Po drugi strani je nastavek za partikularno rešitev $a_n^{(p)} = A = 8$. Seveda velja $a_n^{(p)} = a_{n+1}^{(p)} = a_{n+2}^{(p)} = A$. Vstavimo jih v rekurzijo in dobimo $A + A - 6A = x$, oziroma $x = -32$. S tem smo našli drugo rekurzijo z rešitvijo a_n, ki je

$$a_{n+2} + a_{n+1} - 6a_n = -32, a_0 = 17, a_1 = 6.$$

Naslednja možnost je $a_n^{(p)} = 4(-3)^n$. *Podobno kot prej ima sedaj karakteristični polinom dve različni ničli* $r_1 = 2$ *in* $r_2 = 1$ *in je enak* $p_2(r) = (r-2)(r-1) = r^2 - 3r + 2$. *V tem primeru je rekurzija enaka*

$$a_{n+2} - 3a_{n+1} + 2a_n = y(-3)^n,$$

kjer števila y *še ne poznamo. Dobimo ga iz partikularne rešitve, ki je* $a_n^{(p)} = 4(-3)^n$. *Po drugi strani je nastavek za partikularno rešitev* $a_n^{(p)} = B(-3)^n$, *kar pomeni* $B = 4$. *Vstavimo* $a_n^{(p)} = B(-3)^n$, $a_{n+1}^{(p)} = B(-3)^{n+1}$ *in* $a_{n+2}^{(p)} = B(-3)^{n+2}$ *v rekurzijo in dobimo* $(9B - 9B + 2B)(-3)^n = y(-3)^n$, *oziroma* $y = 8$. *S tem smo našli tretjo rekurzijo z rešitvijo* a_n, *ki je*

$$a_{n+2} - 3a_{n+1} + 2a_n = 8(-3)^n, a_0 = 17, a_1 = 6.$$

Nadaljujemo s primerom $a_n^{(p)} = 5 \cdot 2^n$. *Spet ima karakteristični polinom dve različni ničli* $r_1 = -3$ *in* $r_2 = 1$ *in je enak* $p_2(r) = (r+3)(r-1) = r^2 + 2r - 3$. *V tem primeru je rekurzija enaka*

$$a_{n+2} + 2a_{n+1} - 3a_n = z2^n,$$

kjer števila z *še ne poznamo. Dobimo ga iz partikularne rešitve, ki je* $a_n^{(p)} = 5 \cdot 2^n$. *Po drugi strani je nastavek za partikularno rešitev* $a_n^{(p)} = C2^n$, *kar pomeni* $C = 5$. *Vstavimo* $a_n^{(p)} = C2^n$, $a_{n+1}^{(p)} = C2^{n+1}$ *in* $a_{n+2}^{(p)} = C2^{n+2}$ *v rekurzijo in dobimo* $(4C + 4C - 3C)2^n = z2^n$, *oziroma* $z = 5$. *S tem smo našli četrto rekurzijo z rešitvijo* a_n, *ki je*

$$a_{n+2} + 2a_{n+1} - 3a_n = 5 \cdot 2^n, a_0 = 17, a_1 = 6.$$

Ostanejo še tri možnosti, ko sta v partikularni rešitvi po dva člena. Naj bo najprej $a_n^{(p)} = 5 \cdot 2^n + 4(-3)^n$. *Homogena rešitev je tako* $a_n^{(h)} = C_1$, *kar pomeni, da je* $p_1(r) = r - 1$ *kar karakteristični polinom porojen iz rekurzije* $a_{n+1} - a_n = z_1 2^n + y_1(-3)^n$, *kjer števil* z_1 *in* y_1 *še ne poznamo. Ob tem sta* $a_n^{(p_1)} = 5 \cdot 2^n$ *in* $a_n^{(p_2)} = 4(-3)^n$ *ob nastavkih* $a_n^{(p_1)} = D \cdot 2^n$, *oziroma* $a_n^{(p_2)} = E(-3)^n$, *kar pomeni* $D = 5$ *in* $E = 4$. *Vstavimo* $a_n^{(p_1)}$ *in* $a_{n+1}^{(p_1)}$ *v rekurzijo in dobimo* $(2D - D)2^n = z_1 2^n$, *oziroma* $z_1 = 5$. *Postopek ponovimo tudi z* $a_n^{(p_2)}$ *in* $a_{n+1}^{(p_2)}$, *kjer dobimo* $(-3E - E)(-3)^n = y_1(-3)^n$, *oziroma* $y_1 = -16$. *Tako je peta rekurzija z rešitvijo* a_n *enaka*

$$a_{n+1} - a_n = 5 \cdot 2^n - 16(-3)^n, a_0 = 17.$$

Nadaljujemo z $a_n^{(p)} = 5 \cdot 2^n + 8$. *Homogena rešitev je potem* $a_n^{(h)} = C_2(-3)^n$, *kar pomeni, da je* $p_1(r) = r + 3$ *kar karakteristični polinom porojen iz rekurzije* $a_{n+1} + 3a_n = z_2 2^n + x_2$, *kjer števil* z_2 *in* x_2 *še ne poznamo. Ob tem sta* $a_n^{(p_1)} = 5 \cdot 2^n$ *in* $a_n^{(p_2)} = 8$ *ob nastavkih* $a_n^{(p_1)} = F \cdot 2^n$, *oziroma* $a_n^{(p_2)} = G$, *kar pomeni* $F = 5$ *in* $G = 8$. *Vstavimo* $a_n^{(p_1)}$ *in* $a_{n+1}^{(p_1)}$ *v rekurzijo in dobimo* $(2F + 3F)2^n = z_2 2^n$, *oziroma* $z_2 = 25$. *Postopek ponovimo tudi z* $a_n^{(p_2)}$ *in* $a_{n+1}^{(p_2)}$, *kjer dobimo* $(G + 3G)(-3)^n = z_2(-3)^n$, *oziroma* $z_2 = 32$. *Naslednja rekurzija z rešitvijo* a_n *je tako enaka*

$$a_{n+1} + 3a_n = 25 \cdot 2^n + 32, a_0 = 17.$$

Zadnja možnost je $a_n^{(p)} = 4(-3)^n + 8$. *Homogena rešitev je potem* $a_n^{(h)} = C_3 2^n$, *kar pomeni, da je* $p_1(r) = r - 2$ *kar karakteristični polinom porojen iz rekurzije* $a_{n+1} - 2a_n = y_3(-3)^n + x_3$, *kjer števil* y_3 *in* x_3 *še ne poznamo. Ob tem sta* $a_n^{(p_1)} = 4(-3)^n$ *in* $a_n^{(p_2)} = 8$ *ob nastavkih* $a_n^{(p_1)} = H \cdot (-3)^n$, *oziroma* $a_n^{(p_2)} = K$, *kar pomeni* $H = 4$ *in* $K = 8$. *Vstavimo* $a_n^{(p_1)}$ *in* $a_{n+1}^{(p_1)}$ *v rekurzijo in dobimo* $(-3H - 2H)(-3)^n = y_3(-3)^n$, *oziroma* $y_3 = -20$. *Postopek ponovimo tudi z* $a_n^{(p_2)}$ *in* $a_{n+1}^{(p_2)}$, *kjer dobimo* $K - 2K = x_3$, *oziroma* $x_3 = -8$. *Zadnja rekurzija z rešitvijo* a_n *je enaka*

$$a_{n+1} - 2a_n = -20(-3)^n - 8, a_0 = 17.$$

Vaja 4.5 *Podano je zaporedje* $b_n = (5n - 3)3^n + 7 \cdot 2^n$. *Poiščite vse linearne rekurzivne relacije s konstantnimi koeficienti, katerih rešitev ustrezne začetne naloge je zaporedje* b_n.

Rešitev. *Postopek je podoben kot v prejšnji nalogi, le da pričakujemo manj rešitev. Najprej potrebujemo tri začetne člene, torej* $b_0 = 4$, $b_1 = 20$ *in* $b_2 = 91$.

Naj najprej celotno zaporedje izhaja iz homogene rekurzije, oziroma $b_n^{(p)} = 0$. *Tako ima karakteristični polinom ničle* $r_1 = r_2 = 3$ *in* $r_3 = 2$. *S tem dobimo karakteristični polinom*

$$p_3(r) = (r - 3)^2(r - 2) = r^3 - 8r^2 + 21r - 18$$

in posledično začetno nalogo homogene rekurzije z rešitvijo b_n, *ki je*

$$b_{n+3} - 8b_{n+2} + 21b_{n+1} - 18b_n = 0, b_0 = 4, b_1 = 20, b_2 = 91.$$

Če za partikularno rešitev razglasimo po en člen iz zaporedja a_n, *potem dobimo v tem primeru le dve različni možnosti, saj* $-3 \cdot 3^n$ *ne more biti v partikularni rešitvi, če je v homogeni rešitvi* $5n3^n$. *Naj bo najprej* $b_n^{(p)} = 7 \cdot 2^n$. *Karakteristični polinom ima sedaj dvojno ničlo* $r_1 = r_2 = 3$ *in je enak* $p_2(r) = (r - 3)^2 = r^2 - 6r + 9$. *V tem primeru je rekurzija enaka*

$$b_{n+2} - 6b_{n+1} + 9b_n = x2^n,$$

kjer števila x *še ne poznamo. Partikularna rešitv je* $b_n^{(p)} = 7 \cdot 2^n$, *medtem ko je nastavek zanjo* $b_n^{(p)} = A2^n$, *kar pomeni, da je* $A = 7$. *Vstavimo* $b_n^{(p)} = A2^n$, $b_{n+1}^{(p)} = A2^{n+1}$ *in* $b_{n+2}^{(p)} = A2^{n+2}$ *v rekurzijo in dobimo* $(4A - 12A + 9A)2^n = x2^n$, *oziroma* $x = A = 7$. *S tem smo našli drugo rekurzijo z rešitvijo* b_n, *ki je*

$$b_{n+2} - 6b_{n+1} + 9b_n = 7 \cdot 2^n, b_0 = 4, b_1 = 20.$$

Naslednja možnost je $b_n^{(p)} = 5n3^n$. *Karakteristični polinom ima sedaj dve različni ničli* $r_1 = 3$ *in* $r_2 = 2$ *in je enak* $p_2(r) = (r - 3)(r - 2) = r^2 - 5r + 6$. *V tem primeru je rekurzija enaka*

$$b_{n+2} - 5b_{n+1} + 6b_n = y3^n,$$

kjer števila y *še ne poznamo. Dobimo ga iz partikularne rešitve, ki je* $b_n^{(p)} = 5n3^n$. *Po drugi strani je nastavek za partikularno rešitev* $b_n^{(p)} = Bn3^n$, *kar pomeni* $B = 5$.

Vstavimo $b_n^{(p)} = Bn3^n$, $b_{n+1}^{(p)} = B(n+1)3^{n+1}$ in $b_{n+2}^{(p)} = B(n+2)3^{n+2}$ v rekurzijo in dobimo $(9Bn + 18B - 15Bn - 15B + 6Bn)3^n = y3^n$, oziroma $y = 3B = 15$. S tem smo našli tretjo rekurzijo z rešitvijo b_n, ki je

$$b_{n+2} - 5b_{n+1} + 6b_n = 15 \cdot 3^n, b_0 = 4, b_1 = 20.$$

Tudi ko sta v partikularni rešitvi po dva člena, imamo le dve možnosti, saj če člen $-3 \cdot 3^n$ nastopi v partikularni rešitvi, potem mora v njej nastopiti tudi člen $5n3^n$. Tako naj bo $b_n^{(p)} = (5n-3)3^n$. Homogena rešitev je tako $b_n^{(h)} = C_1 2^n$, kar pomeni, da je $p_1(r) = r - 2$ kar karakteristični polinom porojen iz rekurzije $b_{n+1} - 2b_n = (z_1 n + y_1)3^n$, kjer števil z_1 in y_1 še ne poznamo. Ob tem je nastavek za partikularno rešitev $b_n^{(p)} = (Dn + E)3^n$, kar pomeni $D = 5$ in $E = -3$. Vstavimo $b_n^{(p)}$ in $b_{n+1}^{(p)} = (Dn + D + E)$ v rekurzijo in dobimo $(Dn + D + E - 2Dn - 2E)3^n = (z_1 n + y_1)3^n$, oziroma $z_1 = -D = -5$ in $y_1 = D - E = 8$. Tako je četrta rekurzija z rešitvijo b_n enaka

$$b_{n+1} - 2b_n = (-5n + 8)3^n, b_0 = 17.$$

Zadnja možnost je $a_n^{(p)} = 5n3^n + 7 \cdot 2^n$. Homogena rešitev je potem $b_n^{(h)} = C_2 3^n$, kar pomeni, da je $p_1(r) = r - 3$ karakteristični polinom porojen iz rekurzije $b_{n+1} - 3b_n = y_2 3^n + x_2 2^n$, kjer števil y_2 in x_2 še ne poznamo. Ob tem sta $b_n^{(p_1)} = 5n3^n$ in $b_n^{(p_2)} = 7 \cdot 2^n$ ob nastavkih $b_n^{(p_1)} = Fn3^n$, oziroma $b_n^{(p_2)} = G2^n$, kar pomeni $F = 5$ in $G = 7$. Vstavimo $b_n^{(p_1)}$ in $b_{n+1}^{(p_1)}$ v rekurzijo in dobimo $(3nF + 3F - 3nF)3^n = y_2 3^n$, oziroma $y_2 = 3F = 15$. Postopek ponovimo tudi z $b_n^{(p_2)}$ in $b_{n+1}^{(p_2)}$, kjer dobimo $(2G - 3G)2^n = x_2 2^n$, oziroma $x_2 = -G = -7$. Zadnja rekurzija z rešitvijo b_n je enaka

$$b_{n+1} - 3b_n = 15 \cdot 3^n - 7 \cdot 2^n, b_0 = 17.$$

Vaja 4.6 *Podano je zaporedje $c_n = 3 \cdot 5^n + 2^n(4\cos\frac{\pi n}{2} - \sin\frac{\pi n}{2})$. Poiščite vse linearne rekurzivne relacije s konstantnimi koeficienti, katerih rešitev ustrezne začetne naloge je zaporedje c_n.*

Rešitev. *Postopek je podoben kot v prejšnjih dveh nalogah, le da bo število rešitev še manjše, saj mora del s sinusom in kosinusom vedno biti skupaj, ali v homogeni, ali v partikularni rešitvi. Najprej potrebujemo tri začetne člene za začetno nalogo, torej $c_0 = 7$, $c_1 = 13$ in $c_2 = 59$.*

Začnemo s primerom, ko celotno zaporedje izhaja iz homogene rekurzije, oziroma $b_n^{(p)} = 0$. Tako ima karakteristični polinom ničle $r_1 = 5$, $r_2 = 2i$ in $r_3 = -2i$, saj smo zaradi kota $\varphi = \frac{\pi}{2}$ na imaginarni osi za dva oddaljeni od izhodišča, ker je $r = 2$. S tem dobimo karakteristični polinom

$$p_3(r) = (r-5)(r-2i)(r+2i) = r^3 - 5r^2 + 4r - 20$$

in posledično začetno nalogo homogene rekurzije z rešitvijo c_n, ki je

$$c_{n+3} - 5c_{n+2} + 4c_{n+1} - 20c_n = 0, c_0 = 7, c_1 = 13, c_2 = 59.$$

Če za partikularno rešitev razglasimo po en člen iz zaporedja c_n, potem je edina možnost $c_n^{(p)} = 3 \cdot 5^n$ (obe kotni funkciji sta v homogeni rešitvi). Karakteristični polinom ima ničli $r_1 = 2i$ in $r_2 = -2i$ in je enak $p_2(r) = (r-2i)(r+2i) = r^2 + 4$. V tem primeru je rekurzija enaka

$$c_{n+2} + 4c_n = x5^n,$$

kjer števila x še ne poznamo. Nastavek za partikularno rešitev je $c_n^{(p)} = A5^n$, kar pomeni, da je $A = 3$. Vstavimo $c_n^{(p)} = A5^n$ in $c_{n+2}^{(p)} = A5^{n+2}$ v rekurzijo in dobimo $(25A + 4A)5^n = x5^n$, oziroma $x = 29A = 87$. S tem smo našli drugo rekurzijo z rešitvijo c_n, ki je

$$c_{n+2} + 4c_n = 87 \cdot 5^n, c_0 = 7, c_1 = 13.$$

Zadnja možnost je $c_n^{(p)} = 2^n(4\cos\frac{\pi n}{2} - \sin\frac{\pi n}{2})$ (obe kotni funkciji sta v partikularni rešitvi). Homogena rešitev je tako $c_n^{(h)} = K_1 5^n$, kar pomeni, da je $p_1(r) = r - 5$ karakteristični polinom porojen iz rekurzije $c_{n+1} - 5c_n = 2^n(y\cos\frac{\pi n}{2} + z\sin\frac{\pi n}{2})$, kjer števil y in z še ne poznamo. Ob tem je nastavek za partikularno rešitev $c_n^{(p)} = 2^n(B\cos\frac{\pi n}{2} + D\sin\frac{\pi n}{2})$, kar pomeni $B = 4$ in $D = -1$. Vstavimo $c_n^{(p)}$ in

$$\begin{aligned} c_{n+1}^{(p)} &= 2^{n+1}\left(B\cos\left(\frac{\pi n}{2} + \frac{\pi}{2}\right) + D\sin\left(\frac{\pi n}{2} + \frac{\pi}{2}\right)\right) = \\ &= 2^n\left(-2B\sin\frac{\pi n}{2} - 2D\cos\frac{\pi n}{2}\right) \end{aligned}$$

v rekurzijo in dobimo

$$2^n\left((-2D-5B)\cos\frac{\pi n}{2} + (-2B-5D)\sin\frac{\pi n}{2}\right) = 2^n\left(y\cos\frac{\pi n}{2} + z\sin\frac{\pi n}{2}\right).$$

Enačaj velja, ko je $y = -2D - 5B = -18$ in $z = -2B - 5D = -3$. Tako je četrta rekurzija z rešitvijo a_n enaka

$$c_{n+1} - 5c_n = 2^n(-18\cos\frac{\pi n}{2} - 3\sin\frac{\pi n}{2}), c_0 = 7.$$

Vaja 4.7 *Podana so zaporedja*

(A) $a_n = 2^n - 4 \cdot 5^n + 3(-1)^n$,

(B) $b_n = (n-3)(-1)^n + 6 \cdot 3^n$,

(C) $c_n = 4 \cdot 3^n + 2^n\left(2\cos\frac{\pi n}{3} - \sin\frac{\pi n}{3}\right)$,

(D) $d_n = (3n-2)(-2)^n + \left(\sqrt{2}\right)^n\left(\cos\frac{\pi n}{4} - 3\sin\frac{\pi n}{4}\right)$.

Poiščite vse linearne rekurzivne relacije s konstantnimi koeficienti, katerih ustrezne začetne naloge imajo za rešitev a_n, b_n, c_n oziroma d_n.

5

ČASOVNA ZAHTEVNOST

Namen tega kratkega poglavja je spoznati matematična orodja, ki nam pomagajo primerjati in vrednotiti različne algoritme za reševenje enakega problema. Pogosto lahko namreč več različnih poti vodi do enakega cilja/rezultata. Ob tem nas zanima, ali je katera izmed poti boljša. Z boljša v današnji družbi mislimo predvsem hitrejša ali cenejša. Ta dva vidika se včasih tudi izključujeta. Ker nas tukaj ne zanimajo ekonomski vidiki, se bomo osredotočili na hitrost metode.

Če se zdi komu svet današnjega računalništva dovolj hiter z vedno novimi metodami in pristopi, omenimo, da je temu tako le zaradi tega, ker še ni naletel na dovolj zahteven ali dovolj velik problem. Z razmahom socialnih omrežij tudi velikostni obseg nalog narašča brez predaha. Tako je zelo pomembno, da izbiramo postopke in metode reševanja, ki so dovolj hitre. Za večino problemov nam rešitev, ki bi jo začeli reševati danes in jo pridobili, čez recimo deset let, enostavno ne koristi. Zato je pomembno, da znamo oceniti, katera metoda je hitrejša in v tem poglavju bomo spoznali prav to.

Dodatna literatura v slovenščini iz tega področja avtorju ni poznana. V angleškem jeziku je na voljo precej več primerne literature, tukaj omenimo le [1, 6]. Marsikaj je najti tudi na spletu in pogosto je že Wikipedia (angleška) dober začetni vir informacij. Nekaj izpitnih nalog iz tega poglavja je najti v [12, 13].

5.1 DEFINICIJA

Najprej se je potrebno dogovoriti, kaj algoritem sploh je.

Vsekakor je temeljna značilnost vseh metod, ki se izvajajo na računalniku, ta, da se morajo končati. Torej mora biti postopek **končen**.

Naslednja opazka velja temu, kaj algoritem izračuna/določi na koncu svojega izvajanja. To naj bo **rešitev problema**, ki ga algoritem rešuje.

Nujnost zadnje značilnosti opazimo iz prejšnje. Algoritem ne more določiti rešitve problema iz nič. Za reševanje problema potrebuje informacije o tem problemu. Te mu podamo preko **vhodnih podatkov**, ki jih lahko vnesemo preko tipkovnice, ali pridobimo iz kakšnega vira, ki je že shranjen v ustrezni elektronski obliki.

Torej, **algoritem za problem** P je postopek, ki v končno mnogo korakih iz vhodnih podatkov določi rešitev problema P, ki je podan na izhodu.

Naslednji korak je merilo, s katerim merimo kvaliteto algoritma. Seveda ne gre pričakovati, da bo algoritem za enak problem enako hiter, če mu na vhodu ponudimo majhen oziroma velik vzorec. Tako bomo, recimo, za pregled instagram povezav predsednika države, potrebovali precej več časa, kot za enako nalogo, kjer preverjamo člane lokalnega gobarskega društva. Slednji imajo skupaj morda nekaj sto sledilcev, medtem ko je število sledilcev predsednika države okoli 10000.

S tem smo postavili prvi temelj za iskano merilo. Le-to naj bo odvisno od **velikosti vhodnih podatkov**, saj bomo potem algoritem ocenjevali neodvisno od njih. Dogovorimo se, da velikost vhodnih podatkov na kratko označimo kar z VVP.

Naslednjo težavo predstavlja kar merjenje VVP. Ena izmed možnosti je lahko število udarcev po tipkovnici, da vhodne podatke vnesemo v računalnik. Ker vhodne podatke, kot že omenjeno, pogosto generiramo kar iz elektronsko shranjenih virov, se zdi ta opcija nerealna. Zato se raje odločimo za velikostni red, ki ga vhodni podatki zavzemajo pri hranjenju v računalniškem spominu.

S tem smo prišli do bistva samega. Kako določiti merilo za kvaliteto algoritma? V definiciji za algoritem se skriva fraza 'v končno mnogo korakih'. Če tole prevedemo v bolj otipljiv jezik, to pomeni, da lahko preštejemo število korakov, ki jih algoritem opravi. Ker se, kot že ugotovljeno, število opravljenih korakov razlikuje pri različnih VVP, lahko poiščemo funkcijo f, ki nam določi število korakov algoritma glede na velikost vhodnih podatkov. Ker nam funkcija f šteje korake, njeno definicijsko območje predstavljajo naravna števila in imamo $f : \mathbb{N} \to \mathbb{R}$. Ob tem nas ne zanima $f(n)$, pač pa $f(VVP)$.

Zgled 5.1 *Vprašajmo se, kako je v računalniku skranjeno število, ki ima v desetiškem številskem sistemu obliko $n = (n_k n_{k-1} \dots n_1 n_0)_{10}$. Vsa števila so v računalniku shranjena v dvojiški obliki, zato nas zanima $n = (b_\ell b_{\ell-1} \dots b_1 b_0)_2$, kjer je $b_i \in \{0,1\}$ za vsak $i \in [\ell]_0$. Bolj natančno, zanima nas število ℓ, saj predstavlja število mest, ki jih potrebujemo, da shranimo n. Pretvorbo lahko storimo z naslednjim preprostim algoritmom.*

Algoritem 1: Pretvorba števila iz desetiškega v binarni zapis

Vhod: *Število z zapisano v desetiškem sistemu.*
Izhod: *Število $b = z$ zapisano v binarnem sistemu.*
$b = 0$, $i = 0$
while $z > 0$ **do**
  $b_i = z \pmod 2$
  $z = z \text{ (div 2)}$
  $i = i + 1$
end

Posebej omenimo, da ukaz $(\text{mod } 2)$ *pomeni ostanek pri deljenju števila* z 2 *in je lahko le* 0*, ko je naše število sodo, in* 1*, ko je naše število liho. Tukaj je še ukaz* $(\text{div } 2)$*, ki dano število deli* z 2 *in kot rezultat ohrani le celo število brez decimalnega dela (če ta sploh obstaja). Tako nas zanima, kolikokrat se izvrši zanka iz algoritma. Vsakič, ko se zanka izvrši, to v grobem pomeni, da smo število* n *razpolovili. Oziroma v obratno smer, da je* n *večji od ustrezne potence* 2*. Če se je zanka izvršila* k*-krat, to pomeni, da je* $2^{k-1} \leq n < 2^k$*, oziroma* $k - 1 \leq \lg n < k$*, kjer* lg *označuje dvojiški logaritem. Tako je število bitov, ki jih potrebujemo v računalniku, da shranimo naravno število* n*, navzdol omejeno* z $\lg n$*. Omenimo še, da je* $\lg n = k - 1$ *natanko tedaj, ko je* $n = 2^{k-1}$ *in takrat je* $k = 1 + \lg n$*.*

Sedaj, ko smo se prebili do funkcij, imamo matematično že lažje delo. Naj bosta f in g funkciji, ki obe slikata iz naravnih števil v realna. Oglejmo si, v kakšnem razmerju sta lahko funkciji f in g, ko gre za dovolj velika naravna števila. Če se navežemo na že obstoječe znanje, se lahko spomnimo, da ste v srednji šoli spoznali poševne in vodoravne asimptote. Sedaj bomo pojem asimptote razširili iz premice (poševne ali vodoravne) na poljubno funkcijo g. Oglejmo si naslednje definicije.

Rečemo, da je $f(n)$ **reda največ** $g(n)$, ali $f(n)$ **je veliki** O **od** $g(n)$, kar pišemo $f(n) = O(g(n))$, če obstaja konstanta $C_1 \in \mathbb{R}$, da je $f(n) \leq C_1 g(n)$ za vsa naravna števila, razen končno mnogo. Če je $f(n) = O(g(n))$, potem je $g(n)$ **asimptotična zgornja meja** funkcije $f(n)$.

Rečemo, da je $f(n)$ **reda vsaj** $g(n)$, ali $f(n)$ **je omega** Ω **od** $g(n)$, kar pišemo $f(n) = \Omega(g(n))$, če obstaja konstanta $C_2 \in \mathbb{R}$, da je $f(n) \geq C_2 g(n)$ za vsa naravna števila, razen končno mnogo. Če je $f(n) = \Omega(g(n))$, potem je $g(n)$ **asimptotična spodnja meja** funkcije $f(n)$.

Rečemo, da je $f(n)$ **reda** $g(n)$, ali $f(n)$ **je theta** Θ **od** $g(n)$, kar pišemo $f(n) = \Theta(g(n))$, če je $f(n)$ hkrati reda največ in reda vsaj $g(n)$. Torej, če je hkrati $f(n) = O(g(n))$ in $f(n) = \Omega(g(n))$. Če je $f(n) = \Theta(g(n))$, potem je $g(n)$ **natančna asimptotična meja** funkcije $f(n)$.

Opomba 5.1 *V zgornjih definicijah, se običajno pišejo absolutne vrednosti okoli funkcij* $f(n)$ *in* $g(n)$*. Ker gre tukaj za štetje operacij, le-to ne more biti negativno in zato lahko absolutno vrednost izpustimo.*

Izrek 5.2 *Za polinom* $p_k(n) = a_n n^k + a_{n-1} n^{k-1} + \cdots + a_1 n + a_0$ *velja* $p_k(n) = \Theta(n^k)$.

Dokaz. Za vsako naravno število n velja

$$\begin{aligned} p_k(n) &= a_n n^k + a_{n-1} n^{k-1} + \cdots + a_1 n + a_0 \leq \\ &\leq a_n n^k + a_{n-1} n^k + \cdots + a_1 n^k + a_0 n^k = \\ &= n^k (a_n + a_{n-1} + \cdots + a_1 + a_0) = C_1 n^k. \end{aligned}$$

Ker je $C_1 \in \mathbb{R}$, velja $p_k(n) = O(n^k)$.

Po drugi strani je

$$\begin{aligned} p_k(n) &= a_n n^k + a_{n-1} n^{k-1} + \cdots + a_1 n + a_0 = \\ &= n^k (a_n + \frac{a_{n-1}}{n} + \cdots + \frac{a_1}{n^{k-1}} + \frac{a_0}{n^k}) \geq \\ &\geq n^k (a_n - 1) = C_2 n^k, \end{aligned}$$

kjer je neenakost izpolnjena za vsa naravna števila razen končno mnogo. Podkrepimo to. Za dovolj veliki n je ulomek $\frac{a_i}{n^{k-i}}$, $i < k$, zelo blizu 0, in če seštejemo vse ulomke v oklepaju, dobimo še vedno števila, ki so blizu 0, torej manjša od 1. Zaradi tega neenakost ni izpolnjena za največ končno naravnih števil in velja $p_k(n) = \Omega(n^k)$.

Ker je n^k asimptotična zgornja in tudi asimptotična spodnja meja polinoma $p_k(n)$, je natančna asimptotična meja in velja $p_k(n) = \Theta(n^k)$. ∎

Trditev 5.3 *Če je* $f(n) = O(g(n))$, *potem je* $f(n) + g(n) = \Theta(g(n))$.

Dokaz. Ker je $f(n) = O(g(n))$, potem je $f(n) \leq Cg(n)$ za nek $C \in \mathbb{R}$ in za vsa naravna števila, razen končno mnogo. Tako imamo

$$f(n) + g(n) \leq Cg(n) + g(n) = (C+1)g(n) = O(g(n)).$$

∎

Algoritem za problem P ima **časovno zahtevnost** $f(n) = O(g(VVP))$, če ga izvedemo v $f(n)$ korakih glede na velikost vhodnih podatkov VVP. Torej je za določitev časovne zahtevnosti algoritma potrebno prešteti število operacij v algoritmu.

S tem velja, da ima tudi problem P **časovno zahtevnost** $O(g(VVP))$, saj imamo algoritem v takšni časovni zahtevnosti, ki ta problem reši. Do spodnje asimptotične meje $\Omega(g_1(n))$ problema P se ne moremo prebiti s pomočjo algoritma, pač pa poiščemo lastnost, zaradi katere problema P ni moč rešiti hitreje. To je pogosto precej težje, kot najti algoritem, ki ni nujno optimalen.

Kaj storimo, če algoritem ni optimalen? Poskusimo najti boljšega. Če ga najdemo, potem ima nov algoritem boljšo časovno zahtevnost in s tem se izboljša tudi časovna zahtevnost samega problema.

Omenimo najpomembnejše časovne zahtevnosti, ki so zbrane v naslednjem seznamu. Ob tem velikost vhodnih podatkov označimo z n.

$O(1)$	konstantna časovna zahtevnost,
$O(\lg n)$	logaritemska časovna zahtevnost,
$O(\sqrt{n})$	korenska časovna zahtevnost,
$O(n)$	linearna časovna zahtevnost,
$O(n \lg n)$	časovna zahtevnost $n \lg n$,
$O(n^2)$	kvadratna časovna zahtevnost,
$O(n^3)$	kubična časovna zahtevnost,
$O(n^k)$	polinomska časovna zahtevnost,
$O(2^n)$	eksponentna časovna zahtevnost,
$O(n!)$	fakultetna časovna zahtevnost.

Za hitre oziroma bolje obvladljive algoritme smatramo tiste s polinomsko ali boljšo časovno zahtevnostjo in še tukaj težimo k čim manjši potenci. Nikakor pa ne želimo algoritmov z eksponentno časovno zahtevnostjo, kaj šele s fakultetno časovno zahtevnostjo. Nekateri problemi so dovolj zahtevni, da se verjame, da za njih ne obstaja polinomski algoritem (čeprav to ni dokazano). Takšnim rečemo NP-polni problemi in nekaj jih bomo spoznali v zadnjem poglavju. Obstajajo pa tudi problemi, ki so vmes. Torej za njih ne vemo, ali spadajo k težkim, ali pa so polinomski. Tak je recimo izomorfizem grafov, o čemer bo tudi govora v zadnjem poglavju. Do leta 2002 je bil tak tudi problem, ali je naravno število praštevilo, a takrat so odkrili polinomski algoritem za ta problem, ki pa ima še vedno (pre)veliko časovno zahtevnost.

Zgled 5.2 *V spodnji tabeli je predstavljenih nekaj časovnih zahtevnosti algoritmov skupaj s konstantami in čas, ki ga ti algoritmi potrebujejo za izračun na ustrezno velikem vzorcu. Ob tem predpostavimo, da se ena operacija v povprečju izvrši v eni nano sekundi, to je* $1ns = 10^{-9}s$. *Povedano drugače, v eni sekundi se izvrši milijarda operacij.*

n	$100n \lg n$	$10n^2$	$n^{3.5}$	$n^{\lg n}$	2^n	$n!$
10	$3\mu s$	$1\mu s$	$3\mu s$	$2\mu s$	$1\mu s$	$4ms$
20	$9\mu s$	$4\mu s$	$36\mu s$	$420\mu s$	$1ms$	76 *let*
30	$15\mu s$	$9\mu s$	$148\mu s$	$20ms$	$1s$	$8 \cdot 10^{15}$ *let*
50	$28\mu s$	$25\mu s$	$884\mu s$	$4s$	13 *dni*	
100	$66\mu s$	$100\mu s$	$10ms$	$5h$	$4 \cdot 10^{13}$ *let*	
1000	$1ms$	$10ms$	$32s$	$3 \cdot 10^{13}$ *let*		
10^6	$2s$	$3h$	3169 *let*			
10^{10}	$9h$	$3 \cdot 10^4$ *let*				

Vidimo, da lahko pridemo res do velikih časovnih obdobij, če ima algoritem časovno zahtevnost, ki ni polinomska. Seveda je tudi polinomska časovna zahtevnost lahko preveč, če v njej nastopajo velike potence. V drugem in tretjem stolpcu lahko vidimo tudi vpliv konstante. Ker je 100 *večje od* 10*, so rezultati v drugem stolpcu najprej slabši od tistih v tretjem stolpcu. A konstanta z velikostjo vzorca več ne igra pomembne vloge.*

Zgled 5.3 *Koliko prostora potrebujemo, da v računalniku shranimo s naravnih števil $a_1, a_2, \ldots, a_s$? Kot sledi iz zgleda 5.1, potrebujemo za vsako število a_i, $i \in [s]$, natanko k_i bitov, kjer je $k_i - 1 \leq \lg a_i < k_i$. Tako seštevek $f(s) = \lg a_1 + \lg a_2 + \cdots + \lg a_s + s$ zadošča, da shranimo omenjena števila. Hkrati nam to število ni dovolj 'všeč'. Raje bi ga opisali s kakšno enostavnejšo funkcijo. Za to naj bo $a = \max\{a_1, a_2, \ldots, a_s\}$. Tako je zgornji seštevek zagotovo omejen s $f_1(s) = s \lg a + s$. Pogosto tudi rečemo, da je v najslabšem možnem primeru število potrebnih bitov največ $f_1(s) = s \lg a + s$. V tem primeru je $f_1 = O(s \lg a)$ v skladu s trditvijo 5.3.*

Zgled 5.4 *Spomnimo se algoritma za sortiranje Bubble sort iz zgleda 4.5. Zanj smo rešili rekurzivno relacijo in ugotovili, da velja $b_n = \frac{1}{2}(n^2 - n)$. Zato je časovna zahtevnost algoritma Bubble sort kar $O(n^2) = O\left(\frac{(n \lg \max)^2}{(\lg \max)^2}\right) = O\left(\frac{VVP^2}{(\lg \max)^2}\right)$, če smo z* max *označili največje izmed podanih števil in upoštevali zgled 5.3. Tako vidimo, da je časovna zahtevnost nižja od kvadratne.*

Zgled 5.5 *Kakšna je časovna zahtevnost, da pretvorimo decimalni zapis naravnega števila n v dvojiški zapis? Kot smo videli v zgledu 5.1 je $VVP = O(\lg n)$. V vsakem koraku zanke izvedemo operaciji* mod *in* div*, ki ju štejemo kot samostojni operaciji. Ker sta omenjeni operaciji časovno precej bolj zahtevni od prištevanja* 1 *v zadnjem koraku oziroma prirejanj, imamo $f(n) = 2(\lg n + 1)$ v najslabšem možnem primeru (ko je n potenca števila* 2*). Seveda je $f(n) = O(\lg n) = O(VVP)$ in algoritem iz zgleda 5.1 je linearen.*

Zgled 5.6 *Zapišimo algoritem, ki izračuna potenco a^k za podana $a \in \mathbb{R}$ in $k \in \mathbb{N}$.*

Algoritem 2: Računanje potence

Vhod: *Naravno število k in realno število a.*
Izhod: $ans = a^k$.
$ans = a$
for $i = 2$ ***to*** k **do**
  $ans = a \cdot ans$
end

Ta algoritem opravi $f(n) = 1 + 2(k-1) = O(n)$ operacij. Tokrat ne bomo števila operacij izrazili z VVP, saj je razmislek, koliko prostora potrebujemo za realno število a, malo zahtevnejši. Lahko pa sam algoritem izboljšamo ob upoštevanju dvojiškega zapisa števila $k = (b_n b_{n-1} \ldots b_1 b_0)_2$.

Algoritem 3: Hitro računanje potence

Vhod: *Naravno število v dvojiškem zapisu* $k = b_n b_{n-1} \dots b_1 b_0$ *in realno število* a.
Izhod: $ans = a^k$.
$ans = 1$ *in* $temp = a$
for $i = 0$ ***to*** n **do**
  if $b_i = 1$ **then**
    $ans = b_i \cdot temp$
  end
  $temp = temp \cdot temp$
end

Opazimo lahko, da v spremenljivki temp računamo po vrsti $a, a^2, a^4, a^8, \dots, a^{2^n}$. *S temi potencami pa lahko izrazimo katerokoli potenco* a^k *za* $2^n \leq k < 2^{n+1}$. *Pri tem si pomagamo ravno z dvojiškim zapisom števila k. Tako je recimo* $a^{13} = a \cdot a^4 \cdot a^8$, *kjer je* $13_{10} = 1101_2$. *Preštejmo še operacije izboljšanega algoritma. Velja*

$$f_1(n) = 2 + \sum_{i=0}^{n} 4 = 2 + 4(n-1) = 4 \lg k - 2,$$

saj velja zveza $n = \lg k$. *Vidimo, da smo glede na k časovno zahtevnost dejansko izboljšali iz linearne na logaritemsko.*

Zgled 5.7 *Zapišimo preprost algoritem, ki preveri, ali je naravno število n praštevilo. Sledeči algoritem preveri za vsa števila med* 2 *in* $n-1$, *ali katero izmed njih deli n. Če se to zgodi, postavi kontrolno epremenljivko b na* 0 *in konča algoritem. Sicer b ostane* 1 *in n je praštevilo.*

Algoritem 4: Praštevilo

Vhod: *Naravno število z.*
Izhod: $b = 1$, *če je n praštevilo in* $b = 0$ *sicer.*
$b = 1$
for $i = 2$ ***to*** $n-1$ **do**
  if $n = 0 \pmod i$ **then**
    $b = 0$
    $i = n - 1$
  end
end

Zanka se izvede največ $f(n) = n - 2$ *krat in znotraj imamo vsakič eno operacijo deljenja v pogoju za if stavek (ostalo zanemarimo). Tako je* $f(n) = O(n)$, *kar ni linearna časovna zahtevnost, saj n ni VVP. Za določitev časovne zahtevnosti moramo n izraziti z* $VVP = O(\lg n)$, *kot smo videli v zgledu 5.1. Seveda velja* $n = 2^{\lg n}$ *in imamo* $f(n) = O(n) = O(2^{\lg n}) = O(2^{VVP})$. *Torej ima ta preprost algoritem eksponentno časovno zahtevnost.*

Zgornji algoritem lahko izboljšamo, če uporabimo enostavno dejstvo, da če k deli n, potem tudi $\frac{n}{k}$ deli n. Ob tem je eden zagotovo manjši ali enak $\sqrt{n}$. Tako zadošča, da zgornjo mejo v for zanki zamenjamo s $\lfloor\sqrt{n}\rfloor$. Žal to ne izboljša časovne zahtevnosti, saj imamo $f_1(n) = \sqrt{n}$ in velja $f(n) = O(\sqrt{n}) = O(2^{\lg\sqrt{n}}) = O(2^{\frac{\lg n}{2}}) = O((\sqrt{2})^{VVP})$, kar je še vedno eksponentna časovna zahtevnost. Kot smo že omenili od leta 2002 obstaja polinomski algoritem za preverjanje, ali je naravno število praštevilo.

5.2 NEKATERE (NE)REŠENE NALOGE

Vaja 5.1 *Za polinom $p_n(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ zapišite algoritem za izračun vrednosti polinoma v točki $x = a$ in ugotovite časovno zahtevnost algoritma.*

Rešitev. *Algoritem, ki nas pripelje do željenega rezultata, je naslednji.*

Algoritem 5: Vrednost polinoma v točki

Vhod: *Števila $(a_0, a_1, \ldots, a_n)$, ki določajo polinom $p_n(x)$ in realno število a.*
Izhod: *$ans = p_n(a)$.*
$ans = a_0$ in temp=a
for *$i = 1$* ***to*** *n* **do**
  $ans = ans + a_i \cdot temp$
  $temp = temp \cdot a$
end

Ni težko videti, da je število vseh operacij $f(n) = 2 + 5n$. Algoritem lahko nekoliko izboljšamo, če ga izpeljemo iz vgnezdene oblike zapisa polinoma, ki je

$$p_n(x) = (\cdots(((a_n x + a_{n-1})x + a_{n-2})x + a_{n-3})x + \cdots + a_1)x + a_0,$$

ki je osnova za Hornerjev algoritem (ki ga študentje tako radi zamešajo za algoritem za iskanje ničel polinoma). V tem primeru je časovna zahtevnost $f_1(n) = 1 + 2n$. Algoritem zapišite sami.

Vaja 5.2 *Ocenite časovno zahtevnost algoritma:*

Algoritem 6: Algoritem za vajo 5.2

Vhod: *Števila $a_1, a_2, \ldots, a_n$.*
Izhod: *Minimum in maksimum vhodnih števil.*
min $= a_1$, max $= a_1$
for *$i = 1$* ***to*** *n* **do**
  if *$a_i <$* min **then**
    min $= a_i$
  end
  if *$a_i >$* max **then**
    max $= a_i$
  end
end

Rešitev. *Če štejemo vse operacije in upoštevamo VVP iz zgleda 5.3, imamo*

$$f(n) = 2 + \sum_{i=1}^{n} 4 = 2 + 4n = O(n) = O\left(\frac{n \lg \max}{\lg \max}\right) = O\left(\frac{VVP}{\lg \max}\right),$$

kar pomeni, da je ta algoritem boljši od linearnega.

Vaja 5.3 *Zapišite algoritem za vsoto s prvih n naravnih števil in ugotovi časovno zahtevnost. Kaj pa vsota n zaporednih naravnih števil: $s_1 = (k+1) + (k+2) + \cdots + (k+n)$? Poiščite način za izračun v konstantnem času.*

Rešitev. *Zlahka opazimo, da spodnji algoritem izračuna željeno vsoto prvih n naravnih števil.*

Algoritem 7: Vsota prvih n naravnih števil

Vhod: *Naravno število n.*
Izhod: *Vsota s prvih n naravnih števil.*
$s = 0$
for $i = 1$ ***to*** n **do**
  $s = s + i$
end

Kljub svoji enostavnosti, ima ta algoritem eksponentno časovno zahtevnost. Število operacij je seveda $f(n) = 2n + 1$, kar prinese $f(n) = O(n) = O(2^{\lg n}) = O(2^{VVP})$, saj je $VVP = \lg n$, kot smo videli v zgledu 5.1. Z nekaj znanja matematike se lahko spomnimo, da naravna števila tvorijo aritmetično zaporedje, za takšna zaporedja pa obstaja formula za vsoto prvih n členov. Tako velja tudi $s = \frac{n(n+1)}{2}$, kar že predstavlja algoritem za izračun željene vsote. Število operacij je $f_1(n) = 4 = O(1)$, ne glede na število n. Torej je ta problem rešljiv v konstantni časovni zahtevnosti. Seveda ne gre bolje, zato spada ta problem v $\Theta(1)$. Tudi vsoto s_1 sedaj zlahka izračunamo, saj imamo

$$s_1 = nk + s = nk + \frac{n(n+1)}{2},$$

kar je ponovno konstantna časovna zahtevnost.

Vaja 5.4 *Zapišite algoritem, ki poišče vse delitelje števila n in ugotovite njegovo časovno zahtevnost.*

Rešitev. *Razširimo lahko algoritem iz zgleda 5.7, le da tukaj najdene delitelje shranimo v množico A.*

Algoritem 8: Delitelji števila n

Vhod: *Naravno število z.*
Izhod: *Delitelji števila n shranjeni v seznam A.*

```
A ← 1, n
for i = 2 to ⌊√n⌋ do
    if n = 0 (mod i) then
        A ← i, n/i
    end
end
```

Tukaj je zapisana že izboljšana verzija, kjer gremo v zanki le do $\lfloor\sqrt{n}\rfloor$, vendar to ne izboljša časovne zahtevnosti, ki je, kot smo videli v zgledu 5.7, eksponentna.

Vaja 5.5 *Zapišite algoritem za določanje relacije $R^2 = R * R$, če je $R \subseteq A \times A$ in $|A| = n$, in ugotovite njegovo časovno zahtevnost.*

Rešitev. *Definicijo in način računanja R^2 najdemo proti koncu razdelka 7.2. Potem tudi ni težko videti, da nam R^2 izračuna spodnji algoritem.*

Algoritem 9: Relacija R^2

Vhod: *Relacija R podana z $n \times n$ matriko.*
Izhod: *Relacija R^2 shranjena v $n \times n$ matriko S.*

```
for i = 1 to n do
    for j = 1 to n do
        s_{i,j} = 0
        for k = 1 to n do
            s_{i,j} = s_{i,j} ∨ (r_{i,k} ∧ r_{k,j})
        end
    end
end
```

Ker ima algoritem tri for zanke, je njegova časovna zahtevnost $O(n^3)$. Če je relacija podana z matriko, ima le-ta $VVP = n^2$ in tako je $O(n^3) = O((n^2)^{3/2}) = O(VVP^{3/2})$, kar ni daleč od linearnosti.

Vaja 5.6 *Zapišite algoritem za množenje dveh $n \times n$ matrik in ugotovite njegovo časovno zahtevnost.*

Rešitev. *Produkt matrik računamo podobno kot R^2 in je opisan v opombi 7.3. Tako lahko prejšnji algoritem malenkostno prilagodimo (zamenjamo $\wedge$ z običajnim množenjem in $\vee$ s seštevanjem) in dobimo sledeči algoritem.*

Algoritem 10: Produkt matrik AB

```
M Vhod: Matriki A in B dimenzije n × n.
Izhod: Matrika C = AB dimenzije n × n.
for i = 1 to n do
    for j = 1 to n do
        c_{i,j} = 0
        for k = 1 to n do
            c_{i,j} = c_{i,j} + (a_{i,k} · b_{k,j})
        end
    end
end
```

Tudi časovna zahtevnost se obnaša enako kot pri prejšni nalogi in imamo $O(VVP^{3/2})$.

Vaja 5.7 *Zapišite algoritem, ki reši sistem $Ax = b$, če je A zgornje trikotna matrika dimenzij $n \times n$ in b vektor dolžine n. Preštejte število operacij, ki jih izvede ta algoritem.*

Rešitev. *To storimo s sledečim algoritmom.*

Algoritem 11: Vaja 5.7

```
Vhod: Zgornje trikotna n × n matrika A in vektor b dolžine n.
Izhod: Rešitev sistema Ax = b.
y_1 = b_1 / a_{1,1}
for i = n up to 1 do
    x_i = b_i
    for j = i + 1 to n do
        x_i = x_i − a_{i,j} x_j
    end
    x_i = x_i / a_{i,i}
end
```

Število operacij je $f(n) = 2 + \sum_{i=1}^{n} \left(3 + \sum_{j=i+1}^{n} 3\right)$, če upoštevamo vse operacije (množenje, deljenje, odštevanje in prirejanje). Uredimo sedaj $f(n)$:

$$\begin{aligned} f(n) &= 2 + \sum_{i=1}^{n} \left(3 + 3 \sum_{j=i+1}^{n} 1\right) = 2 + 3 \sum_{i=1}^{n} (1 + n - i) = \\ &= 2 + 3\,(n + n - 1 + n - 2 + \cdots + 1) = \\ &= 2 + 3\frac{n\,(n+1)}{2} = \frac{3n^2}{2} + \frac{3n}{2} + 2 = O(n^2). \end{aligned}$$

Vaja 5.8 *Podan je naslednji algoritem.*

Algoritem 12: Vaja 5.8

```
Vhod: Vhodni podatki.
Izhod: Izhodni podatki.
y_1 = b_1 / ℓ_{1,1}
for i = 2 to n do
    y(i) = b(i)
    for j = 1 to i − 1 do
        y(i) = y(i) − ℓ(i, j)y(j)
    end
    y(i) = y(i) / ℓ(i, i)
end
```

(A) *Preštejte koliko operacij je potrebno, da se izvede algoritem.*

(B) *Kakšne podatke potrebujemo na vhodu?*

(C) *Kaj izračuna ta algoritem?*

Rešitev. *Število vseh operacij izračunamo podobno kot v prejšnji nalogi:*

$$\begin{aligned} f(n) &= 2+\sum_{i=2}^{n}\left(3+\sum_{j=1}^{i-1}3\right) = 2+\sum_{i=2}^{n}\left(3+3\sum_{j=1}^{i-1}\right) = \\ &= 2+3\sum_{i=2}^{n}(1+n-i) = 2+3\,(n-1+n-2+\cdots+1) = \\ &= 2+3\frac{n\,(n-1)}{2} = \frac{3n^2}{2}-\frac{3n}{2}+2 = O(n^2). \end{aligned}$$

Na vhodu potrebujemo vektor b dolžine n in matriko L dimenzije $n \times n$. Algoritem reši spodnje trikoten sistem $Ly = b$.

6

UVOD V TEORIJO ŠTEVIL

Osnova matematike so vsekakor števila in med njimi zagotovo, kot že ime pove, naravna števila, najbolj naraven predstavnik števil. Veliko raziskav je pokazalo, da otroci na začetku šolanja dajejo prednost matematiki pred ostalimi predmeti. Razlog za to zagotovo leži v naravnosti koncepta števil.

Kljub njihovi vseprisotnosti to še zdaleč ne pomeni, da o naravnih številih in njihovih negativnih sorodnikih, ki jim skupaj rečemo cela števila, vemo vse, kar bi želeli. Da ni nerešenih problemov, ki govorijo o teh številih. Da lahko, na koncu koncev, z njimi dovolj hitro računamo. Tako bomo v nadaljevanju pravzaprav spoznali osnovo, lahko bi rekli abecedo, teorije števil. Ta abeceda pravzaprav šele ponuja možnosti za ukvarjanje s težjimi rečmi, povezanimi s celimi števili.

V tem poglavju si bomo ogledali osnovne lastnosti celih števil z vidika deljivosti in relacij, ki iz tega izhajajo. Spoznali bomo pravila računanja glede na ostanek pri deljenju z nekim fiksnim naravnim številom n. Osnova tega poglavja bo nedvomno Evklidov algoritem oziroma njegov obrat, ki omogoča tudi reševanje linearnih enačb glede na ostanek pri deljenju z n. Te metode nato omogočajo kodiranje sporočil, kar je nedvomno pomembna tema v računalništvu.

Dodatno literaturo v slovenščini iz tega področja je moč najti v [7]. V angleškem jeziku je na voljo precej več primerne literature, tukaj omenimo le [6] in v manjšem obsegu [1]. Marsikaj je najti tudi na spletu in pogosto je že Wikipedia (angleška) dober začetni vir informacij. Veliko izpitnih nalog iz tega poglavja je najti v [12, 13].

6.1 DELJIVOST V CELIH ŠTEVILIH

Cilj tega razdelka je vpeljava relacije deli med cela števila in opis njenih lastnosti. Oboje nato privede do izreka o deljenju z ostankom, ki ga bomo veliko uporabljali v nadaljevanju in je osnova Evklidovega algoritma.

Naj bosta a in b celi števili. Rečemo, da a **deli** b, kar označimo z $a|b$, če obstaja celo število k, da velja $b = ka$. Tesno povezana je morda bolj znana terminologija, da je b **deljiv** z a, če obstaja celo število k, da velja $b = ka$, kar se običajno označi z $b : a = k$. Potrebno je omeniti, da je slednje pravzaprav operacija med celimi števili. Njena posplošitev na realna števila je pomembna v analizi realnih števil. Tukaj pa se bomo omejili na relacijo $a|b$. Oglejmo si njene lastnosti.

Trditev 6.1 *Za $a, b, c \in \mathbb{Z}$ veljajo naslednje trditve.*

(I) *Vsako celo število a deli $b = 0$.*

(II) *Število $a = 0$ ne deli poljubnega celega števila $b \neq 0$.*

(III) *Velja $a|b \Leftrightarrow (-a)|b \Leftrightarrow (-a)|(-b) \Leftrightarrow a|(-b)$.*

(IV) *Če $a|b$ in hkrati $b|a$, potem je $a = \pm b$.*

(V) *Če $a|b$ in hkrati $b|c$, potem tudi $a|c$.*

(VI) *Če $a|b$, potem tudi $a|xb$ za poljubno celo število x.*

(VII) *Če $a|b$ in hkrati $a|c$, potem $a|(bx + cy)$ za poljubni celi števili x in y.*

Dokaz. Pišemo lahko $b = 0 = 0 \cdot a = ka$, zato je (i) resnična. Če je $a = 0$, potem je $b \neq 0 = ka$ in (ii) sledi. Trditev (iii) je resnična, ker je $b = ka = (-k)(-a)$ in $-b = k(-a) = (-k)a = -(ka)$.

Za (iv) predpostavimo, da velja $a|b$ in $b|a$ (dokaz s pogojnim sklepom). To pomeni, da obstajata $k, \ell \in \mathbb{Z}$, da velja $b = ka$ in $a = \ell b$. Če a vstavimo v prvo zvezo, dobimo $b = k\ell b$, oziroma $b(1 - kl) = 0$. Ker $b|a$, je $b \neq 0$ zaradi (ii) in je zato $1 - k\ell = 0$. Skratka, iščemo celoštevilsko rešitev zveze $k\ell = 1$. Le-ta ima dve rešitvi in sicer $k = \ell = 1$ in $k = \ell = -1$. V prvem primeru je $a = b$ in v drugem je $a = -b$.

Tudi za (v) ponovno predpostavimo, da velja $a|b$ in $b|c$ (dokaz s pogojnim sklepom), kar pomeni obstoj $k, \ell \in \mathbb{Z}$, da velja $b = ka$ in $c = \ell b$. Ko prvi izraz vstavimo v drugega, dobimo $c = \ell ka$, kar pomeni da $a|c$, saj je $\ell k \in \mathbb{Z}$.

Zaradi pogojnega sklepa lahko predpostavimo za (vi), da velja $a|b$ oziroma $b = ka$ za nek $k \in \mathbb{Z}$. Če to zvezo pomnožimo s poljubnim celim številom x, dobimo $xb = xka$. Tako tudi $a|xb$, saj je $xk \in \mathbb{Z}$.

Za zadnjo trditev naj $a|b$ in $a|c$, kar pomeni, da je $b = ka$ in $c = \ell a$. Prvi izraz pomnožimo z x in drugega z y ter ju seštejemo, da dobimo $bx + cy = xka + y\ell a = (xk + y\ell)a$ in $a|(xk + y\ell)$. ∎

Izrek 6.2 (Deljenje z ostankom) *Naj bosta $a, b \in \mathbb{Z}$ in $b \neq 0$. Tedaj obstajata enolično določena $q, r \in \mathbb{Z}$, da velja $a = qb + r$ in $0 \leq r < |b|$, kjer je r ostanek, q pa količnik pri deljenju a z b.*

Dokaz. Predpostavimo lahko, da je $|a| > |b|$. Naj bo $A = \{a - bx : x \in \mathbb{Z} \wedge a - bx \geq 0\}$. Seveda je $A \subseteq \mathbb{N}_0$ zaradi drugega pogoja. Množica A je tudi neprazna. To lahko vidimo glede na predznak števil a in b. Če je $a \geq 0$, lahko z ustreznim predznakom x-a dobimo predstavnike v A. Če je $a < 0$, potem moramo uporabiti arhimedsko lastnost realnih števil[13] in s tem tudi celih, ki pa je na tem mestu ne bomo podrobneje omenjali. Vsaka navzdol omejena neprazna množica ima natančno spodnjo mejo $\inf A$, kar je posledica Dedekindovega aksioma (glej zgleda 2.15 in 2.18). Ker pa so v A le nenegativna števila, velja $\inf A = \min A$. Označimo z $r = \min A$. Seveda je $r \geq 0$. Naj bo $r = a - bq$ za nek $q \in \mathbb{Z}$. Če je $r \geq |b|$, potem je $r > r - |b| \geq 0$ in velja

$$r > r - |b| = a - bq + |b| = a - b(q \pm 1) \in A,$$

kar je protislovje, saj smo v množici A našli element, ki je manjši kot njen minimum r. Zato je $r < |b|$.

Pokažimo še enoličnost zapisa $a = qb + r$. Predpostavimo, da velja

$$a = qb + r = q'b + r'.$$

To lahko preoblikujemo v

$$(q - q')b = r' - r.$$

Če je $q \neq q'$, potem velja

$$|b| \leq |q - q'|b = |r' - r| < |b|,$$

kar ni mogoče. Zato je $q = q'$ in posledično tudi $r = r'$, s čimer je potrjena tudi enoličnost zapisa. ∎

Enoličen zapis $a = qb + r$, $0 \leq r < |b|$, lahko preoblikujemo v $a - r = qb$, kar pomeni da $b|(a - r)$. V nadaljevanju bomo za to uporabljali oznako $a \equiv r \pmod{b}$, kar preberemo a je **kongruentno** r po modulu b.

Zgled 6.1 *Naj bosta $|a| = 315$ in $|b| = 81$. Oglejmo si vse enolične zapise iz izreka o deljenju z ostankom glede na predznake števil a in b. Če je $a = 315$, potem velja $315 = 3 \cdot 81 + 72$, če je $b > 0$, in $315 = (-3) \cdot (-81) + 72$, ko je $b < 0$. Po drugi strani je v primeru, ko je $a = -315$, zapis najprej $-315 = -4 \cdot 81 + 9$ za $b > 0$ in $-315 = 4 \cdot (-81) + 9$. Opazimo lahko, da je ostanek različen glede na predznak a, vendar je v obeh primerih pozitiven.*

13 Arhimed iz Sirakuze (približno 287-212 pred našim štetjem) je bil starogrški znanstvenik znan po svoji bogati zapuščini. Med drugim slovi kot utemeljitelj matematično natančnega dokaza.

6.2 NAJVEČJI DELITELJ IN EVKLIDOV ALGORITEM

Bodita a in b celi števili, ki sta različni od nič. Največjemu naravnemu številu d, ki deli obe števili a in b, rečemo **največji skupni delitelj** števil a in b in ga označimo z $D(a,b)$. V tem razdelku se bomo posvetili učinkovitemu izračunu največjega skupnega delitelja, kar bomo storili z Evklidovim algoritmom. Najprej pokažimo njegov obstoj.

Trditev 6.3 *Največji skupni delitelj $D(a,b)$ obstaja za vsaki $a,b \in \mathbb{Z} - \{0\}$.*

Dokaz. Število skupnih deliteljev je navzgor omejeno z $\min\{|a|,|b|\}$, saj je delitelj celega števila največ enak absolutni vrednosti omenjenega števila. Množica A, ki vsebuje vse skupne delitelje števil a in b, je tudi neprazna, saj vsebuje 1. Vsaka neprazna navzgor omejena podmnožica realnih števil ima po Dedekindovem aksiomu natančno zgornjo mejo $\sup A$. Ker pa so v A le naravna števila, velja $\sup A = \max A$, ki je ravno $D(a,b)$. ∎

Naslednji rezultat nam prinaša koristen zapis največjega skupnega delitelja, ki hkrati poraja več uporabnih posledic.

Izrek 6.4 *Za $a,b \in \mathbb{Z} - \{0\}$ velja*

$$D(a,b) = \min\{ax + by : x,y \in \mathbb{Z} \wedge ax + by > 0\}.$$

Dokaz. Vpeljimo naslednje oznake $A = \{ax + by : x,y \in \mathbb{Z} \wedge ax + by > 0\}$, $m = \min A$ in $d = D(a,b)$. Ponovno lahko uvidimo, da je A neprazna podmnožica naravnih števil, če le ima x enak predznak kot a in ima y enak predznak kot b. Vsaka neprazna podmnožica naravnih števil pa vsebuje minimum kot smo povedali v dokazu izreka o deljenju z ostankom. Ker $d|a$ in $d|b$, tudi $d|(ax+by)$ za vsaka $x,y \in \mathbb{Z}$ po (vii) trditve 6.1. Torej $d|m$ in velja $d \leq m$, saj sta d in m naravni števili.

Pokažimo sedaj, da $m|a$. Naj bosta x_0 in y_0 tisti celi števili, da je $m = ax_0 + by_0$. Po izreku o deljenju z ostankom velja $a = qm + r$ za $0 \leq r < m$. Če je $r = 0$, smo končali. Sicer je $r > 0$ in imamo

$$r = a - qm = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0) = ax' + by'.$$

Torej je $r \in A$ in hkrati $r < m = \min A$, kar je nemogoče. Torej je $r = 0$ in $m|a$. Na enak način pokažemo, da tudi $m|b$. Tako je m skupni delitelj a in b. Po definiciji največjega skupnega delitelja je zato $m \leq d$. Oba neenačaja zagotavljata $m = d$ in izrek je dokazan. ∎

Celi števili a in b sta si **tuji**, če velja $D(a,b) = 1$. Če sta si a in b tuji, potem po izreku 6.4 obstajata $x,y \in \mathbb{Z}$, da velja $ax + by = 1$. Oglejmo si nekaj posledic izreka 6.4.

Posledica 6.5 *Za $a, b, c, e \in \mathbb{Z}$ in $d = D(a, b)$ veljajo naslednje trditve.*

(I) *Števili $\frac{a}{d}$ in $\frac{b}{d}$ sta si tuji: $D\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.*

(II) *Če $a|c$, $b|c$ in je $D(a, b) = 1$, potem tudi $(ab)|c$.*

(III) *Če $a|(bc)$ in je $D(a, b) = 1$, potem $a|c$.*

(IV) *Če $e|a$ in hkrati $e|b$, potem $e|d$.*

Dokaz. Glede (i) lahko po izreku 6.4 zapišemo $ax_0 + by_0 = d$. Če to zvezo delimo z d, potem dobimo $\frac{a}{d}x_0 + \frac{b}{d}y_0 = 1$ in po izreku 6.4 je $D\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Iz $D(a, b) = 1$ po izreku 6.4 sledi, da je $ax_0 + by_0 = 1$. To zvezo pomnožimo s c in dobimo

$$c = ax_0c + by_0c = ax_0kb + by_0\ell a = ab(kx_0 + \ell y_0).$$

Ob tem smo v drugem enačaju upoštevali preostali predpostavki $b|c$ in $a|c$. Kot vidimo, produkt ab deli c.

Ponovno lahko po izreku 6.4 zapišemo $ax_0 + by_0 = 1$ in to pomnožimo s c. Dobimo

$$c = ax_0c + by_0c = ax_0c + kay_0 = a(x_0c + ky_0),$$

s čimer smo dokazali (iii). Ob tem smo v drugem enačaju upoštevali preostalo predpostavko, da $a|(bc)$.

Za (iv) zadošča naslednji izračun

$$d = ax_0 + by_0 = kex_0 + \ell ey_0 = e(kx_0 + \ell y_0),$$

kjer smo v drugem enačaju upoštevali, da $e|a$ in $e|b$. ∎

V nadaljevanju bomo predstavili Evklidov algoritem in obrat Evklidovega algoritma, ki igrata veliko vlogo pri računanju največjega skupnega delitelja.

Evklidov algoritem je zaporedna uporaba izreka o deljenju z ostankom, dokler ni ostanek enak 0.

Ponazorimo Evklidov algoritem s simbolnim zapisom za celi števili a in b. Ostanke bomo zaporedoma označevali z $r_1, r_2, \ldots$ in količnike s $q_1, q_2, \ldots$. Tako imamo

$$\begin{array}{ccc}
a = q_1b + r_1 & 0 \le r_1 < b & \text{(nadaljujemo z } b \text{ in z } r_1\text{)} \\
b = q_2r_1 + r_2 & 0 \le r_2 < r_1 & \text{(nadaljujemo z } r_1 \text{ in z } r_2\text{)} \\
r_1 = q_3r_2 + r_3 & 0 \le r_3 < r_2 & \text{(nadaljujemo z } r_2 \text{ in z } r_3\text{)} \\
\vdots & \vdots & \vdots \\
r_{k-2} = q_kr_{k-1} + r_k & 0 \le r_k < r_{k-1} & \text{(nadaljujemo z } r_{k-1} \text{ in z } r_k\text{)} \\
r_{k-1} = q_{k+1}r_k + 0 & r_{k+1} = 0 & \text{(konec).}
\end{array} \tag{24}$$

Potrebno je omeniti, da Evklidov algoritem dejansko je algoritem in se zaključi po končno mnogo korakih. To se zgodi, ker je zaporedje ostankov strogo padajoče $r_1 > r_2 > \cdots > r_k > r_{k+1}$ in navzdol omejeno z 0. Po posledici Dedekindovega aksioma (zgled 2.18) obstaja natančna spodnja meja množice ostankov, ki je hkrati tudi minimum te množice, saj gre za naravna števila. Ta minimum je seveda 0 in algoritem se ustavi po končno mnogo korakih.

Tudi Evklidov algoritem je povezan z največjim skupnim deliteljem $D(a,b)$, kot je razvidno iz naslednjega rezultata.

Izrek 6.6 *Naj bosta $a, b \in \mathbb{Z} - \{0\}$ in $b \neq 0$ in naj bo r_k zadnji neničelni ostanek iz Evklidovga algoritma za a in b. Tedaj velja $D(a,b) = r_k$.*

Dokaz. Kot običajno vpeljemo oznako $d = D(a,b)$. Po definiciji d deli oba a in b. Najprej bomo z indukcijo pokazali, da d deli r_i. Za bazo najprej malo preoblikujemo prvo vrstico (24) in dobimo $r_1 = a - q_1 b$. Ker d deli a in b, seveda d deli tudi r_1 po lastnosti (vii) trditve 6.1. Podobno storimo z drugo vrstico (24) in dobimo $r_2 = b - q_2 r_1$. Ponovno d deli r_2, saj deli oba b in r_1 po lastnosti (vii) trditve 6.1, s čimer je baza indukcije zaključena. Po indukcijski predpostavki d deli oba r_{i-1} in r_{i-2}. Če ponovno preoblikujemo i-to vrstico (24), dobimo $r_i = r_{i-2} - q_i r_{i-1}$. Tako d deli tudi r_i ponovno po lastnosti (vii) trditve 6.1. V posebnem primeru, ko je $i = k$, imamo $d | r_k$.

Obratno bomo pokazali, da tudi r_k deli d. Iz zadnje vrstice (24) vidimo, da r_k deli r_{k-1}. Predzanja vrstica (24) nam potem razkrije, da r_k deli tudi $r_{k-2} = q_k r_{k-1} + r_k$ po lastnosti (vii) trditve 6.1. Isto lastnost uporabljamo tudi v naslednjih vrsticah in ugotovimo, da r_k deli vse ostanke $r_{k-3}, r_{k-4}, \ldots, r_1$ in na koncu tudi b in a. Tako je r_k skupni delitelj a in b in točka (iv) posledice 6.5 nam pove, da velja tudi $r_k | d$.

