Obsah

1 Úvod do logiky **1**

1.1 Výroky 1

1.2 Operácie s výrokmi 2

1.3 Negácie zložených výrokov 7

1.4 Kvantifikátory 9

2 Množiny **13**

2.1 Základné pojmy 13

2.2 Ako možno vytvárať množiny 15

2.3 Rekurzívne definované množiny 19

2.4 Doplnok: Zermelov-Fraenkelov systém axióm 20

3 Čísla a číselné množiny **23**

3.1 Prirodzené čísla 23

3.2 Celé čísla 27

3.3 Racionálne čísla 29

3.4 Reálne čísla 31

3.5 Komplexné čísla 33

4 Binárne relácie **39**

4.1 Definícia binárnej relácie 39
4.2 Vlastnosti binárnych relácií na množine 40

5 Funkcie **47**
5.1 Grafická reprezentácia funkcií 48
5.2 Niektoré vlastnosti funkcií 49
5.3 Mohutnosť množín a funkcie 50
5.4 Dôsledky predchádzajúcich úvah v informatike 55

6 Postupnosti **59**
6.1 Základné pojmy 59
6.2 Vlastnosti postupností 63
6.3 Hromadný bod postupnosti 69
6.4 Limita postupnosti 73

7 Reálne funkcie reálnej premennej **79**
7.1 Príklady reálnych funkcií reálnej premennej 80
7.2 Ako merať zmenu veličín 84

8 Súčty a súčiny **95**
8.1 Súčet konečného počtu členov aritmetickej postupnosti . . . 95
8.2 Súčet konečného počtu členov geometrickej postupnosti . . 96
8.3 Práca so symbolmi $\sum$ a $\prod$ 97
8.4 Vlastnosti súčtov 98
8.5 Vlastnosti súčinov 103
8.6 Porovnanie konečných a nekonečných súčtov 103
8.7 Poznámka k reprezentácii racionálnych čísel 107

9 Ako určovať počet možností **109**

9.1 Princíp sčitovania 109
9.2 Princíp násobenia 110
9.3 Princíp delenia 111
9.4 Princíp bijekcie 113
9.5 Dirichletov princíp 114
9.6 Pascalov trojuholník 116

10 Porovnávanie funkcií **119**
10.1 O-notácia 119
10.2 Niektoré nepríjemnosti spojené s používaním $O(g(n))$ 122
10.3 Zložitosť algoritmov 123
10.4 Theta 124
10.5 Malé o 124
10.6 Asymptotická rovnosť 125

11 Úvod do teórie čísel **127**
11.1 Deliteľnosť 127
11.2 Zvyšok 129
11.3 Najväčší spoločný deliteľ 129
11.4 Prvočísla a zložené čísla 131
11.5 Modulárna aritmetika 133
11.6 Niekoľko nevyriešených problémov z teórie čísel 135

12 Niekoľko algoritmov z teórie čísel **139**
12.1 Zisťovanie prvočíselnosti 139
12.2 Rozklad čísla na súčin prvočísel 141
12.3 Rýchle umocňovanie 142
12.4 Výpočet inverzného prvku v poli $(Z_p, \oplus_p, \odot_p)$ 143
12.5 Algoritmus RSA 143

13 Stavové automaty a Turingov stroj 14
13.1 Abeceda 14
13.2 Stavový automat 14
13.3 Niečo o výpočtoch 14
13.4 Trochu teórie 15
13.5 Ešte raz o výpočtoch 15
13.6 Význam Turingovho stroja 15

Kapitola 1

Úvod do logiky

1.1 Výroky

Výrok je tvrdenie, ktoré možno označiť za pravdivé alebo nepravdivé. Napríklad

Vonku prší.

Existujú mimozemské civilizácie.

Obe vety predstavujú výroky, aj keď pravdivosť druhého výroku nie sme schopní posúdiť. Naproti tomu nasledujúca veta:

Nežer toľko!

nepredstavuje výrok, pretože v tomto prípade nemá zmysel uvažovať o pravdivostnej hodnote.
Vo všeobecnosti, ak výrok označíme p, tak mu môžeme priradiť pravdivostnú hodnotu 1 alebo 0, podľa toho, či ide o pravdivý alebo nepravdivý výrok.

1.2 Operácie s výrokmi

Nové výroky môžeme tvoriť z existujúcich výrokov pomocou rôznych operácií. Uvedieme niekoľko najpoužívanejších. Podrobnejší prehľad o operáciách s výrokmi poskytuje napríklad publikácia [5].

Negácia

Z každého výroku môžeme vytvoriť nový výrok vložením slova **nie**, vsunutím predpony **ne-**, alebo iným vyjadrením záporu podľa pravidiel gramatiky. Napríklad vezmime výrok:

Slovensko je majster sveta vo futbale.

Znegujeme tento (žiaľ) nepravdivý výrok:

Slovensko nie je majster sveta vo futbale.

Môžeme však povedať aj:

Nie je pravda, že Slovensko je majster sveta vo futbale.

Ak p je výrok, jeho negáciu označíme $\neg p$. Pre pravdivostné hodnoty platí:

p	$\neg p$
1	0
0	1

Pravdivostné hodnoty výrokov, ktoré vytvárame pomocou operácií možno vypočítať aj pomocou aritmetických operácií. Pre negáciu sa to dá vyjadriť nasledujúco: ak výrok p nadobúda pravdivostnú hodnotu $a \in \{0, 1\}$, potom jeho negácia $\neg p$ nadobudne pravdivostnú hodnotu $1 - a$.

Konjunkcia

Výroky môžeme spájať spojkou **a**, prípadne **a zároveň**. Napríklad

Jupiter je planéta a Slnko je hviezda.

Tento výrok je pravdivý, pretože obe jeho časti sú pravdivé.

Mars je planéta a Žilina vyhrala Ligu majstrov.

Druhá časť výroku je evidentne nepravdivá, takže celý výrok považujeme za nepravdivý.

Konjunkcia je pravdivá len v prípade, keď sú **obidve jej zložky pravdivé**. V zvyšných prípadoch je nepravdivá.
Ak p, q sú výroky, tak konjunkciu zapisujeme $p \wedge q$. Formálne môžeme pravdivostné hodnoty konjunkcie vyjadriť nasledujúcou tabuľkou:

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

Ak predpokladáme, že výrok p má pravdivostnú hodnotu $a \in \{0, 1\}$ a výrok q pravdivostnú hodnotu $b \in \{0, 1\}$, tak $p \wedge q$ nadobúda pravdivostnú hodnotu $a \cdot b$. Konjunkciu tiež nazývame logický súčin.

Disjunkcia

Výroky môžeme spájať spojkou **alebo**. V bežnom jazyku má táto spojka dva významy. Všimnime si nasledujúce dve vety.

Tento človek je slušný alebo gauner.

Ja si dám doma čaj alebo moja žena kávu.

V prvom výroku očakávame, že nastane práve jedna z uvedených možností. Spojku *alebo* chápeme v tomto prípade, ako vylučujúcu spojku. V druhom

výroku na túto spojku nemusíme pozerať, ako na vylučujúcu (pokiaľ máme doma aspoň dve šálky). Výrok bude pravdivý, ak bude splnená aspoň jedna z uvedených možností (ale mohli by aj obe naraz). V matematike (a podobne aj v informatike) sa spojka *alebo* používa len druhým spôsobom! Napríklad:

Číslo $x < 5$ alebo $x > 3$.

Ak je x rovné 4, tak sú splnené obe zložky a celý výrok je pravdivý. Disjunkcia je pravdivá, keď je **aspoň jedna jej zložka pravdivá**. Ak p, q sú výroky, tak disjunkciu zapisujeme $p \vee q$. Formálne môžeme pravdivostné hodnoty disjunkcie vyjadriť nasledujúcou tabuľkou:

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

Ak predpokladáme, že výrok p má pravdivostnú hodnotu $a \in \{0, 1\}$ a výrok q pravdivostnú hodnotu $b \in \{0, 1\}$, tak $p \vee q$ nadobúda pravdivostnú hodnotu $a+b-ab$. Disjunkciu tiež nazývame logický súčet.

Alternatíva

Niekedy je potrebné v matematike aj informatike použiť spojku **alebo** vylučujúcim spôsobom. V takomto prípade príslušný zložený výrok nazývame alternatíva. Ak p, q sú výroky, tak alternatívu zapisujeme napríklad $p \vee\vee q$ (v odbornej literatúre sa používa aj označenie XOR). Formálne môžeme pravdivostné hodnoty alternatívy vyjadriť nasledujúcou tabuľkou:

p	q	$p \vee\vee q$
1	1	0
1	0	1
0	1	1
0	0	0

Ak predpokladáme, že výrok p má pravdivostnú hodnotu $a \in \{0,1\}$ a výrok q pravdivostnú hodnotu $b \in \{0,1\}$, tak $p \vee \vee q$ nadobúda pravdivostnú hodnotu $a+b-2ab$.

Implikácia

Implikáciou sa nazýva výrok vytvorený pomocou dvojice spojok **ak ..., tak ...** (prípadne dvojicou ak ..., potom ...).

Ak prší, tak ulice sú mokré.

Pozrime sa, ako to je s pravdivostnými hodnotami implikácie. Vezmime si nasledujúci príklad.

Ak Žilina vyhrá Ligu majstrov, tak zjem kefu.

Kedy bude táto veta v mojom podaní klamstvom? Ak Žilina vyhrá Ligu majstrov a ja odmietnem zjesť tú kefu. Ak by naozaj vyhrali a ja nechcem byť považovaný za klamára, tak budem musieť tú kefu zjesť.
Čo v prípade, že Ligu majstrov nevyhrajú? V takom prípade nie je splnený predpoklad a ja sa nedopúšťam klamstva bez ohľadu na to, či mávam kefu na večeru, alebo ju zo zásady jesť odmietam. Implikácia je nepravdivá len v prípade, keď je **prvá jej zložka (podmienka) pravdivá a druhá nie**. Ak p, q sú výroky, tak implikáciu zapisujeme $p \Rightarrow q$. Formálne môžeme pravdivostné hodnoty implikácie vyjadriť nasledujúcou tabuľkou.

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

Ak predpokladáme, že výrok p má pravdivostnú hodnotu $a \in \{0,1\}$ a výrok q pravdivostnú hodnotu $b \in \{0,1\}$, tak $p \Rightarrow q$ nadobúda pravdivostnú hodnotu $1-a+ab$.

Ekvivalencia

Ekvivalencia je výrok, ktorý je vytvorený pomocou slovných spojení **... práve vtedy, keď ...** alebo **... vtedy a len vtedy, keď ...**. Príklad:

Sociálny štát vybudujeme práve vtedy, keď zdvojnásobíme platy.

Pozrime sa bližšie na pravdivostné hodnoty ekvivalencie. Tento typ výrokov funguje, ako spojenie dvoch implikácií:

($\Rightarrow$) Ak vybudujeme sociálny štát, tak zdvojnásobíme platy.

($\Leftarrow$) Ak zdvojnásobíme platy, tak vybudujeme sociálny štát.

Aby bol celý výrok pravdivý, musia byť pravdivé obe implikácie. Ak je prvá zložka výroku pravdivá, potom je pravdivá aj druhá zložka výroku. Ak je prvá zložka nepravdivá, tak nemôže byť pravdivá ani druhá zložka, pretože by to spôsobilo nepravdivosť druhej implikácie.
Ekvivalencia je pravdivá, keď majú **obidve jej zložky rovnakú pravdivostnú hodnotu**. V opačnom prípade je nepravdivá.
Ak p, q sú výroky, tak ekvivalenciu zapisujeme $p \Leftrightarrow q$. Formálne môžeme pravdivostné hodnoty ekvivalencie vyjadriť nasledujúcou tabuľkou.

p	q	$p \Leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Ak predpokladáme, že výrok p má pravdivostnú hodnotu $a \in \{0, 1\}$ a výrok q pravdivostnú hodnotu $b \in \{0, 1\}$, tak $p \Leftrightarrow q$ nadobúda pravdivostnú hodnotu $1 - a - b + 2ab$.

1.3 Negácie zložených výrokov

Negácia konjunkcie a disjunkcie

Ako sme už spomenuli, konjunkcia je pravdivá, keď **oba** výroky p a q sú pravdivé. Negácia bude teda pravdivá, ak **aspoň jeden** z nich nie je pravdivý - **aspoň pre jeden** z nich je pravdivá jeho negácia. Slovné spojenie **aspoň jeden** sa však spája s disjunkciou a logickou spojkou **alebo**. Negácia konjunkcie je teda pravdivá, ak je pravdivá negácia prvého výroku, **alebo** je pravdivá negácia druhého výroku. Formálne to môžeme vyjadriť v nasledujúcej tabuľke.

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$
1	1	1	0	0
1	0	0	1	1
0	1	0	1	1
0	0	0	1	1

Napríklad znegujme výrok:

Som hlúpy a šťastný.

Negácia vyzerá nasledujúco:

Nie som hlúpy, alebo nie som šťastný.

Podobne negujeme disjunkciu. Tá je pravdivá, keď je pravdivý **aspoň jeden** z výrokov, ktoré v nej vystupujú. Negácia bude teda pravdivá, keď sú pravdivé negácie **oboch** výrokov, ktoré v disjunkcii vystupujú. Ako sme mali možnosť sa presvedčiť, slovíčko **oboch** sa spája s konjunkciou a spojkou **a zároveň**. Negácia disjunkcie je pravdivá, ak je pravdivá negácia prvého výroku **a zároveň** je pravdivá negácia druhého výroku. Formálne

to môžeme vyjadriť v nasledujúcej tabuľke.

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p \wedge \neg q$
1	1	1	0	0
1	0	1	0	0
0	1	1	0	0
0	0	0	1	1

Napríklad znegujme výrok:

Som šťastný, alebo bohatý.

Negácia vyzerá nasledujúco:

Som nešťastný a chudobný.

Negácia implikácie

Vráťme sa k výroku o žilinských futbalistoch a mojom stravovaní.

Ak Žilina vyhrá Ligu majstrov, tak zjem kefu.

Tento výrok bude nepravdivý len v prípade, že

Žilina Ligu majstrov vyhrá **a** ja kefu nezjem.

Vidíme, že sme obe zložky spojili spojkou **a**. Prvá zložka implikácie je nezmenená, druhú zložku sme negovali. Negáciu implikácie dostaneme, ak prvú jej zložku necháme nezmenenú, druhú zložku znegujeme a zložky spojíme spojkou **a zároveň**, respektíve **a**. Nasledujúca tabuľka nám formálne opisuje spomínanú situáciu.

p	q	$p \Rightarrow q$	$\neg(p \Rightarrow q)$	$p \wedge \neg q$
1	1	1	0	0
1	0	0	1	1
0	1	1	0	0
0	0	1	0	0

Negáciu implikácie teda môžeme vyjadriť v tvare $p \wedge \neg q$. Častou chybou pri negovaní implikácie je jej prevod na tvar $p \Rightarrow \neg q$ alebo $\neg p \Rightarrow \neg q$. Napríklad

Ak Žilina vyhrá Ligu majstrov, tak nezjem kefu.

Keby náhodou Žilinčania neuspeli, tak celý tento výrok bude pravdivý, ale pravdivá bude v tomto prípade aj pôvodná implikácia, z ktorej sme vychádzali, takže toto nemôže byť negácia nášho výroku. Podobne sa dá zdôvodniť, že $\neg p \Rightarrow \neg q$ tiež nie je negáciou tejto implikácie. Aj v nasledujúcej tabuľke vidieť, že spomenuté konštrukcie výrokov nemajú opačné pravdivostné hodnoty, ako pôvodná implikácia.

p	q	$\neg p$	$\neg q$	$p \Rightarrow q$	$\neg(p \Rightarrow q)$	$p \Rightarrow \neg q$	$\neg p \Rightarrow \neg q$
1	1	0	0	1	0	0	1
1	0	0	1	0	1	1	1
0	1	1	0	1	0	1	0
0	0	1	1	1	0	1	1

1.4 Kvantifikátory

Existenčný kvantifikátor

Pozrime sa na výrok

Jano je opilec.

Toto tvrdenie vyjadruje vlastnosť istého konkrétneho objektu - nejakého konkrétneho Jana. Ak chceme vyjadriť, že túto vlastnosť môžu mať objekty z nejakého vymedzeného súboru objektov (z nejakej množiny), tak môžeme povedať

Niektorí Slováci sú opilci.

Čiže tvrdíme, že existujú objekty medzi Slovákmi, ktoré majú danú vlastnosť. Toto tvrdenie je pravdivé, ak aspoň jeden Slovák túto vlastnosť má.

Slová *niektorí, existujú, aspoň jeden* sa používajú v existenčných tvrdeniach a nazývame ich pri tomto použití aj existenčné kvantifikátory. V matematickom zápise používame na vyjadrenie existenčného kvantifikátora znak $\exists$. Napríklad

$$\exists x \in N \;\; x < 3 \, .$$

Ak to chceme preložiť z jazyka matematických symbolov do bežného jazyka, ktorým hovoríme, toto tvrdenie bude znieť:

Existuje také prirodzené číslo, ktoré je menšie, ako tri.

Ak máme množinu A a chceme vyjadriť tvrdenie, že niektoré prvky x tejto množiny majú vlastnosť $P(x)$, formálne to môžeme zapisovať:

$$\exists x \in A \;\; P(x) \, .$$

Pravdivosť existenčného tvrdenia dokážeme, ak nájdeme prvok s touto vlastnosťou, alebo nepriamo ukážeme, že tento prvok musí existovať.

Všeobecný kvantifikátor

Iným typom je všeobecné tvrdenie, ktoré hovorí, že všetky objekty z nejakého vymedzeného súboru objektov (z nejakej množiny) majú danú vlastnosť.

Každý človek má v sebe niečo dobré.

Vo všeobecných tvrdeniach sa na vyjadrenie množstva používajú najčastejšie slová *každý, všetci*. Hovoríme im aj všeobecné kvantifikátory. V matematickom zápise používame na vyjadrenie všeobecného kvantifikátora znak $\forall$. Napríklad

$$\forall x \in R \;\; x^2 \geq 0 \, .$$

Preložené do nášho jazyka

Všetky reálne čísla majú druhú mocninu väčšiu, alebo rovnú nule.

Ak chceme vyjadriť tvrdenie, že každý prvok x množiny A má vlastnosť $P(x)$, formálne to zapisujeme

$$\forall x \in A \;\; P(x) \; .$$

Ak chceme dokázať pravdivosť všeobecného tvrdenia, musíme dokázať, že všetky prvky spĺňajú danú vlastnosť.

Negácie

Pozrime sa na všeobecné tvrdenie

Všetky jablká sú červené.

Ak chceme dokázať, že nie je pravdivé (čiže platí jeho negácia), stačí nájsť aspoň jedno jablko, ktoré túto vlastnosť nespĺňa. Negácia tohto výroku teda bude

Niektoré jablká nie sú červené.

Čo sme pri negovaní urobili? Zmenili sme všeobecný kvantifikátor na existenčný a negovali sme vlastnosť. Formálne to môžeme zapísať

$$\neg(\forall x{\in}A \;\; P(x)) \Leftrightarrow (\exists x{\in}A \;\; \neg P(x)) \; .$$

Čiže negácia všeobecného tvrdenia je ekvivalentná s tvrdením, že existuje v A prvok, ktorý nemá vlastnosť $P(x)$.

Vezmime si existenčné tvrdenie

Niektorí profesori sú holohlaví.

Ak by sme chceli dokázať, že nie je pravdivé, museli by sme dokázať, že

Všetci profesori majú vlasy.

Čiže sme zmenili existenčný kvantifikátor na všeobecný a vlastnosť sme negovali. Formálne to môžeme zapísať

$$\neg(\exists x{\in}A \;\; P(x)) \Leftrightarrow (\forall x{\in}A \;\; \neg P(x)) \; .$$

Kapitola 2

Množiny

V tejto kapitole sa nebudeme venovať priamo teórii množín, len si priblížime základnú terminológiu a značenie, pretože tie sa využívajú aj v iných oblastiach matematiky. (Kto by mal záujem dozvedieť sa z danej problematiky viac, tomu odporúčame napríklad publikácie [23, 1]).

2.1 Základné pojmy

Čo môžeme považovať za množinu? Napríklad všetci študenti zapísaní do prvého ročníka tvoria množinu. Všetky prirodzené čísla tvoria množinu, čo môžeme zapísať $\{1, 2, 3, \dots\}$. Alebo $\{3, 6, 7\}$ je množina tvorená číslami $3, 6, 7$.

Množina je teda súhrn (súbor) určitých dobre rozlíšiteľných objektov, ktoré považujeme za jeden celok.[8]

Predchádzajúci výrok mal za úlohu trochu priblížiť pojem množiny, ale nemožno ho považovať za definíciu, pretože umožňuje rôzne paradoxy a protirečenia. Na začiatku 20. storočia prišli matematici Bertrand Russell (1872-1970), Ernst Zermelo (1871-1953) a niektorí ďalší so sériou paradoxov, ktoré poukázali na potrebu poriadneho definovania pravidiel, pomocou ktorých by bolo možné množiny definovať a pracovať s nimi. Jeden z týchto

paradoxov možno nájsť v knižke [24].

Príklad 2.1.1. *Jednému vojakovi prikázali holiť tých a len tých vojakov jeho čaty, ktorí sa neholia sami. Ako sa má tento vojak zachovať k sebe, ak vojenské predpisy prikazujú, že každý vojak musí byť oholený?*

Čatu môžeme považovať za množinu vojakov. Rozdeľme ju na dve časti, na vojakov, ktorí sa holia sami a na vojakov, ktorí sa neholia sami. Do ktorej skupiny zaradiť nášho holiča? Ak by bol medzi vojakmi, ktorí sa holia sami, tak by sám seba podľa nariadenia nemal oholiť, a teda by sa neholil sám. Ak by bol v skupine vojakov, ktorí sa neholia sami, tak by mal sám seba oholiť, a teda by nebol v skupine, ktorá sa neholí sama. Ak teda chceme vytvoriť množinu vojakov tejto čaty, ktorí sa holia sami, o našom holičovi nevieme povedať, či do nej patrí, ani či do nej nepatrí.

Aby sa matematika vyhla podobným nepríjemnostiam, matematici vypracovali systémy axióm, z ktorých sa dajú odvodiť pravidlá na vytváranie „slušne" sa správajúcich množín. Zrejme najpoužívanejší je Zermelo-Fraenkelov axiomatický systém, ktorý uvedieme na záver tejto kapitoly.

Značenie a základná terminológia

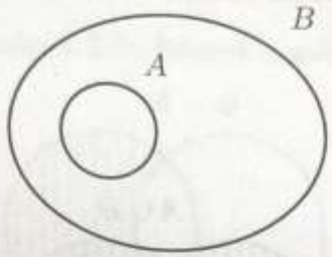
Na vymedzenie množiny používame množinové zátvorky: $\{\dots\}$. Medzi zátvorkami môžeme vymenovať prvky danej množiny alebo uviesť charakteristickú vlastnosť prvkov tejto množiny. Treba si tiež uvedomiť, že pri množinách nezáleží na poradí, v akom vypíšeme ich prvky, ani koľkokrát tie prvky vypíšeme: $\{1,2,3\} = \{2,1,3\} = \{3,2,1\} = \{1,2,3,3\}$. Ak prvok x patrí do množiny A, tak píšeme $x \in A$, v opačnom prípade $x \notin A$. Znakom $\emptyset$ značíme prázdnu množinu. Počet prvkov množiny A označíme $|A|$. Pri nekonečných množinách budeme miesto počtu prvkov používať pojem mohutnosť množiny, čo budeme značiť tiež $|A|$.

Rovnosť množín

Množiny A a B sa rovnajú ($A = B$), ak majú tie isté prvky.

Podmnožiny

Množina A je podmnožinou množiny B, ak každý prvok množiny A je aj prvkom množiny B. Značíme to $A \subseteq B$. Platí tiež $\emptyset \subseteq B$ a $B \subseteq B$. Ak chceme zdôrazniť, že množina A je rôzna od B (hovoríme, že A je vlastná podmnožina množiny B), tak používame zápis $A \subset B$.



Obrázok 2.1: Podmnožina množiny

2.2 Ako možno vytvárať množiny

Pozrime sa na niekoľko spôsobov, ako možno vytvárať množiny. Pri konečných množinách s malým počtom prvkov nám stačí tie prvky vymenovať. Ďalší spôsob je pomocou charakteristickej vlastnosti. Napríklad interval $(-\infty, 1)$ môžeme zapísať aj $A = \{x \in R | x < 1\}$, čo znamená, že prvky tejto množiny sú všetky reálne čísla, ktoré sú mešie ako 1. Pri definovaní množiny pomocou charakteristickej vlastnosti treba byť opatrný, aby sme nedopadli ako náš armádny holič. Ukážeme si ďalšie spôsoby vytvárania nových množín.

Množina všetkých podmnožín

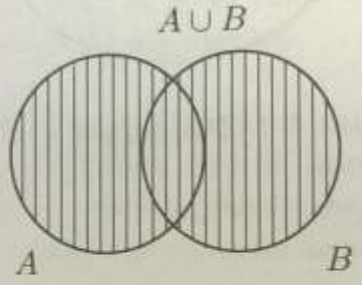
Ak máme množinu A, tak zo všetkých jej podmnožín môžeme vytvoriť množinu $P(A) = \{\emptyset, \ldots, A\}$, ktorú tiež nazývame potenčná množina množiny

A.

Príklad 2.2.1. *Ak $A = \{1, 2\}$, tak zo všetkých podmnožín tejto množiny môžeme vytvoriť potenčnú množinu $P(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.*

Otázka. Ak A je konečná množina, koľko prvkov obsahuje $P(A)$? Čiže koľko podmnožín má konečná množina? (Odpoveď možno nájsť na strane 113.)

Zjednotenie



Obrázok 2.2: Zjednotenie množín

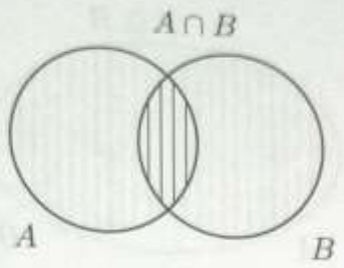
Zjednotenie $A \cup B$ množín A a B obsahuje práve tie prvky, ktoré patria do množiny A **alebo** B. Všimnime si spojku alebo. Tá nám hovorí, že zjednotenie je definované pomocou disjunkcie. Pre ľubovoľný prvok x platí:

$$x \in A \cup B \iff (x \in A \vee x \in B)\,.$$

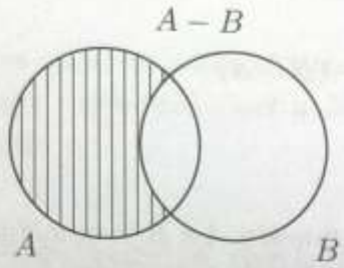
Prienik

Prienik $A \cap B$ množín A a B obsahuje práve tie prvky, ktoré patria do množiny A **a zároveň** B. Podľa spojky a zároveň vieme, že prienik sa dá definovať pomocou konjunkcie. Pre ľubovoľný prvok x platí:

$$x \in A \cap B \iff (x \in A \wedge x \in B)\,.$$



Obrázok 2.3: Prienik množín



Obrázok 2.4: Rozdiel množín

Rozdiel

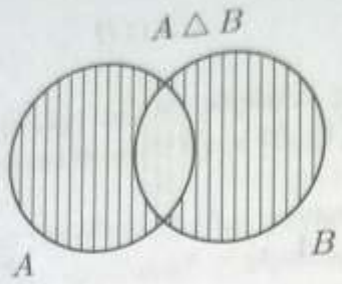
Rozdiel $A - B$ množín A a B obsahuje práve tie prvky, ktoré patria do množiny A **a zároveň** nepatria do B. Podobne ako prienik, aj rozdiel množín možno definovať pomocou konjunkcie. Druhú časť výroku však musíme negovať. Pre ľubovoľný prvok x platí:

$$x \in A - B \iff [x \in A \wedge \neg(x \in B)] \iff (x \in A \wedge x \notin B)\ .$$

Symetrická diferencia

Symetrická diferencia $A \triangle B$ množín A a B obsahuje tie prvky, ktoré patria práve do jednej z množín A, B. Symetrickú diferenciu možno vyjadriť viacerými spôsobmi pomocou predchádzajúcich operácií. Napríklad:

1. $A \triangle B = (A - B) \cup (B - A)$,



Obrázok 2.5: Symetrická diferencia množín

2. $A \triangle B = (A \cup B) - (B \cap A)$.

Karteziánsky súčin

Karteziánsky súčin $A \times B$ množín A a B je množina všetkých usporiadaných dvojíc, kde prvý prvok dvojice je z množiny A a druhý prvok tejto dvojice je z množiny B. Čiže

$$A \times B = \{(x, y) | x \in A, y \in B\} .$$

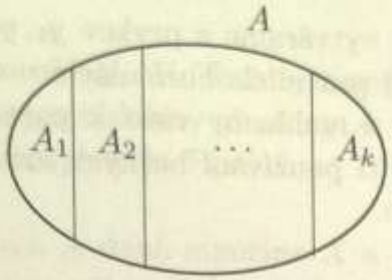
Príklad 2.2.2. *Nech* $A = \{1, 2\}$, $B = \{x, y\}$. *Potom*

- $A \times B = \{(1, x), (1, y), (2, x), (2, y)\}$,
- $A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$.

Rozklad množiny

Množiny $A_1, A_2, \ldots, A_k$ tvoria rozklad množiny A, ak $A = A_1 \cup A_2 \cup \cdots \cup A_k$ a zároveň pre $\forall i, j \in \{1, \ldots, k\}$ $(i \neq j)$ platí $A_i \cap A_j = \emptyset$.

Príklad 2.2.3. *Ak* $A = \{1, 2, 3, 4, 5\}$. *Tak množiny* $A_1 = \{1, 2\}$, $A_2 = \{3\}$ *a* $A_3 = \{4, 5\}$ *tvoria rozklad množiny* A. *Iný rozklad tejto množiny je daný množinami* $B_1 = \{1, 2\}$, $B_2 = \{3, 4\}$ *a* $B_3 = \{5\}$.



Obrázok 2.6: Rozklad množiny A

Príklad 2.2.4. *Vezmime si množinu všetkých prirodzených čísel N. Potom jej podmnožiny N_n všetkých nepárnych čísel a N_p všetkých párnych čísel tvoria rozklad tejto množiny.*

2.3 Rekurzívne definované množiny

Rekurzívne definované množiny sú príkladom rekurzívne definovaných dátových typov, kde nové prvky definujeme pomocou prvkov, ktoré sme definovali v predchádzajúcich krokoch. Začnime príkladom, ktorý je pôvodne uvedený v [17].
Definujme množinu A nasledujúco:

1. základný krok definície: $0 \in A$
2. konštrukčné kroky: ak $n \in A \Rightarrow (-n \in A \wedge n+2 \in A)$.

Prvky množiny A sú nasledujúce: 0, 2, −2, 4, −4, ... Nie je ťažké si uvedomiť, že A je množina všetkých párnych celých čísel. Množina A je definovaná rekurzívne. Vo všeobecnosti je konštrukcia takýchto množín nasledujúca:

1. základný krok definície: $x_1, x_2, \ldots, x_k \in A$,
2. konštrukčné kroky: ak $y_1, y_2, \ldots, y_l \in A \Rightarrow z_1, z_2, \ldots, z_m \in A$,

kde prvky $z_1, z_2, \ldots, z_m$ vytvárame z prvkov $y_1, y_2, \ldots, y_l$ pomocou pevne daných (matematických) pravidiel. Formulácia o vytváraní nových prvkov množiny A je nepresná a mohla by viesť k paradoxom podobným tomu o armádnom holičovi. Pri používaní bežných aritmetických operácií však problémy mať nebudeme.

2.4 Doplnok: Zermelov-Fraenkelov systém axióm

Na ukážku uvádzame Zermelov-Fraenkelov systém axióm (Abraham Fraenkel 1891-1965). Pomocou týchto axióm možno odvodiť všetku matematiku, s ktorou sa bežne stretávate. Treba však poznamenať, že toto odvodzovanie môže byť veľmi komplikované. Keby sme chceli odvodiť z týchto axióm, že $2 + 2 = 4$, potrebovali by sme na to niekoľko tisíc krokov. (Viac možno nájsť v [17] a [19].)

Axióma rovnosti množín. Dve množiny sa rovnajú práve vtedy, keď majú tie isté prvky. Formálne to môžeme zapísať takto:

$$\forall A\ \forall B\ [(\forall x(x \in A \Longleftrightarrow x \in B)) \Longleftrightarrow (A = B)]$$

Axióma zjednotenia množín. Nech S je množina (systém množín). Potom existuje taká množina Z, ktorá obsahuje práve tie prvky, ktoré patria aspoň do jednej množiny systému S.

$$\forall S\ \exists Z\ \forall x\ [x \in Z \Longleftrightarrow (\exists A \in S\ \ x \in A)]$$

Množinu Z nazývame zjednotenie množín systému S.

Axióma dvojprvkovej množiny. Pre každé dve množiny x a y existuje množina $\{x, y\}$, ktorej jedinými prvkami sú x a y.

Axióma nekonečnej množiny. Existuje nekonečná množina. Môžeme ju definovať napríklad takto: nech X je neprázdna množina taká, že pre $\forall y \in X$ aj množina $\{y\}$ je prvkom X.

Axióma potenčnej množiny. Ku každej množine A existuje množina, ktorej prvkami sú všetky podmnožiny množiny A. Táto množina sa nazýva potenčná množina a označujeme ju $P(A)$.

Schéma separácie. Nech je daná množina X a výroková funkcia F. Potom existuje podmnožina množiny X, ktorá obsahuje práve tie prvky $y \in X$, pre ktoré je výrok $F(y)$ pravdivý.

Schéma nahradenia. Obrazom množiny pri zobrazení je opäť množina.

Axióma fundovanosti. Pre každú neprázdnu množinu X platí, že obsahuje aspoň jeden prvok $Y \in X$ taký, že $X \cap Y = \emptyset$. (Táto axióma zabraňuje napríklad existencii množiny, ktorá obsahuje samu seba ako svoj prvok.)

Axióma výberu. Nech S je neprázdny systém navzájom disjunktných množín. Potom existuje taká množina H, že pre každú množinu $A \in S$ je $H \cap A$ jednoprvková množina.

Kapitola 3

Čísla a číselné množiny

3.1 Prirodzené čísla

Prirodzené čísla $N = \{1, 2, 3, \dots\}$ boli prvé čísla, ktoré sa v histórii ľudstva objavili. Odhaduje sa, že to mohlo byť niekedy v období pred 12000 rokmi. Bežne ich používame na označenie počtu objektov alebo na určenie poradia. Počas histórie sa objavilo mnoho spôsobov, ako zapisovať čísla. Od najstarších spôsobov, čo boli zárezy do dreva a do kosti (kde počet zárezov zodpovedal napríklad počtu ulovených zvierat), cez grécke a rímske zapisovanie čísel, až po dnešné zapisovanie čísel pomocou pozičných sústav.

Zápis prirodzených čísel v rôznych pozičných sústavách

Číselná sústava sa nazýva pozičnou sústavou, ak výsledné číslo závisí od pozície cifier. Dnes najviac používame zápis čísla v desiatkovej sústave. Vezmime napríklad nasledujúce číslo zapísané v desiatkovej sústave

$$563014 = 5{\cdot}10^5 + 6{\cdot}10^4 + 3{\cdot}10^3 + 0{\cdot}10^2 + 1{\cdot}10^1 + 4{\cdot}10^0 \ .$$

Pre číslo x s ciframi $a_k a_{k-1} \dots a_2 a_1 a_0$ dostávame

$$x = a_k{\cdot}10^k + a_{k-1}{\cdot}10^{k-1} + \dots + a_2{\cdot}10^2 + a_1{\cdot}10^1 + a_0{\cdot}10^0 \ ,$$

kde $a_i \in \{0, \ldots, 9\}$ je cifra daného čísla a túto číslicu násobíme príslušnou mocninou čísla desať.

Okrem číselnej sústavy so základom desať sa používajú napríklad dvojková, osmičková, šestnástková a jedenástková sústava.

V dvojkovej sústave používame na zápis čísel len číslice 0, 1 a tieto číslice násobíme mocninou čísla dva.

V šestnástkovej sústave potrebujeme na zápis čísla 16 číslic, takže okrem číslic $0, 1, \ldots, 9$ používame aj znaky A, B, C, D, E, F, kde znaku A zodpovedá hodnota 10, znaku B zodpovedá hodnota 11, ... , znaku F zodpovedá hodnota 15.

