

# **Algebra a diskrétna matematika**



---

VLADIMÍR KVASNIČKA  
JIŘÍ POSPÍCHAL

---

# **Algebra a diskrétna matematika**

Slovenská technická univerzita  
v Bratislave  
2008

© prof. Ing. Vladimír Kvasnička, DrSc., prof. RNDr. Jiří Pospíchal, DrSc.

Lektori: doc. RNDr. Ladislav Satko, CSc.  
doc. RNDr. Michal Šabo, CSc.

Publikáciu podporilo združenie Gratex IT Inštitút

Vydala Slovenská technická univerzita v Bratislave  
vo Vydavateľstve STU, Bratislava, Vazovova 5.

Schválilo vedenie Fakulty informatiky a informačných technológií STU v Bratislave  
dňa 25.4.2006, uznesenie číslo 12.1.2006/kd, pre študijný program Informatika a študijný program Počítačové  
systémy a siete

# OBSAH

<b>PREDHOVOR.....</b>	<b>ix</b>
<b>1 METÓDY MATEMATICKÉHO DŔKAZU .....</b>	<b>1</b>
1.1 VÝZNAM DŔKAZU V MATEMATIKE .....	1
1.2 PRAVIDLÁ USUDZOVANIA VO VÝROKOVEJ LOGIKE .....	4
1.3 PRAVIDLÁ USUDZOVANIA V PREDIKÁTOVEJ LOGIKE.....	11
1.4 METÓDY DŔKAZU VIET.....	15
1.5 MATEMATICKÁ INDUKCIA .....	19
ZHRNUTIE.....	22
KLÚČOVÉ POJMY .....	23
CVIČENIA .....	24
<b>2 TEÓRIA MNOŽÍN I.....</b>	<b>29</b>
2.1 DEFINÍCIA MNOŽINY .....	29
2.2 ENUMERÁCIA ELEMENTOV V KONEČNÝCH MNOŽINÁCH .....	37
2.3 KARTEZIÁNSKY SÚČIN MNOŽÍN .....	42
2.4 MNOŽINA AKO DÁTOVÁ ŠTRUKTÚRA V INFORMATIKE.....	46
ZHRNUTIE.....	47
KLÚČOVÉ POJMY .....	48
CVIČENIA .....	49
<b>3 TEÓRIA MNOŽÍN II.....</b>	<b>53</b>
3.1 RELÁCIE .....	53
3.2 RELÁCIA ČIASTOČNÉHO USPORIADANIA.....	62
3.3 FUNKCIE.....	66
ZHRNUTIE.....	72
KLÚČOVÉ POJMY .....	73
CVIČENIA .....	73
<b>4 KOMBINATORIKA I .....</b>	<b>79</b>
4.1 BINOMICKÉ KOEFICIENTY A PASCALOV TROJUHOLNÍK.....	79
4.2 PERMUTÁCIE A KOMBINÁCIE .....	88
ZHRNUTIE.....	94
KLÚČOVÉ POJMY .....	95
CVIČENIA .....	95
<b>5 KOMBINATORIKA II.....</b>	<b>99</b>
5.1 REKURENTNÉ VZŤAHY.....	99
5.2 METÓDA „ROZDELUJ A PANUJ“ .....	108

5.3	PRINCÍP INKLÚZIE A EXKLÚZIE .....	113
	ZHRNUTIE .....	118
	KLÚČOVÉ POJMY .....	119
	CVIČENIA .....	120
<b>6</b>	<b>ALGEBRAICKÉ ŠTRUKTÚRY I.....</b>	<b>123</b>
6.1	BINÁRNE OPERÁCIE .....	123
6.2	POLOGRUPY, MONOIDY A GRUPY .....	126
6.3	MORFIZMY .....	135
	ZHRNUTIE.....	138
	KLÚČOVÉ POJMY .....	139
	CVIČENIA .....	140
<b>7</b>	<b>ALGEBRAICKÉ ŠTRUKTÚRY II .....</b>	<b>143</b>
7.1	BOOLOVA ALGEBRA .....	143
7.2	VLASTNOSTI BOOLOVEJ ALGEBRY.....	146
7.3	BOOLOVE FUNKCIE.....	148
7.4	SPÍNACIE OBVODY .....	155
7.5	LOGICKÉ OBVODY .....	159
7.6	OPTIMALIZÁCIA LOGICKÝCH OBVODOV .....	163
	ZHRNUTIE.....	171
	KLÚČOVÉ POJMY .....	173
	CVIČENIA .....	173
<b>8</b>	<b>MATICOVÁ ALGEBRA I .....</b>	<b>177</b>
8.1	DEFINÍCIA MATICE .....	177
8.2	OPERÁCIE NAD MATICAMI .....	181
8.3	HODNOSŤ MATICE .....	189
8.4	INVERZNÁ MATICA .....	194
	ZHRNUTIE.....	197
	KLÚČOVÉ POJMY .....	198
	CVIČENIA .....	199
<b>9</b>	<b>MATICOVÁ ALGEBRA II.....</b>	<b>205</b>
9.1	SÚSTAVA LINEÁRNYCH ROVNÍC.....	205
9.2	DETERMINANTY .....	214
	ZHRNUTIE.....	223
	KLÚČOVÉ POJMY .....	224
	CVIČENIA .....	224
<b>10</b>	<b>TEÓRIA GRAFOV I.....</b>	<b>227</b>
10.1	ÚVODNÉ POZNÁMKY .....	227
10.2	NEKTORÉ ZÁKLADNÉ DEFINÍCIE.....	230
10.3	REPREZENTÁCIA GRAFOV A IZOMORFIZMUS .....	234
10.4	SÚVISLOSŤ V NEORIENTOVANÝCH GRAFOCH A EULEROVSKÉ ŤAHY .....	237
10.5	HAMILTONOVSKÉ CESTY A KRUŽNICE .....	244
	ZHRNUTIE.....	249
	KLÚČOVÉ POJMY .....	249