Tako imamo da $d | r_k$ in hkrati $r_k | d$, kar pomeni $d = \pm r_k$ po (iv) trditve 6.1. Ker sta oba d in tudi r_k naravni števili, velja $d = r_k$ in dokaz je zaključen. ∎

Če združimo izreka 6.4 in 6.6 vidimo, da za $a, b \in \mathbb{Z} - \{0\}$ obstaja naslednji zapis

$$D(a,b) = r_k = ax + by \text{ za neka } x, y \in \mathbb{Z}. \tag{25}$$

Ta zapis bo v nadaljevanju še koristen, zato si oglejmo postopek, ki nas pripelje do njega. Še pred tem pokažimo naslednjo lemo, kjer označimo $a = r_{-1}$ in $b = r_0$.

Lema 6.7 *Naj bosta $r_{-1}, r_0 \in \mathbb{Z} - \{0\}$ in $r_1, r_2, \ldots, r_k$ ostanki pri Evklidovem algoritmu za r_{-1} in r_0. Tedaj lahko r_k zapišemo v obliki $r_k = x r_i + y r_{i-1}$ za neka $x, y \in \mathbb{Z}$ in $i \in [k-1]_0$.*

Dokaz. Dokažimo to lemo z matematično indukcijo na $j = k-1-i$, kjer je $i \in [k-1]_0$. Opazimo lahko, da je tudi $j \in [k-1]_0$, vendar je $j = 0$ takrat, ko je $i = k-1$. Za $j = 0$ tako imamo $r_k = r_{k-2} - q_k r_{k-1}$, kar dobimo iz predzadnje vrstice (24). Naj bo sedaj $j > 0$, kar pomeni, da je $i < k-1$. Po indukcijski predpostavki velja $r_k = xr_{i+1} + yr_i$, medtem ko dobimo iz $(i+1)$-ve vrstice (24) zvezo $r_{i+1} = r_{i-1} - q_{i+1}r_i$. Le-to vstavimo v prejšnjo in dobimo

$$r_k = x(r_{i-1} - q_{i+1}r_i) + yr_i = xr_{i-1} + (y - q_{i+1})r_i = xr_{i-1} + y'r_i \text{ za neka } x, y' \in \mathbb{Z}$$

in lema je dokazana. ∎

Posebej poudarimo, kaj se zgodi, ko je $i = 0$ v prejšnji lemi, z naslednjo posledico.

Posledica 6.8 *Za $a, b \in \mathbb{Z} - \{0\}$ lahko s pomočjo Evklidovega algoritma poiščemo zapis $D(a,b) = xa + yb$.*

Dokaz. Če v lemi 6.7 uporabimo $j = k-1$, kar pomeni, da je $i = 0$, potem dobimo

$$r_k = D(a,b) = xa + yb \text{ za neka } x, y \in \mathbb{Z}$$

in dokaz je končan. ∎

Postopku, s katerim dobimo zapis $D(a,b) = xa + yb$ s pomočjo Evklidovega algoritma, rečemo **obrat Evklidovega algoritma**. Ob tem postopamo na naslednji način. Najprej izrazimo iz (24) vse ostanke $r_k, r_{k-1}, \ldots, r_1$ v tem vrstnem redu. Tako dobimo

$$\begin{aligned} r_k &= r_{k-2} - q_k r_{k-1} \\ r_{k-1} &= r_{k-3} - q_{k-1} r_{k-2} \\ r_{k-2} &= r_{k-4} - q_{k-2} r_{k-3} \\ &\vdots \\ r_2 &= b - q_2 r_1 \\ r_1 &= a - q_1 b \end{aligned} \quad . \tag{26}$$

Nato začnemo s prvo vrstico (26) in v njej nadomestimo r_{k-1} z zapisom iz druge vrstice (26) in dobimo

$$r_k = r_{k-2} - q_k r_{k-1} = r_{k-2} - q_k(r_{k-3} - q_{k-1}r_{k-2}) = (q_k q_{k-1} + 1)r_{k-2} - q_k r_{k-3}.$$

V zgornjem zapisu sedaj nadomestimo r_{k-2} s tretjo vrstico iz (26). Tako imamo

$$r_k = (1 + q_k q_{k-1})r_{k-2} - q_k r_{k-3} = (q_k q_{k-1} + 1)(r_{k-4} - q_{k-2}r_{k-3}) - q_k r_{k-3},$$

iz česar dobimo

$$r_k = (q_k q_{k-1} + 1)r_{k-4} - (q_k q_{k-1} q_{k-2} + q_{k-2} + q_k)r_{k-3}.$$

Sedaj lahko nadaljujemo tako, da nadomestimo r_{k-3} z zapisom iz četrte vrstice (26) in tako naprej. Ker je v (26) končno mnogo vrstic, se postopek na koncu ustavi, ko je r_k izražen v obliki

$$r_k = xr_{-1} + yr_0 = xa + yb \text{ za neka } x, y \in \mathbb{Z}.$$

Ob tem omenimo, da števil $r_{k-1}, r_{k-2}, \ldots, r_1$ ne smemo množiti s števili, ki jih dobimo zraven njih.

Zgled 6.2 *Za $a = 538$ in $b = 214$ poiščimo $D(a,b)$ in zapis oblike (25). Najprej izvedimo Evklidov algoritem, hkrati pa izrazimo tudi vsakokratni ostanek, kar potrebujemo za obrat Evklidovega algoritma:*

$$\begin{array}{ccc} 538 = 2 \cdot 214 + 110 & \Rightarrow & 110 = 538 - 2 \cdot 214 \\ 214 = 1 \cdot 110 + 104 & \Rightarrow & 104 = 214 - 1 \cdot 110 \\ 110 = 1 \cdot 104 + 6 & \Rightarrow & 6 = 110 - 1 \cdot 104 \\ 104 = 17 \cdot 6 + 2 & \Rightarrow & 2 = 104 - 17 \cdot 6 \\ 6 = 3 \cdot 2. & & \end{array}$$

Tako je $D(538, 214) = 2$. Za zapis (25) uporabimo obrat Evklidovega algoritma in začnemo z zadnjo vrstico v desnem stolpiču

$$2 = 104 - 17 \cdot 6,$$

kjer 6 nadomestimo z predzadnjo vrstico desnega stolpiča

$$2 = 104 - 17 \cdot (110 - 1 \cdot 104) = 18 \cdot 104 - 17 \cdot 110.$$

V dobljenem izrazu 104 nadomestimo z drugo vrstico desnega stolpiča in imamo

$$2 = 18 \cdot 104 - 17 \cdot 110 = 18 \cdot (214 - 1 \cdot 110) - 17 \cdot 110 = 18 \cdot 214 - 35 \cdot 110.$$

Za konec zamenjamo še 110 kot je predstavljeno v prvi vrstici desnega stolpiča in dobimo

$$2 = 18 \cdot 214 - 35 \cdot 110 = 18 \cdot 214 - 35 \cdot (538 - 2 \cdot 214) = 88 \cdot 214 - 35 \cdot 538.$$

Tako imamo $2 = 88 \cdot 214 - 35 \cdot 538$ in glede na zapis (25) lahko vidimo, da je $x = -35$ in $y = 88$. S tem je naloga zaključena, vendar se spomnimo še (i) posledice 6.5, iz katere je razvidno, da velja

$$D\left(\frac{538}{2}, \frac{214}{2}\right) = D(269, 107) = 1.$$

Tako sta si števili 269 in 107 tuji, zapis (25) pa je $1 = 88 \cdot 107 - 35 \cdot 269$ in vidimo, da sta $x = -35$ in $y = 88$ enaki kot prej.

Zgled 6.3 *Za $a = -648$ in $b = 412$ poiščimo $D(a,b)$ in zapis oblike (25). Zgled je podoben kot prejšnji, le da je a negativno število, kar pomeni nekaj previdnosti. Kot v prejšnjem zgledu najprej izvedemo Evklidov algoritem, hkrati pa izrazimo tudi vsakokratni ostanek, kar potrebujemo za obrat Evklidovega algoritma:*

$$\begin{array}{ccc} -648 = -2 \cdot 412 + 176 & \Rightarrow & 176 = -648 + 2 \cdot 412 \\ 412 = 2 \cdot 176 + 60 & \Rightarrow & 60 = 412 - 2 \cdot 176 \\ 176 = 2 \cdot 60 + 56 & \Rightarrow & 56 = 176 - 2 \cdot 60 \\ 60 = 1 \cdot 56 + 4 & \Rightarrow & 4 = 60 - 1 \cdot 56 \\ 56 = 14 \cdot 4. & & \end{array}$$

Tako je $D(-648, 412) = 4$. *Za zapis (25) uporabimo obrat Evklidovega algoritma in začnemo z zadnjo vrstico v desnem stolpiču*

$$4 = 60 - 1 \cdot 56,$$

kjer 56 *nadomestimo s predzadnjo vrstico desnega stolpiča*

$$4 = 60 - 1 \cdot (176 - 2 \cdot 60) = 3 \cdot 60 - 1 \cdot 176.$$

V dobljenem izrazu 60 *nadomestimo z drugo vrstico desnega stolpiča in imamo*

$$4 = 3 \cdot 60 - 1 \cdot 176 = 3 \cdot (412 - 2 \cdot 176) - 1 \cdot 176 = 3 \cdot 412 - 7 \cdot 176.$$

Za konec zamenjamo še 176 *kot je predstavljeno v prvi vrstici desnega stolpiča in dobimo*

$$4 = 3 \cdot 412 - 7 \cdot 176 = 3 \cdot 412 - 7 \cdot (-648 + 2 \cdot 412) = -7 \cdot (-648) - 11 \cdot 412.$$

Tako imamo $4 = -7 \cdot (-648) - 11 \cdot 412$ *in glede na zapis (25) lahko vidimo, da je* $x = -7$ *in* $y = -11$. *Ponovno uporabimo* (i) *posledice 6.5, iz katere je razvidno, da velja*

$$D\left(\frac{-648}{4}, \frac{412}{4}\right) = D(-162, 103) = 1.$$

Tako sta si števili -162 *in* 103 *tuji, zapis (25) pa je* $1 = -7 \cdot (-162) - 11 \cdot 103$ *in vidimo, da sta* $x = -7$ *in* $y = -11$ *enaki kot prej.*

Pokažimo še, da je Evklidov algoritem hiter algoritem.

Izrek 6.9 *Za* $a, b \in \mathbb{N}$, $b < a$, $a, b \leq m$ *in* $m \geq 8$ *potrebujemo v Evklidovem algoritmu za* a *in* b *največ* $\log_{3/2} \frac{2m}{3}$ *operacij deljenja.*

Dokaz. Pokažimo najprej, morda nepričakovano, povezavo s Fibonaccijevim zaporedjem (f_n). Z indukcijo pokažimo, da, če potrebujemo n operacij deljenja v Evklidovem algoritmu, potem velja $a \geq f_{n+2}$ in $b \geq f_{n+1}$. Za $n = 1$ je $f_2 = 1 \leq b$ in $f_3 = 2 \leq a$. Predpostavimo sedaj, da za a in b potrebujemo $n + 1$ operacij deljenja v Evklidovem algoritmu. Potem za b in r_1 potrebujemo n operacij deljenja in po indukcijski predpostavki velja $b \geq f_{n+2}$ in $r_1 \geq f_{n+1}$. Po izreku o deljenju z ostankom imamo

$$a = q_1 b + r_1 \geq b + r_1 \geq f_{n+2} + f_{n+1} = f_{n+3},$$

s čimer je indukcija zaključena.

Spomnimo se zgleda 2.5, kjer smo z uporabo posplošene indukcije pokazali, da velja $\left(\frac{3}{2}\right)^{n+1} < f_{n+2}$, $n \geq 4$. Tako je $\left(\frac{3}{2}\right)^{n+1} < m$, oziroma $n + 1 < \log_{3/2} m$, iz česar sledi

$$n < \log_{3/2} m - 1 = \log_{3/2} m - \log_{3/2} \frac{3}{2} = \log_{3/2} \frac{2m}{3}$$

in dokaz je zaključen. ∎

Ta izrek lahko uporabimo za določitev časovne zahtevnosti Evklidovega algoritma. Ker a in b nista večja od m, je velikost vhodnih podatkov za Evklidov algoritem $O(\lg m)$. Tako imamo

$$\log_{3/2} \frac{2m}{3} = \frac{\lg \frac{2m}{3}}{\lg \frac{3}{2}} = \frac{\lg m + \lg 2 - \lg 3}{\lg \frac{3}{2}} = A \lg m + B = O(\lg m),$$

za konstanti $A, B \in \mathbb{R}$. Dokazali smo naslednjo posledico.

Posledica 6.10 *Evklidov algoritem ima linearno časovno zahtevnost.*

6.3 OSNOVNO O PRAŠTEVILIH

Naravno število p je **praštevilo**, če ima p natanko dva različna delitelja p in 1. Praštevila, predvsem velika praštevila, igrajo pomembno vlogo v kriptografiji, ki je pomembna veja računalništva. V tem razdelku si bomo ogledali le nekaj osnovnih trditev o praštevilih.

Iz definicije je takoj razvidno, da število 1 ni praštevilo, saj ima le en delitelj in ne dveh različnih.

Trditev 6.11 *Če je p praštevilo, ki deli produkt ab, potem $p|a$ ali $p|b$.*

Dokaz. Ker je p praštevilo, je $D(p,a) \in \{1,p\}$. Če je $D(p,a) = p$, potem $p|a$ dokaz je končan. Sicer je $D(p,a) = 1$ in $p|b$ po (iii) posledice 6.5. ∎

Posledica 6.12 *Če je p praštevilo in $p|(a_1 a_2 \cdots a_k)$, potem obstaja $i \in [k]$, da $p|a_i$.*

Dokaz. Uporabimo indukcijo na $k \geq 2$. Če je $k = 2$, potem imamo trditev 6.11, ki je resnična. Zapišimo sedaj $a_1 a_2 \cdots a_k = a_1(a_2 \cdots a_k)$, kar je produkt dveh števil. Če je $D(p,a_1) = p$, potem $p|a_1$ in smo končali. Sicer je $D(p,a_1) = 1$ in $p|(a_2 \cdots a_k)$ po (iii) posledice 6.5. Po indukcijski predpostavki vemo, da obstaja $i \in [k] - \{1\}$, da $p|a_i$ in dokaz je končan. ∎

Naslednji izrek je vsem že dobro znan in ga navedimo brez dokaza.

Izrek 6.13 *Vsako naravno število razen* 1 *lahko zapišemo kot produkt praštevil do vrstnega reda natančno.*

Frazo do vrstnega reda natančno moramo razumeti tako da, recimo 18, lahko zapišemo kot

$$18 = 2 \cdot 3 \cdot 3 \text{ ali } 18 = 3 \cdot 2 \cdot 3 \text{ ali } 18 = 3 \cdot 3 \cdot 2.$$

Če želimo enolični zapis naravnega števila n, potem naj bodo $p_1, p_2, \ldots, p_k$ vsa različna praštevila za n iz zgornjega izreka, ki so razvrščena po velikosti $p_1 < p_2 < \cdots < p_k$. Z α_i, $i \in [k]$, označimo kolikokrat se praštevilo p_i pojavi v zapisu števila n v zgornjem izreku. Tako seveda velja, da je $\alpha_i \in \mathbb{N}$, za vsak $i \in [k]$. Potem lahko zapišemo

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

Ta zapis je enolično določen zaradi urejenosti praštevil v njem in ga imenujemo **kanonični zapis** števila n s potencami praštevil. Seveda si za poljubno naravno število želimo poiskati njegov kanonični zapis, vendar imajo algoritmi za to visoko časovno zahtevnost in še posebej pri velikih številih niso učinkoviti.

Po drugi strani lahko ta zapis uporabimo za eleganten matematični zapis nekaterih pojmov. Eden teh je **najmanjši skupni večkratnik** števil a in b, ki ga označimo z $v(a, b)$ in je najmanjše naravno število, ki ga delita obe števili a in b. Za to naj bodo $p_1, p_2, \ldots, p_k$ vsa praštevila, ki nastopajo bodisi v kanoničnem zapisu za $a \in \mathbb{N}$ bodisi v kanoničnem zapisu za $b \in \mathbb{N}$. Potem lahko zapišemo

$$\begin{aligned} a &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},\ \alpha_i \in \mathbb{N}_0 \text{ za vsak } i \in [k], \\ b &= p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},\ \beta_i \in \mathbb{N}_0 \text{ za vsak } i \in [k]. \end{aligned}$$

Ob tem poudarimo, da če recimo p_i nastopa le v kanoničnem zapisu števila a, ne pa tudi v kanoničnem zapisu števila b, potem je $\alpha_i > 0$ in $\beta_i = 0$. Dodatno označimo še

$$M_i = \max\{\alpha_i, \beta_i\} \text{ in } m_i = \min\{\alpha_i, \beta_i\} \text{ za vsak } i \in [k].$$

Sedaj ni težko videti, da velja

$$\begin{aligned} v(a, b) &= p_1^{M_1} p_2^{M_2} \cdots p_k^{M_k}, \\ D(a, b) &= p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}. \end{aligned} \tag{27}$$

Da a in b oba delita $v(a, b)$, lahko sedaj opazimo že s krajšanjem ulomkov. Prav tako je očitno, iz enakega razloga, da ne obstaja manjše število, ki ga delita oba a in b. Podoben razmislek velja tudi za $D(a, b)$. Je pa iz teh dveh zapisov razvidno tudi naslednje

$$ab = D(a, b)v(a, b).$$

Oglejmo si še veljavnost distributivnosti za največji skupni delitelj in najmanjši skupni večkratnik. Za dokaz tega potrebujemo najprej dokaz distributivnosti za maksimum in minimum.

Trditev 6.14 *Enakosti* $\min\{\alpha, \max\{\beta, \gamma\}\} = \max\{\min\{\alpha, \beta\}, \min\{\alpha, \gamma\}\}$ *in* $\max\{\alpha, \min\{\beta, \gamma\}\} = \min\{\max\{\alpha, \beta\}, \max\{\alpha, \gamma\}\}$ *veljata za vsa* $\alpha, \beta, \gamma \in \mathbb{R}$.

Dokaz. Označimo $L = \min\{\alpha, \max\{\beta, \gamma\}\}$ in $D = \max\{\min\{\alpha, \beta\}, \min\{\alpha, \gamma\}\}$. Sedaj analizirajmo L in D glede na urejenost števil α, β in γ. Ni težko videti, da v primeru $\beta \leq \gamma \leq \alpha$ velja $L = \gamma = D$ in v primeru $\gamma \leq \beta \leq \alpha$ velja $L = \beta = D$. V vseh preostalih primerih je $L = \alpha = D$ in prva enakost drži. Na podoben način dokažemo tudi drugo enakost. ∎

Omenimo, da zgornja trditev velja tudi v primeru, ko so α, β in γ naravna števila, kar bomo uporabili v naslednji trditvi.

Trditev 6.15 *Za vsa naravna števila a, b, c velja $D(a, v(b, c)) = v(D(a, b), D(a, c))$ in $v(a, D(b, c)) = D(v(a, b), v(a, c))$.*

Dokaz. Zapišimo najprej a, b in c v obliki $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ in $c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$ $\alpha_i, \beta_i, \gamma_i \in \mathbb{N}_0$ za vsak $i \in [k]$. Če uporabimo (27), dobimo

$$D(\alpha, v(b, c)) = p_1^{\min\{\alpha_1, \max\{\beta_1, \gamma_1\}\}} \cdots p_k^{\min\{\alpha_k, \max\{\beta_k, \gamma_k\}\}}$$

in

$$v(D(a, b), D(a, c)) = p_1^{\max\{\min\{\alpha_1, \beta_1\}, \min\{\alpha_1, \gamma_1\}\}} \cdots p_k^{\max\{\min\{\alpha_k, \beta_k\}, \min\{\alpha_k, \gamma_k\}\}}.$$

Po trditvi 6.14 so potence pri vsakem praštevilu p_i, $i \in [k]$, enake in velja $D(\alpha, v(b, c)) = v(D(a, b), D(a, c))$. Na podoben način dokažemo tudi drugo enakost. ∎

Za konec si oglejmo še dve trditvi, ki razkrivata težavnost razporeditve praštevil med naravnimi števili.

Trditev 6.16 *Praštevil je neskončno mnogo.*

Dokaz. Predpostavimo nasprotno, da so $p_1, p_2, \ldots, p_k$ vsa različna praštevila in jih je torej končno mnogo. Naj bo $a = p_1 p_2 \ldots p_k$. Število $a + 1$ ni praštevilo, saj je večje od vseh praštevil. Zato obstaja $i \in [k]$, da $p_i | (a + 1)$. Seveda p_i deli tudi a. Tako imamo $p_i | (a + 1 - a) = 1$, kar ni mogoče, saj je $p_i > 1$. Torej je praštevil neskončno mnogo. ∎

Trditev 6.17 *Obstaja poljubno velik interval naravnih števil brez praštevil.*

Dokaz. Oglejmo si interval naravnih števil

$$[n! + 2, n! + n] = \{n! + 2, n! + 3, \ldots, n! + n\},$$

ki ima dolžino $n - 1$. Ob tem $2 | (n! + 2), 3 | (n! + 3), \ldots, n | (n! + n)$, torej noben element tega intervala ni praštevilo. Ker je n poljubno veliko število, je tudi interval poljubno velik. ∎

6.4 LINEARNE KONGRUENCE

Naj bosta $a, b \in \mathbb{Z}$ in $n \in \mathbb{N}$. Kot že omenjeno, je a **kongruentno** b po **modulu** n, če velja, da n deli njuno razliko $a - b$. Definicijo kongruentnost števil a in b po modulu n s simboli predstavimo z

$$a \equiv b \pmod{n} \Leftrightarrow n|(a-b).$$

Če za a in n ter b in n uporabimo izrek o deljenju z ostankom, dobimo $a = qn + r$ in $b = q'n + r'$, kjer sta $r, r' < n$. Tako je razlika

$$a - b = qn + r - q'n + r' = (q - q')n + r - r'.$$

Ker n deli to razliko, velja $(q - q')n + r - r' = \ell n$ za nek $\ell \in \mathbb{Z}$, oziroma $(q - q' - \ell)n = r' - r$. Če je $q - q' - \ell \neq 0$, potem je $|(q - q' - \ell)n| \geq n$ in $|r' - r| < n$, kar ni mogoče. Tako je $q - q' - \ell = 0$, kar pomeni tudi, da je $r = r'$. Tako imata dve med seboj kongruentni števili po modulu n enak ostanek pri deljenju z n. Zaradi tega pogosto računanju s kongurencami, ki bo predstavljeno v nadaljevanju, pravimo tudi računanje z ostanki pri deljenju z n.

Zgled 6.4 *Za $n = 5$ si oglejmo, katera števila so kongruentna med seboj. Za dosego tega si izberimo fiksno število in poglejmo, katera števila so kongruentna z njim po modulu 5. To lahko zapišemo v obliki $x \equiv k \pmod{5}$, kjer je k izbrano število, x se pa, kot običajno, lahko spreminja. Naj bo najprej $k = 0$. Tako imamo $x \equiv 0 \pmod{5}$, oziroma $5|(x - 0) = x$. Po definiciji deljivosti lahko zapišemo $x = 5t$ za poljuben $t \in \mathbb{Z}$. Torej je rešitev v primeru $k = 0$ vsako število iz množice*

$$A_{k=0} = \{5t : t \in \mathbb{Z}\} = \{0, \pm 5, \pm 10, \pm 15, \ldots\}.$$

Izberimo sedaj poljubno število, ki ni iz množice A_0, recimo $k = 1$. Tako imamo $x \equiv 1 \pmod{5}$, oziroma $5|(x - 1)$ in velja $x - 1 = 5t$ za poljuben $t \in \mathbb{Z}$. Seveda je $x = 5t + 1$ in je rešitev za $k = 1$ vsako število iz množice

$$A_{k=1} = \{5t + 1 : t \in \mathbb{Z}\} = \{1, -4, 6, -9, 11, -14, 16, \ldots\}.$$

Naslednje število, ki ni iz $A_0 \cup A_1$, je $k = 2$. Po že videni proceduri imamo $x \equiv 2 \pmod{5}$, oziroma $5|(x - 2)$ in velja $x - 2 = 5t$ za poljuben $t \in \mathbb{Z}$. Seveda je $x = 5t + 2$ in množica

$$A_{k=2} = \{5t + 2 : t \in \mathbb{Z}\} = \{2, -3, 7, -8, 12, -13, 17, \ldots\}$$

je rešitev za $k = 2$. Sedaj je vzorec že dobro razviden in brez težav uvidimo, da je

$$A_{k=3} = \{5t + 3 : t \in \mathbb{Z}\} = \{3, -2, 8, -7, 13, -12, 18, \ldots\}$$

rešitev za $k = 3$ oziroma $x \equiv 3 \pmod{5}$ in množica

$$A_{k=4} = \{5t + 4 : t \in \mathbb{Z}\} = \{4, -1, 9, -6, 14, -11, 19, \ldots\}$$

predstavlja rešitev za $k = 4$ *oziroma* $x \equiv 4 \pmod 5$. *S tem lahko nadaljujemo, vendar takoj uvidimo, da velja* $A_{k=0} = A_{k=5t}$, $A_{k=1} = A_{k=5t+1}$, $A_{k=2} = A_{k=5t+2}$, $A_{k=3} = A_{k=5t+3}$ *in* $A_{k=4} = A_{k=5t+4}$. *Iz množic* $A_{k=i}$ *lahko tudi razvidimo, da so v njih sama števila, ki imajo enak ostanek pri deljenju s* 5.

Posvetimo se sedaj lastnostim kongruenc, ki nam omogočajo preprosto in hitro računanje z njimi.

Trditev 6.18 *Za* $a, b, c, d \in \mathbb{Z}$ *in* $k, n \in \mathbb{N}$ *veljajo naslednje lastnosti.*

(I) $a \equiv a \pmod n$.

(II) *Če je* $a \equiv b \pmod n$, *potem je tudi* $b \equiv a \pmod n$.

(III) *Če je* $a \equiv b \pmod n$ *in* $b \equiv c \pmod n$, *potem je tudi* $a \equiv c \pmod n$.

(IV) *Če je* $a \equiv b \pmod n$ *in* $c \equiv d \pmod n$, *potem je tudi* $a + c \equiv b + d \pmod n$.

(V) *Če je* $a \equiv b \pmod n$, *potem je tudi* $a + c \equiv b + c \pmod n$.

(VI) *Če je* $a \equiv b \pmod n$ *in* $c \equiv d \pmod n$, *potem je tudi* $ac \equiv bd \pmod n$.

(VII) *Če je* $a \equiv b \pmod n$, *potem je tudi* $ac \equiv bc \pmod n$.

(VIII) *Če je* $a \equiv b \pmod n$, *potem je tudi* $a^k \equiv b^k \pmod n$.

Dokaz. Seveda $n|0 = a - a$ po (i) trditve 6.1 in (i) je resnična. Če je $a \equiv b \pmod n$, potem po definiciji $n|(a - b)$. Po točki (iii) trditve 6.1 $n| - (a - b) = b - a$ in tako je tudi $b \equiv a \pmod n$ in (ii) je izpolnjena. Za (iii) naj velja $a \equiv b \pmod n$ in $b \equiv c \pmod n$. Tako $n|(a - b)$ in $n|(b - c)$. Po definiciji deljivosti obstajata $s, t \in \mathbb{Z}$, da velja $a - b = sn$ in $b - c = tn$. Če zadnja izraza seštejemo, dobimo $a - c = (s + t)n$, oziroma $n|(a - c)$. Seveda to pomeni tudi, da je $a \equiv c \pmod n$, kar zaključuje (iii).

Za (iv) predpostavimo, da velja $a \equiv b \pmod n$ in $c \equiv d \pmod n$, oziroma $n|(a - b)$ in $n|(c - d)$. Tako obstajata $s, t \in \mathbb{Z}$, da velja $a - b = sn$ in $c - d = tn$. Če ponovno seštejemo zadnja izraza, dobimo $(s + t)n = a - b + c - d = (a + c) - (b + d)$, kar pomeni, da $n|((a + c) - (b + d))$. V jeziku kongruenc to prinese $a + c \equiv b + d \pmod n$ in (iv) velja. Lastnost (v) dobimo, če v lastnosti (iv) upoštevamo, da je $c \equiv c \pmod n$ po lastnosti (i).

Tudi za (vi) ponovno predpostavimo, da velja $a \equiv b \pmod n$ in $c \equiv d \pmod n$, kar pomeni obstoj $s, t \in \mathbb{Z}$, da velja $a - b = sn$ in $c - d = tn$. Izraza sedaj najprej preoblikujemo v $a = b + sn$ in $c = d + tn$ in ju zmnožimo. Tako dobimo

$$ac = bd + btn + dsn + stn^2$$

oziroma

$$ac - bd = (bt + ds + stn)n.$$

Tako $n|(ac-bd)$, oziroma $ac \equiv bd \pmod{n}$. Lastnost (vii) dobimo, če v lastnosti (vi) upoštevamo, da je $c \equiv c \pmod{n}$ po lastnosti (i).

Zadnjo lastnost dobimo iz lastnosti (vi), kjer nadomestimo $c = a$ in $d = b$, ter uporabimo indukcijo na k. ∎

Omenimo, da so nekatere lastnosti iz zgornje trditve že znane iz računanja z enačbami. Tako lahko lastnost (v) interpretiramo kot prištevanje enakega števila na obeh straneh, kar poznamo tudi pri enačbah. Podobno je z lastnostjo (vii), kjer seštevanje nadomestimo z množenjem, pa tudi z lastnostjo $(viii)$. Po drugi strani pa lastnosti (iv) in (vi) v primeru, ko je $c \neq d$, prinašata možnosti, ki pri enačbah ne veljajo. Tako imamo pri računanju s kongruencami več možnosti kot pri manipuliranju z enačbami. Ob tem se lahko vprašamo, kako je s krajšanjem oziroma deljenjem med kongruencami. Naslednja trditev nas seznani, da je v primeru deljenja pri kongruencah potrebna večja previdnost, kot pri enačbah.

Trditev 6.19 *Naj bodo $a, b, c \in \mathbb{Z}$, $n \in \mathbb{N}$ in $d = D(c, n)$. Če velja $ac \equiv bc \pmod{n}$, potem je $a \equiv b \pmod{\frac{n}{d}}$.*

Dokaz. Naj bo $ac \equiv bc \pmod{n}$, kar pomeni, da je $(a-b)c = kn$ za nek $k \in \mathbb{Z}$. Če delimo ta izraz z $d = D(c, n)$, dobimo $(a-b) \cdot \frac{c}{d} = k \cdot \frac{n}{d}$, kjer sta $\frac{c}{d}, \frac{n}{d} \in \mathbb{Z}$. Vidimo, da $\frac{c}{d} | \left(k \cdot \frac{n}{d}\right)$ in ob tem velja $D\left(\frac{c}{d}, \frac{n}{d}\right) = 1$. Po točki (iii) posledice 6.5 $\frac{c}{d} | k$ in je $\frac{k}{\frac{c}{d}} \in \mathbb{Z}$. Vrnimo se k izrazu $(a-b) \cdot \frac{c}{d} = k \cdot \frac{n}{d}$, ki ga delimo s $\frac{c}{d}$ in dobimo $a - b = \frac{k}{\frac{c}{d}} \cdot \frac{n}{d}$. Tako $\frac{n}{d} | (a-b)$ in rezultat $a \equiv b \pmod{\frac{n}{d}}$ sledi. ∎

Deljenje kongruenc se poenostavi v primeru, ko je število, s katerim delimo, tuje modulu. O tem govori naslednja neposredna posledica trditve 6.19.

Posledica 6.20 *Naj bodo $a, b, c \in \mathbb{Z}$, $n \in \mathbb{N}$ in $D(c, n) = 1$. Če velja $ac \equiv bc \pmod{n}$, potem je $a \equiv b \pmod{n}$.*

Opremljeni z vsemi lastnostmi računanja s kongruencami se lahko sedaj posvetimo glavni temi tega razdelka, po kateri se le-ta tudi imenuje. Zvezi

$$az \equiv b \pmod{n}, a, b \in \mathbb{Z}, n \in \mathbb{N} \tag{28}$$

rečemo **linearna kongruenca**. Seveda je z v linearni kongruenci spremenljivka in **rešitev linearne kongruence** je vsako celo število z, za katero je linearna kongruenca resnična. Ob tem je na mestu vprašanje, ali rešitev linearne kongruence sploh obstaja? Res, kot bomo videli, takšna rešitev ne obstaja vedno, a gremo lepo po vrsti. Glede na lastnost (vii) trditve 6.18 zadošča poiskati takšen $a' \in \mathbb{Z}$, da velja $a'a \equiv 1 \pmod{n}$. Če namreč z a' pomnožimo (28), potem dobimo

$$a'az \equiv a'b \pmod{n},$$

kar se poenostavi v iskano rešitev

$$z \equiv a'b \pmod{n},$$

ponovno zaradi lastnosti (vii) trditve 6.18. Tako smo z nekaj preprostimi argumenti iskanje rešitve linearne kongruence (28) preobrazili v iskanje a' v zvezi $a'a \equiv 1 (\mathrm{mod}\ n)$. Zaradi pomembnosti a' mu rečemo **inverz števila** a **po modulu** n ali kar na kratko **inverz**, če je jasno, kaj sta a in n.

Kot smo že omenili, a' ne obstaja vedno, a ga lahko, po drugi strani, pogosto preprosto uganemo, če le obstaja. To velja še toliko bolj, če je modul n dovolj majhno število. Če nam ugibanje ne steče, ali je n preprosto prevelik, potem upoštevamo, da $n|(a'a-1)$. To pomeni, da obstaja $k \in \mathbb{Z}$, za katerega velja $kn = a'a - 1$, oziroma

$$a'a - kn = 1.$$

Ta oblika zelo spominja na zapis (25), v katerem b zamenjamo z n, in je

$$xa + yn = D(a,n),$$

dobimo pa ga z obratom Evklidovega algoritma. (Seveda morajo veljati povezave $x = a'$, $y = -k$ in $D(a,n) = 1$.) Tako velja za tuji si števili a in n, kar pomeni $D(a,n) = 1$, da je rešitev linearne kongruence (28) enaka $z \equiv xb \pmod{n}$, kjer x preberemo iz zapisa $xa + yn = 1$, ki ga dobimo z obratom Evklidovega algoritma.

Kako pa postopamo, če je $d = D(a,n) > 1$? Potem sta si $\frac{a}{d}$ in $\frac{n}{d}$ tuji in velja $D\left(\frac{a}{d}, \frac{n}{d}\right) = 1$. S pomočjo obrata Evklidovega algoritma dobimo zapis

$$x \cdot \frac{a}{d} + y \cdot \frac{n}{d} = 1,$$

ki po trditvi 6.19 ustreza linearni kongruenci

$$\frac{a}{d} z \equiv \frac{b}{d} \pmod{\frac{n}{d}}.$$

Ob tem mora biti izpolnjen pogoj, da je $\frac{b}{d} \in \mathbb{Z}$, kar se zgodi le, če $d|b$. Dokazali smo naslednji izrek.

Izrek 6.21 *Linearna kongruenca $az \equiv b \pmod{n}$ ima rešitev natanko tedaj, ko $d|b$ za $d = D(a,n)$. V tem primeru je rešitev $z \equiv \frac{b}{d} x \pmod{\frac{n}{d}}$, kjer zapis $x \cdot \frac{a}{d} + y \cdot \frac{n}{d} = 1$ dobimo s pomočjo obrata Evklidovega algoritma.*

Zgled 6.5 *Poiščimo rešitev linearne kongruence*

$$30z \equiv 12 \pmod{42}.$$

Najprej potrebujemo $d = D(30,42)$, da preverimo, ali rešitev sploh obstaja. Ker sta števili dovolj majhni, lahko d preprosto uganemo brez uporabe Evklidovega algoritma. Tako je $d = 6$ in, ker $d|12$, rešitev podane linearne kongruence obstaja. Najprej delimo podano linearno kongruenco z $d = 6$ v skladu s trditvijo 6.19 in dobimo

$$5z \equiv 2 \pmod{7}. \tag{29}$$

Ker je modul majhno število, poskusimo uganiti inverz števila 5 *po modulu* 7*. Vprašanje, ki si ga moramo zastaviti, je, s katerim številom moramo pomnožiti* 5*, da bo imel zmnožek pri deljenju s* 7 *ostanek* 1*. Ni težko uvideti, da je to število* 3*. Z njim pomnožimo (29) in dobimo*

$$z \equiv 6 \pmod 7,$$

kar predstavlja rešitev podane linearne kongruence.

Zgled 6.6 *Poiščimo rešitev linearne kongruence*

$$538z \equiv 4 \pmod{214}.$$

Ponovno najprej potrebujemo $d = D(538, 214)$*. Spomnimo se, da smo* d *že izračunali v zgledu 6.2 in velja* $d = 2$*. Ker* $d|4$*, rešitev ponovno obstaja. Spet najprej delimo podano linearno kongruenco z* 2 *in dobimo*

$$269z \equiv 2 \pmod{107}.$$

Preden uporabimo obrat Evklidovega algoritma, linearno kongruenco še problikujemo v

$$55z \equiv 2 \pmod{107},$$

saj velja $269 \equiv 55 \pmod{107}$*. Sedaj imamo po Evklidovem algoritmu*

$$\begin{aligned} 107 &= 1 \cdot 55 + 52 \quad &\Rightarrow \quad 52 &= 107 - 1 \cdot 55 \\ 55 &= 1 \cdot 52 + 3 \quad &\Rightarrow \quad 3 &= 55 - 1 \cdot 52 \\ 52 &= 17 \cdot 3 + 1 \quad &\Rightarrow \quad 1 &= 52 - 17 \cdot 3. \end{aligned}$$

Dokončajmo še obrat Evklidovega algoritma. Najprej z drugo vrstico dobimo

$$1 = 52 - 17 \cdot 3 = 52 - 17 \cdot (55 - 1 \cdot 52) = 18 \cdot 52 - 17 \cdot 55.$$

Z uporabo prve vrstice tako dobimo

$$1 = 18 \cdot 52 - 17 \cdot 55 = 18(107 - 1 \cdot 55) - 17 \cdot 55 = 18 \cdot 107 - 35 \cdot 55,$$

s čimer smo dobili zapis oblike (25)

$$1 = 18 \cdot 107 - 35 \cdot 55.$$

Za rešitev dane linearne kongruence potrebujemo število $x = -35$*. Po izreku 6.21 velja*

$$z \equiv 2 \cdot (-35) \equiv -70 \equiv 37 \pmod{107}.$$

Ta razdelek bomo zaključili z **Diofantskimi enačbami**, ki imajo naslednjo obliko

$$ax + by = c,\ a, b, c \in \mathbb{Z}.$$

Rešitev Diofantske enačbe je vsak par celih števil (x_0, y_0), za katerega drži zgornja zveza. Diofantske[14] enačbe imajo tudi lepo geometrijsko predstavitev. Sama Diofantska enačba predstavlja implicitni zapis premice v ravnini. Tako nam rešitev Diofanske enačbe pove, ali premica s celo številskimi koeficienti v implicitnem zapisu vsebuje kako točko s celo številskimi koordinatami (x_0, y_0). Kot bomo videli, rešitev za Diofantske enačbe ne obstaja vedno in je zelo povezana z linearnimi kongruencami.

Označimo najprej z $d = D(a, b)$. Tako je $D(\frac{a}{d}, \frac{b}{d}) = 1$ po točki (i) posledice 6.5 in z obratom Evklidovega algoritma lahko poiščemo zapis oblike (25)

$$x_0 \cdot \frac{a}{d} + y_0 \cdot \frac{b}{d} = 1.$$

Preoblikujmo sedaj Diofantsko enačbo v naslednjo obliko

$$ax = c - by,$$

iz česar je razvidno, da a deli razliko $c - by$. To je pravzaprav definicija kongruence in imamo

$$by \equiv c \pmod{a}.$$

Ta linearna kongruenca ima rešitev po izreku 6.21 natanko tedaj, ko $d|c$, sama rešitev pa je

$$y \equiv \frac{c}{d} y_0 \pmod{a}.$$

Ker x in y v Diofantski enačbi nastopata simetrično, lahko postopek ponovimo in izrazimo by:

$$by = c - ax,$$

Ponovno imamo linearno kongruenco

$$ax \equiv c \pmod{b},$$

ki ima rešitev po izreku 6.21 natanko tedaj, ko $d|c$, sama rešitev pa je

$$x \equiv \frac{c}{d} x_0 \pmod{b}.$$

Tako nam izrek 6.21 zagotavlja rešitev Diofantske enačbe v primeru, ko $d|c$ in v tem primeru je ena izmed rešitev $(\frac{c}{d} x_0, \frac{c}{d} y_0)$. Vendar to ni edina rešitev, kot nam zagotavlja naslednji izrek.

14 Diofant Aleksandrijski (med 201-215-med 285-299) je bil antični grški matematik, ki se je ukvarjal z enačbami, katere vse niso imele rešitve.

Izrek 6.22 *Naj bodo $a, b, c \in \mathbb{Z}$ in $d = D(a, b)$. Diofantska enačba $ax + by = c$ ima množico rešitev*

$$R = \left\{ \left(\frac{c}{d}x_0 - \frac{b}{d}t, \frac{c}{d}y_0 + \frac{a}{d}t \right) : t \in \mathbb{Z} \right\},$$

natanko tedaj, ko $d|c$, kjer je zapis $x_0 \cdot \frac{a}{d} + y_0 \cdot \frac{b}{d} = 1$ pridobljen z obratom Evklidovega algoritma.

Dokaz. Vemo že, da če d ne deli c, potem rešitev ne obstaja po izreku 6.21. Če obratno $d|c$, potem smo pokazali, da je ena rešitev $(\frac{c}{d}x_0, \frac{c}{d}y_0)$. Pokažimo, da je potem rešitev tudi $\left(\frac{c}{d}x_0 - \frac{b}{d}t, \frac{c}{d}y_0 + \frac{b}{d}t\right)$ za vsak $t \in \mathbb{Z}$. Račun

$$\begin{aligned} a\left(\frac{c}{d}x_0 - \frac{b}{d}t\right) + b\left(\frac{c}{d}y_0 + \frac{a}{d}t\right) &= a\frac{c}{d}x_0 + b\frac{c}{d}y_0 - a\frac{b}{d}t + b\frac{a}{d}t = \\ c\left(\frac{a}{d}ax_0 + \frac{b}{d}y_0\right) + \frac{t}{d}(-ab + ba) &= c \cdot 1 + 0 = c, \end{aligned}$$

nam zagotavlja, da so elementi iz R dejansko rešitve podane Diofantske enačbe.

Pokažimo še, da ni nobenih drugih rešitev. Za to si oglejmo dve različni rešitvi Diofantske enačbe

$$ax_1 + by_1 = c = ax_2 + by_2.$$

Ta zapis lahko preoblikujemo v

$$\frac{a}{d}(x_1 - x_2) = \frac{b}{d}(y_2 - y_1).$$

Ker velja $D(\frac{a}{d}, \frac{b}{d}) = 1$, potem $\frac{a}{d}|(y_2 - y_1)$ in $\frac{b}{d}|(x_1 - x_2)$ po točki (iii) posledice 6.5. Tako obstaja $t \in \mathbb{Z}$, da je $\frac{b}{d}t = x_1 - x_2$ in $\frac{a}{d}t = y_2 - y_1$, kar pripelje do $x_2 = x_1 - \frac{b}{d}t$ in $y_2 = y_1 + \frac{a}{d}t$, s čimer je dokaz končan. ∎

Zgled 6.7 *Diofantska enačba $38x + 14y = 1$ nima rešitve, saj $d = D(38, 14) = 2$ ne deli $c = 1$.*

Zgled 6.8 *Diofantska enačba $38x + 14y = 4$ ima rešitev, saj $d = D(38, 14) = 2$ deli $c = 4$. Delimo Diofantsko enačbo z 2 in poiščimo zapis $x_0 \cdot \frac{a}{d} + y_0 \cdot \frac{b}{d} = 1$ s pomočjo obrata Evklidovega algoritma:*

$$\begin{aligned} 19 = 2 \cdot 7 + 5 \quad &\Rightarrow \quad 5 = 19 - 2 \cdot 7 \\ 7 = 1 \cdot 5 + 2 \quad &\Rightarrow \quad 2 = 7 - 1 \cdot 5 \\ 5 = 2 \cdot 2 + 1 \quad &\Rightarrow \quad 1 = 5 - 2 \cdot 2. \end{aligned}$$

Izrazimo

$$1 = 5 - 2(7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7 = 3(19 - 2 \cdot 7) - 2 \cdot 7 = 3 \cdot 19 - 8 \cdot 7.$$

Rešitev je sedaj

$$R = \{(6 - 7t, -16 + 19t) : t \in \mathbb{Z}\}.$$

6.5 SISTEMI LINEARNIH KONGRUENC Z ENO NEZNANKO

V tem razdelku si bomo ogledali kako poiskati rešitev več linearnih kongruenc hkrati. Pri tem imamo v mislih naslednje:

$$\begin{aligned} a_1 z &\equiv b_1 \pmod{m_1} \\ a_2 z &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_k z &\equiv b_k \pmod{m_k}. \end{aligned} \tag{30}$$

Če želimo poiskati rešitev za vse linearne kongruence iz (30), potem mora najprej obstajati rešitev za vsako linearno kongruenco sistema (30) posebej. Po izreku 6.21 ima linearna kongruenca

$$a_i z \equiv b_i \pmod{m_i}, i \in [k],$$

rešitev natanko tedaj, ko $d_i = D(a_i, m_i)$ deli b_i. V tem primeru je rešitev

$$z \equiv c_i \pmod{n_i},$$

kjer sta $c_i = \frac{b_i}{d_i} x_i$ in $n_i = \frac{m_i}{d_i}$, pri tem zapis $x_i \cdot \frac{a_i}{d_i} + y_i \cdot \frac{m_i}{d_i} = 1$ dobimo z obratom Evklidovega algoritma za vsak $i \in [k]$. Če vsako linearno kongruenco sistema (30) rešimo na ta način, dobimo sistem

$$\begin{aligned} z &\equiv c_1 \pmod{n_1} \\ z &\equiv c_2 \pmod{n_2} \\ &\vdots \\ z &\equiv c_k \pmod{n_k}. \end{aligned} \tag{31}$$

Seveda je rešitev sistema (31) hkrati tudi rešitev sistema (30). Zato se bomo v nadaljevanju posvetili reševanju sistema (31). Preden poiščemo rešitev, si oglejmo še nekaj oznak, ki jih bomo pri tem uporabili. Najprej vpeljimo

$$n = n_1 n_2 \cdots n_k = \Pi_{i=1}^{k} n_i,$$

kar je produkt vseh modulov sistema (31). Nadaljujemo s produkti vseh modulov razen enega, i-tega. To označimo z

$$N_i = \frac{n}{n_i}, i \in [k].$$

Za konec potrebujemo še rešitev linearne kongruence

$$N_i z_i \equiv 1 \pmod{n_i}, i \in [k],$$

kar označimo z z_i, kot že zapisano. Opazimo lahko, da je z_i inverz števila N_i po modulu n_i. S temi oznakami lahko dokažemo naslednji izrek, ki je poimenovan kitajski, saj je prvi znani zapis za problem tega tipa najti v knjigi kitajskega matematika Sunzi Suanjinga iz tretjega stoletja.

Izrek 6.23 (Kitajski izrek o ostakih) *Če so moduli $n_1, n_2, \ldots, n_k$ paroma tuji, potem ima sistem (31) ob dogovorjenih oznakah rešitev*

$$z \equiv c_1N_1z_1 + c_2N_2z_2 + \cdots + c_kN_kz_k \pmod{n}.$$

Dokaz. Glede na dogovorjene oznake velja $N_jz_j \equiv 1 \pmod{n_j}$ za vsak $j \in [k]$. Če pomnožimo to kongruenco s c_j na obeh straneh, dobimo $c_jN_jz_j \equiv c_j \pmod{n_j}$. Po drugi strani za vsak $i \in [k]$, ki je različen od j, velja $c_iN_iz_i \equiv 0 \pmod{n_j}$, saj je N_i večkratnik števila n_j, ker je $i \neq j$. Sedaj seštejemo omenjene linearne kongruence in po lastnosti (iv) trditve 6.18 dobimo

$$z \equiv c_1N_1z_1 + c_2N_2z_2 + \cdots + c_kN_kz_k \equiv c_j \pmod{n_j},$$

kar je rešitev j-te linearne kongruence sistema (31). Ker je bil na začetku $j \in [k]$ poljubno izbran, vidimo, da je z rešitev sistema (31).

Pokažimo še, da sta poljubni rešitvi z' in z'' sistema (31) kongruentni po modulu n. Seveda je $z' - z'' \equiv 0 \pmod{n_i}$ za vsak $i \in [k]$. Torej vsak $n_i|(z' - z'')$. Potem pa tudi njihov produkt n deli $(z' - z'')$, ker so moduli $n_1, n_2, \ldots, n_k$ paroma tuji po točki (ii) posledice 6.5. Tako velja $z' \equiv z'' \pmod{n}$ in izrek je dokazan. ∎

Z izrekom 6.23 ne dobimo rešitve le za sistem (31), pač pa očitno tudi za sistem (30), o čemer govori naslednja posledica.

Posledica 6.24 *Naj veljajo oznake, dogovorjene v tem razdelku. Če so števila $\frac{m_1}{d_1}, \frac{m_2}{d_2}, \ldots, \frac{m_k}{d_k}$ paroma tuja in $d_i|b_i$ za vsak $i \in [k]$, potem ima sistem (30) rešitev*

$$z \equiv c_1N_1z_1 + c_2N_2z_2 + \cdots + c_kN_kz_k \pmod{n}.$$

Zgled 6.9 *Poiščimo rešitev naslednjega sistema linearnih kongruenc:*

$$\begin{aligned} z &\equiv 2 \pmod{7} \\ z &\equiv 13 \pmod{15} \\ z &\equiv 3 \pmod{4}. \end{aligned}$$

Podane linearne kongruence imajo module paroma tuje in so zapisane v obliki sistema (31), zato lahko uporabimo izrek 6.23, da se dokopljemo do rešitve. Zlahka izračunamo $n = 420$ ter $N_1 = 60$, $N_2 = 28$ in $N_3 = 105$. Sedaj moramo rešiti tri linearne kongruence, da določimo z_1, z_2 in z_3, ki so

$$\begin{aligned} 60z_1 &\equiv 1 \pmod{7}, \\ 28z_2 &\equiv 1 \pmod{15}, \\ 105z_3 &\equiv 1 \pmod{4}. \end{aligned}$$

Prva števila lahko ustrezno zmanjšamo, saj so vsa večja kot moduli in dobimo

$$\begin{aligned} 4z_1 &\equiv 1 \pmod{7}, \\ -2z_2 &\equiv 1 \pmod{15}, \\ z_3 &\equiv 1 \pmod{4}. \end{aligned}$$

Tako smo že dobili $z_3 = 1$. Prvo in drugo vrstico lahko rešimo z ugibanjem, saj ni težko uvideti, da je inverz za prvo kongruenco kar 2 in za drugo 7. Tako dobimo

$$\begin{aligned} z_1 &\equiv 2 \pmod 7, \\ z_2 &\equiv 7 \pmod{15}. \end{aligned}$$

Zapišimo še vse potrebne podatke

$$\begin{array}{lll} c_1 = 2 & N_1 = 60 & z_1 = 2 \\ c_2 = -2 & N_2 = 28 & z_2 = 7 \\ c_3 = -1 & N_3 = 105 & z_3 = 1 \end{array}.$$

Ob tem omenimo, da smo za c_2 raje izbrali -2 kot 13 zaradi lažjega nadaljnjega računanja. Končna rešitev je tako

$$z \equiv 2 \cdot 60 \cdot 2 + (-2) \cdot 28 \cdot 7 + (-1) \cdot 105 \cdot 1 \equiv 240 - 392 - 105 \equiv$$

$$\equiv -257 \equiv 163 \pmod{420}.$$

Zgled 6.10 *Oglejmo si, kako lahko kitajski izrek o ostankih uporabimo pri reševanju linearne kongruence*

$$13z \equiv 8 \pmod{306}.$$

Najprej poiščimo faktorizacijo števila 306 na praštevila. Z nekaj računske spretnosti vidimo, da velja

$$306 = 2 \cdot 153 = 2 \cdot 9 \cdot 17.$$

Tako lahko zapišemo

$$\begin{aligned} 13z &\equiv 8 \pmod 2 \\ 13z &\equiv 8 \pmod 9 \\ 13z &\equiv 8 \pmod{17}, \end{aligned}$$

kar je sistem tipa (30), ki ga najprej prevedemo na sistem tipa (31). Zmanjšajmo števila glede na vsakokraten modul in dobimo

$$\begin{aligned} z &\equiv 0 \pmod 2 \\ 4z &\equiv -1 \pmod 9 \\ -4z &\equiv 8 \pmod{17}. \end{aligned}$$

Drugo vrstico pomnožimo z -2 in tretjo z 4, kar sta ustrezna inverza, in dobimo

$$\begin{aligned} z &\equiv 0 \pmod 2 \\ z &\equiv 2 \pmod 9 \\ z &\equiv -2 \pmod{17}, \end{aligned}$$

sistem tipa (31), ki ga rešujemo s Kitajskim izrekom o ostankih. Najprej lahko opazimo, da je $c_1 = 0$*, zato ne potrebujemo* N_1 *in* z_1*. Seveda so* $n = 306$*,* $N_2 = 34$ *in* $N_3 = 18$*. Rešimo še linearni kongruenci*

$$\begin{aligned} 34z_2 &\equiv 1 \pmod 9 \\ 18z_3 &\equiv 1 \pmod{17}. \end{aligned}$$

Iz druge sledi takoj, da je $z_3 \equiv 1 \pmod{17}$*, medtem ko prvo nadomestimo* z $-2z_2 \equiv 1 \pmod 9$*. Pomnožimo jo še z inverzom* 4 *po modulu* 9 *in dobimo* $z_2 \equiv -4 \pmod 9$*. Sedaj imamo vse potrebne podatke, ki so*

$$\begin{array}{lll} c_1 = 0 & N_1 = * & z_1 = ** \\ c_2 = 2 & N_2 = 34 & z_2 = 4 \\ c_3 = -2 & N_3 = 18 & z_3 = 1 \end{array} .$$

Končna rešitev je sedaj

$$z \equiv 0 + 2 \cdot 34 \cdot 4 + (-2) \cdot 18 \cdot 1 \equiv 272 - 36 \equiv 236 \pmod{306}.$$

Omenimo, da se v primeru velikega modula, metoda predstavljena v zadnjem primeru ne obnese vedno. Razlog za to je faktorizacija števila na praštevila, za kar ne obstajajo učinkovite metode. Seveda je tukaj govora o res velikih številih.

V Kitajskem izreku o ostankih se nahaja predpostavka, da morajo biti moduli paroma tuji. Poraja se vprašanje, kako je z rešitvijo sistema (31) in posledično tudi sistema (30), kadar moduli niso paroma tuji. V tem primeru se lahko pripeti, da rešitev ne obstaja. Problema se lahko lotimo na način, ki izhaja iz zadnjega zgleda. Vse module, ki niso potenca praštevila, razbijemo na potence praštevil, nato pa primerjamo tiste linearne kongruence, ki imajo v modulu potence istih praštevil. Oglejmo si dva zgleda, ki bosta pojasnila potrebne korake.

Zgled 6.11 *V sistemu linearnih knogruenc*

$$\begin{aligned} z &\equiv 3 \pmod{10} \\ z &\equiv 11 \pmod{15} \end{aligned}$$

modula nista paroma tuja in zato ne moremo uporabiti Kitajskega izreka o ostankih. Kot omenjeno, razbijemo modula na potence praštevil in dobimo

$$\begin{aligned} z &\equiv 3 \pmod 2 \\ z &\equiv 3 \pmod 5 \\ z &\equiv 11 \pmod 5 \\ z &\equiv 11 \pmod 3. \end{aligned}$$

Srednji vrstici imata iste module in zapišemo ju lahko

$$\begin{aligned} z &\equiv 3 \pmod 5 \\ z &\equiv 1 \pmod 5. \end{aligned}$$

Seveda ne obstaja celo število z*, ki nam da pri deljenju s* 5 *hkrati ostanek* 3 *in* 1*. Zato rešitev v tem primeru ne obstaja.*

Zgled 6.12 *Ponovno v podanem sistemu linearnih kongruenc*

$$\begin{aligned} z &\equiv 1 \pmod 6 \\ z &\equiv 3 \pmod 4 \end{aligned}$$

modula nista tuja, zato ju razbijemo na potence praštevil in dobimo

$$\begin{aligned} z &\equiv 1 \pmod 3 \\ z &\equiv 1 \pmod 2 \\ z &\equiv 3 \pmod 4. \end{aligned}$$

Oglejmo si podrobneje spodnji vrstici, katerih modula nista paroma tuja. Zlahka opazimo, da vsa liha števila rešijo linearno kongruenco $z \equiv 1 \pmod 2$. *Po drugi strani so le nekatera liha števila rešitev za* $z \equiv 3 \pmod 4$. *Bolj natančno, vsako drugo liho število reši* $z \equiv 3 \pmod 4$. *To pomeni, da nekatere rešitve linearne kongruence* $z \equiv 1 \pmod 2$ *ne rešijo linearne kongruence* $z \equiv 3 \pmod 4$. *Zato moramo te izločiti. Po drugi strani so vse rešitve linearne kongruence* $z \equiv 3 \pmod 4$ *hkrati tudi rešitve linearne kongruence* $z \equiv 1 \pmod 2$. *Kar pomeni, da v nadaljevanju upoštevamo zgolj linearno kongruenco* $z \equiv 3 \pmod 4$, *medtem ko linearno kongruenco* $z \equiv 1 \pmod 2$ *opustimo. Tako rešujemo*

$$\begin{aligned} z &\equiv 1 \pmod 3 \\ z &\equiv 3 \pmod 4 \end{aligned}$$

in imamo $c_1 = 1$, $c_2 = 3$, $n = 12$, $N_1 = 4$ *in* $N_2 = 3$. *Določimo še* z_1 *in* z_2 *iz linearnih kongruenc*

$$\begin{aligned} 4z_1 &\equiv 1 \pmod 3 \\ 3z_2 &\equiv 1 \pmod 4. \end{aligned}$$

Zlahko uvidimo, da je $z_1 = 1$ *in* $z_2 = -1$. *Po Kitajskem izreku o ostankih tako dobimo*

$$z \equiv 1 \cdot 4 \cdot 1 + 3 \cdot 3 \cdot (-1) \equiv -5 \equiv 7 \pmod{12}.$$

6.6 NEKATERE (NE)REŠENE NALOGE

Vaja 6.1 *Določite* $D(-72, -564)$, $D(-102, 652)$, $D(93, -483)$ *in* $D(603, 285)$.

Rešitev. *Uporabimo Evklidov algoritem in v prvem primeru imamo*

$$\begin{aligned} -564 &= 8 \cdot (-72) + 12 \\ -72 &= (-4) \cdot 12 + 0. \end{aligned}$$

Tako je $D(-72, -564) = 12$. *Podrobneje si oglejmo še zadnji primer*

$$\begin{aligned} 603 &= 2 \cdot 285 + 33 \\ 285 &= 8 \cdot 33 + 21 \\ 33 &= 1 \cdot 21 + 12 \\ 21 &= 1 \cdot 12 + 9 \\ 12 &= 1 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0. \end{aligned}$$

Torej je $D(603,285) = 3$. *Podobno določimo* $D(-102,652) = 2$ *in* $D(93,-483) = 3$.

Vaja 6.2 *Poiščite zapis* $ax + by = D(a,b)$, *če sta* $a = 283$ *in* $b = 1722$.

Rešitev. *To storimo z obratom Evklidovega algoritma*

$$\begin{array}{ccc} 1722 = 6 \cdot 283 + 24 & \Rightarrow & 24 = 1722 - 6 \cdot 283 \\ 283 = 11 \cdot 24 + 19 & \Rightarrow & 19 = 283 - 11 \cdot 24 \\ 24 = 1 \cdot 19 + 5 & \Rightarrow & 5 = 24 - 1 \cdot 19 \\ 19 = 3 \cdot 5 + 4 & \Rightarrow & 4 = 19 - 3 \cdot 5 \\ 5 = 1 \cdot 4 + 1. & \Rightarrow & 1 = 5 - 1 \cdot 4. \end{array}$$

Izrazimo še $D(283,1722) = 1$ *kot linearno kombinacijo števil* 283 *in* 1722*:*

$$\begin{aligned} 1 &= 5 - 1 \cdot 4 = 5 - 1 \cdot (19 - 3 \cdot 5) = 4 \cdot 5 - 1 \cdot 19, \\ 1 &= 4 \cdot 5 - 1 \cdot 19 = 4 \cdot (24 - 1 \cdot 19) - 1 \cdot 19 = 4 \cdot 24 - 5 \cdot 19, \\ 1 &= 4 \cdot 24 - 5 \cdot 19 = 4 \cdot 24 - 5 \cdot (283 - 11 \cdot 24) = 59 \cdot 24 - 5 \cdot 283, \\ 1 &= 59 \cdot 24 - 5 \cdot 283 = 59 \cdot (1722 - 6 \cdot 283) - 5 \cdot 283 = 59 \cdot 1722 - 359 \cdot 283. \end{aligned}$$

Tako imamo $59 \cdot 1722 - 359 \cdot 283 = 1$ *in* $x = -359$ *ter* $y = 59$.

Vaja 6.3 *Dokažite* $\max\{\alpha, \min\{\beta,\gamma\}\} = \min\{\max\{\alpha,\beta\}, \max\{\alpha,\gamma\}\}$, *kar je druga enakost iz trditve 6.14.*

Vaja 6.4 *Dokažite drugo enakost* $v(a, D(b,c)) = D(v(a,b), v(a,c))$ *iz trditve 6.15.*

Vaja 6.5 *Poenostavite izraze* $x \equiv 4^{2019} \pmod 5$, $y \equiv 3^{2020} \pmod 5$, $z \equiv 2^{2021} \pmod 5$ *in* $u \equiv 2^{50} \pmod 7$.

Rešitev. *Upoštevaje lastnosti kongruenc lahko računamo*

$$\begin{aligned} x &\equiv 4^{2019} \equiv (-1)^{2019} \equiv -1 \equiv 4 \pmod 5, \\ y &\equiv 3^{2020} \equiv 9^{1010} \equiv (-1)^{1010} \equiv 1 \pmod 5, \\ z &\equiv 2^{2021} \equiv 2 \cdot 2^{2020} \equiv 2 \cdot 4^{1010} \equiv 2 \cdot (-1)^{1010} \equiv 2 \pmod 5, \\ u &\equiv 2^{50} \equiv 2^2 \cdot 2^{48} \equiv 2^2 \cdot (2^3)^{16} \equiv 2^2 \cdot (8)^{16} \equiv 4 \cdot 1^{16} \equiv 4 \pmod 7. \end{aligned}$$

Vaja 6.6 *Pokažite, da za vsako liho celo število* a *velja* $a^2 \equiv 1 \pmod 8$.

Rešitev. *Pokazati želimo, da je* $a^2 - 1 = 8k$ *za nek* $k \in \mathbb{Z}$. *Seveda velja* $a^2 - 1 = (a-1)(a+1)$, *kjer sta* $a-1$ *in* $a+1$ *zaporedni sodi števili, saj je* a *liho število. Izmed dveh zaporednih sodih števil je eno deljivo s* 4 *drugo pa z* 2. *Zato je njun produkt deljiv z* 8.

Vaja 6.7 *Pokažite, da za vsako celo število* a *velja* $a^3 \equiv a \pmod 6$.

Rešitev. *Pokazati želimo, da je* $a^3 - a = 6k$ *za nek* $k \in \mathbb{Z}$. *Seveda velja* $a^3 - a = a(a^2-1) = a(a-1)(a+1)$. *Torej imamo tri zaporedna števila in eno izmed njih je deljivo s* 3, *eno pa z* 2. *Torej je produkt deljiv s* 6.

Vaja 6.8 *Rešite linearno kongruenco* $13z \equiv 8 \pmod{306}$ *iz zgleda 6.10 na direkten način.*

Vaja 6.9 *Podane so linearne kongurence* $12x \equiv 7 \pmod{n}$. *Poiščite rešitev za* $n \in \{21, 35, 84\}$, *če obstaja.*

Rešitev. *Hitro lahko vidimo, da* $D(12, 21) = 3$ *ne deli* 7 *in tudi* $D(12, 84) = 12$ *ne deli* 7. *Zato za* $n = 21$ *in* $n = 84$ *rešitev ne obstaja. Ker* $D(12, 35) = 1$ *deli* 7, *obstaja rešitev v primeru, ko je* $n = 35$. *Rešitev* $12x \equiv 7 \pmod{35}$ *dobimo, če pomnožimo s* 3 *in velja* $x \equiv 21 \pmod{35}$.

Vaja 6.10 *Poiščite rešitev Diofantske enačbe* $365x + 727y = 18$.

Rešitev. *Poiščimo zapis* $365x_0 + 727y_0 = D(365, 727)$ *s pomočjo obrata Evklidovega algoritma:*

$$\begin{array}{ccc} 727 = 1 \cdot 365 + 362 & \Rightarrow & 362 = 727 - 1 \cdot 365 \\ 365 = 1 \cdot 362 + 3 & \Rightarrow & 3 = 365 - 1 \cdot 362 \\ 362 = 120 \cdot 3 + 2 & \Rightarrow & 2 = 362 - 120 \cdot 3 \\ 3 = 1 \cdot 2 + 1 & \Rightarrow & 1 = 3 - 1 \cdot 2. \end{array}$$

Izrazimo še $D(365, 727) = 1$*:*

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 = 3 - 1 \cdot (362 - 120 \cdot 3) = 121 \cdot 3 - 1 \cdot 362, \\ 1 &= 121 \cdot 3 - 1 \cdot 362 = 121 \cdot (365 - 1 \cdot 362) - 1 \cdot 362 = 121 \cdot 365 - 122 \cdot 362, \\ 1 &= 121 \cdot 365 - 122 \cdot 362 = 121 \cdot 365 - 122 \cdot (727 - 1 \cdot 365) = \\ &= 243 \cdot 365 - 122 \cdot 727. \end{aligned}$$

Tako imamo $1 = 243 \cdot 365 - 122 \cdot 727$ *in* $x_0 = 243$ *ter* $y_0 = -122$. *Zapišemo lahko množico rešitev*

$$R = \{(4374 - 727t, -3782 + 365t) : t \in \mathbb{Z}\}.$$

Vaja 6.11 *Poiščite rešitev Diofantske enačbe* $283x + 1722y = 31$.