V jedenástkovej sústave, ktorá sa používa v kódovaní, potrebujeme na zápis čísla 11 číslic. Sú to $0, 1, \ldots, 9, X$, kde X zodpovedá hodnote 10. Napríklad každá kniha má priradený ISBN kód. Posledná (kontrolná) číslica tohto kódu je číslica v jedenástkovej sústave s hodnotou od 0 do X.

Číslo, ktoré je v pozičnej sústave so základom z reprezentované postupnosťou cifier $(a_k a_{k-1} \ldots a_2 a_1 a_0)_z$ nadobúda hodnotu

$$x = a_k \cdot z^k + a_{k-1} \cdot z^{k-1} + \cdots + a_2 \cdot z^2 + a_1 \cdot z^1 + a_0 \cdot z^0 .$$

Príklad 3.1.1. *Číslo, ktoré má v desiatkovej sústave tvar*

$$2589 = 2 \cdot 10^3 + 5 \cdot 10^2 + 8 \cdot 10 + 9 ,$$

možno v šestnástkovej sústave zapísať $(A1D)_{16}$, *pretože*

$$2589 = 10 \cdot 16^2 + 1 \cdot 16 + 13 .$$

Do dvojkovej sústavy možno toto číslo prepísať takto

$$2589 = 2^{11} + 2^9 + 2^4 + 2^3 + 2^2 + 2^0 = (101000011101)_2 .$$

V jedenástkovej sústave to je

$$2589 = 1 \cdot 11^3 + 10 \cdot 11^2 + 4 \cdot 11 + 4 = (1X44)_{11} .$$

Kódovanie prirodzených čísel v počítači

Základný fakt, ktorý si pri reprezentácii čísel v počítači musíme uvedomiť je, že na uloženie čísla máme vyhradený fixný priestor. Na reprezentáciu čísla môžeme použiť napríklad 8 bitov, 16 bitov atď. To znamená, že pri 8 bitovej reprezentácii môžeme zapísať $2^8 = 256$ čísel (na každú pozíciu máme na výber dve možnosti: 0 alebo 1) v rozsahu od $0 = (00000000)_2$ do $255 = (11111111)_2$ a pri n bitovej reprezentácii 2^n čísel v rozsahu od 0 do $2^n - 1$.

Pozrime sa, ako fungujú aritmetické operácie pri takejto reprezentácii. Sčítajme napríklad nasledujúce dve osembitové čísla

$$(00101110)_2 + (10001101)_2 = (10111011)_2 \ ,$$

čo korešponduje so súčtom $46+141 = 187$. Vezmime teraz súčet čísel $255+1$ v dvojkovej sústave:

$$(11111111)_2 + (00000001)_2 = (100000000)_2 \ .$$

Ak máme 8-bitovú reprezentáciu čísel, tak výsledok súčtu bude 8-bitové číslo $(00000000)_2 = 0$ (väčšina softvéru však má túto situáciu ošetrenú a upozorní, že sme mimo daného číselného typu). V počítači teda funguje aritmetika trochu inak, ako sme zvyknutí. Pohybujeme sa akoby po kružnici. Viac o kódovaní prirodzených čísel v počítači možno nájsť v [15].

Matematická indukcia

Množinu prirodzených čísel N možno definovať rekurzívne nasledujúcim spôsobom:

1. základný krok definície: $1 \in N$
2. konštrukčné kroky: ak $n \in N \Rightarrow n + 1 \in N$.

Intuícia nám hovorí (a v tomto prípade nás nesklame), že takto možno generovať každý prvok množiny prirodzených čísel. Tento fakt možno využiť ako

jednu z metód dokazovania. Ide o princíp matematickej indukcie. Ukážme si na príklade, ako to funguje.

Príklad 3.1.2. *Nech A je množina všetkých takých prirodzených čísel k, pre ktoré platí rovnosť*

$$1+2+\cdots+k=\frac{k(k+1)}{2}. \tag{3.1}$$

Keďže $1=1\cdot(1+1)/2$, tak $1\in A$. Predpokladajme teraz, že prirodzené číslo $n\in A$, čiže pre toto číslo platí

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

Potom dostávame:

$$\begin{aligned}1+2+\cdots+n+(n+1) &= \frac{n(n+1)}{2}+(n+1)\\ &= \frac{n(n+1)+2(n+1)}{2}\\ &= \frac{(n+1)(n+2)}{2},\end{aligned}$$

čiže pre $n+1$ dostávame

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

z čoho vyplýva, že $n+1\in A$.

Zhrňme si teda fakty o množine A:

1. $1\in A$,
2. *ak prirodzené číslo $n\in A$, potom aj $n+1\in A$,*

ale to znamená, že množina A je definovaná rekurzívne rovnakým spôsobom ako množina prirodzených čísel, takže $A=N$ a rovnosť (3.1) platí pre všetky prirodzené čísla.

Sformulujme to teraz ako metódu dôkazu [6]:

1. Dokázali sme, že rovnosť (3.1) platí pre $n = 1$.
2. Predpokladali sme, že vlastnosť (3.1) platí pre nejaké prirodzené číslo n (indukčný predpoklad) a z toho sme odvodili, že rovnosť (3.1) musí platiť aj pre prirodzené číslo $n + 1$.

Potom uvedená vlastnosť musí platiť pre všetky prirodzené čísla.

Príklad 3.1.3. *Dokážeme, že*

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2 \ . \tag{3.2}$$

(Napríklad $1 + 3 = 2^2$, alebo $1 + 3 + 5 = 3^2$.) Pre $n = 1$ táto rovnosť platí, pretože $1 = 1^2$. Predpokladajme, že pre nejaké $n \in N$ rovnosť (3.2) platí. Potom pre $n + 1$ dostávame:

$$1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) = n^2 + 2n + 1 = (n + 1)^2 \ .$$

Ak rovnosť (3.2) platí pre prirodzené číslo n, tak platí aj pre $n + 1$. Potom musí platiť pre všetky prirodzené čísla.

3.2 Celé čísla

Kódovanie celých čísel v počítači

Ak chceme reprezentovať v počítači aj záporné čísla, budeme potrebovať o danom čísle informáciu navyše - jeden bit si musíme vyhradiť pre informáciu o znamienku daného čísla. Ak máme n-bitové čísla, najvyšší bit je znamienkový, kde 0 zodpovedá znamienku plus a 1 znamienku mínus. Zvyšných $n - 1$ bitov sa použije na zápis čísla.

Prvá možnosť, ktorá nás pri kódovaní záporných čísel napadne je zrejme **priamy kód**:
vyjadríme najprv absolútnu hodnotu čísla pomocou $n - 1$ bitov a najvyšší (znamienkový) bit zvolíme 1. Napríklad $49 \rightarrow (00110001)_2$ a $-49 \rightarrow$

$(10110001)_2$. Nevýhodou tejto reprezentácie je, že v nej nefungujú základné aritmetické operácie. Sčítajme napríklad čísla -49 a 9 v tejto reprezentácii:

$$(10110001)_2 + (00001001)_2 = (10111010)_2 \ ,$$

kde $(10111010)_2 = -58$.

Z tohto dôvodu sa hľadala reprezentácia celých čísel, ktorá bude zachovávať základné aritmetické operácie. Túto vlastnosť spĺňa **doplnkový kód** (niekde sa nazýva dvojkový doplnok, v angličtine two's complement). Kladné číslo v tomto kóde kódujeme rovnako, ako v priamom kóde, kde najvyšší bit má hodnotu 0 (znamienko plus) a zvyšných $n-1$ bitov obsahuje dvojkový zápis tohto čísla. Záporné číslo vytvoríme tak, že všetky 0 (aj v znamienkovom bite) zmeníme na 1, všetky 1 na 0 a k tomuto číslu pripočítame 1.

Príklad 3.2.1.

$$\begin{array}{rcccccccr}
49 & = & (00110001)_2 & \longrightarrow & (11001110)_2 & \longrightarrow & (11001111)_2 & = & -49 \\
40 & = & (00101000)_2 & \longrightarrow & (11010111)_2 & \longrightarrow & (11011000)_2 & = & -40 \\
127 & = & (01111111)_2 & \longrightarrow & (10000000)_2 & \longrightarrow & (10000001)_2 & = & -127 \\
0 & = & (00000000)_2 & \longrightarrow & (11111111)_2 & \longrightarrow & (00000000)_2 & = & 0
\end{array}$$

Sčítajme -49 a 9 v tomto kódovaní:

$$(11001111)_2 + (00001001)_2 = (11011000)_2 \ ,$$

ale $(11011000)_2$ je v doplnkovom kóde -40.

Sčítajme -1 a 1. Pri súčte

$$(11111111)_2 + (1)_2 = (100000000)_2$$

si musíme uvedomiť, že na reprezentáciu používame obmedzený počet bitov (v príklade len osem) a v tejto reprezentácii daný súčet vyzerá nasledujúco:

$$(11111111)_2 + (00000001)_2 = (00000000)_2 \ .$$

Problémy kódovania v doplnkovom kóde súvisia podobne ako pri prirodzených číslach s obmedzeným rozsahom. Vezmime súčet $127 + 2$:

$$(01111111)_2 + (00000010)_2 = (10000001)_2 \ ,$$

ale $(10000001)_2 = -127$.

Čiže platí niečo podobné, ako sme spomenuli pri prirodzených číslach. Ak sa dostaneme mimo rozsahu, aritmetické operácie nefungujú. V kapitole venovanej teórii čísel sa vrátime k tomu, prečo sa začal používať doplnkový kód a s akou aritmetikou to vlastne počítač pracuje. Ďalšie informácie možno nájsť napríklad v [15].

3.3 Racionálne čísla

Prvé zmienky o racionálnych číslach možno nájsť už v starovekom Egypte a Mezopotámii. Racionálne čísla sú čísla, ktoré vieme zapísať v tvare zlomku $\frac{a}{b}$, kde $a, b \in Z$, $b \neq 0$. Množinu všetkých racionálnych čísel označujeme Q.

Zápis racionálnych čísel v rôznych pozičných sústavách

Zoberme racionálne číslo 3/8. Desatinný rozvoj tohto čísla je $0,375 = 3{\cdot}10^{-1} + 7{\cdot}10^{-2} + 5{\cdot}10^{-3}$. Skúsme ho zapísať v dvojkovej sústave. Musíme toto číslo previesť na tvar

$$a_1{\cdot}2^{-1} + a_2{\cdot}2^{-2} + a_3{\cdot}2^{-3} + \cdots \ ,$$

kde $a_i \in \{0, 1\}$. V tomto prípade máme

$$0,375 = 0{\cdot}2^{-1} + 1{\cdot}2^{-2} + 1{\cdot}2^{-3} = (0,011)_2 \ .$$

Ukážme si postup, pomocou, ktorého môžeme nájsť zápis čísla $z \in (0, 1)$ v dvojkovej sústave. Predpokladajme, že $z = a_1{\cdot}2^{-1} + a_2{\cdot}2^{-2} + a_3{\cdot}2^{-3} +$

$a_4 \cdot 2^{-4} + \dots$. Potrebujeme zistiť hodnotu číslic $a_1, a_2, a_3, \dots$. Vynásobme z číslom dva:

$$2z = a_1 \cdot 2^0 + a_2 \cdot 2^{-1} + a_3 \cdot 2^{-2} + a_4 \cdot 2^{-3} + \dots .$$

Číslica a_1 sa teda dostala pred desatinnú čiarku a nie je ťažké ju zistiť. Vezmime teraz číslo

$$z_1 = a_2 \cdot 2^{-1} + a_3 \cdot 2^{-2} + a_4 \cdot 2^{-3} + \dots .$$

(Číslo z_1 dostaneme z čísla $2z$ tak, že berieme do úvahy len časť za desatinnou čiarkou.) Vynásobme z_1 číslom dva:

$$2z_1 = a_2 \cdot 2^0 + a_3 \cdot 2^{-1} + a_4 \cdot 2^{-2} + \dots .$$

Vidíme, že číslica a_2 sa dostala pred desatinnú čiarku a ľahko ju zistíme. Takto môžeme postupovať ďalej a číslice $a_3, a_4, \dots$ postupne posúvať pred desatinnú čiarku až pokiaľ nedostaneme za desatinnou čiarkou nulu alebo nezistíme, že sa číslice periodicky opakujú (v najhoršom prípade si povieme, že nás to už nebaví a výpočet ukončíme). Ukážme si to na príkladoch.

Príklad 3.3.1. *Preveďme číslo $z = 0,625$ do dvojkovej sústavy.*

$$\begin{array}{lllllllll}
z & = & 0,625 & 2z & = & 1,25 & \longrightarrow & a_1 & = & 1 \\
z_1 & = & 0,25 & 2z_1 & = & 0,5 & \longrightarrow & a_2 & = & 0 \\
z_2 & = & 0,5 & 2z_2 & = & 1,0 & \longrightarrow & a_3 & = & 1 \\
z_3 & = & 0,0 & & & & & & &
\end{array}$$

Čiže $0,625 = (0,101)_2$.

Zapíšme teraz číslo $0,1$ *do dvojkovej sústavy.*

$$\begin{array}{lllllllll}
z & = & 0,1 & 2z & = & 0,2 & \longrightarrow & a_1 & = & 0 \\
z_1 & = & 0,2 & 2z_1 & = & 0,4 & \longrightarrow & a_2 & = & 0 \\
z_2 & = & 0,4 & 2z_2 & = & 0,8 & \longrightarrow & a_3 & = & 0 \\
z_3 & = & 0,8 & 2z_3 & = & 1,6 & \longrightarrow & a_4 & = & 1 \\
z_4 & = & 0,6 & 2z_4 & = & 1,2 & \longrightarrow & a_5 & = & 1 \\
z_5 & = & 0,2 & 2z_5 & = & 0,4 & \longrightarrow & a_6 & = & 0 \\
 & & & & & \dots & & & &
\end{array}$$

Celý postup sa bude ďalej opakovať, takže $0,1 = (0,0\overline{0011})_2$.

To znamená, že číslo 0,1 je vyjadrené v dvojkovej sústave nekonečným periodickým zápisom a dôsledok tohto faktu je, že ani takéto číslo nevieme v počítači presne reprezentovať.

3.4 Reálne čísla

Už Gréci v staroveku prišli na to, že existujú čísla, ktoré nie sú racionálne. Napríklad číslo $\sqrt{2}$ (veľkosť uhlopriečky štvorca so stranou 1) nevieme zapísať v tvare zlomku $\frac{a}{b}$. Sformulujme to ako tvrdenie a dokážme ho.

Veta 3.4.1. *Číslo $\sqrt{2}$ nie je racionálne číslo.*

Dôkaz. (Sporom.) Predpokladajme, že platí negácia tohto tvrdenia, čiže $\sqrt{2}$ je racionálne číslo: $\sqrt{2} = \frac{a}{b}$, kde $a, b \in Z$, $b \neq 0$. Predpokladajme, že zlomok $\frac{a}{b}$ je už upravený na základný tvar. Potom $2 = \frac{a^2}{b^2}$ a $a^2 = 2b^2$. Čiže a^2 je párne číslo. Odtiaľ dostávame, že a je tiež párne číslo. (Ak by nebolo, aj a^2 by bolo nepárne.) Potom existuje $x \in N$ také, že $a = 2x$, $a^2 = 4x^2 = 2b^2$ a tiež $b^2 = 2x^2$. Podobne ako pre a platí, že b musí byť párne. Čiže existuje $y \in N$ také, že $b = 2y$. To je v spore s predpokladom, že $\frac{a}{b}$ je zlomok v základnom tvare, pretože sa dá zjednodušiť dvojkou:

$$\frac{a}{b} = \frac{2x}{2y}.$$

(Mohli by sme si povedať, že $\frac{a}{b}$ síce nie je v základnom tvare, ale $\frac{x}{y}$ už áno. Podobnými úvahami by sme dospeli k tomu, že aj $\frac{x}{y}$ sa dá zjednodušiť dvojkou a takto by to mohlo pokračovať do nekonečna.) Takže musí platiť pôvodné tvrdenie, že $\sqrt{2}$ nie je racionálne číslo.

Ukázalo sa teda, že racionálne čísla nepostačujú, ale historicky to bola ešte dlhá cesta k zavedeniu reálnych čísel. Ďalšie zaujímavosti sa čitateľ môže

dozvedieť napríklad v [14, 2]. Množinu všetkých reálnych čísel označujeme R. Každé reálne číslo vieme zapísať pomocou desatinného rozvoja. Ak je jeho rozvoj za desatinnou čiarkou konečný, alebo nekonečný, periodicky sa opakujúci, tak ide o spomínané racionálne čísla. Ak je desatinný rozvoj tohto čísla nekonečný neperiodický (napríklad $\sqrt{2}$, π), tak hovoríme o číslach iracionálnych.

Kódovanie reálnych čísel v počítači

Hneď na úvod si musíme uvedomiť, že naše možnosti sú veľmi obmedzené a v skutočnosti vieme v počítači reprezentovať len podmnožinu množiny racionálnych čísel. Poznáme dva základné spôsoby ich kódovania: kódovanie v pevnej rádovej čiarke a kódovanie v pohyblivej rádovej čiarke. (Viac možno nájsť v [15].)

1. Pri kódovaní v pevnej rádovej čiarke máme na reprezentáciu celej aj zlomkovej časti čísla pevný počet bitov (povedzme s bitov pre celú a t bitov pre zlomkovú časť). Číslo x potom môžeme vyjadriť zápisom

$$(a_{s-1}a_{s-2}\ldots a_1a_0, a_{-1}a_{-2}\ldots a_{-t})_2 \ ,$$

kde $a_i \in \{0,1\}$, čo predstavuje hodnotu:

$$x = \sum_{i=-t}^{s-1} a_i \cdot 2^i \ .$$

2. Pri kódovaní v pohyblivej rádovej čiarke používame nasledujúce vyjadrenie čísel: $x = m \cdot 2^e$, kde číslo m sa nazýva mantisa a je z intervalu $\langle \frac{1}{2}, 1)$, e sa nazýva exponent a je to celé číslo. Na kódovanie takéhoto čísla potrebujeme s bitov na vyjadrenie čísla m (prvá číslica je vždy 1, takže sa neukladá a jeden bit je znamienkový) a t bitov na vyjadrenie e, ako celého čísla.

3.5 Komplexné čísla

Vieme, že rovnica $x^2 = -1$ nemá riešenie v reálnych číslach, pretože druhá mocnina každého reálneho čísla je väčšia alebo rovná nule. Pri niektorých výpočtoch (konkrétne pri riešení kubických rovníc) sa však ukázalo, že by mohlo byť užitočné, keby sme existenciu riešení rovníc tohto typu pripustili. Dôležitým momentom bolo, keď sa o $\sqrt{-1}$ začalo uvažovať ako o čísle. Toto číslo značíme i. Je jasné, že $\sqrt{-1} = i$ nie je reálne číslo. Toto číslo nazveme imaginárna jednotka. Pomocou nej môžeme konštruovať komplexné čísla - teda čísla, ktoré sa dajú zapísať v tvare $a + b{\cdot}i$, kde $a, b \in R$. Množina všetkých komplexných čísel je teda množina

$$C = \{a + bi | a, b \in R\} .$$

Vieme, že $i^2 = -1$, $i^3 = -i$, $i^4 = 1$. Veľkosť komplexného čísla $z = a + bi$ vypočítame takto:

$$|z| = \sqrt{a^2 + b^2} .$$

Číslo $\overline{z} = a - bi$ nazveme komplexne združené k číslu $z = a + bi$. Pre súčin týchto čísel platí

$$z\overline{z} = a^2 + b^2 = |z|^2 .$$

Aritmetické operácie s komplexnými číslami

Sčitovanie a odčitovanie.

$$(a + bi) + (c + di) = (a + c) + (b + d)i ,$$

$$(a + bi) - (c + di) = (a - c) + (b - d)i .$$

Násobenie.

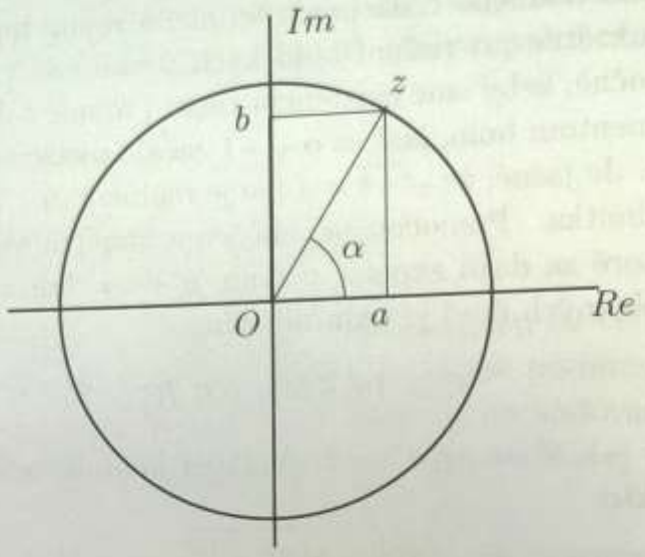
$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i .$$

Delenie.

$$(a + bi) : (c + di) = \frac{a + bi}{c + di} \cdot \frac{c - di}{c - di} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2} .$$

Goniometrický tvar komplexného čísla

Nech je dané komplexné číslo $z = a + bi$. Ako vidieť na obrázku (3.1):



Obrázok 3.1: Komplexné číslo znázornené v komplexnej rovine

$\sin\alpha = b/|z|$ a $\cos\alpha = a/|z|$. Komplexné číslo možno vyjadriť v tvare:

$$z = |z|\cdot(\cos\alpha + i\cdot\sin\alpha)\ .$$

Toto vyjadrenie sa nazýva goniometrický tvar komplexného čísla. Možno ho s výhodou použiť pri počítaní s komplexnými číslami. Nech $z = |z|\cdot(\cos\alpha + i\cdot\sin\alpha)$ a $y = |y|\cdot(\cos\beta + i\cdot\sin\beta)$.
Potom pre násobenie $z\cdot y$ platí:

$$z\cdot y = |z|\cdot|y|(\cos(\alpha+\beta) + i\cdot\sin(\alpha+\beta))\ .$$

Pre delenie:

$$\frac{z}{y} = \frac{|z|}{|y|}(\cos(\alpha-\beta) + i\cdot\sin(\alpha-\beta))\ .$$

Pre r-tú mocninu (kde $r \in R$):

$$z^r = |z|^r(\cos(r\cdot\alpha) + i\cdot\sin(r\cdot\alpha))\ .$$

Keďže r je reálne číslo, tak posledný vzťah nám dáva návod, ako počítať taktiež odmocninu z komplexného čísla. Ak $r = \frac{1}{n}$, tak pre n-tú odmocninu komplexného čísla z platí:

$$z^{\frac{1}{n}} = |z|^{\frac{1}{n}} \left(\cos\left(\frac{\alpha}{n}\right) + i \cdot \sin\left(\frac{\alpha}{n}\right)\right) .$$

Toto číslo sa niekedy nazýva aj hlavná odmocnina čísla z. Za odmocniny z tohto čísla však považujeme všetky riešenia rovnice $x^n = z$ (z algebry vieme, že v množine komplexných čísel je ich presne n), ktoré sa dajú vyjadriť nasledujúco:

$$z_k = z^{\frac{1}{n}} = |z|^{\frac{1}{n}} \left(\cos\left(\frac{2k\pi + \alpha}{n}\right) + i \cdot \sin\left(\frac{2k\pi + \alpha}{n}\right)\right) ,$$

kde $k = 0, 1, \ldots, n-1$.

Príklad 3.5.1. *Vypočítajme druhú a tretiu odmocninu z čísla $z = i$. Pre jeho veľkosť platí $|z| = 1$ a toto číslo zviera s reálnou osou uhol $\pi/2$, takže jeho goniometrický tvar je*

$$z = 1 \cdot \left(\cos\frac{\pi}{2} + i \cdot \sin\frac{\pi}{2}\right) .$$

Druhé odmocniny vypočítame nasledujúco:

$$\begin{aligned}
z_0 &= 1^{\frac{1}{2}} \cdot \left(\cos\left(\frac{1}{2} \cdot \frac{\pi}{2}\right) + i \cdot \sin\left(\frac{1}{2} \cdot \frac{\pi}{2}\right)\right) = \\
&= \cos\left(\frac{\pi}{4}\right) + i \cdot \sin\left(\frac{\pi}{4}\right) = \\
&= \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i , \\
z_1 &= 1^{\frac{1}{2}} \cdot \left(\cos\left(\frac{1}{2} \cdot \left(2\pi + \frac{\pi}{2}\right)\right) + i \cdot \sin\left(\frac{1}{2} \cdot \left(2\pi + \frac{\pi}{2}\right)\right)\right) = \\
&= \cos\left(\frac{5\pi}{4}\right) + i \cdot \sin\left(\frac{5\pi}{4}\right) = \\
&= -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i .
\end{aligned}$$

Tretie odmocniny sú nasledujúce:

$$
\begin{aligned}
z_0 &= 1^{\frac{1}{3}}\cdot\left(\cos\left(\frac{1}{3}\cdot\frac{\pi}{2}\right)+i\cdot\sin\left(\frac{1}{3}\cdot\frac{\pi}{2}\right)\right)= \\
&= \cos\left(\frac{\pi}{6}\right)+i\cdot\sin\left(\frac{\pi}{6}\right)= \\
&= \frac{\sqrt{3}}{2}+\frac{1}{2}i\,, \\
z_1 &= 1^{\frac{1}{3}}\cdot\left(\cos\left(\frac{1}{3}\cdot\left(2\pi+\frac{\pi}{2}\right)\right)+i\cdot\sin\left(\frac{1}{3}\cdot\left(2\pi+\frac{\pi}{2}\right)\right)\right)= \\
&= \cos\left(\frac{5\pi}{6}\right)+i\cdot\sin\left(\frac{5\pi}{6}\right)= \\
&= -\frac{\sqrt{3}}{2}+\frac{1}{2}i\,, \\
z_2 &= 1^{\frac{1}{3}}\cdot\left(\cos\left(\frac{1}{3}\cdot\left(4\pi+\frac{\pi}{2}\right)\right)+i\cdot\sin\left(\frac{1}{3}\cdot\left(4\pi+\frac{\pi}{2}\right)\right)\right)= \\
&= \cos\left(\frac{3\pi}{2}\right)+i\cdot\sin\left(\frac{3\pi}{2}\right)= \\
&= -i\,.
\end{aligned}
$$

Príklad 3.5.2. *Vypočítajme všetky štvrté odmocniny z čísla $z = 1$. Za hlavnú štvrtú odmocninu považujeme číslo 1, štvrté odmocniny sú však všetky štyri riešenia rovnice $x^4 = 1$ z množiny komplexných čísel.*

$$
\begin{aligned}
z_0 &= 1^{\frac{1}{4}}\cdot\left(\cos\left(\frac{1}{4}\cdot 0\right)+i\cdot\sin\left(\frac{1}{4}\cdot 0\right)\right)= \\
&= \cos(0)+i\cdot\sin(0)= \\
&= 1\,, \\
z_1 &= 1^{\frac{1}{4}}\cdot\left(\cos\left(\frac{1}{4}\cdot 2\pi\right)+i\cdot\sin\left(\frac{1}{4}\cdot 2\pi\right)\right)= \\
&= \cos\left(\frac{\pi}{2}\right)+i\cdot\sin\left(\frac{\pi}{2}\right)= \\
&= i\,,
\end{aligned}
$$

$$
\begin{aligned}
z_2 &= 1^{\frac{1}{4}} \cdot \left(\cos\left(\frac{1}{4} \cdot (4\pi)\right) + i \cdot \sin\left(\frac{1}{4} \cdot (4\pi)\right)\right) = \\
&= \cos(\pi) + i \cdot \sin(\pi) = \\
&= -1 \,, \\
z_3 &= 1^{\frac{1}{4}} \cdot \left(\cos\left(\frac{1}{4} \cdot 6\pi\right) + i \cdot \sin\left(\frac{1}{4} \cdot 6\pi\right)\right) = \\
&= \cos\left(\frac{3\pi}{2}\right) + i \cdot \sin\left(\frac{3\pi}{2}\right) = \\
&= -i \,.
\end{aligned}
$$

Kapitola 4

Binárne relácie

4.1 Definícia binárnej relácie

S binárnymi reláciami sa stretávame od prvých ročníkov základnej školy. Napríklad s reláciami na prirodzených číslach, ktoré sú vyjadrené znakmi $=, <, >$.

Definícia 4.1.1. *Nech $A \times B$ je karteziánsky súčin dvoch neprázdnych množín. Každá podmnožina $R \subseteq A \times B$ tohto karteziánskeho súčinu je binárna relácia z A do B. Ak $A = B$ (čiže $R \subseteq A \times A$), tak hovoríme o binárnej relácii na množine A.*

Binárna relácia teda vyjadruje, či je medzi dvomi prvkami x, y nejaký vopred špecifikovaný vzťah (vtedy platí, že usporiadaná dvojica $(x, y) \in R$), alebo nie je (vtedy platí $(x, y) \notin R$). Miesto značenia $(x, y) \in R$ dávame často prednosť značeniu xRy a hovoríme, že x je v relácii R s y. Napríklad používame zápis $x < y$ a nie $(x, y) \in <$.

Uveďme niekoľko príkladov.

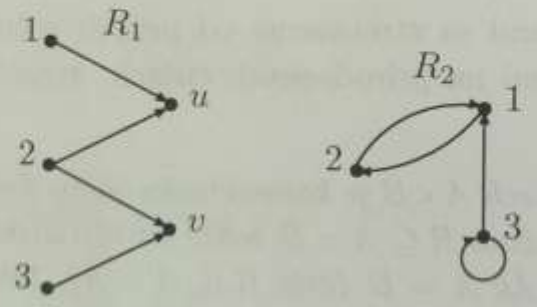
Príklad 4.1.1. *Nech $A = \{1, 2, 3\}$, $B = \{u, v\}$. Príklady relácií z A do B, respektíve na množine A sú $R_1 \subseteq A \times B$ a $R_2 \subseteq A \times A$, kde $R_1 =$*

$\{(1,u),(2,u),(2,v),(3,v)\}$ a $R_2 = \{(2,1),(3,1),(1,2),(3,3)\}$.

Príklad 4.1.2. *Nech S je množina všetkých študentov fakulty XYZ a P množina všetkých predmetov, ktoré možno navštevovať na danej fakulte. Potom $S \times P$ je množina obsahujúca všetky usporiadané dvojice v tvare (študent,predmet). Definujme binárnu reláciu $R_{navst} \subseteq S \times P$ takto: x je v relácii R_{navst} s y (čiže $(x,y) \in R_{navst}$), ak študent $x \in S$ navštevoval predmet $y \in P$.*

Príklad 4.1.3. *Nech F je množina všetkých ľudí s kontom na facebooku. Definujme reláciu $R_p \subseteq F \times F$ nasledujúco: osoba x je v relácii R_p s osobou y, ak x je v zozname priateľov y. Značíme to xR_py. Nie je ťažké si uvedomiť, že pre túto reláciu špeciálne platí: ak xR_py, potom aj yR_px.*

Niekedy je výhodné binárne relácie z A do B (na množine A) reprezentovať pomocou šípkových diagramov. Prvky množín A, B môžeme značiť, ako body v rovine a relačný vzťah xRy značíme šípkou z bodu x do bodu y. Na obrázku 4.1 máme diagramy relácií R_1 a R_2 z príkladu 4.1.1.



Obrázok 4.1: Diagramy relácií z príkladu 4.1.1

4.2 Vlastnosti binárnych relácií na množine

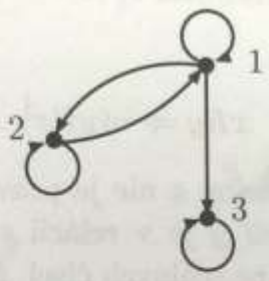
Pozrime sa teraz lepšie na vlastnosti binárnych relácií na množine. Nech je daná množina $A \neq \emptyset$.

1. Hovoríme, že relácia $R \subseteq A \times A$ je **reflexívna** ak pre

$$\forall x \in A \quad xRx\,.$$

Čiže **každý prvok** množiny A je v relácii sám so sebou. Napríklad relácia $\leq$ na množine reálnych čísel (ale aj prirodzených čísel, celých čísel a ďalších množinách) je takouto reláciou. Na obrázku 4.2 máme ďalší príklad reflexívnej relácie na množine $A = \{1, 2, 3\}$. Pri reflexívnej relácii musí byť slučka (šípka začínajúca aj končiaca v tom istom prvku) pri každom prvku tejto množiny. Ak **existuje aspoň jeden** prvok, ktorý nie je v relácii sám so sebou, tak relácia nie je reflexívna.

2. Hovoríme, že relácia $R \subseteq A \times A$ je **symetrická**, ak pre $\forall x, y \in A$ je



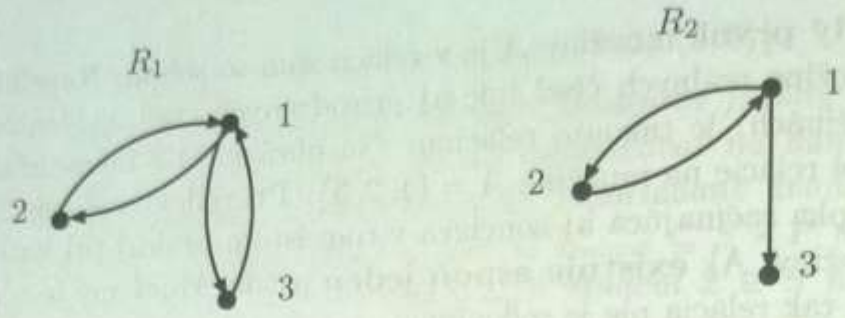
Obrázok 4.2: Reflexívna relácia

nasledujúci výrok pravdivý:

$$xRy \Rightarrow yRx \ .$$

Uvedený výrok je implikácia, takže je nepravdivý len v prípade, ak x je v reácii R s y (je splnený predpoklad), ale y nie je v relácii R s x. Ak nájdeme aspoň jednu dvojicu prvkov $x, y \in A$, pre ktorú výrok nie je pravdivý, tak relácia nie je symetrická. Príkladom symetrickej relácie je relácia „byť priateľom“ na facebooku. Na obrázku 4.3 máme príklad symetrickej relácie R_1 a relácie R_2, ktorá nie je symetrická (pretože 1 je v relácii s 3, ale naopak to neplatí). Pri grafickej reprezentácii symetrickej relácie musí platiť, že medzi každou dvojicou prvkov existuje buď dvojica proti sebe idúcich šípok, alebo žiadna šípka. Ak nájdeme takú dvojicu rôznych prvkov, medzi ktorými je len jedna šípka (na obrázku 4.3 dvojica $1, 3$ pre R_2), tak relácia nie je symetrická.

3. Hovoríme, že relácia $R \subseteq A \times A$ je **asymetrická**, ak pre $\forall x, y \in A$ je

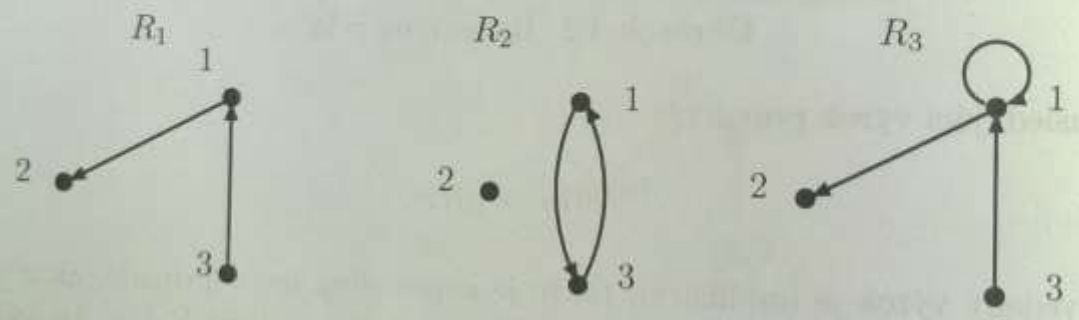


Obrázok 4.3: Symetrická relácia R_1 a relácia R_2, ktorá nie je symetrická

nasledujúci výrok pravdivý:

$$xRy \Rightarrow \neg(yRx) \ .$$

Tento výrok je opäť implikáciou a nie je pravdivý len v tom prípade, keď x je v relácii s y, a zároveň y je v relácii s x. Príkladom asymetrickej relácie je relácia $<$ na množine reálnych čísel. Na obrázku 4.4 máme príklad



Obrázok 4.4: Asymetrická relácia R_1 a relácie R_2, R_3, ktoré nie sú asymetrické

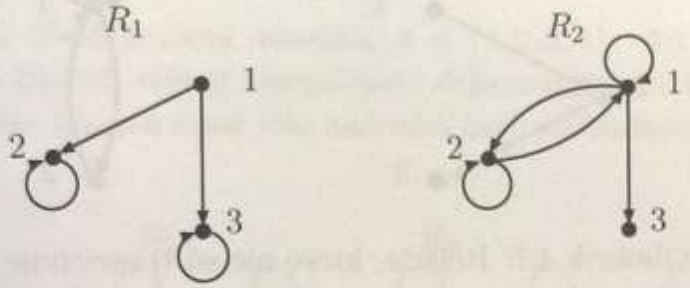
asymetrickej relácie R_1 a relácií R_2, R_3, ktoré nie sú asymetrické. Diagram asymetrickej relácie nemôže obsahovať dvojicu proti sebe idúcich šípok, ani slučku pri žiadnom prvku. Medzi každou dvojicou rôznych prvkov môže byť **najviac jedna** šípka.