CVIČENIA .....	250
<b>11 TEÓRIA GRAFOV II.....</b>	<b>257</b>
11.1 PROBLÉMY NAJKRATŠEJ CESTY .....	257
11.2 PLANÁRNE GRAFY .....	260
11.3 FARBENIE GRAFOV .....	264
ZHRNUTIE.....	271
KLÚČOVÉ POJMY .....	271
CVIČENIA .....	272
<b>12 TEÓRIA GRAFOV III.....</b>	<b>277</b>
12.1 STROMY AKO MODELY A ICH ZÁKLADNÉ VLASTNOSTI .....	277
12.2 BINÁRNE PREHLADÁVACIE STROMY .....	282
12.3 ROZHODOVACIE STROMY .....	283
12.4 PREFIXOVÉ KÓDOVANIE .....	285
12.5 KOREŇOVÉ STROMY REPREZENTUJÚCE ALGEBRAICKÉ VÝRAZY .....	287
12.6 KOREŇOVÝ STROM AKO MODEL HRY.....	288
ZHRNUTIE.....	295
KLÚČOVÉ POJMY .....	296
CVIČENIA .....	296
<b>13 TEÓRIA GRAFOV IV.....</b>	<b>301</b>
13.1 SIETE A METÓDA KRITICKEJ CESTY .....	301
13.2 MAXIMÁLNY TOK V SIETI A MINIMÁLNY REZ .....	305
13.3 NÁJDENIE NAJMEŇŠEJ KOSTRY .....	308
13.4 PREHLADÁVANIE DO HLĚBKY (DEPTH-FIRST SEARCH, DFS).....	310
13.5 PREHLADÁVANIE DO ŠÍRKY (BREADTH-FIRST SEARCH, BFS) .....	319
ZHRNUTIE.....	322
KLÚČOVÉ POJMY .....	323
CVIČENIA .....	323
<b>PRÍLOHA A – RIEŠENÉ PRÍKLADY .....</b>	<b>329</b>
RIEŠENÉ CVIČENIA Z KAPITOLY 1.....	331
RIEŠENÉ CVIČENIA Z KAPITOLY 2.....	347
RIEŠENÉ CVIČENIA Z KAPITOLY 3.....	355
RIEŠENÉ CVIČENIA Z KAPITOLY 4.....	367
RIEŠENÉ CVIČENIA Z KAPITOLY 5.....	375
RIEŠENÉ CVIČENIA Z KAPITOLY 6.....	383
RIEŠENÉ CVIČENIA Z KAPITOLY 7.....	391
RIEŠENÉ CVIČENIA Z KAPITOLY 8.....	401
RIEŠENÉ CVIČENIA Z KAPITOLY 9.....	411
RIEŠENÉ CVIČENIA Z KAPITOLY 10.....	417
RIEŠENÉ CVIČENIA Z KAPITOLY 11.....	433
RIEŠENÉ CVIČENIA Z KAPITOLY 12.....	443
RIEŠENÉ CVIČENIA Z KAPITOLY 13.....	451

<b>PRÍLOHA B – VZOROVÉ PÍSOMKY .....</b>	<b>463</b>
1. KONTROLNÁ PÍSOMKA.....	465
2. KONTROLNÁ PÍSOMKA.....	467
3. KONTROLNÁ PÍSOMKA.....	470
ZÁVEREČNÁ PÍSOMKA .....	473
<b>LITERATÚRA .....</b>	<b>479</b>
<b>REGISTER .....</b>	<b>481</b>



# PREDHovor

Cieľom tejto učebnice je poskytnúť študentom informatiky na Fakulte informatiky a informačných technológií STU ucelený text k prednáške „*Algebra a diskretná matematika*“. Diskretná matematika patrí medzi teoretické základy informatiky. Slúži nielen pre rozvoj matematicko-logických schopností študentov, ale aj ako teoretická príprava pre ďalšie „pokročilejšie“ informatické predmety. Pri koncipovaní obsahu tejto prednášky stáli sme pred neľahkou úlohou, čo zahrnúť do jej obsahu a čo nie. Pretože táto prednáška substituuje čiastočne aj bývalý predmet „*Lineárna algebra*“, zahrnuli sme z tejto oblasti do učebnice v rozsahu dvoch prednášok aj základy lineárnej algebry, teórie matíc a sústav lineárnych rovníc spolu s elementárnou teóriou determinantov.

Učebnica je určená pre študentov prvého ročníka bakalárskeho štúdia, ktorí majú základné stredoškolské vedomosti z teórie množín, algebry a výrokovej logiky. V prednáške sme sa snažili čo najviac vyjsť v ústrety potrebám informatiky, preto aj oproti časti týkajúcej sa algebry je relatívne uprednostnená diskretná matematika. Cieľom učebnice je aj rozvinúť u študentov schopnosť rigorózneho matematického myslenia pri riešení a formulovaní problémov informatiky.