Rešitev. *Ker že poznamo zapis* $59 \cdot 1722 - 359 \cdot 283 = 1 = D(283, 1772)$ *iz naloge 6.2, velja* $x_0 = -359$ *ter* $y_0 = 59$ *in zapišemo lahko rešitev*

$$R = \{(-11129 - 1722t, 1829 + 283t) : t \in \mathbb{Z}\}.$$

Vaja 6.12 *Janez ima dve peščeni uri. Ena izmeri* 6 *minut, druga pa* 11 *minut. Kako naj izmeri* 13 *minut?*

Rešitev. *Ta problem lahko rešimo s pomočjo Diofantske enačbe* $6x + 11y = 13$, *ki ima rešitev, saj* $D(6, 11) = 1$ *deli* 13. *Z obratom Evklidovega algoritma dobimo zapis* $6 \cdot 2 + 11 \cdot (-1) = 1$ *in sta* $x_0 = 2$ *in* $y_0 = -1$. *Splošna rešitev Diofantske enačbe je tako*

$$R = \{(26 - 11t, -13 + 6t) : t \in \mathbb{Z}\}.$$

Najhitreje izmerimo 13 *minut, če izberemo* $t = 2$ *in dobimo par* $(4, -1)$. *To pomeni, da začnemo meriti z obema urama v istem trenutku. Trinajst minut začnemo meriti, ko se izteče ura za* 11 *minut in konča takrat, ko se četrtič izteče* 6 *minutna ura.*

Vaja 6.13 *Sod z volumnom* 500 *litrov polnimo z* 12 *oziroma* 14 *litrskimi vedri. Na koliko načinov lahko napolnimo sod, če napolnitev pomeni, kolikokrat smo uporabili* 12 *litrsko in kolikokrat* 14 *litrsko vedro? V sod vedno zlijemo polno vedro. Vode iz soda ne zajemamo.*

Rešitev. *Tudi tokrat si pomagamo z Diofantsko enačbo* $12x + 14y = 500$. *Rešitev obstaja, saj* $D(12, 14) = 2$ *deli* 500. *S pomočjo obrata Evklidovega algoritma dobimo zapis* $6 \cdot (-1) + 7 \cdot 1 = 1$, *kar pomeni* $x_0 = -1$ *in* $y_0 = 1$. *Tako je splošna rešitev*

$$R = \{(-250 - 7t, 250 + 6t) : t \in \mathbb{Z}\}.$$

Ob tem nas zanima, koliko je rešitev, kjer sta x *in* y *oba nenegativna. Te rešitve so* $(2, 34)$, $(9, 28)$, $(16, 22)$, $(23, 16)$, $(30, 10)$ *in* $(37, 4)$, *torej na* 6 *načinov.*

Vaja 6.14 *Okoli zvezde* Z_1 *krožijo v isti ravnini planeti a, b in c. Planet a obkroži* Z_1 *v* 5 *letih, b obkroži* Z_1 *v* 7 *letih in c obkroži* Z_1 *v* 13 *letih. V tej ravnini leži tudi zvezda* Z_2. *Planet a bo prvič ležal na zveznici* Z_1Z_2 *čez* 1 *leto, planet b čez* 3 *leta in planet c čez* 7 *let. Čez koliko let bodo na zveznici* Z_1Z_2 *ležali vsi trije planeti a, b in c?*

Rešitev. *Če iščemo število let* z, *ko bodo vsi trije planeti poravnani na zveznici* Z_1Z_2, *potem lahko to zapišemo kot sistem linearnih kongruenc*

$$\begin{aligned} z &\equiv 1 \pmod 5 \\ z &\equiv 3 \pmod 7 \\ z &\equiv 7 \pmod{13}. \end{aligned}$$

To je sistem oblike (31), ki ga rešimo s Kitajskim izrekom o ostankih, saj so moduli paroma tuji. Seveda je $c_1 = 1$, $c_2 = 3$ *in* $c_3 = 7$, *kot tudi* $n = 455$, $N_1 = 91$, $N_2 = 65$, *in* $N_3 = 35$. *Rešiti moramo še linearne kongruence*

$$\begin{aligned} 91z_1 &\equiv 1 \pmod 5 \\ 65z_2 &\equiv 1 \pmod 7 \\ 35z_3 &\equiv 1 \pmod{13}. \end{aligned}$$

Preoblikovanje po ustreznem modulu nam prinese

$$\begin{aligned} z_1 &\equiv 1 \pmod 5 \\ 2z_2 &\equiv 1 \pmod 7 \\ -4z_3 &\equiv 1 \pmod{13}. \end{aligned}$$

Če pomnožimo še srednjo vrstico s 4 *in zadnjo vrstico s* 3, *dobimo* $z_2 \equiv 4 \pmod 7$ *oziroma* $z_3 \equiv 3 \pmod{13}$. *Tako so* $z_1 = 1$, $z_2 = 4$ *in* $z_3 = 3$. *Po Kitajskem izreku o ostankih velja*

$$z \equiv 1 \cdot 91 \cdot 1 + 3 \cdot 65 \cdot 4 + 7 \cdot 35 \cdot 3 \equiv 1606 \equiv 241 \pmod{455}.$$

Vaja 6.15 *Poiščite vse celoštevilske rešitve sistema kongurenc*

$$\begin{aligned} z &\equiv 2 \pmod 3 \\ z &\equiv 3 \pmod 4 \\ z &\equiv 4 \pmod 5 \\ z &\equiv 6 \pmod 7. \end{aligned}$$

Rešitev. *Ker so moduli paroma tuji, lahko uporabimo Kitajski izrek o ostankih. Sistem je že zapisan v obliki (31), zato je* $c_1 = 2$, $c_2 = 3$, $c_3 = 4$ *in* $c_4 = 6$. *Zlahko izračunamo tudi* $n = 420$, $N_1 = 140$, $N_2 = 105$, $N_3 = 84$ *in* $N_4 = 60$. *Rešiti moramo še linearne kongruence*

$$\begin{aligned} 140z_1 &\equiv 1 \pmod 3 \\ 105z_2 &\equiv 1 \pmod 4 \\ 84z_3 &\equiv 1 \pmod 5 \\ 60z_4 &\equiv 1 \pmod 7. \end{aligned}$$

Po preoblikovanju prvega števila po ustreznem modulu dobimo

$$\begin{aligned} -z_1 &\equiv 1 \pmod 3 \\ z_2 &\equiv 1 \pmod 4 \\ -z_3 &\equiv 1 \pmod 5 \\ 4z_4 &\equiv 1 \pmod 7. \end{aligned}$$

Tako so $z_1 = -1$, $z_2 = 1$, $z_3 = -1$ *in* $z_4 = 2$, *kjer smo zadnjo vrstico pomnožili z dva. Po Kitajskem izreku o ostankih imamo tako*

$$z \equiv 2 \cdot 140 \cdot (-1) + 3 \cdot 105 \cdot 1 + 4 \cdot 84 \cdot (-1) + 6 \cdot 60 \cdot 2 \equiv 419 \equiv -1 \pmod{420}.$$

Vaja 6.16 *Poiščite vse celoštevilske rešitve sistema kongurenc*

$$\begin{aligned} z &\equiv 6 \pmod 7 \\ 3z &\equiv 5 \pmod{11} \\ 2z &\equiv 1 \pmod 5. \end{aligned}$$

Rešitev. *Ta sistem je oblike (30), zato ga najprej preoblikujemo v obliko (31). Ob tem pomnožimo srednjo vrstico s* 4 *in spodnjo vrstico s* 3, *da dobimo*

$$\begin{aligned} z &\equiv -1 \pmod 7 \\ z &\equiv -2 \pmod{11} \\ z &\equiv 3 \pmod 5. \end{aligned}$$

Sedaj so že znani $c_1 = -1$, $c_2 = -2$ *in* $c_3 = 3$, *kot tudi* $n = 385$, $N_1 = 55$, $N_2 = 35$, *in* $N_3 = 77$. *Rešiti moramo še linearne kongruence*

$$\begin{aligned} 55z_1 &\equiv 1 \pmod 7 \\ 35z_2 &\equiv 1 \pmod{11} \\ 77z_3 &\equiv 1 \pmod 5. \end{aligned}$$

Po preoblikovanju nam ostane

$$\begin{aligned} -z_1 &\equiv 1 \pmod 7 \\ 2z_2 &\equiv 1 \pmod{11} \\ 2z_3 &\equiv 1 \pmod 5 \end{aligned}$$

in iskane rešitve so $z_1 = -1$, $z_2 = 6$ *in* $z_3 = 3$. *Po Kitajskem izreku o ostankih velja*

$$z \equiv (-1) \cdot 55 \cdot (-1) + (-2) \cdot 35 \cdot 6 + 3 \cdot 77 \cdot 3 \equiv 328 \pmod{385}.$$

Vaja 6.17 *Poiščite vse celoštevilske rešitve sistema kongurenc*

$$\begin{aligned} 8z &\equiv 6 \pmod{17} \\ 6z &\equiv 5 \pmod{11} \\ 2z &\equiv 1 \pmod 3. \end{aligned}$$

Rešitev. *Ponovno imamo sistem oblike (30), ki ga preoblikujemo v obliko (31). Ob tem vse vrstice pomnožimo z* 2, *da dobimo*

$$\begin{aligned} -z &\equiv -5 \pmod{17} \\ z &\equiv -1 \pmod{11} \\ z &\equiv 2 \pmod 3. \end{aligned}$$

Sedaj so že znani $c_1 = 5$, $c_2 = -1$ *in* $c_3 = 2$, *kot tudi* $n = 561$, $N_1 = 33$, $N_2 = 51$, *in* $N_3 = 187$. *Rešiti moramo še linearne kongruence*

$$\begin{aligned} 33z_1 &\equiv 1 \pmod{17} \\ 51z_2 &\equiv 1 \pmod{11} \\ 187z_3 &\equiv 1 \pmod 3. \end{aligned}$$

Po preoblikovanju nam ostane

$$\begin{aligned} -z_1 &\equiv 1 \pmod{17} \\ -4z_2 &\equiv 1 \pmod{11} \\ z_3 &\equiv 1 \pmod 3 \end{aligned}$$

in iskane rešitve so $z_1 = -1$, $z_2 = -3$ *in* $z_3 = 1$, *kjer smo srednjo vrstico pomnožili z* -3. *Po Kitajskem izreku o ostankih velja*

$$z \equiv 5 \cdot 33 \cdot (-1) + (-1) \cdot 51 \cdot (-3) + 2 \cdot 187 \cdot 1 \equiv 362 \pmod{561}.$$

Vaja 6.18 *Poiščite vse celoštevilske rešitve sistema kongurenc*

$$\begin{aligned} 3z &\equiv 5 \pmod 7 \\ z &\equiv 13 \pmod 9 \\ 15z &\equiv 8 \pmod{22}. \end{aligned}$$

Rešitev. *Postopek reševanja je kot v prejšnji nalogi in rešitev je* $z \equiv 508 \pmod{1386}$.

Vaja 6.19 *Poiščite vse celoštevilske rešitve sistema kongurenc*

$$\begin{aligned} 9z &\equiv 5 \pmod{14} \\ 5z &\equiv 13 \pmod{9} \\ 14z &\equiv 8 \pmod{5}. \end{aligned}$$

Rešitev. *Postopek reševanja je kot v prejšnji nalogi in rešitev je* $z \equiv 377 \pmod{630}$.

Vaja 6.20 *Linearno kongruenco* $29z \equiv 5 \pmod{385}$ *rešimo na dva načina: direktno, s pomočjo obrata Evklidovega algoritma, in s pomočjo Kitajskega izreka o ostankih!*

Rešitev. *Za direkten način uporabimo izrek 6.21, za kar poiščemo zapis* $x \cdot 29 + y \cdot 385 = D(29, 385)$ *s pomočjo obrata Evklidovega algoritma. Tako je*

$$\begin{aligned} 385 = 13 \cdot 29 + 8 \quad &\Rightarrow \quad 8 = 385 - 13 \cdot 29 \\ 29 = 3 \cdot 8 + 5 \quad &\Rightarrow \quad 5 = 29 - 3 \cdot 8 \\ 8 = 1 \cdot 5 + 3 \quad &\Rightarrow \quad 3 = 8 - 1 \cdot 5 \\ 5 = 1 \cdot 3 + 2 \quad &\Rightarrow \quad 2 = 5 - 1 \cdot 3 \\ 3 = 1 \cdot 2 + 1. \quad &\Rightarrow \quad 1 = 3 - 1 \cdot 2. \end{aligned}$$

Zadnji neničelni ostanek je $d = D(385, 29) = 1$ *in zato obstaja rešitev, saj* $d|5$. *Izrazimo sedaj* $d = 1$ *kot linearno kombinacijo števil* 385 *in* 29*:*

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 = 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5, \\ 1 &= 2 \cdot 3 - 1 \cdot 5 = 2 \cdot (8 - 1 \cdot 5) - 1 \cdot 5 = 2 \cdot 8 - 3 \cdot 5, \\ 1 &= 2 \cdot 8 - 3 \cdot 5 = 2 \cdot 8 - 3 \cdot (29 - 3 \cdot 8) = 11 \cdot 8 - 3 \cdot 29, \\ 1 &= 11 \cdot 8 - 3 \cdot 29 = 11 \cdot (385 - 13 \cdot 29) - 3 \cdot 29 = 11 \cdot 385 - 146 \cdot 29. \end{aligned}$$

Iz zapisa $1 = 11 \cdot 385 - 146 \cdot 29$ *sedaj razberemo* $x = -146$ *in rešitev je* $z \equiv \frac{5}{d}x \equiv \frac{5}{1}(-146) \equiv -730 \equiv 40 \pmod{385}$.

Za drug način, s pomočjo Kitajskega izreka o ostankih, najprej zapišemo modul v kanonični obliki $385 = 5 \cdot 7 \cdot 11$. *Če je* z *rešitev linearne kongruence* $29z \equiv 5 \pmod{385}$, *potem je tudi rešitev sistema linearnih kongruenc*

$$\begin{aligned} 29z &\equiv 5 \pmod{5} \\ 29z &\equiv 5 \pmod{7} \\ 29z &\equiv 5 \pmod{11}. \end{aligned}$$

Le-ta je zapisan v obliki (30) in ga najprej preuredimo v obliko (31). Tako je

$$\begin{aligned} -z &\equiv 0 \pmod{5} \\ z &\equiv 5 \pmod{7} \\ -4z &\equiv 5 \pmod{11} \end{aligned}$$

in imamo $c_1 = 0$, $c_2 = -2$, $c_3 = -4$ *(potem ko zadnjo vrstico pomnožimo z* -3*). Iz* $c_1 = 0$ *sledi, da nas* N_1 *in* z_1 *ne zanimata. Potrebujemo pa* $n = 385$, $N_2 = 55$ *in* $N_3 = 35$*. Rešimo še linearni kongruenci*

$$\begin{aligned} 55z_2 &\equiv 1 \pmod 7 \\ 35z_3 &\equiv 1 \pmod{11}, \end{aligned}$$

ki se s preoblikovanjem po ustreznem modulu spremenita v ekvivalentno obliko

$$\begin{aligned} -z_2 &\equiv 1 \pmod 7 \\ 2z_3 &\equiv 1 \pmod{11}. \end{aligned}$$

Če pomnožimo zadnjo vrstico s 6 *dobimo* $z_3 \equiv 6 \pmod{11}$*. Tako sta* $z_2 = -1$ *in* $z_3 = 6$*. Po Kitajskem izreku o ostankih velja*

$$z \equiv 0 + (-2) \cdot 55 \cdot (-1) + (-4) \cdot 35 \cdot 6 \equiv -730 \equiv 40 \pmod{385}.$$

Seveda nas oba postopka privedeta do enake rešitve.

Vaja 6.21 *Linearno kongruenco* $19z \equiv 7 \pmod{374}$ *rešimo na dva načina: direktno, s pomočjo obrata Evklidovega algoritma, in s pomočjo Kitajskega izreka o ostankih!*

Rešitev. *Postopek reševanja je kot v prejšnji nalogi in rešitev je* $x \equiv 335 \pmod{374}$*.*

Vaja 6.22 *Poišči tri taka zaporedna liha števila, da je prvo deljivo s* 7^2*, drugo s* 5^2 *in tretje s* 3^2*.*

Rešitev. *Ker so to zaporedna liha števila, jih lahko zapišemo* $2z - 5$, $2z - 3$ *in* $2z - 1$*. To pripelje do zapisa z moduli*

$$\begin{aligned} 2z &\equiv 5 \pmod{49} \\ 2z &\equiv 3 \pmod{25} \\ 2z &\equiv 1 \pmod 9. \end{aligned}$$

Ker so moduli paroma tuji, dobimo $z \equiv 1787 \pmod{10125}$ *z uporabo Kitajskega izreka o ostankih. Torej so iskana števila 3569, 3571 in 3573.*

Vaja 6.23 *Poiščite vsa števila z, za katera velja:*

(A) z^2 je liho število,

(B) $5z - 2$ je deljivo s 3,

(C) $2z$ je oblike $10k + 6$, $k \in \mathbb{Z}$,

(D) $4z \equiv 8 \pmod{14}$.

Rešitev. Vse podane informacije lahko predstavimo v zapisu z moduli in sicer

$$\begin{aligned} z^2 &\equiv 1 \pmod 2 \\ 5z &\equiv 2 \pmod 3 \\ 2z &\equiv 6 \pmod{10} \\ 4z &\equiv 8 \pmod{14}. \end{aligned}$$

Dodatno lahko upoštevamo, da je kvadrat liho število le, če je tudi samo število liho (prva vrstica). Drugo vrstico pomnožimo z 2, tretjo vrstico delimo z 2 in zadnjo vrstico delimo s 4. Pri deljenju v skladu s trditvijo 6.19 spremenimo tudi modul. Tako dobimo

$$\begin{aligned} z &\equiv 1 \pmod 2 \\ z &\equiv 1 \pmod 3 \\ z &\equiv 3 \pmod 5 \\ z &\equiv 2 \pmod 7, \end{aligned}$$

ki ga lahko rešimo s pomočjo Kitajskega izreka o ostankih, saj so moduli paroma tuja si števila. Rešitev je $z \equiv 58 \pmod{210}$.

Vaja 6.24 *V košari so jajca. Če jajca razdelimo na dva dela, ostane eno jajce, če na tri dele, ostaneta dve jajci, če na štiri dele, ostanejo tri jajca, če na pet delov ostanejo, štiri jajca, č na šest delov, ostane pet jajc in če na sedem delov, ne ostane nobeno jajce. Kolikšno je najmanjše število jajc v košari?*

Rešitev. *Označimo z z število jajc v košari. Za število z velja*

$$\begin{aligned} z &\equiv 1 \pmod 2 \\ z &\equiv 2 \pmod 3 \\ z &\equiv 3 \pmod 4 \\ z &\equiv 4 \pmod 5 \\ z &\equiv 5 \pmod 6 \\ z &\equiv 0 \pmod 7. \end{aligned}$$

Ker moduli niso paroma tuji, (še) ne moremo uporabiti Kitajskega izreka o ostankih. Opazimo lahko, da je pogoj v tretji vrstici (vsako drugo liho število) strožji kot pogoj v prvi vrstici (vsako liho število). Zato lahko prvo vrstico izpustimo. Tudi pogoj $z \equiv 5 \pmod 6$ *lahko razbijemo na* $z \equiv 5 \pmod 2$ *in* $z \equiv 5 \pmod 3$*, kar prevedemo v* $z \equiv 1 \pmod 2$ *oziroma v* $z \equiv 2 \pmod 3$*. Vidimo, da sta ta pogoja vsebovana že v preostalih pogojih in lahko ignoriramo tudi* $z \equiv 5 \pmod 6$*. Tako ostane*

$$\begin{aligned} z &\equiv 2 \pmod 3 \\ z &\equiv 3 \pmod 4 \\ z &\equiv 4 \pmod 5 \\ z &\equiv 0 \pmod 7, \end{aligned}$$

kar lahko rešimo s Kitajskim izrekom o ostankih. Rešitev je $z \equiv 259 \pmod{420}$.

Vaja 6.25 *Podan je sistem linearnih kongruenčnih enačb*

$$\begin{aligned} z &\equiv a \pmod{15} \\ z &\equiv 4 \pmod{21} \\ z &\equiv 5 \pmod{11}. \end{aligned}$$

Izberite a tako, da bo sistem rešljiv in ga rešite. Za kateri a pa sistem ni rešljiv? Zakaj obstoj takega a ni v nasprotju s Kitajskim izrekom o ostankih?

Rešitev. *Modula* 15 *in* 21 *nista paroma tuja, zato ju razbijemo na dva dela, kjer nas posebej zanima modul* 3*. Tako imamo* $z \equiv a \pmod 3$ *in* $z \equiv 4 \equiv 1 \pmod 3$*. Torej je sistem rešljiv, če je* $a \equiv 1 \pmod 3$*. Za* $a = 4$ *je rešitev* $z \equiv 214 \pmod{1155}$*. Omenimo še, da dobimo različne rešitve za* $a \in \{1, 4, 7, 10, 13\}$*, saj je preostala linearna kongruenca iz prve vrstice* $z \equiv a \pmod 5$ *različna za omenjene vrednosti a. Sistem nima rešitve za vsak a, ki ima ostanek pri deljenju s* 3 *različen od* 1*. To ni v nasprotju s Kitajskim izrakom o ostankih, saj moduli niso paroma tuji.*

Vaja 6.26

Če obstaja, poišči rešitev sistema linearnih kongruenc

$$\begin{aligned} z &\equiv 11 \pmod 9 \\ z &\equiv 2 \pmod 6 \\ 8z &\equiv 3 \pmod{17}. \end{aligned}$$

Rešitev. *Ker moduli niso paroma tuji, drugo enačbo razdelimo na dva dela* $z \equiv 2 \pmod 2$ *in* $z \equiv 2 \pmod 3$*. Opazimo, da je pogoj* $z \equiv 11 \pmod 9$ *strožji kot* $z \equiv 2 \pmod 3$*, zato lahko slednjega opustimo. Torej drugo enačbo nadomestimo z* $z \equiv 2 \pmod 2$ *in rešimo s Kitajskim izrekom o ostankih. Rešitev je* $z \equiv 146 \pmod{306}$*.*

7

RELACIJE

Relacije so eden izmed najsplošnejših matematičnih pojmov. Zanje potrebujemo le dve poljubni množici A in B ter njun kartezični produkt

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

Relacija R je potem poljubna podmnožica kartezičnega produkta $A \times B$.

Kljub omenjeni splošnosti pa preseneča njihova uporabna vrednost, kar še posebej velja v primeru, ko je $A = B$. Ena izmed ključnih vrednosti je, da sta množici A in B lahko poljubni. Če recimo za $A = B = L$ izberemo množico vseh ljudi, dobimo preplet matematike in družboslovja. To pa je v zadnjem desetletju še posebej zaželjeno, saj s tem pripeljemo eksaktne metode v družboslovje. Nekaj primerov relacij, ki so podmnožice $L \times L$, so

$$\begin{aligned} B &= \{(x, y) : x \text{ je brat od } y\}, \\ U &= \{(x, y) : x \text{ je učitelj od } y\}, \\ S &= \{(x, y) : x \text{ je sosed od } y\}, \\ Z &= \{(x, y) : x \text{ je zdravnik od } y\}, \\ D &= \{(x, y) : x \text{ je obiskal enako državo kot } y\}. \end{aligned}$$

Iz naštetega je razvidno, da je za te relacije res veliko možnosti. Je pa potrebna posebna pozornost pri definiciji družboslovnih pojmov, saj je recimo brat lahko tista oseba moškega spola, ki ima enaka mamo in očeta. Pogosto se uporablja kar enak izraz za polbrata, ki ima skupnega le enega roditelja. Včasih se enak izraz uporablja tudi v drugih družbenih strukturah, recimo v raznih religijskih ali drugih interesnih združbah. To je tudi razlog, da se bomo v tem poglavju od sedaj naprej osredotočili le na matematično definirane relacije, zgoraj omenjene pa bomo občasno uporabili le za kak primer.

Naslednja pozitivna lastnost relacij je, da so enostavno predstavljive v računalnikih. To nam omogoča njihovo računalniško obdelavo, kar je z razvojem računalništva prineslo tudi razcvet teorije relacij.

Dodatno literaturo v slovenščini iz tega področja je moč najti v [7, 14]. V angleškem jeziku je na voljo precej več primerne literature, tukaj omenimo le [6]. Posebej omenimo, da je razširjeni seznam sosedov povzet po [8], kjer je predstavljen za grafe. Marsikaj je najti tudi na spletu in pogosto je že Wikipedia (angleška) dober začetni vir informacij. Standardna zbirka nalog za to poglavje je [4]. Veliko izpitnih nalog iz tega poglavja je najti v [12, 13].

7.1 PREDSTAVITVE RELACIJ

Relacija $R \subseteq A \times B$ je seveda podmnožica kartezičnega produkta in je zato tudi sama množica. Tako lahko relacijo predstavimo kot množico na vse običajne načine.

Zgled 7.1 *Naj bo* $A = \{a, b, c, d, e\}$ *in* $B = \{1, 2, 3\}$. *Relaciji* $R \subseteq A \times A$ *in* $S \subseteq A \times B$, *ki ju bomo uporabili večkrat v tem poglavju, sta podani z*

$$\begin{aligned} R &= \{(a,b),(a,d),(a,e),(b,a),(b,c),(c,c),(e,c)\} \\ S &= \{(a,2),(b,1),(b,2),(b,3),(c,1),(d,2),(d,3)\}. \end{aligned}$$

Pogosto uporabljamo zapis aRb namesto $(a,b) \in R$ in $a\neg Rb$ namesto $(a,b) \notin R$. Tako aRb preberemo kot

element a je v relaciji R z elementom b

in $a\neg Rb$ preberemo kot

element a ni v relaciji R z elementom b.

Zapis z množico je neprijazen do shranjevanja in kasnejše uporabe v računalniku. Razlog je v tem, da so lahko elementi v množici shranjeni na poljuben način in pogosto je potrebno preiskati celotno množico, da najdemo željeni par, ali da ugotovimo, da ga ni v relaciji. Tako nas zanima, ali lahko relacije shranimo v računalniku na prijaznejši način. Spoznali bomo dva najpogostejša načina. Prvi je s pomočjo matrike in drugi s pomočjo (razširjenega) seznama sosedov. Oba imata svoje prednosti in slabosti in nekatere izmed njih bomo tudi predstavilli.

Matrika dimenzije $m \times n$ vsebuje m vrstic in n stolpcev. Na vsako mesto, določeno z izbrano vrstico in izbranim stolpcem, lahko shranimo kak objekt, ki je običajno kar število. Kadar želimo predstaviti relacijo $R \subseteq A \times B$ z matriko, vsaki vrstici določimo svoj element množice A in vsakemu stolpcu določimo element množice B. Tako potrebujemo matriko dimenzije $m \times n$, kjer je $m = |A|$ in $n = |B|$. Če je aRb, potem shranimo 1 na mesto, ki je določeno z vrstico za a in stolpcem za b. V primeru, ko $a\neg Rb$, pa na mesto, ki je določeno z vrstico za a in stolpcem določenim za b, shranimo 0. Tako lahko relacijo predstavimo z matriko, ki vsebuje zgolj ničle in enice. Taki matriki rečemo **matrika relacije** oziroma pogosteje **matrika sosednosti**.

Zgled 7.2 *Matriki relacij $R \subseteq A \times A$ in $S \subseteq A \times B$ iz zgleda 7.1 sta*

$$R = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \text{ in } S = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

Ob tem smo vrstice in stolpce elementom množic $A = \{a, b, c, d, e\}$ in $B = \{1, 2, 3\}$ določili na naraven način, kar pomeni po vrsti. Tako v relaciji R pripada elementu a prva vrstica oziroma prvi stolpec, elementu b druga vrstica oziroma drugi stolpec in tako naprej.

Drug način shranjevanja relacije v računalniku predstavlja **seznam sosedov**. Tukaj si pravzaprav relacijo $R \subseteq A \times B$ razdelimo na nekaj podmnožic, kjer so v posamezni podmnožici shranjeni vsi elementi, s katerimi je nek element v relaciji (označimo jih z I), oziroma vsi elementi, ki so v relaciji z nekim elementom (označimo jih s P). Seveda tak seznam (podmnožico) oblikujemo za vsak element iz A oziroma B. Če to primerjamo z matriko, to pomeni, da si shranimo vse enice, ki jih dodatno ločimo na pripadnost po vrstici oziroma stolpcu.

Zgled 7.3 *Ponovno si oglejmo relaciji $R \subseteq A \times A$ in $S \subseteq A \times B$ iz zgleda 7.1, ki imata naslednja seznama sosedov*

R :

Seznam	*Vsebina*
I_a :	b, d, e
I_b :	a, c
I_c :	c
I_d :	$\emptyset$
I_e :	c
P_a :	b
P_b :	a
P_c :	b, c, e
P_d :	a
P_e :	a

in S :

Seznam	*Vsebina*
I_a :	2
I_b :	1, 2, 3
I_c :	1
I_d :	2, 3
I_e :	$\emptyset$
P_1 :	b, c
P_2 :	a, b, d
P_3 :	b, d

Tukaj že lahko omenimo največjo prednost seznama sosedov nasproti matriki sosednosti. Če izvajamo operacijo, za katero je potrebno pregledati vso podatkovno strukturo, moramo pri matriki sosednosti pregledati $O(nm)$ pozicij, kjer sta n in m števili elementov množice A oziroma B. Za to pregledamo vsa mesta v matriki, ki jih je ravno nm. Kadar ponovimo to s podatkovno strukturo seznamov sosedov, nam to prinese $2r = O(r)$ pozicij, kjer je r število parov relacije R. Tukaj imamo dvojko, ker vsakega soseda pogledamo dvakrat, enkrat v množici tipa I in drugič v množici tipa P. Tako vidimo, da ob uporabi matrike sosednosti sploh ne moremo pričakovati linearne časovne zahtevnosti, kar lahko zagotovimo v primeru seznama sosedov.

Po drugi strani v matriki sosednosti točno vemo, katero pozicijo moramo preveriti, če nas zanima, ali je i-ti element iz A v relaciji z j-tim elementom iz B. Pogledamo na (i, j)-to mesto matrike in vidimo, ali je shranjena 1 ali 0. To lahko storimo v konstantni časovni zahtevnosti $O(1)$. Za to isto operacijo, potrebujemo pri seznamu sosedov $O(|I_i|)$.

Kako je z operacijo izbrisa vseh elementov relacije, s katerimi je element $i \in A$ v relaciji? Pri matriki sosednosti je potrebno preveriti vse pozicije v i-ti vrstici in če najdemo 1, potem jo spremenimo v 0. Ker pregledamo celotno vrstico, ki ima $m = |B|$ pozicij, za to potrebujemo $O(m)$ časa. V seznamu sosedov je potrebno pregledati in izbrisati seznam I_i, kar lahko storimo v $O(|I_i|)$ časa, za vsak element, ki ga izbrišemo eno enoto. Nato pa moramo poiskati še vse obratne pozicije, kjer nastopa i v seznamih tipa P_x. Za vse te sezname v najslabšem primeru pregledamo vse sezname P_x, kar pomeni časovno zahtevnost $O(r)$. To pomeni skupaj $|I_i| + r = O(r)$ časa. Kadar imamo malo elementov relacije R in veliko elementov v množicah A in B, se lahko zgodi, da je seznam sosedov boljši kot matrika sosednosti. Običajno pa se pri tej operaciji bolje obnese matrika sosednosti.

Sedaj imamo majhno zagato. Seznam sosedov smo predstavili kot boljšo možnost, sedaj pa smo predstavili že drugo operacijo, kjer je matrika sosednosti boljša kot seznam sosedov. Ideja je v izboljšanju seznama sosedov. Ravno zadnja operacija nam lahko porodi idejo za to. Če imamo vse elemente, ki jih je potrebno izbrisati v eni množici I_i in je vsak od preostalih elementov, ki jih je potrebno izbrisati iz seznamov P_x, $x \in B$, v tesni povezavi z natanko enim od elementov iz I_i, zakaj potem seznama sosedov ne priredimo tako, da bomo iz elementa $j \in I_i$ lahko hitro dostopali do elementa $i \in P_j$?

To lahko storimo z **razširjenim seznamom sosedov**, kjer vsakemu elementu iz seznamov I_x in P_y, $x \in A$ in $y \in B$, dodamo nekaj dodatnih informacij. Dokler je teh dodatnih informacij končno mnogo, recimo c, si s tem ne pokvarimo velikosti podatkov, saj število vpisov, to je $2r$, le pomnožimo s konstanto c. Tako je $2cr = O(r)$, saj je c konstanta. Oglejmo si eno varianto razširjenega seznama sosedov, kjer dodamo $c = 5$ dodatnih informacij. Tako bomo recimo $d \in I_a$ iz zgleda 7.3 nadomestili z naslednjim nizom dolžine pet:

$$p = (a, d, \&q, \&w, \&z).$$

Razložimo pomen simbolov:

- p ime niza,
- a element, katerega seznamu I_a pripada ta niz p,
- d element, s katerim je a v relaciji v tem nizu p,
- $\&q$ kazalec na prejšnji niz q v listi I_a (če je p prvi, potem pišemo $\emptyset$),
- $\&w$ kazalec na naslednji niz w v listi I_a (če je p zadnji, potem pišemo Λ),
- $\&z$ kazalec na niz z iz P_d, ki opisuje isti element $(a, d) \in R$.

Na enak način obdelamo tudi vsak element iz P_x, le da tukaj zadnji vpis predstavlja kazalec na niz, ki opisuje element x iz I_y.

Zgled 7.4 *Oglejmo si razširjen seznam sosedov za relacijo R iz zgleda 7.1. Seznam sosedov relacije R najdemo v zgledu 7.3.*

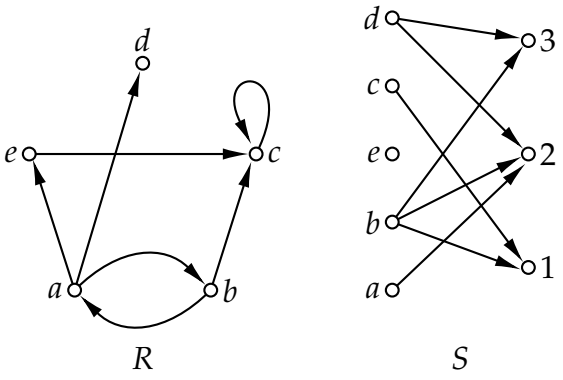
Seznam	*Ime niza*	*Niz*
I_a	q	$(a, b, \emptyset, \&p, \&t)$
	p	$(a, d, \&q, \&w, \&z)$
	w	$(a, e, \&p, \Lambda, \&n)$
I_b	s	$(b, a, \&\emptyset, \&u, \&\ell)$
	u	$(b, c, \&s, \Lambda, \&x)$
I_c	y	$(c, c, \emptyset, \Lambda, \&z)$
I_d	/	/
I_e	v	$(e, c, \emptyset, \Lambda, \&r)$
P_a	t	$(a, b, \emptyset, \Lambda, \&q)$
P_b	ℓ	$(b, a, \emptyset, \Lambda, \&s)$
P_c	x	$(b, c, \emptyset, \&m, \&u)$
	m	$(c, c, \&x, \&r, \&y)$
	r	$(e, c, \&m, \Lambda, \&v)$
P_d	z	$(a, d, \emptyset, \Lambda, \&p)$
P_e	n	$(a, e, \emptyset, \Lambda, \&w)$

Sedaj se lahko vrnemo na operacijo zbrisa vseh elementov relacije, s katerimi je element $i \in A$ v relaciji z razširjenim seznamom sosednosti. Ko brišemo vse elemente seznami I_i, lahko hkrati poiščemo in izbrišemo v konstantnem času isto povezavo v seznamu P_x zaradi kazalca na zadnjem petem mestu v nizu. Tako lahko sedaj to operacijo izvedemo v $O(|I_i|)$ časa, kar je bolje kot z matriko sosednosti.

Za konec tega razdelka si oglejmo še vizualno predstavitev relacij z **usmerjenimi grafi** ali krajše **digrafi**. Za podano relacijo $R \subseteq A \times B$ tvorita digraf D relacije R **množica vozlišč** $V(D) = A \cup B$ in **množica usmerjenih povezav** $A(D) = R$. Vsa vozlišča, to je elemente iz $A \cup B$, narišemo kot točke v ravnini, medtem ko je vsaka usmerjena povezava iz $A(D) = R$ narisana s puščico od začetnega vozlišča $a \in A$ do končnega vozlišča $b \in B$ za vsak par $(a, b) \in R$.

Zgled 7.5 *Na sliki 7 sta digrafa relacij R oziroma S iz zgleda 7.1, ki ju označimo kar z R in S. Opazimo lahko $V(R) = A \cup A = A = \{a, b, c, d, e\}$ in $A(R) = R = \{(a, b), (a, d), (a, e), (b, a), (b, c), (c, c), (e, c)\}$. Podobno je $V(S) = A \cup B = \{a, b, c, d, e, 1, 2, 3\}$ in $A(S) = S = \{(a, 2), (b, 1), (b, 2), (b, 3), (c, 1), (d, 2), (d, 3)\}$.*

Opomba 7.1 *Usmerjeni grafi so samostojna veja matematike in jih pogosto raziskujemo brez navezave na relacije. So v sorodu s teorijo grafov, ki je predmet zadnjega poglavja tega dela.*



Slika 7: Digrafa relacij R in S.

7.2 DVE OPERACIJI NAD RELACIJAMI

V tem razdelku igrata glavno vlogo dve operaciji and relacijami, ki ju potrebujemo kasneje za lažji opis lastnosti.

Inverzna relacija R^{-1} relacije $R \subseteq A \times B$ je relacija, definirana z

$$R^{-1} = \{(b, a) : (a, b) \in R\}.$$

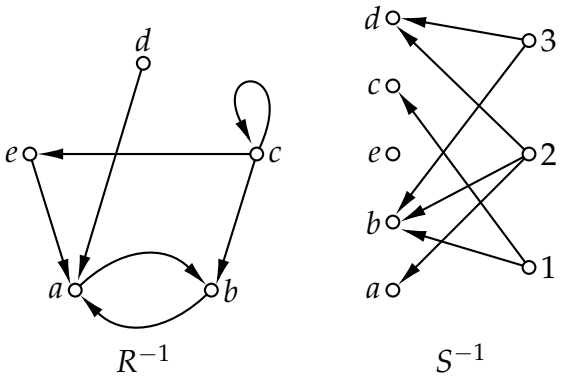
Digraf za inverzno relacijo R^{-1} dobimo iz digrafa za relacijo R tako, da enostavno obrnemo puščice. Matriko sosednosti inverzne relacij R^{-1} dobimo iz matrike sosednosti relacije R tako, da matriko R transponiramo. To pomeni, da vrstice po vrsti zapišemo kot stolpce in dobimo transponirano matriko.

Zgled 7.6 *Spomnimo se relacij R in S iz zgleda 7.1. Na sliki 8 sta digrafa za relaciji R^{-1} oziroma S^{-1} označena kar z R^{-1} in S^{-1}. Matriki sosednosti pa sta*

$$R^{-1} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ in } S^{-1} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Zgled 7.7 *Za relacije B, U, S, Z in D iz uvoda nad množico ljudi so njihove inverzne relacije*

$$\begin{aligned} B^{-1} &= \{(x, y) : x \text{ ima brata } y\}, \\ U^{-1} &= \{(x, y) : x \text{ je učenec od } y\}, \\ S^{-1} &= \{(x, y) : x \text{ je sosed od } y\} = S, \\ Z^{-1} &= \{(x, y) : x \text{ je pacient od } y\}, \\ D^{-1} &= \{(x, y) : x \text{ je obiskal enako državo kot } y\} = D. \end{aligned}$$



Slika 8: Digrafa relacij R^{-1} in S^{-1}.

Opazimo lahko, da velja $S^{-1} = S$ in $D = D^{-1}$. To je značilno za lastnost simetričnost, ki jo bomo, med drugimi spoznali v naslednjem razdelku. Velja še omeniti, da marsikdo zmotno pomisli tudi pri relaciji B, da velja $B = B^{-1}$, a to ni res, saj je lahko x v B^{-1} tudi sestra od y.

Naj bosta $R \subseteq A \times B$ in $S \subseteq B \times C$ relaciji. Definirajmo novo relacijo $R * S \subseteq A \times C$ s predpisom

$$a(R * S)c \Leftrightarrow \exists b \in B : aRb \wedge bRc.$$

Relacijo $R * S$ si lahko razložimo s pomočjo dveh korakov. Tako sta a in c v relaciji $R * S$, če lahko v dveh korakih pridemo iz a do c preko nekega elementa $b \in B$. Prvi korak je narejen z relacijo R in drugi z relacijo S. V primeru, da velja $R = S$, potem pišemo kar $R * S = R * R = R^2$.

Opomba 7.2 *Na operacijo $*$ lahko pogledamo tudi s stališča funkcij, kjer predstavlja kompozitum. Če sta relaciji R in S tudi funkciji, potem velja $R * S = S \circ R$.*

Zgled 7.8 *Za relaciji R in S iz zgleda 7.1 je*

$$R * S = \{(a,1),(a,2),(a,3),(b,1),(b,2),(c,1),(e,1)\},$$

medtem ko $S * R$ ne obstaja.

Zgled 7.9 *Za relacije B, U, S, Z in D iz uvoda nad množico ljudi L velja*

$$\begin{aligned} B^2 &= \{(x,y) : x \text{ ima brata } y\} = B, \\ Z * B &= \{(x,y) : x \text{ je zdravnik od brata od } y\}, \\ Z * S &= \{(x,y) : x \text{ je zdravnik od soseda od } y\}, \\ D * Z &= \{(x,y) : x \text{ je obiskal enako državo kot zdravnik od } y\}, \\ S * U &= \{(x,y) : x \text{ je sosed od učitelja od } y\}. \end{aligned}$$

Vidimo, da velja $B^2 = B$. Oglejmo si tole bolj podrobno. Za xB^2y obstaja $z \in L$, da velja xBz in zBy. Torej je x brat od z in z je brat od y. Če relacija brat pomeni imeti oba starša enaka, to pomeni, da je tudi x brat od y. Ta lastnost, $B^2 = B$, je značilna za lastnost tranzitivnost, kot bomo videli v naslednjem razdelku.

Preverimo lahko, da je operacija $*$ asociativna, torej, da velja

$$R_1 * (R_2 * R_3) = (R_1 * R_2) * R_3.$$

Zato lahko zgornja produkta pišemo tudi brez oklepajev $R_1 * R_2 * R_3$. Seveda lahko s številom zvezdic nadaljujemo. Ob tem smo omejeni z ustreznimi množicami, saj mora biti druga množica relacije pred $*$ enaka prvi množici relacije za $*$. Ta pogoj je najlažje izpolnjen, kadar je relacija $R \subseteq A \times A$ in velja $R_1 = R_2 = R_3 = R$ (in tako naprej po potrebi). V tem primeru pišemo tudi potence, kot že omenjeno. Tako je recimo

$$xR^4y = x(R * R * R * R)y \Leftrightarrow \exists z, u, v \in A : aRz \wedge zRu \wedge uRv \wedge vRy.$$

Kako narisati digraf relacije $R * S$? Med vozlišči x in y imamo puščico v digrafu $R * S$, če obstaja puščica med x in nekim z v digrafu relacije R in puščica med tem istim z in y v digrafu relacije S. Bolj nazorno je to razvidno v digrafu relacije R^k. V tem primeru imamo puščico med x in y v digrafu R^k, če lahko v digrafu za R pridemo iz x v y v k korakih.

Kako je z matriko sosednosti in relacijo $R * S$? Označimo matriki sosednosti kar z R in S, pri čemer je matrika za $R \subseteq A \times B$ razsežnosti $n \times m$ in matrika za $S \subseteq B \times C$ razsežnosti $m \times p$. Tako so $|A| = n$, $|B| = m$ in $|C| = p$ in matrika $R * S$ bo imela razsežnost $n \times p$. Na (i, k)-tem mestu matrike $R * S$ bomo imeli 1, če obstaja $j \in [m]$, da ima matrika R enico na (i, j)-tem mestu in matrika S enico na (j, k)-tem mestu. To lahko zapišemo kot

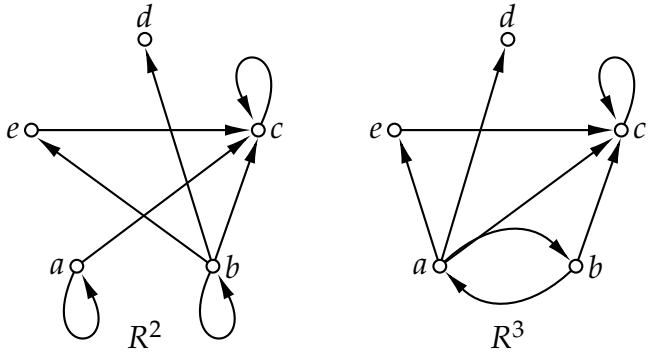
$$(R * S)_{i,k} = (r_{i,1} \wedge s_{1,k}) \vee (r_{i,2} \wedge s_{2,k}) \vee \cdots \vee (r_{i,m} \wedge s_{m,k}) = \vee_{j=1}^{m} (r_{i,j} \wedge s_{j,k}),$$

kjer je $r_{i,j}$ vednost (i, j)-tega mesta matrike R in $s_{j,k}$ vrednost (j, k)-tega mesta matrike S.

Zgled 7.10 *Za relacijo R iz zgleda 7.1 sta digrafa za R^2 in R^3 na sliki 9. Matriki sosednosti za R^2 in R^3 pa sta*

$$R^2 = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} * \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$R^3 = R^2 * R = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} * \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$



Slika 9: Digrafa relacij R^2 in R^3.

Opomba 7.3 *Če v operaciji za računanje $(R * S)_{i,k}$ zamenjamo logični ali $\vee$ z operacijo seštevanja ter logični in $\wedge$ z operacijo množenja, potem dobimo definicijo običajnega matričnega množenja. V tem primeru dobimo*

$$R^2 = \begin{bmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Opazimo lahko, da 2 v običajnem množenju na mestu (a, c) pomeni le, da obstajata dve različni poti med a in c dolžine 2 v relaciji R. Tako vidimo, da z navadnim matričnim množenjem sicer ne dobimo matrike sosednosti relacije (saj lahko matrika vsebuje vrednosti večje od ena), vendar dobimo dodatno informacijo o številu poti določene dolžine med ustreznimi elementi.

7.3 LASTNOSTI RELACIJ

V tem razdelku bomo privzeli dodatno omejitev, ki do sedaj ni bila potrebna. Tako se bomo omejili le na tiste relacije, kjer je $A = B$. Torej od sedaj naprej velja, da je $R \subseteq A \times A$.

Relacija $R \subseteq A \times A$ je

- **refleksivna**, če je aRa za vsak $a \in A$;
- **irefleksivna**, če je $a \neg Ra$ za vsak $a \in A$;
- **simetrična**, če iz aRb sledi bRa za vsaka $a, b \in A$;
- **asimetrična**, če iz aRb sledi $b \neg Ra$ za vsaka $a, b \in A$;

- **antisimetrična**, če iz aRb in bRa sledi $a = b$ za vsaka $a, b \in A$;
- **tranzitivna**, če iz aRb in bRc sledi aRc za vse $a, b, c \in A$;
- **intranzitivna**, če iz aRb in bRc sledi, da $a\neg Rc$ za vse $a, b, c \in A$;
- **sovisna**, če je aRb ali bRa za vsaka $a, b \in A$, $a \neq b$;
- **strogo sovisna**, če je aRb ali bRa za vsaka $a, b \in A$.

Za relacijo $R \subseteq A \times A$ označimo z $E = \{(x, x) : x \in A\}$. Torej množico E sestavljajo vse zanke.

Izrek 7.4 *Za relacijo $R \subseteq A \times A$ veljajo naslednje lastnosti.*

(I) *Relacija R je refleksivna natanko tedaj, ko je $E \subseteq R$.*

(II) *Relacija R je irefleksivna natanko tedaj, ko je $R \cap E = \emptyset$.*

(III) *Relacija R je simetrična natanko tedaj, ko je $R = R^{-1}$.*

(IV) *Relacija R je asimetrična natanko tedaj, ko je $R \cap R^{-1} = \emptyset$.*

(V) *Relacija R je antisimetrična natanko tedaj, ko je $R \cap R^{-1} \subseteq E$.*

(VI) *Relacija R je tranzitivna natanko tedaj, ko je $R^2 \subseteq R$.*

(VII) *Relacija R je intranzitivna natanko tedaj, ko je $R \cap R^2 = \emptyset$.*

(VIII) *Relacija R je sovisna natanko tedaj, ko je $(A \times A) - E \subseteq R \cup R^{-1}$.*

(IX) *Relacija R je strogo sovisna natanko tedaj, ko je $A \times A = R \cup R^{-1}$.*

Dokaz. Naj bo $R \subseteq A \times A$ relacija in $E = \{(x, x) : x \in A\}$.

Relacija R je refleksivna natanko tedaj, ko je aRa za vsak $a \in A$, kar je natanko tedaj, ko R vsebuje vse zanke. Seveda R vsebuje vse zanke natanko tedaj, ko je $E \subseteq R$ in lastnost (i) je dokazana.

Za lastnost (ii) je relacija R irefleksivna natanko tedaj, ko je $a\neg Ra$ za vsak $a \in A$, kar je natanko tedaj, ko R ne vsebuje niti ene zanke. Seveda je R brez zank natanko tedaj, ko je $R \cap E = \emptyset$.

Lastnost (iii) sledi iz naslednjega razmisleka. Relacija R ni simetrična natanko tedaj, ko obstajata $a, b \in A$, da je aRb in $b\neg Ra$, kar je natanko tedaj, ko $R \neq R^{-1}$ in ta alineja je končana.

Relacija R ni asimetrična natanko tedaj, ko obstajata $a, b \in A$, da je aRb in bRa, kar je natanko tedaj, ko je $bR^{-1}a$ in $aR^{-1}b$, kar je natanko takrat, ko je $R \cap R^{-1} \neq \emptyset$, saj sta $(a,b), (b,a) \in R \cap R^{-1}$ in lastnost (iv) je resnična.

Za lastnost (v) relacija R ni antisimetrična natanko tedaj, ko obstajata različna $a, b \in A$, da je aRb in bRa, kar je natanko tedaj, ko je $bR^{-1}a$ in $aR^{-1}b$ za $a \neq b$, kar je natanko takrat, ko je $R \cap R^{-1} \nsubseteq E$, saj sta $(a,b), (b,a) \in R \cap R^{-1}$ za $a \neq b$.

Relacija R ni tranzitivna natanko tedaj, ko obstajajo $a, b, c \in A$, da je aRb, bRc in $a\neg Rc$, kar je natanko tedaj, ko $R^2 \nsubseteq R$, saj je aR^2c. Torej je lastnost (vi) izpolnjena.

Razmislimo še o lastnosti (vii). Relacija R ni intranzitivna natanko tedaj, ko obstajajo $a, b, c \in A$, da je aRb, bRc in aRc, kar je natanko tedaj, ko $R \cap R^2 \neq \emptyset$, saj je $(a,c) \in R \cap R^2$.

Relacija R ni sovisna natanko tedaj, ko obstajata različna $a, b \in A$, da $a\neg Rb$ in $b\neg Ra$, kar je natanko tedaj, ko $(A \times A) - E \nsubseteq R \cup R^{-1}$, saj je $(a,b) \in (A \times A) - E$ a hkrati $(a,b) \notin R \cup R^{-1}$. Tako smo pokazali tudi predzadnjo lastnost.

Za zadnjo lastnost relacija R ni sovisna natanko tedaj, ko obstajata $a, b \in A$, da $a\neg Rb$ in $b\neg Ra$, kar je natanko tedaj, ko $(A \times A) \neq R \cup R^{-1}$, saj $(a,b) \notin R \cup R^{-1}$. ■

Do konca tega razdelka si bomo ogledali povezave med nekaterimi lastnostmi in nekaj primerov relacij, ki bodo utrdile razumevanje lastnosti relacij in jih povezale z nekaterimi dobro znanimi matematičnimi pojmi. Tako bomo spoznali, da je, nekoliko nepričakovano, relacija lahko tranzitivna in intranzitivna hkrati in podobno.

Zgled 7.11 *Pokažimo, da je relacija $R \subseteq A \times A$ strogo sovisna natanko tedaj, ko je R refleksivna in sovisna hkrati. Če je R strogo sovisna, potem po definiciji velja aRb ali bRa za vsak par $a, b \in A$. Seveda to velja tudi v primeru, ko je $a \neq b$ in je R zato sovisna. Podobno aRb ali bRa velja, ko je $a = b$ in imamo aRa, kar pomeni refleksivnost R. Naj bo sedaj R refleksivna in sovisna. Zaradi refleksivnosti velja aRb v primeru, ko je $a = b$. Če je $a \neq b$, potem velja aRb ali bRa zaradi sovisnosti. Torej je aRb ali bRa resnična za vsaka $a, b \in A$ in je R strogo sovisna.*

Zgled 7.12 *Pokažimo, da je relacija $R \subseteq A \times A$ asimetrična natanko tedaj, ko je R irefleksivna in antisimetrična hkrati. Naj bo relacija R najprej asimetrična. Potem ne obstajata $a, b \in A$, da zanju hkrati velja aRb in bRa, saj bi v nasprotnem kršili definicijo asimetričnosti. Potem prvi del implikacije iz definicije antisimetričnosti ni izpolnjen in zato implikacija v celoti drži. Zato antisimetričnost velja. Predpostavimo nasprotno, da irefleksivnost ne velja. Torej obstaja $a \in A$, da velja aRa. Za $b = a$ imamo potem aRb in bRa hkrati, kar je v nasprotju z asimetričnostjo. Zato zanke niso dovoljene in R je irefleksivna. Predpostavimo sedaj obratno, da R ni asimetrična. Potem obstajata $a, b \in A$, da velja aRb in bRa hkrati. Če je $a = b$, potem imamo zanko in R ni irefleksivna. Če je $a \neq b$, potem pa ne velja antisimetričnost, saj imamo aRb in bRa hkrati, kjer je $a \neq b$.*

Zgled 7.13 *Pokažimo, da je relacija $R \subseteq A \times A$ simetrična in antisimetrična hkrati natanko tedaj, ko je $R \subseteq E$. Če je R simetrična in antisimetrična hkrati, potem po izreku 7.4 velja $R = R^{-1}$ in $R \cap R^{-1} \subseteq E$. Ob združitvi teh dveh pogojev dobimo $R = R \cap R^{-1} \subseteq E$. Naj bo obratno $R \subseteq E$. V tem primeru velja $R^{-1} = R$, kar poraja simetričnost po izreku 7.4. Po drugi strani velja tudi $R \cap R^{-1} = R \subseteq E$ in R je antisimetrična ponovno po izreku 7.4.*

Zgled 7.14 *Pokažimo, da če je relacija $R \subseteq A \times A$ simetrična in tranzitivna, potem ni nujno refleksivna. Naj bo relacija R simetrična in tranzitivna. Naj velja aRb. Zaradi simetričnosti potem velja tudi bRa, ter zaradi tranzitivnosti aRa. Izgleda torej, da simetričnost in tranzitivnost porajata refleksivnost. Vendar ima ta razmislek luknjo. Velja zgolj v primeru, ko je element a v relaciji z nekim elementom b. Če a ni v relaciji z nikomer, omenjeni razmislek ne velja in R ni nujno refleksivna. Morda najekstremnejši primer je prazna relacija $R = \emptyset$. Le-ta je simetrična in tranzitivna po izreku 7.4, medtem ko ni refleksivna po istem izreku.*

Zgled 7.15 *Pokažimo, da je relacija $R \subseteq A \times A$ tranzitivna in intranzitivna natanko tedaj, ko za poljubna $a, c \in A$ ne obstaja $b \in R$, da velja aRb in bRc. Naj bo najprej R tranzitivna in intranzitivna hkrati. Po izreku 7.4 velja $R^2 \subseteq R$ in $R \cap R^2 = \emptyset$. Če ta pogoja združimo, vidimo $\emptyset = R \cap R^2 = R^2$. Torej ne obstaja $b \in A$, da velja aRb in bRc za poljubna $a, c \in A$. Obratno, če za poljubna $a, c \in A$ ne obstaja $b \in R$, da velja aRb in bRc, potem je $R^2 = \emptyset$ in veljata oba pogoja $R^2 \subseteq R$ in $R \cap R^2 = \emptyset$, kar po izreku 7.4 implicira tranzitivnost in intranzitivnost.*

Zgled 7.16 *Relacija deljivosti $| \subseteq \mathbb{Z} \times \mathbb{Z}$ je očitno refleksivna, saj je $a = 1 \cdot a$ in tranzitivna po lastnosti (v) trditve 6.1. Ker je refleksivna, seveda ni irefleksivna. Intranzitivna ni zaradi tranzitivnosti in prejšnjega zgleda. Prav tako ni simetrična, saj recimo $5|10$, a $10 \nmid 5$, in asimetrična, saj je refleksivna. Bolj zanimivo postane ob antisimetričnosti. Zaradi lastnosti (iv) trditve 6.1 tudi antisimetričnost ne velja, saj $a|b$ in $b|a$ implicira $a = \pm b$. Če se z relacijo deljivosti namesto na cela števila omejimo na naravna števila, torej $| \subseteq \mathbb{N} \times \mathbb{N}$, potem pa antisimetričnost zaradi enake lastnosti drži. Za konec ni težko videti, da sovisnost in stroga sovisnost ne držita za relacijo deljivosti, saj recimo za poljubni različni praštevili p_1 in p_2 velja $p_1 \nmid p_2$ in $p_2 \nmid p_1$.*

Zgled 7.17 *Oglejmo si lastnosti relacije $\bmod \subseteq \mathbb{Z} \times \mathbb{Z}$. Iz prejšnjega poglavja smo pri tej relaciji bolj vajeni zapisa $a \equiv b \pmod{n}$, zato pri njem tudi ostajamo. Po lastnostih (i), (ii) in (iii) trditve 6.18 je ta relacija refleksivna, simetrična in tranzitivna. Zlahka najdemo protiprimere, da ostale lastnosti ne držijo. Recimo za antisimetričnost je $n \equiv 2n \pmod{n}$ in $2n \equiv n \pmod{n}$ a seveda velja $n \neq 2n$. Edina izjema se zgodi v posebnem primeru, ko je $n = 1$, saj so v tem primeru vsa cela števila paroma med seboj kongruentna in veljata sovisnost in stroga sovisnost.*

Zgled 7.18 *Katere lastnosti ima relacija $\leq \subseteq \mathbb{R} \times \mathbb{R}$? Ta morda malo nenavaden zapis skriva vsem dobro znano relacijo $a \leq b$ za poljubni realni števili a in b. Ker velja $a \leq a$, je $\leq$ refleksivna. Vsem je tudi dobro znano, da $a \leq b$ in $b \leq a$ hkrati implicira $a = b$. Zato je $\leq$ antisimetrična. Tudi tranzitivnost zlahka sledi, saj $a \leq b$ in $b \leq c$ pomeni, da je tudi $a \leq c$. Ker je med dvema poljubnima realnima številoma (lahko enakima), eno zagotovo manjše ali enako od drugega, pa veljata tudi sovisnost in stroga sovisnost. Ostale lastnosti za $\leq$ ne veljajo, saj zlahka poiščemo protiprimere zanje.*

Zgled 7.19 *Sorodna relacija je $< \subseteq \mathbb{R} \times \mathbb{R}$, vendar ima glede na lastnosti relacij pomembne razlike. Najpomembnejša je, da je $<$ asimetrična, saj če velja $a < b$, potem $b \not< a$. Zaradi asimetričnosti je $<$ tudi antisimetrična in irefleksivna po zgledu 7.12. Ker je irefleksivna, seveda ni refleksivna in po zgledu 7.11 tudi ni strogo sovisna. Je pa sovisna, saj je med dvema različnima številoma $a \neq b$ eno zagotovo manjše od drugega. Tudi tranzitivnost je očitno izpolnjena za $<$.*

Zgled 7.20 *Naj bo A poljubna neprazna množica in $\mathcal{P}(A)$ njena potenčna množica (to je množica vseh podmnožic množice A). Vsem dobro znana relacija je tudi $\subseteq \subseteq \mathcal{P}(A) \times \mathcal{P}(A)$ po imenu podmnožica. Zadnji zapis ponovno izgleda nenavadno, vendar je prvi $\subseteq$ simbol za relacijo, medtem ko drugi $\subseteq$ pomeni podmnožico kartezičnega produkta $\mathcal{P}(A) \times \mathcal{P}(A)$. Iz osnovnih lastnosti množic vemo, da velja $A \subseteq A$, torej refleksivnost, iz $A \subseteq B$ in $B \subseteq C$, sledi $A \subseteq C$, torej tranzitivnost in iz $A \subseteq B$ in $B \subseteq A$, sledi $A = B$, torej antisimetričnost. Preostale lastnosti ne držijo in zlahka poiščemo protiprimere za to.*

Zgled 7.21 *Oglejmo si še relacijo $\subset \subseteq \mathcal{P}(A) \times \mathcal{P}(A)$, ki ji rečemo prava podmnožica. Osvežimo definicijo $\subset$:*

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

Seveda je $\subset$ očitno irefleksivna, asimetrična in tranzitivna, medtem ko ostale lastnosti ne držijo.

7.4 EKVIVALENČNE RELACIJE

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

Zgled 7.22 *Relacija $a \equiv b \pmod{n}$ je ekvivalenčna, kot je razloženo v primeru 7.17.*

Zgled 7.23 *Med premicami v ravnini definirajmo relacijo vzporednosti $\parallel$ na naslednji način:*

$$p \parallel q \Leftrightarrow k_p = k_q,$$

kjer sta k_p in k_q smerna koeficienta premic p in q. Ker je $k_p = k_p$ za vsako premico p, velja $p \parallel p$ in $\parallel$ je refleksivna. Za simetričnost naj bo $p \parallel q$. Po definiciji velja $k_p = k_q$. Seveda je potem tudi $k_q = k_p$ in velja $q \parallel p$, kar zaključuje simetričnost. Do ekvivalenčne relacije nam manjka še tranzitivnost. Naj za to velja $p \parallel q$ in $q \parallel r$. Po definiciji $\parallel$ velja $k_p = k_q$ in $k_q = k_r$. Združimo ta pogoja v $k_p = k_r$, kar pomeni, da je $p \parallel r$ in tranzitivnost sledi. Relacija $\parallel$ je torej refleksivna, simetrična in tranzitivna in je kot

taka ekvivalenčna relacija. Omenimo še dve zanimivosti. Če bi vzporednost definirali s 'premici p in q se ne sečeta', potem bi izgubili refleksivnost. Relacijo $\parallel$ lahko vpeljemo tudi med premice v prostoru $\mathbb{R}^3$, vendar moramo v tem primeru za vzporednost p in q zahtevati, da sta njuna smerna vektorja $\overrightarrow{s_p}$ in $\overrightarrow{s_q}$ linearno odvisna.

Zgled 7.24 *Naj bo $f : \mathbb{R} \to \mathbb{R}$ realna funkcija. Definirajmo relacijo $\sim \subseteq \mathbb{R} \times \mathbb{R}$ s predpisom*

$$x_1 \sim x_2 \Leftrightarrow f(x_1) = f(x_2)$$

in pokažimo, da je $\sim$ ekvivalenčna relacija. Ker je $f(x) = f(x)$, je $x \sim x$ za vsak $x \in \mathbb{R}$ in $\sim$ je refleksivna. Za simetričnost naj velja $x_1 \sim x_2$. Po definiciji $\sim$ velja $f(x_1) = f(x_2)$ in potemtakem tudi $f(x_2) = f(x_1)$, kar implicira $x_2 \sim x_1$ in simetričnost sledi. Za tranzitivnost naj bo $x_1 \sim x_2$ in $x_2 \sim x_3$. Po definiciji $\sim$ imamo $f(x_1) = f(x_2)$ in $f(x_2) = f(x_3)$. Združimo oba pogoja v $f(x_1) = f(x_3)$, iz česar sledi $x_1 \sim x_3$ in s tem tudi tranzitivnost. S tem je $\sim$ tudi ekvivalenčna.

V nadaljevanju se bomo posvetili globljemu pomenu ekvivalenčnih relacij. Za to potrebujmo tako imenovana razbitja množic. Neprazne podmnožice $A_1, A_2, \ldots, A_k$ množice A tvorijo **razbitje množice** A, če so paroma disjunktne (to je $A_i \cap A_j = \emptyset$ za vsaka različna $i, j \in [k]$) in velja $\cup_{i=1}^{k} A_k = A$. Razbitje intuitivno pomeni, da vse elemente množice razdelimo na več delov (to je podmnožic), kjer se vsak element nahaja v točno enem delu (podmnožice so paroma disjunktne). V naslednjih dveh izrekih bomo pokazali, da so razbitja in ekvivalenčne relacije neločljivo povezane med sabo.

Izrek 7.5 *Naj bo $A_1, A_2, \ldots, A_k$ razbitje množice A. Potem je relacija $R \subseteq A \times A$ definirana z*

$$xRy \Leftrightarrow x \text{ in } y \text{ pripadata isti množici } A_i$$

ekvivalenčna relacija.

Dokaz. Naj bo $A_1, A_2, \ldots, A_k$ razbitje množice A. Pokažimo, da je relacija R ekvivalenčna. Seveda obstaja nek $i \in [k]$, da je $x \in A_i$, saj je $\cup_{i=1}^{k} A_k = A$. Potem velja $x \in A_i$ in $x \in A_i$ in je zato xRx, kar prinese refleksivnost. Za simetričnost naj bo xRy. Po definiciji obstaja $i \in [k]$, da sta $x, y \in A_i$. Seveda velja tudi $y, x \in A_i$ in s tem tudi yRx, kar zagotovi simetričnost. Za tranzitivnost imejmo xRy in yRz. Torej obstajata $i, j \in [k]$, da velja $x, y \in A_i$ in $y, z \in A_j$. Če je $i \neq j$, potem je $y \in A_i \cap A_j$, kar ni mogoče, saj je $A_i \cap A_j = \emptyset$. Zato je $i = j$ in imamo $x, z \in A_i$, kar pomeni xRz in tranzitivnost sledi. Ker je R refleksivna, simetrična in tranzitivna, je tudi ekvivalenčna relacija. ∎

Vsako razbitje nam torej poraja ekvivalenčno relacijo. Preden pokažemo, da obstaja povezava tudi v obratni smeri, definirajmo podmnožice, ki so neločljivo povezane z ekvivalenčno relacijo. Za to naj bo $R \subseteq A \times A$ ekvivalenčna relacija. Množici

$$[a] = \{x \in A : xRa\}$$

rečemo **ekvivalenčni razred** elementa $a \in A$. Kot vidimo iz naslednjega izreka, tvorijo ekvivalenčni razredi razbitje.

Izrek 7.6 *Naj bo $R \subseteq A \times A$ ekvivalenčna relacija. Potem ekvivalenčni razredi $\{[a] : a \in A\}$ relacije R tvorijo razbitje množice A.*

Dokaz. Naj bo $R \subseteq A \times A$ ekvivalenčna relacija. Ker je R refleksivna, velja aRa za vsak $a \in A$, kar pomeni, da je $a \in [a]$. Tako je $\cup_{a \in A}[a] = A$.

Pokažimo še, da je ali $[a] \cap [b] = \emptyset$, ali $[a] = [b]$ za poljubna različna $a, b \in A$. Povedano drugače, ekvivalenčna razreda $[a]$ in $[b]$ sta paroma disjunktna, ali pa sta enaka. Do tega si pomagajmo z naslednjo pomožno trditvijo:

$$aRb \Rightarrow [a] = [b]. \tag{32}$$

Naj torej najprej velja aRb. Zaradi simetričnosti R velja tudi bRa. Naj bo $x \in [a]$ poljuben element in pokažimo, da velja tudi $x \in [b]$. Ker je $x \in [a]$, velja po definiciji ekvivalenčnega razreda, da je xRa. Tako imamo xRa in aRb, kar pomeni tudi xRb zaradi tranzitivnosti R. Zveza xRb že tudi pomeni $x \in [b]$. Ker je bil $x \in [a]$ poljubno izbran, to pomeni $[a] \subseteq [b]$. Naj bo sedaj $y \in [b]$ poljubno izbran. Tako imamo yRb in bRa, kar pomeni tudi yRa zaradi tranzitivnosti R. Seveda yRa pomeni tudi $y \in [a]$. Ker je bil $y \in [b]$ poljubno izbran, to pomeni tudi $[b] \subseteq [a]$. Zaradi antisimetričnosti relacije $\subseteq$ nam zvezi $[a] \subseteq [b]$ in $[b] \subseteq [a]$ zagotavljata $[a] = [b]$.

Zveza (32) nam sedaj omogoča enostavno nadaljevanje. Če je $[a] \cap [b] = \emptyset$, smo končali. Sicer je $[a] \cap [b] \neq \emptyset$ in naj bo $x \in [a] \cap [b]$. Tako je $x \in [a]$ in hkrati $x \in [b]$, kar pomeni xRa in hkrati xRb. Zaradi zveze (32) velja $[x] = [a]$ in hkrati $[x] = [b]$. Ko združimo oba pogoja, dobimo $[a] = [b]$ in dokaz je zaključen. ∎

Zgled 7.25 *Spomnimo se zgleda 6.4, kjer smo obravnavali relacijo $x \equiv k \pmod 5$. Ta relacija je ekvivalenčna in njeni ekvivalenčni razredi so ravno množice $A_{k=0}$, $A_{k=1}$, $A_{k=2}$, $A_{k=3}$ in $A_{k=4}$ opisane v zgledu 6.4. S sedanjimi oznakami imamo*

$$\begin{aligned}
[0] &= A_{k=0} = \{5t : t \in \mathbb{Z}\} = \{0, \pm 5, \pm 10, \pm 15, \ldots\},\\
[1] &= A_{k=1} = \{5t+1 : t \in \mathbb{Z}\} = \{1, -4, 6, -9, 11, -14, 16, \ldots\},\\
[2] &= A_{k=2} = \{5t+2 : t \in \mathbb{Z}\} = \{2, -3, 7, -8, 12, -13, 17, \ldots\},\\
[3] &= A_{k=3} = \{5t+3 : t \in \mathbb{Z}\} = \{3, -2, 8, -7, 13, -12, 18, \ldots\},\\
[4] &= A_{k=4} = \{5t+4 : t \in \mathbb{Z}\} = \{4, -1, 9, -6, 14, -11, 19, \ldots\}.
\end{aligned}$$

Ni težko videti, da množice $[0]$, $[1]$, $[2]$, $[3]$ in $[4]$ tvorijo razbitje množice $\mathbb{Z}$. Prav tako zlahka vidimo enakost med nekaterimi ekvivalenčnimi razredi, recimo $[-1] = [4]$, $[-2] = [3]$, $[-3] = [2]$ in tako naprej. Omenimo še, da po en predstavnik iz vsakega ekvivalenčnega razreda tvori množico $\mathbb{Z}_5$, ki je recimo $\{0, 1, 2, 3, 4\}$ in v to množico lahko vpeljemo računski operaciji seštevanja in množenja.