4. Hovoríme, že relácia $R \subseteq A \times A$ je **antisymetrická**, ak pre $\forall x, y \in A$ je nasledujúci výrok pravdivý:

$$(xRy \wedge yRx) \Rightarrow x = y \ .$$

Opäť ide o implikáciu. Takže tento výrok nie je pravdivý, ak je prvok x v relácii s prvkom y, aj y s x a x, y sú navzájom rôzne prvky množiny A. Typickým príkladom antisymetrickej relácie je relácia $\leq$ (ak $x \leq y$ a zároveň $y \leq x$, tak $x = y$). Na obrázku 4.5 máme antisymetrickú reláciu R_1 a reláciu R_2, ktorá nie je antisymetrická. Vidíme, že antisymetrickosť je zoslabením asymetrickosti. Opäť máme zakázané dvojice proti sebe idúcich šípok medzi rôznymi prvkami, ale v tomto prípade sú slučky dovolené. Relácia R_3 na obrázku 4.4 je antisymetrická, ale nie je asymetrická.

5. Hovoríme, že relácia $R \subseteq A \times A$ je **tranzitívna**, ak pre $\forall x, y, z \in A$ je

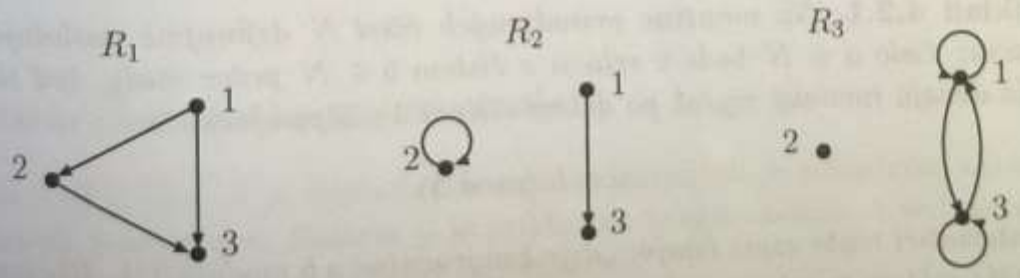


Obrázok 4.5: Antisymetrická relácia R_1 a R_2, ktorá nie je antisymetrická

nasledujúci výrok pravdivý:

$$xRy \wedge yRz \Rightarrow xRz\ .$$

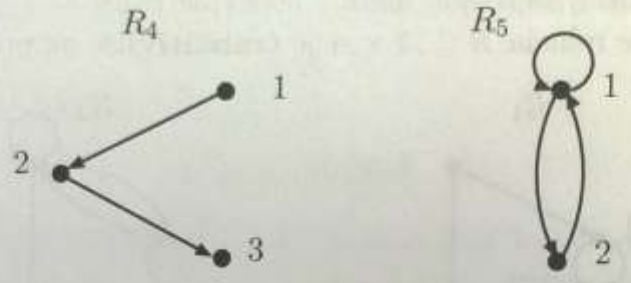
Príkladom tranzitívnych relácií sú $<$, $\leq$ na množine reálnych čísel (ak $x \leq y$



Obrázok 4.6: Tranzitívne relácie R_1, R_2, R_3

a zároveň $y \leq z$, tak $x \leq z$). Keďže spomínaný výrok je opäť implikácia,

relácia nebude tranzitívna, ak existuje aspoň jedna trojica prvkov $x, y, z \in A$ taká, že xRy a zároveň yRz, ale x nie je v relácii s prvkom z. Na obrázku 4.6 máme príklady tranzitívnych relácií R_1, R_2, R_3 na množine $A = \{1, 2, 3\}$. V prípade R_2 si musíme uvedomiť, že predpoklad $(xR_2y \wedge yR_2z)$ implikácie z definície nie je pre túto reláciu nikdy splnený, preto je táto implikácia pre R_2 vždy pravdivá. Na obrázku 4.7 máme príklady relácií R_4, R_5, ktoré nie sú tranzitívne. V druhom prípade máme $2R_51$ a zároveň $1R_52$, ale 2 nie je



Obrázok 4.7: Relácie, ktoré nie sú tranzitívne

v relácii R_5 s 2.

Relácia ekvivalencie

Relácia $R \subseteq A \times A$ je reláciou ekvivalencie, ak je reflexívna, symetrická, tranzitívna.

Príklad 4.2.1. *Na množine prirodzených čísel N definujme nasledujúcu reláciu: číslo $a \in N$ bude v relácii s číslom $b \in N$ práve vtedy, keď tieto čísla dávajú rovnaký zvyšok po delení číslom 3. Zapisujeme to*

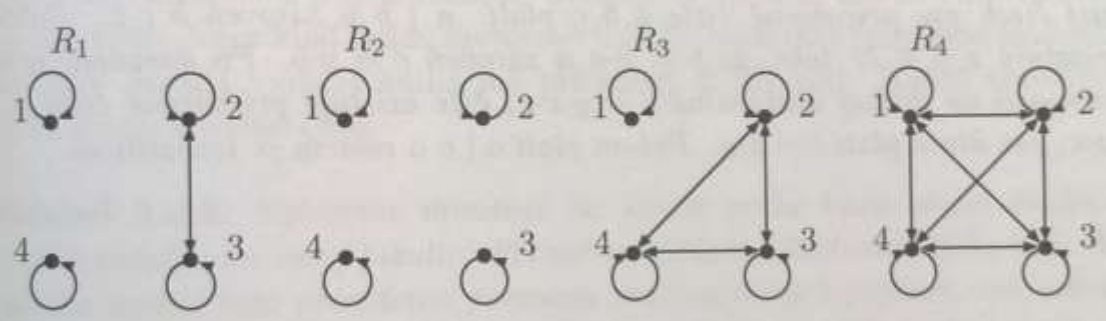
$$a \equiv b \ (mod\ 3)$$

(matematici tento zápis čítajú: „a je kongruentné s b modulo 3“). Ukážeme, že táto relácia je reláciou ekvivalencie.
i) Aby bola relácia reflexívna, pre $\forall x \in N$ má platiť $x \equiv x \ (mod\ 3)$. Čiže x a x majú dávať rovnaký zvyšok po delení číslom 3, čo určite platí.
ii) Ako sme hovorili, ak $x \equiv y \ (mod\ 3)$, číslo x dáva rovnaký zvyšok po

delení číslom 3 ako y. Potom to môžeme otočiť a povedať, že y dáva rovnaký zvyšok po delení trojkou ako x. Takže platí aj $y \equiv x \pmod 3$ a táto relácia je symetrická.
iii) Ak pre nejaké $x, y, z \in N$ platí $x \equiv y \pmod 3$ a zároveň $y \equiv z \pmod 3$, tak čísla x, y, z dávajú rovnaký zvyšok po delení trojkou, preto môžeme písať aj $x \equiv z \pmod 3$, takže ide o tranzitívnu reláciu.
Ako vidieť, táto relácia je reláciou ekvivalencie.

Uveďme ešte príklady relácií ekvivalencie na konečnej množine.

Príklad 4.2.2. *Nech je daná množina $A = \{1, 2, 3, 4\}$. Na obrázku (4.8) máme príklady štyroch relácií ekvivalencie definovaných na tejto množine. (Dvojice protisebe idúcich šípok sme nahradili kvôli prehľadnosti jednou obojstrannou.)*



Obrázok 4.8: Relácie ekvivalencie

Relácia čiastočného usporiadania

Relácia $R \subseteq A \times A$ je čiastočným usporiadaním, ak je reflexívna, antisymetrická, tranzitívna. Relácia $\leq$ je príkladom takejto relácie. Uveďme ešte jeden príklad relácie čiastočného usporiadania.

Príklad 4.2.3. *Ukážeme, že relácia „delí", definovaná na množine prirodzených čísel je reláciou čiastočného usporiadania. Pre túto reláciu používame značenie $a \mid b$. Čítame to a delí b (myslí sa tým, že a je deliteľom b, nie a*

delené b, ako býva častou chybou). Vieme, že prirodzené číslo a je deliteľom prirodzeného čísla b práve vtedy, keď existuje prirodzené číslo x také, že $b = x \cdot a$. *Tento jednoduchý fakt nám pomôže pri dokazovaní, že naša relácia je reflexívna, antisymetrická a tranzitívna.*

i) Pre ľubovoľné $a \in N$ *platí, že a je deliteľom samého seba (čiže* $a \mid a$*), takže táto relácia je reflexívna.*

ii) Nech pre prirodzené čísla a, b *platí:* $a \mid b$ *a zároveň* $b \mid a$. *Potom existujú* $x, y \in N$ *také, že* $b = x \cdot a$ *a zároveň* $a = y \cdot b$. *Po dosadení druhej rovnosti do prvej dostávame* $b = x \cdot y \cdot b$, *čiže* $1 = x \cdot y$, *čo pre* $x, y \in N$ *platí len v prípade, ak* $x = y = 1$. *To znamená, že* $a = b$. *Pre ľubovoľné* $a, b \in N$ *je teda výrok:*

$$\text{ak } (a \mid b \text{ a zároveň } b \mid a), \text{ potom } a = b$$

pravdivý a relácia je antisymetrická.

iii) Nech pre prirodzené čísla a, b, c *platí:* $a \mid b$ *a zároveň* $b \mid c$. *Potom existujú* $x, y \in N$ *také, že* $b = x \cdot a$ *a zároveň* $c = y \cdot b$. *Po dosadení prvej rovnosti do druhej dostávame* $c = y \cdot x \cdot a$, *čiže existuje prirodzené číslo* $z = y \cdot x$, *pre ktoré platí* $c = z \cdot a$. *Potom platí* $a \mid c$ *a relácia je tranzitívna.*

Kapitola 5

Funkcie

Skôr, ako definujeme pojem funkcie, uveďme si situácie, kde sa s nimi môžeme stretnúť. Napríklad každé motorové vozidlo musí mať priradené evidenčné číslo. Každá vydaná kniha má priradený ISBN kód. Každé narodené dieťa dostáva rodné číslo.

Príklad 5.0.4. *Vytvorme množinu A, ktorej prvky budú všetci študenti prvého ročníka na vašej fakulte. Priraďme každému študentovi jeho vek. Ak chceme opísať toto priradenie pomocou matematických pojmov, tak máme funkciu (zobrazenie), ktorá každému prvku množiny A (študentovi) priradí práve jedno prirodzené číslo (jeho vek). Zapisujeme to $f : A \longrightarrow N$.*

V predchádzajúcom príklade sú dôležité slová **každému** prvku množiny A priradíme **práve jeden** prvok množiny N.

Funkcia je pravidlo, ktoré každému prvku nejakej množiny priradí práve jeden prvok inej (alebo tej istej) množiny. Presná definícia je nasledujúca:

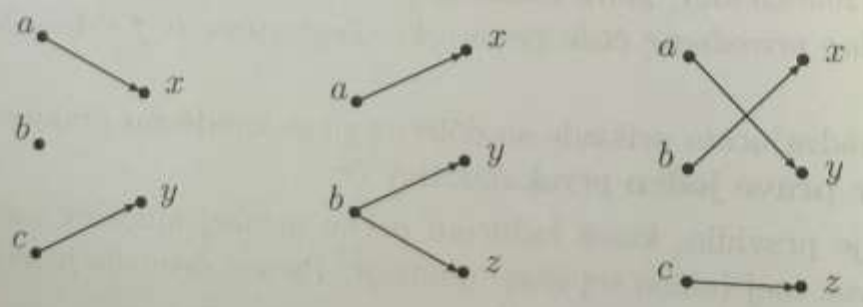
Definícia 5.0.1. *Binárna relácia $f \subset A \times B$ sa nazýva funkcia z množiny A do množiny B (značíme to $f : A \to B$), ak pre $\forall x \in A$ existuje práve jeden prvok $y \in B$ taký, že xfy. Množina A sa nazýva definičný obor (množina vzorov) a množina B sa nazýva obor hodnôt (množina obrazov).*

Predpis xfy, ktorý sme použili v definícii, sa pri funkciách veľmi nepoužíva. Radšej budeme písať $f(x) = y$.

Miesto slova funkcia sa často používa názov zobrazenie. K slovu funkcia sa prikloníme, pretože je to pojem, ktorý je bližší informatike.

5.1 Grafická reprezentácia funkcií

Niektoré funkcie môžeme znázorniť graficky. V mnohých prípadoch nám toto grafické znázornenie umožňuje ľahšie určiť niektoré vlastnosti takto zobrazenej funkcie. Vezmime si funkciu $f : A \to B$. Ak sú množiny A a B malé, môžeme použiť na znázornenie f šípkový diagram. Na obrázku 5.1 máme príklad troch diagramov. Prvky množiny A, teda definičného oboru sú umiestnené vľavo. Prvky množiny B, teda oboru hodnôt vpravo a priradenie je zobrazené šípkou. Vidíme, že len posledný z diagramov zodpovedá funkcii. Prvý nespĺňa podmienku, že každému prvku z A je priradený prvok z B. Druhý diagram nespĺňa podmienku, že priraďujeme práve jeden prvok.



Obrázok 5.1: Čo je a čo nie je funkcia?

5.2 Niektoré vlastnosti funkcií

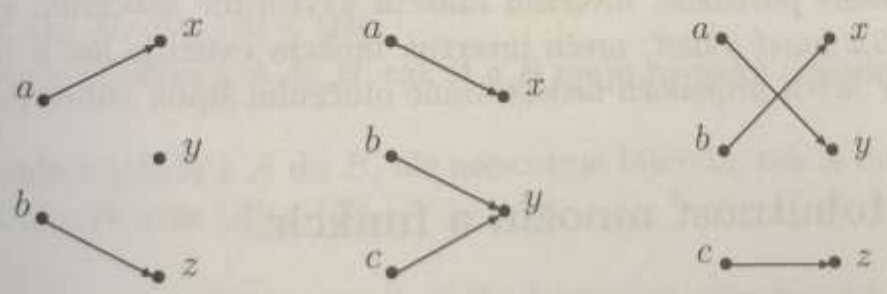
Vráťme sa k príkladu s evidenčnými číslami motorových vozidiel. Vieme, že dve rôzne autá nemôžu mať rovnaké evidenčné číslo. Ak zobrazenie $f : A \to B$ priradí každej dvojici navzájom rôznych prvkov z množiny A dva rôzne prvky z B, tak hovoríme, že f je **injektívna** (alebo **prostá**) funkcia.

Zoberme si množinu všetkých detí narodených na Slovensku v roku 2004. Priraďme každému dieťaťu dátum jeho narodenia. Toto priradenie je funkcia, pretože každé dieťa (prvok množiny A) má priradený práve jeden dátum narodenia (prvok množiny B). Je známe, že každý deň spomenutého roka sa narodilo aspoň jedno dieťa (v skutočnosti to bolo podľa údajov Slovenského štatistického úradu v priemere 136 detí za deň).

Ak ku každému prvku y množiny B existuje prvok x množiny A taký, že $f(x) = y$, potom túto funkciu nazývame **surjektívna**.

Ak je nejaká funkcia súčasne injektívna aj surjektívna, potom takúto funkciu nazývame **bijektívna**.

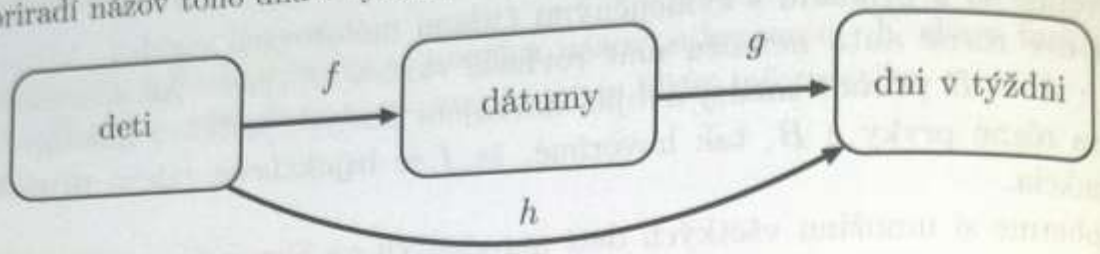
Na obrázku 5.2 sú po poradí príklady funkcií: injektívnej, ale nie surjektívnej; surjektívnej, ale nie injektívnej; bijektívnej.



Obrázok 5.2: Injektívna, surjektívna a bijektívna funkcia

Zoberme si opäť množinu detí narodených na Slovensku v roku 2004 a funkciu f, ktorá priradí každému dieťaťu dátum jeho narodenia. Definujme funkciu g, ktorá každému dňu v roku 2004 priradí deň v týždni, ktorý zodpovedal tomuto dátumu. Spojením týchto funkcií v poradí: najprv ap-

likujeme f, potom g, dostávame zloženú funkciu h, ktorá každému dieťaťu priradí názov toho dňa v týždni, kedy sa narodilo (pozri obrázok 5.3).



Obrázok 5.3: Príklad zloženej funkcie

Všeobecne hovoríme, že pre dvojicu funkcií $f : A \to B$ a $g : B \to C$ je funkcia $h : A \to C$, kde pre ľubovoľné $x \in A$ platí $h(x) = g(f(x))$, **zloženou funkciou**.
Ak je funkcia $f : A \to B$ bijektívna, potom k nej môžeme definovať **inverznú funkciu** $f^{-1} : B \to A$ takú, že pre ľubovoľné $y \in B$ platí:

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

Zjednodušene povedané, inverznú funkciu vytvoríme otočením šípok. Na obrázku 5.2 hneď vidieť, prečo inverzná funkcia existuje len k bijektívnej funkcii. V iných prípadoch nedostávame otočením šípok vôbec funkciu.

5.3 Mohutnosť množín a funkcie

Venujme pozornosť otázke: aký je vzťah medzi počtom prvkov dvojice konečných množín, ak existuje medzi nimi injektívna, surjektívna alebo bijektívna funkcia. Pozrime sa na obrázok 5.2.
Pozorovanie. i) Ak existuje injekcia z A do B (prvý a tretí príklad na zmieňovanom obrázku), tak pre počet prvkov oboch množín platí vzťah $|A| \leq |B|$.
ii) Ak existuje surjekcia z A do B (druhý a tretí príklad na zmieňovanom obrázku), tak pre počet prvkov oboch množín platí vzťah $|A| \geq |B|$.

iii) Ak existuje bijekcia z A do B (tretí príklad na zmieňovanom obrázku), tak pre počet prvkov oboch množín platí vzťah $|A| = |B|$.

Zdôvodnenie. i) Z definície funkcie vieme, že každému prvku množiny A je priradený práve jeden prvok. Z každého prvku množiny A vychádza práve jedna šípka. Máme teda $|A|$ šípok. Z definície injektívnej funkcie vyplýva, že do každého prvku množiny B smeruje najviac jedna šípka, čiže prvkov B nemôže byť menej, ako je šípok.

ii) Do každého prvku množiny B smeruje najmenej jedna šípka. Potom prvkov B nemôže byť viac, ako je šípok.

iii) Spojením nerovností z i) a ii) dostávame $|A| = |B|$.

Presvedčili sme sa, že pomocou funkcií s danými vlastnosťami môžno porovnávať počet prvkov konečných množín. (Neskôr využijeme tieto fakty pri kombinatorickom počítaní možností.) Ako je to s nekonečnými množinami? Dali by sa napríklad injekcia a bijekcia využiť na porovnávanie nekonečných množín?

Nielen dali, ale sa to tak aj robí. Pri nekonečných množinách však radšej, ako o počte prvkov, hovoríme o mohutnosti množiny.

Nech teda A a B sú ľubovoľné množiny.

1. Ak existuje injekcia z A do B, tak A má menšiu, nanajvýš rovnakú mohutnosť ako B, čiže $|A| \leq |B|$.
2. Ak existuje bijekcia z A do B, tak A a B majú rovnakú mohutnosť, čiže $|A| = |B|$.
3. Ak existuje injekcia z A do B, ale neexistuje bijekcia, tak A má menšiu mohutnosť ako B, čiže $|A| < |B|$.

Príklad 5.3.1. *Označme množinu všetkých párnych prirodzených čísel N_p. Nie je ťažké si uvedomiť, že funkcia f_1 z množiny N_p do množiny všetkých prirodzených čísel N daná predpisom $f_1(k) = k$ je injekcia. Platí teda, že $|N_p| \leq |N|$. Toto sme asi očakávali, pretože množina párnych prirodzených čísel je podmnožinou množiny prirodzených čísel. Na druhej strane funkcia f_2 z množiny N do množiny N_p daná predpisom $f_2(k) = 2k$ je bijekcia, pretože každým dvom rôznym prirodzeným číslam m a n sú priradené dve rôzne párne čísla $2m$ a $2n$ (takže ide o injekciu). Každé párne číslo $2k$ má*

svoj vzor k v množine prirodzených čísel (takže je to aj surjekcia).

$$\begin{array}{ccc} 1 & \longrightarrow & 2 \\ 2 & \longrightarrow & 4 \\ 3 & \longrightarrow & 6 \\ & \vdots & \\ k & \longrightarrow & 2k \\ & \vdots & \end{array}$$

Potom dostávame, že $|N_p| = |N|$. Narazili sme na jav, ktorý pri konečných množinách nepozorujeme. Podmnožina N_p množiny N má rovnakú mohutnosť, ako samotná N. Zdalo by sa, že všetkých prirodzených čísel je viac ako párnych, ale bijekcia f_2 nám umožňuje popárovať ich tak, že každému prirodzenému číslu vieme priradiť práve jedno párne číslo.

Príklad 5.3.2. *Porovnajme množiny prirodzených a celých čísel. Použime nasledujúcu funkciu z N do Z:*

$$\begin{array}{ccc} 1 & \longrightarrow & 0 \\ 2 & \longrightarrow & 1 \\ 3 & \longrightarrow & -1 \\ 4 & \longrightarrow & 2 \\ 5 & \longrightarrow & -2 \\ & \vdots & \\ 2k & \longrightarrow & k \\ 2k+1 & \longrightarrow & -k \\ & \vdots & \end{array}$$

Nie je ťažké si uvedomiť, že ľubovoľné dve rôzne prirodzené čísla majú rôzne obrazy v Z a každé celé číslo má svoj vzor v množine N (premyslite si to). Z existencie bijekcie vyplýva, že $|N| = |Z|$.

Toto boli pomerne prekvapujúce výsledky, ktoré nám hovoria, že nekonečné množiny sa správajú inak ako konečné a budeme musieť pri práci s nimi postupovať opatrnejšie.

Príklad 5.3.3. *[24] Ešte väčšie prekvapenie nastane, keď porovnáme množinu prirodzených a kladných racionálnych čísel. Zrejme väčšina z vás očakáva, že kladných racionálnych čísel je viac. V tomto (mylnom) názore nás môže utvrdiť takáto úvaha:*

Vieme, že $N \subset Q^+$. Ak zoberieme ľubovoľné dve za sebou idúce prirodzené čísla n, $n+1$ (ktoré sú samozrejme aj z Q^+), určite nájdeme racionálne číslo q, pre ktoré $n < q < n+1$ (dokonca existuje nekonečne veľa takých čísel). Takže kladných racionálnych čísel by malo byť oveľa viac. Ako sme naznačili, táto úvaha je nesprávna! Zrada spočíva v tom, že sme sa intuitívne snažili previesť skúsenosti, ktoré máme s konečnými množinami, na množiny nekonečné. Ak máme množiny $A = \{1, 2\}$ a $B = \{1, 3/2, 2\}$, tak je jasné, že prvky množiny B nemožno očíslovať číslami z A tak, aby mal každý prvok z B priradené iné číslo. Ak by A bola množina všetkých prirodzených čísel, mohli by sme do nej znova a znova "načrieť" a vybrať ďalšie číslo použiteľné na očíslovanie prvkov množiny B.

Ukážme, ako možno zoradiť a očíslovať všetky racionálne čísla. Pomôžeme si nasledujúcou tabuľkou:

1/1				
1/2	2/1			
1/3	2/2	3/1		
1/4	2/3	3/2	4/1	
1/5	2/4	3/3	4/2	5/1

$\vdots$

V prvom riadku máme zlomok a/b $(a, b \in N)$, pre ktorý platí: $a + b = 2$, v druhom riadku sú zlomky, pre ktoré máme $a + b = 3$, v k-tom riadku sú zlomky, pre ktoré platí $a + b = k + 1$. Číslovať (zoraďovať) tieto zlomky môžeme po riadkoch, pričom pri číslovaní vynechávame zlomky, ktoré nie

sú v základnom tvare. Začiatok číslovania vyzerá takto:

$$\begin{array}{ccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \frac{1}{1} & \frac{1}{2} & \frac{2}{1} & \frac{1}{3} & \frac{3}{1} & \frac{1}{4} & \frac{2}{3} & \frac{3}{2} & \frac{4}{1} & \frac{1}{5} & \frac{5}{1} \end{array} \quad \dots$$

Takto by sme mohli pokračovať. Dá sa dokázať, že funkcia, ktorej začiatok je v predchádzajúcej tabuľke, je bijekcia - to znamená, že $|N| = |Q^+|$. *Podobne sa dá dokázať, že* $|Z| = |Q|$, *z čoho môžeme odvodiť* $|N| = |Q|$.

Príklad 5.3.4. *[24] Porovnajme teraz množiny prirodzených a reálnych čísel. Ukážeme, že reálnych čísel je viac, ako prirodzených, čiže množina reálnych čísel má väčšiu mohutnosť, ako množina prirodzených čísel (podobne celých aj racionálnych). Ukážeme, že prirodzených čísel je dokonca menej, ako reálnych čísel z intervalu* $\langle 0, 1)$. *Budeme postupovať sporom. Predpokladajme, že ich je rovnako. Čiže existuje bijekcia z* N *do* $\langle 0, 1)$ *(ktorá nám usporiadala čísla z* $\langle 0, 1)$ *v nejakom poradí). Napríklad:*

$$\begin{array}{ccc} 1 & \longrightarrow & 0,a_{11}a_{12}a_{13}\dots a_{1n}\dots \\ 2 & \longrightarrow & 0,a_{21}a_{22}a_{23}\dots a_{2n}\dots \\ 3 & \longrightarrow & 0,a_{31}a_{32}a_{33}\dots a_{3n}\dots \\ & \vdots & \\ n & \longrightarrow & 0,a_{n1}a_{n2}a_{n3}\dots a_{nn}\dots \\ & \vdots & \end{array},$$

kde $a_{ij} \in \{0, 1, 2, \dots, 9\}$ *predstavuje* j*-tu cifru* i*-teho čísla. Niektoré reálne čísla môžu mať dva zápisy, napríklad:* $0,1$ *a* $0,099999\dots$ *predstavujú to isté číslo. Všeobecne platí, že*

$$0,a_1a_2a_3\dots a_k000\dots = 0,a_1a_2a_3\dots(a_k-1)999\dots,$$

kde $a_k \neq 0$. *V takýchto prípadoch budeme brať do úvahy zápis používajúci nuly namiesto zápisu, kde sú od istého desatinného miesta samé deviatky. Vezmime teraz číslo* $0,b_1b_2b_3\dots b_n\dots$, *ktoré zostrojíme nasledujúco: vezmeme prvé reálne číslo a jeho prvú cifru* a_{11}. *Ak je táto cifra rovná* 1, *tak*

$b_1 = 2$, ak $a_{11} \neq 1$, tak položíme $b_1 = 1$. Teraz zoberieme druhé reálne číslo a jeho druhú cifru a_{22} a urobíme to isté: ak $a_{22} = 1$, tak $b_2 = 2$, ak $a_{22} \neq 1$, tak položíme $b_2 = 1$. Podobne zostrojíme cifru b_3 z cifry a_{33} a pre ľubovoľné $n \in N$ máme

$$b_n = \begin{cases} 2 & ak\ a_{nn} = 1 \\ 1 & ak\ a_{nn} \neq 1 \end{cases}$$

Objasnime si to na príklade:

$$\begin{array}{lcl} 1 & \longrightarrow & 0{,}165481\ldots \\ 2 & \longrightarrow & 0{,}459283\ldots \\ 3 & \longrightarrow & 0{,}231873\ldots \\ 4 & \longrightarrow & 0{,}112211\ldots \\ 5 & \longrightarrow & 0{,}111117\ldots \\ 6 & \longrightarrow & 0{,}543267\ldots \end{array}$$

Potom číslo b bude začínať nasledujúco: $0,212121\ldots$ Takéto číslo sa však v zozname čísel, ktoré sú spomenutou bijekciou priradené číslam $1, 2, 3, \ldots$ nenachádza, pretože sa od každého z nich odlišuje aspoň na jednom desatinnom mieste. Od prvého sa odlišuje cifrou na prvom desatinnom mieste, od druhého na druhom desatinnom mieste, od tretieho na treťom, všeobecne od n-tého čísla na n-tom desatinnom mieste atď. Dospeli sme k sporu, že uvedené zobrazenie je bijekcia. Takáto bijekcia nemôže existovať. Platí teda, že $|N| < |\langle 0, 1)|$. Potom nie je ťažké odvodiť, že $|N| < |R|$.

Dôkaz z predchádzajúceho príkladu pochádza od nemeckého matematika Georga Cantora (1845-1918). Nazýva sa Cantorova metóda diagonalizácie a tento princíp bol neskôr použitý pri dokazovaní niektorých výsledkov dôležitých pre teoretickú informatiku (napríklad pri dôkaze Ladnerovej vety).

5.4 Dôsledky predchádzajúcich úvah v informatike

Venujme sa otázke, čo vlastne vieme pomocou počítačov vypočítať. Funkciu nazveme **vypočítateľnou**, ak existuje algoritmus (program), pomocou

ktorého možno vypočítať pre ľubovoľný jej vstup funkčné hodnoty. Sú všetky funkcie vypočítateľné? Určite nie. Napríklad funkcia, ktorá priradí každej hviezde vo vesmíre (v niektorom okamihu) počet atómov, z ktorých sa skladá, bude len ťažko vypočítateľná pomocou počítača. Zamerajme sa radšej len na funkcie, ktorých definičný obor a obor hodnôt sú číselné množiny, alebo ešte lepšie - vezmime len funkcie, ktorých definičný obor aj obor hodnôt sú prirodzené čísla. Označme množinu všetkých takýchto funkcií F - čiže $F = \{f : N \to N | f je funkcia\}$. Aká je mohutnosť tejto množiny? Ukážeme, že existuje injekcia z $\langle 0,1)$ do F. Nech $x \in \langle 0,1)$, pričom $x = 0,a_1a_2a_3\ldots a_n\ldots$. Tomuto číslu priradíme funkciu $f_x : N \to N$ danú predpisom $f_x(n) = a_n$. To znamená, že číslu 1 priradí f_x cifru a_1, číslu 2 cifru a_2 atď. Takéto priradenie $x \to f_x$ je injekcia, pretože dvom rôznym číslam x, y (odlišujúcim sa napríklad v k-tej cifre) priradíme dve rôzne funkcie f_x, f_y (musia byť rôzne, pretože $f_x(k) \neq f_y(k)$). Keďže existuje injekcia z $\langle 0,1)$ do F, tak platí $|\langle 0,1)| \leq |F|$.

Zaoberajme sa teraz otázkou, koľko konečných programov (konečných postupností inštrukcií - nebudeme skúmať, či tie programy majú zmysel) existuje? Množinu takýchto programov označme P. Každý program vieme zapísať, ako postupnosť núl a jednotiek a každej takejto postupnosti vieme priradiť prirodzené číslo. Navyše to priradenie vieme uskutočniť tak, že rôznym programom priraďujeme rôzne čísla, čiže máme injekciu z P do N. Platí teda:

$$|P| \leq |N| < |\langle 0,1)| \leq |F|.$$

To znamená, že všetkých programov, ktoré vieme zapísať (vrátane tých nezmyselných) je menej, ako funkcií z N do N. Takže je možné medzi nimi nájsť také funkcie (je ich dokonca nekonečne veľa), pre ktoré neexistuje konečný program, ktorý pre ľubovoľný vstup z N vypočíta funkčnú hodnotu.

Pri skúmaní nevypočítateľných funkcií a problémov sa napríklad zistilo, že nie je možné vytvoriť v žiadnom programovacom jazyku konečný program, ktorý by mal na vstupe program (v ľubovoľnom pevne zvolenom programovacom jazyku) a na výstupe by sme mali práve jednu z odpovedí (tú pravdivú samozrejme):

- áno - program, ktorý je na vstupe, skončí vždy v konečnom čase,

- nie - program, ktorý je na vstupe, neskončí vždy v konečnom čase.

Tento problém sa nazýva: **problém zastavenia** a má dôležité postavenie najmä v teoretickej informatike (pozri napríklad [13]).

Kapitola 6

Postupnosti

6.1 Základné pojmy

Pod pojmom postupnosť rozumieme zobrazenie, ktorého definičným oborom je podmnožina množiny celých čísel. Podľa toho, či je táto podmnožina konečná alebo nekonečná, hovoríme o konečných, respektíve nekonečných postupnostiach. Zvyčajne je dané celé číslo p a definičný obor je množina $\{p, p+1, p+2, \ldots, q\}$ pre konečné postupnosti ($q \geq p$), alebo množina všetkých celých čísel, ktoré nie sú menšie ako p, v prípade nekonečných postupností. V týchto prípadoch používame značenie $\{a_n\}_{n=p}^{q}$ a $\{a_n\}_{n=p}^{\infty}$. Všeobecne používame zápis $\{a_n\}_{n \in I}$, kde $I \subset Z$.

Ak obor hodnôt postupnosti obsahuje iba čísla, hovoríme o číselných postupnostiach.

Spôsoby zadávania postupností:

1. Vymenovaním členov postupnosti. To má význam predovšetkým pri konečných postupnostiach s malým počtom členov. Niekedy bývajú aj nekonečné postupnosti zadané vymenovaním niekoľkých prvých členov, je to však len v prípadoch, kedy sa môžeme spoľahnúť na našu intuíciu a predpokladáme, že pravidlo na vytváranie ďalších členov postupnosti je ľahko uhádnuteľné z prvých členov postupnosti. Napríklad, ak máme prvé čle-

ny postupnosti $1, 2, 3, 4, \ldots$, tak každého napadne, že pôjde o postupnosť všetkých prirodzených čísel. Aj keď v skutočnosti existuje nekonečne veľa postupností, ktoré môžu začínať štvoricou čísel $1, 2, 3, 4, \ldots$.

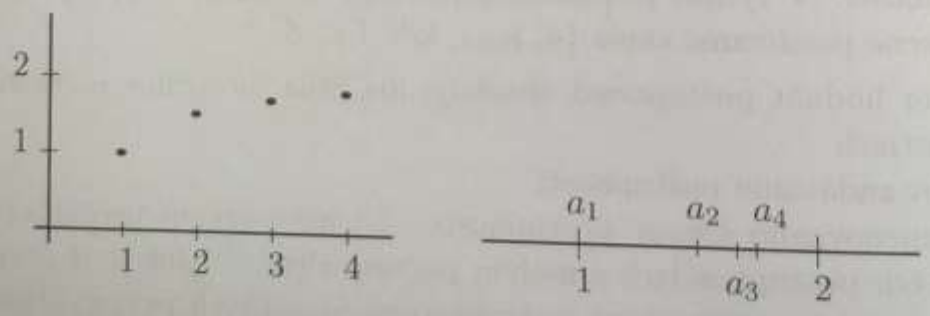
2. Vzorcom na priamy výpočet n-tého člena postupnosti. Napríklad $\{a_n\}_{n=1}^{\infty}$, kde $a_n = \dfrac{3n+4}{7n-1}$. Výpočtom zistíme, že prvý člen tejto postupnosti je $a_1 = \dfrac{3{\cdot}1+4}{7{\cdot}1-1} = \dfrac{7}{6}$, druhý člen $\dfrac{10}{13}$, prípadne člen $a_{99} = \dfrac{3{\cdot}99+4}{7{\cdot}99-1} = \dfrac{301}{692}$. Máme teda predpis, ktorým definujeme všetky členy postupnosti naraz.