Prvá kapitola sa týka metód matematického dôkazu. Kapitoly 2 až 5 sú venované teórii množín a kombinatorike, v 6. a 7. kapitole sa venujeme grupám a boolovskej algebry. Kapitoly 8 až 9 sú venované maticiam, sústavám lineárnych rovníc a determinantom. Zvyšok učebnice sa v 10. až 13. kapitole venuje teórii grafov a základným algoritmom a aplikáciám teórie grafov.

Každá kapitola je sprevádzaná príkladmi, ktorých riešenie poskytne študentom schopnosť dobre sa orientovať v danej problematike. Chceme poďakovať mnohým našim študentom, ktorí nám pomohli nájsť veľa nepríjemných preklepov, nepresností a evidentných chýb, a tým prispeli k zvýšeniu kvality tejto učebnice. Taktiež sa musíme poďakovať nášmu zosnulému kolegovi prof. Ing. Norbertovi Frištackému, PhD., s ktorým sme sa často radili pri koncipovaní sylabu prednášky. Na jeho radu sme zaradili do prednášky Quinovu a McCluskeyho metódu optimalizácie Boolovej funkcie špecifikujúcej logický obvod. Až pri prednášaní tohto predmetu sme zistili, že táto „aplikačná“ časť diskkrétnej matematiky patrí medzi študentmi k najobľúbenejšej časti predmetu.

V slovenskej a českej odbornej spisbe existuje mnoho učebných textov diskkrétnej matematiky. Veríme, že aj tento text sa dôstojne zaradí medzi ne, ako moderná učebnica, ktorej vzorom pri jej písaní bola známa a ťažko prekonateľná Rosenova učebnica „*Discrete Mathematics and Its Applications*“ [14].

Na záver sa chceme poďakovať oponentom doc. RNDr. Ladislavovi Satkovi, PhD. (FEI STU) a doc. RNDr. Michalovi Šabovi, CSc. (FCHPT STU) za cenné pripomienky, ktorými prispeli k vylepšeniu tohto učebného textu.

V Bratislave, júl 2008

Vladimír Kvasnička a Jiří Pospíchal

# 1 METÓDY MATEMATICKÉHO DÔKAZU

DEDUKTÍVNY DÔKAZ • ZÁKLADNÉ PRAVIDLÁ USUDZOVANIA •  
MATEMATICKÁ INDUKCIA

*V tejto kapitole budeme študovať dva dôležité problémy: (1) Za akých podmienok je matematický dôkaz korektný a (2) aké metódy môžu byť použité pri konštrukcii matematických dôkazov. Metódy dôkazu diskutované v tejto kapitole sú dôležité nielen pre tvorbu korektných dôkazov v matematike, ale aj v samotnej informatike. V teoretickej informatike sa napr. študujú rôzne metódy verifikácie korektnosti programu, alebo či operačný systém je bezpečný. V umelej inteligencii pri odvodzovaní nových faktov z danej databázy poznatkov (množiny výrokových formúl, ktorá sa vo výrokovej logike nazýva teória) je dôležité mať zabezpečené, aby daná databáza bola konzistentná (korektná), teda aby z nej súčasne nevyplýval nejaký výrok a taktiež aj jeho negácia. Môžeme teda konštatovať, že zvládnutie metód matematického dôkazu je dôležité nielen v matematike, ale aj v informatike.*

## 1.1 VÝZNAM DÔKAZU V MATEMATIKE

---

V matematike, podobne ako aj v informatike, vystupujú do popredia dve otázky: (1) Za akých podmienok je matematický dôkaz korektný a (2) aké metódy môžu byť použité pri konštrukcii matematických dôkazov. V tejto kapitole budeme hľadať odpovede na tieto dve otázky, budeme špecifikovať rôzne formy matematických dôkazov.

VETA

*Veta* (teoréma, výrok, skutočnosť, fakt, argument, alebo výsledok) je výrok, o ktorom môže byť dokázané, že je pravdivý. V tejto súvislosti hovoríme o *dôkaze* vety, ktorý spočíva v postupnosti jednotlivých „medzikrokov“, ktoré sú odvodené buď z množiny jednoduchých postulátov, nazývaných *axiómy*, alebo z predchádzajúcich viet (pomocných viet, často nazývaných *lemy*) danej postupnosti. Komplikované dôkazy sú obvykle jasnejšie formulované, keď ich dôkaz je rozdelený na jednotlivé medzikroky, ktoré sú formulované ako samostatné vety. Tieto medzikroky – vety v postupnosti sú vytvárané pomocou *pravidiel*

*odvodzovania (pravidiel usudzovania)*, ktoré z niekoľkých pravdivých tvrdení – argumentov vytvorí nové pravdivé tvrdenie – argument.

#### KOREKTNOSŤ V INFORMATIKE

Metódy dôkazu diskutované v tejto kapitole sú dôležité nielen pre tvorbu korektných dôkazov matematických viet v matematike, ale aj v samotnej informatike. V teoretickej informatike sa napr. študujú rôzne metódy verifikácie korektnosti programu, alebo či operačný systém je bezpečný. V umelej inteligencii pri odvodzovaní nových faktov z danej databázy poznatkov (množiny výrokových forml, ktorá sa vo výrokovej logike nazýva teória) je dôležité mať zabezpečené, aby daná databáza bola konzistentná (korektná), teda aby z nej súčasne nevyplýval nejaký výrok a taktiež aj jeho negácia. Môžeme teda konštatovať, že zvládnutie metód matematického dôkazu je dôležité nielen v matematike, ale aj v informatike.