Zgled 7.26 *V zgledu 7.24 smo videli, da je za $f : \mathbb{R} \to \mathbb{R}$ relacija $\sim$ definirana s predpisom $x_1 \sim x_2 \Leftrightarrow f(x_1) = f(x_2)$ ekvivalenčna relacija. Označimo z Z_f zalogo vrednosti funkcije f, to so tisti $y \in \mathbb{R}$, v katere se preslika vsaj en $x \in \mathbb{R}$. Potem so ekvivalenčni razredi relacije $\sim$ enaki*

$$f^{-1}(y) = \{x \in \mathbb{R} : f(x) = y\}$$

za vsak $y \in Z_f$. Oznaka $f^{-1}(y)$ pravzaprav pomeni pra-sliko števila y glede na funkcijo $f(x)$. Omenimo še povezavo te ekvivalenčne relacije z obstojem inverzne funkcije. Inverzna funkcija, kjer se omejimo na zalogo vrednosti Z_f, obstaja natanko takrat, ko ima vsak ekvivalenčni razred natanko en element.

Zgled 7.27 *Definirajmo relacijo $Z \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ s predpisom*

$$(n, m)Z(n', m') \Leftrightarrow n - n' = m - m'.$$

Pokažimo, da je Z ekvivalenčna relacija in opišimo njene ekvivalenčne razrede. Ker je ta primer na prvi pogled nekoliko zahtevnejši, si najprej razjasnimo oznake. Na Z lahko pogledamo kot na relacijo $Z \subseteq A \times A$, kjer je $A = \mathbb{N} \times \mathbb{N}$. Tako so elementi iz A urejeni pari naravnih števil (n, m). Seveda je $0 = 0$, kar drugače zapišemo $n - n = m - m$ in pomeni po definiciji relacije Z, da je $(n, m)Z(n, m)$ in refleksivnost drži za Z. Za simetričnost naj bo $(n, m)Z(n', m')$, kar pomeni $n - n' = m - m'$. Če to enačbo pomnožimo z -1, dobimo $n' - n = m' - m$, kar pomeni $(n', m')Z(n, m)$ in Z je simetrična. Za tranzitivnost naj velja $(n, m)Z(n', m')$ in $(n', m')Z(n'', m'')$, kar po definiciji Z pomeni $n - n' = m - m'$ in $n' - n'' = m' - m''$. Seštejmo obe enačbi in dobimo $n - n'' = m - m''$, kar pomeni $(n, m)Z(n'', m'')$, s čimer je tranzitivnost dokazana. Torej je Z ekvivalenčna relacija.

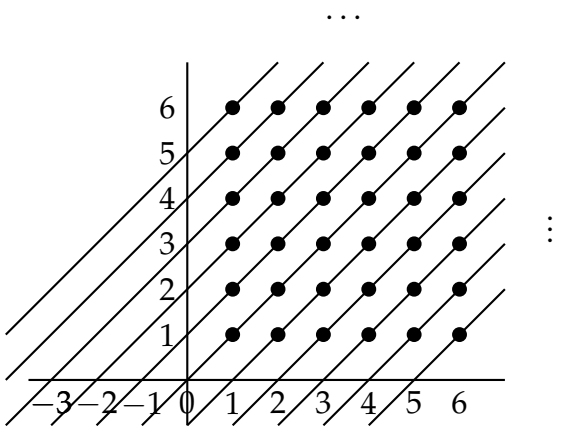
Opišimo še njene ekvivalenčne razrede. Naj bo $(x, y) \in A = \mathbb{N} \times \mathbb{N}$ poljuben element in $(n, m) \in \mathbb{N} \times \mathbb{N}$ fiksen element, za katerega iščemo $[(n, m)]$. Po definiciji ekvivalenčnega razreda je $(x, y) \in [(n, m)]$, če je $(x, y)Z(n, m)$, oziroma $x - n = y - m$. Če izrazimo y, dobimo $y = x + m - n$, kar geometrijsko predstavlja premico v ravnini s smernim koeficientom 1 in presečiščem z y osjo pri vrednosti $m - n$. Zapišemo lahko

$$[(n, m)] = \{(x, y) : y = x + m - n, x \in \mathbb{N}\} = \{(x, x + m - n) : x \in \mathbb{N}\}.$$

Izberimo nekaj posebnih vrednosti za (n, m):

$$\begin{aligned}
[(1,1)] &= \{(1,1),(2,2),(3,3),(4,4),\ldots\} = \{(x,x) : x \in \mathbb{N}\},\\
[(1,2)] &= \{(1,2),(2,3),(3,4),(4,5),\ldots\} = \{(x,x+1) : x \in \mathbb{N}\},\\
[(2,1)] &= \{(2,1),(3,2),(4,3),(5,4),\ldots\} = \{(x,x-1) : x-1 \in \mathbb{N}\},\\
[(1,3)] &= \{(1,3),(2,4),(3,5),(4,6),\ldots\} = \{(x,x+2) : x \in \mathbb{N}\},\\
[(3,1)] &= \{(3,1),(4,2),(5,3),(6,4),\ldots\} = \{(x,x-2) : x-2 \in \mathbb{N}\}.
\end{aligned}$$

Ekvivalenčni razredi relacije Z so predstavljeni na sliki 10, kjer predstavniki istega ekvivalenčnega razreda ležijo na premici vzporedni s premico $y = x$.



Slika 10: Ekvivalenčni razredi relacije Z iz zgleda 7.27.

Če definiramo preslikavo $\phi : \{[(n,m)] : (n,m) \in \mathbb{N} \times \mathbb{N}\} \to \mathbb{Z}$ s predpisom $\phi([(n,m)]) = n - m$, lahko preverimo, da je ϕ bijektivna in zato obstaja za vsako celo število natanko en ekvivalenčni razred relacije Z. Na sliki 10 lahko vidimo, da celo število, v katerega se preslika ekvivalenčni razred s preslikavo ϕ, leži na isti premici (vzporedni s premico $y = x$). S tem smo s pomočjo naravnih števil in ekvivalenčne relacije Z dobili strukturo ekvivalenčnih razredov te relacije, ki se obnašajo kot cela števila (od koder tudi oznaka relacije Z).

Zgled 7.28 *Definirajmo relacijo $Q \subseteq (\mathbb{Z} \times (\mathbb{Z} - \{0\})) \times (\mathbb{Z} \times (\mathbb{Z} - \{0\}))$ s predpisom*

$$(p,q)Q(r,s) \Leftrightarrow ps = rq.$$

Pokažimo, da je Q ekvivalenčna relacija in opišimo njene ekvivalenčne razrede. Seveda je $0 = 0$, kar drugače zapišemo $pq = pq$ in pomeni po definiciji relacije Q, da je $(p,q)Q(p,q)$ in refleksivnost drži za Q. Za simetričnost naj bo $(p,q)Q(r,s)$, kar pomeni $ps = rq$. Pišemo lahko tudi $rq = ps$, kar pomeni $(r,s)Z(p,q)$ in Q je simetrična. Za tranzitivnost naj velja $(p,q)Q(r,s)$ in $(r,s)Q(t,v)$, kar po definiciji Q pomeni $ps = rq$ in $rv = st$. Iz drugega pogoja izrazimo $r = \frac{st}{v}$ in ga vstavimo v prvi pogoj, pri čemer je $v \neq 0$, saj je $v \in \mathbb{Z} - \{0\}$. Tako dobimo $ps = \frac{st}{v}q$. Če dobljeno enačbo pomnožimo z $\frac{v}{s}$, $s \neq 0$, saj je $s \in \mathbb{Z} - \{0\}$, dobimo $pv = tq$, kar pomeni $(p,q)Q(t,v)$, s čimer je tranzitivnost dokazana. Torej je Q ekvivalenčna relacija.

Opišimo še njene ekvivalenčne razrede. Naj bo $(x,y) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$ poljuben element in $(p,q) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$ fiksen element, za katerega iščemo $[(p,q)]$. Po definiciji ekvivalenčnega razreda je $(x,y) \in [(p,q)]$, če je $(x,y)Q(p,q)$, oziroma $xq = py$. To lahko preoblikujemo v zelo znan zapis $\frac{x}{y} = \frac{p}{q}$, kjer sta $y, q \neq 0$, saj sta $y, q \in \mathbb{Z} - \{0\}$. Zapišemo lahko

$$[(p,q)] = \left\{ (x,y) : \frac{x}{y} = \frac{p}{q}, x \in \mathbb{Z}, y \in \mathbb{Z} - \{0\} \right\}.$$

Izberimo nekaj posebnih vrednosti za (p, q):

$$\begin{aligned}
[(0,1)] &= \{(0,1),(0,-1),(0,2),(0,-2),\ldots\} = \{(0,x) : x \in \mathbb{Z} - \{0\}\},\\
[(1,1)] &= \{(1,1),(-1,-1),(2,2),(-2,-2),\ldots\} = \{(x,x) : x \in \mathbb{Z} - \{0\}\},\\
[(1,2)] &= \{(1,2),(-1,-2),(2,4),(-2,-4),\ldots\} = \{(x,2x) : x \in \mathbb{Z} - \{0\}\},\\
[(-1,2)] &= \{(-1,2),(1,-2),(-2,4),(2,-4),\ldots\} = \{(x,-2x) : x \in \mathbb{Z} - \{0\}\},\\
[(2,1)] &= \{(2,1),(-2,-1),(4,2),(-4,-2),\ldots\} = \{(2x,x) : x \in \mathbb{Z} - \{0\}\},\\
[(-2,1)] &= \{(-2,1),(2,-1),(-4,2),(4,-2),\ldots\} = \{(-2x,x) : x \in \mathbb{Z} - \{0\}\}.
\end{aligned}$$

Če bi nadaljevali s tem vzorcem, ni težko videti, da za vsak okrajšan ulomek dobimo natanko en ekvivalenčni razred relacije Q. Na ta način lahko s pomočjo celih števil in ekvivalenčne relacije Q dobimo strukturo ekvivalenčnih razredov te relacije, ki se obnašajo kot racionalna števila (od koder tudi oznaka relacije Q).

7.5 OVOJNICE

V prejšnjem razdelku smo videli, da so ekvivalenčne relacije neločljivo povezane z razbitjem množice, kar običajno prinese določene prednosti. Kako pa postopati, če relacija ni ekvivalenčna, mi pa kljub temu želimo ugodnosti povezave z razbitjem? Lastnosti, ki jih moramo zagotoviti za ekvivalenčnost, so refleksivnost, simetričnost in tranzitivnost. Če katera izmed teh treh lastnosti ne velja, potem lahko z dodajanjem manjkajočih ustreznih parov k relaciji dosežemo, da ima večja relacija iskano lastnost. Vendar pri tem ne želimo pretiravati in dodati preveč, saj lahko hitro izgubimo strukturo, ki jo s seboj nosi ekvivalenčna relacija.

Naj bo $R \subseteq A \times A$ relacija in φ neka lastnost relacij. Relacija $S \subseteq A \times A$ je φ-**ovojnica** relacije R, če velja

(I) $R \subseteq S$,

(II) S ima lastnost φ in

(III) če ima $Q \subseteq A \times A$ lastnost φ in je $R \subseteq Q$, potem je tudi $S \subseteq Q$.

Medtem ko sta pogoja (i) in (ii) jasna, se zdi pogoj (iii) bolj zapleten. Pravi, da je φ-ovojnica S relacije R najmanjša relacija z lastnostjo φ, ki vsebuje relacijo R. To vidimo iz tega, da je tudi S vsebovana v poljubni relaciji Q, ki vsebuje R in ima lastnost φ, o čemer govori pogoj (iii).

V nadaljevanju si bomo pogledali naslednje ovojnice relacije R:

- z $\widetilde{R}$ označujemo refleksivno ovojnico,
- z $\widehat{R}$ označujemo simetrično ovojnico,
- z $\overline{R}$ označujemo tranzitivno ovojnico,

- z R^* označujemo refleksivno-tranzitivno ovojnico in
- z R^e označujemo ekvivalenčno ovojnico.

Izrek 7.7 *Naj bo $R \subseteq A \times A$ in $E = \{(x,x) : x \in A\}$. Potem je*

(I) $\widetilde{R} = R \cup E$,

(II) $\widehat{R} = R \cup R^{-1}$,

(III) $\overline{R} = \cup_{i=1}^{\infty} R^i$,

(IV) $R^* = \cup_{i=1}^{\infty} \widetilde{R}^i = \cup_{i=1}^{\infty} (R \cup E)^i$,

(V) $R^e = \overline{R^{-1} \cup E \cup R} = \cup_{i=1}^{\infty} (R^{-1} \cup E \cup R)^i$.

Dokaz. Naj bo $R \subseteq A \times A$ in $E = \{(x,x) : x \in A\}$.

Za dokaz (i) je seveda $R \subseteq \widetilde{R}$ in $\widetilde{R}$ je refleksivna po točki (i) izreka 7.4. Recimo, da obstaja refleksivna relacija Q, ki vsebuje R, a ne vsebuje $\widetilde{R}$. Ker Q vsebuje R in ne vsebuje $\widetilde{R}$, potem $E \nsubseteq Q$ in Q ni refleksivna po točki (i) izreka 7.4, kar je v nasprotju s predpostavko refleksivnosti Q. Torej je $\widetilde{R}$ najmanjša refleksivna relacija, ki vsebuje relacijo R in je zato tudi njena ovojnica.

Pri (ii) je ponovno $R \subseteq \widehat{R}$ in $\widehat{R}$ je simetrična po točki (iii) izreka 7.4. Recimo, da obstaja simetrična relacija Q, ki vsebuje R, a ne vsebuje $\widehat{R}$. Ker Q vsebuje R in ne vsebuje $\widehat{R}$, potem $R^{-1} \nsubseteq Q$ in Q ni simetrična po točki (iii) izreka 7.4, kar je v nasprotju s predpostavko simetričnosti Q. Ponovno je $\widehat{R}$ najmanjša simetrična relacija, ki vsebuje relacijo R in je zato tudi njena ovojnica.

Za (iii) je ponovno $R \subseteq \overline{R}$. Naj bo $a\overline{R}b$ in $b\overline{R}c$. Po definiciji $\overline{R}$ obstajata $i, j \in \mathbb{N}$, da je aR^ib in bR^jc. Tako obstajajo $a_1, a_2, \ldots, a_{i-1}$ in $b_1, b_2, \ldots, b_{j-1}$, da velja $aRa_1, a_1Ra_2, \ldots, a_{i-1}Rb$ in $bRb_1, b_1Rb_2, \ldots b_{j-1}Rc$. Zaradi obojega velja $aR^{i+j}c$ in je $a\overline{R}c$, kar implicira tranzitivnost $\overline{R}$. Recimo, da $\overline{R}$ ni najmanjša tranzitivna relacija, ki vsebuje R. Potem obstaja tranzitivna relacija Q, da $\overline{R} \nsubseteq Q$ in $R \subseteq Q$. Zato obstajata $a, b \in A$, za katera je $a\overline{R}b$ a $a\neg Qb$. Ker je $a\overline{R}b$, obstaja $i \in \mathbb{N}$, da je aR^ib. To pomeni obstoj $a_1, a_2, \ldots, a_{i-1}$, da velja $aRa_1, a_1Ra_2, \ldots, a_{i-1}Rb$. Ker je $R \subseteq Q$, velja tudi $aQa_1, a_1Qa_2, \ldots, a_{i-1}Qb$. Izmed vseh takšnih i-jev izberimo najmanjšega, pri katerem se to zgodi. Ker je i najmanjši, je $aR^{i-1}a_{i-1}$ in tudi aQa_{i-1}. Sedaj imamo aQa_{i-1} in $a_{i-1}Qb$, toda $a\neg Qb$, kar je protislovje s tranzitivnostjo Q. Zato je $\overline{R}$ najmanjša tranzitivna relacija, ki vsebuje R.

Za dokaz (iv) je očitno, da je $R \subseteq R^*$. Ker je $R \cup E$ refleksivna po točki (i) izreka 7.4, je tudi $R^* = \cup_{i=1}^{\infty} (R \cup E)^i$ tranzitivna zaradi prejšnje točke. Torej je R^* refleksivna in tranzitivna hkrati. Recimo, da R^* ni najmanjša refleksivno-tranzitivna relacija, ki vsebuje R. (Dokaz vsebuje enake razmisleke kot v točki (iii), le da $\overline{R}$ nadomestimo z $R \cup E$. V matematiki potem dokaza običajno ne zapišemo.

Tokrat naredimo izjemo, da je vidna tudi podobnost.) Potem obstaja refleksivno-tranzitivna relacija Q, za katero $R^* \nsubseteq Q$ in $R \subseteq Q$. Zato obstajata $a, b \in A$, za katera je aR^*b a $a \neg Qb$. Če je $a = b$, potem imamo protislovje z refleksivnostjo Q. Tako bodi $a \neq b$. Ker je aR^*b, obstaja $i \in \mathbb{N}$, da je $a(R \cup E)^i b$. To pomeni obstoj $a_1, a_2, \ldots, a_{i-1}$, da velja $a(R \cup E)a_1, a_1(R \cup E)a_2, \ldots, a_{i-1}(R \cup E)b$. Ker je $R \cup E \subseteq Q$, velja tudi $aQa_1, a_1Qa_2, \ldots, a_{i-1}Qb$. Izmed vseh takšnih i-jev izberimo najmanjšega, pri katerem se to zgodi. Ker je i najmanjši, je $a(R \cup E)^{i-1}a_{i-1}$ in tudi aQa_{i-1}. Sedaj imamo aQa_{i-1} in $a_{i-1}Qb$, toda $a \neg Qb$, kar je protislovje s tranzitivnostjo Q. Zato je R^* najmanjša refleksivno-tranzitivna relacija, ki vsebuje R.

Dokažimo še točko (v). Seveda je $R \subseteq R^e$. Relacija $R^{-1} \cup E \cup R$ je refleksivna in simetrična po (i) in (iii) izreka 7.4. Hkrati je $R^e = \cup_{i=1}^{\infty}(R^{-1} \cup E \cup R)^i$ tudi tranzitivna zaradi točke (iii). Torej je R^e refleksivna, simetrična in tranzitivna hkrati, oziroma ekvivalenčna na kratko. Da je R^e najmanjša ekvivalenčna relacija, ki vsebuje R, dokažemo na enak način kot v točkah (iii) in (iv), le da $\overline{R}$ v (iii) oziroma $(R \cup E)$ v (iv) nadomestimo z $R^{-1} \cup E \cup R$. ■

Iz zadnjega izreka lahko vidimo, da če znamo poiskati tranzitivno ovojnico, potem tudi s preostalimi nimamo težav. Tranzitivno ovojnico lahko poiščemo s Floyd-Warshallovim[15] algoritmom, ki ga lahko izvršimo v $O(n^3)$ časa, saj vsebuje tri for zanke.

Algoritem 13: Floyd-Warshallov algoritem za iskanje tranzitivne ovojnice

Vhod: Relacija $R \subseteq A \times A$, kjer množica A vsebuje n elementov, podana z $n \times n$ matriko R.
Izhod: Tranzitivna ovojnica $\overline{R}$ shranjena v matriko R.

```
for i = 1 : n do
    for j = 1 : n do
        if jRi then
            for k = 1 : n do
                if iRk then
                    jRk
                end
            end
        end
    end
end
```

15 Robert W. Floyd (1936-2001) je bil ameriški računalničar, ki najbolj slovi ravno po tem algoritmu. Stephen Warshall (1935-2006) je bil ameriški računalničar, ki je, razen tega algoritma, bil dejaven tudi na razvoju operacijskih sistemov in računalniških jezikov.

Zgled 7.29 *Poiščimo vseh pet omenjenih ovojnic za relacijo R_1, ki smo jo uporabljali v razdelku 7.1 in je*

$$R_1 = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Po izreku 7.7 lahko takoj zapišemo matriki za $\widetilde{R_1}$ in $\widehat{R_1}$, ki sta

$$\widetilde{R_1} = \begin{bmatrix} \mathbf{1} & 1 & 0 & 1 & 1 \\ 1 & \mathbf{1} & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 1 & 0 & \mathbf{1} \end{bmatrix} \text{ in } \widehat{R_1} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & \mathbf{1} & 1 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Omenimo, da so spremembe označene v krepko poudarjenem slogu. V nadaljevanju bomo poiskali tranzitivne ovojnice relacij R_1, $\widetilde{R_1}$ in $R_1^{-1} \cup E \cup R_1$, ter s tem dobili po vrsti $\overline{R_1}$, R_1^* in R_1^e. To bomo storili po korakih zunanje zanke Floyd-Warshallovega algoritma, kjer nam i predstavlja številko vrstice (ozirom stolpca), ki je trenutno aktualna. Mesta, kjer pride do spremembe na ustreznem koraku, bodo krepko poudarjena. V tistih korakih algoritma, kjer ne pride do sprememb matrike, le te ne bomo na novo izpisovali.

$$R_1 = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & \mathbf{0} & 1 & \mathbf{0} & \mathbf{0} \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{i=1} \begin{bmatrix} \mathbf{0} & 1 & \mathbf{0} & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$\xrightarrow{i=2} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{i=3} \xrightarrow{i=4} \xrightarrow{i=5} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} = \overline{R_1}.$$

Dodajmo podrobnejšo razlago. Ko je $i = 1$, imamo $2R_11$ in $1R_12$, prav tako imamo $2R_11$ in $1R_14$ ter na koncu še $2R_11$ in $1R_15$. Zato se 0 na mestih $(2,2)$, $(2,4)$ in $(2,5)$ na tem koraku spremeni v 1. To lahko alternativno opišemo tudi tako, da za vsako 1 v prvem stolpcu ($i = 1$) prečrtamo ustrezno vrstico (v našem primeru drugo vrstico). Nato za vsako 1 v prvi vrstici ($i = 1$) prečrtamo ustrezen stolpec (v našem primeru drugi, četrti in peti stolpec). Povsod, kjer se omenjene črte sekajo na 0, le-to spremenimo v 1. Nato nadaljujemo z naslednjim korakom ($i = 2$) in tako naprej do konca. Določimo še $\widetilde{R_1}$ in $R_1^{-1} \cup E \cup R_1$.

$$\widetilde{R_1} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & \mathbf{0} & \mathbf{0} \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} \xrightarrow{i=1} \begin{bmatrix} 1 & 1 & \mathbf{0} & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} \xrightarrow{i=2}$$

$$\xrightarrow{i=2} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} \xrightarrow{i=3} \xrightarrow{i=4} \xrightarrow{i=5} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} = R_1^*.$$

$$R_1^{-1} \cup E \cup R_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & \mathbf{0} & \mathbf{0} \\ 0 & 1 & 1 & 0 & 1 \\ 1 & \mathbf{0} & 0 & 1 & \mathbf{0} \\ 1 & \mathbf{0} & 1 & \mathbf{0} & 1 \end{bmatrix} \xrightarrow{i=1} \begin{bmatrix} 1 & 1 & \mathbf{0} & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ \mathbf{0} & 1 & 1 & \mathbf{0} & 1 \\ 1 & 1 & \mathbf{0} & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\xrightarrow{i=2} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{i=3} \xrightarrow{i=4} \xrightarrow{i=5} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} = R_1^e.$$

Vidimo, da so se vse spremembe pri iskanju tranzitivne ovojnice v vseh treh primerih zgodile v prvih dveh korakih zunanje zanke. To seveda ni pravilo, pač pa naključje. Omenimo še, da je ekvivalenčna ovojnica R_1^e kar polna relacija, saj je enaka celotnemu kartezičnemu produktu $A \times A$. To hkrati pomeni, da ima le en ekvivalenčni razred. Takšni primeri niso preveč zanimivi v praksi, saj v tem primeru z ekvivalenčno ovojnico ničesar ne pridobimo.

7.6 UREJENOSTI IN POSEBNI ELEMENTI

Relacija $R \subseteq A \times A$

- **delno ureja množico** A, če je R tranzitivna, refleksivna in antisimetrična;
- **linearno ureja množico** A, če je R tranzitivna, strogo sovisna in antisimetrična;
- **strogo delno ureja množico** A, če je R tranzitivna in asimetrična;
- **strogo linearno ureja množico** A, če je R tranzitivna, sovisna in asimetrična.

Iz definicije je takoj razvidno, da je linearna urejenost hkrati tudi delna urejenost, saj stroga sovisnost poraja refleksivnost (zgled 7.11). Prav tako je očitno tudi strogo linearna urejenost vedno tudi strogo delna urejenost.

Zgled 7.30 *Osnovni zgled za*

- delno urejenost je relacija $\subseteq \subseteq \mathcal{P}(A) \times \mathcal{P}(A)$, kjer je $\mathcal{P}(A)$ potenčna množica neke množice A (zgled 7.20);
- linearno urejenost je relacija $\leq \subseteq \mathbb{R} \times \mathbb{R}$, kjer lahko realna števila nadomestimo tudi z naravnimi, celimi ali racionalnimi (zgled 7.18);
- strogo delno urejenost je relacija $\subset \subseteq \mathcal{P}(A) \times \mathcal{P}(A)$, kjer je $\mathcal{P}(A)$ potenčna množica neke množice A (zgled 7.21);
- strogo linearno urejenost je relacija $< \subseteq \mathbb{R} \times \mathbb{R}$, kjer lahko realna števila nadomestimo tudi z naravnimi, celimi ali racionalnimi (zgled 7.19).

Zgled 7.31 *Relacija deljivosti* $\mid \subseteq \mathbb{N} \times \mathbb{N}$ *delno ureja množico* $\mathbb{N}$*, saj je tranzitivna, refleksivna in antisimetrična (zgled 7.16). Spomnimo se še, da je v omenjenem zgledu tudi razloženo, zakaj* $\mid$ *ni antisimetrična za cela števila. Tako* $\mid$ *ne ureja delno množice* $\mathbb{Z}$*.*

Naj bo $R \subseteq A \times A$. Definirajmo **posebne elemente** relacije R. Element $x \in A$ je

- R-**minimalni element**, če za vsak $y \in A$, $y \neq x$, velja $y \neg R x$;
- R-**maksimalni element**, če za vsak $y \in A$, $y \neq x$, velja $x \neg R y$;
- R-**prvi element**, če za vsak $y \in A$ velja xRy;
- R-**zadnji element**, če za vsak $y \in A$ velja yRx.

Posebne elemente si drugače razložimo tudi na naslednji način. Element x je R-minimalni, če noben od njega različen element ni v relaciji z njim. To pomeni, da je edina dovoljena puščica vanj le zanka, če seveda obstaja. Podobno je x R-maksimalni element, če x ni v relaciji z nobenim od njega različnim elementom. To pomeni, da je edina dovoljena puščica iz njega le zanka, če seveda obstaja. Pogoj za R-prvi element x je še strožji, saj mora biti v relaciji R z vsemi preostalimi. Ali drugače, z digrafi, iz njega moramo imeti puščico v vse preostale elemente množice A vključno z zanko. Podobno morajo biti vsi elementi množice A v relaciji z elementom x, vključno z zanko, da x poimenujemo R-zadnji element. Oziroma z digrafi, iz vsakega elementa množice A moramo imeti puščico v x.

Tudi matrike relacij nam omogočajo enostavno prepoznavanje posebnih elementov. Tako je R-prvi element vsak, katerega pripadajoča vrstica vsebuje same enice, saj to pomeni, da je v relaciji R z vsemi drugimi elementi množice A. Podobno prepoznamo R-zadnje elemente po samih enicah v pripadajočem stolpcu, kar zagotavlja, da so vsi preostali elementi iz množice A v relaciji R z njim. Po drugi strani nam R-maksimalnost elementa zagotavljajo ničle v pripadajoči vrstici z možnostjo enice na diagonali. Podobno je element R-minimalni, če je v njegovem stolpcu najti same ničle z možno izjemo enice na diagonali.

Zgled 7.32 *Relacija*

$$R_1 = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix},$$

ki smo jo definirali v razdelku 7.1, nima R_1-minimalnega elementa, saj je bR_1a, aR_1b, bR_1c, aR_1d in aR_1e in v vsak element pride vsaj ena puščica, ki ni zanka. Zato pa sta c in d oba R_1-maksimalna elementa, saj iz d ni nobene puščice navzven in iz c le zanka, ki nas ne moti pri R_1-maksimalnih elementih. Relacija R_1 nima R_1-prvega niti R_1-zadnjega elementa. To lahko vidimo iz matrike za R_1 zato, ker v njej ni nobene vrstice oziroma stolpca samih enic.

Zgled 7.33 *Spomnimo se ekvivalenčne ovojnice R_1^e iz zgleda 7.29. Le ta je bila*

$$R_1^e = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

ki bi ji lahko rekli tudi polna relacija, saj je $R_1^e = \{a,b,c,d,e\} \times \{a,b,c,d,e\}$. Ni težko videti, da so vsi elementi množice A hkrati R_1^e-prvi in tudi R_1^e-zadnji elementi. Po drugi strani, ne obstaja R_1^e-minimalni element in tudi ne R_1^e-maksimalni element.

Zgled 7.34 *Z $E = \{(x,x) : x \in A\}$ smo označevali množico vseh zank. Na E lahko pogledamo kot na relacijo, saj je $E \subseteq A \times A$. Matrika relacije E ima enice na diagonali, povsod drugod pa so ničle. Zato so vsi njeni elementi hkrati R-minimalni in tudi R-maksimalni. Po drugi strani E nima R-prvega niti R-zadnjega elementa, če le množica A vsebuje vsaj dva elementa.*

Zgled 7.35 *Naj bo A množica in $P(A)$ njena potenčna množica. Relacija $\subseteq$, ki delno ureja $P(A)$, ima $\subseteq$-prvi element $\emptyset$, saj je prazna množica podmnožica vseh podmnožic množice A in $\subseteq$-zadnji element A, saj je vsaka podmnožica množice A kar podmnožica množice A. Pojasnimo nenavaden zadnji stavek: vsak element množice $P(A)$, kar je podmnožica množice A, mora biti v relaciji $\subseteq$ z $\subseteq$-zadnjim elementom, ki je ponovno množica A.*

Zgled 7.36 *Kot že vemo, relacija | delno ureja množico* $\mathbb{N}$. *Seveda* 1 *deli vsako izmed naravnih števil in je zato |-prvi element. Hkrati je* 1 *tudi |-minimalni element, saj samo* 1 *deli* 1, *nobeno naravno število različno od* 1 *pa ga ne deli. Po drugi strani poljubno naravno število* n *vedno deli* $2n$. *Zato ne obstajata |-zadnji in |-maksimalni element, saj iz vsakega elementa poteka vsaj ena puščica navzven (pravzaprav jih je neskončno mnogo). Poglejmo si še, kaj se spremeni, če se namesto na naravna števila omejimo na njihovo podmnožico* $\mathbb{N} - \{1\}$. *Sedaj nimamo |-prvega elementa, saj vsak* $n \in \mathbb{N} - \{1\}$ *ne deli* $n + 1$. *Po drugi strani imamo precej več |-minimalnih elementov. To so vsa praštevila, ki jih je neskončno mnogo po trditvi 6.16. Vsako praštevilo* p *ima natanko dva različna delitelja* 1 *in* p. *Ker* 1 *ni v množici* $\mathbb{N} - \{1\}$, *ostane le še en delitelj* p, *ki pa je zanka in je dovoljena za minimalne elemente. Pri |-zadnjih in |-maksimalnih elementih ni razlike med množicama* $\mathbb{N} - \{1\}$ *in* $\mathbb{N}$.

Kot smo videli iz zgornjih zgledov, se glede posebnih elementov relacije lahko primerijo raznovrstne reči. V nadaljevanju si bomo ogledali nekaj trditev, ki to raznovrstnost zelo omejijo v primeru (strogo) delnih urejenosti in posledično tudi v primeru (strogo) linearnih urejenosti.

Trditev 7.8 *Naj relacija* R *(strogo) delno ureja množico* A. *Tedaj v* A *obstaja največ en* R*-prvi in največ en* R*-zadnji element.*

Dokaz. Naj relacija R (strogo) delno ureja množico A. Predpostavimo, da sta x in y oba R-prva elementa. Ker je x R-prvi element, velja za vsak $z \in A$, da je xRz. Izberimo $z = y$ in dobimo xRy. Podobno, ker je y R-prvi element, velja za vsak $z \in A$, da je yRz. Izberimo $z = x$ in dobimo yRx. Tako imamo xRy in yRx.

Če R delno ureja A, potem je R antisimetrična in iz xRy in yRx sledi $x = y$. Torej so vsi R-prvi elementi delno urejene množice enaki, oziroma je največ en (če obstaja).

Če R strogo delno ureja A, potem je R asimetrična in xRy in yRx poraja protislovje. Tako lahko obstaja največ en (če obstaja) R-prvi element v strogo delni urejeni množici.

Dokaz je enak tudi v primeru R-zadnjih elementov, le da upoštevamo definicijo R-zadnjih elementov. ∎

Naj bo $R \subseteq A \times A$ in naj bodo $a_1, a_2, \ldots, a_k \in A$ različni elementi. Zaporedju $a_1 a_2 \ldots a_k$ rečemo **pot dolžine** $k - 1$, če je $a_1 R a_2$, $a_2 R a_3, \ldots, a_{k-1} R a_k$. Zaporedju $a_1 a_2 \ldots a_k a_1$ rečemo **sklenjeni osnovni sprehod dolžine** k, če je $a_1 R a_2$, $a_2 R a_3, \ldots, a_{k-1} R a_k$ in $a_k R a_1$. Tako je zanka $a_1 a_1$ sklenjeni osnovni sprehod dolžine 1, medtem ko je $a_1 a_2 a_1$ sklenjeni osnovni sprehod dolžine 2, če le velja $a_1 R a_2$ in $a_2 R a_1$.

Trditev 7.9 *Naj relacija R delno ureja množico A. Tedaj lahko v A obstajajo le sklenjeni osnovni sprehodi dolžine ena (kar so zanke).*

Dokaz. Recimo, da obstaja sklenjeni osnovni sprehod $a_1a_2 \ldots a_ka_1$ dolžine $k > 1$. Torej so $a_1, a_2, \ldots, a_k \in A$ različni. Torej velja a_1Ra_2 in a_2Ra_3. Zaradi tranzitivnosti imamo a_1Ra_3. Sedaj imamo a_1Ra_3 in a_3Ra_4, kar zaradi tranzitivnosti R pomeni a_1Ra_4. S tem lahko nadaljujemo, dokler ne dobimo a_1Ra_k. Če k temu dodamo še a_kRa_1, velja $a_1 = a_k$ zaradi antisimetričnosti R. To pa je protislovje z definicijo osnovnega sklenjenega sprehoda, saj sta a_1 in a_k različna. Torej v delnih urejenostih ne obstajajo daljši osnovni sprehodi od zank. ∎

Trditev 7.10 *Naj relacija R strogo delno ureja množico A. Tedaj v A ni sklenjenih osnovnih sprehodov.*

Dokaz. Recimo, da obstaja sklenjeni osnovni sprehod $a_1a_2 \ldots a_ka_1$. Torej so $a_1, a_2, \ldots, a_k \in A$ različni. Velja a_1Ra_2 in a_2Ra_3. Zaradi tranzitivnosti imamo a_1Ra_3. Sedaj imamo a_1Ra_3 in a_3Ra_4, kar zaradi tranzitivnosti R pomeni a_1Ra_4. S tem lahko nadaljujemo, dokler ne dobimo a_1Ra_k. Če k temu dodamo še a_kRa_1, dobimo protislovje zaradi asimetričnosti R. Torej v strogo delnih urejenostih sklenjeni osnovni sprehodi ne obstajajo. ∎

Trditev 7.11 *Naj relacija R (strogo) delno ureja končno množico A. Tedaj v A obstaja vsaj en R-minimalni in vsaj en R-maksimalni element.*

Dokaz. Naj relacija R (strogo) delno ureja končno množico A in naj bo a_1 poljuben element iz množice A. Če je a_1 R-maksimalni element, smo končali. Sicer obstaja $a_2 \in A$, ki je različen od a_1, in zanju velja a_1Ra_2. Če je a_2 R-maksimalni element smo končali. Sicer obstaja $a_3 \in A$, ki je različen od a_2, in zanju velja a_2Ra_3. S tem postopkom lahko nadaljujemo. Ker je A končna množica, se mora ta postopek ali ustaviti, ali pa se nek element ponovi. Ker bi nam ponovitev elementa prinesla osnovni sprehod daljši kot ena, imamo protislovje s trditvijo 7.9 v primeru delne urejenosti in s trditvijo 7.10 v primeru strogo delne urejenosti. Skratka, omenjeni postopek se ustavi in zadnji element a_k je R-maksimalni element.

Enak dokaz je tudi v primeru R-minimalnega elementa, le da upoštevamo definicijo R-minimalnega elementa. ∎

Trditev 7.12 *Naj relacija R (strogo) delno ureja množico A in naj bo $B \subset A$. Tedaj R (strogo) delno ureja tudi množico B.*

Dokaz. Naj relacija R (strogo) delno ureja množico A in naj bo $B \subset A$. Če R ni tranzitivna, refleksivna, antisimetrična ali asimetrična na B, potem enaka lastnost tudi ni izpolnjena za A, kar ni mogoče. Zato R (strogo) delno ureja tudi množico B. ∎

Zgled 7.37 *V zgledu 7.31 smo videli, da relacija deljivosti delno ureja množico naravnih števil. Po trditvi 7.12 relacija deljivosti delno ureja katerokoli podmnožico naravnih števil. Tako ureja tudi množico vseh deliteljev nekega izbranega naravnega števila n, ki je* $\mathrm{del}(n) = \{x \in \mathbb{N} : x|n\}$. *Bolj splošno lahko definiramo množico deliteljev dveh naravnih števil* $\mathrm{del}(m,n) = \{x \in \mathbb{N} : x|m \vee x|n\}$ *ali celo več naravnih števil* $\mathrm{del}\{n_1,\ldots,n_k\} = \{x \in \mathbb{N} : x|n_1 \vee \cdots \vee x|n_k\}$, *ki sta prav tako delno urejeni z relacijo deljivosti po trditvi 7.12.*

Trditev 7.13 *Naj bo $R \subseteq A \times A$ tranzitivna relacija brez osnovnih sprehodov dolžine več kot ena. Tedaj obstaja natanko ena intranzitivna relacija R', da velja $\overline{R'} = R$.*

Dokaz. Naj bo R tranzitivna relacija brez osnovnih sprehodov dolžine več kot ena. Relacijo R' dobimo iz R tako, da odstranimo vse pare aRb iz relacije R, za katere obstaja pot dolžine več kot ena med a in b v R. Če R' ni intranzitivna, potem obstajajo $a,b,c \in A$, da velja $aR'b, bR'c$ in $aR'c$, kar je že protislovje, saj imamo med a in c pot dolžine dva in zato $a\neg R'c$. Torej je R' intranzitivna. Seveda je $R' \subseteq R$ in je po definiciji tranzitivne ovojnice tudi $\overline{R'} \subseteq R$, saj je R tranzitivna.

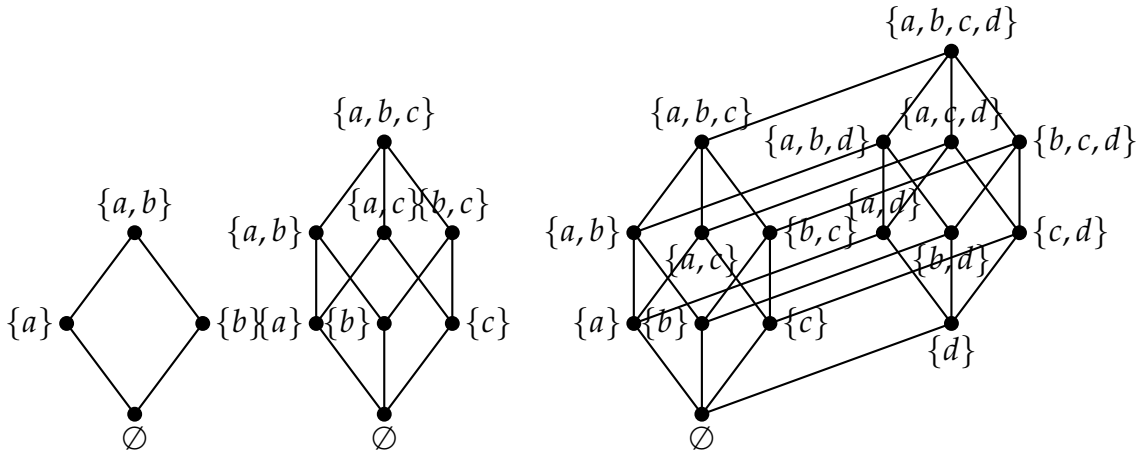
Pokažimo še, da je tudi $R \subseteq \overline{R'}$. Naj bo aRb poljuben element relacije R. Naj bo $P = aa_1a_2\ldots a_kb$ najdaljša pot v R med a in b. Pokažimo, da je tudi $a\overline{R'}b$ z indukcijo na dolžino najdaljše poti, ki je $n = k+1$. Če je $n = 1$, potem je tudi $aR'b$ in sledi tudi $a\overline{R'}b$. Naj bo sedaj $n > 1$. Po indukcijski predpostavki je $x\overline{R'}y$, če ima najdaljša pot med elementoma x in y v R dolžino manj kot n. Dolžina najdaljše poti med elementoma a in a_k v R je $k = n-1$, saj bi daljša pot med njima implicirala daljšo pot med a in b. Po indukcijski predpostavki je $a\overline{R'}a_k$. Če med a_k in b v R obstaja pot P' dolžine več kot ena, potem $aa_1a_2\ldots a_kP'$ pomeni daljšo pot med a in b v R, kar ni mogoče zaradi izbire P, ali osnovni sprehod dolžine več kot ena, če je $a_i \in P'$ za nek $i \in [k-1]$. Torej je $a_k\overline{R'}b$. Zaradi tranzitivnosti $\overline{R'}$ iz $a\overline{R'}a_k$ in $a_k\overline{R'}b$ sledi $a\overline{R'}b$ in velja tudi $R \subseteq \overline{R'}$. ∎

Digrafu intranzitivne relacije R' iz zadnje trditve rečemo tudi **Hassejev[16] diagram**. Zaradi trditev 7.9 in 7.10 se Hassejevi diagrami dobro odrežejo na delnih in strogo delnih urejenostih. Trditev 7.11 pa implicira uporabnost Hassejevih diagramov za končne množice. V tem primeru lahko Hassejev diagram definiramo tudi na drugačen način. Naj torej $R \subseteq A \times A$ (strogo) delno ureja A, kjer je A končna množica. Element $b \in A$ je **neposredni naslednik** elementa $a \in A$, če je aRb in ne obstaja $c \in A$, za katerega velja aRc in cRb. Z drugimi besedami, b je neposredni naslednik a, če med njima ni poti dolžine več kot ena. (Na podoben način bi lahko definirali tudi neposrednega predhodnika, ki ga pa tukaj ne potrebujemo.) Elemente množice A razdelimo v nivoje na naslednji način.

16 Helmut Hasse (1898–1979) je bil nemški matematik, ki se je med drugim ukvarjal z algebrajsko teorijo števil in Diofantsko geometrijo. Hassejevi diagrami so poimenovani po njem, ker je te diagrame učinkovito uporabljal.

- Nivo 1 N_1 tvorijo vsi R-minimalni elementi množice A.
- Nivo 2 N_2 tvorijo vsi R-minimalni elementi množice $A - N_1$.
- Nivo 3 N_3 tvorijo vsi R-minimalni elementi množice $A - (N_1 \cup N_2)$.

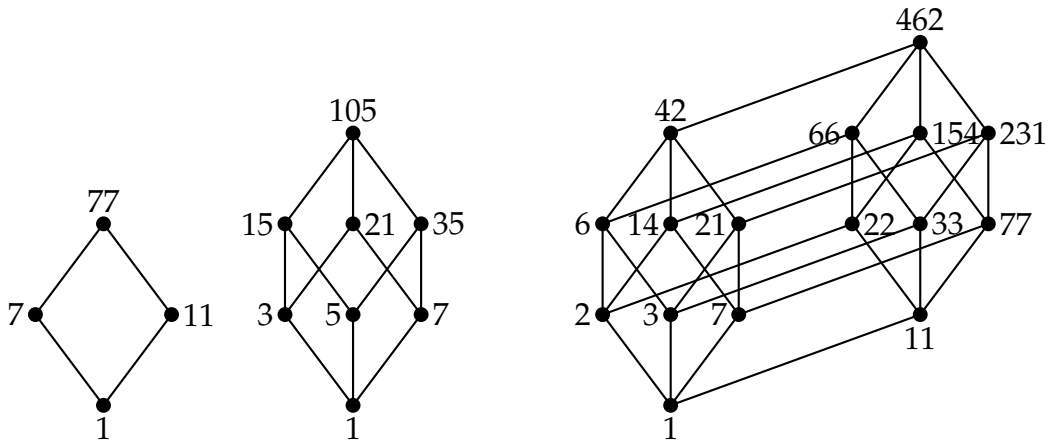
S tem nadaljujemo, dokler nismo razporedili vseh elementov množice A v nivoje. Predpostavimo, da imamo k nivojev. Seveda je vsak element iz A v natanko enem nivoju. Zaradi trditve 7.12 relacija R (strogo) delno ureja tudi množico $A - (N_1 \cup N_2 \cup \cdots \cup N_i)$ za vsak $i \in [k]$. Po trditvi 7.11 je vsak nivo tudi neprazen. Običajno narišemo elemente iz istega nivoja v enaki horizontalni liniji, pri čemer začnemo spodaj s prvim nivojem, ki mu sledi drugi nivo in tako naprej. Definirajmo še, kdaj med elementoma iz različnih nivojev narišemo črto, ki ji rečemo **povezava**. Od elementa $x \in N_i$ narišemo povezavo do elementa $y \in N_j$, $i < j$, če je y neposredni naslednik od x. S tem narišemo Hassejev diagram, ki je pravzaprav digraf relacije R' brez osti na puščicah z dodatno določenim nivojem vozlišč digrafa. Ob tem velja, da sta različna elementa $a, b \in A$ v relaciji R, če sta v različnih nivojih $a \in N_i$ in $b \in N_j$, $i < j$, in lahko iz a pridemo do b po poti, ki vodi le navzgor. Do konca tega razdelka si oglejmo nekaj primerov Hassejevih diagramov.



Slika 11: Hassejev diagram potenčne množice $\mathcal{P}(X)$ za $X = \{a, b\}$ (na levi), $X = \{a, b, c\}$ (na sredini) in $X = \{a, b, c, d\}$ (na desni).

Na sliki 11 so predstavljeni trije Hassejevi diagrami potenčne množice $\mathcal{P}(A)$. Ob tem je za levi diagram množica $A = \{a, b\}$ sestavljena iz dveh elementov, na srednjem diagramu vsebuje $A = \{a, b, c\}$ tri elemente in na desnem diagramu štiri elemente $A = \{a, b, c, d\}$. Podobni diagrami so na sliki 12, le da so tokrat prikazani Hassejevi diagrami za množico $\mathrm{del}(n)$, ki je delno urejena z relacijo deljivosti (glej zgled 7.37). Bolj natančno, na levem diagramu slike 12 je prikazan Hassejev diagram množice $\mathrm{del}(77)$, na sredi je Hassejev diagram množice

del(105) in na desni Hassejev diagram množice del(462). Seveda Hassejevi diagrami s slike 11 niso enaki Hassejevim diagramom s slike 12, saj imajo prvi za elemente podmnožice množice A, drugi pa števila, ki delijo neko število n. Če pa odmislimo to podrobnost, je struktura Hassejevih diagramov s slike 11 enaka strukturi Hassejevih diagramov s slike 12. Ker se to večkrat dogaja, se pogosto lotimo preučevanja zgolj strukture Hassejevih diagramov in odmislimo iz katere matematične strukture oziroma relacije smo jih dobili. V to smer bomo zavili v naslednjem poglavju.



Slika 12: Hassejev diagram množice del(77) (na levi), del(105) (na sredini) in del(462) (na desni).

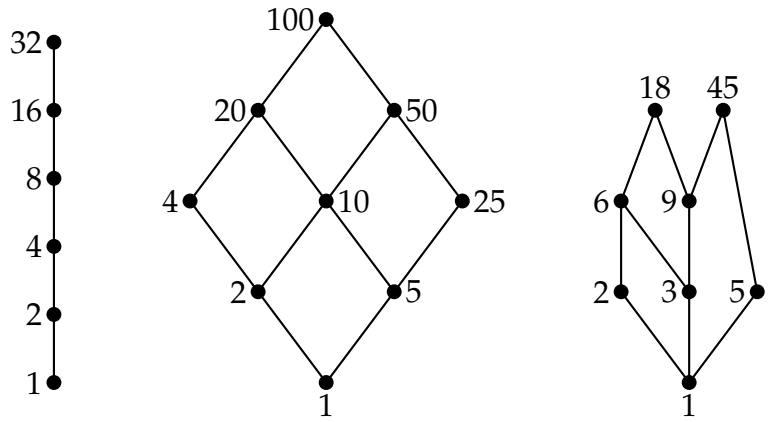
Na sliki 13 so še Hassejevi diagrami množic del(32) (levo), del(100) (sredina) in del(18, 45) (desno). Opazimo lahko, da množica del(32) ni zgolj delno urejena z relacijo deljivosti, temveč jo deljivost celo linarno ureja. Po drugi strani imamo z del(18, 45) primer Hassejevega diagrama, v katerem obstaja povezava med elementom drugega in elementom četrtega nivoja. Prav tako omenimo, da imajo vsi Hassejevi diagrami s slik 11, 12 in 13 prvi in zadnji element z izjemo desnega Hassejevega diagrama za del(18, 45), ki nima zadnjega elementa, ima pa dva $|$-maksimalna elementa, ki sta 18 in 45.

7.7 NEKATERE (NE)REŠENE NALOGE

Vaja 7.1 *Na množici vseh ljudi imamo definirane naslednje relacije:*

$$xLy \Leftrightarrow x \text{ in } y \text{ sta rojena v istem letu;}$$
$$aSb \Leftrightarrow a \text{ in } b \text{ imata istega (vsaj enega) starša;}$$
$$uMv \Leftrightarrow u \text{ in } v \text{ sta obiskala isto mesto.}$$

Ali so te tri relacije ekvivalenčne? Če katera izmed njih je, določite njene ekvivalenčne razrede. Določite še S^2, $M * M^{-1}$ *in* $M^{-1} * M$.



Slika 13: Hassejev diagram množice del(32) (na levi), del(100) (na sredini) in del(18, 45) (na desni).

Rešitev. *Relacija L je ekvivalenčna, v enem ekvivalenčnem razredu so vsi ljudje rojeni istega leta. S in M nista ekvivalenčni (ne velja tranzitivnost). Zveza aS^2b pomeni, da imata a in b istega (pol)brata ali (pol)sestro. Ker je M simetrična relacija, velja $M * M^{-1} = M^{-1} * M = M^2$. Elementa u in v sta v relaciji M^2, kadar obstaja nek človek, ki je obiskal isto mesto kot u in isto mesto kot v.*

Vaja 7.2 *Na množici celih števil definiramo relacijo*

$$R = \{(m, n)\,;\ mn > 0\} \cup \{(0, 0)\}\,.$$

Pokažite, da je R ekvivalenčna relacija in določite ekvivalentne razrede.

Rešitev. *Ker velja $m^2 > 0$ ali $m = 0$ za vsak $m \in \mathbb{Z}$, je mRm in je R refleksivna. Če je mRn, potem je $mn > 0$ ali $m = n = 0$. To pomeni tudi, da je $nm > 0$ ali $n = m = 0$ in sledi nRm. Torej je R simetrična. Naj bo še mRn in nRp. Če sta $mn > 0$ in $np > 0$, potem imajo m, n in p enake predznake in je tudi $mp > 0$, oziroma mRp. Za dokončanje tranzitivnosti preverimo še drugo možnost $m = 0 = n$, kar pomeni tudi $n = 0 = p$. Torej je $m = 0 = p$ in ponovno velja mRp. Pokazali smo, da je R ekvivalenčna relacija. Ima le tri ekvivalenčne razrede $[1] = \{x \in \mathbb{N}\}$, $[-1] = \{x : -x \in \mathbb{N}\}$ in $[0] = \{0\}$.*

Vaja 7.3 *Na množici $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ je definirana relacija R s predpisom*

$$mRn \Leftrightarrow (m \mid n) \vee (n \mid m)\,.$$

Preverite, ali je R ekvivalenčna relacija.

Rešitev. *Ker $2R6$ in $6R3$ in $2\neg R3$, relacija ni tranzitivna in s tem tudi ni ekvivalenčna. (Sicer je R refleksivna in simetrična.)*

Vaja 7.4 *Na množici celih števil je definirana relacija R s predpisom*

$$aRb \Leftrightarrow 5 \mid (3a + 2b)\,.$$

Ali je R ekvivalenčna relacija? Če je, določite še ekvivalenčne razrede!

Rešitev. *Ker 5 deli $3a + 2a = 5a$, je R refleksivna. Za simetričnost naj velja aRb, kar pomeni, da $5|\,(3a + 2b)$. Z drugim zapisom imamo $3a \equiv -2b \pmod 5$, kateremu prištejemo $5b - 5a$, da dobimo $-2a + 5b \equiv 3b + 5a \pmod 5$ oziroma $3b \equiv -2a \pmod 5$. Torej velja tudi $5|(3b + 2a)$ in R je simetrična. Za tranzitivnost naj bo aRb in bRc. Torej $3a + 2b = 5k$ in $3b + 2c = 5\ell$. Ko enačbi seštejemo in uredimo, dobimo $3a + 2c = 5(k + \ell - b)$. Torej $5|(3a + 2c)$ oziroma aRc in tranzitivnost velja. Ekvivalenčnih razredov je pet in sicer $[k] = \{k + 5\ell : \ell \in \mathbb{Z}\}$ za $k \in [4]_0$. Račun, ki to potrdi, je sledeč: $2(k + 5\ell) + 3(k + 5\ell') = 5(k + \ell + \ell')$.*

Vaja 7.5 *Na množici $\{1, 2, 3, \ldots, 10\}$ je definirana relacija R s predpisom*

$$aRb \Leftrightarrow a - b = 3k,\ k \in \mathbb{Z}.$$

Ali je R ekvivalenčna relacija? Če je, določite še ekvivalenčne razrede!

Rešitev. *Pri reševanju se lahko zgledujemo po prejšnji nalogi, le da so tukaj le trije ekvivalenčni razredi.*

Vaja 7.6 *Za kanonični zapis naravnega števila $n = p_1^{a_1} p_2^{a_2} \ldots p_i^{a_i}$, kjer so $p_1 < p_2 < \ldots < p_i$ praštevila in $a_1, a_2, \ldots, a_i$ naravna števila, priredimo številu n zaporedji:*

$$a(n) = (a_1, a_2, \ldots, a_i, 0, 0, \ldots) \quad in\ p(n) = (p_1, p_2, \ldots, p_i, 0, 0, \ldots).$$

Na množici naravnih števil definiramo relaciji A in P takole:

$$mAn \Leftrightarrow a(m) = a(n)\ in\ mPn \Leftrightarrow p(m) = p(n).$$

Opišite relacijo $A * P$. Katere izmed relacij $A, P, A * P$ so ekvivalenčne?

Rešitev. *Zveza $m(A * P)n$ pomeni obstoj naravnega števila r, za katerega velja mAr in rPn. To hkrati pomeni, da imata m in r enake eksponente v kanoničnem zapisu, r in n pa enaka praštevila v kanoničnem zapisu. Zlahka se obrazloži, da sta A in P ekvivalenčni. Relacija $A * P$ je tudi tranzitivna in s tem tudi ekvivalenčna. Razmislite zakaj!*

Vaja 7.7 *Naj bo $f : A \to B$ surjektivna funkcija. Na A definiramo relacijo $\sim$ s predpisom*

$$a \sim b \Leftrightarrow f(a) = f(b)\,.$$

Dokažite, da je $\sim$ ekvivalenčna relacija in ugotovite, kaj so ekvivalenčni razredi. Kdaj je ekvivalenčnih razredov končno in kdaj številno mnogo?

Rešitev. *V zgledu 7.24 smo pokazali, da je $\sim$ vedno ekvivalenčna (ne le za surjektivne funkcije). Nadalje so v zgledu 7.26 opisani tudi ekvivalenčni razredi relacije $\sim$. Iz surjektivnosti sledi, da je število ekvivalenčnih razredov končno, ko je končna množica B, in številno mnogo, ko je številna množica B.*

Vaja 7.8 *Na realnih številih je definirana relacija $\sim$:*

$$\forall x, y \in \mathbb{R},\ x \sim y \Leftrightarrow x - y \in \mathbb{Z}.$$

Pokažite, da je $\sim$ ekvivalenčna relacija in opišite ekvivalenčne razrede.

Rešitev. *Zlahka se pokaže, da relacija je ekvivalenčna. Ekvivalenčni razredi so: $[x] = \{y \in \mathbb{R} \mid y = x - k, k \in \mathbb{Z}\}$ za vsak $x \in [0, 1)$.*

Vaja 7.9 *Naj bosta $\sim_1$ in $\sim_2$ ekvivalenčni relaciji na množici X.*

(A) *Ugotovite, ali je relacija R definirana s predpisom*

$$\forall x, y \in X,\ xRy \Leftrightarrow (x \sim_1 y) \vee (x \sim_2 y)$$

ekvivalenčna relacija na X!

(B) *Ugotovite, ali je relacija S definirana s predpisom*

$$\forall x, y \in X,\ xSy \Leftrightarrow (x \sim_1 y) \wedge (x \sim_2 y)$$

ekvivalenčna relacija na X!

Rešitev. *Naj bodo $x, y, z \in X$ taki, da velja $x \sim_1 y$, $x\neg \sim_1 z$, $y \sim_2 z$ in $x\neg \sim_2 z$. Potem velja xRy in yRz in $x\neg Rz$, zato R ni tranzitivna in posledično tudi ni ekvivalenčna relacija. Po drugi strani je S ekvivalenčna relacija, kar sledi iz ekvivalenčnosti relacij $\sim_1$ in $\sim_2$ ter lastnosti izjavne povezave $\wedge$.*

Vaja 7.10 *Na množici $\mathbb{Z} \times \mathbb{Z}$ vpeljemo relacijo R s predpisom $(a, b)\ R\ (c, d) \Leftrightarrow ad = bc$. Ali je R ekvivalenčna relacija?*

Rešitev. *Ta relacija ni ekvivalenčna, saj ni tranzitivna. Protiprimer je $(1, 5)R(0, 0)$ in $(0, 0)R(4, -2)$, a $(1, 5)$ ni v relaciji R s $(4, -2)$.*

Vaja 7.11 *Števili m in n iz množice $S = \{00001, 00002, 00003, \ldots, 09999, 10000\}$ sta v relaciji R natanko takrat, ko lahko m dobimo iz n tako, da spremenimo vrstni red cifer števila n. (Na primer $o1301Ro1130$.)*

(A) *Pokažite, da je R ekvivalenčna relacija.*

(B) *Poiščite ekvivalenčni razred števila $o0024$.*

(C) *Koliko je ekvivalenčnih razredov?*

Rešitev. *Zlahka se obrazloži, da je R ekvivalenčna relacija; $[00024] = \{00024, 00204, 00240, 02004, 02040, 02400, 00042, 00402, 00420, 04002, 04020, 04200\}$; za konec je $\#_c = C_p(10, 5) - C_p(9, 5) - 1 = 714$.*

Vaja 7.12 *Na množici $\mathbb{C}-\{0\}$ je definirana relacija $\sim$: $x \sim y \Leftrightarrow \frac{x}{y} \in \mathbb{R}$. Pokažite, da je $\sim$ ekvivalenčna relacija in ugotovite, kaj so ekvivalenčni razredi.*

Rešitev. *Ker je $\frac{x}{x} = 1 \in \mathbb{R}$ za vsak $x \in \mathbb{C}-\{0\}$, je $\sim$ refleksivna. Za simetričnost naj bo $x \sim y$ in s tem $\frac{x}{y} \in \mathbb{R}$. Seveda je inverz realnega števila tudi realno število in velja $\left(\frac{x}{y}\right)^{-1} = \frac{y}{x} \in \mathbb{R}$. Torej je tudi $y \sim x$ in $\sim$ je simetrična relacija. Za dokaz tranzitivnosti naj bo $x \sim y$ in $y \sim z$. Torej velja $\frac{x}{y} \in \mathbb{R}$ in $\frac{y}{z} \in \mathbb{R}$. Ker je produkt dveh realnih števil realno število, velja $\frac{x}{y}\frac{y}{z} = \frac{x}{z} \in \mathbb{R}$. Torej je tudi $x \sim z$ in $\sim$ je tranzitivna in s tem tudi ekvivalenčna relacija. En ekvivalenčni razred tvorijo vsa kompleksna števila, ki pripadajo premici skozi izhodišče brez izhodišča samega. Recimo $[1+i] = \{a(1+i) : a \in \mathbb{R}-\{0\}\}$.*

Vaja 7.13 *Na množici $A = \{a,b,c,d,e,f\}$ imamo definirano relacijo*

$$R = \{(a,e),(b,a),(b,c),(b,f),(c,d),(d,e),(f,e)\}.$$

Poiščite tranzitivno ovojnico $\overline{R}$ relacije R in pokažite, da je $\overline{R}$ strogo delno urejena. Narišite še digraf relacije R.

Rešitev. *Izvedimo Floyd-Warschalov algoritem po zunanji zanki in dobimo*

$$R = \begin{bmatrix} 0&0&0&0&1&0\\ 1&0&1&0&\mathbf{0}&1\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&0\\ 0&0&0&0&1&0 \end{bmatrix} \xrightarrow{i=a} \begin{bmatrix} 0&0&0&0&1&0\\ 1&0&1&\mathbf{0}&\mathbf{1}&1\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&0\\ 0&0&0&0&1&0 \end{bmatrix} \xrightarrow{i=b}\xrightarrow{i=c}$$

$$\xrightarrow{i=c} \begin{bmatrix} 0&0&0&0&1&0\\ 1&0&1&\mathbf{1}&1&1\\ 0&0&0&1&\mathbf{0}&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&0\\ 0&0&0&0&1&0 \end{bmatrix} \xrightarrow{i=d} \begin{bmatrix} 0&0&0&0&1&0\\ 1&0&1&1&1&1\\ 0&0&0&1&\mathbf{1}&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&0\\ 0&0&0&0&1&0 \end{bmatrix} \xrightarrow{i=e}\xrightarrow{i=f}$$

$$\xrightarrow{i=f} \begin{bmatrix} 0&0&0&0&1&0\\ 1&0&1&1&1&1\\ 0&0&0&1&1&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&0\\ 0&0&0&0&1&0 \end{bmatrix} = \overline{R}.$$

Omenimo, da so tiste vrednosti, ki so se spremenile in 0 v 1 v ustreznem koraku, poudarjene krepko. Seveda je $\overline{R}$ tranzitivna. Iz matrike se zlahka vidi, da če imamo na (i,j)-tem mestu 1, potem je na (j,i)-tem mestu 0 (to še posebej velja na (i,i)-tih mestih). To že zadošča za asimetričnost $\overline{R}$. Torej je $\overline{R}$ strogo delno urejena.

Vaja 7.14 *Na množici $A = \{a, b, c, d, e, f\}$ je definirana relacija*

$$R = \{(a,b), (a,e), (b,c), (b,e), (c,b), (d,a), (d,c), (f,e)\}.$$

Opišite korake Floyd-Warschalovega algoritma in tudi izračunajte $\overline{R}$!

Rešitev. *Kot v prejšnji nalogi si oglejmo korake zunanje zanke.*

$$R = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & \mathbf{0} & 1 & 0 & \mathbf{0} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \underset{\longrightarrow}{i=a} \begin{bmatrix} 0 & 1 & \mathbf{0} & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & \mathbf{1} & 1 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \underset{\longrightarrow}{i=b}$$

$$\underset{\longrightarrow}{i=b} \begin{bmatrix} 0 & 1 & \mathbf{1} & 0 & 1 & 0 \\ 0 & \mathbf{0} & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \underset{\longrightarrow}{i=c} \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & \mathbf{1} & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \underset{\longrightarrow}{i=d} \underset{\longrightarrow}{i=e} \underset{\longrightarrow}{i=f}$$

$$\underset{\longrightarrow}{i=f} \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \overline{R}.$$

Vaja 7.15 *Na množici $A = \{a, b, c, d, e, f\}$ je definirana relacija*

$$R = \{(a,d), (b,f), (c,e), (d,b), (e,b), (f,a)\}.$$

S Floyd-Warschalovim algoritmom (korake utemelji) poišči tranzitivno ovojnico $\overline{R}$.

Rešitev. *Matrika tranzitivne ovojnice je* $\overline{R} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$.

Vaja 7.16 *Na množici $A = \{1, 2, \ldots, 8\}$ poišči tranzitivno ovojnico $\overline{R}$ relacije*

$$R = \{(2,3), (2,5), (3,8), (4,1), (4,7), (5,2), (5,6), (6,8), (7,1), (8,2)\}.$$

Ali je $\overline{R}$ ekvivalenčna relacija?

Rešitev. $\overline{R} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$ *ni ekvivalenčna, saj ni simetrična, niti refleksivna.*

Vaja 7.17 *Na množici ljudi je definirana relacija S s predpisom*

$$xSy \Leftrightarrow x \text{ je starš od } y.$$

Ugotovite kaj predstavljajo relacije S^2, S^{-1}, $S * S^{-1}$ in $S^{-1} * S$. Preverite še, ali tranzitivna ovojnica $\overline{S}$ strogo delno ureja množico ljudi.

Rešitev. *Relacije predstavljajo po vrsti: stari starš, otrok, starša istega otroka, otroka istega starša; $\overline{S}$ očitno strogo delno ureja množico ljudi, saj je tranzitivna in asimetrična.*

Vaja 7.18 *Ali je množica $A = \{0, 1, 2, \ldots, 9\}$ z relacijo*

$$S = \left\{ \begin{array}{c} (1,0), (1,2), (1,3), (1,4), (1,5), (1,6), (1,7), (1,8), \\ (1,9), (2,0), (2,4), (2,6), (2,8), (3,6), (3,9), (4,8), (5,0) \end{array} \right\}$$

delno urejena? Poišči še posebne elemente!

Rešitev. *Množica A ni delno urejena s S, saj S ni refleksivna. (Je pa recimo S tranzitivna.) Edini S-minimalni element je 1, ki pa ni S-prvi element, saj ni v relaciji S s sabo. Tudi S-zadnji element ne obstaja, zato pa so 0, 6, 7, 8 in 9 vsi S-maksimalni elementi, saj niso v relaciji S z nobenim drugim elementom.*

Vaja 7.19 *Na množici $A = [n]_0 \times [n]_0$, $n \in \mathbb{N}$, definiramo relacijo R s predpisom*

$$(a,b)\, R\, (c,d) \Leftrightarrow a - b > c - d.$$

Ali je R strogo delno ureja množico A? Poiščite posebne elemente (minimalne in maksimalne ter prvega in zadnjega, če obstajajo).