3. Rekurzívne (rekurentne). Postupnosť môžeme definovať aj tak, že určíme niekoľko začiatočných členov a zadáme pravidlá na vytváranie ďalších členov tejto postupnosti pomocou členov, ktoré sú už určené. Príkladmi sú známa Fibonacciho postupnosť a faktoriál:

1. $f_0 = 0$, $f_1 = 1$, pre $\forall n \in N$ $f_{n+1} = f_n + f_{n-1}$,

2. $a_0 = 1$, pre $\forall n \in N$ $a_n = n{\cdot}a_{n-1}$.

4. Graficky. Na lepšiu ilustráciu sa v niektorých prípadoch používa aj grafické znázornenie malého počtu členov číselných postupností. Na obrázku (6.1) sú dva spôsoby grafickej reprezentácie prvých štyroch členov postupnosti $\left\{\dfrac{2n-1}{n}\right\}_{n=1}^{\infty}$.



Obrázok 6.1: Grafická reprezentácia postupností

Aritmetická a geometrická postupnosť

Aritmetická postupnosť je postupnosť, v ktorej rozdiel každých dvoch po sebe idúcich členov je rovný konštante: $\forall n \in N\ a_{n+1} - a_n = d$. Napríklad $1, 2, 3, 4, 5, \ldots$ alebo $-5, -2, 1, 4, 7, \ldots$ Vyjadrime n-tý člen aritmetickej postupnosti rekurentne aj vzorcom:

$$\begin{array}{lllll} a_1 & a_2 = a_1 + d & a_3 = a_2 + d & \ldots & a_n = a_{n-1} + d & \ldots \\ a_1 & a_2 = a_1 + d & a_3 = a_1 + 2d & \ldots & a_n = a_1 + (n-1)d & \ldots \end{array}$$

Geometrická postupnosť je postupnosť, v ktorej podiel každých dvoch po sebe idúcich členov je rovný konštante: $\forall n \in N\ a_{n+1}/a_n = q$. Napríklad $1, 2, 4, 8, 16, \ldots$ alebo $4, 2, 1, 1/2, 1/4, 1/8, \ldots$ Vyjadrime n-tý člen geometrickej postupnosti rekurentne aj vzorcom:

$$\begin{array}{lllll} a_1 & a_2 = a_1 q & a_3 = a_2 q & \ldots & a_n = a_{n-1} q & \ldots \\ a_1 & a_2 = a_1 q & a_3 = a_1 q^2 & \ldots & a_n = a_1 q^{n-1} & \ldots \end{array}$$

Reprezentácia reálnych čísel

Reálne čísla zapísané v pozičnej sústave so základom z sa dajú prirodzeným spôsobom vyjadriť pomocou postupností. Nech

$$x = a_0 + a_1 \cdot z^{-1} + a_2 \cdot z^{-2} + \ldots,$$

kde $a_0 \in Z$, $\forall i \in N\ a_i \in \{0, 1, \ldots, z-1\}$. Postupnosť $\{a_n\}_{n=0}^{\infty}$ zodpovedá číslu x.

Iný spôsob vyjadrenia reálnych čísel je pomocou reťazových zlomkov. Je to nasledujúci spôsob:

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ddots}}}},$$

kde a_0 je ľubovoľné celé číslo a koeficienty $a_1, a_2, \ldots$ sú prirodzené čísla. Každý čitatel je rovný jednej, v menovateli je súčet koeficientu a_i a zlomku. V prípade, že x je racionálne číslo, na jeho vyjadrenie nám stačí konečný reťazový zlomok, to znamená, že potrebujeme konečný počet koeficientov a postupnosť $\{a_n\}_{n=1}^{q}$ je konečná. Ak je x iracionálne číslo, tak rozvoj tohto zlomku je nekonečný, podobne ako postupnosť koeficientov $\{a_n\}_{n=1}^{\infty}$. Miesto tohto zápisu sa pri reťazových zlomkoch zaužíval zápis $x = [a_0; a_1, a_2, \ldots]$.

Príklad 6.1.1. *Zapíšme číslo 3/2 pomocou reťazového zlomku:*

$$\frac{3}{2} = 1 + \frac{1}{2} = [1; 2] \ .$$

Príklad 6.1.2. *Skúsme zapísať číslo 49/5 pomocou reťazového zlomku:*

$$\frac{49}{5} = 9 + \frac{4}{5} = 9 + \frac{1}{\frac{5}{4}} = 9 + \frac{1}{1 + \frac{1}{4}} = [9; 1, 4] \ .$$

Príklad 6.1.3. *Na čísle $x_0 = 59/26$ si ukážme podrobnejšie postup, ako nájsť reťazový zlomok zodpovedajúci tomuto číslu.*

$$x_0 = \frac{59}{26} \to x_0 = 2\frac{7}{26} \to a_0 = 2 \to r_0 = \frac{7}{26} \to \frac{1}{r_0} = \frac{26}{7}$$

Číslo $1/r_0 = x_1$ použijeme ako vstup a znova zopakujeme postup z predchádzajúceho riadku.

$$x_1 = \frac{26}{7} \to x_1 = 3\frac{5}{7} \to a_1 = 3 \to r_1 = \frac{5}{7} \to \frac{1}{r_1} = \frac{7}{5}$$

Zopakujeme postup pre $x_2 = 1/r_1$.

$$x_2 = \frac{7}{5} \to x_2 = 1\frac{2}{5} \to a_2 = 1 \to r_2 = \frac{2}{5} \to \frac{1}{r_2} = \frac{5}{2}$$

$$x_3 = \frac{5}{2} \to x_3 = 2\frac{1}{2} \to a_3 = 2 \to r_3 = \frac{1}{2} \to \frac{1}{r_3} = \frac{2}{1}$$

$$x_4 = \frac{2}{1} \to x_4 = 2\frac{0}{1} \to a_4 = 2 \to r_4 = \frac{0}{1} \to \frac{1}{r_4} = \nexists$$

V tejto chvíli postup končí. Hľadané koeficienty sú $[2; 3, 1, 2, 2]$, *takže hľadaný reťazový zlomok má nasledujúci tvar:*

$$2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2}}}}$$

Ako sme už spomenuli, iracionálne čísla majú nekonečný rozvoj. Na ukážku uveďme koeficienty niektorých známych iracionálnych čísel pri ich rozvoji do reťazových zlomkov: $\sqrt{2} = [1; 2, 2, \dots]$, $\pi = [3; 7, 15, 1, 292, 1, \dots]$, $e = [2; 1, 2, 1, 1, 4, 1, \dots]$.

6.2 Vlastnosti postupností

Prejdime si teraz niektoré dôležité vlastnosti, ktoré môžu mať číselné postupnosti. Budeme uvažovať len o postupnostiach, ktorých členy sú reálne čísla.

1. Hovoríme, že postupnosť $\{a_n\}_{n \in I}$ je **konštantná**, ak existuje konštanta $c \in R$ taká, že pre $\forall n \in I$ platí, že $a_n = c$. Napríklad postupnosť $\{a_n\}_{n=1}^{\infty}$, kde pre $\forall n \in N$ $a_n = 3$ je konštantná.

2. Hovoríme, že postupnosť $\{a_n\}_{n \in I}$ je **rastúca**, ak pre $\forall n_1, n_2 \in I$ platí: ak $n_1 < n_2$, potom $a_{n_1} < a_{n_2}$.

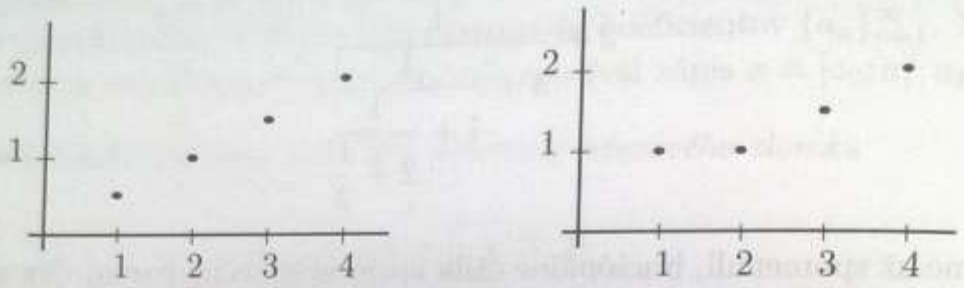
Špeciálne pre postupnosti v tvare $\{a_n\}_{n=p}^{\infty}$ stačí uviesť: $\forall n \in N$ $n \geq p$ $a_n < a_{n+1}$.

Čiže hodnota každého člena postupnosti musí byť väčšia, ako hodnoty všetkých jeho predchodcov.

3. Hovoríme, že postupnosť $\{a_n\}_{n \in I}$ je **neklesajúca**, ak pre $\forall n_1, n_2 \in I$ platí: ak $n_1 < n_2$, potom $a_{n_1} \leq a_{n_2}$.

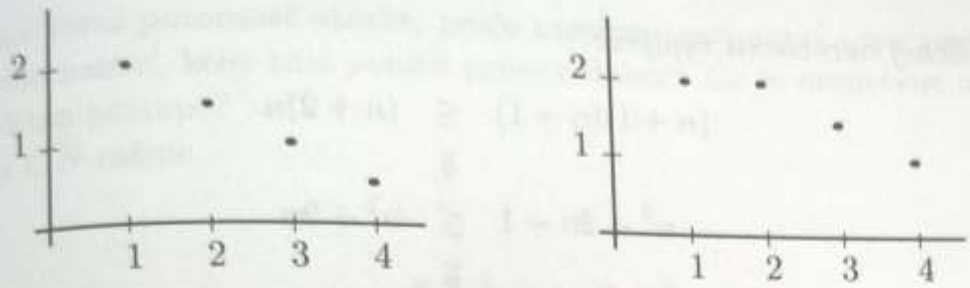
Špeciálne pre postupnosti v tvare $\{a_n\}_{n=p}^{\infty}$ stačí uviesť: $\forall n \in N$ $n \geq p$ $a_n \leq a_{n+1}$.

Čiže hodnota žiadneho člena postupnosti nie je menšia, ako hodnoty všetkých jeho predchodcov. Každá rastúca postupnosť je aj neklesajúcou, ale naopak to neplatí. Na obrázku (6.2) máme porovnanie rastúcej postupnosti (vľavo) a neklesajúcej postupnosti, ktorá nie je rastúca.



Obrázok 6.2: Rastúca a neklesajúca postupnosť

4. Hovoríme, že postupnosť $\{a_n\}_{n\in I}$ je **klesajúca**, ak pre $\forall n_1, n_2 \in I$ platí: ak $n_1 < n_2$, potom $a_{n_1} > a_{n_2}$.
Špeciálne pre postupnosti v tvare $\{a_n\}_{n=p}^{\infty}$ stačí uviesť: $\forall n \in N\ n \geq p$ $a_n > a_{n+1}$.
Čiže hodnota každého člena postupnosti musí byť menšia, ako hodnoty všetkých jeho predchodcov.
5. Hovoríme, že postupnosť $\{a_n\}_{n\in I}$ je **nerastúca**, ak pre $\forall n_1, n_2 \in I$ platí: ak $n_1 < n_2$, potom $a_{n_1} \geq a_{n_2}$.
Špeciálne pre postupnosti v tvare $\{a_n\}_{n=p}^{\infty}$ stačí uviesť: $\forall n \in N\ n \geq p$ $a_n \geq a_{n+1}$.
Čiže hodnota žiadneho člena postupnosti nie je väčšia, ako hodnoty všetkých jeho predchodcov. Každá klesajúca postupnosť je aj nerastúcou, ale naopak to neplatí. Na obrázku (6.3) máme porovnanie klesajúcej postupnosti (vľavo) a nerastúcej postupnosti, ktorá nie je klesajúca.
6. Hovoríme, že postupnosť $\{a_n\}_{n\in I}$ je **zhora ohraničená**, ak $\exists k \in R$ také, že pre $\forall n \in I$ platí $a_n \leq k$.
7. Hovoríme, že postupnosť $\{a_n\}_{n\in I}$ je **zdola ohraničená**, ak $\exists k \in R$ také, že pre $\forall n \in I$ platí $a_n \geq k$.
8. Ak je postupnosť ohraničená zdola aj zhora, tak hovoríme, že je **ohraničená**.



Obrázok 6.3: Klesajúca a nerastúca postupnosť

Ako zisťovať vlastnosti postupností

Ukážme na niekoľkých príkladoch, ako určovať spomínané vlastnosti postupností.

Príklad 6.2.1. *Zistime vlastnosti postupnosti* $\left\{\frac{n+1}{n}\right\}_{n=1}^{\infty}$. *Prvé členy tejto postupnosti sú*

$$2, \frac{3}{2}, \frac{4}{3}, \frac{5}{4}, \frac{6}{5}, \ldots$$

Podľa týchto členov by mala byť postupnosť klesajúca. Potrebujeme však dokázať, že to platí pre všetky členy postupnosti, takže musíme dokázať, že nasledujúci výrok je pravdivý:

$$\forall n \in N \quad \frac{n+1}{n} > \frac{n+2}{n+1}.$$

Z dôvodov, ktoré vysvetlíme nižšie musíme pravdivosť tohto výroku dokazovať nepriamo. Budeme predpokladať, že platí negácia daného výroku. To znamená: $\exists n \in N$ *také, že*

$$\frac{n+1}{n} \leq \frac{n+2}{n+1}.$$

Z uvedenej nerovnosti vyplýva:

$$\begin{aligned} (n+1)(n+1) &\leq (n+2)n \\ &\Downarrow \\ n^2+2n+1 &\leq n^2+2n \\ &\Downarrow \\ 1 &\leq 0\,. \end{aligned}$$

Posledná nerovnosť je samozrejme hlúposť. Z negovaného výroku sme odvodili nezmysel, potom musí platiť pôvodný výrok:

$$\forall n \in N \quad \frac{n+1}{n} > \frac{n+2}{n+1}$$

a postupnosť $\left\{\frac{n+1}{n}\right\}_{n=1}^{\infty}$ *je klesajúca.*

Ďalej ukážeme, že táto postupnosť je zdola ohraničená číslom 1 *(potom bude samozrejme zdola ohraničená aj každým číslom, ktoré je menšie ako* 1*). To znamená, že dokazujeme pravdivosť výroku:*

$$\forall n \in N \quad \frac{n+1}{n} \geq 1\,.$$

Opäť budeme postupovať nepriamo. Predpokladajme, že platí negácia tohto výroku: $\exists n \in N$ *také, že*

$$\frac{n+1}{n} < 1\,.$$

Z tejto nerovnosti vyplýva:

$$\begin{aligned} n+1 &< n \\ &\Downarrow \\ 1 &< 0\,. \end{aligned}$$

Ako vidieť, znova sme dospeli k nezmyslu. Postupnosť je zdola ohraničená číslom 1.

Venujme teraz pozornosť otázke, prečo musíme postupovať nepriamo. Čo by mohlo nastať, keby sme použili priamy dôkaz? Čo je nesprávne na nasledujúcom postupe?
Pre $\forall n \in N$ máme

$$\begin{aligned} \frac{n+1}{n} &> \frac{n+2}{n+1} \\ &\Downarrow \\ (n+1)(n+1) &> (n+2)n \\ &\Downarrow \\ n^2+2n+1 &> n^2+2n \\ &\Downarrow \\ 1 &> 0\,. \end{aligned}$$

Posledná nerovnosť platí, takže máme čo sme potrebovali. Alebo nie? Problém je, že tvrdenie

$$\forall n \in N \ \frac{n+1}{n} > \frac{n+2}{n+1}\,,$$

ktoré dokazujeme a jeho pravdivosť nepoznáme, sme použili, ako predpoklad v implikácii. Vieme však, že implikácia $p \Longrightarrow q$ je v prípade, že výrok p má pravdivostnú hodnotu 0, pravdivá vždy, bez ohľadu na pravdivosť q. Takto by sme sa mohli prepracovať od nepravdivého výroku k pravdivému. K akým absurdnostiam sa môžeme dopracovať pri takomto „dokazovaní", sa presvedčíme na nasledujúcich príkladoch (prevzaté z [17]):

$$\begin{aligned} 0 &= 1 \\ &\Downarrow \\ 1 &= 0 \\ &\Downarrow \\ 0+1 &= 1+0 \\ &\Downarrow \\ 1 &= 1\,. \end{aligned}$$

Posledná rovnosť triviálne platí, každá z troch implikácií je pravdivá, ale naše tvrdenie to nedokazuje. Aby sme toto vedeli dokázať, museli by platiť aj všetky tri opačné implikácie, ale z rovnosti $0+1=1+0$ *nevyplýva* $1=0$, *táto implikácia je nepravdivá.*

Príklad 6.2.3. *Podobne „dokážeme", že pre každé prirodzené číslo* n *platí:* $n \geq n+1$.

$$\begin{aligned} n &\geq n+1 \\ &\Downarrow \\ 0{\cdot}n &\geq 0{\cdot}(n+1) \\ &\Downarrow \\ 0 &\geq 0\,. \end{aligned}$$

Posledná nerovnosť platí, ale nerovnosť $n \geq n+1$ *zjavne pre žiadne prirodzené číslo nie (stačilo by nájsť jediné, aby sme pôvodné tvrdenie popreli). Implikácia*

$$[n \geq n+1] \Rightarrow [0{\cdot}n \geq 0{\cdot}(n+1)]$$

je síce pravdivá pre ľubovoľné $n \in N$, *ale my by sme potrebovali dokázať pravdivosť obrátenej implikácie*

$$[0{\cdot}n \geq 0{\cdot}(n+1)] \Rightarrow [n \geq n+1]\,,$$

čo sa nám určite nepodarí.

6.3 Hromadný bod postupnosti

Nech a je reálne číslo. Každý otvorený interval taký, že $a \in (x, y)$, kde $x, y \in R$ nazveme okolie bodu a. Pre okolie bodu a sa používa značenie $O(a)$. Každý otvorený interval (x, ∞), respektíve $(-\infty, y)$ nazveme okolie bodu ∞, respektíve $-\infty$. Pre tieto okolia sa používa značenie $O(\infty)$, respektíve $O(-\infty)$. Hovorí sa im tiež okolia nevlastných bodov ∞, resp. $-\infty$. Napríklad interval $(-1, 2) = O(1)$ je okolím bodu 1 a intervaly $(-1, \infty)$, $(10001, \infty)$ okoliami (nevlastného) bodu nekonečno.
Nech je a reálne číslo alebo ∞ alebo $-\infty$. Hovoríme, že a je hromadným bodom postupnosti $\{a_n\}_{n=p}^{\infty}$, ak pre ľubovoľné okolie bodu a platí, že nekonečne veľa členov tejto postupnosti patrí do tohto okolia. Priblížme si tento pojem na niekoľkých príkladoch.

Príklad 6.3.1. *Konštantná postupnosť $\{c\}_{n=p}^{\infty}$, kde $p \in Z$, $c \in R$ má jediný hromadný bod - číslo c.*

Príklad 6.3.2. *Vezmime postupnosť $\{(-1)^n\}_{n=1}^{\infty}$. Členy tejto postupnosti nadobúdajú striedavo hodnoty -1 a 1. Nech si zvolíme ľubovoľné okolie bodu 1, nekonečne veľa členov tejto postupnosti (všetky párne) budú ležať v tomto okolí. Podobne to platí aj pre -1. Táto postupnosť má práve dva hromadné body: -1 a 1.*

Všeobecne platí: ak nekonečne veľa členov postupnosti nadobudne hodnotu c, tak c je hromadný bod tejto postupnosti.

Príklad 6.3.3. *V postupnosti $\left\{\sin\left(n\frac{\pi}{2}\right)\right\}_{n=0}^{\infty}$ sa striedajú hodnoty 0, 1, -1 a tie tvoria hromadné body tejto postupnosti.*

Doteraz sme mali príklady, keď hromadný bod postupnosti patril do oboru hodnôt postupnosti. V mnohých prípadoch to tak nie je. Ukážme si teraz príklady postupností, v ktorých hromadný bod nie je rovný žiadnemu členu postupnosti.

Príklad 6.3.4. *Pozrime sa lepšie na postupnosť $\left\{\frac{1}{n}\right\}_{n=1}^{\infty}$. Členy tejto postupnosti sú vždy kladné a postupnosť je klesajúca. Zdá sa, že členy tejto*

postupnosti sú „rozložené v blízkosti" nuly - čím väčšie n zvolíme, tým je člen $a_n = \frac{1}{n}$ bližšie k nule. Presvedčíme sa, že 0 je hromadným bodom tejto postupnosti. Potrebujeme ukázať, že v ľubovoľnom okolí 0 nájdeme nekonečne veľa členov našej postupnosti. Zvoľme si okolie $O_1(0) = (-x_1, x_1)$. Na dolnej hranici okolia samozrejme nezáleží, keďže všetky členy postupnosti sú kladné. Zaujímavá bude pre nás horná hranica tohto intervalu. Hľadáme také členy postupnosti, pre ktoré platí $0 < \frac{1}{n} < x_1$. Nie je ťažké zistiť, že to budú práve tie členy postupnosti $\left\{\frac{1}{n}\right\}_{n=1}^{\infty}$, pre ktoré $n > \frac{1}{x_1}$. Nech je x_1 akékoľvek kladné reálne číslo, vždy bude existovať nekonečne veľa prirodzených čísel n, ktoré sú väčšie ako $\frac{1}{x_1}$ a preto nekonečne veľa členov $\frac{1}{n}$ bude patriť tomuto okoliu. Nech je okolie $O_1(0)$ akékoľvek, bude v ňom nekonečne veľa členov tejto postupnosti a 0 je jej hromadným bodom.

Príklad 6.3.5. *Postupnosť $\left\{(-1)^n \frac{n+1}{n}\right\}_{n=1}^{\infty}$ má hromadné body -1 a 1. Ak vezmeme okolie $O_1(1) = (0, 2)$, budú do neho patriť členy $a_2 = \frac{3}{2}$, $a_4 = \frac{5}{4}$, $a_6 = \frac{7}{6}$, ... (všetky členy postupnosti s párnymi indexmi). Ak okolie zúžime, vypadne z neho len niekoľko prvých členov postupnosti, nekonečne veľa ich tam zostane. Napríklad vezmime okolie $O_2(1) = \left(\frac{1}{2}, \frac{3}{2}\right)$. Vidíme, že $a_2 \notin O_2(1)$, ale ostatné členy s párnymi indexmi tam budú patriť. Ak vezmeme ľubovoľné okolie $O(1) = (x, y)$, hľadáme také párne čísla n, pre ktoré*

$$\frac{n+1}{n} < y\,.$$

Po úprave máme

$$1 < ny - n = n(y-1)$$

a keďže $y > 1$, tak musí platiť

$$n > \frac{1}{y-1}\,.$$

Nech si zvolíme ľubovoľné okolie bodu 1 s hornou hranicou y, vďaka predchádzajúcej nerovnosti ľahko nájdeme najmenšie párne číslo n také, že počnúc týmto číslom budú všetky členy s párnym indexom patriť do zvoleného okolia. Napríklad vezmime okolie $O_3(1) = (0; 1,01)$. Potom platí

$$n > \frac{1}{1,01 - 1} = 100 .$$

Počnúc členom a_{102}, všetky členy s párnymi indexmi (je ich nekonečne veľa) budú patriť do okolia $O_3(1)$. Keď to zhrnieme, tak v každom okolí bodu 1 nájdeme nekonečne veľa členov tejto postupnosti. To znamená, že 1 je hromadný bod tejto postupnosti. Pomocou podobných úvah možno ukázať, že -1 je tiež hromadným bodom tejto postupnosti.

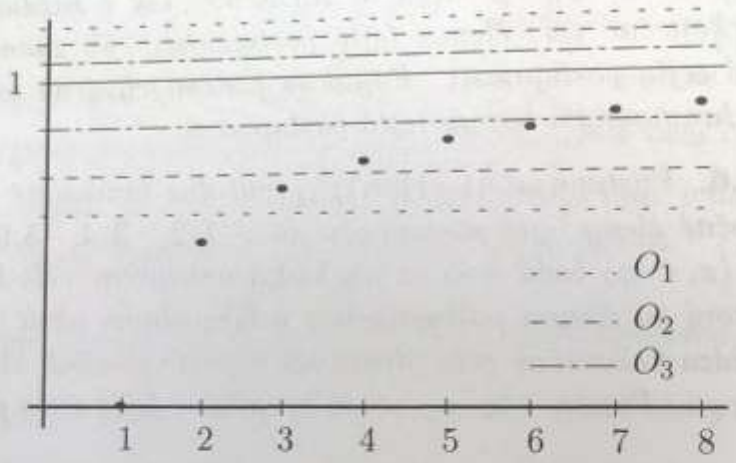
Príklad 6.3.6. *Postupnosť $\{(-1)^n n\}_{n=1}^{\infty}$ má dva hromadné body: $+\infty$ a $-\infty$. Počiatočné členy tejto postupnosti sú: $-1, 2, -3, 4, -5, 6, \ldots$ V ľubovoľnom okolí $(x, +\infty)$ bodu $+\infty$ sa nachádza nekonečne veľa kladných párnych čísel, ktoré sú členmi postupnosti a v ľubovoľnom okolí $(-\infty, y)$ bodu $-\infty$ sa nachádza nekonečne veľa záporných nepárnych čísel, ktoré sú členmi tejto postupnosti. Potom $+\infty$ a $-\infty$ sú hromadné body tejto postupnosti.*

Zamerajme sa teraz špeciálne na postupnosti, ktoré majú práve jeden hromadný bod. Predpokladajme, že postupnosť $\{a_n\}_{n=p}^{\infty}$ má jediný hromadný bod L. V každom okolí L sa teda nachádza nekonečne veľa členov postupnosti a mimo tohto okolia ich musí byť len konečný počet. Ak by tomu tak nebolo a mimo niektorého okolia $O_i(L)$ by sa nachádzalo nekonečne veľa členov tejto postupnosti, tak by tam nutne musel existovať ďalší hromadný bod okrem L. Zjednodušene (ale z matematického hľadiska trochu nepresne) si to môžeme predstaviť tak, že tých nekonečne veľa členov mimo okolia $O_i(L)$ možno „schovať" do jedného, alebo viacerých intervalov, pričom každý z týchto intervalov bude obsahovať nekonečne veľa členov postupnosti a v každom zo spomenutých intervalov vieme potom nájsť ďalšie hromadné body.

Ak má teda postupnosť len jeden hromadný bod L, tak pri zvolení akéhokoľvek okolia tohto bodu zostane mimo tohto okolia len konečný počet

členov postupnosti. Z toho možno odvodiť záver, že pre ľubovoľné okolie bude existovať index $n_0 \in Z$, $n_0 \geq p$ taký, že všetky členy tejto postupnosti počnúc členom a_{n_0} budú patriť do daného okolia.

Príklad 6.3.7. *Situáciu máme na obrázku (6.4) pre postupnosť* $\left\{\frac{n-1}{n}\right\}_{n=1}^{\infty}$. *Jej jediný hromadný bod je* 1 *a hodnoty prvých členov* $a_1 = 0, a_2 = \frac{1}{2}, a_3 =$



Obrázok 6.4: Postupnosť s jedným hromadným bodom

$\frac{2}{3}, a_4 = \frac{3}{4}, a_5 = \frac{4}{5}, a_6 = \frac{5}{6}, a_7 = \frac{6}{7}, a_8 = \frac{7}{8}, \ldots$. *Do okolia* $O_1(1)$ *patria všetky členy postupnosti počnúc členom* a_3, *do* $O_2(1)$ *všetky členy počnúc* a_4, *do* $O_3(1)$ *všetky členy počnúc* a_7.

Z predchádzajúcich úvah a príkladov si možno uvedomiť, že postupnosti, ktoré majú jeden hromadný bod z množiny R, sa správajú nasledujúco: čím sú indexy členov väčšie, tým sú členy postupnosti viac „nalepené“ na tento hromadný bod (trochu slušnejšie povedané - blížia sa k tejto hodnote). Ak je tento hromadný bod $+\infty$ (resp. $-\infty$) tak členy postupnosti rastú nad všetky hranice - blížia sa k $+\infty$ (resp. klesajú pod všetky hranice - blížia sa k $-\infty$).

6.4 Limita postupnosti

Postupnosti s jedným hromadným bodom, o ktorých sme hovorili v závere predchádzajúcej časti, majú v matematike dôležité postavenie a toto postavenie súvisí s pojmom limita, ktorému sa teraz budeme venovať.

Definícia 6.4.1. *Hovoríme, že postupnosť $\{a_n\}_{n=p}^{\infty}$ má limitu rovnú L, keď L je jediný hromadný bod tejto postupnosti ($L \in R$, alebo $L = \pm\infty$). Zapisujeme to*

$$\lim_{n\to\infty} a_n = L \, .$$

Pojem limita teda vyjadruje približovanie sa členov postupnosti k jednej hodnote - jedinému hromadnému bodu tejto postupnosti. Aby sme nezostali len pri abstraktnej definícii, uveďme niekoľko príkladov.

Príklad 6.4.1. *Konštantná postupnosť $\{c\}_{n=p}^{\infty}$, kde $c \in R$ má jediný hromadný bod c, takže*

$$\lim_{n\to\infty} c = c \, .$$

Príklad 6.4.2. *Mali sme spomenuté postupnosti $\{1/n\}_{n=1}^{\infty}$ a $\{(n-1)/n\}_{n=1}^{\infty}$, ktoré majú jeden hromadný bod: 0, resp. 1. Preto*

$$\lim_{n\to\infty} \frac{1}{n} = 0 \quad a \quad \lim_{n\to\infty} \frac{n-1}{n} = 1 \, .$$

Príklad 6.4.3. *Postupnosti $\{n\}_{n=1}^{\infty}$, respektíve $\{-n\}_{n=1}^{\infty}$ majú jediný hromadný bod $+\infty$ resp. $-\infty$. Preto*

$$\lim_{n\to\infty} n = +\infty \quad a \quad \lim_{n\to\infty} (-n) = -\infty \, .$$

Vlastnosti limít

Určovanie limít pomocou hromadných bodov je dosť ťažkopádne. Výhodnejšie je využiť k ich výpočtu niektoré ich vlastnosti. Dôkazy platnosti týchto vlastností možno nájsť napríklad v [7].

1. Ak je postupnosť neklesajúca a zhora ohraničená (nerastúca a zdola ohraničená), potom má limitu. Napríklad postupnosť $\{1/n\}_{n=1}^{\infty}$ je klesajúca (takže aj nerastúca) a zdola ohraničená. Jej limita je 0, ako bolo spomenuté v príklade 6.4.2.

2. Nech

$$\lim_{n\to\infty} a_n = a \quad \text{a} \quad \lim_{n\to\infty} b_n = b$$

sú limity postupností $\{a_n\}_{n=p}^{\infty}$ a $\{b_n\}_{n=p}^{\infty}$, pričom a, b sú reálne čísla a $c \in R$ je konštanta. Potom

$$\begin{aligned}
\lim_{n\to\infty} (a_n + b_n) &= a + b \\
\lim_{n\to\infty} (a_n - b_n) &= a - b \\
\lim_{n\to\infty} (ca_n) &= c \cdot a \\
\lim_{n\to\infty} (a_n \cdot b_n) &= a \cdot b\,.
\end{aligned}$$

Ak navyše pre ľubovoľné $n \in Z$, $n \geq p$ máme $b_n \neq 0$ a $b \neq 0$, tak platí:

$$\lim_{n\to\infty} \frac{a_n}{b_n} = \frac{a}{b}\,.$$

Príklad 6.4.4. *Vypočítajme limitu*

$$\lim_{n\to\infty} \frac{n^2+n}{n^2}\,.$$

Vieme, že

$$\frac{n^2+n}{n^2} = \frac{n^2}{n^2} + \frac{n}{n^2} = 1 + \frac{1}{n}\,.$$

Keďže

$$\lim_{n\to\infty} 1 = 1 \quad a \quad \lim_{n\to\infty} \frac{1}{n} = 0\,,$$

tak podľa vlastností limity súčtu dvoch postupností dostávame:

$$\lim_{n\to\infty} \frac{n^2+n}{n^2} = \lim_{n\to\infty} 1 + \lim_{n\to\infty} \frac{1}{n} = 1 + 0 = 1\,.$$

Príklad 6.4.5. *Vypočítajme limitu postupnosti* $\{(-1)/n\}_{n=1}^{\infty}$.

$$\lim_{n\to\infty} \frac{-1}{n} = \lim_{n\to\infty} \left(-\frac{1}{n}\right) = (-1)\cdot \lim_{n\to\infty} \frac{1}{n} = (-1)\cdot 0 = 0\,.$$

Príklad 6.4.6. *Podobne vypočítajme limitu*

$$\lim_{n\to\infty} \frac{1}{n^2}\,.$$

Keďže $1/n^2 = (1/n)\cdot(1/n)$ *a limita postupnosti* $\{1/n\}_{n=1}^{\infty}$ *je 0, tak platí:*

$$\lim_{n\to\infty} \frac{1}{n^2} = 0\cdot 0 = 0\,.$$

3. Nech $\{a_n\}_{n=p}^{\infty}$, $\{b_n\}_{n=p}^{\infty}$, $\{c_n\}_{n=p}^{\infty}$ sú také postupnosti, že $\forall n \in Z$, $n \geq p$ platí $a_n \leq b_n \leq c_n$ a

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} c_n\,.$$

Potom

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n = \lim_{n\to\infty} c_n\,.$$

Príklad 6.4.7. *Vypočítajme*

$$\lim_{n\to\infty} \frac{(-1)^n}{n}\,.$$

Pre $\forall n \in N$ *platí, že*

$$\frac{-1}{n} \leq \frac{(-1)^n}{n} \leq \frac{1}{n}$$

a tiež

$$\lim_{n\to\infty} \frac{-1}{n} = \lim_{n\to\infty} \frac{1}{n} = 0\,.$$

Potom platí:

$$\lim_{n\to\infty} \frac{(-1)^n}{n} = 0\,.$$

4. Nech

$$\lim_{n\to\infty} a_n = c \in R \text{ a } \lim_{n\to\infty} b_n = \pm\infty .$$

Potom

$$\lim_{n\to\infty} \frac{a_n}{b_n} = 0 \text{ a } \lim_{n\to\infty} \frac{b_n}{a_n} = \begin{cases} \pm\infty & ,ak \quad c > 0 \\ \mp\infty & ,ak \quad c < 0 \end{cases}$$

Príklad 6.4.8. *Vezmime postupnosti* $\{1\}_{n=1}^{\infty}$ *a* $\{n\}_{n=1}^{\infty}$. *Keďže*

$$\lim_{n\to\infty} 1 = 1 \in R \quad a \quad \lim_{n\to\infty} n = \infty ,$$

tak platí

$$\lim_{n\to\infty} \frac{1}{n} = 0 \quad a \quad \lim_{n\to\infty} \frac{n}{1} = \infty ,$$

čo sa zhoduje s našimi predchádzajúcimi úvahami o týchto limitách.