#### DEDUKTÍVNY DÔKAZ

Nižšie uvedená forma dôkazu sa nazýva *deduktívny dôkaz*, ktorý obsahuje:

- *systém elementárnych pojmov*, ktoré sú používané pri formulácii základných zložiek deduktívneho dôkazu,
- *systém axióm* (základné elementárne poznatky, ktoré sú pokladané za evidentné),
- *pravidlá odvodzovania* (pomocou ktorých sa uskutočňuje dôkaz),
- *vety* (deduktívne poznatky – argumenty), ktoré boli odvodené z axióm pomocou pravidiel odvodzovania a ktoré podstatne zjednodušujú a skracujú dôkazy ďalších nových deduktívnych poznatkov.

#### INDUKTÍVNE USUDZOVANIE

Poznamenajme, že tak v matematike, ako aj v informatike, sa v ojedinelých prípadoch používa aj *induktívne usudzovanie* (dôkaz), ktoré je založené na pozorovaní určitých skutočností, ktoré sa často opakujú v analogických situáciách. Tieto pozorované skutočnosti sú „induktívne“ zovšeobecnené. Nové pojmy, ktoré boli zavedené týmto „induktívnym“ spôsobom sa neskôršie buď dokážu deduktívne v rámci daného systému pojmov, alebo sa postulujú ako nové špeciálne axiómy. Tieto ojedinelé situácie v dejinách matematiky vždy znamenali vznik nových oblastí matematiky, ktoré nie sú striktne deduktívne dokázateľné zo známych pojmov a reprezentujú akty kreativity v matematike, ktoré taktiež znamenajú, že matematika nie je len veda deduktívneho charakteru, kde sa dá každý pojem odvodiť z iných jednoduchších poznatkov<sup>1</sup>.

## Ilustratívny príklad axiomatického systému

Uvažujme jednoduchý axiomatický systém, ktorý obsahuje tri *elementárne pojmy* – ‘vrchol’, ‘hrana’, ‘ležať na’ a tri *axiómy*

A<sub>1</sub>. Každý vrchol leží aspoň na jednej hrane.

A<sub>2</sub>. Pre každú hranu existujú práve dva vrcholy, ktoré na nej ležia.

<sup>1</sup> To že matematika nie je veda čisto deduktívna má aj iné hlboké dôvody.

$A_3$ . Máme práve 5 vrcholov.

Tento axiomatický systém môže mať rôzne interpretácie. Interpretácia, v ktorej sú axiómy pravdivé výroky, sa nazýva *model* axiomatického systému. Už použitá terminológia navodzuje zavedenie modelu *grafu*<sup>2</sup>, kde vrchol je bod a hrana je čiara obsahujúca na svojich koncoch dva vrcholy, pozri obr. 1.1. Dokážeme tieto dve vety, ktoré vyplývajú z axiomatického systému.

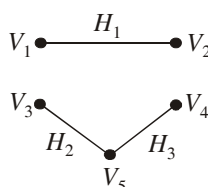
**VETA 1.1.** Každý graf má aspoň tri hrany.

Podľa axiómy  $A_1$  každý vrchol leží aspoň na jednej hrane, čiže pre ľubovoľný vrchol  $V_1$  existuje taká hrana  $H_1$ , na ktorej daný vrchol leží. Týmto máme zabezpečenú existenciu hrany  $H_1$ , ktorá podľa axiómy  $A_2$  leží na dvoch vrcholoch, tento druhý vrchol označíme  $V_2$ . Pre zostávajúce tri vrcholy  $V_3$ ,  $V_4$  a  $V_5$  musia existovať aspoň dve hrany  $H_2$  a  $H_3$ , ktoré ležia na týchto troch vrcholoch.

**VETA 1.2.** Každý graf má jeden vrchol, ktorý leží aspoň na dvoch hranách.

Dôkaz tejto vety priamo vyplýva zo spôsobu dôkazu vety 1.1. Pretože v druhej časti grafu máme tri vrcholy a dve hrany, musí existovať aspoň jeden vrchol, ktorý leží aspoň na dvoch hranách, čo bolo potrebné dokázať (QED). Model, ktorý ilustruje tieto dve vety je znázornený na obr. 1.1.

**OBRÁZOK 1.1.**  
GRAFOVÝ MODEL



Grafový model jednoduchého axiomatického systému z vety 1.1. Diagram znázorňuje model, ktorý obsahuje 3 hrany, pričom práve jeden vrchol leží na dvoch hranách.

Z našich predchádzajúcich výsledkov vyplýva, že môžeme deduktívny systém rozšíriť o nový elementárny pojem „komponent“, ktorý popisuje takú časť grafu, z ktorej vrcholy nie sú spojené cestou pozostávajúcou z postupnosti hrán s vrcholmi z ostatných častí, ale vždy existuje cesta medzi ľubovoľnou dvojicou vrcholov komponentu. Z obr. 1.1 vyplýva jednoduchá veta.

**VETA 1.3.** Ak má graf dva komponenty, potom jeden z komponentov obsahuje len jednu hranu.

Z definície komponentu vyplýva, že množina vrcholov je separovaná na dve disjunktné podmnožiny vrcholov, ktoré nie sú prepojené spoločnou hranou a pre každú hranu existujú práve dva vrcholy, ktoré na nej ležia. Z týchto dvoch skutočností vyplýva, že toto disjunktné rozdelenie množiny vrcholov je možné len na dve podmnožiny, ktoré obsahujú dva a tri vrcholy. Podmnožina s dvoma vrcholmi reprezentuje komponent.