Rešitev. *Tranzitivnost in asimetričnost R sledita iz tranzitivnosti oziroma asimetričnosti relacije $>$ nad realnimi števili. Torej R strogo delno ureja A. Prvi element relacije R je $(n, 0)$ in zadnji element relacije R je $(0, n)$. Torej je $(n, 0)$ edini R-minimalni element in $(0, n)$ edini R-maksimalni element.*

Vaja 7.20 *Naj bo n naravno število. Na množici $A = [n] \times [n]$ definiramo relacijo R s predpisom*

$$(a, b)R(c, d) \Leftrightarrow a + b > c + d.$$

(A) *Ali relacija R strogo delno ureja množico A?*

(B) *Ali je R sovisna?*

(C) *Poiščite posebne elemente relacije R, če obstajajo.*

Rešitev. *Tranzitivnost in asimetričnost R sledita iz tranzitivnosti oziroma asimetričnosti relacije $>$ nad realnimi števili. Torej R strogo delno ureja A. Protiprimer za sovisnost tvorita recimo $(1, 0)$ in $(0, 1)$. Element (n, n) je v relaciji R z vsemi elementi A, razen s seboj. Zato ni prvi element, saj ni v relaciji s seboj. Tako R nima prvega elementa. Je pa (n, n) R-minimalni, saj noben drugi element ni v relaciji z njim. Podobno je $(1, 1)$ R-maksimalni, vendar ni R-zadnji in zato R-zadnji element ne obstaja.*

Vaja 7.21 *Pokažite, da relacija deljivosti $|$ linearno ureja množico $\mathrm{del}(p^k)$, če je p praštevilo in k naravno število. Predstavi še mrežo $\mathrm{del}(64, D, v)$ s Hassejevim diagramom.*

Rešitev. *Velja $\mathrm{del}(p^k) = \{1, p, p^2, \ldots, p^k\}$ in seveda vsak element te množice deli vse naslednje (z večjim eksponentom). Zlahka se pokaže, da $|$ res ureja $\mathrm{del}(p^k)$ linearno. Potem je tudi jasno kaj je Hassejev diagram od $\mathrm{del}(64, D, v)$.*

8

MREŽE IN BOOLEOVE ALGEBRE

Cilj tega poglavja je predstaviti strukturo, ki je iz mnogo vidikov idealna struktura za svet diskretnih objektov. Matematično rečemo temu Booleova algebra in do nje vodita dve poti. Ena je preko relacij in druga preko algebrskih lastnosti. Tukaj si bomo ogledali obe. Sama struktura, ki je bila napovedana, je Hassejev diagram in predstavlja diskretni model krogle. V zadnjem poglavju, kjer bomo zanemarili nivoje iz Hassejevega diagrama, kot tudi relacijo, ki poraja Hassejev diagram, pa bomo tej strukturi rekli hiperkocka ali r-kocka. Zanimivo je, da lahko do te strukture pridemo z različnimi pristopi, vendar je sam objekt nekako enak. Nekaj teh pristopov bomo tudi predstavili.

Dodatno literatura v slovenščini iz tega področja avtorju ni poznana. V angleškem jeziku je na voljo precej več primerne literature, tukaj omenimo le [1]. Marsikaj je najti tudi na spletu in pogosto je že Wikipedia (angleška) dober začetni vir informacij. Standardna zbirka nalog za to poglavje je [5]. Veliko izpitnih nalog iz tega poglavja je najti v [12, 13].

8.1 MREŽE

Mreže, osrednji pojem tega razdelka, bomo definirali na dva načina: s pomočjo relacij in s pomočjo algebrskih lastnosti. Nato bomo v izreku 8.2 pokazali, da sta oba načina enakovredna. Do tedaj bomo govorili o algebrski mreži in o relacijski mreži, kasneje pa bomo pridevnika algebrska in relacijska opustili, saj med njima ni razlik. Algebrski način lahko zapišemo takoj s pomočjo nekaterih lastnosti, ki smo jih spoznali v uvodnem poglavju.

Množica M skupaj z operacijama $\sqcup, \sqcap : M \times M \to M$, je **algebrska mreža,** če so za poljubne $a, b, c \in M$ izpolnjene naslednje lastnosti:

(i)	$a \sqcup b = b \sqcup a$	in	$a \sqcap b = b \sqcap a$	komutativnost,
(ii)	$(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$	in	$(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)$	asociativnost,
(iii)	$a \sqcup (a \sqcap b) = a$	in	$a \sqcap (a \sqcup b) = a$	absorpcija,
(iv)	$a \sqcup a = a$	in	$a \sqcap a = a$	idempotentnost.

Ker je algebrska mreža M neločljivo povezana z operacijama $\sqcup$ in $\sqcap$, jih bomo skupaj označevali z $(M, \sqcup, \sqcap)$. Oznaki za operaciji $\sqcup$ in $\sqcap$ sta nekako bolj oglata simbola za unijo množic $\cup$ oziroma presek množic $\cap$. To ni naključje, saj bomo v zgledu 8.2 videli, da običajna presek in unija množic izpolnjujeta vse lastnosti algebrske mreže. Omenimo še, da bi lahko zadnjo lastnost, torej idempotentnost, izločili iz definicije, saj sledi iz absorpcije, kot je razvidno iz naslednjih računov, če vpeljemo oznaki $a \sqcap b = c$ in $a \sqcup b = d$:

$$\begin{aligned} a \sqcup a &= a \sqcup (a \sqcap (a \sqcup b)) = a \sqcup (a \sqcap d) = a \\ a \sqcap a &= a \sqcap (a \sqcup (a \sqcap b)) = a \sqcap (a \sqcup c) = a. \end{aligned}$$

Kljub temu smo idempotentnost ohranili v definiciji, ker je tako običajno, lahko bi dejali tudi iz zgodovinskih razlogov.

Zgled 8.1 *Najpreprostejša algebrska mreža je $(B, \vee, \wedge)$, kjer je $B = \{0, 1\}$, operacija $\vee$ je logični **ali** in operacija $\wedge$ je logični **in**. Da operaciji $\vee$ in $\wedge$ izpolnjujeta lastnosti (i)-(iv) iz definicije algebrske mreže, smo videli v razdelku 1.2.*

Zgled 8.2 *Naj bo X poljubna množica in $M = \mathcal{P}(X)$. Torej je M potenčna množica množice X in vsebuje vse podmnožice množice X. Spomnimo se Hassejevih diagramov s slike 11, ki opisujejo ta zgled. Pokažimo, da je $(M, \cup, \cap)$ algebrska mreža za običajno unijo množic $\cup$ in običajni presek množic $\cap$. Naj bodo A, B, C poljubne podmnožice množice X. Seveda je*

$$A \cup B = \{x \in X : x \in A \vee x \in B\} = \{x \in X : x \in B \vee x \in A\} = B \cup A$$

*zaradi komutativnosti **ali**. Podobno velja tudi $A \cap B = B \cap A$, zaradi komutativnosti **in**. S čimer je (i) resnična. Podobno bi lahko formalno zapisali tudi dokaze za resničnost preostalih lastnosti, vendar je le te možno zlahka videti iz Vennovih diagramov za eno (za lastnost (iv)), za dve (za lastnost (iii)), oziroma za tri (za lastnost (ii)) množice. Torej je $(M, \cup, \cap)$ algebrska mreža.*

Za relacijsko definicijo mreže bomo uporabili strukturo, ki smo jo spoznali v zadnjem razdelku prejšnjega poglavja, to je delna urejenost. Najprej moramo vpeljati pojem zgornje oziroma spodnje meje podmnožice B množice A s pomočjo relacije $R \subseteq A \times A$. Naj bo torej $R \subseteq A \times A$ relacija in $B \subseteq A$. Element $z \in A$ je **zgornja meja** množice B, če je bRz za vsak element $b \in B$. Podobno je element $s \in A$ je **spodnja meja** množice B, če je sRb za vsak element $b \in B$.

Včasih igrajo nekatere zgornje oziroma spodnje meje prav posebno vlogo. Zgornja meja z množice B je **natančna zgornja meja** ali **supremum** množice B, če za vsako drugo zgornjo mejo $z' \in A$ množice B velja zRz'. Podobno je spodnja meja s množice B **natančna spodnja meja** ali **infimum** množice B, če za vsako drugo spodnjo mejo s' množice B velja $s'Rs$. Natančno zgornjo mejo množice B označimo s $\sup(B)$ in natančno spodnjo mejo množice B označimo z $\inf(B)$. Omenimo, da supremum in infimum ne obstajata vedno.

Zgled 8.3 *Največ izkušenj glede zgornjih oziroma spodnjih mej imamo z relacijo $\leq$ na realnih številih. Le-ta so celo definirana s pomočjo natančne zgornje meje. O tem govori Dedekindov aksiom iz zgleda 2.15, ki pravi, da ima vsaka navzgor omejena podmnožica realnih števil natančno zgornjo mejo. Iz tega se na enostaven način izpelje podobna trditev za navzdol omejene množice. Tako velja tudi, da ima vsaka navzdol omejena podmnožica realnih števil natančno spodnjo mejo (tudi zgled 2.18). Oglejmo si množico*

$$A = \{x \in \mathbb{R} : x^2 \leq 2\},$$

ki je seveda podmnožica realnih števil. Ni težko videti, da je A navzgor omejena, recimo s 100. Po Dedekindovem aksiomu ima A natančno zgornjo mejo, ki je $\sup(A) = \sqrt{2}$. Podobno je množica $-A = \{x \in \mathbb{R} : -x \in A\}$ navzdol omejena, recimo z -100. Njena natančna spodnja meja je $\inf(-A) = -\sup(A) = -\sqrt{2}$. (S pomočjo trika z množico $-A$ v splošnem pokažemo obstoj $\inf(A)$ za navzdol omejeno množico A.)

Kaj se zgodi, če realna števila v zgornjem primeru nadomestimo z racionalnmi števili? V tem primeru $\sqrt{2} \notin \mathbb{Q}$ in zato $\sup(A)$ ne obstaja med racionalnimi števili. Podobno tudi ne obstaja $\inf(-A)$ med racionalnimi števili. Ta primer se običajno navede v srednji šoli kot motivacija za vpeljavo realnih števil.

Naj bo sedaj B še končna podmnožica realnih (ali racionalnih) števil. V tem primeru natančna zgornja in natančna spodnja meja množice B vedno obstaja in je enaka kar največjemu oziroma najmanjšemu elementu iz množice: $\sup(B) = \max(B)$ in $\inf(B) = \min(B)$.

Zgled 8.4 *Naj bo S množica vseh sodih števil. Oglejmo si relaciji $\leq$ in $<$ na množici naravnih števil. Ni težko videti, da ima S dve spodnji meji glede na relacijo $\leq$, ki sta 1 in 2. Seveda je $\inf_{\leq}(S) = 2$. Po drugi strani ima S za relacijo $<$ le eno spodnjo mejo 1, ki je zato tudi njena natančna spodnja meja. Za obe relaciji množica S nima zgornje meje in zato tudi ne natančne zgornje meje.*

Zgled 8.5 *Oglejmo si relacijo deljivosti na naravnih številih in podmnožico $A = \mathrm{del}(m,n) = \{x \in \mathbb{N} : x|m \vee x|n\}$, ki je delno urejena z relacijo deljivosti (glej zgled 7.37). Tako so v A tista naravna števila, ki delijo vsaj enega izmed m in n. Recimo $\mathrm{del}(15,21) = \{1,3,5,7,15,21\}$. Ni težko videti, da je $1 \in \mathrm{del}(m,n)$ za katerikoli naravni števili m in n. Edini delitelj enke je seveda enka sama in tako je $\inf(A) = 1$, saj 1 deli tudi vsa preostala naravna števila. Tudi natančno zgornjo mejo smo že spoznali in je najmanjši skupni večkratnik števil m in n, torej $\sup(A) = v(m,n)$. Vsa števila iz A delijo $v(m,n)$ in hkrati ni števila x, ki bi delilo $v(m,n)$ in bi vsi elementi iz A delili x po sami definiciji najmanjšega skupnega večkratnika.*

Če množico B tvorijo vsi delitelji naravnega števila n, $B = \mathrm{del}(n)$, seveda velja $\inf(B) = 1$ in $\sup(B) = n$. Za množico C, ki jo sestavljajo delitelji več števil, $\mathrm{del}(n_1, n_2, \ldots, n_k)$, pa imamo $\inf(C) = 1$ in $\sup(C) = v(n_1, n_2, \ldots, n_k)$. Nekaj Hassejevih diagramov množic tega tipa je na slikah 12 in 13.

Zgled 8.6 *Oglejmo si še primer polne relacije R, za katero velja $R = A \times A$. Naj bo B poljubna podmnožica A. Potem je poljuben element množice A njena natančna zgornja meja kot tudi njena natančna spodnja meja in obstaja več natančnih zgornjih oziroma natančnih spodnjih mej.*

Zadnji zgled nas opozarja, da natančne zgornje oziroma spodnje meje niso primerno orodje za vsako relacijo. To se ne more primeriti v primeru delne urejenosti, o čemer govori naslednja trditev.

Trditev 8.1 *Če relacija $R \subseteq A \times A$ delno ureja množico A, potem obstaja največ ena natančna zgornja oziroma največ ena natančna spodnja meja množice $B \subseteq A$.*

Dokaz. Recimo, da obstajata dve natančni zgornji meji a in a' množice B. Po definiciji natančne zgornje meje za a je aRa' in ponovno po definiciji natančne zgornje meje, tokrat za a', velja $a'Ra$. Ker R delno ureja A, je R tudi antisimetrična in velja $a = a'$. Tako je največ ena natančna zgornja meja. Podoben argument velja tudi za natančno spodnjo mejo. ∎

Delno urejena množica M z relacijo R je **relacijska mreža**, če obstajata $\sup(\{a, b\})$ in $\inf(\{a, b\})$ za poljubna $a, b \in M$.

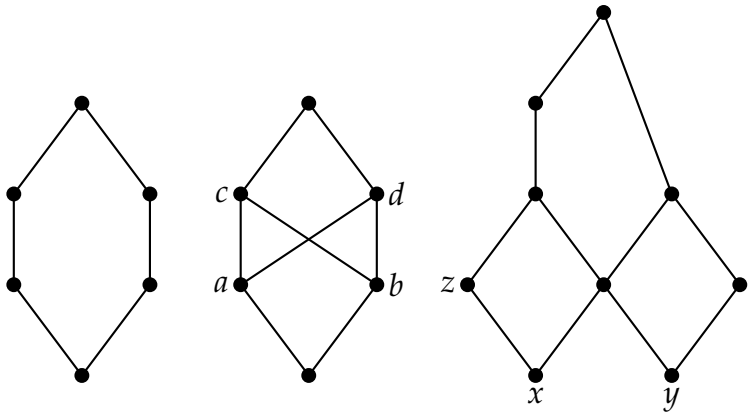
Dogovorimo se, da bomo namesto $\sup(\{a, b\})$ in $\inf(\{a, b\})$, uporabili poenostavljeno notacijo $\sup(a, b)$ in $\inf(a, b)$. Relacijsko mrežo bomo označevali z $(M_R, \sup, \inf)$, saj so iz te označitve razvidni tako množica M, relacija R ter supremum in infimum. Opozorimo posebej, da v zgornji definiciji ni nujno, da obstajata natančna zgornja in natančna spodnja meja vsake podmnožice B množice A, pač pa le tistih podmnožic, ki vsebujejo dva elementa. Ta omejitev lahko privede do razlike le v primeru podmnožice B z neskončnim številom elementov, saj za končno množico B lahko združujemo po dva in dva elementa in tako manjšamo število elementov in na koncu ostanemo z dvema elementoma. To je ponazorjeno z naslednjim računom za $B = \{a, b, c\}$ in $\inf(a, b) = d$:

$$\inf(a, b, c) = \inf(\inf(a, b), c) = \inf(d, c),$$

ki obstaja. Podobno lahko izračunamo tudi $\sup(a, b, c)$. Tako nam obstoj $\sup(a, b)$ in $\inf(a, b)$ zagotavlja tudi obstoj $\sup(B)$ in $\inf(B)$ za vsako končno podmnožico B množice A. Omenimo še, da v primeru, ko je $a = b$, velja $\sup(a, a) = a = \inf(a, a)$ zaradi refleksivnosti relacije R.

V Hassejevem diagramu je supremum elemetov a in b tisti element c iz najnižjega nivoja, da obstaja pot iz a do c, ki gre ves čas navzgor, in tudi pot od b do c, ki se tudi le vzpenja. Do infimuma elementov a in b pridemo na, lahko bi rekli, nasproten način. Tako je $\inf\{a, b\} = d$ element iz najvišjega nivoja Hassejevega diagrama, da obstajata poti med a in d ter med b in d, ki obe vodita samo navzdol.

Zgled 8.7 *Na slikah 11, 12 in 13 vsi primeri Hassejevih diagramov tvorijo mrežo, razen* $\mathrm{del}\{18,45\}$*, ki je desni diagram na sliki 13. Le-ta nima* $\sup(18,45)$*, saj sta ta dva elementa maksimalna v tej množici. Več primerov Hassejevih diagramov najdemo na sliki 14. Ni težko preveriti, da levi Hassejev diagram s te slike predstavlja mrežo. Srednji in desni Hassejev diagram s slike 14 pa nista mreži. Pri srednjem diagramu imata elementa a in b dve natančni zgornji meji c in d, kar v delnih urejenostih ni mogoče po trditvi 8.1. Velja tudi obratno: c in d imata dve natančni spodnji meji a in b, kar je nemogoče po trditvi 8.1. Desni Hassejev diagram s slike 14 ni mreža, saj ima dva minimalna elementa x in y in zato ne obstaja* $\inf(x,y)$*. Podobno ne obstaja tudi* $\inf(z,y)$ *in še nekaj drugih.*



Slika 14: Hassejevi diagrami nekaterih množic.

Zgled 8.8 *Kot v zgledu 8.2, je potenčna množica* $M = \mathcal{P}(X)$ *množice X tudi relacijska algebra za relacijo* $\subseteq$*, ki delno ureja M (glej zgled 7.30) ter* $\sup(A,B) = A \cup B$ *in* $\inf(A,B) = A \cap B$ *za poljubni podmnožici* $A, B \subseteq X$*.*

Zgled 8.9 *Oglejmo si strukturo* $(\mathbb{N}_{\leq}, \max, \min)$*. Naravna števila so delno urejena z relacijo* $\leq$ *po trditvi 7.12, saj je* $\mathbb{R}$ *delno urejena z relacijo* $\leq$ *(glej zgled 7.30) in je* $\mathbb{N} \subset \mathbb{R}$*. Seveda* $\max\{a,b\}$ *in* $\min\{a,b\}$ *obstajata za poljubni naravni števili a in b. Torej je* $(\mathbb{N}_{\leq}, \max, \min)$ *relacijska mreža. Omenimo še, da lahko naravna števila nadomestimo s celimi, racionalnimi ali realnimi in relacija* $\leq$ *nam ponovno porodi relacijsko mrežo za enako definirana supremum in infimum.*

Zgled 8.10 *Množica naravnih števil* $\mathbb{N}$ *je delno urejena tudi z relacijo deljivosti* $|$*, glej zgled 7.31. Če vpeljemo* $\sup(a,b) = v(a,b)$ *in* $\inf(a,b) = D(a,b)$*, potem supremum in infimum vedno obstajata za poljubna* $a, b \in \mathbb{N}$ *in* $(\mathbb{N}_{|}, v, D)$ *je relacijska mreža.*

Zgled 8.11 *Po trditvi 7.12 je vsaka podmnožica naravnih števil delno urejena z relacijo deljivosti. Tako je* $(M_|, v, D)$ *mreža za* $M \subseteq \mathbb{N}$*, če le* M *vsebuje vsak* $v(a,b)$ *in vsak* $D(a,b)$ *za poljubna* $a, b \in M$*. Ta pogoj ni vedno izpolnjen. Recimo za* $M = \mathrm{del}(15,21) = (1,3,5,7,15,21)$ *množica* M *ne vsebuje* $v(15,21) = 105$ *in zato ni relacijska mreža. Podobno velja za* $M = \mathrm{del}(18,45)$*, čigar Hassejev diagram je na desni slike 13. To se ne more zgoditi za* $M = \mathrm{del}(a)$*, ki vedno poraja relacijsko mrežo z relacijo* $|$*. Bolj splošno* $M = \mathrm{del}(a_1, a_2, \ldots, a_k)$ *poraja mrežo* $(M_|, v, D)$ *natanko takrat, ko obstaja* $i \in [k]$*, da velja* $v(a_1, a_2, \ldots, a_k) = a_i$*. V tem primeru pravzaprav velja* $\mathrm{del}(a_1, a_2, \ldots, a_k) = \mathrm{del}(a_i)$*.*

Pokažimo sedaj, da med algebrskimi in relacijskimi mrežami ne ločimo. Tako bomo po tem izreku uporabljali le termin mreža za oboje: algebrsko mrežo in relacijsko mrežo.

Izrek 8.2 *Struktura* $(M, \sqcup, \sqcap)$ *je algebrska mreža natanko tedaj, ko je* $(M_R, \sup, \inf)$ *relacijska mreža.*

Dokaz. Naj bo najprej $(M, \sqcup, \sqcap)$ algebrska mreža. Definirajmo relacijo $R \subseteq M \times M$ s predpisom

$$aRb \Leftrightarrow a \sqcup b = b$$

in pokažimo, da R delno ureja M. Seveda je $a \sqcup a = a$ zaradi idempotentnosti $\sqcup$ in relacija R je refleksivna. Za dokaz antisimetričnosti naj velja aRb in bRa. Torej je $a \sqcup b = b$ in $b \sqcup a = a$. Upoštevajmo prvo enakost v drugi in dobimo

$$a = b \sqcup a = (a \sqcup b) \sqcup a = (b \sqcup a) \sqcup a = b \sqcup (a \sqcup a) = b \sqcup a = a \sqcup b = b.$$

Tukaj smo pri tretjem in šestem enačaju upoštevali komutativnost $\sqcup$, pri četrtem enačaju asociativnost $\sqcup$ in pri petem idempotentnost $\sqcup$. Tako je R tudi antisimetrična. Za tranzitivnost naj velja aRb in bRc, kar implicira $a \sqcup b = b$ in $b \sqcup c = c$. Ponovno upoštevamo prvo enakost v drugi in dobimo

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

kjer smo upoštevali le asociativnost $\sqcup$ na tretjem koraku. S tem je relacija R tudi tranzitivna in zato delno ureja množico M. Če vpeljemo še $\sup(a,b) = a \sqcup b$ in $\inf(a,b) = a \sqcap b$, potem supremum in infimum množice z dvema elementoma vedno obstaja in struktura $(M_R, \sup, \inf)$ je relacijska mreža.

Naj bo obratno $(M_R, \sup, \inf)$ relacijska mreža. Definirajmo operaciji

$$\sqcup, \sqcap : M \times M \to M$$

s predpisoma $a \sqcup b = \sup(a,b)$ in $a \sqcap b = \inf(a,b)$. Ker velja $\{a,b\} = \{b,a\}$, veljata tudi oba predpisa za komutativnost $\sqcup$ in $\sqcap$:

$$\begin{aligned} a \sqcup b &= \sup(a,b) = \sup(b,a) = b \sqcup a, \\ a \sqcap b &= \inf(a,b) = \inf(b,a) = b \sqcap a. \end{aligned}$$

Za asociativnost vpeljimo oznake $\sup(a,b) = d$, $\sup(d,c) = e$, $\sup(b,c) = f$ in $\sup(a,f) = g$. To hkrati pomeni, da velja $aRd, bRd, dRe, cRe, bRf, cRf, aRg$ in fRg. Nadalje zaradi tranzirivnosti dobimo aRe in bRe ter bRg in cRg. Tako sta oba e in g zgornji meji množice $\{a,b,c\}$. Natančna zgornja meja množice $\{a,b,c\}$ obstaja in jo označimo $h = \sup\{a,b,c\}$. Sedaj imamo

$$\begin{aligned} (a \sqcup b) \sqcup c &= \sup(a,b) \sqcup c = d \sqcup c = \sup(d,c) = e, \\ a \sqcup (b \sqcup c) &= a \sqcup \sup(b,c) = a \sqcup f = \sup(a,f) = g. \end{aligned} \tag{33}$$

Če je $h \neq e$, potem imamo protislovje z zgornjo vrstico iz (33). Podobno, če je $h \neq g$, potem imamo protislovje s spodnjo vrstico iz (33). Tako velja $e = h = g$, s čimer je asociativnost $\sqcup$ dokazana. Podobno pokažemo tudi asociativnost $\sqcap$.

Za dokaz absorpcije označimo $a \sqcap b = \inf(a,b) = c$ in $a \sqcup b = \sup(a,b) = d$, kar pomeni med drugim tudi cRa in aRd. Sedaj imamo

$$a \sqcup (a \sqcap b) = a \sqcup c = a \text{ in } a \sqcap (a \sqcup b) = a \sqcap d = a,$$

saj je cRa in aRd. Torej je tudi absorpcija izpolnjena. Tudi idempotentnost zlahka sledi iz

$$a \sqcup a = \sup(a,a) = a \text{ in } a \sqcap a = \inf(a,a) = a,$$

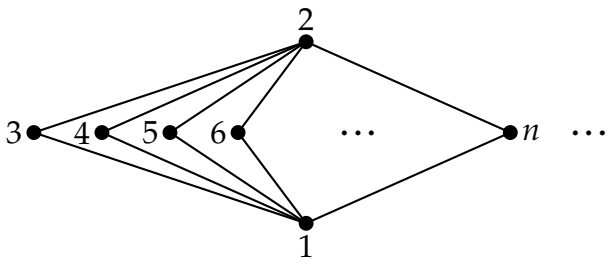
s čimer smo pokazali, da je $(M, \sqcup, \sqcap)$ algebrska mreža. ∎

Opomba 8.3 *Pozoren bralec lahko opazi, da v dokazu, da je algebrska mreža tudi relacijska mreža, sploh nismo uporabili absorpcije.*

Kot že omenjeno, od sedaj naprej govorimo le o mrežah in ne več o algebrskih oziroma relacijskih mrežah. Kljub temu bomo ločili med njimi s pomočjo oznake $(M_R, \sqcup, \sqcap)$ oziroma $(M_R, \sup, \inf)$, s čimer bomo tudi namignili, katero definicijo uporabljamo.

Posebno mesto imajo mreže $(M_R, \sup, \inf)$, ki vsebujejo prvi oziroma zadnji element. Ob tem prvi element mreže označimo z $\mathbf{0}$, če obstaja, in zanji element mreže označimo z $\mathbf{1}$, če obstaja. Mreža $(M_R, \sup, \inf)$ je **navzdol omejena**, če obstaja R-prvi element $\mathbf{0}$ in je **navzgor omejena**, če obstaja R-zadnji element $\mathbf{1}$. O **omejeni mreži** govorimo, če obstajata oba, R-prvi element $\mathbf{0}$ in R-zadnji element $\mathbf{1}$.

Zgled 8.12 *Mreža $(\mathbb{N}_{\leq}, \max, \min)$ je navzdol omejena, saj obstaja $\leq$-prvi element 1, ni pa navzgor omejena. Tako imamo $\boldsymbol{o} = 1$. Pojasnimo zadnji nenavadni zapis $\boldsymbol{o} = 1$. To ne pomeni, da je število $\boldsymbol{o}$ enako številu 1, pač pa, da je $\leq$-prvi element, ki ga označimo z $\boldsymbol{o}$ enak številu 1. Če v tej strukturi naravna števila zamenjamo s celimi, z racionalnimi ali z realnimi, dobimo mrežo, ki ni navzdol ne navzgor omejena.*



Slika 15: Mreža iz zgleda 8.13.

Zgled 8.13 *Relacija $R \subseteq \mathbb{N} \times \mathbb{N}$ je definirana s predpisom $R = \{(1,n),(n,2); n \in \mathbb{N}\}$. Njen Hassejev diagram je na sliki 15. Opazimo lahko, da je omejena in da velja $\mathbf{0} = 1$ in $\mathbf{1} = 2$. (Ponovno sta $\mathbf{0}$ in $\mathbf{1}$ R-prvi oziroma R-zadnji element in ne števili.) Iz tega primera lahko vidimo, da je mreža lahko omejena, četudi jo sestavlja neskončna množica.*

Zgled 8.14 *Kot smo že videli v zgledu 8.10 je $(\mathbb{N}_|, v, D)$ mreža. Le-ta je navzdol omejena z $\mathbf{0} = 1$, ni pa navzgor omejena, saj ne obstaja naravno število, ki bi ga delila vsa naravna števila. Tako število $2n$ ne deli števila n za poljuben $n \in \mathbb{N}$.*

Omejena mreža $(M_R, \sup, \inf)$ je **komplementirana**, če obstaja preslikava $' : M \to M$, za katero velja $\sup(a, a') = \mathbf{1}$ in $\inf(a, a') = \mathbf{0}$ za vsak $a \in M$. (Ne pozabimo, da je $\mathbf{0}$ R-prvi in $\mathbf{1}$ R-zadnji element, ki obstajata, saj je mreža omejena.)

Zgled 8.15 *Naj bo X poljubna množica in $M = \mathcal{P}(X)$. Mreža $(M, \cup, \cap)$ je omejena z $\mathbf{0} = \emptyset$ in $\mathbf{1} = X$. Spomnimo se, da je $A^c = \{x \in X : x \notin A\}$ komplement množice A, kjer je A poljubna podmnožica množice X. Seveda velja $A \cup A^c = X = \mathbf{1}$ in $A \cap A^c = \emptyset = \mathbf{0}$. Tako sta za preslikavo $^c : M \to M$ izpolnjena oba pogoja in je $(M, \cup, \cap)$ komplementirana mreža. Omenimo še, da ime komplementirana izhaja iz tega primera.*

Zgled 8.16 *Spomnimo se mreže $(B, \vee, \wedge)$ za $B = \{0, 1\}$ iz zgleda 8.1. Tudi ta mreža je omejena z $\mathbf{0} = 0$ in $\mathbf{1} = 1$. Če na negacijo pogledamo kot na preslikavo $\neg : a \mapsto \neg a$ postane mreža $(B, \vee\wedge)$ komplementirana, saj velja $a \vee \neg a \sim 1$ in $a \wedge \neg a \sim 0$ za vsak $a \in B$.*

Zadnja lastnost, ki nas zanima pri mrežah, je distributivnost. Mreža $(M, \sqcup, \sqcap)$ je **distributivna**, če je izpolnjen eden izmed distributivnostnih zakonov

$$a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c) \tag{34}$$

ali

$$a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c). \tag{35}$$

Pokažimo, da sta pogoja (34) in (35) ekvivalentna v mrežah. To pomeni, da veljavnost enega pomeni tudi veljavnost drugega in obratno. Tako za dokaz distributivnosti v mrežah zadošča veljavnost le enega izmed njiju.

Trditev 8.4 *V mreži $(M, \sqcup, \sqcap)$ velja pogoj (34) natanko tedaj, ko velja pogoj (35).*

Dokaz. Naj bo najprej izpolnjen pogoj (34). Pogoj (35) sledi iz računa

$$\begin{aligned}(a \sqcup b) \sqcap (a \sqcup c) &= ((a \sqcup b) \sqcap a) \sqcup ((a \sqcup b) \sqcap c) \\ &= (a \sqcap (a \sqcup b)) \sqcup (c \sqcap (a \sqcup b)) \\ &= a \sqcup ((c \sqcap a) \sqcup (c \sqcap b)) \\ &= (a \sqcup (a \sqcap c)) \sqcup (c \sqcap b) \\ &= a \sqcup (b \sqcap c).\end{aligned}$$

Ob tem smo na prvem koraku uporabili pogoj (34). V drugem koraku smo dvakrat uporabili komutativnost. Tretji korak dobimo s pomočjo absorpcije v prvem delu in pogoja (34) v drugem delu. V četrtem koraku si pomagamo z asociativnostjo in zadnji korak sledi iz absorpcije in komutativnosti.

Če velja pogoj (35), potem dobimo pogoj (34) z enakim računom, le da zamenjamo operaciji $\sqcup$ in $\sqcap$. ∎

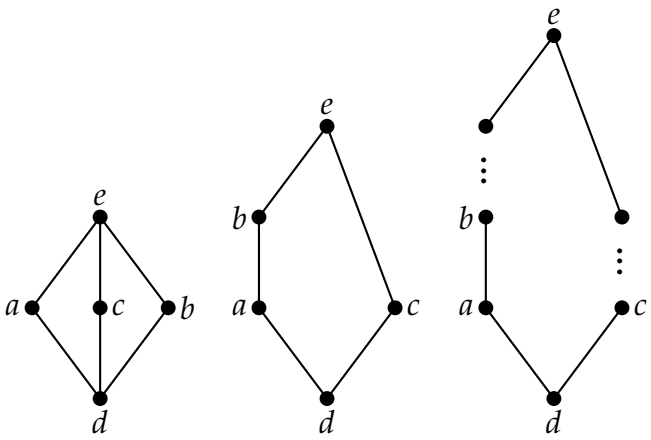
Zgled 8.17 *Naj bo A poljubna množica in $M = \mathcal{P}(A)$ njena potenčna množica. Mreža $(M, \cup, \cap)$ je distributivna, kar zlahka vidimo iz Vennovega diagrama za tri podmnožice X, Y in Z množice A.*

Zgled 8.18 *Za $B = \{0, 1\}$ je mreža $(B, \vee, \wedge)$ seveda distributivna, saj smo distributivnost za logični in ter logični ali dokazali že v razdelku 1.2.*

Zgled 8.19 *Naj bo $n \in \mathbb{N}$ in $M = \mathrm{del}(n)$. Mreža $(M_{|}, v, D)$ je distributivna, saj smo distributivnost operacij najmanjši skupni večkratnik in največji skupni delitelj pokazali v trditvi 6.15.*

Zgled 8.20 *Vprašajmo se, kdaj mreža ni distributivna. Odgovor na to najdemo na sliki 16. Za mrežo na levem delu slike 16 imamo $a \sqcup (b \sqcap c) = a \sqcup d = a$ in $(a \sqcup b) \sqcap (a \sqcup c) = e \sqcap e = e$ in pogoj (35) ni izpolnjen. Za mreži na sredini in na levi strani slike 16 velja $a \sqcup (b \sqcap c) = a \sqcup d = a$ in $(a \sqcup b) \sqcap (a \sqcup c) = b \sqcap e = b$ in pogoj (35) ponovno ne velja. Tako mreže s slike 16 niso distributivne. Velja še več. Če Hassejev diagram poljubne mreže vsebuje kakšno izmed struktur opisanih na sliki 16, potem mreža ni distributivna, saj lahko izvedemo identične račune.*

Trditev 8.4 in njen dokaz nas lahko motivirata tudi za naslednji razmislek. V definiciji mreže $(M, \sqcup, \sqcap)$ so vsi pogoji zastopani simetrično glede na operaciji $\sqcup$ in $\sqcap$. Če iz njih izpeljemo kakšno lastnost, to pomeni, da lahko izpeljemo enako lastnost, le da zamenjamo operaciji $\sqcup$ in $\sqcap$. Tudi izpeljava, kot v dokazu trditve 8.4, je enaka, le da zamenjamo operaciji $\sqcup$ in $\sqcap$. Temu rečemo, da za mreže velja **princip dualnosti** operacij $\sqcup$ in $\sqcap$.



Slika 16: Prepovedane strukture v Hassejevih diagramih za distributivne mreže.

8.2 BOOLEOVE ALGEBRE

Podobno kot mreže lahko tudi Booleove[17] algebre definiramo na dva različna načina: z relacijami in z algebrskimi operacijami. Obe definiciji sta ponovno ekvivalentni, kot bomo videli v izreku 8.6. Tokrat začnimo z relacijsko definicijo.

Relacijska Booleova algebra je komplementirana distributivna mreža $(B_R, \sup, \inf)$. Ker so komplementirane mreže tudi omejene, obstajata R-prvi element $\mathbf{0}$ in R-zadnji element $\mathbf{1}$. Komplementiranost hkrati zagotavlja tudi obstoj preslikave $' : B \to B$, za katero je $\sup(a, a') = \mathbf{1}$ in $\inf(a, a') = \mathbf{0}$. Tako relacijsko Booleovo algebro označimo z $(B_R, \sup, \inf, ', \mathbf{0}, \mathbf{1})$, saj nam ta zapis prinaša dodatne informacije.

Algebrska Booleova algebra je struktura $(B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1})$, kjer so $\sqcup, \sqcap : B \times B \to B$ in $' : B \to B$ operacije, za katere so za poljubne $a, b, c \in B$ izpolnjene naslednje lastnosti:

(i)	$(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$	in	$(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)$,
(ii)	$a \sqcup b = b \sqcup a$	in	$a \sqcap b = b \sqcap a$,
(iii)	$a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c)$	in	$a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c)$,
(iv)	$a \sqcup \mathbf{0} = a$	in	$a \sqcap \mathbf{1} = a$,
(v)	$a \sqcup a' = \mathbf{1}$	in	$a \sqcap a' = \mathbf{0}$.

Seveda lastnosti iz točke (i) rečemo asociativnost, pod točko (ii) imamo komutativnost. Pod točko (iii) je najti distributivnost. Lastnosti iz točke (iv) rečemo **obstoj nevtralnega elementa** in zadnja točka predstavlja komplementiranost.

17 George Boole (1815-1864) je bil angleški matematik, ki je najbolj znan po svojem delu iz algebrske logike. Njegov vrhunec so strukture, ki jih danes poimenujemo po njem: Booleove algebre.

Opazimo lahko, da v algebrski Booleovi algebri nastopata le dve lastnosti iz definicije algebrske mreže. V nadaljevanju bomo videli, da lastnosti iz algebrske Booleove algebre porajajo tudi idempotentnost in absorpcijo za operaciji $\sqcup$ in $\sqcap$. Ponovno pa velja pricip dualnosti, saj operaciji $\sqcup$ in $\sqcap$ nastopata simetrično.

Trditev 8.5 *Za algebrsko Booleovo algebro veljata idempotentnosti $a \sqcup a = a$ in $a \sqcap a = a$ za vsak $a, b \in B$.*

Dokaz. Idempotentnost pokažemo s pomočjo distributivnosti

$$a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c),$$

kjer izberemo $b = a$ in $c = a'$. Tako imamo

$$a \sqcup (a \sqcap a') = (a \sqcup a) \sqcap (a \sqcup a').$$

Ob upoštevanju komplementiranosti dobimo

$$a \sqcup \mathbf{0} = (a \sqcup a) \sqcap \mathbf{1}.$$

Idempotentnost $a = a \sqcup a$ sedaj sledi, ker sta $\mathbf{0}$ in $\mathbf{1}$ nevtralna elementa za $\sqcup$, oziroma $\sqcap$. Idempotentnost $a \sqcap a = a$ dobimo na enak način, le da začnemo z drugo distributivnostjo. ∎

S tem že lahko dokažemo, da pojma algebrska Booleova algebra in relacijska Booleova algebra sovpadata.

Izrek 8.6 *Struktura $(B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1})$ je algebrska Booleova algebra natanko tedaj, ko je $(B_R, \sup, \inf, ', \mathbf{0}, \mathbf{1})$ relacijska Booleova algebra.*

Dokaz. Naj bo najprej $(B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1})$ algebrska Booleova algebra. Definirajmo relacijo $R \subseteq B \times B$ s predpisom

$$aRb \Leftrightarrow a \sqcup b = b$$

kot v dokazu izreka 8.2. Kot omenjeno v opombi 8.3, smo v dokazu izreka 8.2 uporabili le asociativnost, komutativnost in idempotentnost, da smo pokazali, da ta relacija delno ureja B. Tudi sedaj veljata asociativnost in komutativnost, saj je $(B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1})$ algebrska Booleova algebra. Po trditvi 8.5 velja tudi idempotentnost in R zato delno ureja B in je mreža za $\sup(a, b) = a \sqcup b$ in $\inf(a, b) = a \sqcap b$. Ta mreža je tudi distributivna zaradi (iii) in komplementirana zaradi (v). Torej je $(B_R, \sup, \inf, ', \mathbf{0}, \mathbf{1})$ relacijska Booleova algebra.

Naj bo obratno $(B_R, \sup, \inf, ', \mathbf{0}, \mathbf{1})$ relacijska Booleova algebra. Vpeljimo $a \sqcup b = \sup(a, b)$ in $a \sqcap b = \inf(a, b)$. Potem je tudi mreža in veljata asociativnost in komutativnost. Ker je ta mreža tudi komplementirana velja, (v) in ker je distributivna, velja (iii). Komplementiranost nadalje zagotavlja obstoj R-prvega

elementa $\mathbf{0}$ in R-zadnjega elementa $\mathbf{1}$, za katera seveda velja $a \sqcup \mathbf{0} = \sup(a, \mathbf{0}) = a$ in $a \sqcap \mathbf{1} = \inf(a, \mathbf{1}) = a$ za vsak $a \in B$. Tako velja tudi lastnost (iv) in $(B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1})$ je algebrska Booleova algebra. ∎

Kot pri mrežah bomo tudi v tem razdelku sedaj opuščali pridevnika relacijska oziroma algebrska in bomo govorili zgolj o Booleovih algebrah. Preden si ogledamo nekatere primere Booleovih algebr, dokažimo še nekaj njihovih lastnosti.

Trditev 8.7 *V Booleovi algebri $(B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1})$ veljajo naslednje lastnosti za vsak $a, b, c \in B$.*

(I) *Absorpcija: $a \sqcup (a \sqcap b) = a$ in $a \sqcap (a \sqcup b) = a$.*

(II) *Dominantnost $\mathbf{0}$ in $\mathbf{1}$: $a \sqcup \mathbf{1} = \mathbf{1}$ in $a \sqcap \mathbf{0} = \mathbf{0}$.*

(III) *Involucija: $(a')' = a$.*

(IV) *$\mathbf{0}' = \mathbf{1}$ in $\mathbf{1}' = \mathbf{0}$.*

(V) *Enoličnost komplementa: $(a \sqcup b = 1 \wedge a \sqcap b = 0) \Rightarrow b = a'$.*

(VI) *De Morganova zakona: $(a \sqcup b)' = a' \sqcap b'$ in $(a \sqcap b)' = a' \sqcup b'$.*

(VII) *Pravili krajšanja: $(a \sqcup b = a \sqcup c \wedge a' \sqcup b = a' \sqcup c) \Rightarrow b = c$ in $(a \sqcap b = a \sqcap c \wedge a' \sqcap b = a' \sqcap c) \Rightarrow b = c$.*

Dokaz. Ker je Booleova algebra $(B, \sqcup, \sqcap, ', \mathbf{0}, \mathbf{1})$ tudi mreža, seveda velja absorpcija (i). Lastnost (ii), dominantnost $\mathbf{0}$ in $\mathbf{1}$, sledi iz njune vloge kot R-prvi oziroma R-zadnji element. Tako je $0Ra$ in $aR1$ za vsak $a \in B$, kar pomeni $a \sqcup \mathbf{1} = \sup(a, \mathbf{1}) = \mathbf{1}$ in $a \sqcap \mathbf{0} = \inf(a, \mathbf{0}) = \mathbf{0}$.

Lastnost (v) je razvidna iz naslednjega računa

$$\begin{aligned} b &= \mathbf{1} \sqcap b = (a \sqcup a') \sqcap b = (a \sqcap b) \sqcup (a' \sqcap b) = 0 \sqcup (a' \sqcap b) \\ &= (a' \sqcap a) \sqcup (a' \sqcap b) = a' \sqcap (a \sqcup b) = a' \sqcap \mathbf{1} = a', \end{aligned}$$

kjer smo uporabljali nevtralnost $\sqcup$ in $\sqcap$ za $\mathbf{0}$ oziroma $\mathbf{1}$, distributivnost, komplementiranost in seveda obe predpostavki iz prvega dela implikacije.

Lastnost (iv) sledi iz dominantnosti $\mathbf{0}$ in $\mathbf{1}$ točke (ii) in enoličnosti komplementa (v), saj iz $0 \sqcup \mathbf{1} = \mathbf{1}$ in $\mathbf{1} \sqcap \mathbf{0} = \mathbf{0}$ in enoličnosti komplementa sledi $\mathbf{0}' = \mathbf{1}$ in $\mathbf{1}' = \mathbf{0}$. Involucija, lastnost (iii), sledi iz definicije komplementiranosti in enoličnosti komplementa (v), saj $a \sqcup a' = \mathbf{1}$ in $a \sqcap a' = \mathbf{0}$ že implicirata, da je komplement od a' kar a. Torej velja $(a')' = a$.

Tudi za dokaz DeMorganovega zakona lahko sedaj uporabimo lastnost (v), da je torej komplement enoličen. Pokažimo torej, da je $a' \sqcup b'$ komplement od $a \sqcap b$. To storimo v dveh korakih:

$$\begin{aligned}(a \sqcap b) \sqcup (a' \sqcup b') &= ((a \sqcap b) \sqcup a') \sqcup b' = ((a \sqcup a') \sqcap (b \sqcup a')) \sqcup b' = \\ &= (\mathbf{1} \sqcap (b \sqcup a')) \sqcup b' = (b \sqcup a') \sqcup b' = (a' \sqcup b) \sqcup b = \\ &= a' \sqcup (b \sqcup b') = a' \sqcup \mathbf{1} = \mathbf{1}\end{aligned}$$

in

$$\begin{aligned}(a \sqcap b) \sqcap (a' \sqcup b') &= a \sqcap (b \sqcap (a' \sqcup b')) = a \sqcap ((b \sqcap a') \sqcup (b \sqcap b')) = \\ &= a \sqcap ((b \sqcap a') \sqcup \mathbf{0}) = a \sqcap (b \sqcap a') = a \sqcap (a' \sqcap b) = \\ &= (a \sqcap a') \sqcap b = \mathbf{0} \sqcap b = \mathbf{0}.\end{aligned}$$

Omenimo, da smo v teh dveh izračunih uporabili asociativnost, distributivnost, komplementiranost, komutativnost in dominantnost. Vidimo, da je $a' \sqcup b'$ komplement elementa $a \sqcap b$ in, ker je komplement enoličen po (v), velja $(a \sqcap b)' = a' \sqcup b'$. Omenimo, da drugi DeMorganov zakon pokažemo na podoben način.

Za pravilo krajšanja predpostavimo, da veljata $a \sqcap b = a \sqcap c$ in $a' \sqcap b = a' \sqcap c$ in pokažimo enakost $b = c$. Le-ta sledi iz računa

$$\begin{aligned}b &= \mathbf{1} \sqcap b = (a \sqcup a') \sqcap b = (a \sqcap b) \sqcup (a' \sqcap b) = \\ &= (a \sqcap c) \sqcup (a' \sqcap c) = (a \sqcup a') \sqcap c = \mathbf{1} \sqcap c = c.\end{aligned}$$

V tem računu smo uporabili, da je $\mathbf{1}$ nevtralni element za $\sqcap$, komplementiranost in distributivnost ter obe predpostavki. Drugo pravilo krajšanja pokažemo na dualen način. ■

Zgled 8.21 *Naj bo A poljubna množica in $B = \mathcal{P}(A)$ njena potenčna množica. V zgledu 8.2 smo videli, da je $(B, \cup, \cap)$ mreža. V zgledu 8.15 smo videli, da je omenjena mreža komplementirana za $B^c = A - B$ in v zgledu 8.17 smo videli, da je ta mreža tudi distributivna. Torej je $(B, \cup, \cap, ^c, \emptyset, A)$ Booleova algebra. Nekaj Hassejevih diagramov teh Booleovih algeber v primeru, ko ima A dva, tri ali štiri elemente najdemo na sliki 11.*

Zgled 8.22 *Naj bo $B = \mathrm{del}(n)$ za neko naravno število n. V zgledu 8.11 smo videli, da je (B, v, D) mreža, ki je distributivna po trditvi 6.15 (glej tudi zgled 8.19). Tako je $(B, v, D, ', 1, n)$ Booleova algebra, če le obstaja preslikava $' : B \to B$, za katero velja $v(a, a') = 1$ in $D(a, a') = 0$ za vsak $a \in B$. Oglejmo si najprej primer, ko ima vsako praštevilo iz razcepa števila n na praštevila potenco 1. Torej je $n = p_1 \dots p_k$. V tem primeru definirajmo $a' = \frac{n}{a}$ za vsak $a \in B$. Ob tem lahko zapišemo $a = p_{i_1} \dots p_{i_t}$ in $a' = p_{j_1} \dots p_{j_{k-t}}$, kjer je $[k] = \{i_1, \dots i_t\} \cup \{j_1, \dots, j_{k-t}\}$. Seveda velja $D(a, a') = 1$ in $v(a, a') = n$. Torej je v tem primeru $(B, v, D, ', 1, n)$ Booleova algebra.*

Pokažimo še, da v nasprotnem primeru $(B, v, D, ', 1, n)$ ni Booleova algebra, za katerokoli preslikavo $' : B \to B$. Nasprotni primer je tak, da razcep števila n na praštevila vsebuje vsaj eno potenco višjo kot ena. Tako lahko zapišemo $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, kjer lahko predpostavimo, da je $\alpha_1 > 1$ in $\alpha_2, \dots, \alpha_k$ so naravna števila. Izberimo $a = p_1$ in predpostavimo nasprotno, da obstaja preslikava $' : B \to B$, ki nam zagotavlja komplementiranost. Potem obstaja a', za katerega velja $D(a, a') = 1$. Ni težko opaziti, da je

$$a' \in \{p_2^{\beta_2} \dots p_k^{\beta_k} : \beta_i \in [\alpha_i]_0, \forall i \in \{2, 3, \dots, k\}\},$$

da zadostimo pogoju $D(a, a') = 1$. V tem primeru imamo $v(a, a') = p_1 a' \neq a$, saj je $\alpha_1 > 1$, kar je protislovje s predpostavko, da obstaja preslikava $' : B \to B$, ki nam zagotavlja komplementiranost. Torej (B, v, D) ni komplementirana mreža in s tem tudi ni Booleova algebra.

Če združimo oba dela, lahko opazimo, da smo pravzaprav pokazali, da je $(B, v, D, ', 1, n)$ Booleova algebra natanko tedaj, ko ima število n pri razcepu na praštevila vse potence enake ena. Hassejevi diagrami nekaterih mrež (B, v, D) so predstavljeni na slikah 12 in 13. Vsi trije Hassejevi diagrami s slike 12 predstavljajo Booleovo algebro, medtem ko primeri Hassejevih diagramov s slike 13 ne predstavljajo Booleovih algeber.

Zgled 8.23 *Za $B = \{0, 1\}$ smo videli v zgledu 8.1, da je mreža. Vemo tudi, da je komplementirana (glej zgled 8.16) za negacijo in distributivna (glej zgled 8.18). Torej je struktura $(B, \vee\wedge, \neg, 0, 1)$ Booleova algebra.*

Zgled 8.24 *Naj bo $B = \{0, 1\}$ in $B^n = B \times \dots \times B$ kartezični produkt n množic B. Preslikavi $f : B^n \to B$ rečemo **Booleova funkcija**. Za $n = 3$ je primer Booleove funkcije recimo $f(x_1, x_2, x_3) = x_1 \vee \neg(x_2 \wedge \neg x_3)$. V množico $U_n = \{f, f : B^n \to B\}$ vpeljimo operacije*

$$\begin{aligned} f \sqcup g &= f(x_1, \dots, x_n) \vee g(x_1, \dots, x_n), \\ f \sqcap g &= f(x_1, \dots, x_n) \wedge g(x_1, \dots, x_n), \\ f' &= \neg f(x_1, \dots, x_n). \end{aligned}$$

*Ker so $\sqcup$, $\sqcap$ in $'$ definirane s pomočjo logičnega **ali**, logičnega **in** ter negacije, vemo iz razdelka 1.2, da so izpolnjeni vsi pogoji, potrebni za Booleovo algebro $(U_n, \sqcup, \sqcap, ', 0, 1)$, če le z 0 označimo laž in z 1 tavtologijo.*

8.3 NEKATERE (NE)REŠENE NALOGE

Vaja 8.1 *Pokažite, da je množica vseh realnih funkcij $f : [0,1] \to [0,1]$ delno urejena množica z relacijo $\geq$:*

$$f \geq g \Leftrightarrow f(x) \geq g(x) \ \ \forall x \in [0,1].$$

Smiselno definirajte $\sqcap$ in $\sqcup$, da zgornja struktura postane mreža.

Rešitev. *Relacija $\geq$ je refleksivna, saj je $f(x) \geq f(x)$ za vsak $x \in [0,1]$. Naj bo $f \geq g$ in $g \geq h$, potem je $f(x) \geq g(x)$ in $g(x) \geq h(x)$ za vsak $x \in [0,1]$. Torej je tudi $f(x) \geq h(x)$ za vsak $x \in [0,1]$ in je $\geq$ tranzitivna. Za antisimetričnost $\geq$ naj velja $f \geq g$ in $g \geq f$. To pomeni $f(x) \geq g(x)$ in $g(x) \geq f(x)$ za vsak $x \in [0,1]$. Torej velja $f(x) = g(x)$ za vsak $x \in [0,1]$. Torej relacija $\geq$ delno ureja množico vseh realnih funkcij $f : [0,1] \to [0,1]$. Če definiramo še*

$$\begin{aligned} (f \sqcap g)(x) &= \min\{f(x), g(x)\}, \\ (f \sqcup g)(x) &= \max\{f(x), g(x)\}, \end{aligned}$$

potem postane množica vseh realnih funkcij $f : [0,1] \to [0,1]$ mreža.

Vaja 8.2 *Podana je množica točk*

$$[a,b] = \left\{ (x,y) \in \mathbb{R}^2;\, x,y \geq 0, y \leq -\frac{bx}{a} + b, a, b > 0 \right\}.$$

(A) *Skicirajte $[1,1]$, $[2,\frac{1}{2}]$ in $[\frac{1}{2},2]$.*

(B) *Pokažite, da je množica $P = \{[a,b]\,;\, a,b > 0\}$ za relacijo $\subseteq$ mreža. Kaj sta* inf *in* sup*?*

(C) *Ali je ta mreža distributivna?*

Rešitev. *Množica $[a,b]$ je trikotnik z oglišči $(0,0)$, $(a,0)$ in $(0,b)$. Recimo $[2,\frac{1}{2}]$ ima oglišča $(0,0)$, $(2,0)$ in $(0,\frac{1}{2})$. Seveda $\subseteq$ delno ureja množico P. Če vpeljemo za infimum $\inf\{[a,b],[c,d]\} = [\min\{a,c\}, \min\{b,d\}]$ in za supremum $\sup\{[a,b],[c,d]\} = [\max\{a,c\}, \max\{b,d\}]$, potem postane P mreža. Ta mreža je distributivna zaradi distributivnosti* min *in* max *(opravite račun, ki je malo daljši, vendar nezahteven).*

Vaja 8.3 *Množici točk*

$$[a,b] = \left\{ (x,y) \in \mathbb{R}^2;\, 0 \leq x \leq a,\, 0 \leq y \leq b \right\},$$

rečemo pravokotnik. Pokažite, da je množica pravokotnikov $P = \left\{ [a,b] : a,b \in \mathbb{R}_0^+ \right\}$ za relacijo $\subseteq$ (vsebovanost množic) mreža. Kaj sta $\sqcap$ in $\sqcup$? Ali obstajata prvi in zadnji element?

Rešitev. *Zlahka se preveri, da je P delno urejena množica; presek in unijo definiramo z $[a,b] \sqcap [c,d] = [\min\{a,c\}, \min\{b,d\}]$ in $[a,b] \sqcup [c,d] = [\max\{a,c\}, \max\{b,d\}]$; prvi element je $[0,0]$, zadnjega pa mreža nima.*

Vaja 8.4 *Naj bo X množica in $R(X)$ množica vseh razbitij množice X. (Spomnimo se, da za razbitje $\pi = \{A_1, A_2, \ldots, A_k\}$ množice X velja $A_1 \cup A_2 \cup \cdots \cup A_k = X$ in $A_i \cap A_j = \emptyset$ za vsak $i \neq j$.) Naj bosta $\pi_1 = \{A_1, A_2, \ldots, A_s\}$ in $\pi_2 = \{B_1, B_2, \ldots, B_t\}$ razbitji množice X. Na množici $R(X)$ vpeljemo relacijo $\sqsubseteq$ s predpisom*

$$\pi_1 \sqsubseteq \pi_2 \iff \forall i \in [s], \exists j \in [t] : A_i \subseteq B_j.$$

Pokažite, da relacija $\sqsubseteq$ poraja omejeno mrežo, ki ni distributivna, če le X vsebuje vsaj tri elemente.

Rešitev. *Relacija $\sqsubseteq$ je refleksivna, saj je $A_i \subseteq A_i$ za vsak $i \in [s]$. Za dokaz antisimetričnosti predpostavimo, da je $\pi_1 \sqsubseteq \pi_2$ in $\pi_2 \sqsubseteq \pi_1$. To pomeni, da za vsak $i \in [s]$ obstaja $j \in [t]$, da je $A_i \subseteq B_j$ in za vsak $k \in [t]$ obstaja $\ell \in [s]$, da je $B_k \subseteq A_\ell$. Torej obstajata $j \in [t]$ in $\ell \in [s]$ za vsak fiksno izbani $i \in [s]$, da velja $A_i \subseteq B_j \subseteq A_\ell$. Če je $i \neq \ell$, potem je $A_i \cap A_\ell \neq \emptyset$, kar je v nasprotju z definicijo razbitja. Tako je $A_i = A_\ell$ in s tem tudi $A_i = B_j$. Torej velja, da sta razbitji π_1 in π_2 enaki in antisimetričnost velja za $\sqsubseteq$. Za dokaz tranzitivnosti naj bo še $\pi_3 = \{C_1, C_2, \ldots, C_r\}$. Predpostavimo, da velja $\pi_1 \sqsubseteq \pi_2$ in $\pi_2 \sqsubseteq \pi_3$. To pomeni, da za vsak $i \in [s]$ obstaja $j \in [t]$, da je $A_i \subseteq B_j$ in za vsak $k \in [s]$ obstaja $\ell \in [r]$, da je $B_k \subseteq C_\ell$. Potem tudi za $j \in [s]$ obstaja $\ell_j \in [r]$, da velja $B_j \subseteq C_{\ell_j}$. Potem pa za vsak $i \in [s]$ obstaja $\ell_j \in [r]$, da je $A_i \subseteq C_{\ell_j}$ in $\sqsubseteq$ je tudi tranzitivna.*

Definirati je potrebno še $\inf(\pi_1, \pi_2)$ *in* $\sup(\pi_1, \pi_2)$ *za poljubna $\pi_1, \pi_2 \in R(X)$. Naj bo*

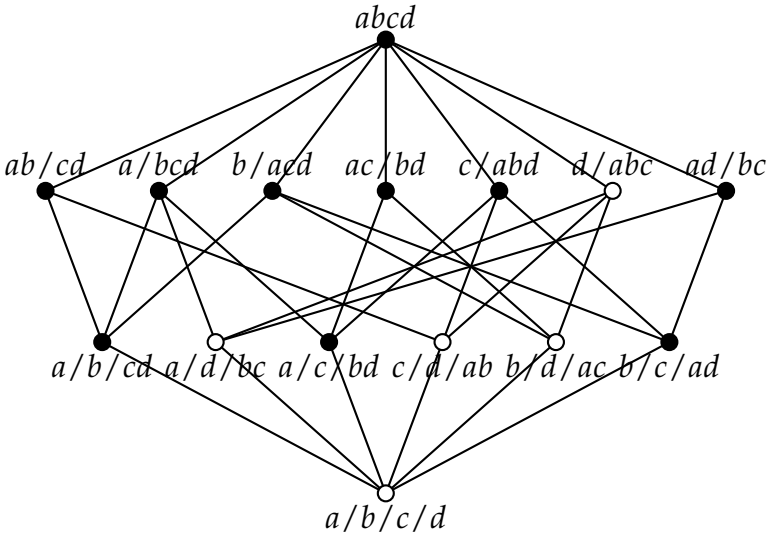
$$\inf(\pi_1, \pi_2) = \{A_i \cap B_j : i \in [s], j \in [t]\}$$

in pokažimo, da je tudi $\inf(\pi_1, \pi_2) = \{D_1, D_2, \ldots, D_q\}$ *razbitje množice X. Ker je vsak element $x \in X$ v natanko eni množici A_i in natanko eni množici B_j, je $x \in A_i \cap B_j = D_k$. Tako je $D_1 \cup D_2 \cup \cdots \cup D_k = X$. Recimo, da je nasprotno $d \in D_i \cap D_j$ za različna $i, j \in [q]$. Naj bosta $D_i = A_{k_i} \cap B_{\ell_i}$ in $D_j = A_{k_j} \cap B_{\ell_j}$. Ker je $i \neq j$, je $A_{k_i} \neq A_{k_j}$ ali $B_{\ell_i} \neq B_{\ell_j}$. Če je $A_{k_i} \neq A_{k_i}$, potem je $d \in A_{k_i} \cap A_{k_j}$ za $k_i \neq k_j$, kar je nemogoče za razbitje π_1. Če je $B_{k_j} \neq B_{\ell_j}$, potem je $d \in B_{\ell_i} \cap B_{\ell_j}$ za $\ell_i \neq \ell_j$, kar je nemogoče za razbitje π_2. Torej je $D_i \cap D_j = \emptyset$ za različna $i, j \in [q]$ in* $\inf(\pi_1, \pi_2)$ *je razbitje množice X.*

Pokažimo še, da je $\sup(\pi_1, \pi_2) = \{D_1, D_2, \ldots, D_p\}$ *natančna zgornja meja, če v π_1 in π_2 obstajata podrazbitji $\{A_{i_1}, A_{i_2}, \ldots, A_{i_{m_i}}\}$ in $\{B_{i_1}, B_{i_2}, \ldots, B_{i_{m_i}}\}$ množice D_i za vsak $i \in [p]$ in je p največje tako število. Da je tako definiran* $\sup(\pi_1, \pi_2)$ *tudi razbitje, sledi neposredno iz dejstva, da sta razbitji tudi π_1 in π_2. Po drugi strani je ta zgornja meja tudi natančna zaradi maksimalnosti števila p.*

Oglejmo si nekaj primerov, kjer je razbitje $\{A_1, A_2, \cdots, A_s\}$ označeno kar z $A_1/A_2/\ldots/A_s$ in izpustimo zavite oklepaje. Tako z $a/bc/d$ označimo razbitje $\{\{a\}, \{b, c\}, \{d\}\}$. Če je $\pi_1 = 12/34/56$ in $\pi_2 = 13/45/26$ v množici $X = \{1, 2, 3, 4, 5, 6\}$, potem je $\sup(\pi_1, \pi_2) = 123456$, *torej kar celotna množica. V primeru $\pi_1 = 1/234/5/6$ in $\pi_2 = 15/2/34/6$ pa je* $\sup(\pi_1, \pi_2) = 15/234/6$. *Zgornja meja v zadnjem primeru je*

tudi razbitje $156/234$*, a to ni natančna zgornja meja, saj število množic v tem razbitju ni največje možno. Na sliki 17 je mreža* $(R(X)_{\sqsubseteq}, \sup, \inf)$*, kjer je* $X = \{a, b, c, d\}$*.*



Slika 17: Mreža razbitij množice $X = \{a, b, c, d\}$.

Pokažimo še, da mreža $(R(X)_{\sqsubseteq}, \sup, \inf)$ *ni distributivna, ko* X *vsebuje vsaj tri elemente. Naj bodo* $a, b, c \in X$*. Najprej vpeljimo oznako* $X' = X - \{a, b, c\}$*. Sedaj si oglejmo razbitja* $a/b/c/X'$*,* $ab/c/X'$*,* $a/bc/X'$*,* $ac/b/X'$ *in* abc/X' *(to so bela vozlišča na sliki 17). Ni težko videti, da v Hassejevem diagramu tvorijo levi diagram s slike 16, kar po zgledu 8.20 že pomeni, da mreža* $(R(X)_{\sqsubseteq}, \sup, \inf)$ *ni distributivna, ko je* $|X| \geq 3$*.*

Vaja 8.5 *Na sliki 16 v vseh treh primerih poiščite elemente* a, b *in* c*, da pogoj (34) ne bo izpolnjen.*

Vaja 8.6 *Izpeljite dokaz za* $a \sqcap a = a$ *iz trditve 8.5.*

Vaja 8.7 *Dokažite De Morganov zakon* $(a \sqcup b)' = a' \sqcap b'$ *na podoben način kot* $(a \sqcap b)' = a' \sqcup b'$ *v dokazu trditve 8.7.*

Vaja 8.8 *Dokažite pravilo krajšanja* $(a \sqcup b = a \sqcup c \wedge a' \sqcup b = a' \sqcup c) \Rightarrow b = c$ *na podoben način kot njegov dual v dokazu trditve 8.7.*

Vaja 8.9 *Kdaj je struktura* $(\mathrm{del}(n), v, D,', 1, n)$ *Booleova algebre za* $a' = \frac{n}{a}$*, če je* $n \in \{60, 231, 323, 625, 1470\}$*? Narišite tudi njihove Hassejeve diagrame.*

Rešitev. *V skladu z zgledom 8.22 je* $(\mathrm{del}(n), v, D,', 1, n)$ *Booleova algebra za* $231 = 3 \cdot 7 \cdot 11$ *in* $323 = 17 \cdot 19$*. Ni pa Booleova algebra za* $60 = 2^2 \cdot 3 \cdot 5$ *in za* $625 = 5^4$ *in za* $1470 = 2 \cdot 3 \cdot 5 \cdot 7^2$*.*

Vaja 8.10 *Naj bosta* $(B_1, \sqcup_1, \sqcap_1, ^*, 0_1, 1_1)$ *in* $(B_2, \sqcup_2, \sqcap_2, ^\circ, 0_2, 1_2)$ *Booleovi algebri. Pokažite, da je struktura* $(B_1 \times B_2, \sqcup, \sqcap, ', 0, 1)$, *če za vsaka* $(a, b), (c, d) \in B_1 \times B_2$ *velja*

$$\begin{aligned}(a,b) \sqcup (c,d) &= (a \sqcup_1 c, b \sqcup_2 d),\\ (a,b) \sqcap (c,d) &= (a \sqcap_1 c, b \sqcap_2 d),\\ (a,b)' &= (a^*, b^\circ),\\ 0 &= (0_1, 0_2),\\ 1 &= (1_1, 1_2).\end{aligned}$$

Rešitev. *Za* $\sqcup$ *in* $\sqcap$ *je potrebno pokazati asociativnost, komutativnost, distributivnost, obstoj nevtralnega elementa za* 0 *in* 1 *ter komplementiranost za preslikavo* $'$. *Vse naštete lastnosti sledijo iz istih lastnosti operacij* $\sqcup_1, \sqcap_1, \sqcup_2, \sqcap_2, ^*, ^\circ, 0_1, 1_1, 0_2$ *in* 1_2. *Bolj natančno si oglejmo eno distributivnost in komplementiranost, izpeljave ostalih lastnosti pa prepuščamo za vajo. Pri (eni) distributivnosti poteka račun takole*

$$\begin{aligned}(a,b) \sqcap ((c,d) \sqcup (e,f)) &= (a,b) \sqcap (c \sqcup_1 e, d \sqcup_2 f)\\ &= (a \sqcap_1 (c \sqcup_1 e), b \sqcap_2 (d \sqcup_2 f))\\ &= ((a \sqcap_1 c) \sqcup_1 (a \sqcap_1 e), (b \sqcap_2 d) \sqcup_2 (b \sqcap_2 f))\\ &= (a \sqcap_1 c, b \sqcap_2 d) \sqcup (a \sqcap_1 e, b \sqcap_2 f)\\ &= ((a,b) \sqcap (c,d)) \sqcup ((a,b) \sqcap (e,f)),\end{aligned}$$

kjer smo v prvih dveh in zadnjih dveh korakih le upoštevali definicijo $\sqcup$ *in* $\sqcap$, *medtem ko smo v srednjem koraku uporabili isto distributivnost za operacije* $\sqcup_1$, $\sqcup_2$, $\sqcap_1$ *in* $\sqcap_2$. *Komplementiranost sledi iz*

$$\begin{aligned}(a,b) \sqcup (a,b)' &= (a,b) \sqcup (a^*, b^\circ) = (a \sqcup_1 a^*, b \sqcup_2 b^\circ) = (1_1, 1_2)\\ (a,b) \sqcap (a,b)' &= (a,b) \sqcap (a^*, b^\circ) = (a \sqcap_1 a^*, b \sqcap_2 b^\circ) = (0_1, 0_2).\end{aligned}$$

Vaja 8.11 *V oziru na prejšnjo nalogo skicirajte Hassejeve diagrame mrež*

$$(B_1 \times B_2, \sqcup, \sqcap, ', 0, 1),$$

če so

(A) $(B_1, \sqcup_1, \sqcap_1, ^*, 0_1, 1_1) = (\{0,1\}, \vee, \wedge, \neg, 0, 1)$ *in*
$(B_2, \sqcup_2, \sqcap_2, ^\circ, 0_2, 1_2) = (\mathrm{del}\{22\}, v, D, ', 1, n)$,

(B) $(B_1, \sqcup_1, \sqcap_1, ^*, 0_1, 1_1) = (\{0,1\}, \vee, \wedge, \neg, 0, 1)$ *in*
$(B_2, \sqcup_2, \sqcap_2, ^\circ, 0_2, 1_2) = (\mathcal{P}(\{a,b,c\}), \cup, \cap, ^c, \emptyset, \{a,b,c\})$,

(C) $(B_1, \sqcup_1, \sqcap_1, ^*, 0_1, 1_1) = (\mathrm{del}\{21\}, v, D, ', 1, 21)$ *in*
$(B_2, \sqcup_2, \sqcap_2, ^\circ, 0_2, 1_2) = (\mathrm{del}\{35\}, v, D, ', 1, 35)$,

(D) $(B_1, \sqcup_1, \sqcap_1, ^*, 0_1, 1_1) = (\mathrm{del}\{33\}, v, D, ', 1, 33)$ *in*
$(B_2, \sqcup_2, \sqcap_2, ^\circ, 0_2, 1_2) = (\mathcal{P}(\{a,b\}), \cup, \cap, ^c, \emptyset, \{a,b\})$,

(E) $(B_1, \sqcup_1, \sqcap_1, ^*, 0_1, 1_1) = (\mathcal{P}(\{a,b\}), \cup, \cap, ^c, \emptyset, \{a,b\})$ *in*
$(B_2, \sqcup_2, \sqcap_2, ^\circ, 0_2, 1_2) = (\mathcal{P}(\{1,2,3\}), \cup, \cap, ^c, \emptyset, \{1,2,3\})$.