5. Nech

$$\lim_{n\to\infty} a_n = c \in R, \quad \lim_{n\to\infty} b_n = 0$$

a pre $\forall n \in Z$, $n \geq p$ platí $b_n > 0$. Potom

$$\lim_{n\to\infty} \frac{a_n}{b_n} = \infty .$$

Niektoré dôležité limity postupností

1. Pre geometrickú postupnosť $\{q^n\}_{n=1}^{\infty}$ platí:

$$\lim_{n\to\infty} q^n = \begin{cases} \infty & ,ak \quad q > 1 \\ 1 & ,ak \quad q = 1 \\ 0 & ,ak \quad q \in (-1, 1) \\ \nexists & ,ak \quad q \leq -1 \end{cases}$$

2. V prípade, že $\{a_n\}_{n=p}^{\infty}$, $\{b_n\}_{n=p}^{\infty}$ sú rastúce postupnosti,

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n = \infty$$

a

$$\lim_{n\to\infty} \frac{a_n}{b_n} = 0 \,,$$

tak postupnosť v menovateli rastie oveľa rýchlejšie. Tieto úvahy sa využívajú pri porovnávaní výpočtovej náročnosti algoritmov. Ak máme algoritmus (počítačový program) na riešenie nejakého problému, ktorý pri vstupe veľkosti n (napríklad počet bitov) vykoná v najhoršom prípade a_n krokov a iný algoritmus (program) na riešenie toho istého problému, ktorý pri vstupe veľkosti n vykoná v najhoršom prípade b_n krokov, pričom pre postupnosti $\{a_n\}_{n=p}^{\infty}$, $\{b_n\}_{n=p}^{\infty}$ platia už spomenuté podmienky, tak môžeme skonštatovať, že prvý algoritmus je rýchlejší, ako druhý. Z tohto pohľadu sú pre nás dôležité nasledujúce postupnosti a limity:
Nech $k \in R^+$ a $q > 1$ sú konštanty. Pre postupnosti $\{n^2\}_{n=1}^{\infty}$, $\{n^k\}_{n=1}^{\infty}$, $\{2^n\}_{n=1}^{\infty}$, $\{q^n\}_{n=1}^{\infty}$, $\{n!\}_{n=1}^{\infty}$ a $\{n^n\}_{n=1}^{\infty}$ platí:

$$\lim_{n\to\infty} \frac{n^2}{2^n} = 0, \quad \lim_{n\to\infty} \frac{n^k}{q^n} = 0, \quad \lim_{n\to\infty} \frac{q^n}{n!} = 0, \quad \lim_{n\to\infty} \frac{n!}{n^n} = 0 \,.$$

3. Za jedno z najdôležitejších čísel v matematike je považované číslo $e = 2,71828\ldots$, ktoré je nazvané podľa švajčiarskeho velikána matematiky Leonharda Eulera (1707-1783) - Eulerovo číslo. Definujeme ho pomocou nasledujúcej limity

$$e = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n \,.$$

Je prekvapujúce, kde všade sa toto číslo vyskytuje. Môžeme sa s ním stretnúť pri zloženom úročení, pri určovaní počtu nerozpadnutých jadier pri rádioaktívnom rozpade, pri popise javov v atmosfére alebo v elektrickom kondenzátore, nezaobíde sa bez neho ani moderná štatistika. Toto nenápadné číslo je natoľko dôležité, že je mu venovaný pekný článok aj v jednom obrázkovom týždenníku [18].

Kapitola 7

Reálne funkcie reálnej premennej

Reálna funkcia reálnej premennej je funkcia, ktorá priraďuje reálnemu číslu hodnotu z množiny reálnych čísel. Budeme používať predpis $y = f(x)$, ktorý je bežný pre takéto funkcie. Pri reálnych funkciách reálnej premennej sa za definičný obor zvykne považovať „maximálna" podmnožina množiny reálnych čísel, ktoré môžeme dosadiť za x do predpisu $y = f(x)$. Čiže definičný obor (budeme ho označovať D_f) aj obor hodnôt (označenie H_f) sú podmnožiny reálnych čísel.

Zopakujme si niektoré vlastnosti reálnych funkcií.
Nech je daná funkcia $f(x)$ a interval $(a, b) \subseteq D_f$.
Nech pre ľubovoľné $x_1, x_2 \in (a, b)$ $x_1 < x_2$ platí $f(x_1) < f(x_2)$ (resp. $f(x_1) > f(x_2)$). Potom hovoríme, že funkcia f je na intervale (a, b) **rastúca** (resp. **klesajúca**).
Nech existuje okolie $O(x_0)$ bodu $x_0 \in D_f$ také, že pre ľubovoľné $x \in O(x_0)$, $x \neq x_0$ platí $f(x) < f(x_0)$ (resp. $f(x) > f(x_0)$). Potom hovoríme, že funkcia $f(x)$ má v bode x_0 **lokálne maximum** (resp. **lokálne minimum**).
Lokálne maximá aj minimá nazývame **lokálne extrémy** funkcie.

7.1 Príklady reálnych funkcií reálnej premennej

Konštantná funkcia

Konštantná funkcia je funkcia, ktorej definičný obor je celá množina reálnych čísel a jej predpis je $f(x) = c$, kde c je reálne číslo.

Lineárna funkcia

Auto sa pohybuje rovnomerne rýchlosťou $40km/h$. Ako závisí prejdená dráha s od doby jazdy auta t? Trochu zlomyseľná, ale pravdivá odpoveď by mohla znieť, že lineárne. To znamená, že čas t vynásobíme konštantou (v tomto prípade rýchlosťou v): $s(t) = vt$. Ak sme čas začali merať neskôr, ako auto vyrazilo, tak celková dráha je $s(t) = vt + s_0$, kde s_0 je dráha, ktorú auto prešlo do okamihu, kedy sme začali merať čas.

Lineárna funkcia je daná predpisom $f(x) = kx + q$, kde $k, q \in R$. Grafom tejto funkcie je priamka, ktorá pretína os x v bode so súradnicami $\left(-\frac{q}{k}, 0\right)$ a os y v bode so súradnicami $(0, q)$.

Polynómy

Polynóm je funkcia v tvare

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

kde $a_n \neq 0$, $a_i \in R$. Konštantnú a lineárnu funkciu považujeme za špeciálne prípady polynómov.

Exponenciálna funkcia

Väčšina z vás určite pozná historku o mudrcovi, ktorý vymyslel šach. Jeho vládca ho chcel odmeniť a spýtal sa ho, čo žiada za túto hru. Mudrc sa zamyslel a odvetil, že žiada obilie. Za prvé políčko šachovnice jedno zrnko,

za druhé políčko dve zrnká, za tretie políčko štyri zrnká, za každé ďalšie políčko dvojnásobok počtu zrniek z predchádzajúceho políčka. Vieme, ako to dopadlo. Vládca nebol schopný túto požiadavku splniť, napriek tomu, že na začiatku krútil hlavou, aká je to slabá požiadavka - žiadny z jeho dobre platených radcov mu totiž nepovedal nič o záludnostiach exponenciálneho rastu.

Pod slovíčkom exponenciálny si väčšina ľudí predstaví zdvojnásobenie počtu v každom ďalšom kroku, čiže čísla $2^0, 2^1, 2^2, \ldots, 2^n, \ldots$ Exponenciálna funkcia je však definovaná na celej množine reálnych čísel. Zápis je $f(x) = a^x$, kde základ $a \in R^+$, $a \neq 1$. Najčastejšie používané základy sú asi $a = 2$, $a = 10$, $a = e$. Definičným oborom tejto funkcie je celá množina reálnych čísel (do predpisu a^x môžeme dosadiť ľubovoľné reálne číslo). Oborom hodnôt je množina kladných reálnych čísel.

Logaritmická funkcia

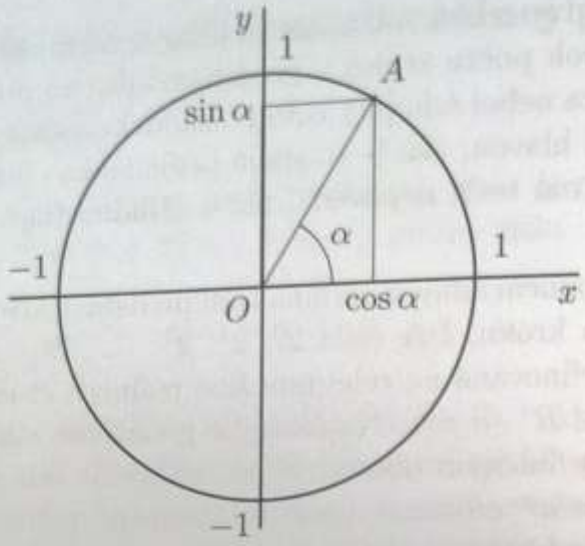
Položme si takúto otázku. Koľko bitov potrebujeme na zápis čísel od 0 až po 255 (číselný typ byte)? Potrebujeme zapísať 256 čísel pomocou núl a jednotiek. Aby sme zistili počet bitov, potrebujeme zistiť, akým exponentom musíme umocniť dvojku, aby sme dostali 256? Alebo sa pýtame, čomu sa rovná $\log_2 256$? Všeobecne sa môžeme pýtať: akým exponentom y musíme umocniť základ z, aby sme dostali číslo x? Hľadaný exponent je

$$y = \log_z x \ ,$$

čiže logaritmus z čísla x pri základe z.

Goniometrické funkcie

Predstavme si bod A, ktorý sa pohybuje po kružnici s polomerom 1 (pozri obrázok 7.1). Ak vieme, že sa bude stále pohybovať po tej kružnici, tak na presné určenie jeho polohy potrebujeme jeden údaj. Najjednoduchšie je uviesť uhol α, ktorý zvierajú úsečka OA s kladnou polosou x. Ak však chceme určiť x-ovú a y-ovú súradnicu bodu A v pravouhlej súradnicovej



Obrázok 7.1: Jednotková kružnica

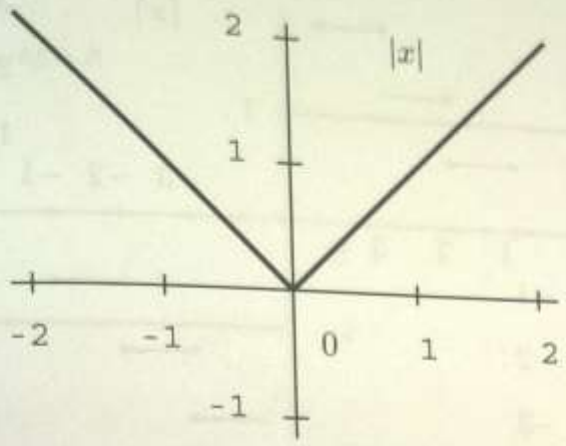
sústave s počiatkom v bode O, tak x-ová súradnica zodpovedá hodnote $\cos\alpha$ a y-ová zasa hodnote $\sin\alpha$. Čiže funkcie $\sin x$ a $\cos x$ vyjadrujú zmenu y-ovej a x-ovej súradnice pri pohybe na kružnici v závislosti od meniaceho sa uhla.

Niektoré ďalšie funkcie

Absolútna hodnota z reálneho čísla je funkcia, pre ktorú platí predpis

$$f(x) = |x| = \begin{cases} x & \text{ak } x \in \langle 0, \infty), \\ -x & \text{ak } x \in (-\infty, 0). \end{cases}$$

Definičný obor tejto funkcie je celá množina reálnych čísel.
Dolná a horná celá časť z reálneho čísla. Pre každé reálne číslo x, ktoré nie je celé číslo ($x \in R - Z$) existuje také celé číslo k, že $k < x < k+1$. Číslo k nazveme dolná celá časť z x - značíme to $\lfloor x \rfloor$ a číslo $k+1$ nazveme horná celá časť z x - značíme to $\lceil x \rceil$. Ak je x celé číslo, potom $x = \lfloor x \rfloor = \lceil x \rceil$. Definičný obor týchto funkcií je celá množina reálnych čísel a grafy týchto funkcií sú



Obrázok 7.2: Graf funkcie $f(x) = |x|$

na obrázku 7.3. Funkciu dolná celá časť môžeme napríklad využiť pri určení minimálneho počtu bitov potrebných na reprezentáciu prirodzeného čísla n:

$$\lfloor \log_2 n \rfloor + 1 .$$

Funkcia signum, alebo „znamienková" funkcia je daná predpisom

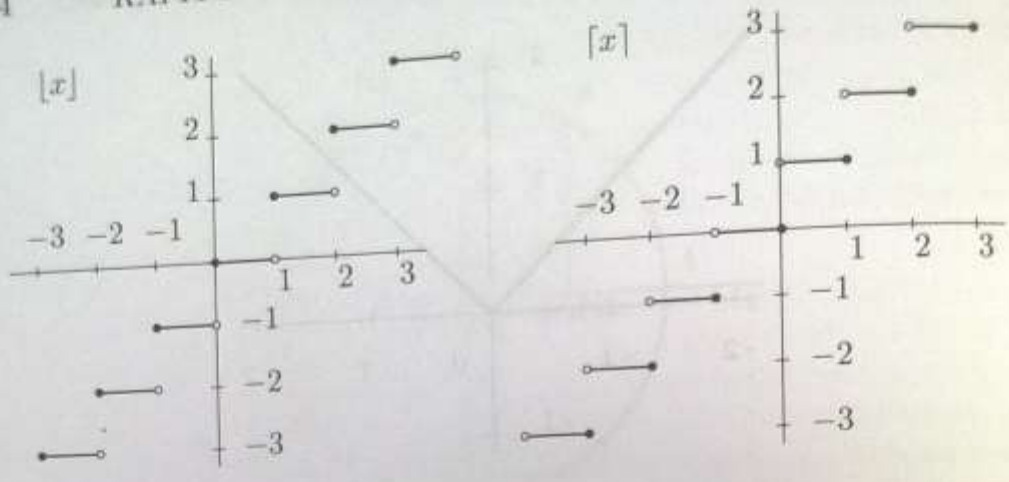
$$f(x) = sgn\ x = \begin{cases} 1 & \text{ak } x \in (0, \infty), \\ 0 & \text{ak } x = 0, \\ -1 & \text{ak } x \in (-\infty, 0). \end{cases}$$

Jej definičný obor je tiež celá množina reálnych čísel a jej graf je na obrázku 7.4.

Dirichletova funkcia je veľmi špeciálna funkcia definovaná na celej množine reálnych čísel. Často slúži ako kontrapríklad k rôznym tvrdeniam. Jej predpis je

$$\chi(x) = \begin{cases} 1 & \text{ak } x \in Q, \\ 0 & \text{ak } x \in R - Q. \end{cases}$$

Čiže funkcia nadobúda hodnotu 1, ak x je racionálne číslo a hodnotu 0, ak x je iracionálne číslo. (Graf tejto funkcie by sa nám asi nepodarilo nakresliť.)



Obrázok 7.3: Grafy funkcií $\lfloor x \rfloor$ a $\lceil x \rceil$

7.2 Ako merať zmenu veličín

Všetko okolo nás sa neustále mení. Pri javoch, ktorých správanie vieme opísať (aspoň približne) pomocou funkcií, vieme často kvantitatívne vyhodnotiť aj to, ako sa menia. Jednoduchý príklad takéhoto javu nám poskytuje fyzika.

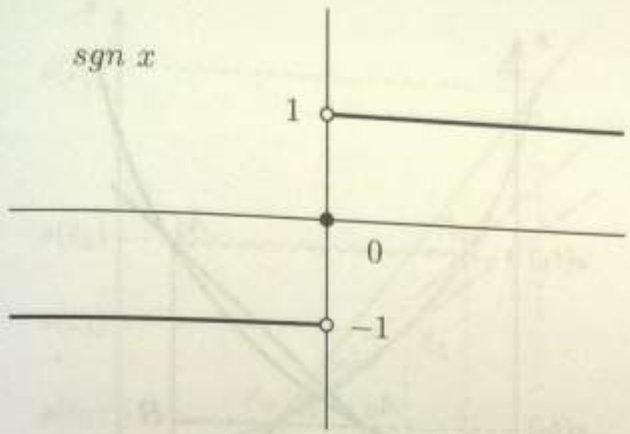
Vezmime si funkciu $s(t)$ vyjadrujúcu dráhu (napríklad v metroch), ktorú prejde teleso v závislosti od času (v sekundách). Z fyziky vieme, že priemerná rýchlosť telesa v dobe medzi časovými okamihmi t_0 a t_1 sa dá vypočítať ako podiel dráhy a času, čo v našom prípade znamená

$$v_p = \frac{s(t_1) - s(t_0)}{t_1 - t_0} .$$

Na obrázku (7.5) vidíme, že pre tento podiel platí

$$\frac{|A_1B|}{|A_0B|} = \frac{s(t_1) - s(t_0)}{t_1 - t_0} = \tan\alpha .$$

Venujme sa teraz otázke, ako vypočítať okamžitú rýchlosť v čase t_0. Ak je zvolený časový úsek od t_0 po t_1 príliš veľký, priemerná rýchlosť môže byť od



Obrázok 7.4: Graf funkcie $f(x) = sgn\ x$

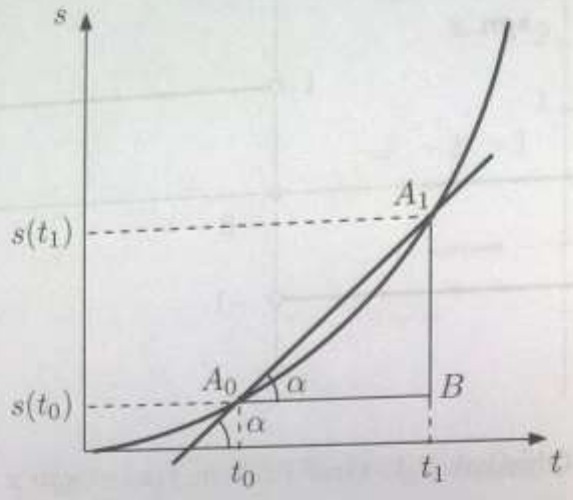
okamžitej rýchlosti veľmi ďaleko. Z priemernej rýchlosti nevieme povedať, aká bola okamžitá rýchlosť v danom čase t_0. Nie je ťažké si však predstaviť, že pri skracovaní tohto časového úseku, z ktorého počítame priemernú rýchlosť (ako je to na obrázku (7.6)), sa bude priemerná rýchlosť na danom úseku blížiť k okamžitej rýchlosti v čase t_0 a geometricky sa dá vyjadriť okamžitá rýchlosť ako tangens uhla, ktorý zviera dotyčnica ku krivke v bode t_0 s časovou osou. Ak by sme zvolili čas t_n, ktorý by bol „nekonečne blízko" k t_0, tak priemerná rýchlosť na tomto úseku by bola „nekonečne blízko" k okamžitej rýchlosti v čase t_0. Recept, ako pristupovať k slovnému spojeniu „nekonečne blízko", nám dala limita postupnosti. Ak by sme hodnoty $t_1, t_2, \ldots, t_n, \ldots$ volili tak, že pre postupnosť $\{t_n\}_{n=1}^{\infty}$ (kde $t_n \neq t_0$) by platilo

$$\lim_{n\to\infty} t_n = t_0 \ ,$$

potom výpočtom limity

$$\lim_{n\to\infty} \frac{s(t_n) - s(t_0)}{t_n - t_0} \tag{7.1}$$

dostaneme okamžitú rýchlosť v čase t_0. Ak chceme vyjadriť vzťah pre okamžitú rýchlosť v ľubovoľnom čase t z intervalu (a, b) ako funkciu času, tak miesto dosadenia konkrétnej hodnoty t_0 vyjadrujeme výslednú limitu ako



Obrázok 7.5: Výpočet priemernej rýchlosti

funkciu premennej t. Objasnime si to na nasledujúcom príklade.

Príklad 7.2.1. *Dráha telesa pri voľnom páde je daná vzťahom* $s(t) = 1/2gt^2$ *(*$g = 9,8\,ms^{-2}$*). Skúsme určiť rýchlosť telesa v čase* $t_0 = 2$ *a vzťah pre rýchlosť tohto telesa v čase* $t \in \langle 0, t_d \rangle$*, kde* t_d *je čas dopadu. Predpokladajme, že máme nejakú postupnosť hodnôt* $\{t_n\}_{n=1}^{\infty}$ *(*$t_n \neq 2$*) takú, že*

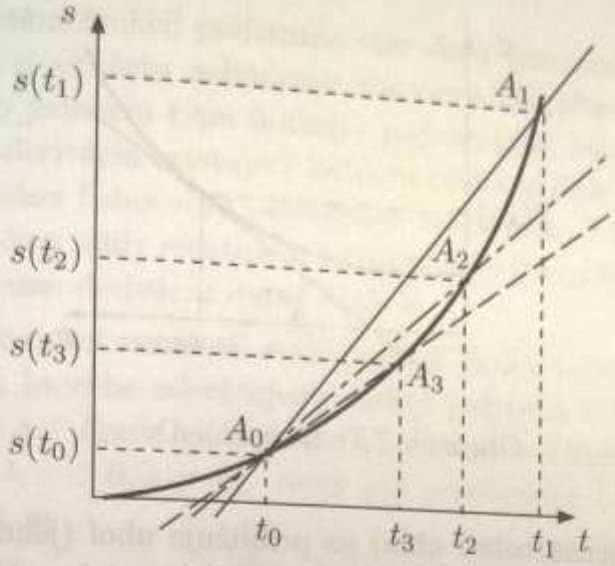
$$\lim_{n\to\infty} t_n = 2$$

a vypočítajme limitu

$$\lim_{n\to\infty} \frac{s(t_n) - s(2)}{t_n - 2} = \lim_{n\to\infty} \frac{1/2gt_n^2 - 1/2g2^2}{t_n - 2} = \frac{1}{2}g \lim_{n\to\infty} \frac{t_n^2 - 2^2}{t_n - 2} =$$
$$\frac{1}{2}g \lim_{n\to\infty} (t_n + 2) = \frac{1}{2}g(\lim_{n\to\infty} t_n + \lim_{n\to\infty} 2) = 2 \cdot g\ ,$$

to znamená, že $v(2) = 19,6\,m \cdot s^{-1}$*. Určíme teraz všeobecný vzťah. Nech je dané* $t \in \langle 0, t_d \rangle$ *a postupnosť* $\{t_n\}_{n=1}^{\infty}$ *(*$t_n \neq t$*), pre ktorú platí*

$$\lim_{n\to\infty} t_n = t\ .$$



Obrázok 7.6: K výpočtu okamžitej rýchlosti

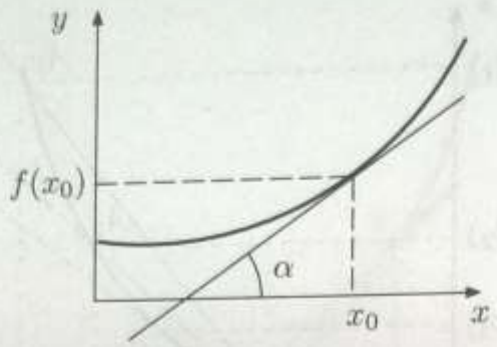
Všeobecný vzťah je

$$\lim_{n\to\infty}\frac{s(t_n)-s(t)}{t_n-t} = \lim_{n\to\infty}\frac{1/2gt_n^2-1/2gt^2}{t_n-t} = \frac{1}{2}g\lim_{n\to\infty}\frac{t_n^2-t^2}{t_n-t} =$$
$$\frac{1}{2}g\lim_{n\to\infty}(t_n+t) = \frac{1}{2}g(\lim_{n\to\infty}t_n+\lim_{n\to\infty}t) = \frac{1}{2}g(t+t) = gt\ ,$$

čo je presne v zhode s poznatkami z fyziky o rýchlosti telesa pri voľnom páde.

Prechod od funkcie $s(t) = \frac{1}{2}gt^2$ k funkcii $v(t) = gt$ sa nazýva derivovanie funkcie $s(t)$ podľa premennej t a $v(t)$ nazývame deriváciou funkcie $s(t)$ podľa t. Rýchlosť (teda derivácia dráhy) vyjadruje zmenu dráhy v závislosti od t.

Skúsme teraz zovšeobecniť naše úvahy. Nahraďme $s(t)$ ľubovoľnou reálnou funkciou $f(x)$ a hľadajme jej deriváciu v bode $x_0 \in D_f$. Geometricky vyjadrené, derivácia v bode x_0 zodpovedá tangensu uhla α, ktorý zviera dotyčnica ku krivke $f(x)$ v bode x_0 s x-ovou osou. Spôsob, ako hľadáme deriváciu je veľmi podobný postupu, ktorý sme použili v príklade o dráhe a rýchlosti. Bodmi $x_1, x_2, \ldots, x_n, \ldots$ sa približujeme k x_0 a snažíme sa zistiť, k akému



Obrázok 7.7: Dotyčnica v x_0

uhlu (resp. tangensu tohto uhla) sa približuje uhol (jeho tangens) sečníc, ktoré prechádzajú dvojicami bodov so súradnicami $(x_0, f(x_0))$ a $(x_i, f(x_i))$ $(i = 1, 2, \dots)$. Dôležitá vec, ktorú musíme spomenúť je, že derivácia funkcie $f(x)$ v tomto bode vôbec nemusí existovať (to je rozdiel oproti dráhe a rýchlosti), pretože ani dotyčnica v tom bode nemusí existovať. Napríklad funkcia $|x|$ nemá dotyčnicu a deriváciu pre $x_0 = 0$. Aby derivácia v bode x_0 existovala, tak nestačí zobrať jednu postupnosť hodnôt $\{x_n\}_{n=1}^{\infty}$ (kde $x_n \in D_f$) takú, že

$$\lim_{n\to\infty} x_n = x_0 \tag{7.2}$$

a vypočítať

$$\lim_{n\to\infty} \frac{f(x_n) - f(x_0)}{x_n - x_0}, \tag{7.3}$$

ale pre každú postupnosť hodnôt z definičného oboru spĺňajúcu (7.2) by sa limita (7.3) musela rovnať tomu istému číslu. Deriváciu funkcie $f(x)$ v bode $x_0 \in D_f$ budeme označovať $f'(x_0)$. Podobne, ako pri dráhe a rýchlosti, aj vo všeobecnosti možno vyjadriť deriváciu funkcie pre každé $x \in D_f$, pre ktoré existuje, ako novú funkciu, odvodenú z $f(x)$. Túto funkciu budeme označovať $f'(x)$, nazývame ju deriváciou funkcie $f(x)$ podľa premennej x, jej definičný obor značíme $D_{f'}$, pričom platí $D_{f'} \subseteq D_f$. Platí teda, že $v(t) = s'(t)$. Poznamenajme, že pre deriváciu $f(x)$ podľa premennej x sa používa (hlavne vo fyzike) aj značenie $\frac{df}{dx}$, čiže $v(t) = \frac{ds}{dt}$.

Keďže je deriváciám funkcií podstatne viac času venovaného v matematickej analýze, my si situáciu nebudeme zbytočne komplikovať a budeme sa venovať ďalej len jednému typu funkcií - polynómom, ktoré majú tú peknú vlastnosť, že ich derivácia existuje v každom reálnom čísle. Nám stačí na jej určenie zobrať jednu ľubovoľnú postupnosť spĺňajúcu (7.2) a z limity (7.3) (ktorá pre polynómy vždy existuje a nezávisí od výberu členov postupnosti $\{x_n\}_{n=1}^{\infty}$) dostávame deriváciu danej funkcie.

Aby sme pri derivovaní nemuseli stále počítať limity, odvoďme jednoduchý vzorec, pomocou ktorého zderivujeme každý polynóm v ľubovoľnej pevne zvolenej hodnote $x \in R = D_f$. Začnime polynómom druhého stupňa $f(x) = ax^2 + bx + c$ $(a, b, c \in R, a \neq 0)$. Nech pre postupnosť $\{x_n\}_{n=1}^{\infty}$, $(x_n \neq x)$ hodnôt z R platí, že

$$\lim_{n\to\infty} x_n = x \,. \tag{7.4}$$

Potom

$$\begin{aligned}
f'(x) &= \lim_{n\to\infty} \frac{f(x_n) - f(x)}{x_n - x} \\
&= \lim_{n\to\infty} \frac{ax_n^2 + bx_n + c - ax^2 - bx - c}{x_n - x} \\
&= a\cdot \lim_{n\to\infty} \frac{x_n^2 - x^2}{x_n - x} + b\cdot \lim_{n\to\infty} \frac{x_n - x}{x_n - x} + \lim_{n\to\infty} \frac{c - c}{x_n - x} \\
&= a\cdot \lim_{n\to\infty} \frac{(x_n - x)(x_n + x)}{x_n - x} + b\cdot 1 + 0 \\
&= a(\lim_{n\to\infty} x_n + \lim_{n\to\infty} x) + b \\
&= 2ax + b \,.
\end{aligned}$$

To znamená, že derivácia $f'(x)$ polynómu druhého stupňa $f(x)$ sa dá jednoducho spočítať podľa vzťahu $f'(x) = 2ax + b$ $(a, b \in R,\ a \neq 0)$.

Napríklad zderivujme polynóm $f(x) = 3x^2 + 4x + 2$. Derivácia $f'(x) = 2\cdot 3\cdot x + 4 = 6x + 4$.

Vypočítajme deriváciu polynómu

$$f_k(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0$$

v pevne zvolenom bode $x \in R$. Nech $\{x_n\}_{n=1}^{\infty}$ (kde $x_n \neq x$) je postupnosť spĺňajúca

$$\lim_{n\to\infty} x_n = x$$

a počítajme

$$\begin{aligned} f_k'(x) &= \lim_{n\to\infty} \frac{f_k(x_n) - f_k(x)}{x_n - x} \\ &= \lim_{n\to\infty} \frac{a_k x_n^k + \cdots + a_1 x_n + a_0 - a_k x^k - \cdots - a_1 x - a_0}{x_n - x} \\ &= a_k \lim_{n\to\infty} \frac{x_n^k - x^k}{x_n - x} + \cdots + a_1 \lim_{n\to\infty} \frac{x_n - x}{x_n - x} + 0 \end{aligned}$$

Vypočítajme limitu

$$\lim_{n\to\infty} \frac{x_n^i - x^i}{x_n - x},$$

kde $i = 2, 3, \ldots, k$. Využijeme rovnosť

$$a^i - b^i = (a-b)(a^{i-1} + a^{i-2}b + \cdots + a^2 b^{i-3} + ab^{i-2} + b^{i-1}) .$$

Čiže

$$\begin{aligned} \lim_{n\to\infty} \frac{x_n^i - x^i}{x_n - x} &= \lim_{n\to\infty} \frac{(x_n - x)(x_n^{i-1} + x_n^{i-2}x + \cdots + x^{i-1})}{x_n - x} \\ &= \lim_{n\to\infty} x_n^{i-1} + x \lim_{n\to\infty} x_n^{i-2} + \cdots + x^{i-2} \lim_{n\to\infty} x_n + x^{i-1} \\ &= i x^{i-1} . \end{aligned}$$

Ak sa teraz vrátime k derivácii polynómu $f_k(x)$, dostávame:

$$f_k'(x) = k a_k x^{k-1} + (k-1) a_{k-1} x^{k-2} + \cdots + a_1 . \tag{7.5}$$

Príklad 7.2.2. *Vypočítajme deriváciu polynómu*

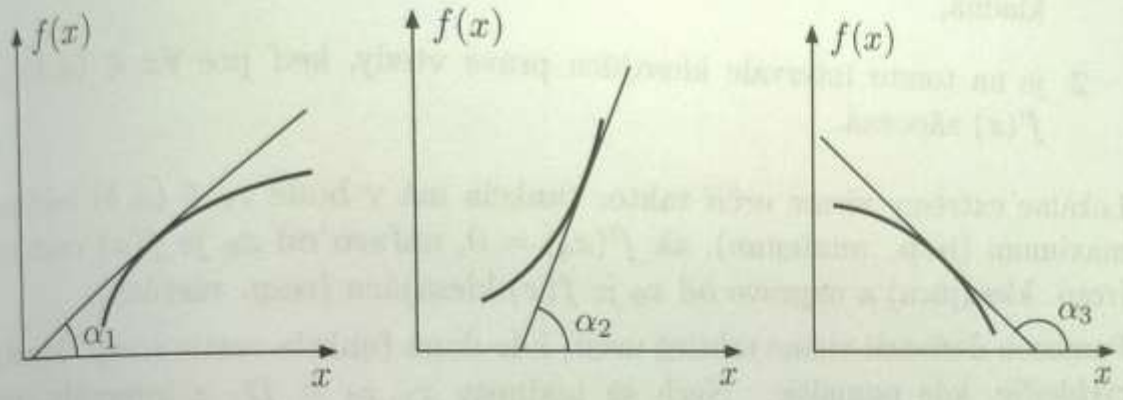
$$f(x) = 5x^3 + 4x^2 + 3x + 2 .$$

Podľa (7.5)

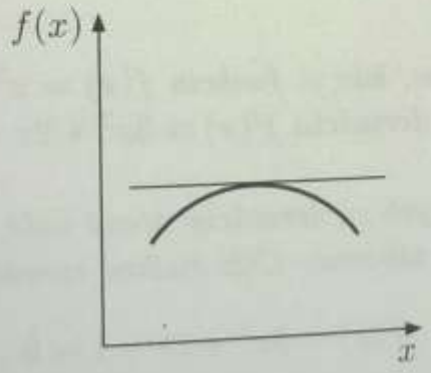
$$f'(x) = 3{\cdot}5{\cdot}x^2 + 2{\cdot}4{\cdot}x + 3 = 15x^2 + 8x + 3 .$$

Využitie derivácií

Ako sme spomenuli už skôr, derivácia funkcie v nejakom bode x_0 zodpovedá tangensu uhla, ktorý zviera dotyčnica ku krivke opísanej funkciou f v danom bode x_0. Na obrázkoch (7.8) a (7.9) máme niekoľko príkladov. Môžeme si



Obrázok 7.8: Vzťah medzi uhlom dotyčníc, rastom a klesaním funkcie



Obrázok 7.9: Dotyčnica a lokálne maximum

všimnúť, že pre rastúce funkcie na obrázku je uhol α z intervalu $(0, \pi/2)$, pre klesajúce z intervalu $(\pi/2, \pi)$ a dotyčnica v maxime (podobne by to platilo pre minimum) zviera s x-ovou osou uhol 0 stupňov. Spomínané fakty platia všeobecne (ovšem dôkaz a zdôvodnenie tu nebudeme uvádzať - možno ho nájsť v [7]). Je známe, že funkcia tangens je na intervale $(0, \pi/2)$ rastúca a

kladná, na intervale $(\pi/2, \pi)$ rastúca a záporná a $\tan 0 = 0$.
Z toho možno odvodiť nasledujúce fakty:
Ak má funkcia f v každom bode intervalu (a, b) deriváciu, tak

1. je na tomto intervale rastúca práve vtedy, keď pre $\forall x \in (a, b)$ je $f'(x)$ kladná,
2. je na tomto intervale klesajúca práve vtedy, keď pre $\forall x \in (a, b)$ je $f'(x)$ záporná.

Lokálne extrémy vieme určiť takto: funkcia má v bode $x_0 \in (a, b)$ lokálne maximum (resp. minimum), ak $f'(x_0) = 0$, naľavo od x_0 je $f(x)$ rastúca (resp. klesajúca) a napravo od x_0 je $f(x)$ klesajúca (resp. rastúca).

Pomocou derivácií vieme taktiež určiť, kde daná funkcia rastie (resp. klesá) rýchlejšie, kde pomalšie. Nech sú hodnoty $x_1, x_2 \in D_f$ z intervalu, na ktorom je f rastúca. Ak $f'(x_1) < f'(x_2)$, tak $\tan \alpha_1 < \tan \alpha_2$ a tiež $\alpha_1 < \alpha_2$. Ak je uhol α_2 väčší, tak funkcia f v nejakom malom okolí hodnoty x_2 rastie určite rýchlejšie, ako v nejakom okolí hodnoty x_1. Podobné úvahy urobte pre klesanie funkcie.

Príklad 7.2.3. *Zistime, kde je funkcia $f(x) = x^3 + x^2 - x$ rastúca a kde klesajúca. Vypočítame deriváciu $f'(x) = 3x^2 + 2x - 1$.*

Ak zistíme body, v ktorých sa derivácia rovná nule, dostaneme aj intervaly, na ktorých je kladná a záporná. Čiže riešme rovnicu

$$f'(x) = 3x^2 + 2x - 1 = 0 \ .$$

Jej korene sú $x_1 = -1$, $x_2 = 1/3$. Výsledok je v nasledujúcej tabulke:

	$(-\infty, -1)$	-1	$(-1, 1/3)$	$1/3$	$(1/3, \infty)$
$f'(x)$	$+$	0	$-$	0	$+$
$f(x)$	$\nearrow$	*max*	$\searrow$	*min*	$\nearrow$

Takže sme zistili, kde daná funkcia rastie, klesá, kde má lokálne extrémy. Vezmime si hodnoty $x_1 = -2$ a $x_2 = -3$. Obe sú z intervalu, kde daná

funkcia rastie. Dosaďme ich do derivácie: $f'(-2) = 3\cdot(-2)^2+2\cdot(-2)-1 = 7$ *a* $f'(-3) = 3\cdot(-3)^2+2\cdot(-3)-1 = 20$. *Takže v nejakom malom okolí hodnoty* $x_2 = -3$ *funkcia* f *rastie určite rýchlejšie, ako v niektorom okolí hodnoty* $x_1 = -2$.