<sup>2</sup> Pojem grafu bude podrobne študovaný v kapitolách 10 až 13.

## 1.2 PRAVIDLÁ USUDZOVANIA VO VÝROKOVEJ LOGIKE

Pravidlá usudzovania vo výrokovej logike tvoria schému

$$\frac{\begin{array}{l} \text{predpoklad}_1 \\ \dots\dots\dots \\ \text{predpoklad}_n \end{array}}{\text{záver}} \quad (1.1)$$

ktorá obsahuje  $n$  predpokladov a jeden záver. Táto schéma usudzovania je totožná so symbolom *logického dôkazu*

$$\{\text{predpoklad}_1, \dots, \text{predpoklad}_n\} \vdash \text{záver} \quad (1.2a)$$

alebo formálne

$$\{\varphi_1, \dots, \varphi_n\} \vdash \varphi \quad (1.2b)$$

Táto formula logického dôkazu môže byť prepísaná do formuly

$$\vdash \varphi_1 \wedge \dots \wedge \varphi_n \Rightarrow \varphi \quad (1.3a)$$

alebo v ekvivalentnom tvare, kde konjunkcie sú nahradené implikáciami

$$\vdash \varphi_1 \Rightarrow (\varphi_2 \Rightarrow (\dots (\varphi_n \Rightarrow \varphi))) \quad (1.3b)$$

**Tabuľka 1.1. Schémy usudzovania výrokovej logiky**



Schéma usudzovania	Teoréma výrokovej logiky	Názov schémy
$\frac{p}{p \vee q}$	$p \Rightarrow (p \vee q)$	adícia
$\frac{p \wedge q}{p}$	$(p \wedge q) \Rightarrow p$	simplifikácia (zjednodušenie)
$\frac{p}{q} \quad \frac{q}{p \wedge q}$	$p \Rightarrow (q \Rightarrow (p \wedge q))$	konjunkcia
$\frac{p}{p \Rightarrow q} \quad q$	$p \Rightarrow ((p \Rightarrow q) \Rightarrow q)$	modus ponens
$\frac{\neg q}{p \Rightarrow q} \quad \neg p$	$\neg q \Rightarrow ((p \Rightarrow q) \Rightarrow \neg p)$	modus tollens
$\frac{p \Rightarrow q}{q \Rightarrow r} \quad p \Rightarrow r$	$(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$	hypotetický sylogizmus

$\frac{\begin{array}{l} p \vee q \\ \neg p \\ \hline q \end{array}}{(p \vee q) \Rightarrow (\neg p \Rightarrow q)}$	disjunktívny sylogizmus
$\frac{\begin{array}{l} p \Rightarrow q \\ \neg q \Rightarrow \neg p \\ \hline \end{array}}{(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)}$	inverzia implikácie
$\frac{\begin{array}{l} p \Rightarrow q \\ p \Rightarrow \neg q \\ \hline \neg p \end{array}}{(p \Rightarrow q) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \neg p)}$	reductio ad absurdum

KONZISTENTNÉ  
PREDPOKLADY =  
 $\exists$  INTERPRETÁCIA,  
KEDY SÚ PRAVDIVÉ

Tab. 1.1 obsahuje 9 obvyklých schém usudzovania výrokovej logiky, pričom každá schéma je sprevádzaná aj zákonom (tautológiou) výrokovej logiky (v tvare formuly (1.3b)) a obvyklým historickým názvom. Hovoríme, že predpoklady sú *konzistentné* vtedy a len vtedy, ak existuje aspoň jedna interpretácia<sup>3</sup> pravdivostných hodnôt výrokových premenných, pre ktorú sú všetky predpoklady pravdivé. V opačnom prípade je množina predpokladov *nekonzistentná* (*kontradiktórna*) a je charakterizovaná tým, že z nej súčasne logicky vyplýva nejaký záver a aj jeho negácia.

**PRÍKLAD 1.1.**

Majme dva predpoklady: prvý predpoklad je výrok 'prší' a druhý predpoklad je implikácia 'ak prší, potom je cesta mokrá'. Použitím pravidla usudzovania modus ponens, z pravdivosti týchto dvoch predpokladov vyplýva pravdivý záver 'cesta je mokrá', čo môžeme formálne vyjadriť pomocou schémy

$$\frac{\begin{array}{l} \text{prší} \\ \text{ak prší, potom cesta je mokrá} \\ \hline \text{cesta je mokrá} \end{array}}$$

**PRÍKLAD 1.2.**

Použitím schémy usudzovania adície k pravdivému výroku 'teplota je pod bodom mrazu' môžeme pomocou disjunkcie priradiť ľubovoľný výrok (pravdivý alebo nepravdivý), napr. 'prší', dostaneme pravdivý záver 'teplota je pod bodom mrazu alebo prší'

$$\frac{\begin{array}{l} \text{teplota je pod bodom mrazu} \\ \hline \text{teplota je pod bodom mrazu alebo prší} \end{array}}$$

**PRÍKLAD 1.3.**

Uvažujme dva výroky 'ak dnes bude pršať, potom sa nepôjdem kúpať' a 'ak sa nepôjdem kúpať, potom navštívim príbuzného'. Použitím schémy usudzovania nazvanej hypotetický sylogizmus dostaneme z týchto dvoch predpokladov záver 'ak dnes bude pršať, potom navštívim príbuzného'

$$\frac{\begin{array}{l} \text{ak dnes bude pršať, potom sa nepôjdem kúpať} \\ \text{ak sa nepôjdem kúpať, potom navštívim príbuzného} \\ \hline \text{ak dnes bude pršať, potom navštívim príbuzného} \end{array}}$$

<sup>3</sup> Nech  $p, q, \dots, r$  sú atomické výrokové premenné, potom *interpretácia* (vzhľadom k týmto premenným) je označená symbolom  $\tau = (p/1, q/0, \dots, r/1)$ . Špecifikuje pravdivostné hodnoty jednotlivých premenných; v tomto konkrétnom prípade premenná  $p$  je pravdivá, premenná  $q$  je nepravdivá, ... a premenná  $r$  pravdivá. Ak máme  $n$  premenných, potom existuje  $2^n$  rôznych interpretácií. (Pozri kapitolu 1.4 v našej knihe Matematická logika [11].)