9

UVOD V TEORIJO GRAFOV

Teorija grafov je moderna veja matematike, ki se je začela bolj razvijati po letu 1950, pravi bum pa je doživela z razcvetom računalništva. Tako hitrejši in zmogljivejši računalniki omogočajo podporo pri reševanju vedno večjih in zahtevnejših problemov. Računalniško pridobljene rešitve na nekaj primerih nato pogosto porodijo tudi ideje za matematično izražene rešitve v večjih razredih grafov ali celo med vsemi grafi.

Moč grafov je, da predstavljajo model, ki je vsestransko uporaben od kemije (modeliranje spojin,...), biologije (model za RNK,...), sociologije (raziskovanje družbenih omrežij,...) do številnih drugih področij. Po drugi strani so vsa omrežja, ki smo jih zgradili ljudje, na nek način kar grafi. Recimo železniško omrežje, cestno omrežje, vodovodno omrežje, internetno omrežje, električno omrežje in tako naprej. Vsekakor je računalništvo v središču panog povezanih s teorijo grafov, saj ne le da je vedno več omrežij v računalništvu, z računalniškimi algoritmi lahko tudi rešujemo probleme iz teorije grafov.

V tem poglavju si bomo ogledali osnovne pojme v zvezi s teorijo grafov, nato pa spoznali več lastnosti, ki jih lahko preučujemo na grafih. Pri tem smo seveda omejeni s časom in prostorom, ki ga imamo za to na razpolago, saj so lastnosti na grafih omejene zgolj z domišljijo, nekaj pa tudi z njihovo uporabnostjo.

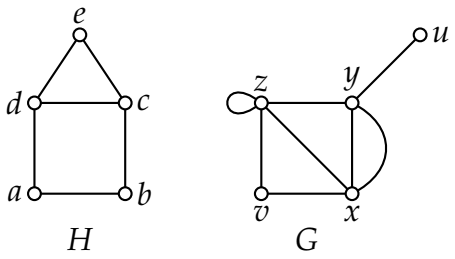
Še to, graf v tem poglavju **NI** graf funkcije, ki ga večina pozna is srednje šole.

Dodatno literaturo v slovenščini iz tega področja je moč najti v [2, 7, 10, 11, 14]. Posebej omenimo [15], ki je primerna za začetno spoznavanje s teorijo grafov. V angleškem jeziku je na voljo precej več primerne literature, tukaj omenimo le [1, 6, 8]. Marsikaj je najti tudi na spletu in pogosto je že Wikipedia (angleška) dober začetni vir informacij. Standardni zbirki nalog za to poglavje sta [5, 9]. Veliko izpitnih nalog iz tega poglavja je najti v [12, 13].

9.1 OSNOVNI POJMI O GRAFIH

Graf $G = (V(G), E(G))$ sestavljata neprazna množica vozlišč $V(G)$ in množica povezav $E(G)$. V **množici vozlišč** $V(G)$ lahko imamo poljubne elemente, medtem ko so elementi **množice povezav** že delno določeni z množico vozlišč $V(G)$. Tako so v $E(G)$ lahko le neurejene podmnožice množice vozišč $V(G)$ z dvema elementoma. Elementom množice $V(G)$ pravimo **vozlišča** grafa G, elementom množice $E(G)$ pa rečemo **povezave** grafa G. **Slika grafa** je vsaka predstavitev elementov množice $V(G)$ z različnimi točkami in množice $E(G)$ s črtami med vozlišči, ki določajo povezave.

Zgled 9.1 *Graf H je podan z množico vozlišč $V(H) = \{a, b, c, d, e\}$ in množico povezav $E(H) = \{\{a, b\}, \{b, c\}, \{d, a\}, \{e, c\}, \{d, e\}, \{c, d\}\}$. Predstavljen je na sliki 18. Zaradi te slike grafu H pravimo tudi graf hiša. Drugi graf s slike 18 je G in zanj velja $V(G) = \{u, v, x, y, z\}$ in $E(G) = \{\{v, x\}, \{z, z\}, \{z, x\}, \{y, z\}, \{u, y\}, \{x, y\}, \{y, x\}, \{v, z\}\}$. Pozorem bralec lahko opazi, da sta v $E(G)$ dva elementa $\{x, y\}$ in $\{y, x\}$ enaka. Tako je bolj pravilno govoriti o multimnožici povezav. Hkrati v $E(G)$ nastopa multimnožica $\{z, z\}$.*



Slika 18: Grafa H in G.

Zapis množice povezav iz zgleda 9.1 že na prvi pogled vsebuje preveč oklepajev, zato ga običajno poenostavimo in namesto $\{x, y\}$ pišemo kar xy ali yx. Tako množico povezav grafa G iz zgleda 9.1 zapišemo kar $E(G) = \{ab, bc, da, ec, de, cd\}$, kar je očesu bolj prijazno.

Naj bo G graf. Če vozlišči $u, v \in V(G)$ tvorita povezavo grafa G, torej če je $uv \in E(G)$, potem rečemo, da sta u in v **sosednji vozlišči** ali kar **sosedi**. V takšnem primeru pišemo $u \sim v$. Če vozlišči u in v ne tvorita povezave grafa G, potem u in v nista sosedi in pišemo $u \nsim v$.

Naj bo $e \in E(G)$. Potem povezavo e določata dve vozlišči grafa G, recimo x in y. Običajno pišemo kar $e = xy$ in pravimo, da sta vozlišči x in y **krajišči povezave** e ter da je vozlišče x **incidenčno** s povezavo e, kot tudi z vozliščem y. Povezavi $e = xy$ in $f = ab$ sta **sosednji**, če imata enako vsaj eno krajišče. Torej sta e in f sosednji, če je $x = a$, ali $x = b$, ali $y = a$, ali $y = b$. Kadar imata povezavi e in f

enaki obe krajišči, potem tvorita **večkratno povezavo**. Če ima povezava e enaki krajišči, torej če je $x = y$, potem rečemo povezavi e **zanka**. Med grafi se pogosto omejimo na takšne brez večkratnih povezav in zank, ki jim rečemo **enostavni grafi**.

Zgled 9.2 *V grafu H s slike 18 ima vozlišče a dva seseda b in d in pišemo $a \sim b$ oziroma $a \sim d$. Povezava $e = cd$ ima krajišči c in d. Tako sta tudi vozlišči c in d incidenčni s povezavo e. Povezava e je sosednja s povezavo $f = bc$, saj imata skupno krajišče c. V grafu H ni zank niti večkratnih povezav, zato je graf H enostaven graf.*

Po drugi strani imamo v grafu G s slike 18 zanko $e_1 = zz$. V tem primeru je z edino vozlišče incidenčno s povezavo e_1 in e_1 ima dve krajišči, ki pa sta med seboj enaki. Povezavi $f_1 = xy$ in $f_2 = xy$ sta različni in tvorita večkratno povezavo grafa G. Seveda sta f_1 in f_2 tudi sosednji povezavi. Povezavi e_1 in f_2 nista sosednji v G, saj nimata skupnega krajišča. Seveda G ni enostaven graf.

Množici vseh sosed $\{u \in V(G) : u \sim v\}$ nekega vozlišča v rečemo **odprta okolica** vozlišča v in jo označimo z $N_G(v)$. Če odprti okolici dodamo vozlišče v, potem dobimo **zaprto okolico** vozlišča v, ki jo označimo z $N_G[v]$. Torej velja zveza $N_G[v] = N_G(v) \cup \{v\}$. Če ni možnosti zamenjave med grafi, indeks G izpuščamo in pišemo kar $N[v]$ za zaprto okolico in $N(v)$ za odprto okolico. Če za vozlišče v velja $N_G[v] = V(G)$, potem rečemo, da je v **univerzalno vozlišče**. Z drugimi besedami, univerzalno vozlišče je sosed od vseh preostalih vozlišč.

Pomembno je tudi število povezav, katerim je vozlišče v krajišče. Temu številu rečemo **stopnja vozlišča** v in ga označimo z $\delta_G(v)$ ali bolj enostavno $\delta(v)$, če je graf G jasno določen. Opazimo lahko, da je v enostavnih grafih stopnja vozlišča kar enaka številu sosedov vozlišča v. Tako v enostavnih grafih velja $\delta(v) = |N(v)|$. Če je G enostaven graf in v njegovo univerzalno vozlišče, potem je $\delta(v) = |V(G)| - 1$. Vozlišču stopnje ena rečemo **list**, vozlišču stopnje nič pa **izolirano vozlišče**.

Vozlišča imajo lahko v grafu različne stopnje. Zgodi se pa lahko, da imajo vsa vozlišča enako stopnjo r, torej $\delta(v) = r$ za vsako vozlišče v iz $V(G)$. Tedaj govorimo o **regularnem**, oziroma natančneje, r-**regularnem grafu**.

Naj bo G graf z vozlišči $V(G) = \{v_1, v_2, \ldots, v_n\}$, ki so urejena po velikosti stopenj od največje stopnje do najmanjše stopnje. Torej velja $\delta(v_i) \geq \delta(v_j)$ za vsak $i < j$, kjer sta $i, j \in [n]$. Tako dobimo končno padajoče zaporedje[18] $(\delta(v_1), \delta(v_2), \ldots, \delta(v_n))$, ki mu rečemo **zaporedje stopenj vozlišč**. V zvezi s tem sta zanimivi vprašanji, ali je vsako končno padajoče zaporedje tudi zaporedje stopenj vozlišč kakega grafa in ali imata različna grafa tudi različni zaporedji

18 Spomnimo se, da sta sosednja člena v padajočem zaporedju lahko enaka, le naslednji člen ne sme biti večji od prejšnjega.

stopenj vozlišč. Kmalu bomo odgovorili na prvo vprašanje, na odgovor na drugo vprašanje pa moramo počakati do konca razdelka, saj zaenkrat še ne vemo, kaj pomeni, da sta grafa različna.

Zgled 9.3 *Spomnimo se grafov H in G s slike 18. Odprte okolice grafa H so $N_H(a) = \{b,d\}$, $N_H(b) = \{a,c\}$, $N_H(c) = \{b,d,e\}$, $N_H(d) = \{a,c,e\}$ in $N_H(e) = \{c,d\}$. Podobno so njegove zaprte okolice $N_H[a] = \{a,b,d\}$, $N_H[b] = \{a,b,c\}$, $N_H[c] = \{b,c,d,e\}$, $N_H[d] = \{a,c,d,e\}$ in $N_H[e] = \{c,d,e\}$. Stopnje vozlišč so $\delta_H(a) = 2$, $\delta_H(b) = 2$, $\delta_H(c) = 3$, $\delta_H(d) = 3$ in $\delta_H(e) = 2$. Tako je zaporedje stopenj vozlišč grafa H enako $(3,3,2,2,2)$. Seveda H ni regularen, saj stopnje vseh vozlišč niso enake.*

Nadaljujmo z grafom G. Njegove odprte okolice so $N_G(u) = \{y\}$, $N_G(v) = \{x,z\}$, $N_G(x) = \{v,z,y\}$, $N_G(y) = \{u,x,z\}$ in $N_G(z) = \{v,x,y,z\}$. Podobno so njegove zaprte okolice $N_G[u] = \{u,y\}$, $N_G[v] = \{v,x,z\}$, $N_G[x] = \{v,x,z,y\}$, $N_G[y] = \{u,x,y,z\}$ in $N_G[z] = \{v,x,y,z\}$. Stopnje vozlišč so $\delta_G(u) = 1$, $\delta_G(v) = 2$, $\delta_G(x) = 4$, $\delta_G(y) = 4$ in $\delta_G(z) = 5$. Tako je zaporedje stopenj vozlišč grafa H enako $(5,4,4,2,1)$. Seveda H ni regularen, saj stopnje vseh vozlišč niso enake. Vozlišče u je list v grafu H, le-ta pa nima univerzalnega vozlišča. Omenimo še, da je $N_G(z) = N_G[z]$ kar se zgodi, če je v vozlišču zanka. Pri stopnjah je potrebno opozoriti, da zanka prispeva 2 k stopnji vozlišča, saj je vozlišče z zanko dvakrat krajišče tej zanki. Dodajmo še, da vsaka povezava iz večkratne povezave prispeva ena k stopnji vozlišča.

Kmalu bomo lahko odgovorili na prvo prej postavljeno vprašanje v zvezi z zaporedji stopenj vozlišč. Pri tem nam bo pomagala naslednja trditev, ki ima več imen, mi ji bomo rekli kar Lema o rokovanju.

Trditev 9.1 (Lema o rokovanju) *Za poljuben graf G velja*

$$\sum_{v \in V(G)} \delta(v) = 2|E(G)|.$$

Dokaz. Naj bo G poljuben graf in naj bo $e \in E(G)$ njegova poljubna povezava. Opaziti je potrebno le, da vsaka povezava e prispeva 2 k vsoti vseh stopenj na levi, saj ima e dve krajišči. (To se zgodi tudi, če je e zanka, le da sta ti dve krajišči potem enaki.) ∎

Lema o rokovanju ima zanimivo posledico, ki govori o številu vozlišč lihe stopnje v poljubnem grafu.

Posledica 9.2 *Vsak graf G ima sodo število vozlišč lihe stopnje.*

Dokaz. Naj bo G graf. Njegova vozlišča lahko razbijemo na dva dela in sicer $V(G) = A \cup B$, kjer sta

$$\begin{aligned} A &= \{v \in V(G) : \delta(v) \text{ je sodo število}\} \text{ in} \\ B &= \{u \in V(G) : \delta(u) \text{ je liho število}\}. \end{aligned}$$

Sedaj lahko vsoto iz Leme o rokovanju razdelimo na dva dela

$$2|E(G)| = \sum_{v \in V(G)} \delta(v) = \sum_{v \in A} \delta(v) + \sum_{u \in B} \delta(v).$$

Seveda je $\sum_{v \in A} \delta(v)$ sodo število, saj seštevamo le soda števila. Tako je tudi

$$\sum_{u \in B} \delta(v) = 2|E(G)| - \sum_{v \in A} \delta(v)$$

sodo število, saj ga dobimo kot razliko dveh sodih števil. Ker pa v $\sum_{u \in B} \delta(v)$ seštevamo liha števila, je ta vsota soda natanko tedaj, ko je teh števil v vsoti sodo mnogo. To pomeni, da je v B in s tem tudi v $V(G)$ sodo mnogo vozlišč lihe stopnje. ■

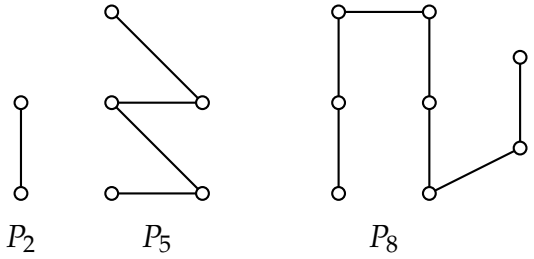
Sedaj že lahko odgovorimo negativno na prvo zastavljeno vprašanje, ki se glasi: ali je vsako končno padajoče zaporedje tudi zaporedje stopenj vozlišč. Oglejmo si na primeru.

Zgled 9.4 *Podana končna padajoča zaporedja* (5), $(8,7,6,5,4,3)$, $(1,1,1,1,1,1,1)$, $(6,6,5,5,4,3,2)$ *niso zaporedja stopenj vozlišč, saj vsebujejo liho število lihih števil, kar po posledici 9.2 ni mogoče za noben graf.*

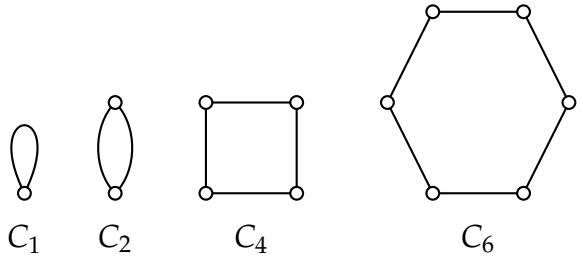
Nadaljujemo z vpeljavo nekaj standardnih družin grafov in razreda dvodelnih grafov.

Družina grafov poti
Pot na n vozliščih je graf P_n z množico vozlišč $V(P_n) = \{v_1, v_2, \ldots, v_n\}$ in množico povezav $E(P_n) = \{v_i v_{i+1} : i \in [n-1]\}$. Seveda ima P_n n vozlišč in $n-1$ povezav, oziroma $|V(P_n)| = n$ in $|E(P_n)| = n-1$. Pot P_n zapišemo tudi krajše z $v_1 v_2 \ldots v_n$ Opazimo lahko, da je $P_1 = v_1$ le eno vozlišče brez povezav, medtem ko ima pot $P_2 = v_1 v_2$ dve med seboj sosednji vozlišči. Pot P_n ima natanko dva lista, če je le $n > 1$. To sta vozlišči v_1 in v_n. Vsa preostala vozlišča imajo stopnjo 2, ko je $n > 2$. Torej je zaporedje stopenj vozlišč poti P_n kar $(2,2,\ldots,2,1,1)$, kjer je na začetku $n-2$ dvojk. Seveda ima to zaporedje sodo število, to je dve v tem primeru, lihih števil v skladu s posledico 9.2. Poti P_2, P_5 in P_8 so na sliki 19.

Družina grafov ciklov
Cikel na n vozliščih je graf C_n z množico vozlišč $V(C_n) = \{v_1, v_2, \ldots, v_n\}$ in množico povezav $E(C_n) = \{v_i v_{i+1} : i \in [n-1]\} \cup \{v_n v_1\}$. Seveda ima C_n n vozlišč in n povezav, oziroma $|V(C_n)| = n$ in $|E(C_n)| = n$. Cikel C_n zapišemo tudi krajše z $v_1 v_2 \ldots v_n v_1$. Opazimo lahko, da je $C_1 = v_1 v_1$, kar je zanka, medtem ko ima cikel $C_2 = v_1 v_2 v_1$ večkratno povezavo. Tako v enostavnih grafih ni moč najti ciklov C_1 in C_2. Ker se pogosto omejimo le na enostavne grafe, se v tem primeru pri ciklih običajno dodatno zahteva, da je $n \geq 3$. Vsa vozlišča cikla C_n so stopnje 2, kar pomeni, da je cikel 2-regularen graf. Torej je zaporedje stopenj vozlišč cikla C_n kar $(2,2,\ldots,2)$, kjer je n dvojk. Seveda ima to zaporedje sodo



Slika 19: Poti P_2, P_5 in P_8.



Slika 20: Cikli C_1, C_2, C_4 in C_6.

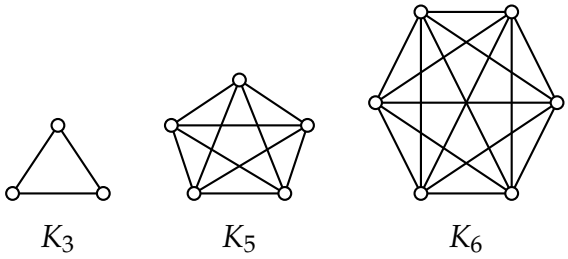
število, to je nič v tem primeru, lihih števil v skladu s posledico 9.2. Cikli C_1, C_2, C_4 in C_6 so na sliki 20.

Družina polnih grafov

Polni graf na n vozliščih je graf K_n z množico vozlišč $V(K_n) = \{v_1, v_2, \ldots, v_n\}$ in množico povezav $E(K_n) = \{v_iv_j : i, j \in [n], i \neq j\}$. Ponovno velja $|V(K_n)| = n$, medtem ko število povezav zahteva malo več pozornosti. Tako imamo v K_n povezavo med poljubnima različnima vozliščema. Z drugimi besedami nas zanima, koliko neurejenih izbir brez ponavljanja moči 2 obstaja nad n elementi. V tretjem poglavju smo reševali takšne probleme in spomniti se velja, da je $|E(K_n)| = \binom{n}{2} = \frac{n(n-1)}{2}$. Opazimo lahko, da je K_1 kar eno vozlišče (tako kot P_1), da je K_2 kar ena povezava (tako kot P_2) in da ima K_3 tri vozlišča v_1, v_2, v_3 in zaporedne povezave v_1v_2, v_2v_3, v_3v_1 (tako kot cikel C_3). Vsa vozlišča polnega grafa K_n so stopnje $n-1$, kar pomeni, da je K_n $(n-1)$-regularen graf in so vsa njegova vozlišča univerzalna. Torej je zaporedje stopenj vozlišč polnega grafa K_n kar $(n-1, n-1, \ldots, n-1)$. Če je n sodo število imamo sodo število (to je n) vozlišč lihe stopnje (to je $n-1$). Če je n liho število, potem imamo liho število vozlišč (to je n), sode stopnje (to je $n-1$) in nič vozlišč lihe stopnje. Oba primera sta skladna s posledico 9.2. Polni grafi K_3, K_5 in K_6 so na sliki 21.

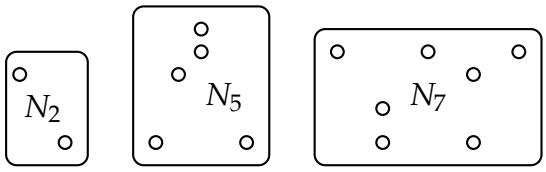
Družina praznih grafov

Prazni graf na n vozliščih je graf N_n z množico vozlišč $V(N_n) = \{v_1, v_2, \ldots, v_n\}$ in množico povezav $E(N_n) = \emptyset$. Velja $|V(N_n)| = n$ in $|E(N_n)| = 0$. Ponovno je N_1 le eno vozlišče. Opazimo lahko, da preostali prazni grafi N_n, $n \geq 2$, niso sestavljeni iz enega dela. Vsa njihova vozlišča so izolirana, saj imajo stopnjo 0.



Slika 21: Polni grafi K_3, K_5 in K_6.

Torej je zaporedje stopenj vozlišč praznega grafa N_n kar $(0, 0, \ldots, 0)$. Prazni grafi N_2, N_5 in N_7 so na sliki 22.



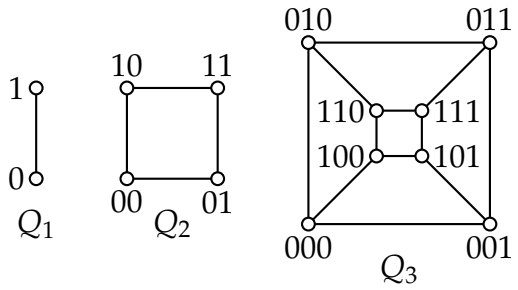
Slika 22: Prazni grafi N_2, N_5 in N_7.

Družina hiperkock ali r-kock

Hiperkocka ali r-kocka je graf Q_r definiran s pomočjo bitnih besed dolžine r. Tako je množica vozlišč $V(Q_r) = \{b_1 b_2 \ldots b_r : b_i \in \{0, 1\}, i \in [r]\}$. Dve bitni besedi sta sosedi v hiperkocki, če se razlikujeta na točno enem mestu. Formalno lahko tole zapišemo kot

$$E(Q_r) = \{b_1 b_2 \ldots b_r c_1 c_2 \ldots c_r : \exists i \in [r], b_i \neq c_i \wedge \forall j \in [r] - \{i\} : b_j = c_j\}.$$

Ponovno lahko uporabimo vsebine tretjega poglavja in ugotovimo, da število vozlišč r-kocke Q_r lahko izrazimo kot urejene izbire s ponavljanjem dveh elementov 0 in 1. Zato je $|V(Q_r)| = 2^r$. Preden določimo število povezav r-kocke, določimo stopnjo vozlišč. Ker ima vsako vozlišče r bitov, se lahko na enem bitu razlikuje od natanko r drugih r-bitnih besed. Zato ima vsako vozlišče r sosedov in Q_r je r-regularen graf z zaporedjem stopenj vozlišč $(r, r, \ldots, r)$. Sedaj uporabimo Lemo o rokovanju in dobimo $2|E(C_n)| = \sum_{v \in V(Q_r)} \delta(v) = \sum_{v \in V(Q_r)} r = r2^r$, oziroma $|E(Q_r)| = r2^{r-1}$. Na sliki 23 najdemo r-kocke Q_1, Q_2 in Q_3. Opazimo lahko, da je Q_1 kar povezava (tako kot P_2 in K_2), da ima Q_2 enako strukturo kot cikel C_4 in da povezave hiperkockeQ_3 tvorijo ogrodje kocke (od tukaj tudi ime r-kocke). Spomnimo se tudi, da so vsi ti trije primeri predstavljali Hassejeve diagrame Booleovih algeber, le da sedaj ni več važen nivo elementov. Dejansko najdemo r-kocke Q_2, Q_3 in Q_4 tudi na slikah 12 in 13, le da moramo odmisliti oznake vozlišč, oziroma jih je potrebno nadomestiti z ustreznimi bitnimi besedami.



Slika 23: Hiperkocke Q_1, Q_2 in Q_3.

Preden spoznamo razred dvodelnih grafov, si oglejmo še nekaj potrebnih pojmov. Graf H je **podgraf** grafa G, če je $V(H) \subseteq V(G)$ in $E(H) \subseteq E(G)$. Pogosto nas zanimajo podgrafi s kakšno dodatno lastnostjo. Tako je podgraf H grafa G **vpeti podgraf**, če imata enaki množici vozlišč, torej $V(H) = V(G)$. Po drugi strani je podgraf H grafa G **inducirani podgraf**, če iz $uv \in E(G)$ sledi, da je tudi $uv \in E(H)$ za poljubni vozlišči u in v iz H. To pomeni, da je podgraf H induciran, čim obstajajo v njem vse povezave iz G, ki nastopajo med vozlišči iz H, tudi v grafu H. Seveda je graf G tudi svoj podgraf. Edini podgraf grafa G, ki je hkrati vpet in induciran, je kar graf G sam. Pogosto nas zanima ali kak znan graf, recimo pot, cikel, polni ali prazni graf, obstaja kot (induciran ali vpet) podgraf v danem grafu G. Tako bomo o obstoju vpetega cikla oziroma vpete poti govorili v razdelku o Hamiltonovih grafih. Podgrafe pogosto tudi uporabljamo za opis novih pojmov. Sledita dva primera.

Graf G je **povezan**, če med poljubnima vozliščema u in v iz G obstaja podgraf, ki je pot z začetkom v u in zaključkom v v. Po domače lahko rečemo, da so povezani grafi iz enega dela, medtem ko imajo nepovezani grafi več delov. Naj bo graf G nepovezan. Potem ga sestavlja več delov, ki je vsak zase povezan. Tem delom rečemo **komponente** grafa G. Edini nepovezani graf, ki smo ga do sedaj spoznali, je prazni graf N_n za $n > 1$. Njegove komponente predstavlja kar vsako vozlišče zase in ima tako n različnih komponent. Vozlišče v je **presečno vozlišče**, če ima graf $G - v$ (izbrišemo vozlišče v in vse povezave incidenčne z v) več komponent kot originalni graf G. Povezava e je **most** v grafu G, če ima graf $G - e$ (izbrišemo le povezavo e, vsa vozlišča ohranimo) več komponent kot originalni graf G.

Naj bosta u in v poljubni vozlišči grafa G. **Razdalja** med u in v je najmanjše število povezav v podgrafu, ki je pot z začetkom v u in koncem v v. Označimo jo z $d_G(u, v)$ ali krajše $d(u, v)$, kadar grafa G ni moč zamenjati. Seveda je lahko med u in v več različnih podgrafov, ki so poti, vendar nas za določitev razdalje zanimajo le tiste z najmanj povezavami. Vsaki taki poti rečemo **najkrajša pot** med vozlišči u in v. Če sta a in b sosedi v grafu, potem je najkrajša pot med njima

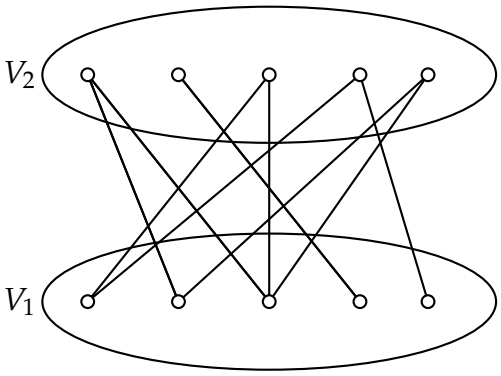
kar povezava ab in velja $d_G(a,b) = 1$. Velja tudi $d_G(a,a) = 0$, saj se pot a začne v a in zaključi v a, vsebuje le eno vozlišče in nobene povezave.

Zgled 9.5 *Na grafu H s slike 18 lahko opazimo, da je abcda inducirani podgraf, ki je cikel na štirih vozliščih. Če izpustimo zadnjo povezavo, potem dobimo pot abcd na štirih vozliščih, ki ni inducirana, saj ne vsebuje povezave da, ki je povezava grafa H. Omenjena cikel in pot nista vpeta podgrafa, saj ne vsebujeta vozlišča e. Pot badce predstavlja vpeti podgraf, ki pa ni induciran, saj ne vsebuje povezav ed in bc. Graf H vsebuje tudi vpeti cikel, ki je abceda, ki tudi ni induciran, saj ne vsebuje povezave cd. Seveda je H povezan graf, saj zlahka najdemo pot med poljubnim parom vozlišč. Pot adec ni najkrajša pod med vozliščema a in c, saj vsebuje tri povezave, medtem ko poti adc in abc vsebujeta le dve povezavi. Ker ne obstaja pot med a in c z eno povezavo, je $d_H(a,c) = 2$. Tako sta adc in abc dve najkrajši poti med a in c.*

Graf G s slike 18 vsebuje presečno vozlišče y, saj vsebuje $G - y$ dve komponenti. Ena je vozlišče u, druga pa je podgraf grafa G, induciran z vozlišči v, x in z. Graf G vsebuje tudi most, ki je povezava yu, saj $G - yu$ vsebuje dve komponenti. Prva je ponovno vozlišče x, medtem ko je druga induciran podgraf grafa G na vozliščih v, x, y in z. Graf H ne vsebuje nobenega mosta niti presečnega vozlišča.

Razred dvodelnih grafov

Graf G je **dvodelen graf**, če lahko množico vozlišč $V(G)$ razbijemo na dve množici V_1 in V_2 tako, da ima vsaka povezava grafa G eno krajišče v V_1 in drugo v V_2. Dvodelni graf je shematično predstavljen na sliki 24.



Slika 24: Shematični prikaz dvodelnega grafa.

Razbitje dvodelnega grafa lahko poiščemo s preprostim algoritmom. Začnemo v poljubnem vozlišču v in ga postavimo v V_1. Vsi njegovi sosedi so potem v V_2 in vsi njihovi sosedi v V_1. Z nadaljevanjem te procedure najdemo razbitje tiste komponente dvodelnega grafa, ki vsebuje v. Sedaj nadaljujemo s poljubnim vozliščem, če obstaja, za katero še ni bilo določeno, ali pripada V_1 ali V_2.

Obstaja veliko dvodelnih grafov, zato le-ti ne predstavljajo več družine grafov, pač pa temu rečemo razred dvodelnih grafov. Ni težko videti, da je pot P_n dvodelen graf za vsako naravno število n (razbitje tvorijo vozlišča s sodim in z lihim indeksom). Prav tako je vsak prazen graf N_n dvodelen (tukaj lahko razbitje izberemo na poljuben način). Po drugi strani sta K_1 in K_2 edina polna dvodelna grafa, medtem ko je cikel C_n dvodelen natanko tedaj, ko je n sodo število. Pokažimo bolj splošen rezultat, ki karakterizira dvodelne grafe s pomočjo neobstoja lihih ciklov v grafu G.

Izrek 9.3 *Graf G je dvodelen natanko tedaj, ko ne vsebuje lihega cikla.*

Dokaz. Recimo najprej, da G vsebuje lihi cikel $v_1v_2 \dots v_{2k+1}v_1$. Poskusimo razvrstiti vozlišča tega cikla v množici V_1 in V_2. Naj bo najprej $v_1 \in V_1$. Potem je $v_2 \in V_2$. Njegov sosed je v_3 in je zato $v_3 \in V_1$. Z nadaljevanjem vidimo, da vsa liha vozlišča v_{2i-1}, $i \in [k+1]$, pripadajo V_1, vsa soda v_{2i}, $i \in [k]$, pa so v V_2. To že pomeni, da graf G ni dvodelen, saj oba v_1 in v_{2k+1} pripadata isti množici V_1, hkrati pa je v_1v_{2k+1} povezava grafa G.

Nasprotno predpostavimo, da graf G ne vsebuje lihega cikla. Z indukcijo na število povezav m grafa G bomo pokazali, da je G dvodelen. Naj bo najprej $m = 1$ in $e = uv$ edina povezava v G. Ker G ne vsebuje lihega cikla, povezava ni zanka in velja $u \neq v$. Naj bo $u \in V_1$ in $v \in V_2$. Razporedimo še preostala možna vozlišča stopnje 0 na poljuben način v V_1 in V_2. Tako imamo željeno razbitje grafa G in G je dvodelen.

Naj bo sedaj $m > 1$. Izberimo poljubno povezavo $e = uv$ in si oglejmo graf $G - uv$, torej grafu G izbrišemo povezavo uv, sami krajišči pa pustimo. Ker je bil G brez lihih ciklov, je brez njih tudi $G - uv$ in po indukcijski predpostavki je dvodelen. Naj bo V_1 in V_2 dvodelno razbitje grafa $G - uv$. Če sta u in v v različnih množicah V_1 in V_2, potem imamo tudi dvodelno razbitje grafa G in smo končali z dokazom. Zato predpostavimo, da sta u in v v isti množici, recimo V_1. Če graf $G - uv$ ni povezan in sta u in v v različnih komponentah A in B grafa $G - uv$, potem vozliščem iz ene komponente zamenjamo mesta v V_1 in V_2. Bolj natančno, tvorimo novi množici $V_1' = (V_1 - V(A)) \cup (V(A) \cap V_2)$ in $V_2' = (V_2 - V(A)) \cup (V(A) \cap V_1)$. Seveda tudi V_1' in V_2' tvorita dvodelno razbitje $G - uv$, le da sta sedaj u in v v različnih množicah V_1' in V_2'. Torej V_1' in V_2' tvorita dvodelno razbitje grafa G, ki je zato dvodelen.

Zadnja možnost je, da sta u in v v isti komponenti grafa $G - uv$. Tedaj obstaja pot $ux_1x_2 \dots x_kv$. Ker sta u in v oba v V_1 in je $G - uv$ dvodelen, so vsa vozlišča x_i z lihim indeksom v V_2 in vsa vozlišča x_i s sodim indeksom v V_1. Posebej mora biti $x_k \in V_2$, saj je sosed od v. Zato je k liho število. Tako je cikel $ux_1x_2 \dots x_kvu$ v grafu G lihe dolžine, kar je v nasprotju s predpostavko in to ni mogoče. Torej je G dvodelen graf in dokaz je zaključen. ∎

Posebej še pokažimo, da so tudi r-kocke dvodelni grafi.

Trditev 9.4 *Hiperkocka Q_r je dvodelen graf za vsako naravno število r.*

Dokaz. Nad bitnimi besedami dolžine r, ki so vozlišča hiperkocke Q_r, tvorimo razbitje

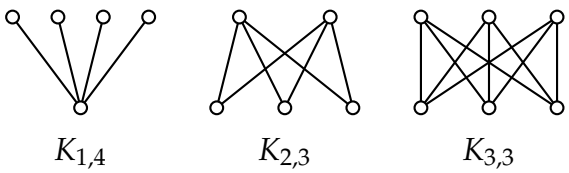
$$\begin{aligned} V_1 &= \{b_1b_2\ldots b_r : b_1b_2\ldots b_r \text{ vsebuje liho število enic}\} \text{ in} \\ V_2 &= \{b_1b_2\ldots b_r : b_1b_2\ldots b_r \text{ vsebuje sodo število enic}\}. \end{aligned}$$

Naj bo $B = b_1b_2\ldots b_r \in V_1$ in tako vsebuje liho število enic. Vsi njegovi sosedje se od B razlikujejo točno v enem bitu. To pomeni, da se je enica iz B spremenila v ničlo pri sosedu, oziroma ničla iz B se je spremenila v enico pri sosedu. Torej ima sosed enico manj ali enico več kot B. V vsakem primeru ima sodo število enic in je v V_2.

Podoben razmislek lahko ponovimo za poljubno vozlišče iz V_2 in vidimo, da ima vse sosede v V_1. Tako tvorita V_1 in V_2 dvodelno razbitje r-kocke Q_r, ki je zato dvodelna. ■

Družina polnih dvodelnih grafov

Tudi med dvodelnimi grafi lahko najdemo družine grafov in najpomembnejša je zagotovo družina polnih dvodelnih grafov. Dvodelen graf $K_{s,t}$ je **poln dvodelen graf**, če ima dvodelno razbitje $V_1 = \{v_1, v_2, \ldots, v_s\}$ in $V_2 = \{u_1, u_2, \ldots, u_t\}$ in vse možne povezave med V_1 in V_2. Torej je $E(K_{s,r}) = \{v_iu_j : i \in [s], j \in [t]\}$. Število vozlišč je seveda $|V(K_{s,r})| = s + r$. Vsako vozlišče iz V_1 ima natanko t sosedov v V_2, zato je število povezav kar $|E(K_{s,t})| = st$. Zato imajo vozlišča iz V_1 stopnjo t in podobno imajo vozlišča iz V_2 stopnjo s. Tako je $(s, s, \ldots, s, t, t, \ldots, t)$ zaporedje stopenj vozlišč grafa $K_{s,t}$, če je le $s \geq t$ in je s na prvih t mestih in t na zadnjih s mestih. Opazimo lahko, da je $K_{1,1}$ kar ena povezava (tako kot P_2, K_2 in Q_1). Polnim dvodelnim grafom $K_{1,t}$ pravimo tudi **zvezde**. Polni dvodelni grafi $K_{1,4}$, $K_{2,3}$ in $K_{3,3}$ so na sliki 25.



Slika 25: Polni dvodelni grafi $K_{1,4}$, $K_{2,3}$ in $K_{3,3}$.

Razdelek zaključujemo z razpravo o enakostih med grafi. Omenili smo že, da grafe P_2, K_2, Q_1, $K_{1,1}$ sestavljata dve vozlišči in ena povezava med njima. Ali to pomeni, da so si ti grafi med seboj enaki? Pri odgovoru na to moramo biti matematično strogi. To pomeni, da so si grafi med seboj enaki, če imajo enako množico vozlišč in enako množico povezav. Tako sta recimo P_2 in K_2 enaka, če velja $V(P_2) = V(K_2)$ in $E(P_2) = E(K_2)$. Ta pogoj ni vedno izpolnjen. Tako lahko vozlišči grafa P_2 predstavljata povezana serverja, vozlišči grafa K_2 pa recimo zaporedni križišči na neki cesti. Seveda v tem primeru grafa nista enaka.

Kljub vsej matematični doslednosti se vendarle zdi, da sta si grafa K_2 in P_2, če odmislimo kaj predstavljajo njuna vozlišča, dovolj podobna, da je to potrebno nekako izraziti. Dejansko v takšnem primeru govorimo o izomorfnosti med grafi, kar pomeni enako strukturo kot grafa, ne glede na izvor vozlišč. Tako sta grafa G in H **izomorfna**, če obstaja bijekcija $\varphi : V(G) \to V(H)$, ki ohranja povezave in nepovezave. Izomorfnost grafov G in H označimo z $G \cong H$.

Razmislimo še kaj pomeni, da preslikava iz množice vozlišči enega grafa v množico vozlišč drugega grafa ohranja povezave in nepovezave. Naj bo $e = uv$ povezava grafa G. Preslikava φ krajišči povezave e preslika v vozlišči $\varphi(u)$ in $\varphi(v)$. Če torej želimo, da se povezava uv ohrani, mora biti tudi $\varphi(u)\varphi(v)$ povezava grafa H. Podobno se ohranjajo nepovezave. Če torej x in y ne tvorita povezave v G, potem tudi njuni sliki $\varphi(x)$ in $\varphi(y)$ ne tvorita povezave v H. S simboli lahko tole zapišemo

$$\begin{aligned} uv &\in E(G) \Rightarrow \varphi(u)\varphi(v) \in E(H) \text{ in} \\ xy &\notin E(G) \Rightarrow \varphi(x)\varphi(y) \notin E(H). \end{aligned}$$

Če zadnji pogoj zapišemo v obliki kontrapozicije, potem dobimo

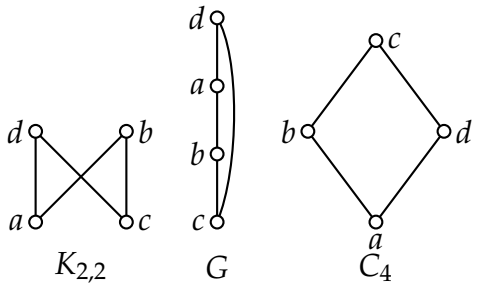
$$\varphi(x)\varphi(y) \in E(H) \Rightarrow xy \in E(G).$$

Tako vidimo, da lahko pogoj ohranjati povezave in nepovezave zapišemo kot ekvivalenco

$$uv \in E(G) \Leftrightarrow \varphi(u)\varphi(v) \in E(H).$$

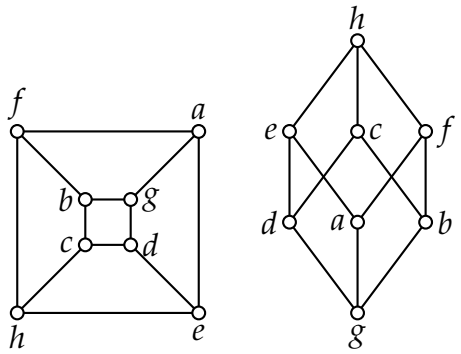
Izomorfnost dveh grafov seveda najprej pomeni, da imata isto število vozlišč, zaradi bijekcije med množicama vozlišč. Tudi število povezav mora biti isto, saj se povezave in nepovezave ohranjajo. Še več, zaradi zadnjega pogoja se v grafu H ohranijo vse lastnosti grafa G in obratno. Neformalno si lahko izomorfne grafe predstavljamo tudi kot grafe, ki imajo enako strukturo, a so drugače narisani.

Zgled 9.6 *Na sliki 26 so trije med seboj izomorfni grafi. Bijekcija med njihovimi vozlišči je podana z oznakami vozlišč. Ker so ti grafi dovolj majhni, lahko dejansko preverimo, ali se vse povezave in nepovezave ohranjajo. Tako je recimo bc povezava na vseh treh grafih, med b in d pa ni povezave na vseh treh grafih. Torej velja $K_{2,2} \cong G \cong C_4$. Omenimo, da, zaradi lažjega zapisa, namesto $\varphi(x)$ običajno pišemo kar x.*



Slika 26: Izomorfni grafi $K_{2,2}$, G in C_4, ter bijekcije med njimi, ki ohranjajo povezave in nepovezave.

Zgled 9.7 *Na sliki 27 sta dva med seboj izomorfna grafa. Bijekcija med njihovimi vozlišči je ponovno podana z oznakami vozlišč. Ponovno lahko preverimo, da se vse povezave in nepovezave ohranjajo. Kot omenjeno pa se ohranjajo tudi vse preostale lastnosti. Tako imamo med vozliščema h in g šest različnih najkrajših poti in sicer hcdg, hcbg, hfag, hfbg, hedg in heag. Poiščite jih na obeh grafih. Oba grafa imata tudi vpeti podgraf hfbcdgae, ki je cikel. Oba imata tudi šest podgrafov, ki so izomorfni C_4. Poiščite jih sami.*



Slika 27: Izomorfna grafa G in H, ter bijekcija med njima, ki ohranja povezave in nepovezave.

Seveda se porodi vprašanje, kako poiskati bijekcijo, ki ohranja povezave in nepovezave, če sploh obstaja. V splošnem za ta problem (še) ni znano, ali zanj obstaja polinomski algoritem, ali sodi med NP-polne probleme. Kar pomeni, da zaenkrat ni kakšnega enostavnega recepta za iskanje take bijekcije. Vsekakor je smiselno preizkusiti nekaj možnosti in pri tem se, predvsem na manjših grafih, pogosto vidi, ali takšna bijekcija obstaja.

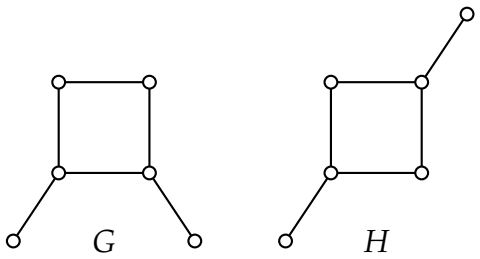
Kaj pa če takšna bijekcija ne obstaja? To pomeni, da grafa nista izomorfna. Lažja možnost je seveda, da imata grafa različno število vozlišč. Potem seveda nista izomorfna. Predpostavimo torej lahko, da imata G in H isto število vozlišč. Negacija definicije izomorfnosti je, da za vsako bijekcijo med množicama vozlišč

obstaja povezava ali nepovezava, ki je bijekcija ne ohranja. Če je $|V(G)| = n = |V(H)|$, to pomeni $n!$ različnih bijekcij. Za $n = 10$ to pomeni 3628800 različnih bijekcij. Tudi s pomočjo računalnika preverjanje vseh takšnih bijekcij vzame kar veliko časa. Ob tem je seveda 10 zelo majhno število. Kaj če ima graf 1000 vozlišč? To v realnem času ni izvedljivo.

Kako torej pokazati, da grafa nista izomorfna? Za izomorfna grafa velja, da se vse lastnosti med njima ohranijo. Če pa nista izomorfna, potem obstaja vsaj ena lastnost, ki je različna pri obeh grafih. Če najdemo eno samo takšno lastnost, to že zadošča za dokaz, da grafa nista izomorfna. Nekaj takšnih lastnosti si bomo ogledali v naslednjih razdelkih.

Zgled 9.8 *Na sliki 28 sta dva grafa G in H na šestih vozliščih. Oba imata isto zaporedje stopenj vozlišč $(3,3,2,2,1,1)$. Pri iskanju bijekcije nam delo olajša dejstvo, da imajo vozlišča različne stopnje, saj se recimo list lahko preslika le v list. S tem se zelo zmanjša število bijekcij, ki pridejo v poštev. Kljub temu bijekcije, ki bi ohranjala povezave in nepovezave, ni moč najti. Ali to pomeni, da nista izomorfna? Zato je potrebno poiskati kakšno lastnost, ki jo en graf ima, drugi pa ne. Že na tem majhnem primeru je teh lastnosti kar nekaj in zato $G \ncong H$. Naštejmo najbolj očitne:*

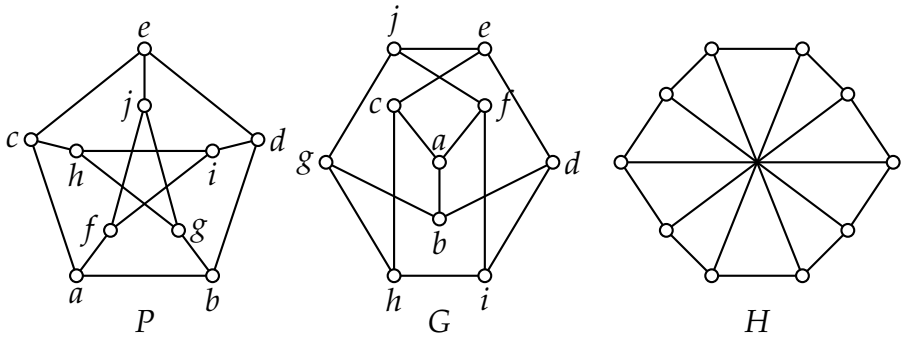
- *vozlišči stopnje tri sta sosedi v G, v H pa ne;*
- *vozlišči stopnje dva sta sosedi v G, v H pa ne;*
- *med listoma je razdalja 3 v G in 4 v H;*
- *v G obstaja vpeti podgraf, ki je pot, v H pa ne;*
- *V H imamo dve vozlišči na razdalji 4 (oba lista), v G pa ne.*



Slika 28: Neizomorfna grafa G in H z enakim zaporedjem stopenj vozlišč $(2,2,2,2,1,1)$.

V zadnjem zgledu smo mimogrede odgovorili na drugo vprašanje iz zaporedij stopenj vozlišč. Ali isti zaporedji pomenita tudi izomorfna grafa? Kot vidimo v tem zgledu, to ni res.

Zgled 9.9 *Na sliki 29 so trije 3-regularni grafi na desetih vozliščih. Skrajno levi graf P je zelo znani Petersenov graf. Srednji graf G je izomorfen Petersenovemu grafu, saj je z oznakami vozlišč podana bijekcija, ki ohranja povezave in nepovezave. Omenimo še, da je graf P tako simetričen, da bi lahko v sredinsko vozlišče grafa G preslikali katerokoli vozlišče grafa P. Poskusite poiskati še kakšno drugo bijekcijo, ki ohranja povezave in nepovezave. Graf H po drugi strani ni izomorfen P in s tem tudi ne G. Morda najbolj očitna lastnost, ki jo ima H, ne pa tudi P, je obstoj več ciklov dolžine štiri v H, medtem ko jih v P ni. Graf H ima tudi vpeti cikel, ki ga ni najti v P.*



Slika 29: Izomorfna Petersenov graf P in graf G ter njima neizomorfen graf H.

9.2 EULERJEVI GRAFI

Pot P_n ima vsa vozlišča različna, tako kot graf kot tudi, če na P_n pogledamo kot na podgraf grafa G. Kaj pa, če se vozlišča lahko ponavljajo? Tedaj govorimo o sprehodu. **Sprehod** W v grafu je zaporedje vozlišč $w_1w_2 \dots w_k$, za katera velja, da zaporedni vozlišči tvorita povezavo v grafu G. Tako v sprehodu W velja $w_iw_{i+1} \in E(G)$ za vsak $i \in [k-1]$. Ob tem ni nobenega pogoja za vozlišča, ki se lahko ponavljajo. Če je prvo vozlišče sprehoda enako zadnjemu, torej $w_1 = w_k$, potem govorimo o **sklenjenem sprehodu**. Če so povezave na sprehodu W različne, potem je W **enostaven sprehod**. Če pa zahtevamo, da so vozlišča sprehoda različna, potem dobimo pot, ki jo že poznamo.

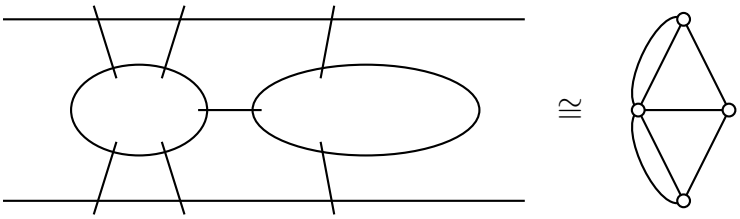
Enostavnemu sklenjenemu sprehodu, ki vsebuje vse povezave, rečemo **Eulerjev**[19] **sprehod**. Eulerjev sprehod vsebuje vsako povezavo in, ker je enostaven, se povezave ne ponavljajo. Tako vidimo, da Eulerjev sprehod vsebuje vsako povezavo natanko enkrat. Še več, ker je Eulerjev sprehod tudi sklenjen, se začne in konča v istem vozlišču.

19 Leonhard Euler (1707-1783) je bil švicarski matematik, ki je bil zelo ploden. Med drugim velja za začetnika teorije grafov. Bil naj bi zadnji, ki naj bi obvladal vso matematiko svojega časa. Pri sestavljanju seznama možnih zgodovinskih oseb, ki so najverjetneje potovale v času nazaj, so ga postavili na prvo mesto.

Sprehod, ki vsebuje vse povezave, je **pol-Eulerjev**, če je enostaven. Tudi pol-Eulerjev sprehod vsebuje vsako povezavo natanko enkrat, a za razliko od Eulerjevega sprehoda, začetno in končno vozlišče nista nujno enaki. Lahko sta tudi enaki in zato je vsak Eulerjev sprehod tudi pol-Eulerjev sprehod.

Zgled 9.10 *Spomnimo se grafov H in G s slike 18. Sprehod abcdeda grafa H je sklenjen, a ni enostaven, saj vsebuje povezavo de dvakrat. Sprehod abcda v H je enostaven sklenjen sprehod, a ni Eulerjev, saj ne vsebuje povezav de in ce. Sprehod dabcdec v H je enostaven in vsebuje vse povezave, a ni sklenjen. Zato ni Eulerjev, je pa pol-Eulerjev. Kot bomo videli kasneje, glejte izrek 9.7, v grafu H Eulerjev sprehod ne obstaja. Tudi graf G je pol-Eulerjev, a ni Eulerjev. Eden izmed pol-Eulerjevih sprehodov je zzxyzvxyu. Ob tem dodajmo, da sta povezavi xy iz tega sprehoda različni, saj G vsebuje dvojno povezavo xy. Torej lahko (pol-)Eulerjeve sprehode iščemo tudi na grafih, ki niso enostavni.*

Namenimo sedaj nekaj vrstic zgodovinskemu orisu, saj velja vsebina tega razdelka za začetek teorije grafov. V mestu Königsberg, danes znano po imenu Kaliningrad, je reka Pregel izoblikovala dva otoka, ki sta bila povezana z bregovi reke in med sabo s sedmimi mostovi, kot je nakazano na levi strani slike 30 (bolj realistično sliko oziroma zemljevid najdete recimo na Wikipediji). Med meščani, predvsem med mlajšo populacijo, je bilo popularno vprašanje, ali lahko prehodijo vsak most natanko enkrat in končajo na začetku? Takemu sprehodu sedaj rečemo Eulerjev, saj je Euler takrat to uganko preoblikoval v graf na desni strani slike 30 in pokazal bolj splošen rezultat, kdaj takšen sprehod obstaja in kdaj ne, glej izrek 9.7. Seveda sam takrat takim sprehodom ni rekel Eulerjevi, tako so jih poimenovali kasneje.



Slika 30: Shematični prikaz mostov na reki Pregel in graf, s katerim se opiše situacija.

Kot smo videli v zadnjem zgledu, Eulerjev sprehod ne obstaja za vsak graf. Zato grafu G rečemo **Eulerjev graf**, če vsebuje kak Eulerjev sprehod. Podobno poznamo tudi **pol-Eulerjeve grafe**, ki so tisti, ki vsebujejo kak pol-Eulerjev sprehod. Seveda je vsak Eulerjev graf tudi pol-Eulerjev, medtem ko obratno ne drži, kot smo videli v zadnjem zgledu.

Preden podrobno opišemo Eulerjeve grafe, potrebujemo dve pomožni trditvi.

Lema 9.5 *Če je graf G brez vozlišč stopnje nič Eulerjev graf, potem lahko Eulerjev sprehod začnemo v poljubnem vozlišču.*

Dokaz. Naj bo $W = w_1w_2 \dots w_kw_1$ Eulerjev sprehod v grafu G. Ker v G ni izoliranih vozlišč, je vsako vozlišče grafa G krajišče kake povezave in zato ga najdemo na W. Izberimo poljubno vozlišče $v \in V(G)$, ki je $v = w_i$ za nek $i \in [k]$. S premikom po Eulerjevem sprehodu W dosežemo, da je tudi sprehod $w_iw_{i+1} \dots w_kw_1w_2 \dots w_{i-1}w_i$ Eulerjev sprehod, ki se začne in konča v v. ∎

Lema 9.6 *Če obstaja sprehod med vozliščema u in v grafa G, potem v G obstaja tudi pot med u in v.*

Dokaz. Naj bo $W = uw_1w_2 \dots w_kv$ sprehod med vozliščema u in v v grafu G. Premikamo se po sprehodu W in, če naletimo na vozlišče, ki se ponovi, vmesni del izpustimo, oziroma izbrišemo iz W. Ta postopek ponavljamo, dokler so vsa preostala vozlišča različna. To pa pomeni, da je ostala pot med u in v. ∎

Sedaj lahko opišemo Eulerjeve grafe na zelo eleganten način s preprostim pogojem, ki je algoritmično hitro preverljiv.

Izrek 9.7 *Graf G brez izoliranih vozlišč je Eulerjev natanko tedaj, ko je povezan in imajo vsa njegova vozlišča sodo stopnjo.*

Dokaz. Naj bo G Eulerjev graf brez vozlišč stopnje nič z Eulerjevim sprehodom $W = w_1w_2 \dots w_kw_1$. Potem je vsako vozlišče krajišče kake povezave in ga zato najdemo na W. Izberimo poljubni vozlišči $u, v \in V(G)$. Naj zanju velja $u = w_i$ in $v = w_j$. Torej obstaja sprehod med u in v, če začnemo v $u = w_i$ in nadaljujemo po W do $w_j = v$. Po lemi 9.6 obstaja v G tudi pot med u in v. Ker sta bili u in v izbrani poljubno, sledi, da je graf G povezan. Pokažimo še, da imajo vsa vozlišča sodo stopnjo. Izberimo poljubno vozlišče u, ki je različno od w_1. Vsakič, ko po W pridemo v u, ga z nadaljevanjem po W tudi zapustimo. Tako vsak obisk vozlišča u s sprehodom W prinese 2 k stopnji vozlišča u. Torej velja

$$\delta(u) = 2 + 2 + \dots + 2 = 2\ell,$$

če vozlišče u najdemo ℓ-krat na sprehodu W. Podobno je tudi z začetnim vozliščem w_1, le da sedaj začnemo šteti z 1, saj smo v w_1 začeli, pri vsakem nadaljnem obisku W v w_1 dodamo 2. Končamo pa ponovno z 1, saj se sprehod zaključi v w_1 in več ne nadaljujemo. Tako je

$$\delta(u) = 1 + 2 + 2 + \dots + 2 + 1 = 2p,$$

če vozlišče w_1 obiščemo $p + 1$-krat (vključno z začetkom in koncem). Torej ima vsako vozlišče sodo stopnjo in prva implikacija je dokazana.

Naj bo sedaj graf G povezan in vsa njegova vozlišča naj imajo sodo stopnjo. Z indukcijo na število povezav $m = |E(G)|$ bomo pokazali, da je graf G Eulerjev. Če je $m = 1$, potem ima G eno vozlišče v z zanko, saj je stopnja vseh vozlišč soda. To pomeni hkrati, da ima G le eno vozlišče, saj je povezan in tako nima izoliranih

vozlišč. Seveda je vv Eulerjev sprehod za tak graf. Preverimo še posebej, kaj se zgodi, ko ima G dve vozlišči u in v. Ker je G povezan, obstaja vsaj ena povezava med u in v. Ker je stopnja obeh vozlišč sodo število, je povezav med u in v sodo mnogo in imamo večkratno povezavo. Hkrati imata lahko u in v poljubno število zank. Eulerjev sprehod dobimo tako, da začnemo v u in najprej prehodimo vse zanke v u, nato po eni povezavi v v in prehodimo vse zanke v v. Ostalo je še liho število povezav med u in v, tako da, ko vsako prehodimo enkrat, končamo v u. Ker ima G Eulerjev sprehod, je tudi Eulerjev graf.

Naj bo sedaj $m \geq 3$. Zato obstajajo tri vozlišča u, v in w, da sta $e_1 = uv$ in $e_2 = vw$ povezavi grafa G, saj je G povezan graf. Določimo nov graf G', ki ga dobimo iz G tako, da izbrišemo povezavi e_1 in e_2, ter dodamo povezavo $e_3 = uw$. Število vozlišč se v grafu G' ne spremeni, zato pa ima G' eno povezavo manj kot G. Opazimo še, da se stopnja vozlišč u in w ni spremenila, saj smo eno povezavo s krajiščem u oziroma w izbrisali, eno pa dodali. Po drugi strani se stopnja vozlišča v zmanjša za dva, saj smo izbrisali dve povezavi, katerih krajišče je v. Če je G' povezan graf, potem je G' Eulerjev graf po indukcijski predpostavki. Zato obstaja Eulerejev sprehod $W = x_1x_2 \dots x_iuwx_{i+3}x_{i+4} \dots x_kx_1$. Po lemi 9.6 je Eulerjev sprehod tudi $W' = uwx_{i+3}x_{i+4} \dots x_kx_1x_2 \dots x_iu$. Če sedaj nadomestimo povezavo uw s povezavama uv in vw, dobimo $W'' = uvwx_{i+3}x_{i+4} \dots x_kx_1x_2 \dots x_iu$, ki je Eulerjev sprehod grafa G.

Lahko se zgodi tudi, da G' ni povezan graf. V tem primeru indukcijske predpostavke ne moremo uporabiti direktno. Ima pa graf G dve komponenti C_u, ki vsebuje vozlišči u in w, ter C_v, ki vsebuje vozlišče v. Vsaka komponenta zase je povezana, zato ima vsa vozlišča sode stopnje in manj povezav kot graf G. Zato lahko uporabimo indukcijsko predpostavko za vsako posebej. Tako sta C_u in C_v Eulerjeva grafa z Eulerjevima sprehodoma $W_1 = uwy_1y_2 \dots y_ku$ oziroma $W_2 = vz_1z_2 \dots z_\ell v$, kjer smo že upoštevali lemo 9.6. Sedaj je $W = uvz_1z_2 \dots z_\ell vwy_1y_2 \dots y_ku$ Eulerjev sprehod v G, kar zaključuje dokaz. ∎

Dokaz izreka 9.7 nam da tudi idejo, kako je s pol-Eulerjevimi grafi. Ker v tem primeru ne rabimo začeti in končati v istem vozlišču, lahko imamo največ dve vozlišči lihe stopnje. Seveda to pomeni ali nič vozlišč lihe stopnje (to so Eulerjevi grafi), ali dve vozlišči lihe stopnje (to so pol-Eulerjevi grafi, ki niso Eulerjevi), saj graf ne more imeti enega vozlišča lihe stopnje po posledici 9.2. Tako velja naslednji izrek.

Izrek 9.8 *Graf G brez izoliranih vozlišč je pol-Eulerjev natanko tedaj ko je povezan in vsebuje največ dve vozlišči lihe stopnje.*

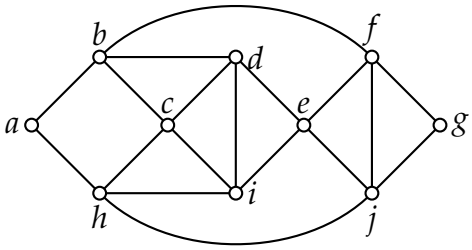
Pogoj iz izreka 9.7 je lahko algoritmično preverljiv. Določiti moramo le stopnje vozlišč, za kar preštejemo vse povezave, katerih krajišče je ustrezno vozlišče. Za to pregledamo vsako povezavo natanko dvakrat. Povezanost grafa se lahko preveri z BFS ali z DFS algoritmom (glej razdelek o algoritmih), ki imata oba

linearno časovno zahtevnost glede na število povezav. Tako lahko preverimo, ali je graf Eulerjev, kot tudi ali je pol-Eulerjev, v lineranem času $O(m)$, kjer je m število povezav grafa.

To pa nam še ne da samega Eulerjevega sprehoda. Le tega poiščemo s **Fleuryjevim algoritmom**, ki ga lahko izvedemo za Eulerjev oziroma pol-Eulerjev graf. Algoritem je zelo preprost in ga sestavljata le dva koraka:

- začni v poljubnem vozlišču (ozirom v vozlišču lihe stopnje, če je graf pol-Eulerjev);
- ponavljaj dokler je še kaj povezav: izberi poljubno povezavo ki ni most, most izberemo le, če ni druge možnosti, jo prehodimo in izbrišemo.

Zgled 9.11 *Oglejmo si Eulerjev graf (povezan z vsemi vozlišči sode stopnje) s slike 31. Recimo, da začnemo v vozlišču a. Ena izmed možnosti za Eulerjev sprehod je abchjfgjeidbfedciha. Opazimo lahko, da je povezava ha most, ko smo prvič v vozlišču h. Zato v tem primeru ne smemo nadaljevati s to povezavo. Ko smo prvič v vozlišču g, je povezava gj most, a tokrat ni druge izbire, zato gremo po tem mostu. Tudi na naslednjem koraku je povezava ej most, ki pa ne pušča druge možnosti, zato ga prehodimo. Ta situacija se še nekajkrat ponovi v nadaljevanju.*



Slika 31: Eulerjev graf za zgled 9.11.

Na koncu tega razdelka si oglejmo še **Kitajski problem poštarja**. Model za ta problem predstavlja območje, na katerem mora poštar raznositi pošto. Križišča na tem območju in konci slepih ulic predstavljajo vozlišča grafa. Med posameznimi vozlišči, to je križišči, pa so ulice, poti, ceste, ki predstavljajo povezave našega grafa. Tako sta dve križišči sosednji na grafu, če je med njima kakšna ulica in na tej ulici ni vmes nobenega drugega križišča. Tako lahko cestno omrežje predstavimo z grafom.

Povezave dodatno ocenimo po težavnosti. To pomeni, da je recimo ulica, ki ni asfaltirana, težavnejša, saj je ob dežju veliko blata. Druga merila, ki so lahko pomembna za poštarja, so recimo prisotnost psov v ulici, naklon ulice, ali je v ulici kakšna gostilna in podobno. Zahtevnejše ulice dobijo večjo številko, ki ji pogosto rečemo utež ali cena. Skupaj pa imamo graf z uteženimi povezavami.

Ker mora poštar dostaviti reklame vsaki hiši vsak dan, mora vsako povezavo (ulico) prehoditi vsaj enkrat in se na koncu vrniti na pošto, kjer je začel, da poda poročilo. Če je dobljen graf Eulerjev, se lepo izide in lahko vsako povezavo prehodi natanko enkrat. Kako pa postopamo, če graf ni Eulerjev? Oglejmo si na primeru pol-Eulerjevih grafov, ki niso Eulerjevi. Le-ti imajo natanko dve vozlišči lihe stopnje. Vprašajmo se, kako bi določili ulice, ki jih bo potrebno prehoditi dvakrat, da bo zahtevnost poti najmanjša? Skratka, povezave, ki se bodo podvojile, morajo imeti čim manjšo utež. Hkrati morajo te dodane povezave, skupaj z na začetku podanim grafom, tvoriti Eulerjev graf. Najmanjšo dodano utež bomo dobili, če bomo med vozliščema lihe stopnje na grafu poiskali pot, ki ima najmanjšo skupno utež in jo dodali začetnemu grafu. S tem bomo zagotovili, da je dobljeni graf Eulerjev in da bodo skupne uteži (ali cena) najnižja.

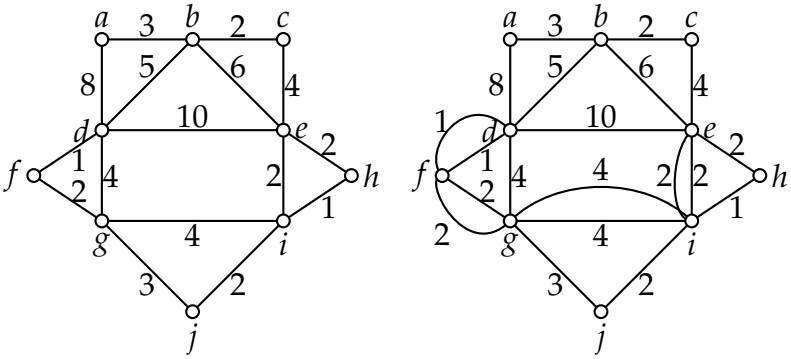
Zgled 9.12 *Rešimo Kitajski problem poštarja na uteženem grafu na levi na sliki 32. Opazimo lahko, da graf vsebuje dve vozlišči d in e, ki sta lihe stopnje. Torej imamo pol-Eulerjev graf. Poiščimo pot med d in e s skupno najnižjimi utežmi. Opazimo lahko, da je to pot dfgie s skupno utežjo 9 in povezave na tej poti podvojimo. Ta graf je na desni strani slike 32. Sedaj s Fleuryjevim algoritmom poiščemo Eulerjev sprehod in sproti seštevamo uteži za rešitev Kitajskega problema poštarja. Če začnemo v a, je en možen Eulerjev sprehod*

$$abcebdehieigijgfgdfda,$$

ki ima vsoto uteži

$$3+2+4+6+5+10+2+1+2+2+4+4+2+3+2+2+4+1+1+8=68,$$

kar je rešitev Kitajskega problema poštarja za uteženi graf s slike 32.



Slika 32: Pol-Eulerjev graf z utežnimi povezavami za zgled 9.12.