Kapitola 8

Súčty a súčiny

8.1 Súčet konečného počtu členov aritmetickej postupnosti

Doteraz sme pracovali s členmi postupností. Teraz sa pozrieme na ich súčty a súčiny. Najprv na súčty a súčiny konečného počtu členov postupnosti, potom si povieme niečo aj o nekonečných súčtoch.

Skúsme najprv sčitovať členy aritmetickej postupnosti. Najjednoduchšia aritmetická postupnosť je postupnosť s členmi $1, 2, 3, 4, \ldots$. Jedna historka súvisiaca so sčitovaním členov tejto postupnosti hovorí, že istý učiteľ potreboval zamestnať svojich žiakov, tak ich nechal sčítať čísla od 1 do 500. Mal však „smolu", pretože mal v triede žiaka menom Carl Friedrich Gauss (1777-1855), ktorý po krátkej chvíli zahlásil výsledok. Čo vlastne mladý Gauss urobil? Napísal si oba súčty pod seba, ako je to v nasledujúcej tabuľke.

$$\begin{array}{rcrcrcrcr}
1 & + & 2 & + \ldots + & 499 & + & 500 & = & S_{500} \\
500 & + & 499 & + \ldots + & 2 & + & 1 & = & S_{500} \\
\hline
= 501 & & = 501 & & = 501 & & = 501 & & = 2S_{500}
\end{array}$$

Čiže dostal $2S_{500} = 501 \cdot 500$ a súčet S_{500} už poľahky vypočítal. Všeobecne

môžeme súčet prvých n prirodzených čísel vypočítať pomocou vzťahu $S_n = (n+1)n/2$.

Tento postup možno zovšeobecniť na súčet členov ľubovoľnej aritmetickej postupnosti. Vieme, že v aritmetickej postupnosti platí $a_n = a_{n-1} + d$ a $a_n = a_1 + (n-1)d$. Ak máme sčítať prvých n členov aritmetickej postupnosti $a_1 + a_2 + \cdots + a_n$, môžeme postupovať ako Gauss. Napíšeme si tie súčty pod seba:

$$\begin{array}{ccccccccccccc} & & & & & & & & & & & & \\ a_1 & + & a_2 & + & \dots & + & a_k & + & \dots & + & a_n & = & S_n \\ a_n & + & a_{n-1} & + & \dots & + & a_{n-k+1} & + & \dots & + & a_1 & = & S_n \end{array}$$

Teraz si stačí uvedomiť, že pre ľubovoľné $k \in \{1, \dots, n\}$ platí $a_k + a_{n-k+1} = a_1 + a_n$. Nakoľko $a_1 + a_n = a_1 + a_1 + (n-1)d$ a $a_k + a_{n-k+1} = a_1 + (k-1)d + a_1 + (n-k)d = 2a_1 + (n-1)d$. Takže v každom stĺpci máme súčet $a_1 + a_n$ a stĺpcov je n. Potom $2S_n = (a_1 + a_n)n$ a

$$S_n = \frac{(a_1 + a_n)n}{2}.$$

8.2 Súčet konečného počtu členov geometrickej postupnosti

Videli sme, že súčet prvých n členov aritmetickej postupnosti možno vyjadriť pomocou vzorca. Skúsme niečo podobné pre súčet prvých n členov geometrickej postupnosti. Vieme, že v tejto postupnosti platí $a_n = qa_{n-1} = q^{n-1}a_1$. Potom $a_1 + \cdots + a_n = a_1 + a_1q + a_1q^2 + \cdots + a_1q^{n-1} = a_1(1 + q + q^2 + \cdots + q^{n-1})$. Potrebujeme určiť súčet

$$S_n = 1 + q + \cdots + q^{n-1}. \tag{8.1}$$

Gaussov trik použiť nemôžeme (skúste zdôvodniť prečo), ale môžeme využiť rovnako vtipnú fintu - vynásobíme rovnosť (8.1) výrazom $-q$.

$$\begin{array}{ccccccccccccc} 1 & + & q & + & q^2 & + & \dots & + & q^{n-1} & & & = & S_n \\ & - & q & - & q^2 & - & \dots & - & q^{n-1} & - & q^n & = & -qS_n \end{array}$$

Sčítaním oboch rovností dostávame

$$1 - q^n = S_n - qS_n$$

a po úprave pre $q \neq 1$

$$S_n = \frac{1 - q^n}{1 - q} .$$

8.3 Práca so symbolmi $\sum$ a $\prod$

Aby bolo možné súčty a súčiny väčšieho počtu členov postupností zapisovať pohodlnejšie, začali sa používať symboly $\sum$ a $\prod$. Vezmime členy ľubovoľnej postupnosti $a_p, a_{p+1}, a_{p+2}, \ldots, a_m$. Ich súčet $a_p + a_{p+1} + a_{p+2} + \cdots + a_m$ zapisujeme

$$\sum_{i=p}^{m} a_i$$

a ich súčin

$$\prod_{i=p}^{m} a_i .$$

Napríklad

$$-1 + 0 + 1 + \cdots + 100 = \sum_{i=-1}^{100} i$$

alebo

$$3 \cdot 4 \cdot \ldots \cdot 100 = \prod_{i=3}^{100} i .$$

Úloha. Ako by ste naprogramovali

- $\sum_{i=1}^{n} a_i$,
- $\prod_{i=1}^{n} a_i$,
- $\sum_{i \in I} a_i$?

8.4 Vlastnosti súčtov

Pozrime sa teraz na niektoré vlastnosti konečných súčtov. Budeme uvažovať, že sčitujeme konečný počet členov postupností $\left\{a_n\right\}_{n=p}^{\infty}$ a $\left\{b_n\right\}_{n=p}^{\infty}$, kde p je celé číslo. Dôkazy všeobecnej platnosti uvedených vlastností neuvádzame. Čitateľ, ktorý by mal záujem, ich nájde napríklad v [8], alebo sa môže pokúsiť urobiť ich sám.

1. Rozpíšme a upravme nasledujúci súčet:

$$a_0 + \sum_{i=1}^{3} a_i = a_0 + (a_1 + a_2 + a_3) = \sum_{i=0}^{3} a_i \ .$$

Využili sme asociatívnosť súčtu. Všeobecne môžeme písať

$$a_{p-1} + \sum_{i=p}^{n} a_i = \sum_{i=p-1}^{n} a_i \ .$$

2. Podobne, ako v predchádzajúcom prípade, môžeme rozpísať nasledujúcu sumu:

$$\sum_{i=1}^{6} a_i = (a_1 + a_2 + a_3) + (a_4 + a_5 + a_6) = \sum_{i=1}^{3} a_i + \sum_{i=4}^{6} a_i \ .$$

Opäť sme využili asociatívnosť. Keď to chceme zapísať všeobecne, situácia vyzerá nasledujúco (predpokladáme, že $m < n$):

$$\sum_{i=p}^{n} a_i = \sum_{i=p}^{m} a_i + \sum_{i=m+1}^{n} a_i \ .$$

3. Pri súčte členov geometrickej postupnosti sme písali

$$a_1 + a_1 q + a_1 q^2 + \cdots + a_1 q^{n-1} = a_1(1 + q + q^2 + \cdots + q^{n-1}) \ .$$

Zapíšme obe strany tejto rovnosti pomocou súm:

$$\sum_{i=1}^{n} a_1 q^{i-1} = a_1 \sum_{i=1}^{n} q^{i-1} .$$

Vidíme, že distributívnosť násobenia vzhľadom na sčitovanie sa v sume prejavila tak, že konštantu, ktorou sme násobili členy postupnosti, možno písať pred sumu. Všeobecne teda môžeme písať:

$$c \sum_{i=p}^{n} a_i = \sum_{i=p}^{n} c a_i .$$

4. Sčítajme teraz členy dvoch rôznych postupností:

$$\begin{aligned} \textstyle\sum_{i=1}^{3} a_i + \sum_{i=1}^{3} b_i &= (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3) \\ &= a_1 + b_1 + a_2 + b_2 + a_3 + b_3 \\ &= \textstyle\sum_{i=1}^{3} (a_i + b_i) . \end{aligned}$$

Využívame komutatívnosť a asociatívnosť súčtu. Pre súčet n za sebou idúcich členov oboch postupností môžeme písať:

$$\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = \sum_{i=1}^{n} (a_i + b_i) .$$

Ak je jedna z postupností konštantná, tak dostávame:

$$\sum_{i=1}^{n} (a_i + c) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} c = \sum_{i=1}^{n} a_i + nc .$$

Príklad 8.4.1. *Vypočítajte*

$$\sum_{i=1}^{20} \frac{1}{i(i+1)} .$$

Pri riešení využijeme rovnosť

$$\frac{1}{i(i+1)} = \frac{1}{i} - \frac{1}{i+1} ,$$

ktorú môžeme dostať pomocou rozkladu na parciálne zlomky. Teraz môžeme písať

$$\sum_{i=1}^{20} \frac{1}{i(i+1)} = \sum_{i=1}^{20} \frac{1}{i} - \sum_{i=1}^{20} \frac{1}{i+1} .$$

Ak si to rozpíšeme, dostávame

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{19} + \frac{1}{20} - \frac{1}{2} - \frac{1}{3} - \cdots - \frac{1}{19} - \frac{1}{20} - \frac{1}{21} = 1 - \frac{1}{21} .$$

5. Vezmime si nasledujúci súčet:

$$1 + 2 + 3 + 4 = \sum_{i=1}^{4} i .$$

Niekedy však môže byť výhodné, ak tento súčet zapíšeme pomocou sumy trochu inak:

$$\sum_{i=2}^{5} (i-1) = \sum_{i=-1}^{2} (i+2) = \ldots$$

Ľahko sa presvedčíme, že ide o ten istý súčet. Všeobecne platí, že pre ľubovoľné dve celé čísla p, q a pre každé celé číslo $m \geq 0$ dostávame

$$\sum_{i=p}^{p+m} a_i = \sum_{i=q}^{q+m} a_{i+p-q} .$$

Príklad 8.4.2. *Ak vezmeme rozdiel súm z predchádzajúceho príkladu*

$$\sum_{i=1}^{20} \frac{1}{i} - \sum_{i=1}^{20} \frac{1}{i+1}$$

a v druhej sume prepíšeme indexy a hranice, tak dostaneme rozdiel

$$\sum_{i=1}^{20} \frac{1}{i} - \sum_{i=2}^{21} \frac{1}{i} ,$$

v ktorom hneď vidieť, že sa vzájomne neodčítajú len 1 *a* $\frac{1}{21}$ *a výsledok musí byť* $1 - \frac{1}{21}$.

6. Sčítajme hodnoty v nasledujúcej tabuľke dvomi spôsobmi.

2	3	1	$= r_1$
1	1	1	$= r_2$
1	2	1	$= r_3$
$= s_1$	$= s_2$	$= s_3$	

Je jasné, že ak ich sčítame po riadkoch, alebo po stĺpcoch, výsledok musí byť rovnaký: $r_1 + r_2 + r_3 = s_1 + s_2 + s_3$. Zapíšme tieto súčty pomocou súm. Prvok tabuľky nachádzajúci sa v riadku číslo i a stĺpci číslo j budeme značiť $a_{i,j}$. Pre každé $i \in \{1, 2, 3\}$ platí

$$r_i = \sum_{j=1}^{3} a_{i,j} \ .$$

Celkový súčet môžeme zapísať nasledujúco

$$s = \sum_{i=1}^{3} r_i = \sum_{i=1}^{3} (\sum_{j=1}^{3} a_{i,j}) = \sum_{i=1}^{3} \sum_{j=1}^{3} a_{i,j} \ .$$

Použili sme teda dvojitú sumu na vyjadrenie tohto súčtu. Podobne môžeme pre každé $j \in \{1, 2, 3\}$ písať

$$s_j = \sum_{i=1}^{3} a_{i,j}$$

a celkový súčet môžeme zapísať

$$s = \sum_{j=1}^{3} s_j = \sum_{j=1}^{3} (\sum_{i=1}^{3} a_{i,j}) = \sum_{j=1}^{3} \sum_{i=1}^{3} a_{i,j} \ .$$

Platí teda

$$s = \sum_{i=1}^{3}\sum_{j=1}^{3} a_{i,j} = \sum_{j=1}^{3}\sum_{i=1}^{3} a_{i,j} \ ,$$

čo môžeme všeobecne zapísať:

$$\sum_{i=p}^{n}\sum_{j=q}^{m} a_{i,j} = \sum_{j=q}^{m}\sum_{i=p}^{n} a_{i,j} \ .$$

7. Pracujme teraz s nasledujúcim súčinom:

$$(\sum_{i=1}^{3} a_i)\cdot(\sum_{j=1}^{3} b_j) \ .$$

Vieme, že

$$(a_1 + a_2 + a_3)(b_1 + b_2 + b_3) = a_1b_1 + a_1b_2 + \cdots + a_3b_3 \ .$$

Ak to chceme zapísať ako sumu súčinov, potrebujeme dvojitú sumu

$$\sum_{j=1}^{3} a_1b_j + \sum_{j=1}^{3} a_2b_j + \sum_{j=1}^{3} a_3b_j = \sum_{i=1}^{3}\sum_{j=1}^{3} a_ib_j \ .$$

Iný spôsob zápisu, ktorý sa používa je

$$\sum_{1\le i\le 3; 1\le j\le 3} a_ib_j \ .$$

Všeobecne píšeme

$$(\sum_{i=1}^{n} a_i)\cdot(\sum_{j=1}^{m} b_j) = \sum_{1\le i\le n; 1\le j\le m} a_i\cdot b_j \ .$$

8.5 Vlastnosti súčinov

Podobne ako pri súčtoch, sa pozrieme aj na vlastnosti súčinov. Vzhľadom na to, že vlastnosti sčitovania a násobenia čísel (komutatívnosť, asociatívnosť) sú rovnaké, môžeme očakávať, že niektoré vlastnosti konečných súčinov budú rovnaké.

1. Z asociatívnosti vyplýva

$$a_{p-1} \cdot \prod_{i=p}^{n} a_i = \prod_{i=p-1}^{n} a_i \, .$$

2. Podobne máme

$$\prod_{i=p}^{n} a_i = \prod_{i=p}^{m} a_i \cdot \prod_{i=m+1}^{n} a_i \, .$$

3. Pre dva súčiny dostávame

$$\prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{n} b_i = \prod_{i=1}^{n} (a_i \cdot b_i) \, .$$

4. Pre násobenie členov postupnosti konštantou

$$\prod_{i=1}^{n} (c \cdot a_i) = \prod_{i=1}^{n} c \cdot \prod_{i=1}^{n} a_i = c^n \prod_{i=1}^{n} a_i \, .$$

8.6 Porovnanie konečných a nekonečných súčtov

Doteraz sme pracovali s konečnými súčtami. Len v krátkosti nahliadnime, ako to vyzerá, keď sčitujeme členy nekonečnej postupnosti $\{a_n\}_{n=1}^{\infty}$.

Nájdime súčet členov geometrickej postupnosti $\left\{\left(\frac{1}{2}\right)^n\right\}_{n=1}^{\infty}$. Môžeme si pomôcť príkladom o tabuľke čokolády a štedrej školáčke (pozri napríklad [8]). Dievča vytiahne cez prestávku tabuľku čokolády. Príde k nej jedna

kamarátka, tak rozpolí čokoládu a polovicu jej dá. Potom sa pri nej pristaví ďalšia kamarátka, tak dievča rozpolí zvyšok a jednu polovicu toho zvyšku jej dá. Takto to pokračuje ďalej, vždy keď sa chystá zahryznúť do čokolády, objaví sa ďalšia kamarátka a naša hlavná hrdinka jej dá polovicu toho čo jej zostalo. „Súčet" kúskov čokolády rozdelených medzi kamarátky dievčaťa sa musí rovnať celej tabuľke čokolády. Matematicky to môžeme vyjadriť nasledovne

$$\sum_{n=1}^{\infty}\left(\frac{1}{2}\right)^n = \frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots = 1\ .$$

Teraz vezmime postupnosť, ktorej n-tý člen je $a_n = (-1)^n$. Skúsme si vyjadriť jej súčet. Ak využijeme vlastnosti konečných súčtov, nastane zvláštna (a trochu nepríjemná) situácia:

$$\sum_{i=1}^{\infty}(-1)^i = ((-1)+1)+((-1)+1)+((-1)+\cdots = 0\ .$$

Ak sme popárovali členy po dvojiciach, súčet bol nula. Skúsme členy tej postupnosti sčítať inak. Prvý člen nechajme bez páru a ostatné popárujme so svojím susedom do zátvoriek:

$$\sum_{i=1}^{\infty}(-1)^i = (-1)+(1+(-1))+((-1)+1)+\cdots = -1\ .$$

Zdá sa, že asociatívnosť (posun zátvoriek) pre nekonečné súčty nemusí platiť. Čo s prehadzovaním poradia sčítancov. V konečných súčtoch sme si to mohli "beztrestne" dovoliť. Pri nekonečných postupnostiach to pravda nemusí byť. Poprehadzujme a uzátvorkujme členy našej postupnosti nasledujúcim spôsobom:

$$\begin{array}{ccccccc}
(a_1+a_2+a_4) & + & (a_3+a_6+a_8) & + & (a_5+a_{10}+a_{12}) & \ldots & = \\
\underbrace{((-1)+1+1)} & + & \underbrace{((-1)+1+1)} & + & \underbrace{((-1)+1+1)} & \ldots & = \\
1 & + & 1 & + & 1 & \ldots & = \infty\ .
\end{array}$$

Čiže ani komutatívnosť (prehadzovanie poradia sčítancov) nemusí pri nekonečných súčtoch fungovať.

Úloha. Usporiadajte členy postupnosti $\{(-1)^n\}_{n=1}^{\infty}$ tak, aby vyšiel súčet a) -1, b) 3, c) $-\infty$.

Pri určovaní súčtu členov nekonečnej postupnosti $\{a_n\}_{n=p}^{\infty}$ je užitočné zaviesť novú postupnosť - postupnosť čiastočných súčtov $\{s_n\}_{n=p}^{\infty}$, ktorej členy dostaneme takto:

$$\begin{aligned}
s_p &= a_p \\
s_{p+1} &= a_p + a_{p+1} \\
s_{p+2} &= a_p + a_{p+1} + a_{p+2} \\
&\vdots \\
s_n &= a_p + a_{p+1} + a_{p+2} + \ldots + a_n \\
&\vdots
\end{aligned}$$

Za súčet členov nekonečnej postupnosti považujeme limitu postupnosti čiastočných súčtov

$$\lim_{n\to\infty} s_n ,$$

ak existuje a je rovná reálnemu číslu. Ak postupnosť čiastočných súčtov postupnosti $\{a_n\}_{n=p}^{\infty}$ má limitu rovnú reálnemu číslu, tak hovoríme, že $\{a_n\}_{n=p}^{\infty}$ **je sumovateľná**. Ak spomenutá limita neexistuje, alebo je rovná $\pm\infty$, tak hovoríme, že postupnosť **nie je sumovateľná** [8].

Pozrime sa na postupnosti, s ktorými sme pracovali v tejto časti. Začnime aritmetickou postupnosťou $\{a_n\}_{n=1}^{\infty}$, kde $a_n = 1 + (n-1)2$. Postupnosť čiastočných súčtov vyzerá nasledujúco:

$$\begin{aligned}
s_1 &= 1 \\
s_2 &= 1 + 3 = 4 \\
&\vdots \\
s_n &= 1 + 3 + \ldots + (1 + (n-1)2) = n^2 \\
&\vdots
\end{aligned}$$

Asi každému je jasné, že táto postupnosť nie je sumovateľná, pretože

$$\lim_{n\to\infty} n^2 = \infty .$$

Pozrime sa na geometrickú postupnosť $\{a_0q^n\}_{n=0}^{\infty}$ s koeficientom q. Postupnosť čiastočných súčtov vyzerá nasledujúco:

$$\begin{aligned}
s_0 &= a_0 \\
s_1 &= a_0 + a_0q \\
s_2 &= a_0 + a_0q + a_0q^2 \\
&\vdots \\
s_n &= a_0 + a_0q + \dots + a_0q^n = a_0\tfrac{1-q^{n+1}}{1-q} \\
&\vdots
\end{aligned}$$

Limita postupnosti čiastočných súčtov pre $q \in (-1,1)$ je

$$a_0 \cdot \lim_{n\to\infty} \frac{1-q^{n+1}}{1-q} = \frac{a_0}{1-q},$$

čiže táto postupnosť je pre $q \in (-1,1)$ sumovateľná, pre $q \notin (-1,1)$ sumovateľná nie je.

Vezmime teraz postupnosť $\{(-1)^n\}_{n=1}^{\infty}$. Jej postupnosť čiastočných súčtov je

$$\begin{aligned}
s_1 &= -1 \\
s_2 &= -1 + 1 = 0 \\
s_3 &= -1 + 1 + (-1) = -1 \\
&\vdots \\
s_n &= -1 + 1 + \dots + (-1)^n = \tfrac{-1+(-1)^n}{2} \\
&\vdots
\end{aligned}$$

Táto postupnosť ovšem nemá limitu. Takže postupnosť $\{(-1)^n\}_{n=1}^{\infty}$ nie je sumovateľná.

8.7 Poznámka k reprezentácii racionálnych čísel

Už sme hovorili o reprezentácii čísel v rôznych pozičných sústavách. Povedzme si niečo o jednom probléme, ktorý sprevádza tento spôsob reprezentácie (v kapitole o funkciách už bol spomenutý). Začnime desiatkovou sústavou. Porovnajme čísla $x_1 = 0,9999\cdots = 0,\overline{9}$ a $x_2 = 1$. Vieme, že číslo x_1 možno vyjadriť nasledujúco:

$$x_1 = 9{\cdot}10^{-1} + 9{\cdot}10^{-2} + 9{\cdot}10^{-3} + \dots$$

Čísla $9{\cdot}10^{-1}$, $9{\cdot}10^{-2}$, $9{\cdot}10^{-3}$, ... však predstavujú členy geometrickej postupnosti s koeficientom $q = 10^{-1} \in \langle 0, 1)$. Takže x_1 je súčet členov tejto postupnosti:

$$x_1 = \sum_{n=1}^{\infty} 9{\cdot}10^{-n} = \frac{9{\cdot}10^{-1}}{1-0,1} = 1\,.$$

To znamená, že x_1 a x_2 zodpovedajú tomu istému číslu - číslu 1. Čísla, ktoré majú v desiatkovej sústave tento dvojtvar môžeme písať nasledujúco: $a, a_1a_2a_3\dots a_k000\cdots = a, a_1a_2a_3\dots(a_k-1)999\dots$, kde $a_1,\dots,a_k \in \{0,\dots,9\}$, $a_k \neq 0$, $a \in Z$.

V sústave so základom z vyzerajú čísla s takýmto dvojtvarom nasledujúco: $a, a_1a_2a_3\dots a_k000\cdots = a, a_1a_2a_3\dots(a_k-1)(z-1)(z-1)(z-1)\dots$, kde $a_1,\dots,a_k \in \{0,\dots,z-1\}$, $a_k \neq 0$, $a \in Z$.

Kapitola 9

Ako určovať počet možností

Ak chceme naprogramovať nejaký výpočet, je užitočné vedieť odhadnúť počet krokov, ktoré náš program bude musieť vykonať. Je napríklad veľký rozdiel, či má program vykonať, pri vstupe o veľkosti 1000 bitov, 1000^2, alebo 2^{1000} krokov. V tejto kapitole si prejdeme niekoľko základných kombinatorických princípov, ktoré je možné využiť pri určovaní (v praxi skôr pri odhadovaní) počtu krokov aj veľkosti pamäte potrebnej na uskutočnenie výpočtu. Pri výklade sme zvolili podobný prístup ako v učebných textoch [17]. Pre ďalšie štúdium tejto problematiky môžeme odporučiť literatúru [16, 11].

9.1 Princíp sčitovania

Počet študentov na našej univerzite môžeme zistiť tak, že sčítame počet študentov študujúcich na jednotlivých fakultách (samozrejme za predpokladu, že žiadny študent neštuduje na viacerých fakultách naraz). Formálne to môžeme zapísať takto: ak Fri, $Pedas$, Sjf, Ef, Svf, Fhv, Fsi sú množiny študentov jednotlivých fakúlt a množina Un je množina študentov tejto univerzity, tak platí

$$Fri \cup Pedas \cup Sjf \cup Ef \cup Svf \cup Fhv \cup Fsi = Un$$

a pre počet študentov (znak $|A|$ označuje počet prvkov množiny A)

$$|Fri| + |Pedas| + |Sjf| + |Ef| + |Svf| + |Fhv| + |Fsi| = |Un|.$$

Všeobecne pre množiny

$$S_1 \cup S_2 \cup \cdots \cup S_k = S,$$

kde $S_i \cap S_j = \emptyset$ platí:

$$|S_1| + |S_2| + \cdots + |S_k| = |S|.$$

9.2 Princíp násobenia

Koľko čísel vieme zapísať pomocou piatich bitov?
Na každé miesto máme práve dve možnosti - vyberáme si z číslic 0 a 1. Čiže počet možností je $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5$.

Koľko je všetkých trojciferných čísel, deliteľných číslom päť?
Na miesto stoviek vyberáme z deviatich možností: sú to cifry $1, \ldots, 9$, na miesto desiatok vyberáme z desiatich možností: sú to cifry $0, 1, \ldots, 9$, na miesto jednotiek vyberáme z dvoch možností: čísla deliteľné piatimi končia cifrou 0 alebo 5. Možnosti medzi sebou násobíme, pretože na každú číslicu na mieste stoviek pripadá desať možností na mieste desiatok a na každú dvojicu číslic na mieste stoviek a desiatok pripadajú dve rôzne možnosti na mieste jednotiek, takže výsledok je $9 \cdot 10 \cdot 2$.

Ak vytvárame usporiadané k-tice, kde prvý prvok vyberáme z množiny A_1, druhý prvok z množiny A_2, až nakoniec k-ty prvok z množiny A_k, tak počet všetkých usporiadaných k-tic, ktoré takto môžeme vytvoriť je

$$|A_1| \cdot |A_2| \cdot \ldots \cdot |A_k|.$$

Príklad 9.2.1. *Koľko hesiel vieme vytvoriť, ak máme k dispozícii malé a veľké písmená anglickej abecedy, číslice od 0 po 9, môžeme použiť najviac osem znakov a prvý znak je písmeno?*

Behu na 100 metrov sa zúčastnilo osem pretekárov. Koľko je rôznych poradí, ako mohli preteky skončiť?
Na prvé miesto máme osem možností, na druhé miesto máme sedem možností, pretekár, ktorý skončil na prvom mieste nemôže samozrejme skončiť aj na druhom. Podobne na tretie miesto vyberáme zo šiestich možností, až nakoniec na posledné miesto zostáva jeden pretekár. Možnosti medzi sebou násobíme, takže výsledok je $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 8!$.

Väčšinu ľudí zaujíma len výsledok na prvých troch miestach, takže si položme otázku, koľko je rôznych poradí na týchto miestach?
Postupujeme veľmi podobne, ako v predchádzajúcom prípade, ale zostavujeme len usporiadané trojice: na prvé miesto máme osem možností, na druhé sedem a na tretie miesto vyberáme už len zo šiestich možností. Počty možností medzi sebou násobíme, takže výsledok je $8 \cdot 7 \cdot 6$.

Vidíme, že v predchádzajúcich príkladoch ide opäť o princíp násobenia, ale možnosti, ktoré pripadajú na druhé miesto, sú ovplyvnené možnosťou na prvom mieste, možnosti prichádzajúce do úvahy na tretie miesto, sú ovplyvnené možnosťami na prvom a druhom mieste a takto to pokračuje ďalej. Princíp násobenia môžeme teda sformulovať takto: vytvárame usporiadanú k-ticu, ak na prvé miesto máme n_1 možných prvkov, na druhé miesto n_2 možných prvkov vzhľadom na prvý prvok, až na k-te miesto n_k možných prvkov vzhľadom na prvky umiestnené na predchádzajúcich $k-1$ miestach. Počet všetkých možností je potom

$$n_1 \cdot n_2 \cdot \ldots \cdot n_k \, .$$

9.3 Princíp delenia

Ak chceme spočítať počet ľudí v miestnosti, môžeme postupovať aj nasledujúcim (trochu absurdným) spôsobom (pozri [17]). Spočítame všetky uši v miestnosti a tento počet delíme dvoma. Toto je základ princípu, ktorý tu uvedieme.

Začnime úlohou: Máme šesť bodov v rovine, pričom žiadne tri neležia na jednej priamke. Koľko priamok a koľko trojuholníkov je určených týmito bodmi?

Každá priamka je určená dvoma bodmi, takže sa pýtame, koľko dvojíc bodov vieme vytvoriť. Na prvé miesto máme šesť možností, na druhé miesto máme päť možností. Keď však zoberieme dvojicu bodov A, B a dvojicu bodov B, A, tak je jasné, že týmito dvojicami je určená práve jedna priamka. Každej priamke zodpovedajú dve usporiadané dvojice (dve „uši"), ktoré „splynú" do jednej neusporiadanej dvojice. Počet priamok je teda daný počtom „uší", t. j. usporiadaných dvojíc a tento počet musíme vydeliť dvoma. Podobne je to s trojuholníkmi. Počet usporiadaných trojíc je $6{\cdot}5{\cdot}4$, ale usporiadané trojice ABC, ACB, BAC, BCA, CAB, CBA zodpovedajú tomu istému trojuholníku. Ak máme trojuholník XYZ, tak z jeho vrcholov možno vytvoriť šesť usporiadaných trojíc: na prvé miesto máme tri možnosti, na druhé dve, na tretie jednu možnosť. To znamená, že každý trojuholník má $3{\cdot}2{\cdot}1 = 3!$ „uší" - usporiadaných trojíc vrcholov. Počet rôznych trojuholníkov je teda

$$\frac{6{\cdot}5{\cdot}4}{3{\cdot}2{\cdot}1}\,.$$

Ak to vezmeme všeobecne, vyberáme k-tice z n prvkov. Usporiadaných k-tic je podľa princípu násobenia

$$n{\cdot}(n-1){\cdot}\ldots{\cdot}(n-k+1) \tag{9.1}$$

ale ak nám nezáleží na poradí prvkov v k-tici, tak tento súčin musíme deliť počtom všetkých poradí, v akom tieto k-tice môžeme zapísať:

$$\frac{n{\cdot}(n-1){\cdot}\ldots{\cdot}(n-k+1)}{k{\cdot}(k-1){\cdot}\ldots{\cdot}1}\,. \tag{9.2}$$

Súčin (9.1) zapíšeme ako podiel faktoriálov, to je:

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

Potom podiel (9.2) môžeme zapísať v tvare

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

Toto číslo nazývame kombinačné číslo, zodpovedá počtu k prvkových podmnožín n prvkovej množiny a značíme ho

$$\binom{n}{k}.$$

9.4 Princíp bijekcie

V časti o funkciách sme hovorili, že bijekcia medzi dvoma konečnými množinami znamená rovnaký počet prvkov medzi nimi. Tento princíp možno využiť na počítanie všetkých možností.

Zaoberajme sa otázkou, koľko podmnožín má n prvková množina A_n?

Riešme túto úlohu najprv pre $n = 2$. Nech $A_2 = \{x_1, x_2\}$. Potom jej podmnožiny sú:

$$\emptyset,\ \{x_1\},\ \{x_2\},\ \{x_1, x_2\}.$$

Každú z uvedených podmnožín môžeme reprezentovať usporiadanou dvojicou núl a jednotiek nasledujúco: ak x_1 patrí do danej podmnožiny, tak na prvom mieste je jednotka, ak nepatrí, potom je na tom mieste nula. Podobne pre x_2. Ak patrí do danej podmnožiny, na druhom mieste bude jednotka, ak nepatrí, tak na tom mieste bude nula.

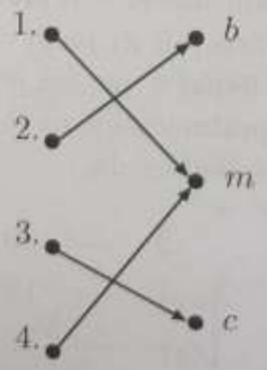
$$\begin{aligned} \emptyset &\longrightarrow 00 \\ \{x_1\} &\longrightarrow 10 \\ \{x_2\} &\longrightarrow 01 \\ \{x_1, x_2\} &\longrightarrow 11 \end{aligned}$$

Ak množinu všetkých podmnožín množiny A označíme $P(A)$, tak predchádzajúce priradenie je bijekcia z $P(A_2)$ do množiny $\{0,1\}^2$. Tento postup

možno zovšeobecniť aj na určenie počtu podmnožín n prvkovej množiny. Túto množinu a jej prvky označme $A_n = \{x_1, x_2, x_3, \ldots, x_n\}$. Zvoľme si funkciu $f : P(A_n) \to \{0,1\}^n$, ktorá priradí každej podmnožine usporiadanú n-ticu, kde na k-tom mieste bude jednotka práve vtedy, keď prvok x_k patrí do danej podmnožiny. Potom f musí byť injekcia, pretože dvom rôznym podmnožinám musíme vždy priradiť dve rôzne postupnosti núl a jednotiek. Funkcia f je tiež surjekciou, pretože ku každej n miestnej postupnosti núl a jednotiek nájdeme podmnožinu, ktorá je touto postupnosťou charakterizovaná. Teda f je bijekcia a množiny $P(A_n)$ a $\{0,1\}^n$ majú rovnaký počet prvkov. Ale prvky množiny $\{0,1\}^n$ sú n miestne postupnosti núl a jednotiek a my už vieme, že ich je presne 2^n. Preto aj podmnožín n prvkovej množiny je 2^n.

9.5 Dirichletov princíp

Predstavme si situáciu, že máme v škatuli šesť ponožiek (biely, modrý a čierny pár), ale pre našu neporiadnosť nie sú popárované. Ak chceme potme, aby sme nezobudili spolubývajúcich vybrať dve rovnaké ponožky, koľko ich musíme vytiahnuť, aby sme mali istotu, že máme medzi nimi aspoň jeden pár? Odpoveď je samozrejme aspoň štyri ponožky.



Táto jednoduchá úvaha nás vedie k veľmi dôležitému kombinatorickému princípu, ktorý nazývame Dirichletov princíp. Jeho základná verzia znie, ak máme n škatúľ a $n+1$ predmetov v nich umiestnených, tak existuje

škatuľa, v ktorej sú aspoň dva predmety. V anglickej literatúre sa používa názov "Pigeonhole principle" a na jeho vysvetlenie sa používa verzia: ak máme $n+1$ holubov v n hniezdach, tak existuje hniezdo, v ktorom sú aspoň dva holuby. Princíp je jednoduchý na pochopenie, ale dajú sa vďaka nemu dokázať aj netriviálne tvrdenia. Ukážme si jeden príklad:

Tvrdenie. Nech máme 100 ľubovoľných prirodzených čísel $a_1, a_2, \ldots, a_{100}$, vždy z nich vieme vybrať takú podmnožinu, že súčet čísel v tejto podmnožine je deliteľný číslom sto.

Vezmime si nasledujúce súčty:

$$\begin{aligned} S_1 &= a_1 \\ S_2 &= a_1 + a_2 \\ &\vdots \\ S_{100} &= a_1 + a_2 + \cdots + a_{100} \end{aligned}$$

Ak je niektorý z týchto súčtov deliteľný číslom sto, tak je úloha vyriešená. Predpokladajme, že žiadny z týchto súčtov nie je deliteľný stovkou. Potom každé z čísel dáva po delení stovkou zvyšok z množiny $\{1, 2, \ldots, 99\}$. Teraz využijeme Dirichletov princíp. Máme sto čísel a deväťdesiatdeväť zvyškov, to znamená, že existujú aspoň dve čísla, ktoré dávajú rovnaký zvyšok po delení číslom sto. Nech sú to čísla S_i a S_j, kde $i < j$. Ich rozdiel $S_j - S_i$ je deliteľný stovkou (premyslite si prečo) a dá sa vyjadriť ako nasledujúci súčet:

$$(a_1 + \cdots + a_i + a_{i+1} + \cdots + a_j) - (a_1 + \cdots + a_i) = a_{i+1} + \cdots + a_j \,.$$

Čo je súčet čísel jednej z podmnožín spomínaných v tvrdení.

9.6 Pascalov trojuholník

Na záver sa pozrime ešte na známy Pascalov trojuholník a uveďme niektoré identity.