Túto schému môžeme sformalizovať pomocou výrokov

$$\begin{aligned} p &= \text{'dnes prší'} \\ q &= \text{'kúpem sa'} \\ r &= \text{'navštívim príbuzného'} \end{aligned}$$

potom schéma má tento formálny tvar mierne modifikovaného hypotetického sylogizmu

$$\frac{\begin{array}{l} p \Rightarrow \neg q \\ \neg q \Rightarrow r \end{array}}{p \Rightarrow r}$$

ktorá je odvodená z pôvodnej schémy hypotetického sylogizmu substitúciou, kde výroková premenná  $q$  je substituovaná negáciou  $\neg q$ .

V poslednom príklade 1.3 boli už použité výrokové premenné, ktoré nám umožnia vykonať formalizáciu celého procesu dôkazu pomocou postupnosti elementárnych krokov. Obrátíme našu pozornosť na formulu (1.2b) logického vyplývania výrokovej formuly  $\varphi$  z predpokladov, ktoré sú reprezentované formulami  $\varphi_1, \varphi_2, \dots, \varphi_n$ . Logické vyplývanie ilustrujeme jednoduchým príkladom.

#### PRÍKLAD 1.4.

Postulujeme, že množina predpokladov obsahuje tieto formuly – zložené výroky:

$$\begin{aligned} \varphi_1 &= \text{'dnes poobede nie je slnečno a je chladnejšie ako včera'} \\ \varphi_2 &= \text{'pôjdeme sa kúpať len vtedy, ak bude slnečno'} \\ \varphi_3 &= \text{'ak sa nepôjdeme kúpať, potom sa budeme člnkovať na rieke'} \\ \varphi_4 &= \text{'ak sa budeme člnkovať na rieke, potom sa vrátíme domov podvečer'} \end{aligned}$$

požadovaný záver má tvar

$$\varphi = \text{'budem doma podvečer'}$$

Pomocou výrokových premenných

$$\begin{aligned} p &= \text{'dnes poobede je slnečno'} \\ q &= \text{'je chladnejšie ako včera'} \\ r &= \text{'pôjdeme sa kúpať'} \\ s &= \text{'budeme člnkovať na rieke'} \\ t &= \text{'vrátíme sa domov podvečer'} \end{aligned}$$

vykonáme formalizáciu schémy logického vyplývania do tvaru

$$\{\neg p \wedge q, (r \Rightarrow p) \wedge (p \Rightarrow r), \neg r \Rightarrow s, s \Rightarrow t\} \vdash t$$

Ukážeme, že táto schéma je platná pomocou postupnosti elementárnych krokov, kde budeme používať schémy usudzovania z tab. 1.1.

1.	$\neg p \wedge q$	predpoklad <sub>1</sub>
2.	$(r \Rightarrow p) \wedge (p \Rightarrow r)$	predpoklad <sub>2</sub>
3.	$\neg r \Rightarrow s$	predpoklad <sub>3</sub>
4.	$s \Rightarrow t$	predpoklad <sub>4</sub>
5.	$\neg p$	simplifikácia predpokladu <sub>1</sub>
6.	$q$	simplifikácia predpokladu <sub>1</sub>
7.	$r \Rightarrow p$	simplifikácia predpokladu <sub>2</sub>



- 8.  $\neg r$       medzivýsledok 5 a modus tollens na predpoklad<sub>2</sub>
- 9.  $s$         medzivýsledok 8 a modus ponens na predpoklad<sub>3</sub>
- 10.  $t$         medzivýsledok 9 a modus ponens na predpoklad<sub>4</sub>

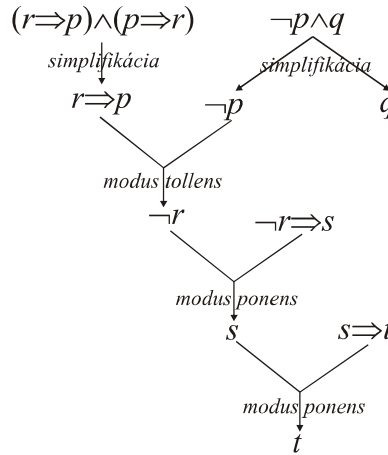
DŔKAZ AKO  
POSTUPNŔ  
FORMŔL

V Ŕvodnej časti kapitoly 1.1 bolo poznamenané, že dôkaz je možné charakterizovať ako postupnosť formŔl, kde posledná formula sa rovná požadovanému záveru, môžeme teda písať

$$(\neg p \wedge q) \rightarrow (r \Rightarrow p) \rightarrow (\neg r \Rightarrow s) \rightarrow (s \Rightarrow t) \rightarrow (\neg p) \rightarrow (q) \rightarrow (\neg r) \rightarrow (s) \rightarrow (t)$$

TŔto postupnosť formŔl môžeme reprezentovať aj pomocou „stromu dôkazu“ znázorneného na obr. 1.2.