Kako pa postopati, kadar ima graf več vozlišč lihe stopnje, recimo $2k$? Recept je podoben, le da poiščemo poti z najmanjšimi skupnimi utežmi med vsemi pari vozlišč lihe stopnje. Tako lahko tvorimo poln graf K_{2k} iz vseh vozlišč lihe stopnje začetnega grafa in utežimo vse povezave novega grafa K_{2k} z najmanjšimi

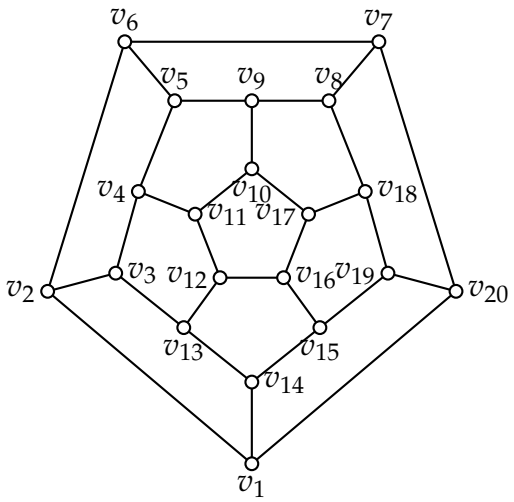
skupnimi utežmi poti med ustreznima vozliščema lihe stopnje. V tem grafu je potrebno nato poiskati minimalno prirejanje (to je k povezav v K_{2k} paroma brez skupnih krajišč) glede na uteži v K_{2k}, za kar obstajajo polinomski algoritmi, a niso tema tega dela, zato podrobnosti izpustimo.

9.3 HAMILTONOVI GRAFI

V tem razdelku bomo razglabljali o lastnosti, ki je nekako komplementarna Eulerjevemu sprehodu, saj povezave nadomestimo z vozlišči. Tako nas zanima, ali obstaja sklenjen sprehod, ki vsebuje vsako vozlišče natanko enkrat. Ta pogoj lahko opišemo drugače. Tak sprehod mora biti vpet podgraf, saj vsebuje vsa vozlišča. Še več, to je tudi cikel, saj je govora o sklenjenem sprehodu. Torej iščemo vpeti podgraf, ki je cikel.

Graf je **Hamiltonov,**[20] če v njem obstaja vpeti cikel, to je cikel na vseh vozliščih. Takemu ciklu rečemo **Hamiltonov cikel**. Podobno kot s pol-Eulerjevimi grafi imamo tudi tukaj analogijo. Tako je graf **pol-Hamiltonov**, če vsebuje vpeto pot, to je pot, ki vsebuje vsa vozlišča. Takšni poti rečemo **Hamiltonova pot**. Seveda vsi grafi niso Hamiltonovi, kot tudi ne pol-Hamiltonovi. Je pa vsak Hamiltonov graf tudi pol-Hamiltonov.

Zgled 9.13 *Graf dodekaeder na sliki 33 je Hamiltonov. Za to si oglejmo Hamiltonov cikel, ki je podan z vozlišči $v_1v_2 \dots v_{20}v_1$. Najdemo ga lahko z nekaj poskušanja, saj je graf dovolj majhen, da nam to lahko uspe.*



Slika 33: Dodekaeder ali mreža pravilnega telesa z dvanajstimi ploskvami.

20 Sir William Rowan Hamilton (1805-1865) je bil angleški matematik. Njegova dela so, paradoksalno, največji pečat pustila v fiziki. S teorijo grafov se sicer ni ukvarjal.

Kljub temu, da se zdijo Hamiltonske lastnosti grafov podobne Eulerjevim lastnostim grafov, le da povezave zamenjajo vozlišča, je iz algoritmičnega stališča problem biti Hamiltonski graf težko preverljiv in spada med NP-polne probleme. To pomeni, da nimamo hitrega algoritma, ki bi nas pripeljal do odgovora, ali je graf (pol-)Hamiltonov ali ne. Tako tudi ne obstaja kakšna lepa karakterizacija Hamiltonskih grafov. V takšnem primeru iščemo tako imenovane potrebne oziroma zadostne pogoje, da je graf Hamiltonov. Tako je potreben pogoj vsaka implikacija oblike:

če je graf Hamiltonov, potem velja potreben pogoj.

Razlog za ime potreben pogoj se skriva v kontrapoziciji in se glasi:

če potreben pogoj ni izpolnjen, potem graf ni Hamiltonov.

Potrebne pogoje običajno uporabljamo, da pokažemo, da graf ni Hamiltonov. Podobno tudi zadostne pogoje predstavimo kot implikacijo:

če je izpolnjen zadosten pogoj, potem je graf Hamiltonov.

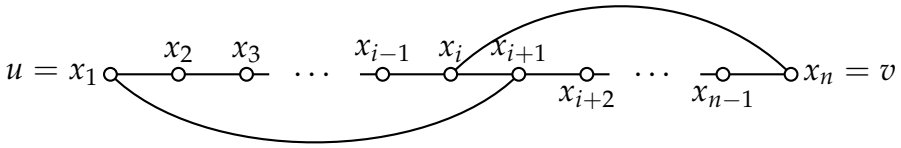
Do konca razdelka si poglejmo dva zadostna pogoja (Dirac-ov[21] in Ore-jev[22] izrek) in en potreben pogoj.

Izrek 9.9 (Dirac) *Naj bo G enostaven graf na n vozliščih. Če velja $\delta(u) \geq \frac{n}{2}$ za poljubno vozlišče u grafa G, potem je graf G Hamiltonov.*

Dokaz. Naj bo G enostaven graf na n vozliščih in naj bo $\delta(u) \geq \frac{n}{2}$ za vsako vozlišče $u \in V(G)$. Predpostavimo, da zaključek ni resničen in da G ni Hamiltonov. Med vsemi takšnimi grafi lahko izberemo tistega z največ povezavami. To pomeni, da če dodamo eno samo povezavo med nesosednji vozlišči u in v grafa G, graf postane Hamiltonov. To po drugi strani pomeni, da je G pol-Hamiltonov, saj obstaja Hamiltonova pot P med vozlišči u in v v G. Naj bo $P = x_1x_2 \dots x_n$, kjer je $x_1 = u$ in $x_n = v$. Definirajmo množici $A = \{j \in [n-1] : u \sim x_{j+1}\}$ in $B = \{j \in [n-1] : v \sim x_j\}$, ki vsebujeta vsaj $\frac{n}{2}$ elementov, saj velja $\delta(u) \geq \frac{n}{2}$ in $\delta(v) \geq \frac{n}{2}$. Po principu golobnjaka (imamo $n-1$ golobjih lukenj, to so elementi v A oziroma v B, in skupaj n golobov iz pogojev $\delta(u) \geq \frac{n}{2}$ in $\delta(v) \geq \frac{n}{2}$) obstaja vsaj en element, ki je v obeh množicah. Naj bo $i \in A \cap B$ in tako velja $u \sim x_{i+1}$ in $v \sim x_i$, glej sliko 34. Cikel $x_1x_2 \dots x_{i-1}x_ix_nx_{n-1}x_{n-2} \dots x_{i+2}x_{i+1}x_1$ je očitno Hamiltonov cikel (pomagamo si lahko s sliko 34), kar je protislovje s predpostavko, da G ni Hamiltonov. Torej je G Hamiltonov in dokaz je zaključen. ∎

21 Gabriel Andrew Dirac (1925-1984) je bil madžarsko-britanski matematik, ki je ta izrek dokazal leta 1952.

22 Oystein Ore (1899-1968) je bil norveški matematik znan po svojem delu v teoriji kolobarjav in teoriji grafov.



Slika 34: Situacija iz dokaza Diracovega izreka.

Izrek 9.10 (Ore) *Naj bo G enostaven graf na n vozliščih. Če velja $\delta(u) + \delta(v) \geq n$ za poljubni nesosednji vozlišči u in v grafa G, potem je graf G Hamiltonov.*

Dokaz. Dokaz je podoben kot dokaz Diracovega izreka, le da sedaj velja pogoj $\delta(u) + \delta(v) \geq n$ za poljubni nesosednji vozlišči u in v grafa G. Predpostavimo, da zaključek ni resničen in da G ni Hamiltonov. Med vsemi takšnimi grafi lahko izberemo tistega z največ povezavami. To pomeni, da če dodamo eno samo povezavo med nesosednji vozlišči u in v grafa G, graf postane Hamiltonov. To po drugi strani pomeni, da je G pol-Hamiltonov, saj obstaja Hamiltonova pot P med vozlišči u in v v G. Naj bo $P = x_1x_2 \dots x_n$, kjer je $x_1 = u$ in $x_n = v$. Spet definirajmo množici $A = \{j \in [n-1] : u \sim x_{j+1}\}$ in $B = \{j \in [n-1] : v \sim x_j\}$. Ker velja $\delta(u) + \delta(v) \geq n$, se vsaj en element pojavi v obeh dveh množicah po principu golobnjaka (imamo $n-1$ golobjih lukenj, to so elementi v A oziroma v B, in n golobov iz pogoja $\delta(u) + \delta(v) \geq n$). Naj bo $i \in A \cap B$ in tako velja $u \sim x_{i+1}$ in $v \sim x_i$, tudi tukaj je uporabna slika 34. Cikel $x_1x_2 \dots x_{i-1}x_ix_nx_{n-1}x_{n-2} \dots x_{i+2}x_{i+1}x_1$ je spet Hamiltonov cikel (slika 34), kar je protislovje s predpostavko, da G ni Hamiltonov. Torej je G Hamiltonov in dokaz je zaključen. ∎

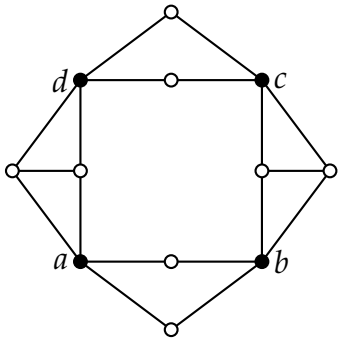
Zgled 9.14 *Izreka 9.9 in 9.10 sta uporabna pri potrjevanju, ali je nek graf Hamiltonov, saj lahko njuna zadostna pogoja hitro preverimo. Žal pa se njunima zadostnima pogojema izmakne marsikateri Hamiltonov graf. Najenostavnejši primer so kar cikli C_n, kjer za $n \geq 5$ zadostna pogoja $\delta(u) \geq \frac{n}{2}$ in $\delta(u) + \delta(v) \geq n$ Diracovega oziroma Orejevega izreka nista izpolnjena. To med drugim pomeni, tudi, da omenjena zadostna pogoja ne predstavljata karakterizacije Hamiltonovih grafov.*

Izrek 9.11 *Naj bo G graf in $A \subseteq V(G)$. Če je graf G Hamiltonov, potem graf $G - A$ vsebuje največ $|A|$ komponent.*

Dokaz. Naj bo G Hamiltonov graf s Hamiltonovim ciklom C in naj bo $A \subseteq V(G)$. Ker je C cikel, ima graf $C - A$ največ $|A|$ komponent, ko poljubni vozlišči iz A nista zaporedni na ciklu C. Graf $G - A$ ima kvečjemu manj komponent kot $C - A$. Torej ima tudi $G - A$ največ $|A|$ komponent. ∎

Zgled 9.15 *Tudi potreben pogoj izreka 9.11 ne karakterizira Hamiltonovih grafov. To lahko uvidimo iz Petersenovega grafa P s slike 29, ki ni Hamiltonov. Kakorkoli bomo izbrali množico $A \subseteq V(P)$, bo imel graf $G - A$ največ $|A|$ komponent. Preveriti zadostuje možnosti, ko vsebuje A tri ali štiri elemente. Za to je potrebno opaziti, da izbris enega ali dveh vozlišč ohranja ostanek Petersenovega grafa povezan. Po drugi strani pa z izbrisom petih ali več vozlišč ostane največ pet vozlišč, kar je vedno manj od števila izbrisanih vozlišč. Sami preverite, da z izbrisom treh ali štirih vozlišč dobimo največ tri oziroma štiri komponente.*

Zgled 9.16 *Izrek 9.11 lahko uporabimo na grafu G na sliki 35, da pokažemo, da G ni Hamiltonov. Če je $A = \{a, b, c, d\}$, potem graf $G - A$ vsebuje 6 komponent. Ker je $6 > 4 = |A|$, potreben pogoj izreka 9.11 ni izpolnjen, kar pomeni, da G ni Hamiltonov.*



Slika 35: Graf, ki ni Hamiltonov.

Na koncu razdelka omenimo še **problem trgovskega potnika**, ki je zelo znamenit problem s stališča časovne zahtevnosti iskanja njegove rešitve, saj nam direkten pristop (pregled vseh možnosti) porodi fakultetno časovno zahtevnost $O(n!)$. Model za ta problem predstavlja n mest, ki jih mora obiskati trgovski potnik, pri čemer je poznana razdalja med poljubnima mestoma. To generira polni graf K_n z uteženimi povezavami, kjer utež predstavlja razdaljo med mesti. Vprašanje je, v kakšnem vrstnem redu naj trgovski potnik obišče ta mesta, da bo opravil najkrajšo razdaljo. (Alternativna razlaga uteži je cena prevoza med poljubnima mestoma.) Kot že omenjeno, je to zelo zahteven optimizacijski problem, s katerim ponovno vidimo razliko med Eulerjevimi in Hamiltonskimi principi. Medtem ko za Kitajski problem poštarja, ki je problem Eulerjevega tipa, obstaja polinomski algoritem, ki poišče rešitev, takšnega algoritma ne poznamo za problem trgovskega potnika, ki je problem Hamiltonovega tipa.

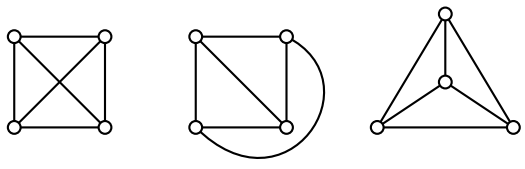
9.4 RAVNINSKI GRAFI

V tem razdelku bomo spregovorili o grafih, ki jih lahko narišemo tako, da se različne povezave med seboj ne sekajo. Kot smo že vajeni, grafe raje rišemo, kot da na njih gledamo kot na dve množici: množico povezav in množico vozlišč. Spoznali smo tudi že, da lahko graf narišemo na več različnih načinov, spomnimo se izomorfnih grafov P in G s slike 29 ali tistih s slik 27 in 26. Nekatere izmed teh risb se nam lahko zdijo lepše od preostalih in pogosto so nam bolj všeč tiste, na katerih se povezave med seboj ne sekajo.

Vsaki sliki grafa rečemo risba grafa. Če so risbe narisane na ravni površini, jih lahko nadalje ločimo na ravninske in neravninske risbe. Risba je **ravninska**, če se različne povezave na njej ne sekajo in **neravninska** sicer. Vsaka ravninska risba nam razdeli ravnino, na kateri je narisana, na več območij, ki jim rečemo **lica**. Eno izmed lic je neomejeno in mu rečemo **zunanje lice**. Ostalim licem pravimo **notranja lica**.

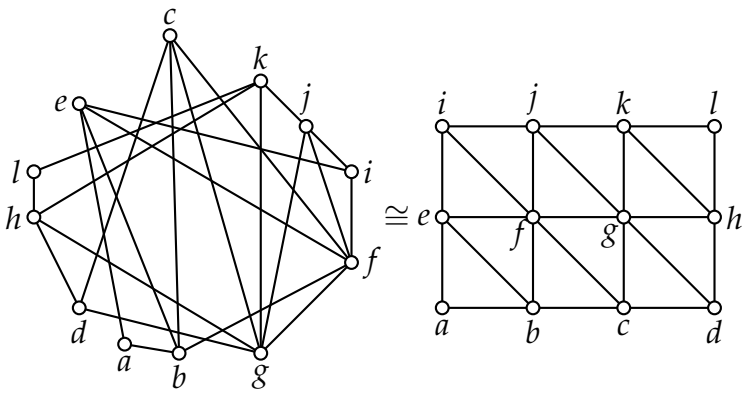
Graf je **ravninski**, če obstaja kakšna njegova ravninska risba. Preostali grafi niso ravninski. To pomeni, da se na vsaki njihovi risbi različne povezave sečejo med seboj (vsaj dve se sečeta med sabo). Že definicija ravninskosti grafa nam implicira, da za graf G pokažemo, da je ravninski tako, da narišemo njegovo ravninsko risbo. Malce bolj težavno je pokazati, da graf ni ravninski, saj ne moremo preveriti vseh risb nekega grafa.

Zgled 9.17 *Na sliki 36 so tri risbe polnega grafa K_4. Leva risba ni ravninska, saj se na njej dve povezavi sečeta. Srednja in desna risba pa sta ravninski, saj se na njih povezave med seboj ne sečejo. Ker obstaja ravninska risba grafa K_4, je ta graf ravninski. Opazimo lahko še, da imata obe ravninski risbi štiri lica. Lica lahko dobimo tako, da list papirja, na katerem je narisana ravninska risba, razrežemo s škarjami po povezavah. Tako dobimo tri majhna lica, ki so notranja in eno veliko, ki je zunanje lice. Opazimo lahko, da imata obe ravninski risbi enako število lic. Število lic se, tako kot vse lastnosti med seboj izomorfnih grafov, ne razlikujejo med različnimi risbami grafa. Omenimo še, da o licih ne moremo govoriti pri neravninskih risbah.*



Slika 36: Dve ravninski in ena neravninska risba grafa K_4.

Zgled 9.18 *Tudi na sliki 37 je neravninska (na levi) in ravninska (na desni) risba grafa. Če bi videli zgolj levo risbo s slike 37, bi najbrž predvidevali, da gre za neravninski graf, saj je risba res neprijazna na pogled. Po drugi strani nas ta primer opozarja, da lahko zelo hitro narišemo očem neprijazno risbo grafa, če se risanja lotimo nenačrtovano. Da sta grafa res izomorfna, lahko preverimo z oznakami vozlišč na risbah.*



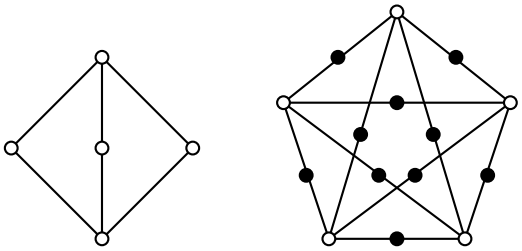
Slika 37: Ravninska in neravninska risba grafa.

Če ravninskost grafa pokažemo z njegovo ravninsko risbo, kako potem preverimo, da graf ni ravninski? Delni odgovor nam poda že naslednja trditev. Njen dokaz matematično ni popolnoma natančen, a ustreza nivoju tega učbenika.

Trditev 9.12 *Grafa K_5 in $K_{3,3}$ nista ravninska grafa.*

Dokaz. Oglejmo si najprej ravninsko risbo grafa K_4 (desna risba s slike 36). Opazimo lahko, da ima K_4 štiri lica. Še več, vsako izmed njegovih lic ne vsebuje enega vozliša in to velja za vse risbe K_4, saj se lastnosti ohranjajo med izomorfnimi grafi. Graf K_5 dobimo iz K_4 tako, da dodamo eno vozlišče in ga povežemo s povezavami z vsemi preostalimi vozlišči. Seveda novo vozlišče u dodamo na eno izmed lic f grafa K_4. Ker eno izmed vozlišč grafa K_4, recimo v, ni na robu lica f, potem nam novo dodana povezava seče eno izmed že obstoječih povezav. Ker to velja za vsako risbo, graf K_5 ni ravninski.

Nadaljujmo z ravninsko risbo $K_{2,3}$ (glej sliko 38). Ravninska risba tega grafa ima tri lica in na vsakem izmed teh treh lic se ne nahajajo vsa tri vozlišča stopnje dva. Ponovno to velja za vsako risbo grafa $K_{2,3}$, saj se vse lastnosti ohranjajo med izomorfnimi grafi. Graf $K_{3,3}$ dobimo iz $K_{2,3}$ tako, da dodamo eno vozlišče, recimo v in ga povežemo s povezavami z vsemi tremi vozlišči stopnje dva. Dodajmo v na poljubno lice f. Ker eno vozlišče stopnje dva, recimo u, ni na robu lica f, bo povezava uv sekala eno izmed preostalih povezav grafa $K_{2,3}$. Ker to velja za vsako risbo, graf $K_{3,3}$ ni ravninski. ∎



Slika 38: Ravninska risba grafa $K_{2,3}$ in 1-subdivizija K_5. Dodana vozlišča subdivizije so označena s črno.

Kot bomo videli v nadaljevanju, je vsak neravninski graf na naraven način povezan z grafoma K_5 ali $K_{3,3}$. Za to potrebujemo še nekaj terminologije. Naj bo G graf in $e = uv$ neka njegova povezava. **Subdivizijo reda** k ali k**-subdivizija** povezave e v grafu G dobimo, če povezavo e v grafu G nadomestimo s potjo $ux_1x_2 \dots x_kv$, kjer so x-i nova vozlišča. Torej subdivizijo reda k dobimo tako, da na povezavo uv dodamo k novih vozlišč. Ob tem je k lahko poljubno naravno število, hkrati pa dopuščamo tudi $k = 0$. Tako se pri subdiviziji reda $k = 0$ v grafu nič ne spremeni. Kadar je $k = 1$, pa dodamo eno vozlišče na izbrano povezavo e.

Bolj splošno je k**-subdivizija grafa** G nov graf, ki ga iz G dobimo tako, da na vsaki povezavi grafa G izvedemo k-subdivizijo. Na desni strani slike 38 je 1-subdivizija grafa K_5. Seveda pa subdivizije vseh povezav niso nujno vedno enakega reda. Tako pravimo, da je graf H **subdivizija grafa** G, če H dobimo iz G s k_e-subdivizijo vsake povezave $e \in E(G)$. Seveda je k_e lahko različen od k_f za različni povezavi e in f. Tukaj pride prav, da dovolimo, da je k lahko enak tudi 0. Saj je k_e-subdivizija, $k_e > 0$, zgolj ene povezave e hkrati že tudi subdivizija grafa G, saj je lahko $k_f = 0$ za vse preostale povezave $f \in E(G)$. Na desni strani slike 38 je 1-subdivizija grafa K_5, medtem ko je na desni strani slike 39 subdivizija grafa $K_{3,3}$, ki je podgraf Petersenovega grafa.

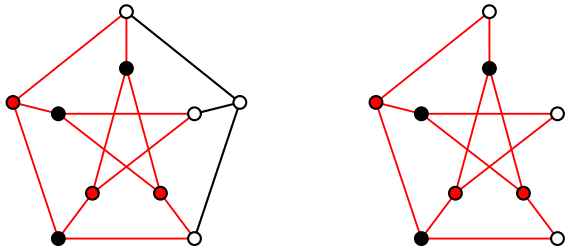
S pomočjo subdivizij grafov K_5 in $K_{3,3}$ lahko opišemo vse neravninske grafe, kot je razvidno iz naslednjega izreka. Le-tega navajamo brez dokaza, saj njegov dokaz bistveno presega nivo tega učbenika.

Izrek 9.13 (Kuratowski) [23] *Graf G je ravninski natanko tedaj, ko ne vsebuje subdivizije grafa K_5 ali grafa $K_{3,3}$.*

Zgled 9.19 *Izrek Kuratovskega se uporablja, da se pokaže, da graf ni ravninski. Tako si oglejmo Petersenov graf na sliki 39. Ker je na tej risbi Petersenov graf povezan s pet ciklom, lahko to koga premami in začne iskati subdivizijo grafa K_5. To je napačen pristop, saj je Petersenov graf 3-regularen in ne more vsebovati subdivizije K_5, za katero*

23 Kazimierz Kuratowski (1896-1980) je bil poljski matematik, znan po svojem delu v topologiji.

potrebujemo vsaj pet vozlišč stopnje štiri. Za subdivizijo $K_{3,3}$ potrebujemo šest vozlišč razporejenih v dve množici s po tremi vozlišči. Na levem delu slike 39 so ta vozlišča označena s črno in z rdečo barvo. Nadalje so vse povezave, potrebne za subdivizijo, tudi označene z rdečo barvo. Sama subdivizija, brez preostalega vozlišča in povezav, je narisana na desni strani slike 39 in vidimo lahko, da je šest povezav direktnih med rdečimi in črnimi vozlišči, medtem ko so preostale tri subdividirane z enim vozliščem.



Slika 39: Subdivizija $K_{3,3}$ na Petersenovem grafu na levi strani in ista subdivizija samostojno na desni strani.

Izrek 9.14 (Eulerjeva formula) *Če povezan ravninski graf G vsebuje n vozlišč, m povezav in f lic, potem velja $n - m + f = 2$.*

Dokaz. Eulerjevo formulo bomo dokazali s pomočjo indukcije na število povezav m. Če je $m = 0$, potem je $n = 1$, saj je G povezan, in $f = 1$. Zato velja $n - m + f = 1 - 0 + 1 = 2$. Naj bo sedaj $m = 1$. Torej je $n_1 = 2$, ko je $G \cong K_2$, ali $n_2 = 1$, ko je G zanka. V prvem primeru je $f_1 = 1$ in v drugem je $f_2 = 2$. Tako je $n_1 + m + f_1 = 2 - 1 + 1 = 2$ in $n_2 + m + f_2 = 1 - 1 + 2 = 2$. S tem je baza indukcije zaključena.

Naj bo sedaj $m > 1$. Opazimo lahko, da je vsaka povezava največ na dveh licih. Izberimo poljubno povezavo e in si oglejmo graf $G' = G - e$. Če je povezava e na dveh licih, potem imamo $n' = n$, $m' = m - 1$ in $f' = f - 1$. Torej se število povezav in število lic grafa G' zmanjšata za ena glede na graf G. Po indukcijski predpostavki Eulerjeva formula velja za graf G'. Računajmo

$$2 = n' - m' + f' = n - m + 1 + f - 1 = n - m + f$$

in Eulerjeva formula velja tudi za graf G.

Preostane nam še primer, ko povezava e leži na le enem licu (recimo most). V tem primeru graf G' ni več povezan in bodita C_1 in C_2 njegovi komponenti. Naj komponenta C_1 vsebuje n_1 vozlišč, m_1 povezav in f_1 lic. Prav tako naj komponenta C_2 vsebuje n_2 vozlišč, m_2 povezav in f_2 lic. Veljajo zveze $n = n_1 + n_2$, $m = m_1 + m_2 - 1$ in $f = f_1 + f_2 - 1$, saj se eno lice komponente C_1 pokriva z enim licem komponente C_2. Vsaka izmed komponent ima manj povezav kot graf G,

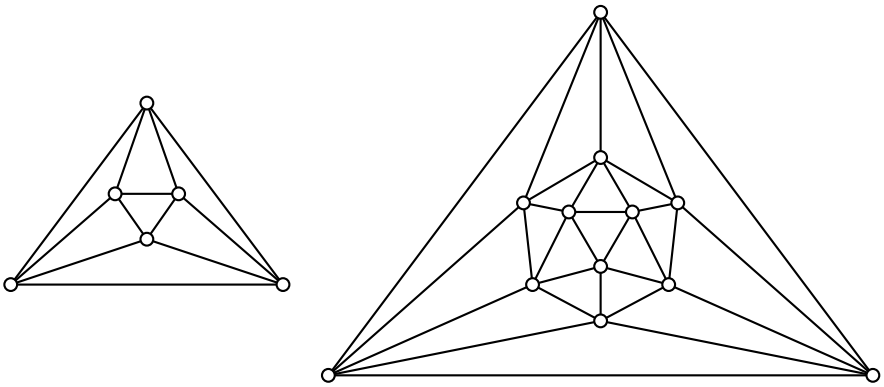
zato lahko uporabimo indukcijsko predpostavko za vsako komponento posebej in dobimo $2 = n_1 - m_1 + f_1$ in $2 = n_2 - m_2 + f_2$. Ko seštejemo obe enakosti, dobimo

$$4 = n_1 - m_1 + f_1 + n_2 - m_2 + f_2 = (n_1 + n_2) - (m_1 + m_2) + (f_1 + f_2) =$$

$$= n - m + 1 + f + 1,$$

iz česar takoj sledi Eulerjeva formula $n - m + f = 2$ za graf G in dokaz je zaključen. ■

Zgled 9.20 *S pomočjo Eulerjeve formule lahko dokažemo, da obstaja le pet Platonskih*[24] *teles, ki so tetraeder (glej desni graf na sliki 36), kocka (glej levi graf na sliki 27), oktaeder (glej levi graf na sliki 40), dodekaeder (glej graf na sliki 33) in ikozaeder (glej desni graf na sliki 40). To so edina telesa, ki imajo za ploskve skladne like (enakostranične trikotnike pri tetraedru, oktaedru in ikozaedru, kvadrate pri kocki in pravilne petkotnike pri dodekaedru), enako število robov v vseh ogljiščih (stopnja vozlišč na ustreznih grafih) in enake kote.*



Slika 40: Mreži Platonskih teles oktaedera z 8. ploskvami in ikozaedra z 20. ploskvami.

Zanimiv podrazdred ravninskih grafov so tisti, ki imajo ob danem številu vozlišč največje število povezav. Takšnim grafom rečemo **triangulirani ravninski grafi** ali kar **triangulacije**, saj vsako njihovo lice obkrožajo tri povezave, torej tricikel. Do triangulacije ravninskega grafa pridemo na enostaven način, saj podanemu ravninskemu grafu na kaki njegovi ravninski risbi tako dolgo dodajamo povezave, ki so diagonale na licih obkroženih s k-ciklom, $k > 3$, dokler vsa lica ne obkrožajo tricikli (vključno z zunanjim licem).

24 Platon (približno 425-347 pred našim štetjem) je bil antični grški filozof, ki je ustanovil platonsko šolo misli.

Trditev 9.15 *V vsaki triangulaciji ravninskega grafa G z m povezavami in f lici velja $3f = 2m$.*

Dokaz. V triangulaciji ravninskega grafa G vsako lice obkrožajo tri povezave. Po drugi strani je vsaka povezava v dveh licih. Zato velja $3f = 2m$. ∎

Zgled 9.21 *Na povezanem ravninskem grafu s petimi vozlišči po Eulerjevi formuli velja $m - f = n - 2 = 3$. Tako je lahko $m \in \{4, 5, 6, 7, 8, 9\}$, ob tem pa imamo število lic točno določeno s $f = m - n + 2 = m - 3$. Omenimo še, da ne obstaja več povezav, saj sicer ne velja $3f = 2m$. To je hkrati tudi dokaz, da K_5 ni ravninski graf, saj K_5 vsebuje 10 povezav.*

Končajmo razdelek z vprašanjem, kako je z algoritmično kompleksnostjo prepoznavanja ravninskih grafov? Ali so enostavni kot prepoznavanje Eulerjevih grafov, ali težki kot prepoznavanje Hamiltonovih grafov, ali pa še ne vemo, kot pri izomorfizmih grafov (kar pomeni, da je zaenkrat še težko)? Obstaja celo linearni algoritem za prepoznavanje ravninskih grafov, ki pa je tako kompliciran, da ga še ni nihče implementiral v praksi. Tako se običajno uporabljajo algoritmi s časovno zahtevnostjo $O(m \lg n)$, kjer je m število povezav in n število vozlišč grafa G, ki so dovolj enostavni in tudi zelo hitri.

9.5 DREVESA

V tem razdelku si bomo podrobneje ogledali grafe, ki ne vsebujejo ciklov. Grafu brez cikla rečemo **gozd**. Pogosto pa nas zanimajo povezani grafi in povezanemu grafu brez ciklov rečemo **drevo**. Seveda gozd sestavlja več komponent, ki so vse brez cikla in tako dobimo analogijo z realnim življenjem, da gozd sestavlja več dreves. Družine dreves, ki smo jih do sedaj spoznali, so poti P_n in zvezde $K_{1,n}$, od gozdov pa smo spoznali le prazne grafe N_n. Drevesa so pomembna v računalništvu, saj do podatkov, ki so shranjeni v obliki (razvejanega) drevesa, hitreje dostopamo, kot sicer.

Za poglaviten rezultat tega razdelka potrebujemo še naslednjo trditev, ki je zanimiva tudi sama zase.

Trditev 9.16 *Vsako drevo T na $n \geq 2$ vozliščih ima vsaj dva lista.*

Dokaz. Pokažimo to trditev z indukcijo na $m = |E(T)|$. Če je $m = 1$, potem je $T \cong P_2$ in obe vozlišči sta lista. Naj bo sedaj $m > 1$. Izberimo poljubno povezavo $e = ab$ in jo izbrišimo. Graf $T - e$ razpade na dve drevesi T_1 in T_2, saj je vsaka povezava drevesa most (sicer bi imeli cikel). Obe, T_1 in T_2 imata manj kot m povezav. Zato lahko uporabimo indukcijsko predpostavko, če le imata obe drevesi vsaj dve vozlišči. Tako ima T_1 dva lista u in v ter T_2 dva lista x in y. Tudi če je e povezava med listoma T_1 in T_2, recimo $a = u$ in $b = x$, v drevesu T ostaneta vsaj dva lista v in y.

Druga možnost je, da je eno izmed dreves, recimo T_1, kar eno samo vozlišče x. Opazimo, da ima potem T_2 vsaj dve vozlišči, saj je $m > 1$. Zato ima T_2 po indukcijski predpostavki vsaj dva lista, recimo u in v. Po drugi strani je x list v T. Tudi če je x sosed od enega izmed u in v v T, recimo u, sta potemtakem x in v lista v T in dokaz je končan. ∎

Izrek 9.17 *Če je T graf na n vozliščih, potem so naslednje trditve ekvivalentne.*

(I) *T je drevo.*

(II) *T je povezan in vsebuje $n-1$ povezav.*

(III) *T je brez ciklov in vsebuje $n-1$ povezav.*

(IV) *T lahko dobimo iz K_1 v $n-1$ korakih tako, da na vsakem koraku dodamo eno vozlišče in ga povežemo s povezavo z enim že obstoječim vozliščem.*

(V) *Med poljubnima vozliščema je natanko ena pot.*

Dokaz. Pokažimo naslednje implikacije $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (v) \Rightarrow (i)$, ki nam s pomočjo hipotetičnega silogizma (HS) zagotovijo vse potrebne ekvivalence.

$(i) \Rightarrow (ii)$ Ker je T drevo, je T tudi povezan graf. Z indukcijo na $m = |E(T)|$ pokažimo, da T vsebuje $n-1$ povezav. Če je $m = 0$, potem je $T \cong K_1$ in graf ima $m = 0 = 1-1 = n-1$ povezav. Naj bo sedaj $m > 0$. Izberimo eno povezavo in jo izbrišimo. Tako T razpade na dve drevesi T_1 in T_2, ki imata manj povezav m_1 oziroma m_2 kot m. Tako lahko uporabimo indukcijsko predpostavko in velja $m_1 = n_1 - 1$ za T_1 in $m_2 = n_2 - 1$, kjer sta n_1 in n_2 števili vozlišč dreves T_1 oziroma T_2. Seveda velja $n = n_1 + n_2$, kar uporabimo v računu $m = m_1 + m_2 + 1 = n_1 - 1 + n_2 - 1 + 1 = n - 1$ in ta implikacija je zaključena.

$(ii) \Rightarrow (iii)$ Seveda T vsebuje $n-1$ povezav, kar je pogoj v obeh točkah. Predpostavimo nasprotno, da T vsebuje tudi kak cikel. Iz T brišemo posamezne povezave v ciklih tako dolgo, da ostanemo s povezanim grafom T^-, ki ne vsebuje ciklov. Seveda ima T^- manj kot $n-1$ povezav, saj smo nekatere izbrisali iz T. Toda T^- je drevo. Ker smo že dokazali implikacijo $(i) \Rightarrow (ii)$, to pomeni, da je T^- povezan in vsebuje $n-1$ povezav, kar je protislovje. Zato je T brez ciklov.

$(iii) \Rightarrow (iv)$ Ker je T brez ciklov in vsebuje $n-1$ povezav, je vsaka njegova komponenta z vsaj eno povezavo drevo. V drevesu po trditvi 9.16 obstaja list. Odstranimo ga. Postopek lahko ponovimo $(n-1)$-krat. Ker smo v vsakem koraku odstranili eno vozlišče, smo na koncu ostali z enim vozliščem. Iskana procedura točke (iv) je obratni postopek.

$(iv) \Rightarrow (v)$ Pokažimo resničnost trditve (v) z induktivno posplošitvijo, saj je v točki (iv) pravzaprav definiran induktivni razred. V bazi imamo le eno vozlišče v in obstaja le ena pot med v in v, ki je kar $P_1 = v$. Recimo, da je po k korakih natanko ena pot med vsakim parom vozlišč. Pokažimo, da nam pravilo dodajanja vozlišča x, ki je sosednje nekemu vozlišču u, ohrani enoličnost poti med poljubnima vozliščema. To je jasno, če sta vozlišči različni od x, saj ne obstaja pot preko x, ki je list. Med x in poljubnim vozliščem z tudi obstaja natanko ena pot in sicer od x do u in nato enolično določena pot od u do z.

$(v) \Rightarrow (i)$ Ker je med poljubnima vozliščema natanko ena pot, v grafu T ni cikla. Seveda je T tudi povezan, saj obstaja pot med poljubnima vozliščema. Torej je T drevo. ■

Kot omenjeno v dokazu izreka, imamo v točki (iv) izreka 9.17 induktivno definicijo dreves. Vse preostale alineje izreka 9.17 pa tvorijo enak konceptualni razred z različnimi opisi.

Izrek 9.17 nam tudi omogoči razmislek o številu povezav v gozdu.

Posledica 9.18 *Če je F gozd s k drevesi in n vozlišči, potem F vsebuje $n - k$ povezav.*

Dokaz. Za vsako drevo T_i, $i \in [k]$, po izreku 9.17 velja $m_i = n_i - 1$, kjer sta m_i in n_i števili vozlišč in povezav drevesa T_i. Če seštejemo po vseh $i \in [k]$, potem dobimo

$$m = m_1 + m_2 + \cdots + m_k = n_1 - 1 + n_2 - 1 + \cdots + n_k - 1 = n - k.$$

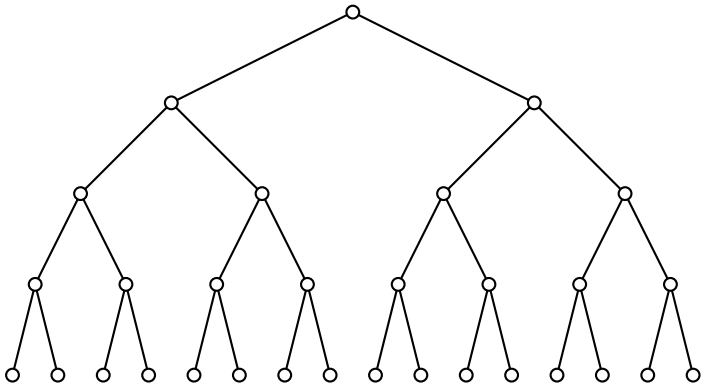
■

Pogosto v drevesu določimo eno posebno vozlišče, ki mu rečemo **koren drevesa**. Za koren lahko izberemo katerokoli vozlišče, a ko je enkrat izbrano, ima poseben status. Običajno koren na risbi narišemo na vrh risbe, vsi njegovi sosedje nato sledijo v naslednjem nivoju. Njihovi sosedje, ki še niso bili narisani, nato sledijo v naslednjem nivoju in tako naprej. Opis nas spomni na definicijo Hassejevih diagramov, le da smo tam risali le-te od spodaj navzgor.

Če ima drevo koren r, potem za vozlišče u iz tega drevesa obstaja natanko en sosed v, za katerega je $d(u,r) = d(v,r) + 1$. Potem rečemo, da je vozlišče v **starš** vozlišča u in je u **otrok** vozlišča v. Seveda ima vsako vozlišče natanko enega starša (če le ni koren r), lahko pa ima več otrok. Edina vozlišča brez otrok so listi (razen če je list koren drevesa). Vsa vozlišča w, za katera velja $d(w,r) > d(u,r)$ in najkrajša pot med w in r vsebuje vozlišče u, so **potomci** vozlišča u. Glede na koren tudi ločimo med sosedi drevesa. Tako je starš **zgornji sosed** in otrok je **spodnji sosed**. Včasih je koristno ločiti tudi med **povezavo navzgor**, ki pripelje do starša in med **povezavo navzdol**, ki pripelje do otroka.

Zgled 9.22 *Na sliki 41 imamo binarno drevo s korenom. Koren je seveda najvišje vozlišče. Binarno ga imenujemo zato, ker ima vsako vozlišče navzdol natanko dva soseda (do nekega nivoja, kjer se ustavimo). Binarna drevesa se pogosto pojavljajo v računalništvu. Zelo znan primer najdemo v algoritmu 'deli in vladaj' za sortiranje. Pogosto je posledica binarnega drevesa faktor* $\lg n$ *v časovni zahtevnosti problema, ki ga rešujemo.*

Poseben primer uporabe binarnih dreves je v športu, ko gre za turnirski način tekmovanja. Binarnemu drevesu s slike 41 lahko tako priredimo pare osmine finala kakšnega tekmovanja na izločanje. V Sloveniji je trenutno med bolj aktualnimi končnica lige NBA, lahko pa tudi zapišemo moštva v končnici lige prvakov ali posameznike na teniškem turnirju.



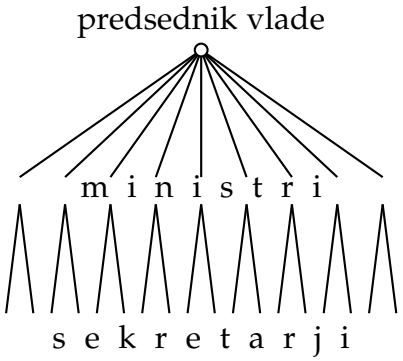
Slika 41: Binarno drevo do četrtega nivoja.

Zgled 9.23 *Na sliki 42 je shematičen prikaz organizacije izvršne oblasti v Republiki Sloveniji. Prvo mesto seveda zaseda predsednik vlade (moški spol je uporabljen za oba spola), ki je koren tega drevesa. V naslednjem nivoju so ministri. Za ministri so na vrsti sekretarji na ministrstvih. Seveda se diagram še nadaljuje. Tako je v izbrani terminologiji predsednik vlade starš ministrov in ti so njegovi otroci. Vsak minister je nadalje starš nekaj sekretarjem in tako naprej.*

V podanem grafu G pogosto iščemo njegovo vpeto drevo T. To seveda pomeni, da je $V(T) = V(G)$. S pomočjo vpetih dreves lahko podamo karakterizacijo povezanih grafov.

Izrek 9.19 *Graf G ima vpeto drevo natanko tedaj, ko je G povezan.*

Dokaz. Če ima G vpeto drevo T, potem je povezan, saj je že drevo T povezano. Če je G povezan in vsebuje $n-1$ povezav, potem je po (ii) izreka 9.17 drevo, ki je kar samo sebi vpeto drevo. Če ima povezan graf G več kot $n-1$ povezav, potem po vrsti odstranjamo povezave, ki se nahajajo v kakšnem ciklu. Ko ni več ciklov, potem ostane drevo, ki je vpeto. ∎



Slika 42: Hierarhična struktura izvršne oblasti.

Problem vpetih dreves je zanimiv tudi med uteženimi grafi (utežene so povezave). V tem primeru iščemo minimalno vpeto drevo, kjer minimalnost pomeni najmanjšo možno skupno utež na vseh povezavah vpetega drevesa. Dva algoritma, ki rešita ta problem, bomo spoznali kasneje.

9.6 NEKATERE POMEMBNEJŠE INVARIANTE

Invarianta na grafu je vsaka lastnost grafa, ki se izraža kot številčna vrednost in je enaka za vse izomorfne grafe. Biti Eulerjev, Hamiltonski ali ravninski graf ni številčna vrednost, zato te lastnosti niso invariante. V tem razdelku bomo spoznali nekatere pomembne grafovske invariante kot so kromatično, dominantno in neodvisno število grafa.

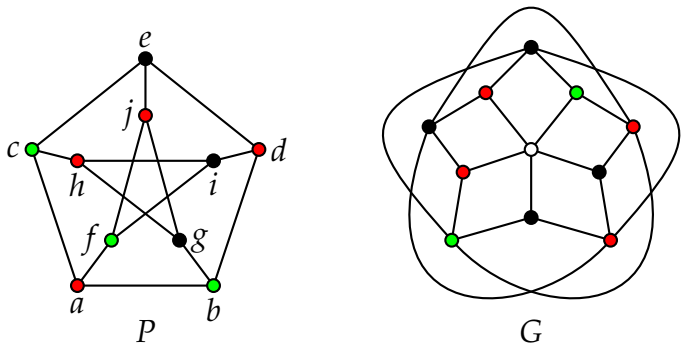
Naj bo G graf in $A \subseteq V(G)$. Množici A rečemo **neodvisna množica vozlišč**, če med vozlišči iz A ni nobene povezave v grafu G. To pomeni tudi, da je podgraf induciran z vozlišči iz A, izomorfen praznemu grafu $N_{|A|}$. **Neodvisno število** grafa G je velikost največje neodvisne množice vozlišč grafa G in ga označimo z $\alpha(G)$.

Določanje neodvisnega števila sodi med algoritmično težke NP-polne probleme. Na manjših grafih se ga lotimo tako, da poiščemo čim večjo neodvisno množico. Njena moč je potem spodnja meja za neodvisno število. Nato poskusimo preko lastnosti grafa pokazati, da ne gre bolje, oziroma da ni večje neodvisne množice. Če nam to uspe, potem smo neodvisno število natančno določili.

Zgled 9.24 *Med znanimi družinami velja $\alpha(N_n) = n$, saj prazen graf sploh ne vsebuje povezav in je $V(N_n)$ njegova neodvisna množica. Lahko je videti tudi, da je $\alpha(K_n) = 1$, saj med poljubnima različnima vozliščema obstaja povezava in lahko neodvisna množica vsebuje le eno vozlišče. Pri povezanem dvodelnem grafu G, kjer je razbitje določeno z V_1 in V_2, sta ti dve množici po definiciji neodvisni. Tako je $\alpha(G) \geq \max\{|V_1|, |V_2|\}$. Pogosto velja tudi enakost in tako dobimo naslednja neodvisna števila znanih dvodelnih*

grafov $\alpha(P_n) = \lceil \frac{n}{2} \rceil$, $\alpha(C_{2n}) = n$, $\alpha(Q_r) = \frac{|V(Q_r)|}{2} = 2^{r-1}$ *in* $\alpha(K_{s,t}) = \max\{s,t\}$. *Največja neodvisna množica dvodelnega grafa lahko vsebuje tudi nekaj vozlišč iz* V_1 *in nekaj iz* V_2. *Naj bo* G *graf, dobljen iz* $K_{1,s}$ *in* $K_{1,t}$ *tako, da med univerzalni vozlišči grafov* $K_{1,s}$ *in* $K_{1,t}$ *dodamo povezavo. Ni težko videti, da* $s+t$ *listov dvodelnega grafa* G *tvori neodvisno množico, ki je maksimalna, če sta le* $s,t > 1$. *Ob tem je* s *listov v drugi množici particije kot* t *listov.*

Zgled 9.25 *Oglejmo si še Petersenov graf* P *in Grötzschev*[25] *graf* G *s slike 43. Zunanja vozlišča* P *tvorijo* C_5, *ki lahko vsebuje največ dve vozlišči v neodvisni množici. Podobno tudi notranja vozlišča grafa* P *tvorijo* C_5 *in lahko tudi med njimi izberemo največ dve vozlišči v neodvisno množico. Zato je* $\alpha(P) \leq 4$. *Ker zlahka najdemo neodvisno množico moči štiri na* P *(na sliki 43 so to, recimo, rdeča vozlišča), velja* $\alpha(P) = 4$. *Zaključimo z Grötzschevim grafom* G *s slike 43. Če je v neodvisni množici centralno vozlišče (bele barve na sliki 43), potem v njej ni ni njegovih sosed. Preostala vozlišča inducirajo* C_5 *in lahko dodamo največ dve. Skupaj torej tri vozlišča. To zlahka presežemo, če v neodvisno množico postavimo vseh pet sosed centralnega vozlišča. Tudi če je v neodvisni množici kakšno vozlišče zunanjega pet-cikla, dobimo kvečjemu manj vozlišč v neodvisni množici (zakaj?). Tako je* $\alpha(G) = 5$.



Slika 43: Petersenov graf P in Grötzschev graf G ter njuni optimalni barvanji.

Naj bo G graf in $B \subseteq V(G)$. Množici B rečemo **vozliščno pokritje** grafa G, če je v B vsaj eno krajišče vsake povezave grafa G. **Število vozliščnega pokritja** grafa G je velikost najmanjše množice vozliščnega pokritja grafa G. To število označimo z $\beta(G)$. Pokažimo, da sta $\alpha(G)$ in $\beta(G)$ zelo povezana v poljubnem grafu G.

25 Camillo Herbert Grötzsch (1902-1993) je bil nemški matematik, ki se je ukvarjal s teorijo grafov.

Izrek 9.20 (Gallaijeva formula) [26] *Za poljuben graf G na n vozliščih velja*

$$\alpha(G) + \beta(G) = n.$$

Dokaz. Pokažimo, da je množica $A \subseteq V(G)$ neodvisna natanko tedaj, ko je $B = V(G) - A$ vozliščno pokritje (s kontrapozicijo). Če A ni neodvisna, potem obstaja povezava $e = uv$ med njenima vozliščema $u, v \in A$. Potem povezava e nima krajišča v B in B ni vozliščno pokritje. Obratno, če B ni vozliščno pokritje, obstaja povezava $f = xy$, ki nima krajišča v B. Potem sta oba x in y v A in A ni neodvisna, saj vsebuje povezavo f.

Naj bo sedaj A neodvisna množica moči $\alpha(G)$. Potem je $B = V(G) - A$ vozliščno pokritje. Če obstaja kakšno vozliščno pokritje B' manjše moči, potem je $A' = V(G) - B'$ neodvisna množica moči več kot $\alpha(G)$. To seveda ni mogoče, zato je $\beta(G) = |B|$ in velja $\alpha(G) + \beta(G) = n$. ∎

Zgled 9.26 *Z zvezo pokazano v izreku 9.20 vemo, glede na zgled 9.24, da velja* $\beta(N_n) = 0$, $\beta(K_n) = n - 1$, $\beta(P_n) = \lfloor \frac{n}{2} \rfloor$, $\beta(C_{2n}) = n$, $\beta(Q_r) = \frac{|V(Q_r)|}{2} = 2^{r-1}$ *in* $\beta(K_{s,t}) = \min\{s, t\}$ *in* $\beta(P) = 6$.

Ker spada določanje $\alpha(G)$ med algoritmično težke probleme, mora biti tak tudi problem določanja$\beta(G)$, saj bi v nasprotnem tudi $\alpha(G)$ lahko določili s pomočjo povezave iz izreka 9.20.

Če je smiselno iskati velikost največjega praznega podgrafa grafa G, lahko to storimo tudi za največji polni podgraf grafa G. (Spomnimo se da je Hamiltonov cikel največji cikel v grafu, če le obstaja, in tudi Hamiltonova pot je največja pot v grafu, če le obstaja.) Naj bo $Q \subseteq V(G)$. Množica Q je **klika** grafa G, če sta poljubni vozlišči iz Q sosedi v G. Z drugimi besedami, vozlišča iz Q inducirajo polni podgraf grafa G. Velikosti največje klike grafa G rečemo **klično število** grafa G in ga označimo z $\omega(G)$.

Zgled 9.27 *Seveda velja* $\omega(N_n) = 1$ *in* $\omega(K_n) = n$. *Za dvodelni graf G imamo* $\omega(G) = 2$, *saj dvodelni grafi ne vsebujejo lihih ciklov po izreku 9.3, s tem pa tudi ne triciklov, ki so nujno potrebni za večje klike. Za cikle je* $\omega(C_n) = 2$, *če je le* $n \neq 3$.

Tudi klično število grafa je v sorodu z neodvisnim številom grafa, le da moramo za to spoznati komplement grafa. Komplement grafa G je graf $\overline{G}$, za katerega velja $V(\overline{G}) = V(G)$, medtem ko sta vozlišči sosednji v $\overline{G}$ natanko tedaj, ko nista sosedi v G. Tako dobimo komplement $\overline{G}$ iz grafa G tako, da izbrišemo vse povezave grafa G in narišemo vse možne povezave, ki jih v G ni bilo. Sedaj ni težko videti, da velja zveza

$$\omega(G) = \alpha(\overline{G}),$$

26 Tibor Gallai (1912-1992) je bil madžarski matematik, ki je raziskovalno deloval v teoriji grafov.

saj je neodvisna množica iz G klika v $\overline{G}$ in obratno. Zaradi te zveze vidimo, da je tudi iskanje kličnega števila algoritmično težek problem, saj bi v nasprotnem tudi neodvisno število lahko poiskali.

Naj bo G graf. Preslikavi $c : V(G) \to \{1, 2, \ldots, k\}$ rečemo k-**barvanje vozlišč**, elementom množice $\{1, 2, \ldots, k\}$ pa **barve**. Če za k-barvanje vozlišč velja $c(u) \neq c(v)$ za vsako povezavo $uv \in E(G)$, potem je c **pravilno** k-**barvanje**. Z drugimi besedami, c je pravilno barvanje, če imata krajišči vsake povezave različni barvi. Kot zelo težek problem se izkaže iskanje najmanjšega števila k, za katero obstaja pravilno k-barvanje. Takemu številu rečemo **kromatično število** grafa G in ga označimo s $\chi(G)$.

Na pravilno barvanje lahko pogledamo tudi s stališča množice $V(G)$. Vsako vozlišče dobi svojo barvo. S tem je $V(G)$ razdeljena na k podmnožic, v katerih so vozlišča iste barve. Tem podmnožicam pravimo **barvni razredi**. Seveda ima vsako vozlišče natanko eno barvo, zato barvni razredi tvorijo razbitje $V_1, V_2, \ldots, V_k$ množice $V(G)$. (Spomnimo se, da je v ozadju vsakega razbitja tudi ekvivalenčna relacija, ki pa je v tem primeru žal ne poznamo.) Zaradi pravilnega barvanja vozlišča iz istega barvnega razreda niso krajišča povezav. Torej tvorijo barvni razredi neodvisne množice grafa G. Tako je kromatično število najmanjše število k, da lahko vozlišča grafa razdelimo na k neodvisnih množic. To nas tudi pripelje do prvega rezultata.

Posledica 9.21 *Za graf G je $\chi(G) = 1$ natanko tedaj, ko je $G \cong N_n$.*

Tako postane kromatično število zanimivo šele, ko graf vsebuje povezave. Z nekaj več dela lahko opišemo tudi grafe, ki vsebujejo natanko dva barvna razreda (ob barvanju z najmanjšim številom barv).

Izrek 9.22 *Za graf G je $\chi(G) = 2$ natanko tedaj, ko je G dvodelen graf z vsaj eno povezavo.*

Dokaz. Če je G dvodelen, potem po njegovi definiciji obstaja razbitje $V(G) = V_1 \cup V_2$, kjer sta V_1 in V_2 neodvisni množici. Torej je $\chi(G) \leq 2$. Ker G vsebuje vsaj eno povezavo, velja tudi $\chi(G) \geq 2$ in dobimo željen enačaj $\chi(G) = 2$. Obratno naj velja $\chi(G) = 2$ in naj bosta V_1 in V_2 pripadajoča barvna razreda. Med vozlišči v V_1 ni povezav, saj je V_1 neodvisna množica. Enako tudi med vozlišči iz V_2 ni povezav. Tako tvorita V_1 in V_2 particijo grafa G, ki je zato dvodelen. Seveda vsebuje tudi vsaj eno povezavo zaradi posledice 9.21. ∎

Spomnimo se izreka 9.3, kjer smo dvodelne grafe opisali z ne obstojem lihih ciklov. Torej velja sledeče.

Posledica 9.23 *Za graf G je $\chi(G) = 2$ natanko tedaj, ko v grafu G ne obstaja lihi cikel in G vsebuje vsaj eno povezavo.*

Zanimiva je tudi kontrapozicija te posledice, ki se glasi.

Posledica 9.24 *V grafu G je $\chi(G) \geq 3$ natanko tedaj, ko v G obstaja lihi cikel.*

Tudi določanje kromatičnega števila je algoritmično težek problem. Za posamezen graf se ga lotimo tako, da poiščemo barvanje s čim manj barvami (to je zgornja meja za $\chi(G)$). Nato poskusimo z lastnostmi grafa utemeljiti, zakaj ga ne moremo pobarvati z manj barvami (to je spodnja meja za $\chi(G)$, ki je običajno težja). Pri tem nam pomaga naslednja spodnja meja.

Izrek 9.25 *Za graf G je $\chi(G) \geq \omega(G)$.*

Dokaz. Naj bo Q največja klika grafa G (z $\omega(G)$ elementi). Ko barvamo G, dobijo vsa vozlišča iz Q različno barvo, saj so si med seboj sosednja. Zato velja $\chi(G) \geq \omega(G)$. ∎

Spodnjo mejo za $\chi(G)$ lahko dobimo tudi s pomočjo neodvisnega števila, saj je v poljubnem barvnem razredu največ $\alpha(G)$ elementov. Tako je idealno, če imamo v vseh barvnih razredih $\alpha(G)$ elementov, kar se ne zgodi pogosto. Velja pa naslednja spodnja meja.

Izrek 9.26 *Za graf G je $\chi(G) \geq \frac{|V(G)|}{\alpha(G)}$.*

Zgled 9.28 *Za Petersenov graf P s slike 29 zlahka vidimo, da je $\omega(P) = 2$, saj ne vsebuje nobenega tricikla. Tako velja $\omega(P) \geq 2$ po izreku 9.25. Po drugi strani smo v zgledu 9.25 videli, da je $\alpha(P) = 4$. Tako dobimo $\chi(P) \geq \frac{|V(P)|}{\alpha(P)} = \frac{10}{4} = 2,5$ po izreku 9.26. Ker je kromatično število vedno naravno število, tako velja $\chi(P) \geq 3$. Po drugi strani imamo barvanje grafa P s tremi barvami na sliki 43 in velja $\chi(P) = 3$.*

Zgled 9.29 *Oglejmo si še Grötzschev graf G s slike 43. Tudi ta graf ima $\omega(G) = 2$, saj ne vsebuje triciklov, in velja $\chi(G) \geq 2$ po izreku 9.25. Hkrati je $\alpha(G) = 5$, kot smo videli v zgledu 9.25, zato je $\chi(G) \geq \frac{|V(G)|}{\alpha(G)} = \frac{11}{5} = 2,2$ po izreku 9.26. Tako je $\chi(G) \geq 3$. Po drugi strani je na sliki 43 barvanje grafa G s štirimi barvami in zato velja $\chi(G) \leq 4$. Torej moramo ali poiskati barvanje s tremi barvami, ali pokazati, da to ni mogoče. Izvedimo slednje. Predpostavimo, da lahko G pobarvamo s tremi barvami. Zunanja vozlišča G tvorijo C_5, zato zanje potrebujemo vsaj tri barve 1, 2 in 3. Ne glede na to, kako jih razporedimo, imajo vozlišča iz notranjega kroga po dva soseda in med njihovimi sosedi na zunanjem krogu se nahajajo vse tri kombinacije 1 in 2 (zato imamo v notranjem krogu barvo 3), 2 in 3 (zato imamo v notranjem krogu barvo 1) ter 1 in 3 (zato imamo v notranjem krogu barvo 2). Tako ima vozlišče v centru risbe med sosedi vse tri barve, ne glede na to, kako jih razporejamo, in tega vozlišča ne moremo pobarvati z barvami 1, 2 ali 3. Torej rabimo četrto barvo in velja $\chi(G) = 4$.*

Zaključimo ta razdelek s še dvema sorodnima invariantama na grafih. Množici $D \subseteq V(G)$ rečemo **dominanta množica** grafa G, če ima vsako vozlišče iz $V(G) - D$ soseda v D. Torej mora imeti vsako vozlišče izven D soseda v D. **Dominantno število** grafa G je najmanjše število elementov v dominantni množici. Označimo ga z $\gamma(G)$. Ni težko opaziti, da je vsaka neodvisna množica A z $\alpha(G)$ elementi tudi dominantna množica. Če to ne bi bilo res, bi obstajalo vozlišče u v množici $V(G) - A$, ki nima soseda v A. Potem pa je $A \cup \{u\}$ neodvisna množica z več elementi kot je $\alpha(G)$. Ker taka neodvisna množica ne obstaja, smo dobili protislovje in A je tudi dominantna množica. Tako velja naslednji izrek.

Izrek 9.27 *Za graf G je $\gamma(G) \leq \alpha(G)$.*

Na dominantno množico lahko pogledamo kot na nadzornike celotnega grafa. Ker pa živimo v svetu, ki ni idealen, se lahko vprašamo kdo bo nadzoroval nadzornike? Eno rešitev ponuja **celotno dominantno število** grafa G, ki ga označimo z $\gamma_t(G)$. To je najmanjša moč množice $S \subseteq V(G)$, za katero velja, da ima vsako vozlišče iz G soseda v S. Taki množici rečemo **celotno dominantna množica**. To pomeni, da morajo imeti soseda v S tudi vozlišča iz S. S tem nadzorniki nadzorujejo tudi nadzornike. Opazimo lahko, da celotno dominantna množica ne obstaja, če graf vsebuje vozlišče stopnje 0, saj le-ta preprosto nima soseda, ki bi ga lahko nadziral. Ker s celotno dominantno množico S nadziramo tudi vse elemente izven S, je S tudi dominantna množica. Tako velja naslednja zveza.

Izrek 9.28 *Za graf G brez izoliranih vozlišč je $\gamma(G) \leq \gamma_t(G)$.*

Tudi dominantno število in celotno dominantno število grafa sodita med algoritmično težke probleme.

Na dominacijo in celotno dominacijo lahko pogledamo tudi s stališča zaprtih in odprtih okolic. Naj bo D dominantna množica in S celotno dominantna množica grafa G. Tako družina zaprtih okolic okoli vozlišč iz D, to je $\{N_G[v] : v \in D\}$, in družina odprtih okolic okoli vozlišč iz S, to je $\{N_G(v) : v \in S\}$, obe pokrivata vsa vozlišča grafa G. Včasih se zgodi, da ti dve družini ne le pokrivata, pač pa tvorita razbitje vozlišč grafa G. V tem primeru govorimo o **učinkovito zaprto dominiranemu grafu** oziroma **učinkovito odprto dominiranemu grafu**. Z drugimi besedami je graf G učinkovito zaprto dominiran, če obstaja taka dominantna množica D, da ima vsako vozlišče iz $V(G) - D$ natanko enega soseda v D. Podobno je graf G učinkovito odprto dominiran, če obstaja celotno dominantna množica S, da ima vsako vozlišče iz $V(G)$ natanko enega soseda v S.

Zgled 9.30 *Za nekatere znane družine grafov imamo $\gamma(K_n) = 1$, $\gamma(N_n) = n$, $\gamma(P_n) = \lceil \frac{n}{3} \rceil$ (vzamemo drugo vozlišče in nato vsakega tretjega in pazimo še na koncu), $\gamma(C_n) = \lceil \frac{n}{3} \rceil$ (vzamamemo vsako tretje vozlišče) in za $s, t \geq 2$ velja $\gamma(K_{s,t}) = 2$ (vzamemo po eno vozlišče iz vsake množice particije). Še za celotno dominantno število $\gamma_t(K_n) = 2$,*

$\gamma_t(P_n) = \lceil \frac{n}{2} \rceil$, ko ima n pri deljenju s štiri ostanek različen od 2, sicer moramo še prišteti 1 (prvo vozlišče spustimo, nato jemljemo po dve zaporedni v množici in dve zaporedni izven množice in pazimo na koncu), $\gamma_t(C_n) = \lceil \frac{n}{2} \rceil$ (jemljemo po dve zaporedni v množici in dve zaporedni izven množice in pazimo na koncu) in $\gamma_t(K_{s,t}) = 2$ (vzamemo po eno vozlišče iz vsake množice particije).

Zgled 9.31 *Kljub povezavi v izreku 9.27 je lahko razlika med $\gamma(G)$ in $\alpha(G)$ poljubno velika. Tako je $\gamma(K_{1,k}) = 1$ in $\alpha(K_{1,k}) = k$. Ker je k poljubno naravno število, je lahko tudi razlika poljubno velika.*

Zgled 9.32 *Za Petersenov graf je $\gamma(P) = 3$ (vzamemo dve nesosednji vozlišči na zunanjem ciklu in nato še vozlišče, ki je sosednje preostalima dvema, ki še nista dominirana; seveda ne gre z le enim ali dvema vozliščema) in $\gamma_t(P) = 4$ (celotno dominantna množica je zaprta okolica kateregakoli vozlišča, medtem ko se zlahka vidi, da z le dvema ali tremi vozlišči ne gre). Podobno je za Grötzschev graf $\gamma(G) = 3$ (vzamemo dve nesosednji vozlišči na zunanjem ciklu in centralno vozlišče z risbe, kar je optimalno; če želimo zunanji cikel dominirati drugače, takoj potrebujemo vsaj tri vozlišča) in $\gamma_t(G) = 4$ (celotno dominantna množica je zaprta okolica kateregakoli vozlišča iz notranjega kroga risbe, medtem ko se zlahka vidi, da z le dvema ali tremi vozlišči ne gre).*

Zgled 9.33 *Cikel C_n je učinkovito zaprto dominiran natanko tedaj, ko je $n \equiv 0 \pmod 3$ in je učinkovito odprto dominiran natanko tedaj, ko je $n \equiv 0 \pmod 4$. Ustrezne množice, opisane v zgledu 9.30, se lepo zaključijo. Pot P_n je učinkovito zaprto dominirana za vsako naravno število n (poiščite ustrezne množice), medtem ko je učinkovito odprto dominirana vedno, ko ima n pri deljenju s štiri ostanek različen od 2 (poiščite ustrezne množice).*

9.7 NEKATERE OPERACIJE NAD GRAFI

Ena izmed močnejših strani grafov je zagotovo, da s pomočjo enega, dveh, ali več grafov lahko tvoriš nove, običajno večje grafe. Tem postopkom rečemo operacije nad grafi in v tem razdelku bomo na kratko opisali definicije nekaterih operacij in si jih ogledali na nekaj enostavnih primerih.

Velja tudi obratno. Za običajno velik graf se lahko vprašamo, ali je bil dobljen iz manjših grafov s pomočjo katere izmed operacij. Takšna zveza je koristna, saj lahko pogosto grafovske lastnosti večjega grafa na tak ali drugačen način povežemo z enakimi ali drugačnimi lastnostmi manjšega grafa. To je lahko koristno pri algoritmični obdelavi grafa, saj hitreje algoritmično preverjamo manjše kot velike grafe.

Omenimo, da smo dve operaciji že spoznali. Prva je bila subdivizija v razdelku o ravninskih grafih in druga je bil komplement grafa ob povezavi kličnega in neodvisnega števila.

Najprej opišimo nekaj manjših, tako rekoč lokalnih operacij. Grafu lahko izbrišemo vozlišče v skupaj s povezavami, s katerimi je to vozlišče incidenčno. To operacijo označimo kar z $G - v$. Grafu lahko izbrišemo tudi povezavo e, kar označimo z $G - e$, pri čemer krajišči te povezave pustimo pri miru. (Pozoren bralec lahko opazi, da smo oznako $G - e$ ali $G - uv$ že nekajkrat uporabili.) Obe operaciji imata tudi svoji nasprotni operaciji. Grafu lahko med vozlišči grafa tudi dodamo povezavo e in to označimo z $G + e$. Ob tem moramo vedeti le, kateri sta krajišči povezave e. Če med izbranima vozliščema povezava že obstaja, dobimo pač večkratno povezavo. Spomnimo se, da smo to že počeli pri Kitajskem problemu poštarja. Grafu vozlišče v lahko tudi dodamo in pišemo $G + v$, vendar moramo ob tem definirati tudi, s katerimi novimi povezavami je incidenčno vozišče v. Kot bomo omenili kasneje, lahko to operacijo izrazimo z nekaterimi drugimi.

Opišimo sedaj **graf povezav** $L(G)$ grafa G. Zanj velja, da ima za vozlišča povezave grafa G, torej $V(L(G)) = E(G)$. Dve povezavi grafa G pa sta sosedi v $L(G)$, če imata skupno krajišče v G. Opazimo lahko, da vozlišče $v \in V(G)$ stopnje k generira kliko velikosti k v $L(G)$. Tako je največja stopnja grafa G klično število grafa $L(G)$.

Ker je tudi $L(G)$ graf, lahko na njem naredimo graf povezav, torej $L(L(G)) = L^2(G)$. Seveda lahko s tem postopkom nadaljujemo in vprašamo se lahko, ali znamo opisati $L^k(G)$ za naravno število k.