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}
$$

Pomocou kombinačných čísel to možno zapísať takto:

$$
\begin{array}{ccccccccccccc}
 & & & & & & \binom{0}{0} & & & & & & \\
 & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
 & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
 & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & \\
\binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6}
\end{array}
$$

Uveďme niektoré identity, ktoré platia pre kombinačné čísla. Ľahko možno nahliadnuť, že

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

Túto rovnosť možno ľahko interpretovať tak, že počet k prvkových podmnožín n prvkovej množiny je rovnaký ako počet $n-k$ prvkových podmnožín tejto množiny.

Vieme, že čísla v Pascalovom trojuholníku dostávame súčtom dvoch čísel nad ním. Napríklad

$$\binom{4}{1} + \binom{4}{2} = 4 + 6 = 10 = \binom{5}{2}.$$

Všeobecne to možno vyjadriť vzťahom

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

Počet $k+1$ prvkových podmnožín $n+1$ prvkovej množiny A_{n+1} môžeme určiť tak, že zoberieme n prvkovú množinu $A_n \subset A_{n+1}$, spočítame jej $k+1$ prvkové podmnožiny, tie budú aj podmnožinami A_{n+1}. Podobne spočítame k prvkové podmnožiny A_n, pridaním zostávajúceho $n+1$-vého prvku ku každej z nich dostávame zvyšné $k+1$ prvkové podmnožiny A_{n+1}.

Ak sčítame čísla v n-tom riadku Pascalovho trojuholníka (riadky číslujeme od nuly, takže $n = 0, 1, 2, \dots$), tak ich súčet je 2^n. Čiže platí:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n .$$

Kapitola 10

Porovnávanie funkcií

Porovnávanie funkcií má v informatike význam pri posudzovaní časovej a pamäťovej náročnosti výpočtov. Určenie presného počtu krokov, ktoré program vykoná, alebo presného počtu bitov, ktoré pri výpočte počítač využije, je veľmi komplikované. Pre funkcie vyjadrujúce dobu výpočtu (počet krokov) a veľkosť použitej pamäte v závislosti od vstupu je jednoduchšie určiť len hranice, do ktorých ich môžeme „vtesnať". V tejto kapitole si priblížime notáciu, ktorá sa používa okrem iného aj na určenie týchto hraníc.

10.1 O-notácia

Pri posudzovaní výpočtovej zložitosti algoritmov sa veľmi často používa O-notácia. Začneme dvomi príkladmi.

Vezmime zoznam prirodzených čísel $a_1, \ldots, a_n$. Chceme zistiť, koľkokrát sa nachádza číslo x v tomto zozname. Koľko krokov v najhoršom prípade urobí nasledujúci postup?

```
FOR i=1 TO n
  IF x=a[i] THEN k:=k+1
```

Cyklus sa opakuje n-krát. Pri každom opakovaní musíme porovnať dvojicu čísel. Ak predpokladáme, že na zadanie každého čísla sme použili konštantný počet bitov, tak na porovnanie dvoch čísel potrebujeme vykonať počet operácií ohraničený konštantou (porovnávame v najhoršom prípade každý bit). Túto konštantu označme c_1. Ak sa čísla v podmienke rovnajú, tak navyše musíme vykonať jeden súčet, čo znamená tiež konštantný počet operácií (povedzme c_2). V najhoršom prípade teda program vykoná $(c_1 + c_2)n$ operácií. Čiže existuje konštanta $c \in R^+$ taká, že počet krokov $p_1(n)$, ktoré program v najhoršom prípade vykoná (v závislosti od počtu čísel n v zozname) je menší, alebo rovný, ako cn.

Vezmime súčet prirodzených čísel, ktoré sú zadané v tabuľke tvaru $n \times n$, čo môžeme zapísať

$$\sum_{j=1}^{n} \sum_{i=1}^{n} a_{i,j}$$

a v programátorskom „pseudokóde" to možno zapísať:

```
FOR j=1 TO n
  FOR i=1 TO n
    suma:=suma+a[i,j]
```

Počet krokov $p_2(n)$, ktoré program v najhoršom prípade vykoná v závislosti od n je cn^2, kde c je konštanta, ktorou vyjadrujeme, že na súčet dvoch čísel potrebujeme konštantný počet operácií (predpokladáme, že čísla sú reprezentované konštantným počtom bitov a čísla sčitujeme po bitoch).

V oboch príkladoch teda existovala konštanta c taká, že $p_1(n) \leq cn$, respektíve $p_2(n) \leq cn^2$. Aby sme sa nemuseli zaoberať konštantami pri posudzovaní zložitosti algoritmov, dohodla sa konvencia, že sa bude miesto uvedených nerovností a vyjadrení o existencii vhodnej konštanty používať zápis $p_1(n) = O(n)$ pre prvý prípad a $p_2(n) = O(n^2)$ pre druhý prípad.

Definujme to presnejšie (podľa [17, 20]).

Definícia 10.1.1. *Nech sú dané funkcie $f : N \to R^+$ a $g : N \to R^+$. Hovoríme, že*

$$f(n) = O(g(n)) ,$$

ak existuje konštanta $c > 0$ a $n_0 \in N$ také, že pre $\forall n \in N$, $n \geq n_0$ platí $f(n) \leq cg(n)$.

Niekoľko príkladov.

1. Funkcia $f(n) = 100n^3$ a $g(n) = n^3$. Potom pre $\forall n \in N$ platí $100n^2 \leq cn^2$, kde $c = 100$. Čiže $100n^2 = O(n^2)$.
2. Nech $f(n) = 10n!$ a $g(n) = 2n!$. Potom pre $\forall n \in N$ platí $10n! \leq c2n!$, kde $c = 5$. Čiže $10n! = O(2n!)$. Tiež ale platí $10n! = O(n!)$. Platí dohoda, že funkciu $g(n)$ sa snažíme voliť čo najjednoduchšie a pokiaľ možno bez konštánt. Takže v poslednom príklade volíme radšej $g(n) = n!$, ako $g(n) = 2n!$.
3. Nech $f(n) = n^2 + 100n + 5$ a $g(n) = n^2$. Pre $\forall n \in N$ platí

$$n^2 + 100n + 5 \leq n^2 + 100n^2 + 5n^2 = 106n^2 .$$

Takže existuje konštanta $c = 106$ taká, že pre $\forall n \in N$ $n^2+100n+5 \leq 106n^2$. Takže $n^2 + 100n + 5 = O(n^2)$.

4. Nech $f(n) = n^2$ a $g(n) = n^3$. Potom pre $\forall n \in N$ platí $n^2 \leq n^3$.
5. Nech $f(n) = n$ a $g(n) = n \log n$. Z vlastností logaritmov vieme, že pre ľubovoľné $n \geq 10$ platí $\log n \geq 1$. Takže pre $\forall n \in N$, $n \geq 10$ platí $n \leq n \log n$, pričom konštantu c možno zvoliť rovnú jednej.

Na zjednodušenie výpočtov v predchádzajúcich príkladoch sa dá použiť nasledujúce tvrdenie.

Veta 10.1.1. *Ak pre funkcie $f(n)$ a $g(n)$, kde $f : N \to R^+$ a $g : N \to R^+$, existuje limita ich podielu*

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = c,$$

pričom c je reálne číslo, tak platí $f(n) = O(g(n))$. Ak je táto limita rovná ∞, tak $f(n) \neq O(g(n))$.

Predchádzajúce tvrdenie sa dalo využiť v príkladoch 1 až 5, pretože tam uvedené limity existujú. Ukážme si príklad, kde toto tvrdenie nemožno využiť.

6. Nech $f(n) = (2 + (-1)^n)n$ a $g(n) = n$. Ľahko sa presvedčíme, že

$$\lim_{n\to\infty} \frac{(2+(-1)^n)n}{n} = \lim_{n\to\infty} (2 + (-1)^n)$$

neexistuje, pretože postupnosť $(2 + (-1)^n)$ osciluje medzi hodnotami 1 a 3. Ak však zvolíme konštantu $c = 3$, tak pre $\forall n \in N$ platí, že $(2 + (-1)^n)n \leq 3n$. Takže podľa definície máme $(2 + (-1)^n)n = O(n)$.

10.2 Niektoré nepríjemnosti spojené s používaním $O(g(n))$

Pri narábaní so zápisom $f(n) = O(g(n))$ môžeme naraziť na niekoľko problémov. Ukážme si niektoré záludnosti, s ktorými by sme sa mohli stretnúť [17].

1. Vieme, že relácia "=" je tranzitívna. To znamená, že pre $\forall a, b, c \in R$ platí: ak $a = b \wedge b = c$, potom $a = c$. Z predchádzajúcej časti vieme, že $n = O(n)$ a $2n = O(n)$, avšak $n \neq 2n$. To znamená, že na "=" použité v tomto zápise nemôžeme pozerať, ako na klasické rovná sa. Platí dohovor, že zápis $f(n) = O(g(n))$ sa používa len v tomto smere. Opačný smer $O(g(n)) = f(n)$ sa nepoužíva, aby sme sa vyhli predchádzajúcej nepríjemnosti. Zjednodušene povedané, zápis $f(n) = O(g(n))$ nám hovorí, že funkcia $f(n)$ nemá právo sa veľmi povyšovať nad funkciu $g(n)$.

2. Pre ľubovoľnú konštantu k platí $k = O(1)$. Pozrime sa teraz lepšie na tento zápis. Vezmime súčet

$$\sum_{i=1}^{n} i = 1 + 2 + \cdots + n = O(1) + O(1) + \cdots + O(1) = nO(1) = O(n) .$$

Avšak už vieme, že

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} = \frac{1}{2}n^2 + \frac{1}{2}n = O(n^2)\,.$$

Kde sa stala chyba? Hlavný problém je, že v prvom zápise sme použili $n = O(1)$, čo samozrejme neplatí.

10.3 Zložitosť algoritmov

Ako bolo spomenuté, O-notácia sa používa na vyjadrenie výpočtovej zložitosti algoritmov. Pod pojmom výpočtová zložitosť budeme rozumieť počet krokov, ktoré musí v najhoršom prípade algoritmus vykonať. Ukážme, prečo je dôležité posudzovať, koľko krokov v najhoršom prípade algoritmus urobí. V nasledujúcej tabuľke máme vyznačené, aká je približná doba výpočtu algoritmov na počítači, ktorý je schopný spracovať 10^{10} operácií za sekundu. Brali sme algoritmy, kde počet krokov v závislosti od veľkosti vstupu n nepresiahne n, n^2, n^4, 2^n, $n!$. Za n sme dosadili postupne hodnoty 20, 50, 100, 500, 1000.

$g(n)\backslash n$	20	50	100	500	1000
n	2 ns	5 ns	10 ns	50 ns	0,1 μs
n^2	40 ns	0,25 μs	1 μs	25 μs	100 μs
n^4	16 μs	625 μs	10 ms	6,25 s	100 s
2^n	0,1 ms	$\doteq$ 31 hod	$\doteq 4{\cdot}10^{12}$ rokov	-	-
$n!$	$\doteq$ 8 rokov	$\doteq 9{\cdot}10^{47}$ rokov	-	-	-

Vidíme, že algoritmy, kde počet krokov je 2^n, respektíve $n!$ nie sú z praktického hľadiska veľmi výhodné, pretože doba výpočtu pre väčšie n je nepríjemne dlhá. Z toho vyplýva, že algoritmy, ktorých výpočtovú zložitosť nevieme vyjadriť lepšie ako $O(2^n)$ a $O(n!)$, nie sú vhodné pre praktické použitie. Naproti tomu algoritmy so zložitosťou $O(n)$, $O(n^2)$, $O(n^4)$ sú väčšinou (ak konštanta c, ktorú sme pri použití O-notácie ukryli, nie je príliš veľká, čo sa väčšinou nestáva) v praxi veľmi dobre použiteľné.

10.4 Theta

Pri použití O-notácie sme videli, že pre funkcie $f(n) = n^2 + 100n + 5$ a $g(n) = n^2$ platí: $f(n) = O(g(n))$. Tiež však platí pre $\forall n \in N$, že $n^2 \leq n^2 + 100n + 5$. Takže môžeme tiež písať: $g(n) = O(f(n))$. Naproti tomu, ak sme mali príklad s funkciami $f(n) = n^2$ a $g(n^3)$, tak platilo: $f(n) = O(g(n))$, ale opak neplatí: $n^3 \neq O(n^2)$. Pre algoritmy by teda platilo, že algoritmus, ktorý urobí v najhoršom prípade n^2 krokov je aj typu $O(n) = n^3$, pretože pomocou n^3 dostaneme horné ohraničenie pre n^2. Avšak vidíme, že toto ohraničenie nie je „tesné". Ak chceme vyjadiť túto tesnosť matematicky presne, používame zápis $f(n) = \Theta(g(n))$. Uvedieme dve (ekvivalentné) definície.

Definícia 10.4.1. *Ak pre funkcie $f : N \to R^+$ a $g : N \to R^+$ platí $f(n) = O(g(n))$ aj $g(n) = O(f(n))$, tak pre tieto funkcie používame zápis*

$$f(n) = \Theta(g(n)) \ .$$

Definícia 10.4.2. *Ak pre funkcie $f : N \to R^+$ a $g : N \to R^+$ existujú konštanty $c, d \in R$ a n_0 také, že $0 < c < d$ a pre $\forall n \in N$, $n \geq n_0$ platí $cg(n) \leq f(n) \leq dg(n)$, tak píšeme: $f(n) = \Theta(g(n))$.*

Tento zápis sa teda používa, ak chceme vyjadriť, že funkcie $f(n)$ a $g(n)$ sú, čo sa týka ich rastu, podobné.

10.5 Malé o

Pri limitách sme mali aj nasledujúce príklady:

$$\lim_{n\to\infty} \frac{n^2}{n^3} = 0, \quad \lim_{n\to\infty} \frac{n^2}{2^n} = 0, \quad \lim_{n\to\infty} \frac{2^n}{n!} = 0.$$

V týchto prípadoch postupnosť (funkcia definovaná na N) v čitateli rastie rádovo oveľa pomalšie ako postupnosť v menovateli.

Definícia 10.5.1. *Ak pre funkcie $f : N \to R^+$ a $g : N \to R^+$ platí*

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0,$$

tak pre tieto funkcie používame zápis

$$f(n) = o(g(n))$$

a hovoríme, že $f(n)$ je asymptoticky menšia, ako $g(n)$.

10.6 Asymptotická rovnosť

Vypočítajme nasledujúcu limitu.

$$\lim_{n\to\infty} \frac{\binom{n}{2}}{\frac{n^2}{2}} = \lim_{n\to\infty} \frac{\frac{n^2-n}{2}}{\frac{n^2}{2}} = 1\ .$$

Môžeme tiež povedať, že postupnosti v čitateli a v menovateli rastú rovnako rýchlo a môžeme to zapísať $\binom{n}{2} \sim \frac{n^2}{2}$.

Definícia 10.6.1. *Ak pre funkcie $f : N \to R^+$ a $g : N \to R^+$ platí*

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1,$$

tak pre tieto funkcie používame zápis

$$f(n) \sim g(n)$$

a hovoríme, že $f(n)$ a $g(n)$ sú asymptoticky rovné.

Príklad použitia tohto zápisu je Stirlingova formula pre faktoriál:

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n\ .$$

Táto formula nám hovorí, že pre dostatočne veľké n sa nedopustíme príliš veľkej chyby, ak miesto $n!$ použijeme výraz na pravej strane. Pre $n = 8$ je tá chyba napríklad približne 1% a pri zväčšujúcom sa n klesá k nule.

Kapitola 11

Úvod do teórie čísel

Teória čísel je oblasť matematiky, ktorej základy sa objavili už pred tisícročiami, no pre svoje zaujímavé a dôležité aplikácie, je jej stále venovaná veľká pozornosť. Pojmy, s ktorými budeme pracovať (deliteľnosť, zvyšok) sa učia už na základnej škole, tu uvedieme ich presné definície, ktoré nám umožnia poznávať nové vlastnosti týchto pojmov. Viac informácií čitateľ nájde napríklad v knihe [25] (ktorá je trochu staršia, ale bežne ju možno nájsť v knižniciach) alebo v knihe [9] (čo je publikácia, ktorá prináša najnovšie výsledky a množstvo aplikácií z teórie čísel).

11.1 Deliteľnosť

Hovoríme, že číslo $k \in Z$ je deliteľom čísla $n \in Z$, ak existuje také $q \in Z$, že $n = qk$. Môžeme to tiež označiť $k \mid n$ a hovoríme „k delí n". Číslo n je násobkom čísla k. Relácia $\mid$ je binárna relácia, ktorú môžeme definovať na množine celých aj prirodzených čísel. Pozrime sa na niektoré vlastnosti tejto relácie.

Veta 11.1.1. *Nech $a, b \in Z$. Ak $a \mid b$, potom pre $\forall c \in Z$ platí $a \mid bc$.*

Dôkaz. Ak $a \mid b$, tak existuje $q \in Z$ také, že $b = aq$. Potom však platí: $bc = aqc$, kde číslo $qc \in Z$, to znamená, že $a \mid bc$.

Veta 11.1.2. *Nech $a, b, c \in Z$. Ak $a \mid b$ a zároveň $a \mid c$, potom $a \mid (b + c)$.*

Dôkaz. Ak $a \mid b$ a $a \mid c$, tak existujú $q, r \in Z$ také, že $b = aq$ a $c = ar$. Potom však platí: $b + c = a(q + r)$, kde číslo $(q + r) \in Z$, to znamená, že $a \mid (b + c)$.

Veta 11.1.3. *Nech $a, b, c \in Z$. Ak $a \mid b$ a zároveň $a \mid c$, potom pre $\forall x, y \in Z$ platí $a \mid (xb + yc)$.*

Dôkaz. Využijeme predchádzajúce tvrdenia. Ak $a \mid b$ a $a \mid c$, tak $a \mid xb$ a $a \mid yc$. Potom však platí aj $a \mid (xb + yc)$.

Veta 11.1.4. *Nech $a, b, c \in Z$. Ak $a \mid b$ a zároveň $b \mid c$, potom $a \mid c$.*

Dôkaz. Ak $a \mid b$ a $b \mid c$, tak existujú $q, r \in Z$ také, že $b = aq$ a $c = br$. Potom však platí: $c = a(qr)$, kde číslo $qr \in Z$, to znamená, že $a \mid c$.

Otázky spojené s deliteľnosťou zaujímali už Grékov v staroveku. (Keďže nepoznali záporné čísla a nulu, pracovali len s prirodzenými číslami.) Vieme napríklad, že ich fascinovali dokonalé čísla. Číslo n nazveme dokonalé, ak súčet jeho deliteľov (prirodzených, okrem n) je rovný samotnému číslu n. Najmenšie známe dokonalé čísla sú $6 = 1+2+3$ a $28 = 1+2+4+7+14$. Gréci v staroveku objavili ešte dve ďalšie: 496 a 8128. Dnes ich stále poznáme menej ako päťdesiat - všetko párne.

11.2 Zvyšok

Začnime takouto úlohou: Aký deň bude o 25 dní, ak je dnes utorok? Nájdenie riešenia je samozrejme veľmi jednoduché, nám však táto úloha poslúži ako východisko pre naše ďalšie úvahy. To čo je pre výsledok dôležité, je zvyšok, ktorý dáva číslo 25 po delení číslom 7. Platí, že $25 = 3 \cdot 7 + 4$ a pre výpočet výsledku je dôležitá len tá štvorka na konci.
Poslednú rovnosť je možno sformulovať aj všeobecne, ako hovorí nasledujúca dôležitá veta:

Veta 11.2.1. *Pre ľubovoľné celé číslo n a ľubovoľné prirodzené číslo k existujú $q \in Z$ a $r \in \{0, 1, \ldots, k-1\}$ také, že $n = qk + r$. Navyše toto vyjadrenie je pre dané k a n jediné možné.*

Číslo r nazývame zvyšok po delení čísla n číslom k.

11.3 Najväčší spoločný deliteľ

V tejto časti sa budeme zaoberať len prirodzenými číslami. Hľadajme spoločných deliteľov čísel 20 a 24. Sú to čísla 1, 2, 4. Najväčšie z týchto čísel - číslo 4 nazývame najväčší spoločný deliteľ čísel 20 a 24.

Spoločný deliteľ čísel x, y je číslo k, pre ktoré platí $k \mid x$ a $k \mid y$. Každé dve prirodzené čísla majú spoločného deliteľa a to číslo 1. Ak majú aspoň jedného spoločného deliteľa, tak majú aj najväčšieho spoločného deliteľa. Najväčšieho spoločného deliteľa dvoch čísel x, y označíme $NSD(x, y)$. Jeden z postupov využívaných na hľadanie najväčšieho spoločného deliteľa sa nazýva Euklidov algoritmus. Ukážme si, ako funguje.

Nájdime najväčšieho spoločného deliteľa čísel 276 a 120. Vyjadrujme postupne zvyšky

$$\begin{aligned} 276 &= 2 \cdot 120 + 36 \\ 120 &= 3 \cdot 36 + 12 \\ 36 &= 3 \cdot 12 + 0 \end{aligned}$$

Posledný nenulový zvyšok je najväčším spoločným deliteľom čísel 276 a 120.

Vo všeobecnosti to vyzerá takto: hľadáme najväčšieho spoločného deliteľa dvoch čísel a a b. Predpokladajme, že $a > b$. Postupne vyjadrujme zvyšky, ako v predchádzajúcom príklade.

$$\begin{array}{lcll} a & = & q_1 \cdot b & + \; r_1 \\ b & = & q_2 \cdot r_1 & + \; r_2 \\ r_1 & = & q_3 \cdot r_2 & + \; r_3 \\ & \vdots & & \\ r_{i-2} & = & q_i \cdot r_{i-1} & + \; r_i \\ r_{i-1} & = & q_{i+1} \cdot r_i & + \; 0 \end{array}$$

Pre zvyšky platí

$$\begin{array}{lcll} 0 & < & r_1 & < \; b \\ 0 & < & r_2 & < \; r_1 \\ 0 & < & r_3 & < \; r_2 \\ & & \vdots & \\ 0 & < & r_i & < \; r_{i-1} \\ 0 & = & r_{i+1} & \end{array}$$

Najväčší spoločný deliteľ čísel a a b je posledný nenulový zvyšok, čiže

$$NSD(a, b) = r_i \; .$$

Postupnosť zvyškov $r_1, \ldots, r_i$ je teda klesajúca a zdola ohraničená nulou, takže tento algoritmus je konečný.
Čísla, ktoré majú najväčšieho spoločného deliteľa rovného 1 nazývame **nesúdeliteľné**.

Euklidov algoritmus má praktické využitie napríklad v kryptografii, ale svoje dôležité postavenie má aj v teórii výpočtovej zložitosti. Je to zrejme prvý algoritmus, pri ktorom sa matematici pokúsili odvodiť počet krokov výpočtu ako funkciu veľkosti vstupu. V roku 1844 Gabriel Lamé (1795 - 1870)

dokázal, že pre počet delení D, ktoré musí Euklidov algoritmus uskutočniť, platí:

$$D \leq 5 \log_{10} b \ ,$$

kde b je menšie z oboch čísel na vstupe algoritmu. Ak použijeme O-notáciu, tak počet delení je $O(x)$, kde x je počet cifier čísla b v desiatkovej sústave (vieme, že $x = 1 + \lfloor \log_{10} b \rfloor$).

11.4 Prvočísla a zložené čísla

Prirodzené čísla môžeme rozdeliť na tri druhy podľa počtu deliteľov. Špeciálne postavenie má číslo 1, ktoré má len jedného deliteľa (samého seba). Potom sú to čísla, ktoré majú práve dvoch deliteľov: jednotku a samého seba. Tieto čísla nazveme prvočísla (sú to napríklad čísla $2, 3, 5, 7, \ldots$). Tretiu skupinu tvoria čísla, ktoré majú viac ako dvoch deliteľov. Nazývame ich zložené čísla (sú to napríklad čísla $4, 6, 8, 9, \ldots$).

Veta 11.4.1. *Každé zložené číslo je deliteľné prvočíslom.*

Dôkaz. Predpokladajme, že toto tvrdenie nie je pravdivé a existujú zložené čísla, ktoré nie sú deliteľné prvočíslom. Najmenšie takéto číslo označme x. Keďže x je zložené číslo, musí byť deliteľné číslom (označme ho y), ktoré je rôzne od 1 aj x. Číslo y musí byť zložené číslo (x nie je deliteľné prvočíslom) a keďže $y < x$, tak je deliteľné nejakým prvočíslom p. Čiže máme $p \mid y$ a $y \mid x$. Podľa tvrdenia 4 platí $p \mid x$. To je spor s tým, že x nie je deliteľné prvočíslom. Takže musí platiť pôvodné tvrdenie, že každé zložené číslo je deliteľné prvočíslom.

O prvočísla sa (ako inak) zaujímali už Gréci v staroveku. Euklides (žil v štvrtom storočí pred Kristom) napríklad dokázal:

Veta 11.4.2. *Prvočísel je nekonečne veľa.*

Dôkaz. Predpokladajme, že toto tvrdenie neplatí a prvočísel je konečne veľa. Označme ich $p_1, p_2, \ldots, p_k$. Nech $P = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$. Číslo P nemôže

byť prvočíslo, pretože je väčšie ako každé z prvočísel $p_1, \ldots, p_k$. Teda P by malo byť zložené číslo, ale podľa predchádzajúceho tvrdenia potom P musí byť deliteľné prvočíslom. Avšak číslo P dáva po delení ľubovoľným z prvočísel $p_1, \ldots, p_k$ zvyšok 1. Takže P nemôže byť ani zložené číslo. Dospeli sme k sporu. Musí platiť pôvodné tvrdenie, čiže prvočísel je nekonečne veľa.

Číslo 12 sa dá rozpísať na súčin prvočísel nasledujúco $12 = 2{\cdot}2{\cdot}3 = 2^2{\cdot}3$. Ak by sme takto skúsili rozpísať niektoré ďalšie čísla, zistíme, že je to tiež možné. O tomto hovorí nasledujúce tvrdenie, ktoré sa nazýva základná veta aritmetiky.

Veta 11.4.3. *Každé prirodzené číslo $n > 1$ sa dá jediným spôsobom zapísať v tvare*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k},$$

kde $p_1 < p_2 < \cdots < p_k$ sú prvočísla a $\alpha_1, \alpha_2, \ldots, \alpha_k$ sú prirodzené čísla.

Vyjadrenie prirodzeného čísla v tomto tvare sa nazýva faktorizácia alebo rozklad čísla na súčin prvočísel.

Vráťme sa ešte k dokonalým číslam. Dnes vieme (vďaka dvom velikánom matematiky: Euklidovi a Eulerovi), že párne číslo n je dokonalé práve vtedy, keď sa dá zapísať v tvare

$$n = 2^{p-1}(2^p - 1)\,, \tag{11.1}$$

pričom p a $2^p - 1$ sú prvočísla. Prvočísla zapísateľné v tvare $2^p - 1$ nazývame Mersennove prvočísla. Ak nájdeme nejaké Mersennovo prvočíslo, tak vďaka vzťahu (11.1) vieme z neho odvodiť dokonalé číslo. Ak máme párne dokonalé číslo, postupným delením dvojkou z neho vieme vyrobiť Mersennovo prvočíslo. To znamená, že párnych dokonalých čísel a Mersennových prvočísel je rovnako veľa (a stále nevieme koľko). Zaujímavé je, že to čo vyzeralo storočia ako zábava a hra s číslami, našlo v 20. a 21. storočí celkom nečakané aplikácie. Mersennove prvočísla sa dnes využívajú v niektorých generátoroch pseudonáhodných čísel.

11.5 Modulárna aritmetika

V tejto časti si povieme viac o aritmetike, ktorá funguje na kružnici s konečným počtom dielikov. Je to aritmetika javov, ktoré sa cyklicky opakujú. Vezmime napríklad dni v týždni. Ak je sobota a niekto nám povie, že príde o tri dni, tak vieme, že príde v utorok. Pri počítaní sa pohybujeme po kružnici, ktorá má sedem dielikov.

Podobne funguje počítanie hodín. Hodinový ciferník predstavuje kružnicu s dvanástimi dielikmi. Ak je 10 hodín a povieme, že prídeme o 7 hodín, na hodinovom ciferníku bude 5 hodín.

Podobne to funguje so zvyškami po delení číslom $k \in N$. Venujme sa najprv otázke, ako vyzerá zvyšok súčtu a súčinu dvoch čísel po delení číslom k. Začnime prípadom, keď $k = 2$. Každému je jasné, že súčtom dvoch párnych čísel dostávame párny výsledok, nepárne číslo s párnym dáva nepárny súčet atď. Je ľahké si uvedomiť, že zvyšok súčtu a súčinu po delení dvojkou závisí len od toho, či pôvodné čísla boli párne alebo nepárne. Prehľadnejšie je to v nasledujúcich tabuľkách (zápis je vyjadrený pomocou zvyškov).

$\oplus_2$	0	1
0	0	1
1	1	0

$\odot_2$	0	1
0	0	0
1	0	1

V tabuľkách máme definovanú modulárnu aritmetiku, alebo aritmetiku modulo 2. (Aritmetiku na zvyškových triedach modulo 2.) Skôr než si povieme viac o aritmetike modulo k, uveďme dva dôležité fakty. Majme dve prirodzené čísla n_1, n_2 a ich zvyšky po delení číslom k. Ako sme videli skôr, n_1 a n_2 sa dajú jednoznačne zapísať v tvare $n_1 = q_1 \cdot k + r_1$ a $n_2 = q_2 \cdot k + r_2$. Potom

$$n_1 + n_2 = (q_1 \cdot k + r_1) + (q_2 \cdot k + r_2) = (q_1 + q_2) \cdot k + (r_1 + r_2)\,.$$

Časť $(q_1 + q_2) \cdot k$ je deliteľná číslom k a neprispieva k zvyšku výsledku ničím. Zvyšok výsledku závisí len od súčtu zvyškov $r_1 + r_2$. Podobne to platí pre súčin

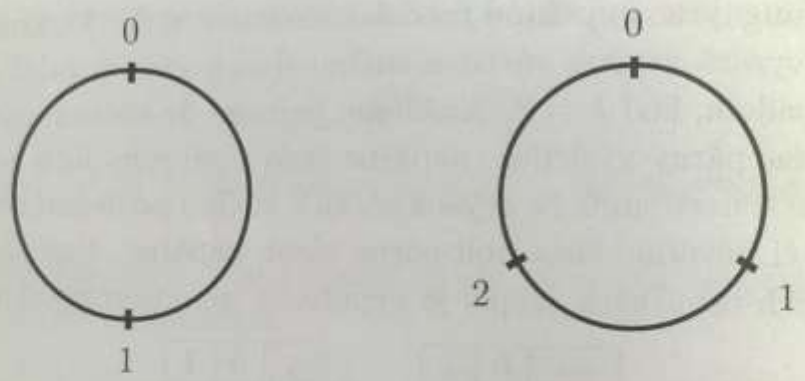
$$n_1 \cdot n_2 = (q_1 \cdot k + r_1) \cdot (q_2 \cdot k + r_2) = (k \cdot q_1 \cdot q_2 + q_1 \cdot r_2 + q_2 \cdot r_1) \cdot k + r_1 \cdot r_2\,.$$

Podobne ako pri súčte, zvyšok súčinu závisí len od súčinu zvyškov $r_1 \cdot r_2$. Pre $k = 3$ máme zvyšky $0, 1, 2$ a aritmetika zvyškových tried modulo 3 je daná nasledujúcimi tabuľkami.

$\oplus_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\odot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Ako sme spomínali, toto je aritmetika, v ktorej sa pohybujeme na kružnici s daným počtom dielikov.



V aritmetike, ktorú poznáme zo základnej školy sa pohybujeme na číselnej osi. Súčet $2+1$ si môžeme predstaviť aj tak, že z čísla 0 sa posunieme o dva dieliky na číslo 2 a potom sa posunieme o jeden dielik a zastavíme na čísle 3. V aritmetike modulo 3, teda na kružnici s tromi dielikmi to je podobné. Súčet $2 \oplus_3 1$ si môžeme predstaviť aj tak, že sa posunieme z čísla 0 o dva dieliky na číslo 2 a potom o jeden dielik na číslo 0. Podobne to funguje pre súčin. Napríklad $2 \odot_3 2$ znamená, že sa z čísla 0 dvakrát posunieme o dva dieliky, na číslo 1. Nie je ťažké si uvedomiť, že aritmetika na kružnici, ktorá má k dielikov, plne korešponduje s aritmetikou zvyškových tried modulo k. Pre $k = 2$ a $k = 3$ sú operácie sčitovania a násobenia na kružnici definované tabuľkami, ktoré máme vyššie. Pre malé k môže byť prístup cez kružnicu názornejší, ale pre väčšie k a pri skúmaní a dokazovaní vlastností operácií $\oplus_k$, $\odot_k$ (napríklad asociatívnosť, komutatívnosť, definovanie opačných a inverzných prvkov) je vhodnejší prístup využívajúci zvyšky.

Označme znakom Z_k množinu všetkých zvyškov po delení číslom k. Čiže $Z_k = \{0, 1, \ldots, k-1\}$. Z algebry vieme, že algebraická štruktúra $(Z_k, \oplus_k, \odot_k)$ je okruh a ak je k prvočíslo, tak $(Z_k, \oplus_k, \odot_k)$ je pole.

Modulárna aritmetika má v informatike množstvo aplikácií. Na tomto mieste si povedzme o jednej z nich. Pri reprezentácii prirodzených a celých čísel v počítači sme hovorili o tom, že pri použití základných aritmetických operácií sa pohybujeme na kružnici. Počítače pracujú s aritmetikou modulo 2^n, kde n je počet bitov, ktoré sú použité na reprezentáciu. Vráťme sa k reprezentácii celých čísel pomocou doplnkového kódu. Vysvetlime si na osembitovej reprezentácii, ako tento kód funguje. Pre kladné čísla je prvý bit rovný nule, ostatné slúžia na zakódovanie čísel od 0 po 127. Nech x je kladné celé číslo z tohto rozsahu. Ukážeme, že záporné číslo $-x$ v doplnkovom kóde je vlastne inverzný prvok k prvku x v okruhu $(Z_{256}, \oplus_{256}, \odot_{256})$ vzhľadom na sčitovanie modulo 256. Inverzný prvok k $x \in Z_{256}$ vzhľadom na operáciu $\oplus_{256}$ je číslo $256 - x = 255 + 1 - x = 255 - x + 1$. V osembitovej reprezentácii máme $255 = (11111111)_2$, $x = (a_7a_6a_5a_4a_3a_2a_1a_0)_2$ a $255 - x = (11111111)_2 - (a_7a_6a_5a_4a_3a_2a_1a_0)_2 = (b_7b_6b_5b_4b_3b_2b_1b_0)_2$, kde $b_i = 1 - a_i$. To vlastne znamená zmenu každého bitu na opačný. Pripočítaním čísla $1 = (00000001)_2$ k tomuto výsledku dostávame osembitovú reprezentáciu inverzného prvku vzhľadom k prvku x. Tento postup je identický s postupom na hľadanie doplnkového kódu, ktorý sme opísali v tretej kapitole.

11.6 Niekoľko nevyriešených problémov z teórie čísel

Mnohé problémy z teórie čísel majú tú vlastnosť, že ich možno sformulovať veľmi jednoducho a zrozumiteľne, ale ich riešenie dodnes odoláva matematikom. Záver tejto kapitoly venujme niekoľkým takýmto problémom.

Problém 1. Koľko je párnych dokonalých čísel a Mersennových prvočísel? Je ich konečný, alebo nekonečný počet?

Problém 2. Existuje nepárne dokonalé číslo?

Tieto problémy sme už spomínali, svoj pôvod majú v staroveku, podobne ako nasledujúci problém.

Problém 3. Koľko je prvočíselných dvojčiat?

Prvočíselné dvojčatá sú dvojice prvočísel, ktorých rozdiel je rovný dvom. Napríklad 3 a 5, 5 a 7, 11 a 13. Nevieme, či existuje nekonečne veľa takýchto dvojíc.

Problém 4. (Goldbachova domnienka.) Dá sa každé párne prirodzené číslo počnúc štvorkou zapísať ako súčet dvoch prvočísel?

Napríklad máme $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$. Ako napovedá názov, tento problém pochádza od nemeckého matematika Christiana Goldbacha (1690 - 1764) a je z roku 1742 (nachádza sa v Goldbachovej korešpondencii s L.Eulerom).