**OBRÁZOK 1.2.**  
STROM  
ODVODENIA PRE  
PRÍKLAD 1.4.



Strom odvodenia pre logický dôkaz z príkladu 1.4.

**PRÍKLAD 1.5.**

Nech množina predpokladov obsahuje tieto zložené výroky:

- $\varphi_1 = \text{'ak mi pošleš email, potom program dokončím'}$
- $\varphi_2 = \text{'ak mi nepošleš email, potom pôjdem spať skôr'}$
- $\varphi_3 = \text{'ak pôjdem spať skôr, potom sa ráno zobudím odpočínutý'}$

požadovaný záver má tvar

$$\varphi = \text{'ak nedokončím program, potom sa ráno zobudím odpočínutý'}$$

Pomocou výrokových premenných

- $p = \text{'pošleš mi email'}$
- $q = \text{'program dokončím'}$
- $r = \text{'pôjdem spať skôr'}$
- $s = \text{'ráno sa zobudím odpočínutý'}$

vykonáme formalizáciu schémy logického vyplývania do tvaru

$$\{p \Rightarrow q, \neg p \Rightarrow r, r \Rightarrow s\} \vdash \neg q \Rightarrow s$$

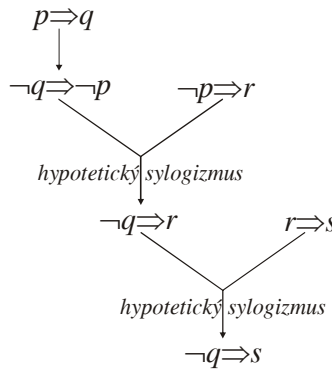
Pomocou postupnosti elementárnych krokov, kde budeme používať schémy usudzovania z tab. 1.1, ukážeme, že táto schéma je platná

- 1.  $p \Rightarrow q$       predpoklad<sub>1</sub>
- 2.  $\neg p \Rightarrow r$     predpoklad<sub>2</sub>
- 3.  $r \Rightarrow s$         predpoklad<sub>3</sub>

- 4.  $\neg q \Rightarrow \neg p$  inverzia implikácie na predpoklad<sub>1</sub>
- 5.  $\neg q \Rightarrow r$  hypotetický sylogizmus na medzivýsledok 4 a predpoklad<sub>2</sub>
- 6.  $\neg q \Rightarrow s$  hypotetický sylogizmus na medzivýsledok 5 a predpoklad<sub>3</sub>

Diagramatická interpretácia tohto logického dôkazu je vykonaná pomocou stromu dôkazu znázorneného na obr. 1.3.

**OBRÁZOK 1.3.**  
STROM  
ODVODENIA PRE  
PRÍKLAD 1.5.



Strom odvodenia pre logický dôkaz z príkladu 1.5.

**VETA O DEDUKCII**

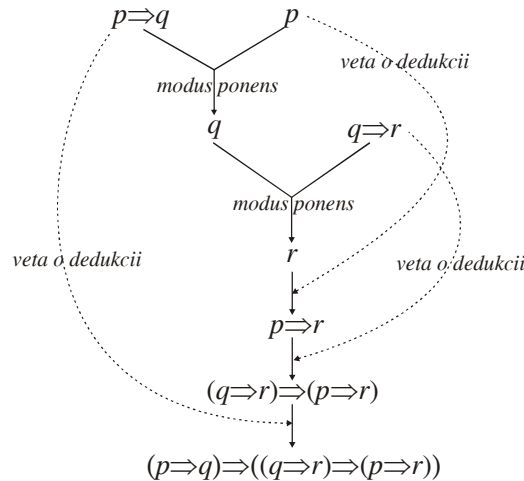


Uskutočnenie logického dôkazu  $\{\varphi_1, \dots, \varphi_n\} \vdash \varphi$  môže byť podstatne zjednodušené. Ak množinu predpokladov  $\{\varphi_1, \dots, \varphi_n\}$  rozšírime o nový „pomocný“ predpoklad  $\psi$ , potom vo výrokovej logike platí **veta o dedukcii** (pozri vetu 2.3 v Matematickej logike [11]), ktorá má tvar

$$(\{\varphi_1, \dots, \varphi_n\} \cup \{\psi\} \vdash \varphi) \Rightarrow (\{\varphi_1, \dots, \varphi_n\} \vdash (\psi \Rightarrow \varphi)) \quad (1.4)$$

To znamená, že logický dôkaz formuly  $\varphi$  pomocou rozšírenej množiny predpokladov  $\{\varphi_1, \dots, \varphi_n\} \cup \{\psi\}$  je rovnocenný logickému dôkazu formuly  $\psi \Rightarrow \varphi$  pomocou pôvodnej množiny predpokladov.

**OBRÁZOK 1.4.**  
STROM  
ODVODENIA PRE  
PRÍKLAD 1.6.



Strom odvodenia pre logický dôkaz z príkladu 1.6.

**PRÍKLAD 1.6.**

Pomocou logického dôkazu založeného na (1.4) dokážeme zákon hypotetického sylogizmu výrokovej logiky

$$\{p \Rightarrow q, q \Rightarrow r\} \cup \{p\} \vdash r$$

kde množina  $\{p \Rightarrow q, q \Rightarrow r\}$  obsahujúca pôvodné predpoklady je rozšírená o pomocný predpoklad  $p$ .