Zgled 9.34 *Pot P_n ima $n-1$ povezav in prva in začetna povezava imata le eno sosednjo povezavo, vse vmesne povezave pa imajo po dve sosednji povezavi. Tako je $L(P_n) = P_{n-1}$. Če nadaljujemo, potem dobimo $L(P_{n-1}) = L^2(P_n) = P_{n-2}$. Tako dobimo $L^{n-1}(P_n) = K_1$. Drug, relativno dolgočasen primer so cikli, kjer imamo $L(C_n) = C_n$, ali bolj splošno $L^k(C_n) = C_n$ za vsako naravno število k. Velja tudi $L(K_{1,t}) = K_t$ za vsako naravno število t.*

Graf povezav je tipični predstavnik večjega razreda operacij, ki jim pravimo **presečni grafi**. Za to si je potrebno izbrati objekte nekega tipa v grafu G (recimo povezave za graf $L(G)$). Ti objekti nato predstavljajo vozlišča novega grafa. Sosednost v novem grafu pa definiramo s pomočjo nepraznega preseka začetnih objektov (povezavi z nepraznim presekom, to je skupnim krajiščem, sta sosedi v $L(G)$). Za objekte si lahko izberemo recimo klike, cikle, neodvisne množice, drevesa, poti in še in še. Omenimo le še **klični graf** $Q(G)$, ki ima za vozlišča vse maksimalne klike grafa G (to so klike, ki niso vsebovane v kakšni večji kliki). Dve kliki sta nato sosednji v $Q(G)$, če imata v G neprazen presek. Opaziti velja, da če graf G ne vsebuje trikotnikov, potem je vsaka povezava hkrati maksimalna klika, saj ni vsebovana v kakšni večji kliki. Tako za grafe brez trikotnikov velja $Q(G) = L(G)$. Podobno kot prej lahko induktivno definiramo $Q^k(G) = Q(Q(G^{k-1}))$.

Zgled 9.35 *Ker sta pot in cikel brez trikotnikov, velja $Q(P_n) = L(P_n) = P_{n-1}$, oziroma $Q^{n-1}(P_n) = L^{n-1}(P_n) = K_1$ ter $Q^k(C_n) = L^k(C_n) = C_n$, če je le $n \neq 3$ v primeru cikla. Seveda je tudi $Q(K_n) = 1$. Za graf hiša H s slike 18 pa velja $Q(H) = C_4$.*

Do sedaj smo omenjali le operacije na enem grafu. Pogosto pa imamo operacije nad dvema ali več grafi. Najpreprostejša taka operacija je disjunktna unija dveh ali več grafov. Naj bosta G in H povezana grafa. Njuna **disjunktna unija** $G \sqcup H$ je preprosto nepovezan graf s komponentama G in H. Seveda lahko začnemo z več kot enim grafom, ki tudi niso nujno povezani. Spomnimo se operacije $G + v$. Njo lahko sedaj izrazimo kot $G \sqcup K_1$, nakar izvedemo nekaj operacij $(G \sqcup K_1) + e$, kjer je $K_1 = v$ in je eno krajišče vsake dodane povezave e vozlišče v.

Disjunktna unija je uporabna predvsem v drugo smer. Če imamo nepovezan graf, to pomeni, da je disjunktna unija svojih komponent in nato lahko pogosto preučujemo same komponente in njihove lastnosti. To je tudi razlog, da se pogosto omejimo le na povezane grafe.

Zgled 9.36 *Če je G nepovezan graf s komponentami $H_1, H_2, \ldots, H_k$, potem lahko kromatično število grafa G iščemo tako, da poiščemo kromatična števila vsake komponente posebej, nato pa imamo*

$$\chi(G) = \max\{\chi(H_1), \chi(H_2), \ldots, \chi(H_k)\}.$$

Skoraj identična je slika pri kličnemu številu, saj tam velja

$$\omega(G) = \max\{\omega(H_1), \omega(H_2), \ldots, \omega(H_k)\}.$$

Drug možen pristop je pri neodvisnem številu, številu vozliščnega pokritja, dominantnem številu in celotnemu dominantnemu številu, kjer imamo, za recimo $\alpha(G)$, sledečo povezavo

$$\alpha(G) = \alpha(H_1) + \alpha(H_2) + \cdots + \alpha(H_k).$$

Graf G je učinkovito odprto ali zaprto dominiran, če je taka vsaka njegova komponenta H_i, $i \in [k]$.

Omenimo še, da obstaja tudi (navadna) **unija** grafov G in H in sicer $G \cup H$, kjer velja $V(G \cup H) = V(G) \cup V(H)$ in $E(G \cup H) = E(G) \cup E(H)$. Razlika je lahko v tem, da imata lahko grafa nekaj istih vozlišč in tudi nekaj istih povezav. Če sta recimo $u, v \in V(G) \cap V(H)$ in $uv \in E(G) \cap E(H)$, potem imamo v grafu $G \cup H$ le eno vozlišče v in le eno povezavo uv.

Disjunktno unijo lahko nadgradimo v **spoj** grafov G in H. To je graf $G \oplus H$, ki ga iz $G \sqcup H$ dobimo tako, da dodamo vse povezave $E = \{uv : u \in V(G), v \in V(H)\}$. Če torej v $G \sqcup H$ med kopijama grafov G in H ni nobene povezave, imamo sedaj v $G \oplus H$ med kopijama G in H vse možne povezave. Za neodvisno število v spoju $G \oplus H$ velja

$$\alpha(G \oplus H) = \max\{\alpha(G), \alpha(H)\},$$

saj neodvisna množica ne more imeti nepraznega preseka z obema $V(G)$ in $V(H)$. Za klično število v spoju $G \oplus H$ imamo

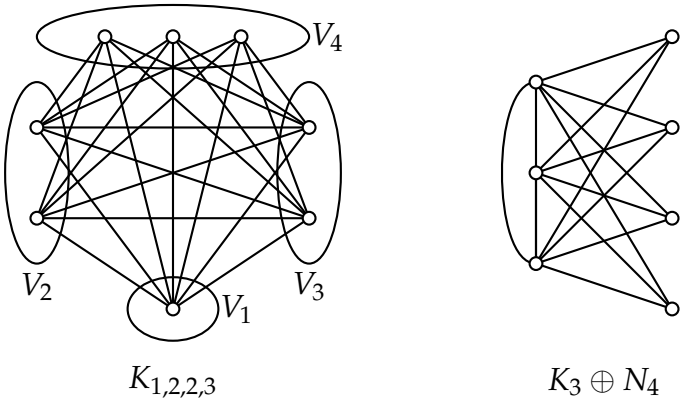
$$\omega(G \oplus H) = \omega(G) + \omega(H),$$

kjer največji kliki iz G in H skupaj tvorita kliko v spoju. Po drugi strani pa ni večje klike, saj bi imeli protislovje z največjo kliko v G ali v H. Tudi za kromatično število velja

$$\chi(G \oplus H) = \chi(G) + \chi(H),$$

saj barve, uporabljene v G, ne moremo uporabiti v H in obratno, zaradi povezav iz E.

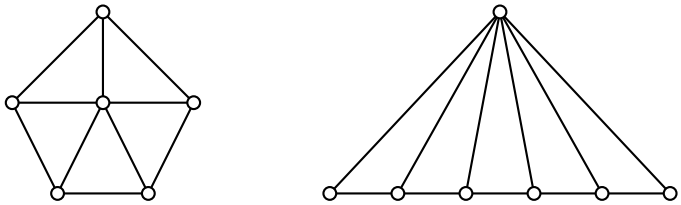
Zgled 9.37 *Nekatere znane družine grafov lahko dobimo s pomočjo spoja grafov. Tako je $K_s \oplus K_t = K_{s+t}$ in $N_s \oplus N_t = K_{s,t}$. Če nadaljujemo s spoji več praznih grafov, to je $(N_s \oplus N_t) \oplus N_r = K_{s,t} \oplus N_r = K_{s,t,r}$ dobimo polni trodelni graf, ki ga sestavljajo tri neodvisne množice V_1, V_2 in V_3 s s, t oziroma r elementi in vsemi preostalimi možnimi povezavami. Bolj splošno k-delni polni graf $K_{r_1,r_2,\ldots,r_k}$ vsebuje k neodvisnih množic $V_1, V_2, \ldots, V_k$ moči zaporedoma $r_1, r_2, \ldots, r_k$, in vse možne povezave med V_i in V_j za vsak $i, j \in [k]$, $i \neq j$. Opazimo lahko, da je $K_{1,1,\ldots,1} \cong K_k$, kjer imamo k enic v $K_{1,1,\ldots,1}$. Graf $K_{1,2,2,3}$ je na sliki 44. V ta sklop spojev sodi še poln razcepljen graf $K_s \oplus N_t$, ki spada v širši razred razcepljenih grafov. Na sliki 44 je $K_3 \oplus N_4$.*



Slika 44: Štiridelni polni graf $K_{1,2,2,3} = N_1 \oplus N_2 \oplus N_2 \oplus N_3$ in spoj $K_3 \oplus N_4$.

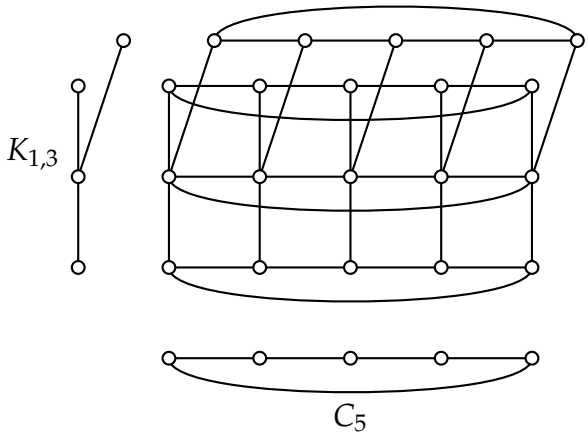
Zgled 9.38 *Do sedaj še nismo omenjali kolesa $W_n = K_1 \oplus C_{n-1}$ za $n \geq 4$ in pahljače $F_n = K_1 \oplus P_{n-1}$ za $n \geq 3$. Opazimo lahko, da velja $W_4 \cong K_4$ in $F_3 \cong K_3$. Na sliki 45 sta W_6 in F_7.*

Do konca razdelka si oglejmo še štiri standardne grafovske produkte. Osnovna značilnost grafovskega produkta dveh grafov G in H je, da ima množico vozlišč definirano na kartezičnem produktu $V(G) \times V(H)$. Povezave lahko nato definiramo na veliko različnih načinov in najbolj ekstremna sta zagotovo, da je med poljubnima vozliščema povezava, kar nas privede do polnega grafa, oziroma da je ni, kar privede do praznega grafa. Najpogostejši so štirje pristopi: kartezični, krepki, direktni in leksikografski produkt, ki jim rečemo standardni grafovski produkti. Njihove definicije in nekatere lastnosti bomo spoznali do konca razdelka.



Slika 45: Kolo $W_6 = K_1 \oplus C_5$ in pahljača $F_7 = K_1 \oplus P_6$.

Kartezični produkt grafov G in H je graf, ki ga označimo z $G \,\square\, H$. Velja $V(G \,\square\, H) = V(G) \times V(H)$. Dve vozlišči (g,h) in (g',h') grafa $G \,\square\, H$ sta sosedi, če je ($g = g'$ in $hh' \in E(H)$) ali ($gg' \in E(G)$ in $h = h'$). Slika grafa $C_5 \,\square\, K_{1,3}$ je na sliki 46. Omenimo še, da je $K_2 \,\square\, K_2 = C_4$, kar je pravzaprav pomen simbola $\square$ za kartezični produkt.



Slika 46: Kartezični produkt $C_5 \,\square\, K_{1,3}$.

Opazimo lahko, da so povezave definirane tako, da nam vozlišča $G^h = \{(g,h) : g \in V(G)\}$ v produktu inducirajo podgraf, ki je izomorfen grafu G. V množici G^h je vozlišče h vedno enako, spreminjajo se le $g \in V(G)$. Tako rečemo množici G^h **sloj grafa** G **skozi vozlišče** h ali kar krajše G-**sloj**. Tako vidimo, da skozi vozlišča, ki imajo enako drugo koordinato pravzaprav narišemo kopijo grafa G. Zgodba se ponovi, če izberemo fiksno vozlišče $g \in V(G)$ in spreminjamo vozlišča grafa H. Tako dobimo H-**sloj** $H^g = \{(g,h) : h \in V(H)\}$. Seveda nam H-sloji v produktu $G \,\square\, H$ inducirajo podgraf izomorfen grafu H. To se lepo vidi na sliki 46. Tako lahko kartezični produkt opišemo tudi kot graf na $V(G) \times V(H)$, kjer skozi vsako fiksno vozlišče $g \in V(G)$ narišemo kopijo H-ja in skozi vsako vozlišče $h \in V(H)$ kopijo G-ja.

V kartezičnem produktu se iz obeh faktorjev lepo prenese razdalja med vozlišči. Tako velja

$$d_{G\,\square\, H}((g,h),(g',h')) = d_G(g,g') + d_H(h,h').$$

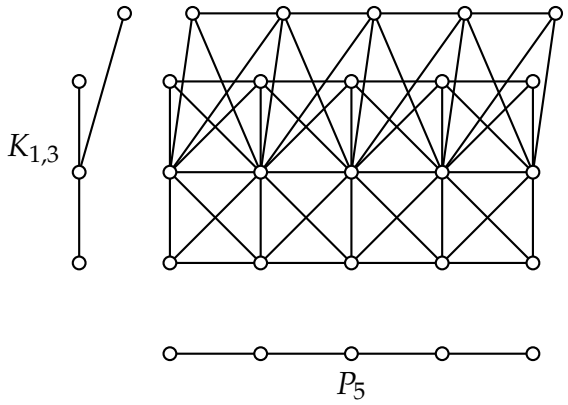
Eno najkrajšo pot dobimo tako, da najprej naredimo v G^h sloju najkrajšo pot od (g,h) do (g',h), nato pa nadaljujemo v $H^{g'}$ sloju od (g',h) do (g',h'). Da ne obstaja pot krajša od dolžine $d_G(g,g') + d_H(h,h')$, se dokaže s pomočjo projekcij na faktorja in dokaz tukaj opuščamo.

Tudi za kromatično število velja lepa zveza

$$\chi(G\,\square\, H) = \max\{\chi(G),\chi(H)\}.$$

Tokrat se lažje vidi, da manj barv ne moremo porabiti, saj $G\,\square\, H$ vsebuje grafa G in H kot svoja podgrafa. Za samo barvanje pa se je potrebno malo potruditi. Omenimo še dominantno število, ki se je izkazalo za notorično težak problem na kartezičnih produktih in že 60 let vznemirja matematike, ki se ukvarjajo s teorijo grafov.

Krepki produkt grafov G in H označimo z $G \boxtimes H$. Seveda je $V(G \boxtimes H) = V(G) \times V(H)$. Dve vozlišči (g,h) in (g',h') grafa $G \boxtimes H$ sta sosedi, če je ($g = g'$ in $hh' \in E(H)$) ali ($gg' \in E(G)$ in $h = h'$) ali ($gg' \in E(G)$ in $hh' \in E(H)$). Slika grafa $P_5 \boxtimes K_{1,3}$ je na sliki 47. Spet imamo s $K_2 \boxtimes K_2 = K_4$ predstavljen pomen simbola $\boxtimes$ za krepki produkt.



Slika 47: Krepki produkt $P_5 \boxtimes K_{1,3}$.

Takoj lahko opazimo, da krepki produkt vsebuje vse povezave kartezičnega produkta, ki jim zato rečemo kar **kartezične povezave**. Preostalim povezavam pravimo **nekartezične povezave**. Torej je kartezični produkt vpeti podgraf krepkega produkta. Ponovno lahko definiramo G-sloje in H-sloje na enak način in ponovno vozlišča G-sloja inducirajo podgraf izomorfen G in vozlišča H-sloja

podgraf izomorfen H. Tudi v krepkem produktu je vredno omeniti obnašanje razdalje, ki je

$$d_{G\boxtimes H}((g,h),(g',h')) = \max\{d_G(g,g'), d_H(h,h')\}.$$

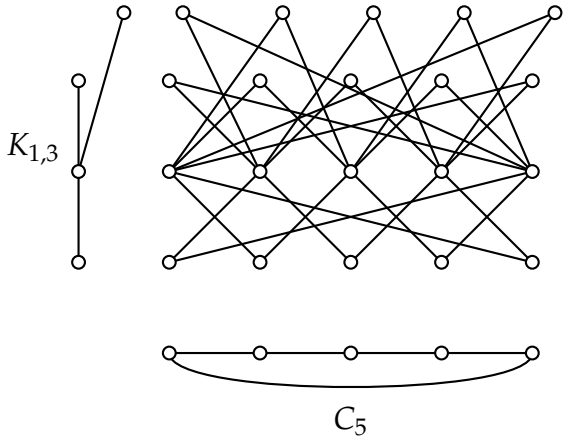
Tukaj lahko opišemo najkrajšo pot med (g,h) in (g',h') v krepkem produktu, kot pot dolžine $\min\{d_G(g,g'), d_H(h,h')\}$, ki gre po samih nekartezičnih povezavah, nato pa nadaljujemo ali v $G^{h'}$-sloju ali v $H^{g'}$ sloju do (g',h'). V krepkem produktu se ohranjajo zaprte okolice, kar pomeni

$$N_{G\boxtimes H}[(g,h)] = N_G[g] \times N_H[h].$$

Zaradi te lastnosti ni težko videti, da je krepki produkt $G \boxtimes H$ učinkovito zaprto dominiran natanko tedaj, ko sta oba G in H učinkovito zaprto dominirana. Omenimo še, da je $A_G \times A_H$ dveh neodvisnih množic A_g iz G in A_H iz H ponovno neodvisna množica v krepkem produktu $G \boxtimes H$. To je že dovolj, da velja

$$\alpha(G \boxtimes H) \geq \alpha(G)\alpha(H).$$

Direktni produkt grafov G in H je graf $G \times H$ na množici vozlišč $V(G \times H) = V(G) \times (H)$. Dve vozlišči (g,h) in (g',h') grafa $G \times H$ sta sosedi, če je $gg' \in E(G)$ in $hh' \in E(H)$. Slika grafa $C_5 \times K_{1,3}$ je na sliki 48. Spet nam $K_2 \times K_2 = K_2 \sqcup K_2$ simbolizira $\times$, kjer je vsaka črtica ena povezava K_2.



Slika 48: Direktni produkt $C_5 \boxtimes K_{1,3}$.

Takoj lahko opazimo zvezo med povezavami kartezičnega, krepkega in direktnaga produkta, ki je

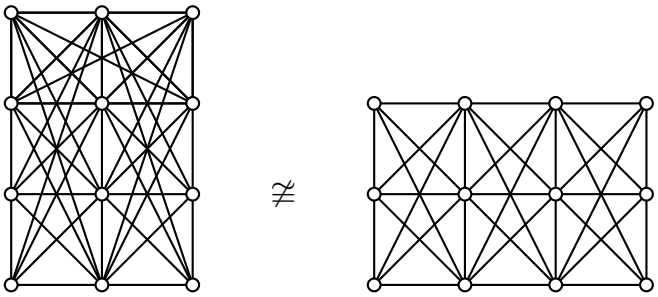
$$E(G \boxtimes H) = V(G \square H) \cup V(G \times H).$$

Tokrat so G-sloji in H-sloji popolnoma brez povezav, če nanje gledamo kot na podgrafe $G \times H$. Že primer $K_2 \times K_2 = K_2 \sqcup K_2$ nam pove, da direktni produkt ni nujno povezan, tudi če sta oba faktorja povezana grafa, kar se v kartezičnem in krepkem produktu ne zgodi. Tudi razdalja se v direktnem produktu ne prenaša lepo glede na faktorja. To so že razlogi, da je direktni produkt pogosto zelo težaven, celo najzahtevnejši med produkti. Se pa v direktnem produktu ohranjajo odprte okolice in velja

$$N_{G\times H}((g,h)) = N_G(g) \times N_H(h).$$

Zaradi tega je direktni produkt grafov učinkovito odprto dominiran natanko tedaj, ko sta oba faktorja učinkovito odprto dominirana.

Za konec si oglejmo še **leksikografski produkt** $G \circ H$ grafov G in H. Seveda je $V(G \circ H) = V(G) \times V(H)$ in vozlišči (g,h) in (g',h') grafa $G \circ H$ sta sosedi, če je ($g = g'$ in $hh' \in E(H)$) ali $gg' \in E(G)$. Takoj lahko opazimo, da tokrat povezave niso definirane simetrično glede na oba faktorja G in H. Zato upravičeno pomislimo, da grafa $G \circ H$ in $H \circ G$ najbrž nista izomorfna. Že ne primeru grafov $P_4 \circ P_3$ in $P_3 \circ P_4$, ki sta na sliki 49, vidimo, da sta različna. To lahko vidimo že po številu povezav obeh grafov, ki sta različni.



Slika 49: Leksikografska produkta $P_3 \circ P_4$ in $P_4 \circ P_3$.

Leksikografski produkt je nekoliko v sorodu s spojem, saj velja

$$K_2 \circ H \cong H \oplus H.$$

V posebnem primeru lahko podobno zvezo najdemo tudi s krepkim produktom, saj velja

$$G \circ K_n \cong G \boxtimes K_n.$$

Razdalja v leksikografskem produktu je zelo odvisna od razdalje v prvem faktorju G in velja

$$d_{G\circ H}((g,h),(g',h')) = \begin{cases} d_G(g,g') & : \ g \neq g' \\ \min\{d_H(h,h'),2\} & : \ g = g' \end{cases}.$$

V leksikografskem produktu ni težko opaziti zveze med kličnimi števili

$$\omega(G \circ H) = \omega(G)\omega(H).$$

Če je podan nek graf, lahko za kartezični, krepki in direktni produkt v polinomskem času preverimo, ali je ta graf produkt kakšnih manjših grafov in katerih. V kartezičnem primeru je časovna odvisnost celo linearna. Tega zaenkrat še ni moč potrditi za leksikografski produkt, saj je razcep grafa na faktorje leksikografskega produkta enakovreden problemu preverjanja izomorfizma grafov.

9.8 NEKATERI IZBRANI ALGORITMI

V tem, zadnjem, razdelku si bomo ogledali le nekaj izbranih algoritmov. Ker je tale učbenik namenjen študentom računalništva in informatike, jih večina že pozna, ali jih bo spoznala tekom nadaljnega študija.

Glede podatkovne strukture grafa, shranjenega v računalnik, lahko govorimo o dveh osnovnih pristopih. Eno je matrika sosednosti, ki smo jo za relacije že spoznali v razdelku 7.1. Razlika je le v tem, da je matrika sosednosti za graf vedno simetrična. Z drugimi besedami, i-ta vrstica je enaka i-temu stolpcu. Druga možnost je razširjeni seznam sosedov, ki smo ga prav tako podrobneje že spoznali v razdelku 7.1 za relacije oziroma digrafe. Ta seznam se sedaj skrči, saj ne potrebujemo različnih seznamov I_x in P_x, pač pa ohranimo le en tip seznamov, drugega pa preprosto ni.

Začnimo z algoritmom **iskanja v širino** (angleško breadth first search), ki mu na kratko rečemo kar BFS-algoritem (glejte začetnice besed v angleščini). Ideja algoritma je, da začnemo v nekem vozlišču u grafa G, ki mu dodelimo oznako $b(u) = 0$. Nato v poljubnem vrstnem redu pregledamo vse njegove sosede in jim po vrsti dodelimo oznake od 1 do $\delta(u)$. Nato nadaljujemo z vozliščem z oznako 1 in pregledamo vse njegove še neoznačene sosede in jim po vrsti dodelimo oznake začenši z $\delta(u) + 1$. To najlaže naredimo, če znotraj algoritma dodatno tvorimo seznam že pregledanih vozlišč L. Na začetku je $L = \{u\}$, torej začetno vozlišče. Nato nanj vključimo na konec seznama vse njegove sosede v poljubnem vrstnem redu, samo vozlišče u pa izbrišemo s seznama L. Sedaj nadaljujemo z naslednjim vozliščem. To počnemo tako dolgo, dokler ni seznam L prazen.

Hkrati se izkaže kot zelo uporabna druga oznaka ℓ. Tudi z njo začnemo v začetnem vozlišču u z $\ell(u) = 0$. Vsakemu naslednjemu vozlišču nato dodelimo $\ell(v) = \ell(w) + 1$, če smo do vozlišča v (prvič) prišli iz vozlišča w.

Algoritem 14: BFS Algoritem

Vhod: Seznam sosedov grafa G in vozlišče v_0.
Izhod: Označitev vozlišč s pari števil $(b(v), \ell(v))$.
Začnimo s seznamom $L = \{v_0\}$, $b = 0$ in $b(v_0) = 0$ ter $\ell(v_0) = 0$;
while *seznam L je neprazen* **do**
  Odstrani prvo vozlišče w s seznama L
  forall $v \in N(w)$, *za katere $b(v)$ še ni določen* **do**
    $b(v) = b + 1$
    $b = b + 1$
    $\ell(v) = \ell(w) + 1$
    Dodaj v na konec seznama L
  end
end

Seveda nam $b(v)$ predstavlja števec korakov in s tem določi, v katerem koraku je bilo vozlišče v na vrsti. Po drugi strani velja $\ell(v) = d(v, v_0)$. Torej je $\ell(v)$ razdalja med začetnim vozliščem v_0 in v. Tako nam BFS algoritem razdeli vozlišča v nivoje vozlišč, ki so enako oddaljena od v_0. To so vozlišča z enako oznako $\ell(v)$.

Oglejmo si še časovno zahtevnost BFS algoritma. V vsakem vozlišču pregledamo največ vse njegove sosede, kar po lemi o rokovanju storimo v $2|E(G)| = 2m$ korakih. Ker vse ostale korake izvedemo le enkrat v zanki, to skupaj prinese $n = |V(G)|$ korakov. Tako imamo časovno zahtevnost $4n + 2m = O(n + m)$. Ker je v povezanem grafu število povezav kvečjemu enakega reda kot število vozlišč, ima BFS algoritem v povezanih grafih časovno zahtevnost $O(m)$.

Izvedimo BFS algoritem na povezanem grafu G z n vozlišči. Če vozlišča postavimo po vrsti $v_0, v_1, \ldots, v_{n-1}$ kot so prišla na vrsto v BFS algoritmu, rečemo temu **BFS ureditev**. Tako velja $i = b(v_i)$. Če tem vozliščem dodamo še povezave, preko katere so bili pregledani, dobimo drevo, ki mu rečemo **BFS drevo**. Seveda je BFS drevo drevo s korenom, ki je začetno vozlišče v_0. Tudi v tem drevesu imamo starše, otroke, potomce, zgornje in spodnje sosede in podobno.

Naštejmo še nekaj posledic BFS algoritma.

- V linearnem času $O(m)$ lahko preverimo, ali je graf G povezan. To vemo, če so na koncu BFS algoritma vsa vozlišča označena.

- V linearnem času lahko preverimo, ali je graf dvodelen. Če obstaja povezava $e = uv$ z obema krajiščema z enako oznako $\ell(u) = \ell(v)$, potem G ni dvodelen, saj v njem obstaja lih cikel.

- V času $O(mn)$ lahko določimo vse razdalje med vozlišči v (povezanem) grafu. Za to iz vsakega vozlišča izvedemo BFS algoritem.

Algoritem, ki je nekoliko soroden BFS algoritmu, je algoritem **iskanja v globino** ali krajše DFS algoritem. Tudi ta algoritem označi vsa vozlišča komponente grafa, iz katerega je začetno vozlišče, in določi vpeto drevo te komponente. Po drugi strani pa ne prinaša informacije o razdalji in se posledično manj uporablja.

Algoritem 15: DFS Algoritem

Vhod: Seznam sosedov grafa G in vozlišče v_0.
Izhod: Označitev vozlišč s števil $d(v)$.
Začnimo s seznamom $L = \{v_0\}$, $d = 0$ in $d(v_0) = 0$
while *seznam L je neprazen* **do**
  if *prvo vozlišče w s seznama L nima neoznačenega soseda* **then**
    izbriši w iz L
  else
    za neoznačenega soseda $v \in N(w)$ postavi v na začetek L
    $d(v) = d + 1$
    $d = d + 1$
  end
end

Izvedimo DFS algoritem na povezanem grafu G z n vozlišči. Če vozlišča postavimo po vrsti $v_0, v_1, \ldots, v_{n-1}$ kot so prišla na vrsto v BFS algoritmu, rečemo temu **DFS ureditev**. Tako velja $i = d(v_i)$. Če tem vozliščem dodamo še povezave, preko katere so bila pregledana, dobimo drevo, ki mu rečemo **DFS drevo**. Seveda je DFS drevo drevo s korenom, ki je začetno vozlišče v_0. Tudi v tem drevesu imamo starše, otroke, potomce, zgornje in spodnje sosede in podobno.

Nadaljujemo z družino algoritmov, ki jim na kratko rečemo kar **požrešni** algoritmi. Ideja požrešnega algortima je preprosta, izberimo lokalno najbolj idealno možnost. Na celotnem območju to sicer pogosto ne prinese optimalnega rezultata, vendar lahko s tem pristopom pridobimo vsaj možnost optimalne rešitve. Takšnim algoritmom pravimo **hevristični**. Algoritem je hevristično, če poišče rešitev problema, ki pa ni vedno najboljša možna. Tako je zelo znan požrešen algoritem za iskanje barvanja grafa.

Algoritem 16: Barvanje s požrešnim algoritmom

Vhod: Graf G.
Izhod: Barvanje vozlišč grafa G.
$L = V(G)$
while *seznam L je neprazen* **do**
  izberi poljubno vozlišče v iz L
  dodeli mu najmanjšo barvo $c(v)$, ki je nima noben sosed od v
  izbriši v iz L
end

Seveda dobi prvo izbrano vozlišče v_1 barvo 1. Naslednje izbrano vozlišče v_2 dobi barvo 1, če v_2 ni sosed od v_1, oziroma barvo 2, če je v_2 sosed od v_1. Ko s tem postopkom nadaljujemo, dobimo barvanje, ki je pravilno, ni pa vedno optimalno.

V vsakem vozlišču, ki ga izberemo, moramo pregledati barve vseh njegovih sosedov. To po lemi o rokovanju pomeni, da preverjamo sosede $2|E(G|)$-krat. To že pomeni, da ima ta algoritem linearno časovno zahtevnost $O(|E(G)|)$.

Zgled 9.39 *Požrešni algoritem optimalno pobarva vozlišča polnega grafa K_n, saj je vsako naslednje vozlišče v_i sosednje z vsemi prejšnjimi in dobi barvo i. Tako dobimo pravilno n barvanje, ki je optimalno. Že na poti $P_n = v_1v_2 \dots v_n$, $n \geq 4$, barvanje dobljeno s požrešnim algoritmom ni nujno optimalno. Če vozlišča izbiramo po vrstnem redu $v_1, v_2, \dots, v_n$, dobimo optimalno barvanje, saj dobi v_1 barvo 1, nato v_2 barvo 2. Naslednje vozlišče v_3 ima v okolici že barvo 2, vendar nima barve 1, ki jo tako dobi. Sedaj se vzorec nadaljuje zaporedoma z barvami $2, 1, 2, \dots$. Če pa začnemo z barvanjem v_1 in v_4, dobita obe vozlišči barvo 1. Ko pride na vrsto v_2 ali v_3, recimo v_2, dobi le-ta barvo 2, saj že ima soseda v_1 z barvo 1. Vozlišče v_3 ima sedaj soseda v_4 z barvo 1 in soseda v_2 z barvo 2. Tako dobi v_3 barvo 3, kar ni optimalno za pot, ki je dvodelni graf.*

Podobno lahko zgradimo tudi požrešni algoritem, ki poišče neodvisno množico.

Algoritem 17: Neodvisna množica s požrešnim algoritmom

Vhod: Graf G.
Izhod: Neodvisna množica vozlišč A grafa G.
$L = V(G)$
while *seznam L je neprazen* **do**
  izberi poljubno vozlišče $v \in L$ in $A \leftarrow v$
  izbriši $N[v]$ iz L
end

Ker za vsako vozlišče v, ki ga shranimo v A, nato iz L izbrišemo njegovo zaprto okolico, v A kasneje ne moremo dobiti soseda vozlišča v. Tako je množica A neodvisna.

Zgled 9.40 *Ponovno je polni graf primer, kjer se ne more zgoditi nič napačnega, saj po izbiri enega vozlišča izbrišemo njegovo zaprto okolico, kar so vsa vozlišča in smo končali. Podobno se zgodi v primeru polnega dvodelnega grafa $K_{n,n}$. Ko izberemo prvo vozlišče in izbrišemo njegovo zaprto okolico, ostane še $n-1$ neodvisnih vozlišč, ki vsa pridejo v množico A. Tako s požrešnim algoritmom dobimo neodvisno množico moči n, ki je optimalna v $K_{n,n}$. Že v primeru polnega dvodelnega grafa $K_{s,t}$, $s \neq t$, lahko zgrešimo najboljšo možnost. Naj bo $s < t$ in V_1 in V_2 tvorita dvodelno razbitje $K_{s,t}$, kjer je $|V_1| = s$. Če prvo vozlišče izberemo iz množice V_1, končamo z $A = V_1$ s podobnim razmislekom kot prej. Ker je s lahko poljubno manjše kot t, vidimo, da je lahko tudi razlika med močjo dobljene neodvisne množice s požrešnim algoritmom in največjo neodvisno množico, poljubno velika.*

Kot problem, s katerim lahko precej zgrešimo optimalno rešitev, omenimo problem trgovskega potnika. Za ta problem obstaja za vsako število mest takšna porazdelitev razdalj med mesti, da z izbiro najkrajših razdalj, torej požrešnim algoritmom, dobimo najslabšo možno rešitev.

Za konec si oglejmo dva požrešna algoritma, ki vedno porodita optimalno rešitev. Oba rešujeta problem najmanjšega vpetega drevesa na primeru grafov z uteženimi povezavami. Pri prvem izbiramo povezave z najnižjimi utežmi, pri čemer je potrebno paziti, da z novo dodano povezavo ne ustvarimo cikla. Temu algoritmu rečemo Kruskalov[27] algoritem.

Algoritem 18: Kruskalov algoritem

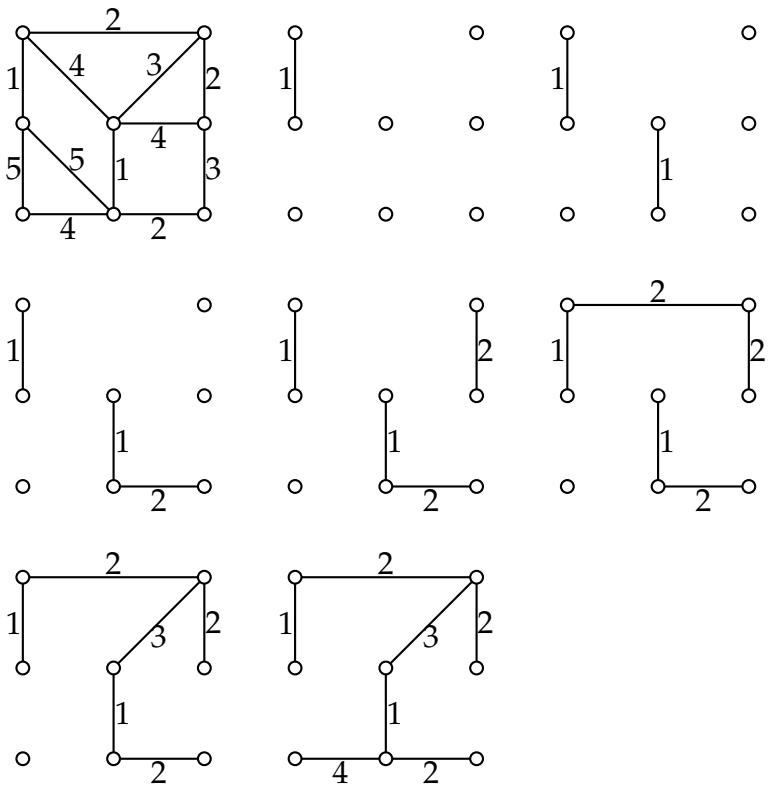
Vhod: Povezan graf G z uteženimi povezavami.
Izhod: Minimalno vpeto drevo grafa G.
$S = E(G)$ in $F = V(G)$
while *seznam* S *je neprazen* **do**
  izberi poljubno povezavo z minimalno utežjo e
  izbriši e iz S
  if e *je povezava med dvema drevesoma* T_1 *in* T_2 *iz* F **then**
    dodaj e in združi drevesi T_1 in T_2 v F
  end
end

Ker imamo na vhodu povezan graf G, dobimo na izhodu vpet podgraf, ki je drevo. To nam zagotovi tudi dodatni pogoj, ki dodaja le povezave med dvema drevesoma, ki tako ohranjano F brez ciklov (z vedno manj drevesi), dokler ne ostanemo z enim samim drevesom. Ob primerni izbiri podatkovne strukture (za hitro združevanje dveh dreves), ima Kruskalov algoritem časovno zahtevnost $O(m \lg n)$, kjer je $m = |E(G)|$ in $n = |V(G)|$, kar je pravzaprav tudi časovna zahtevnost sortiranja uteženih povezav po velikosti.

Zgled 9.41 *Na sliki 50 so predstavljeni koraki Kruskalovega algoritma. Opazimo lahko, da se šele v zadnjem koraku zgodi, da ne izberemo še neizbrane povezave z najmanjšo utežjo* 3*, saj bi tvorila cikel. Namesto nje izberemo povezavo z utežjo* 4 *(tudi druge povezave z utežjo* 4 *ne smemo izbrati, saj tvori cikel).*

Sledi Primov[28] algoritem, ki zahteva še dodatno lokalno omejitev, da je drevo, ki ga gradimo, povezano od začetka do konca izvajanja algoritma.

27 Joseph Bernard Kruskal (1928-2010) je bil ameriški matematik, statistik in računalničar.
28 Robert Clay Prim (1921-) je ameriški matematik in računalničar.

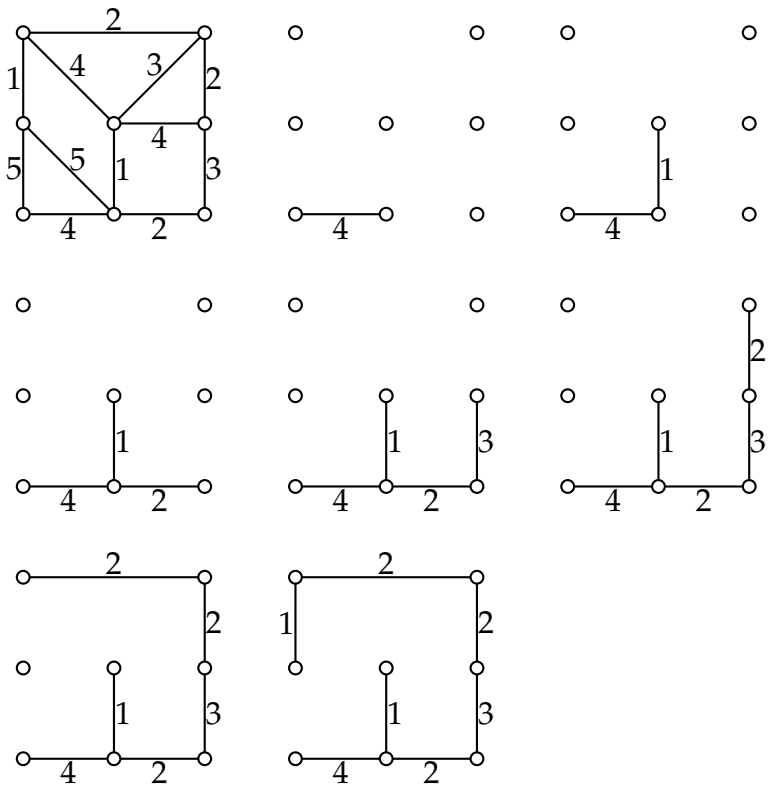


Slika 50: Analiza Kruskalovega algoritma.

Algoritem 19: Primov algoritem

Vhod: Povezan graf G z uteženimi povezavami.
Izhod: Minimalno vpeto drevo grafa G.
Izberi poljubno vozlišče $v \in V(G)$ in $T = v$
while $V(T) \neq V(G)$ **do**
  dodaj poljubno povezavo z minimalno utežjo, ki ima eno krajišče v T
end

Ponovno nam povezan graf na vhodu in dodaten pogoj, da je eno krajišče dodane povezave že na prejšnjem drevesu, zagotavlja, da imamo na izhodu vpeto drevo. Le-to je minimalno, saj vedno izberemo povezavo z minimalno utežjo. Časovna zahtevnost Primovega algoritma je odvisna od izbire podatkovne strukture. Za $m = |E(G)|$ in $n = |V(G)|$ imamo časovno zahtevnost $O(n^2)$ v primeru matrike sosednosti in $O(m \lg n)$ v primeru seznama sosedov, kjer so podatki nadalje shranjeni v obliki binarnega drevesa. To lahko izboljšamo do časovne zahtevnosti $O(m + n \lg n)$, če namesto binarnega drevesa uporabimo tako imenovano Fibonaccijevo kopico.



Slika 51: Analiza Primovega algoritma.

Zgled 9.42 *Na sliki 51 so predstavljeni koraki Primovega algoritma. Lepo je opazno, da je konstruiran graf ves čas povezan. Končno drevo je tudi drugačno od drevesa, dobljenega s Kruskalovim algoritmom iz zgleda 9.41.*

9.9 NEKATERE (NE)REŠENE NALOGE

Vaja 9.1 *Podan je graf* $G = (V(G), E(G))$ *z* $V(G) = \{a, b, c, d, e, f, g, h, i, j, k, l\}$ *in*

$E(G) = \{ab, ae, aj, ag, bc, bh, bf, cd, ci, cg, de, dh, dj, ei, ef, fk, fl, gk, gl, hi, hl, ik, jk, jl\}$.

(A) *Narišite graf G.*

(B) *Izvedite BFS algoritem iz vozlišča a (določi BFS ureditev in BFS drevo).*

(C) *Ali je G Hamiltonov?*

(D) *Ali je G ravninski?*

(E) *Ali je G Eulerjev?*

(F) *Določite* $\chi(G)$.

Rešitev. *Graf G je na sliki 52, (ena) BFS ureditev je $(a, b, j, g, e, f, c, h, l, k, d, i)$; G je Hamiltonov, cikel je $agcbfljkihdea$; ni ravninski, saj (zlahka vidimo da) vozlišča a, b, c, d in e tvorijo subdivizijo K_5; je Eulerjev: $abcdeagcihbfeikglhdjkflja$ in $\chi(G) = 4$. Možno barvanje s štirimi barvami je: barvo 1 dobijo vozlišča b, d, g, i, barvo 2: a, c, f, h, barvo 3: e, j in barvo 4: k, ℓ.*

Vaja 9.2 *Ali je graf G podan z $V(G) = \{u_1, u_2, \ldots, u_{12}\}$ in*

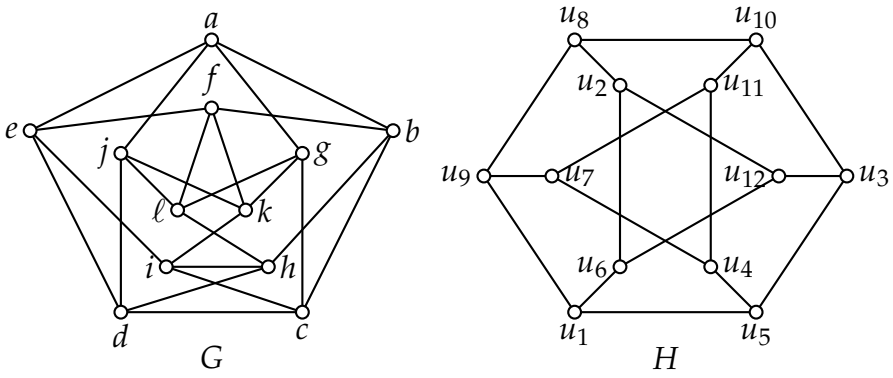
$$E(G) = \{u_1u_5, u_1u_6, u_1u_9, u_2u_6, u_2u_8, u_2u_{12}, u_3u_5, u_3u_{10}, u_3u_{12}, u_4u_5, u_4u_7, u_4u_{11}, u_6u_{12}, u_7u_9, u_7u_{11}, u_8u_9, u_8u_{10}, u_{10}u_{11}\}$$

izomorfen grafu H s slike 52? Preverite še, ali je H Hamiltonov in ravninski graf!

Rešitev. *Grafa sta izomorfna (glej vozlišča na sliki); H ima Hamiltonov cikel*

$$u_1u_5u_4u_{11}u_7u_9u_8u_{10}u_3u_{12}u_2u_6u_1;$$

H je ravninski (le vozlišča u_2, u_6 in u_{12} narišemo "od zunaj").



Slika 52: Graf G za vajo 9.1 in graf H za vajo 9.2.

Vaja 9.3 *Graf $G = (V, E)$ je določen z množicama $V(G) = \{i \mid 1 \leq i \leq 9\}$ in*

$$E(G) = \{ij \mid i + j \text{ je liho število}\}.$$

(A) *Narišite graf G.*

(B) *Ali je G povezan graf?*

(C) *Ali je G dvodelen graf?*

(D) *Ali je G Hamiltonov graf?*

(E) *Ali je G Eulerjev ali pol-Eulerjev?*

Rešitev. *To je graf $K_{4,5}$, ki je seveda povezan in dvodelen, ni pa Hamiltonov (dvodelen graf na liho vozliščih) niti Eulerjev niti pol-Eulerjev (štiri vozlišča lihe stopnje).*

Vaja 9.4 *V grafu G imamo vozlišča $V_G = \{1,2,3,4,5,6,7,8\}$, povezave pa so definirane s predpisom*

$$E_G = \{pq \mid p+q \text{ je praštevilo}\}.$$

Narišite graf G in preverite ali je Hamiltonov in ravninski.

Rešitev. *Graf je Hamiltonski s ciklom* 123856741. *Je tudi ravninski, saj zlahka narišemo njegovo ravninsko risbo.*

Vaja 9.5 *Danemu besedilu T priredimo graf $G = (V, E)$ na naslednji način:*

$$V = \{t\,;\ \text{črka } t \text{ nastopa v besedilu } T\},$$
$$E = \{(u,v);\ \text{črki } u \text{ in } v \text{ sta sosedi v besedilu } T\},$$

če ne upoštevamo presledkov in ločil. Za besedilo FAKULTETA ZA ELEKTROTEHNIKO, RAČUNALNIŠTVO IN INFORMATIKO narišite graf in preverite ali je ravninski in Eulerjev.

Rešitev. *Graf ni ravninski, saj A, U, L, T, N tvorijo subdivizijo K_5 (skupaj s* Č, *K, E in H). Tudi Eulerjev ni, saj ima vozlišče F stopnjo* 1.

Vaja 9.6 *Posplošeni Petersenov graf $P_{n,k}$, $n \geq 3$, $0 < k < n$, je definiran z*

$$V(P_{n,k}) = \{u_i, v_i \mid i \in [n]\},$$
$$E(P_{n,k}) = \{u_iu_{i+1}, u_iv_i, v_iv_{i+k} \mid i \in [n]\}.$$

Dokažite, da je $P_{n,k}$ dvodelen natanko takrat, ko je n sodo in k liho število. (Operacije v indeksih so po modulu n.)

Rešitev. *($\Rightarrow$) Če je n lih, tvorijo vozlišča u_i lih cikel in G ni dvodelen; če je k sod, je cikel $u_1u_2\ldots u_{k+1}v_{k+1}v_1u_1$ lih cikel in G ni dvodelen. ($\Leftarrow$) Naj bo n sod in k lih. Videti je potrebno, da množici $A = \{u_{2i}, v_{2i+1}\}$ in $B = \{u_{2i+1}, v_{2i}\}$ tvorita particijo grafa G in da inducirata prazna podgrafa (da ni povezav med vozlišči iz množice A, oziroma vozlišči iz množice B).*

Vaja 9.7 *Graf G vsebuje natanko en cikel, vsa vozlišča iz G pa so stopnje 1, 3 ali 4. Vozlišč stopnje 3 je 4-krat več kot vozlišč stopnje 4, vozlišč stopnje 1 pa je 12. Koliko vozlišč vsebuje G? Narišite še kak tak graf.*

Rešitev. *Če je G povezan, je $n =$ 22 (uporabimo lemo o rokovanju in da je število vozlišč enako kot število povezav); če G ni povezan, je lahko $n =$ 17; takih grafov je mnogo, morda najenostavnejši je cikel na 10 vozliščih, ki mu v dveh vozliščih dodamo dva lista, v preostalih osmih vozliščih pa en list.*

Vaja 9.8 *Vozlišču na grafu, ki ima stopnjo ena, rečemo list, vsem preostalim vozliščem pa notranja vozlišča. Razred grafov T sestavljajo vsa drevesa, v katerih imajo vsa notranja vozlišča stopnjo tri.*

(A) *Pokažite, da je za grafe iz razreda T število listov za 2 večje od števila notranjih vozlišč.*

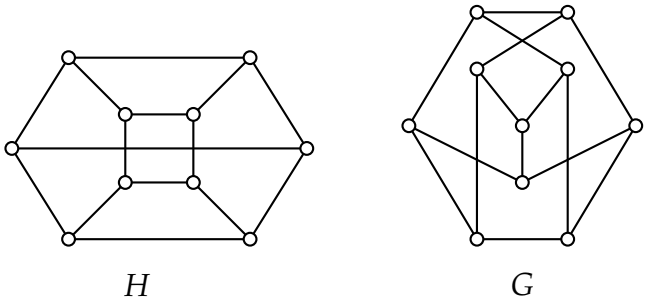
(B) *Narišite vse neizomorfne grafe razreda T na 12 vozliščih.*

(C) *Ali obstaja drevo iz T na 13 vozliščih?*

Rešitev. *Zvezo dobimo iz leme o rokovanju in povezave med številom vozlišč in povezav na drevesu. Obstajata le dve taki drevesi na 12 vozliščih. Tako drevo na 13 vozlišč ne obstaja, saj bi imeli liho število vozlišč lihe stopnje.*

Vaja 9.9 *Ali sta grafa na sliki 53 izomorfna? Preverite še, ali je graf G Hamiltonov!*

Rešitev. *Nista izomorfna, saj ima recimo H cikle C_4 kot podgrafe, G pa ne. Graf G tudi ni Hamiltonov.*



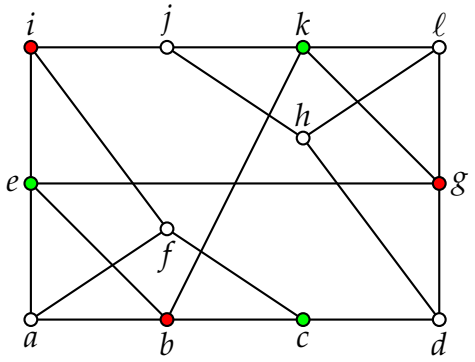
Slika 53: Grafa za vajo 9.9.

Vaja 9.10 *Za graf na sliki 54 preverite ali je ravninski, Hamiltonov in določite njegovo kromatično število.*

Rešitev. *Ni ravninski (vozlišča particije subdivizije grafa $K_{3,3}$ so na sliki označena z rdečo in zeleno barvo); je Hamiltonov (cikel je recimo $afcdhlgkjieba$); $\chi(G) = 3$ (ker G vsebuje K_3, je $\chi(G) \geq 3$, barvanje se zlahka najde).*

Vaja 9.11 *Dvodelno kolo BW_n je graf, ki ga dobimo kot spoj cikla C_n in enega centralnega vozlišča, kjer na koncu subdividiramo vsako povezavo C_n z enim vozliščem. Nariši BW_3 in BW_5. Ugotovite, koliko vozlišč in koliko povezav ima graf BW_n, ali je dvodelen, ravninski in ali je Hamiltonov?*

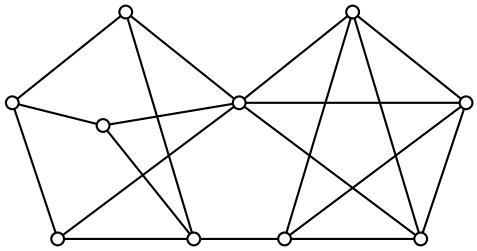
Rešitev. *Velja $|V(BW_n)| = 2n + 1$, $|E(BW_n)| = 3n$, so dvodelni (ustrezno razbitje tvorijo vozlišča začetnega cikla in vsa preostala) in ravninski, niso pa Hamiltonovi (če izbrišemo n vozlišč začetnega cikla, dobimo $n + 1$ komponent).*



Slika 54: Graf za vajo 9.10.

Vaja 9.12 *Za graf G na sliki 55 določite $\chi(G)$ in preverite, ali je ravninski in ali je Hamiltonov.*

Rešitev. *$\chi(G) = 4$. Ni ravninski, saj šest vozlišč na levi tvori podgraf $K_{3,3}$. Če izbrišemo levo vozlišče in srednji vozlišči, potem graf razpade na štiri dele in ni Hamiltonov po izreku 35.*



Slika 55: Graf G za vajo 9.12

Vaja 9.13 *Rešite Kitajski problem poštarja za grafa na sliki 56!*

Rešitev. *Na levem grafu najdemo pot težavnosti 4 med vozliščema lihe stopnje. Skupna rešitev za levi graf je tako 52. Na desnem grafu najdemo pot težavnosti 14 med vozliščema lihe stopnje. Skupna rešitev za levi graf je tako 88.*

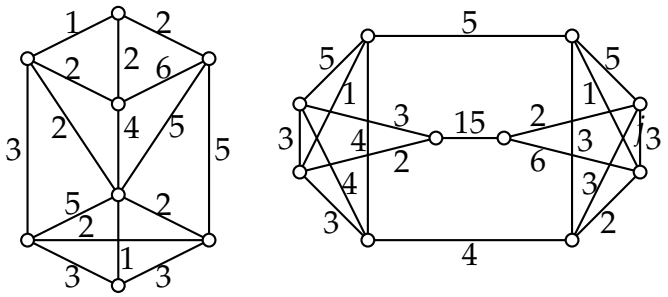
Vaja 9.14 *Povezavi $e = uv$ in $f = u'v'$ na grafu sta v relaciji Θ, če velja*

$$d(u,u') + d(v,v') \neq d(u,v') + d(u',v).$$

(A) *Zapišite, katere povezave na ciklu C_5 so v relaciji Θ.*

(B) *Ali je Θ tranzitivna relacija?*

(C) *Poiščite ekvivalenčne razrede relacije $\overline{\Theta}$ na ciklu C_6.*



Slika 56: Grafa za vajo 9.13.

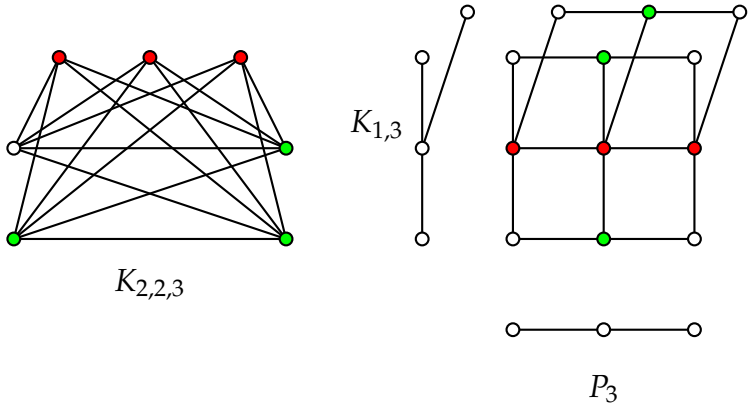
***Rešitev**: Za cikel abcdea imamo abΘcd, abΘde, bcΘde, bcΘea in cdΘea. Relacija Θ ni tranzitivna, saj imamo na C_5 abΘcd, in cdΘea in ab¬Θea. Relacija Θ je tranzitivna na $C_6 = uvxywzu$ in njeni ekvivalenčni razredi so trije $\{uv, yw\}$, $\{vx, wz\}$ in $\{xy, zu\}$.*

Vaja 9.15 *Graf $K_{k,m,n}$, $k \geq m \geq n \geq 1$, je sestavljen iz treh disjunktnih množic vozlišč s k, m in n elementi ter vseh povezav med vozlišči iz različnih množic. Narišite $K_{2,2,3}$. Ali je ravninski? Za katere vrednosti k, m in n je graf $K_{k,m,n}$ Eulerjev?*

***Rešitev**: Graf $K_{2,2,3}$ je na sliki 57, če odstranimo eno vozlišče stopnje 5, preostala tvorijo subdivizijo $K_{3,3}$, tako da ni ravninski. Eulerjev je natanko tedaj, ko so ali vsa tri števila k, m in n soda, ali vsa tri števila k, m in n liha, saj morajo imeti vsa vozlišča Eulerjevega grafa sodo stopnjo, stopnje vozlišč iz $K_{k,m,n}$ pa so $k + m$ ali $k + n$ ali $m + n$.*

Vaja 9.16 *Narišite kartezični produkt $P_3 \,\square\, K_{1,3}$ in ugotovite, ali je ravninski ali ne.*

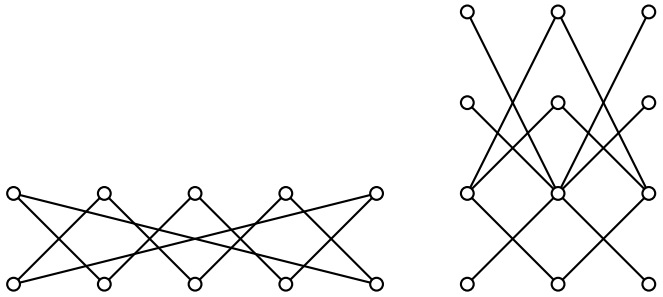
***Rešitev**: Graf je na sliki 57, označena vozlišča tvorijo subdivizijo $K_{3,3}$, tako da ni ravninski.*



Slika 57: Graf $K_{2,2,3}$ s subdivizijo $K_{3,3}$ in kartezični produkt $P_3 \,\square\, K_{1,3}$ s subdivizijo $K_{3,3}$.

Vaja 9.17 *Narišite direktna produkta $H_1 = C_5 \times K_2$ in $H_2 = P_3 \times K_{1,3}$. Kateremu znanemu grafu je izomorfen H_1? Ali je H_2 dvodelen?*

***Rešitev.** H_1 in H_2 sta na sliki 58; $H_1 \cong C_{10}$, H_2 pa je dvodelen (ni pa povezan).*



Slika 58: Grafa $H_1 = C_5 \times K_2$ in $H_2 = P_3 \times K_{1,3}$.

Vaja 9.18 *Narišite leksikografski produkt $P_3 \circ C_4$ in $P_4 \circ N_4$. Ali je kateri od njiju dvodelen?*

Rešitev. *Graf $P_3 \circ C_4$ ni dvodelen, saj zlahka najdemo tricikel. Graf $P_4 \circ N_4$ je dvodelen.*

Vaja 9.19 *Naj graf G vsebuje vsaj eno povezavo. Pokažite, da je leksikografski produkt $G \circ H$ dvodelen natanko tedaj, ko je G dvodelen in $H \cong N_n$.*

Rešitev. *($\Leftarrow$) Če je G dvodelen, potem vsebuje dvodelno razbitje $V(G) = V_1 \cup V_2$. Potem je $V_1 \times V(N_n)$ in $V_2 \times V(N_n)$ dvodelno razbitje $G \circ H$, ki je zato dvodelen. ($\Rightarrow$) S kontrapozicijo. Če G ni dvodelen, potem tudi $G \circ H$ ni dvodelen, saj je podgraf, induciran z vozlišči sloja G^h, izomorfen G. Če H ni prazen graf N_n, potem vsebuje vsaj eno povezavo. Le-ta skupaj s povezavo iz G porodi K_4 v produktu in ta vsebuje tricikle. Zato ponovno $G \circ H$ ni dvodelen.*

STVARNO KAZALO

LITERATURA

[1] M. Aigner, *Discrete Mathematics*, American Mathematical Society, Rhode Island, 2007.

[2] V. Batagelj, *Diskretne strukture : zapiski predavanj, 4. zvezek, Grafi*, samozaložba, Ljubljana, 1998.

[3] V. Batagelj, *Diskretne strukture : zapiski predavanj, 1. zvezek* samozaložba, Ljubljana, 2002.

[4] V. Batagelj, S. Kalvžar, *DS1. Logika in množice*, DMFA - založništvo, Ljubljana, 1997.

[5] V. Batagelj, S. Kalvžar, *DS2. Algebra in teorija grafov*, DMFA - založništvo, Ljubljana, 2005.

[6] N. L. Biggs, *Discrete mathematics, Second Edition*, Oxford university press, Oxford, 2002.

[7] G. Fijavž, *Diskretne strukture. 2. izd.*, Založba FRI, Ljubljana, 2017. http://matematika.fri.uni-lj.si/ds/ds.pdf.

[8] R. Hammack, W. Imrich, S. Klavžar, *Handbook of Product Graphs, Second Edition*. CRC Press, Boca Raton, FL, 2011.

[9] M. Juvan, P. Potočnik, *Teorija grafov in kombinatorika : primeri in rešene naloge*, DMFA - založništvo, Ljubljana, 2007.

[10] S. Klavžar, P. Žigert. Pleteršek, *Izbrana poglavja uporabne matematike, (Knjižna zbirka Učbeniki, 3)*, Pedagoška fakulteta, Maribor, 2002.

[11] M. Konvalinka, P. Potočnik, *Diskretna matematika I*, Fakulteta za matematiko in fiziko, Ljubljana, 2019.

[12] I. Peterin, *Izpitne naloge iz Diskretnih struktur : RI-UNI, RIT-UNI, ITK-UNI*, Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor, 2008. http://mp.feri.um.si/osebne/peterin/naloge/ds/izpiti.pdf.

[13] I. Peterin, *Naloge iz kolokvijev iz Diskretnih struktur : RI-UNI, RIT-UNI, ITK-UNI*, Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor, 2008. http://mp.feri.um.si/osebne/peterin/naloge/ds/kolokviji.pdf.

[14] A. Tepeh, R. Škrekovski, Diskretna matematika, Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor, 2018.

[15] R. J. Wilson, J. J. Watkins, *Uvod v teorijo grafov*, DMFA - založništvo, Ljubljana, 1997.

DISKRETNE STRUKTURE

IZTOK PETERIN

Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor, Slovenija. E-pošta: iztok.peterin@um.si

Povzetek V učbeniku so predstavljene nekatere veje diskretne matematike, ki so še posebej uporabne v računalništvu. Tako se sprehodimo skozi logiko, s posebnim poudarkom na dokazu. Sledijo teorije, pri katerih igra poglavitno vlogo matematična indukcija oziroma bolj splošno induktivna posplošitev. Spoznamo osnove kombinatorike in teorije števil. Predstavljene so rekurzivne relacije, s katerimi lahko opišemo ponavljajoče se procese. To nam omogoča tudi vrednotenje algoritmov glede na čas potreben za njegovo izvedbo. Relacije, ki so podmnožice kartezičnega produkta poljubnih množic, predstavljajo širok vir presenetljivih rezultatov. Eden izmed njih rezultira v mrežah in njihovih posebnih predstavnikih Booleovih algebrah. Končamo z grafi, ki predstavljajo neverjetno uporaben matematični model za simuliranje procesov iz realnega življenja.

Ključne besede:
izjavni račun,
indukcija,
kombinatorika,
rekurzivna relacija,
časovna zahtevnost,
teorija števil,
relacija,
mreža,
Booleova algebra,
graf.

Univerzitetna založba Univerze v Mariboru

DOI https://doi.org/10.18690/978-961-286-400-2

ISBN 978-961-286-400-2

DISCRETE STRUCTURES

IZTOK PETERIN

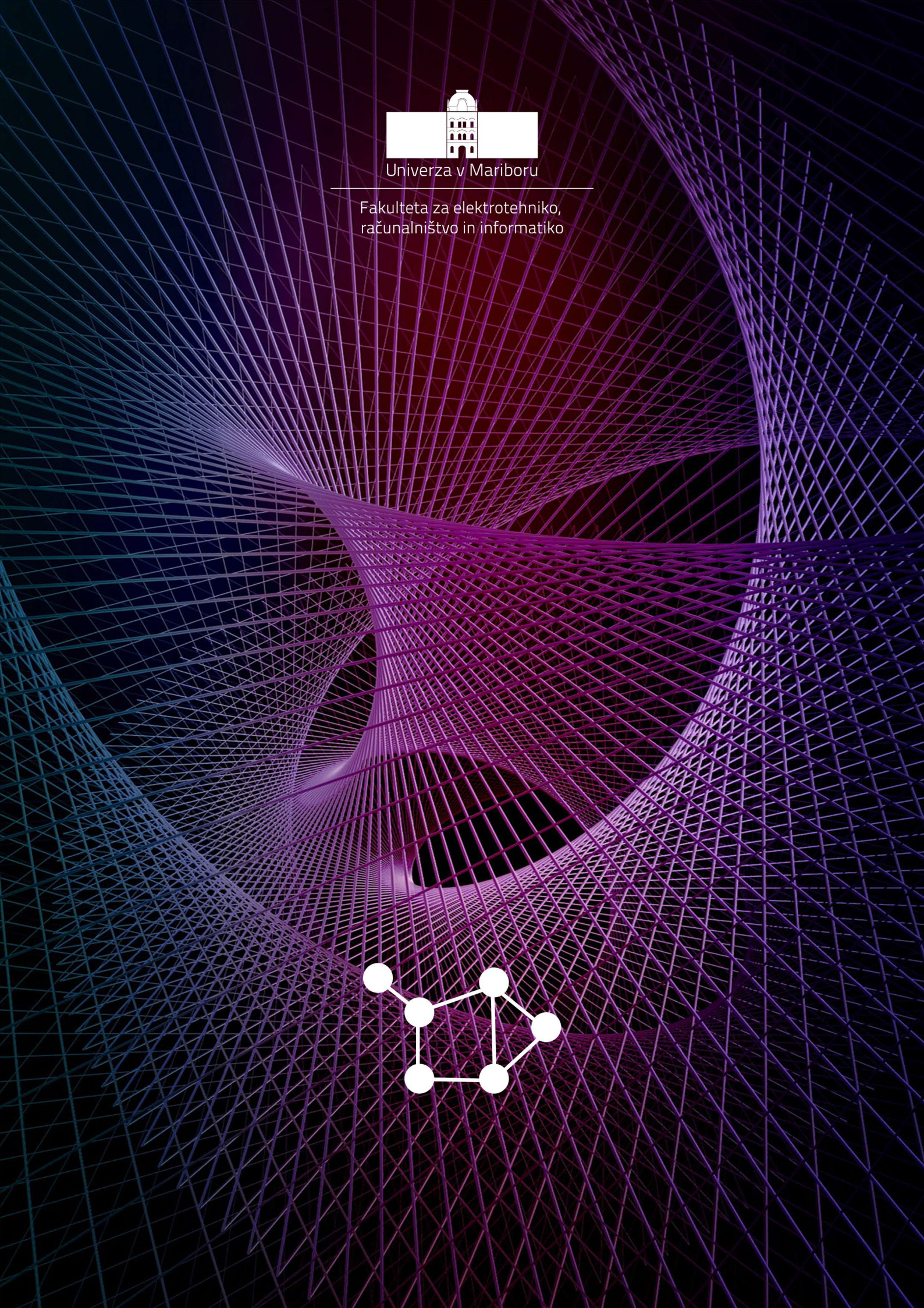
University of Maribor, Faculty of Electrical Engineering and Computer Science, Maribor, Slovenia. E-mail: iztok.peterin@um.si

Abstract This text book brings some branches of Discrete mathematics, which are very applicable in Computer science. As such we start with logic and special emphasis on the proof. The chapter on inductive processes follows. We present the fundamentals of counting and number theory. One part is devoted to recurrence relations, that are a basic tool to describe the processes that are repeating. This enables to quantify the algorithms with respect to the time used by them for their execution. Relations are subsets of the Cartesian product of two sets and present a surprising palette of different results. One direction results in latices and Boolean algebras. We end with graphs. A tool that is incredibly useful mathematical model for all sorts of real life processes.

Keywords: logic, induction, combinatorics, recursive relation, time complexity, number theory, relation, latice, Boolean algebra, graph.

ISBN 978-961-286-400-2 DOI https://doi.org/10.18690/978-961-286-400-2

University of Maribor Press


Univerza v Mariboru
Fakulteta za elektrotehniko,
računalništvo in informatiko