Uveďme ešte jeden problém, sformulovaný Bernhardom Riemannom (1826 - 1866) v roku 1859, ktorý nie je až taký ľahký na sformulovanie, ale bol Davidom Hilbertom (1862 - 1943) zaradený v roku 1900 do zoznamu 23 otvorených matematických problémov, na vyriešenie ktorých, by sa mali matematici v dvadsiatom storočí zamerať. Momentálne je zaradený medzi sedem najdôležitejších matematických problémov, ktoré čakajú na vyriešenie v treťom tisícročí (zostalo ich už iba šesť, keďže Poincarého domnienka bola vyriešená). Za vyriešenie tohto, bezpochyby kráľovského problému matematiky, bola vypísaná odmena milión dolárov. O týchto problémoch sa populárnym spôsobom píše v knihe [4].

Problém 5. (Riemannova hypotéza.) Zeta funkcia nasledujúca špe-

ciálna funkcia:

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x} ,$$

ktorej definičný obor je množina všetkých komplexných čísel. Riemannova hypotéza hovorí, že každý netriviálny koreň tejto funkcie je v tvare $x = 1/2 + bi$ (kde $b \in R$).

Za triviálne korene sú považované čísla $-2, -4, -6, \ldots$. Ako vidieť, zadanie problému je oveľa náročnejšie na pochopenie ako tie predchádzajúce. Jeho vyriešenie by však znamenalo značný pokrok v matematike. Napríklad by to pomohlo rozšíriť naše poznatky o rozložení prvočísel, umožnilo by to zvýšiť účinnosť a zrýchliť niektoré, v praxi používané, algoritmy.

Kapitola 12

Niekoľko algoritmov z teórie čísel

V tejto časti si priblížime niekoľko algoritmov pracujúcich s matematikou z predchádzajúcej kapitoly. Praktické využitie týchto algoritmov je predovšetkým v oblasti počítačovej bezpečnosti, v kryptografii a v kódovaní.

12.1 Zisťovanie prvočíselnosti

Pozrime sa na problém: Dané je prirodzené číslo n. Zistite či je n prvočíslom.
Tento problém sa nazýva problém prvočíselnosti. Už Gréci v staroveku poznali algoritmus na riešenie tohto problému. Tento algoritmus nazývame Eratosthenovo sito. Postup môžeme opísať nasledujúco:
Chceme zistiť, či je číslo n prvočíslo.

1. Vytvoríme zoznam všetkých prirodzených čísel od 2 po n.

2. Zakrúžkujeme prvé číslo v zozname, ktoré ešte nie je zakrúžkované ani zaškrtnuté.

3. Ak sme zakrúžkovali n, algoritmus končí - n je prvočíslo. Inak pokračujeme ďalej.
4. Vyškrtáme všetky násobky posledného zakrúžkovaného čísla zo zoznamu.
5. Ak sme vyškrtli n, algoritmus končí - n je zložené číslo. Inak pokračujeme krokom 2.

Iný algoritmus na zisťovanie prvočíselnosti, s ktorým sa stretávajú už stredoškoláci je algoritmus, v ktorom skúšame všetky prirodzené čísla menšie alebo rovné ako $\sqrt{n}$, či sú deliteľmi čísla n.

1. Vypočítaj $\sqrt{n}$.
2. Pre všetky prirodzené čísla x, kde $2 \leq x \leq \sqrt{n}$ urob: Ak x je deliteľom n, tak algoritmus končí - x nie je prvočíslo. Inak prejdi na ďalšie číslo v poradí.
3. Ak žiadne x nie je deliteľom n, tak n je prvočíslo.

Zdá sa, že druhý algoritmus by pre veľké čísla mohol byť rýchlejší. Je však naozaj efektívny? Zoberme číslo zapísané pomocou 256 bitov. Toto číslo môže mať hodnotu až $2^{256} - 1$. Aby sme si situáciu zjednodušili, odmocnime číslo 2^{256}. Čiže v najhoršom prípade by sme museli testovať deliteľov od 2 po 2^{128}. To je približne $3 \cdot 10^{38}$ čísel. Ak máme k dispozícii počítač, ktorý otestuje približne 10^{10} čísel za sekundu, zistíme, že by nám to mohlo trvať zhruba $3 \cdot 10^{28}$ sekúnd, čo je okolo 10^{21} rokov. Ak by bola rýchlosť počítača desaťnásobne vyššia, doba výpočtu by sa znížila len na 10^{20} rokov. Vzhľadom na to, že zadať do počítača číslo, na ktorého zápis potrebujeme 256 bitov, nie je problém, tento algoritmus nie je veľmi efektívny a v praxi, kde sa táto matematika využíva je nevhodný.

Ukážme si základný princíp, na ktorom je založený momentálne najpoužívanejší algoritmus na testovanie prvočíselnosti - tzv. Rabinov-Millerov test. Jeho základom je nasledujúce tvrdenie, pochádzajúce od P. Fermata (1601 - 1665).

Veta 12.1.1. *(Malá Fermatova veta.) Ak p je prvočíslo a a je prirodzené číslo nesúdeliteľné s p. Potom platí*

$$a^{p-1} \equiv 1 \ (mod\ p)\ .$$

Zápis $x \equiv y \ (mod\ p)$ znamená, že čísla x a y dávajú rovnaký zvyšok po delení číslom p. Zápisu $x \equiv 1 \ (mod\ p)$ možno rozumieť aj tak, že x dáva zvyšok 1 po delení číslom p. Zápis $x \equiv y \ (mod\ p)$ čítame: „x je kongruentné s y modulo p" (nazýva sa aj kongruencia) a $\equiv$ je binárna relácia nazývaná relácia kongruencie.

1. Nech $p = 3$, $a = 2$. Potom $2^2 \equiv 1 \ (mod\ 3)$.
2. Nech $p = 5$, $a = 2$. Potom $2^4 \equiv 1 \ (mod\ 5)$.
3. Nech $p = 9$, $a = 2$. Potom $2^8 \not\equiv 1 \ (mod\ 9)$ $(2^8 \equiv 4 \ (mod\ 9))$.

V poslednom príklade sme videli, že pre zložené číslo $p = 9$ mocnina 2^8 nedávala zvyšok 1 po delení číslom p. Dá sa tento fakt využiť na testovanie prvočíselnosti? Odpoveď znie, že dá, avšak tento postup nie je úplne perfektný, občas môže dôjsť k chybe. Malá Fermatova veta je implikácia. Ak je p prvočíslo, tak uvedená kongruencia platí. O prípadoch, keď p nie je prvočíslom však nič nehovorí. Zlá správa je, že boli nájdené také zložené čísla x, že pre ne existuje číslo a, ktoré je s nimi nesúdeliteľné, ale kongruencia $a^{x-1} \equiv 1 \ (mod\ x)$ platí. Boli dokonca nájdené zložené čísla (nazývané Carmichaelove čísla) také, že pre každé prirodzené číslo a, ktoré je nesúdeliteľné s x, platí $a^{x-1} \equiv 1 \ (mod\ x)$. Našťastie sa ukázalo, že takýchto čísel je veľmi málo a algoritmus využívajúci malú Fermatovu vetu, doplnený Rabinom a Millerom o niektoré ďalšie podmienky sa z praktického hľadiska ukazuje, ako veľmi dobrý algoritmus na testovanie prvočíselnosti. Aj keď určitá veľmi malá pravdepodobnosť, že zložené číslo prehlási za prvočíslo tu existuje (ide o tzv. pravdepodobnostný algoritmus).

12.2 Rozklad čísla na súčin prvočísel

Faktorizácia alebo rozklad čísla na súčin prvočísel je ďalší problém, ktorému sa budeme venovať. Tento problém možno sformulovať nasledujúco: nech

je dané prirodzené číslo n. Nájdite rozklad tohto čísla na súčin prvočísel. Jeden algoritmus, ktorý by nás mohol napadnúť je nasledujúci: Máme číslo n a skúšame všetky prvočísla od 2. Ak číslo 2 je deliteľom $n = n_0$, potom $n = 2 \cdot n_1$ a pokračujeme ďalej, skúšame či 2 je deliteľom n_1. Ak je deliteľom n_1, potom $n_1 = 2 \cdot n_2$ a $n = 2^2 \cdot n_2$ a opakujeme to isté pre 2 a n_2. Ak 2 nie je deliteľom niektorého n_i, tak prejdeme na ďalšie prvočíslo v poradí. Takto pokračujeme, až kým nenájdeme $n_k = 1$.

Podobnými úvahami ako v časti o zisťovaní prvočíselnosti dospejeme k záveru, že tento postup je pre veľké čísla nevhodný. Stačí si zobrať zložené číslo $n = p^2$, kde p je prvočíslo, na ktorého zápis potrebujeme napríklad 256 bitov. Zistili by sme, že tento postup je na uvedené číslo nepoužiteľný. A navyše treba dodať, že na rozdiel od problému prvočíselnosti, na problém faktorizácie nebol nájdený žiadny algoritmus použiteľný v praxi aj pre veľké čísla.

12.3 Rýchle umocňovanie

Vypočítajme mocninu 7^{17}. Spôsob, ktorý nás určite napadne ako prvý je postupne násobiť číslom 7 čiastkové výsledky, čo znamená počítať 16 súčinov.

Postupujme teraz inak. Číslo 17 zapisujeme v dvojkovej sústave $(10001)_2$. Čiže $17 = 2^0 + 2^4$ a $7^{17} = 7^{2^0+2^4} = 7^1 \cdot 7^{16}$. Hodnotu 7^1 máme a 7^{16} vieme vypočítať nasledujúco: počítame postupne

$$7^2 \to (7^2)^2 = 7^4 \to (7^4)^2 = 7^8 \to (7^8)^2 = 7^{16}\,.$$

To znamená štyri súčiny na výpočet 7^{16} a jeden súčin $7^1 \cdot 7^{16}$. To je spolu 5 súčinov miesto 16.

Uvedený postup využíval len asociatívnosť súčinu a je použiteľný aj pre ďalšie asociatívne operácie, napríklad súčin a umocňovanie matíc a takto vieme rýchlo umocňovať aj prvky v ľubovoľnom poli $(Z_p, \oplus_p, \odot_p)$, kde p je prvočíslo. Ešte viac si uvedomíme výhodnosť tohto postupu, keď máme vypočítať mocninu a^x, kde napríklad $x = 2^{999} + 2^{998} + \cdots + 2^1 + 2^0$ ($x = 2^{1000} - 1$), čiže číslo zapísané pomocou 1000 bitov. Ak by sme to umocňovali

"klasicky", tak by to znamenalo počítať $2^{1000} - 2$ súčinov, čo je nemožné realizovať aj na tých najvýkonnejších počítačoch. Ak by sme zvolili druhý postup, tak postupne počítame mocniny

$$a^2 \to a^4 \to \cdots \to a^{2^{998}} \to a^{2^{999}},$$

čo znamená 999 súčinov. Treba ešte vynásobiť

$$a^1 \cdot a^2 \cdot a^4 \cdot \ldots \cdot a^{2^{998}} \cdot a^{2^{999}},$$

čo je ďalších 999 súčinov. Spolu je to teda len 1998 súčinov, namiesto $2^{1000} - 2$ súčinov z prvého postupu. Ak navyše pracujeme v poli $(Z_p, \oplus_p, \odot_p)$, tak nám nehrozí, že by hodnota a^x neúmerne rástla a neboli by sme schopní držať ju v pamäti.

12.4 Výpočet inverzného prvku v poli $(Z_p, \oplus_p, \odot_p)$

Inverzný prvok k prvku a v poli $(Z_p, \oplus_p, \odot_p)$ je prvok a^{-1}, pre ktorý platí $a \odot a^{-1} = 1$. Ak je p veľmi veľké prvočíslo, tak hľadanie inverzného prvku postupným skúšaním prvkov tohto poľa nie je z časových dôvodov vhodné. Na hľadanie inverzného prvku môžeme využiť malú Fermatovu vetu. Keďže p je prvočíslo a číslo $a \in Z_p = \{0, 1, \ldots, p-1\}$ (navyše $a \neq 0$), tak čísla a, p sú nesúdeliteľné (inak by malo p deliteľa rôzneho od 1 a p a nebolo by prvočíslom). Potom spĺňajú predpoklady malej Fermatovej vety a platí:

$$a^{p-1} = a \cdot a^{p-2} \equiv 1 \ (mod\ p)\ .$$

Čiže súčin $a \cdot a^{p-2}$ dáva zvyšok 1 po delení číslom p. To však znamená, že $a \odot a^{p-2} = 1$ a $a^{-1} = a^{p-2}$. Vďaka algoritmu na rýchle umocňovanie vieme inverzný prvok vypočítať aj v poli$(Z_p, \oplus_p, \odot_p)$, keď p je veľké prvočíslo.

12.5 Algoritmus RSA

Algoritmus RSA je ukážkou využitia poznatkov teórie čísel v praxi (pozri tiež [17, 9]). Tento algoritmus sa používa na šifrovanie pomocou verejného

kľúča. Princíp tohto šifrovania spočíva v tom, že ten, kto chce prijať zašifrovanú správu, zverejní kľúč na jej zašifrovanie. Každý, kto má záujem, mu môže poslať zašifrovanú správu. Ak však niekto chce dešifrovať správu, potrebuje ešte tajný kľúč. V algoritme RSA na získanie tajného kľúča potrebujeme zistiť rozklad zvoleného čísla na súčin prvočísel. Ako sme spomenuli v časti o faktorizácii, takýto algoritmus zatiaľ nebol objavený.

Popis algoritmu

Príjemca vytvorí verejný a tajný kľúč nasledujúco:

1. Vygeneruj dve rôzne (dostatočne veľké) prvočísla p a q.
2. Vypočítaj $n = pq$.
3. Vyber celé číslo e také, že $NSD(e, (p-1)(q-1)) = 1$.
4. Vypočítaj číslo d také, že súčin de dáva po vydelení číslom $(p-1)(q-1)$ zvyšok 1 (čiže pracujeme s aritmetikou modulo $(p-1)(q-1)$).

Dvojica (e, n) predstavuje verejný kľúč a dvojica (d, n) tajný kľúč.
Posielajúci pomocou verejného kľúča zašifruje správu m_1 na m_2 nasledujúco: $m_2 = mod(m_1^e, n)$.
Príjemca dešifruje pomocou tajného kľúča správu m_2 na m_1 nasledujúco: $m_1 = mod(m_2^d, n)$.
Funkcia $mod(x, y)$ vracia na výstupe zvyšok r zo zápisu $x = qy + r$. Zápis $mod(m_1^e, n)$ vlastne vyjadruje výpočet mocniny m_1^e v aritmetike modulo n.

Ukážme si tento postup na príklade s malými číslami. Nech $p = 5$ a $q = 11$. Potom $n = 55$. Číslo e volíme tak, aby bolo nesúdeliteľné s číslom $(p-1)(q-1) = 40$. Napríklad $e = 3$. Dvojica $(3, 55)$ predstavuje verejný kľúč. Vypočítame $d = 27$. Dvojica $(27, 55)$ predstavuje tajný kľúč. Ak odosielateľ chce poslať správu m_1, zapíše ju ako postupnosť núl a jednotiek. Tejto postupnosti zodpovedá v dvojkovej sústave prirodzené číslo, označme ho tiež m_1. Nech je teda správa reprezentovaná číslom

$m_1 = 25$. Ten kto nám chce poslať správu, ju zašifruje pomocou verejného kľúča na správu $m_2 = mod(25^3, 55) = 5$. Na dešifrovanie použijeme postup $m_1 = mod(5^{27}, 55) = 25$.

Tento algoritmus využíva určitú asymetriu vo výpočtovej zložitosti problémov, ako je napríklad problém faktorizácie. Ak máme dve prvočísla p, q, tak vypočítať ich súčin $n = pq$ nepredstavuje pre naše počítače problém, ani keď na reprezentáciu týchto čísel potrebujeme stovky bitov. Na druhej strane, ako sme spomenuli, ak máme zadané veľmi veľké prirodzené číslo n, nájsť jeho rozklad v rozumnom čase je úloha, ktorá je zatiaľ nad sily našej výpočtovej techniky.

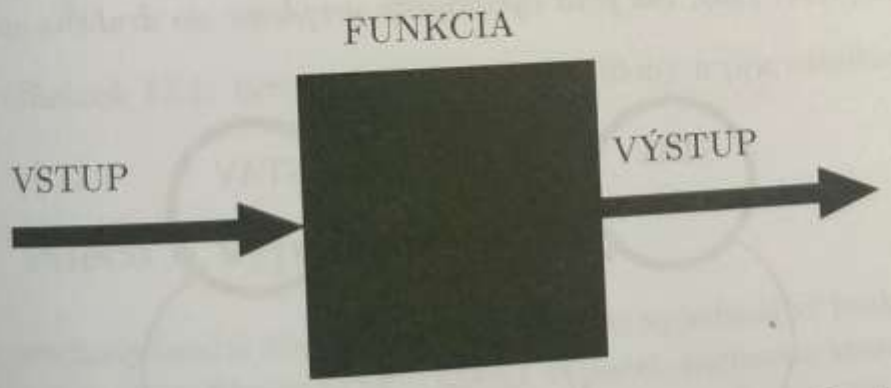
Ešte doplňme, že algoritmus RSA sa používa napríklad pri internet bankingu a elektronickom podpise. V praxi sa momentálne používajú čísla, ktoré majú veľkosť 512 bitov.

Ďalšie zaujímavosti o šifrovaní, dešifrovaní a úlohe matematiky v nich, možno nájsť napríklad v populárno-náučnej knihe [22].

Kapitola 13

Stavové automaty a Turingov stroj

V časti o funkciách sme sa zmienili aj o problematike výpočtu hodnoty funkcie. Doteraz sme hľadeli na funkcie, ako na „čierne skrinky", kde niečo prichádza na vstup a následne na výstupe dostávame funkčnú hodnotu.



Pokúsme sa nahliadnuť do vnútra tejto „čiernej skrinky". Predovšetkým si musíme uvedomiť, že výpočet hodnôt funkcie je postupnosť krokov, pri ktorej prechádzame z jedného stavu do iného. Pre daný vstup musí byť táto postupnosť krokov jednoznačne určená. Ukážeme si, ako možno formálne popísať, čo sa deje počas výpočtu. Na to využijeme pojem stavový automat

a tento pojem rozšírime na Turingov stroj.

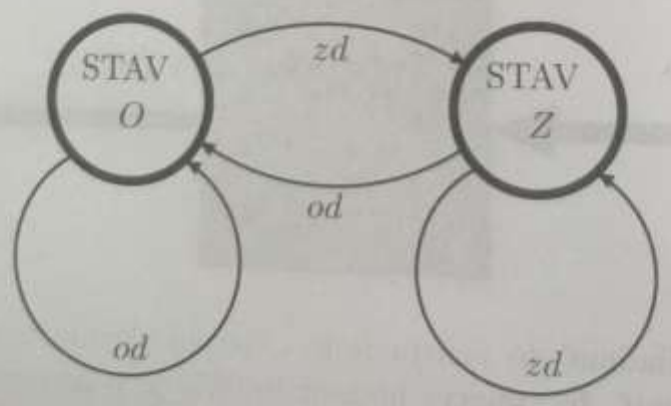
13.1 Abeceda

Konečnú množinu znakov nazveme abeceda. Konečné postupnosti prvkov tejto množiny (abecedy) nazveme slová. Napríklad množina $\{0, 1\}$ je dvojprvková abeceda a každú konečnú postupnosť núl a jednotiek nazveme slovo (napríklad 001101). Často abecedu dopĺňame znakom vyjadrujúcim prázdne miesto, budeme používať symbol _ .

13.2 Stavový automat

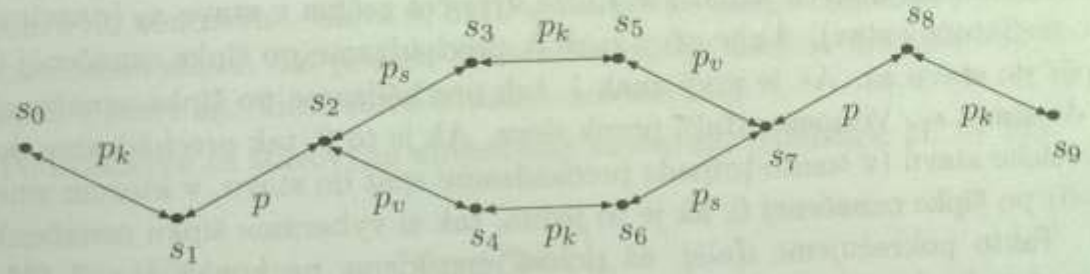
Stavový automat je model, ktorý sa využíva na popis správania sa systému s konečným počtom stavov. Začnime jednoduchými príkladmi.

Príklad 13.2.1. *Dvere môžu byť v dvoch stavoch. Otvorené (O), alebo zatvorené (Z). Ak pracujeme ako „ otvárač " dverí, reagujeme na dva príkazy: otvor dvere (od) a zatvor dvere (zd). Ak sú dvere otvorené (v stave O) a dostaneme príkaz (zd), tak jeho vykonaním prejdeme do druhého stavu (Z).*



Obrázok 13.1: Dvere ako príklad stavového automatu

Príklad 13.2.2. *Prievozník chce previezť na druhý breh rieky vlka, kozu a seno. Ako to má urobiť, ak môže previezť vždy len jedného pasažiera a na žiadnom z brehov nemôžu zostať bez dozoru koza s vlkom, alebo koza so senom. Riešenie úlohy určite nájde každý. Naším cieľom je popísať úlohu formálnejšie. Každý prípustný stav úlohy môžeme definovať zápisom, v ktorom je určené, kto bude na jednom brehu a kto na druhom. Celkovo máme desať prípustných stavov:* $s_0 = (p, k, v, s; \emptyset)$, $s_1 = (v, s; p, k)$, $s_2 = (p, v, s; k)$, $s_3 = (v; p, k, s)$, $s_4 = (s; p, k, v)$, $s_5 = (p, k, v; s)$, $s_6 = (p, k, s; v)$, $s_7 = (k; p, v, s)$, $s_8 = (p, k; v, s)$, $s_9 = (\emptyset; p, k, v, s)$. *Prechod medzi dvomi stavmi existuje práve vtedy, keď sa z jedného stavu do druhého dostaneme jedným prechodom cez rieku. Každý prechod je charakterizovaný „inštrukciou", ktorá hovorí, koho má prievozník previezť cez rieku. Tieto „inštrukcie" môžeme označiť* p, p_k, p_v, p_v, *kde index znamená, koho musí prievozník previezť. Celá situácia je znázornená na obrázku (13.2).*

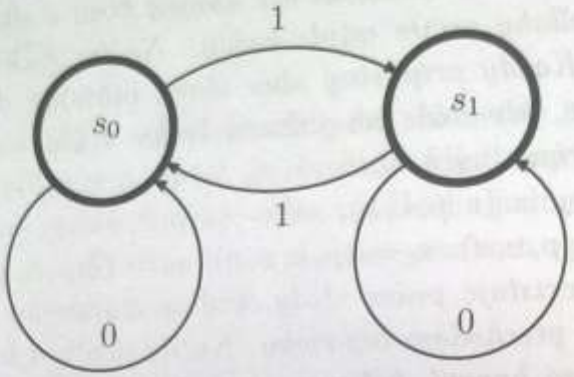


Obrázok 13.2: Grafická reprezentácia úlohy o prievozníkovi

13.3 Niečo o výpočtoch

Stavy a prechody medzi nimi môžu predstavovať aj jednotlivé kroky výpočtu nejakého programu. Skúsme takto opísať výpočet, pomocou ktorého možno zistiť, či dané slovo nad abecedou $\{0, 1\}$ obsahuje nepárny počet jednotiek. Výpočet prebieha tak, že prechádzame jednotlivé znaky slova a pri každej jednotke sa zmení parita. Počas výpočtu môžeme mať teda dva stavy: s_0, ak sme doteraz našli párny počet jednotiek a s_1, ak sme doteraz našli nepárny počet jednotiek. Ak je ďalší znak slova 0, tak zostávame v tom stave,

kde sme boli, ak je znak 1, mení sa parita počtu jednotiek a prechádzame do druhého stavu. Situácia je znázornená na obrázku 13.3. Na začiatku



Obrázok 13.3: Reprezentácia výpočtu pomocou stavového automatu

máme nula nájdených jednotiek, takže výpočet začína v stave s_0 (nazvime ho počiatočný stav). Ak je prvý znak 0, prechádzame po šípke označenej 0 opäť do stavu s_0. Ak je prvý znak 1, tak prechádzame po šípke označenej 1 do stavu s_1. Vezmeme ďalší prvok slova. Ak je to 0, tak prechádzame do ďalšieho stavu (v tomto prípade prechádzame späť do stavu, v ktorom sme boli) po šípke označenej 0, ak je to jedna, tak si vyberáme šípku označenú 1. Takto pokračujeme ďalej, až pokiaľ neprídeme na koniec slova. Ak výpočet skončil v stave s_1 (nazvime ho koncový stav), tak odpoveď je, že slovo obsahuje nepárny počet jednotiek.

13.4 Trochu teórie

Konečný stavový automat je teda zariadenie, ktoré je dané množinou stavov S, množinou prechodov medzi stavmi P (každý prechod je usporiadaná dvojica stavov), každému prechodu je priradený znak abecedy, pričom požadujeme, aby každé dva rôzne prechody začínajúce v tom istom stave mali priradené rôzne hodnoty. V prípade dvojprvkovej abecedy môžu z každého stavu vychádzať najviac dva prechody (na diagrame dve šípky). Jeden zo stavov môžeme označiť ako počiatočný a jeden (nie nutne rôzny od počia-

točného) ako koncový.

Zo slušnosti to sformulujme ako poriadnu definíciu:

Definícia 13.4.1. *Stavový automat nad abecedou A je usporiadaná trojica (S, P, f), kde $S \neq \emptyset$ je množina stavov, $P \subseteq S \times S$ je množina prechodov medzi stavmi a $f : P \to A$ je funkcia, pre ktorú platí:*

$$\forall (s_i, s_j), (s_i, s_l) \in P \quad f((s_i, s_j)) \neq f((s_i, s_l)) .$$

Ak existuje také slovo, vďaka ktorému prejdeme z počiatočného stavu do koncového, tak hovoríme, že automat **akceptuje** toto slovo. Inak hovoríme, že automat **neakceptuje** toto slovo.

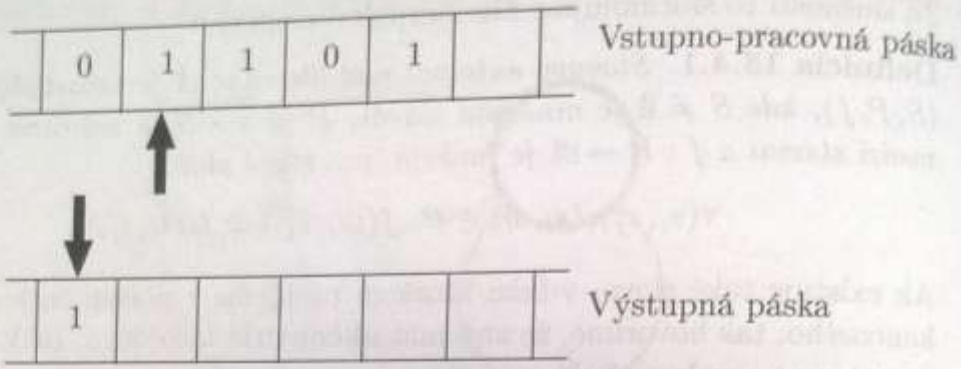
Vezmime posledný príklad. Stav s_0 je počiatočný a stav s_1 koncový. Tento automat akceptuje práve tie slová, ktoré obsahujú nepárny počet jednotiek. Napríklad 1, 0010, 0110100, ktoré nám opisujú prechod z počiatočného stavu do koncového. Slová 0, 0110 alebo 00110 nám neumožnili prechod do koncového stavu. Po použití posledného znaku daného slova sme sa ocitli opäť v stave s_0. Tieto slová automat neakceptuje.

Podrobnejšie sa stavovými automatmi zaoberajú publikácie [3, 13, 21].

13.5 Ešte raz o výpočtoch

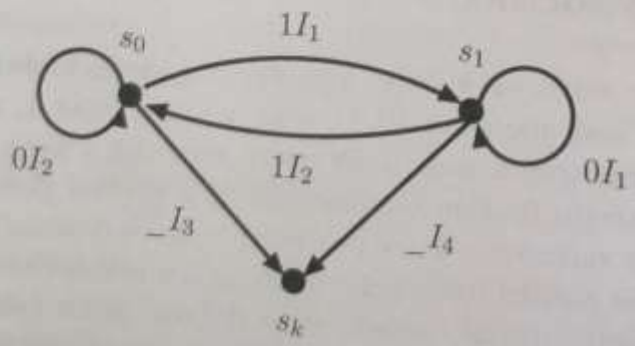
Vráťme sa k výpočtu parity jednotiek v slove. Výpočtu zodpovedá funkcia, ktorá má na vstupe slovo nad abecedou $\{0, 1\}$ a na výstupe znak 1, ak počet jednotiek v slove je nepárny a znak 0, ak počet jednotiek v slove je párny. Výpočet hodnôt takejto funkcie môžeme formálne popísať pomocou Turingovho stroja, čo je zariadenie, ktoré pozostáva z dvoch dostatočne dlhých pások rozdelených na políčka (teoreticky uvažujeme o nekonečne dlhých páskach). Pásky môžeme posúvať doprava alebo doľava. Jednu pásku budeme považovať za vstupno-pracovnú (na začiatku bude na nej zapísaný vstup, bude sa využívať na výpočet) a druhú za výstupnú (na konci výpočtu bude na nej výstup). Pri každej páske je hlava, ktorá slúži na čítanie znakov v jednotlivých políčkach a tiež zapisuje znaky do jednotlivých políčok vstupno-pracovnej pásky. Prázdne políčko reprezentujeme znakom _.

Turingov stroj je doplnený „programom“, ktorý možno reprezentovať veľmi



Obrázok 13.4: Pásky Turingovho stroja

podobne, ako stavový automat. Požadujeme však, aby z koncového stavu s_k žiadna šípka nevychádzala. Akonáhle dosiahneme tento stav, výpočet končí. Hodnoty priradené prechodom sú doplnené o inštrukcie, ktoré hovoria, na ktorú pásku zapisujeme, ktorý znak (vždy len do políčka, pri ktorom je hlava), ako sa pásky posúvajú (každá sa môže posunúť o jedno políčko doprava, doľava, alebo sa neposúva). Na obrázku (13.5) je „program“ k úlohe o parite jednotiek v slove. Vidíme, že je odvodený zo stavového automatu



$I_1 = (_, 1, L, _)$

$I_2 = (_, 0, L, _)$

$I_3 = (_, 0, _, _)$

$I_4 = (_, 1, _, _)$

Obrázok 13.5: „Program“ výpočtu Turingovho stroja

pre tú istú úlohu, ale sme tam doplnili ďalší stav, ktorý bude koncový. Začíname v stave s_0. Ak na vstupnej páske prečíta znak 1, vykoná inštrukciu

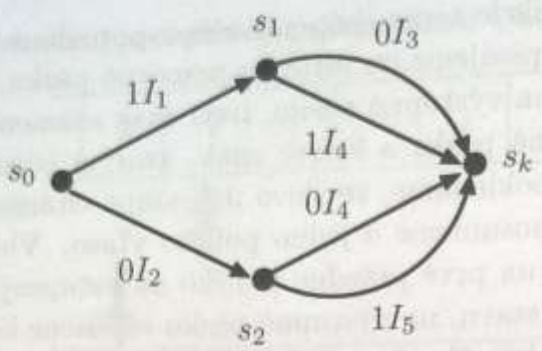
I_1 a prejde do stavu s_1. Inštrukcie teraz chápeme ako usporiadané štvorice, kde prvý znak určuje, čo zapisujeme na vstupno-pracovnú pásku, druhý znak znamená, čo zapisujeme na výstupnú pásku, tretí znak znamená, ktorým smerom sa posúva vstupná páska a štvrtý znak, ktorým smerom sa posúva výstupná páska. Predpokladáme, že slovo na vstupe čítame zľava, preto pásku v každom kroku posunieme o jedno políčko vľavo. Vieme, že výpočet skončí, keď narazíme na prvé prázdne políčko na vstupnej páske. Vtedy prejdeme do koncového stavu, na výstupnú pásku zapíšeme hodnotu 0 alebo 1 (závisí to od stavu, z ktorého do s_k prichádzame). Vstupnú pásku sme v poslednom kroku nepotrebovali posunúť, výstupná páska sa počas výpočtu neposúvala vôbec.

Ukážme ešte jeden príklad - súčet dvoch jednobitových čísel (v dvojkovej sústave). Výpočet zrealizujeme opäť pomocou Turingovho stroja s dvomi páskami. Inštrukcie budú tak, ako v predchádzajúcom príklade, usporiadané štvorice. Môžeme postupovať nasledujúco: na vstupnej páske sú zapísané obe čísla hneď za sebou. Teda dvojprvkovým slovám na vstupe potrebujeme priradiť nasledujúce slová na výstupnej páske:

$$00 \to 0,\ 01 \to 1,\ 10 \to 1,\ 11 \to 10\ .$$

Ak vstup začína 0, tak výstup bude 0 alebo 1 v závislosti od druhej hodnoty na vstupe. Ak vstup začína znakom 1, potom prvý znak výstupu bude 1 a druhý znak bude 0 alebo prázdne políčko, podľa druhej hodnoty vstupu. „Program" výpočtu aj s inštrukciami máme na obrázku (13.6). V počiatočnom stave sa teda rozhodujeme podľa prvého znaku na vstupe, vykonáme príslušné inštrukcie a prejdeme do stavu s_1 alebo s_2. V každom z týchto dvoch stavov sa rozhodujeme podľa druhého znaku na vstupe, akú inštrukciu vykonať a prechádzame do koncového stavu s_k. „Program" kvôli zjednodušeniu nie je ošetrený pre prípady nekorektne zadaných slov.

Tu treba povedať, že pôvodná verzia Turingovho stroja, navrhnutá Alanom Turingom, pozostáva len z jednej pásky a z hlavy schopnej čítať aj zapisovať na túto pásku, Na začiatku výpočtu je na páske zapísaný vstup, na konci je na nej zapísaný výstup. Dá sa dokázať, že to, čo sa dá vypočítať na dvojpáskovom stroji sa dá vypočítať aj na jednopáskovom a samozrejme



$I_1 = (_, 1, L, L)$
$I_2 = (_, 0, L, _)$
$I_3 = (_, _, _, _)$
$I_4 = (_, 0, _, _)$
$I_5 = (_, 1, _, _)$

Obrázok 13.6: „Program" Turingovho stroja na súčet čísel

naopak.

13.6 Význam Turingovho stroja

Môžeme si položiť otázku, na čo sú tieto úvahy dobré? Základnú myšlienku sme naznačili už v úvode tejto kapitoly. Chceme formálne opísať výpočet hodnôt funkcie. Na toto nám práve môže poslúžiť Turingov stroj. Vstup funkcie môžeme zapísať pomocou núl a jednotiek na vstupnú pásku. Výstup podobne môžeme zapísať na výstupnú pásku. Samotný priebeh výpočtu je charakterizovaný diagramom a postupnosťou stavov, ktoré prechádzame počas výpočtu. Turingov stroj v prvom príklade teda zodpovedá funkcii, ktorá každému slovu na vstupe priradí 1 alebo 0. V druhom príklade máme Turingov stroj, ktorý reprezentuje funkciu, ktorú môžeme formálne zapísať nasledovne: $f : \{0,1\}^2 \to \{0,1\}^2$, kde $f(00) = 0$, $f(01) = f(10) = 1$, $f(11) = 10$. Čiže spomenuté funkcie a ich výpočet môžeme reprezentovať pomocou uvedených Turingových strojov.

Ukazuje sa, že funkcia je vypočítateľná na počítači práve vtedy, keď existuje Turingov stroj, ktorý reprezentuje výpočet hodnôt danej funkcie pre ľubovoľný vstup z jej definičného oboru.

Existujú mnohé výpočtové modely, pomocou ktorých možno charakterizovať funkcie vypočítateľné na počítači. Turingov stroj je však zrejme prvý takýto

model. Bol navrhnutý anglickým matematikom Alanom Turingom (1912 - 1954) v jeho článku publikovanom v roku 1937, teda v dobe, keď ešte žiadne počítače neexistovali. Dnes vieme, že práve Turingove myšlienky stáli pri zrode moderných počítačov a informatiky. Viac o tejto problematike možno nájsť v [13, 21]. Život Alana Turinga približuje kniha [10].