1.	$p \Rightarrow q$	predpoklad <sub>1</sub>
2.	$q \Rightarrow r$	predpoklad <sub>2</sub>
3.	$p$	pomocný predpoklad
4.	$q$	modus ponens na predpoklad <sub>1</sub> a pomocný predpoklad
5.	$r$	modus ponens na predpoklad <sub>2</sub> a medzivýsledok 4
6.	$p \Rightarrow r$	použitie (1.4) na výsledok 5 a pomocný predpoklad
7.	$(q \Rightarrow r) \Rightarrow (p \Rightarrow r)$	použitie (1.4) na výsledok 6 a predpoklad <sub>2</sub>
8.	$(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$	použitie (1.4) na výsl. 7 a predpoklad <sub>1</sub>

**TAUTOLÓGIA PLATÍ  
PRE PRÁZDNU  
MNOŽINU  
PREDPOKLADOV**

V krokoch 7 a 8 sme opakovane použili vzťah (1.4), kde sme z množiny predpokladov vždy eliminovali jeden predpoklad. Finálny výsledok už platí pre prázdnu množinu predpokladov, čo znamená, že formula je zákonom (tautológiou) výrokovej logiky.

V kapitole 1.1 bolo zdôraznené postavenie viet vo formálnom logickom systéme ako efektívnej skratky logických dôkazov, kde sa už nemusí opakovať to, čo už raz bolo dokázané. Tento prístup výstavby formálnych systémov pomocou viet a ich využívania patrí medzi základné črty formálnych systémov, ktorých výstavba sa uskutočňuje hlavne pomocou prepojenej siete viet, ktoré sú dokazované pomocou už dokázaných viet v predošlých krokoch.

Nech  $\psi$  je veta (tautológia), potom logický dôkaz  $\{\varphi_1, \dots, \varphi_n\} \vdash \varphi$  môže byť rozšírený o vetu  $\psi$  takto

$$(\{\varphi_1, \dots, \varphi_n\} \vdash \varphi) \Rightarrow (\{\varphi_1, \dots, \varphi_n\} \cup \{\psi\} \vdash \varphi) \quad (1.5)$$

Význam tohto rozšírenia spočíva v tom, že zahrnutie vhodnej vety (tautologie)  $\psi$  môže podstatne zjednodušiť dôkaz vety.

**PRÍKLAD 1.7.**

Dokážte zákon rezolventy<sup>4</sup>

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

pomocou zákona hypotetického sylogizmu

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

a pomocou vety o disjunktnej tvare implikácie,  $(p \Rightarrow q) \equiv (\neg p \vee q)$ , formálne

<sup>4</sup> V knihe Matematická logika [11] je rezolventa (alebo rezolučný princíp) formulovaná pomocou vety 5.2 ako formula  $(B \vee I) \wedge (C \vee \neg I) \Rightarrow (B \vee C)$ , ktorá sa dá jednoduchými úpravami previesť na rezolventu z príkladu 1.7.

$$\underbrace{\{(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))\}}_{\varphi_1} \cup \underbrace{\{(p \Rightarrow q) \equiv (\neg p \vee q)\}}_{\psi}$$

$$\vdash \underbrace{((p \vee q) \Rightarrow ((\neg p \vee r) \Rightarrow (q \vee r)))}_{\varphi}$$

Logický dôkaz pozostáva z tejto postupnosti medzivýsledkov:

1.	$(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$	predpoklad <sub>1</sub>
2.	$(p \Rightarrow q) \equiv (\neg p \vee q)$	pomocný predpoklad - veta
3.	$(\neg p \vee q) \Rightarrow ((\neg q \vee r) \Rightarrow (\neg p \vee r))$	prepis 1 pomocou vety 2
4.	$(\neg q \vee p) \Rightarrow ((\neg p \vee r) \Rightarrow (\neg q \vee r))$	prepis 3 pomocou zámenny $p \leftrightarrow q$
5.	$(p \vee q) \Rightarrow ((\neg p \vee r) \Rightarrow (q \vee r))$	prepis 4 pomocou substitúcie $\neg q/q$

Úplne analogickým spôsobom by sme mohli dokázať, že zákon rezolventy je možné prepísať na zákon hypotetického sylogizmu, z čoho plynie, že tieto dva zákony sú navzájom ekvivalentné:

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

## Chybné pravidlá usudzovania

POTVRDENIE  
DÔSLEDKU

Existujú jednoduché modifikácie schém usudzovania modus ponens a modus tollens, ktoré nie sú korektné. Prvá nekorektná schéma sa nazýva *potvrdenie dôsledku* (*affirming the consequent*)

$$\frac{\begin{array}{l} q \\ p \Rightarrow q \end{array}}{p} \quad (1.6a)$$

POPRETIE  
PREDPOKLADU

Druhá sa nazýva *popretie predpokladu* (*denying the antecedent*)

$$\frac{\begin{array}{l} \neg p \\ p \Rightarrow q \end{array}}{\neg q} \quad (1.6b)$$

Prvá schéma „popretie predpokladu“ je ilustrovaná príkladom

$$\frac{\begin{array}{l} \text{vydala som sa} \\ \text{ak som pekná, tak sa vydám} \end{array}}{\text{som pekná}}$$

Záver nie je korektný, môže sa vydať aj vtedy, keď nie je pekná. Druhá schéma „potvrdenie dôsledku“ môže byť ilustrovaná podobným príkladom

$$\frac{\begin{array}{l} \text{nie som pekná} \\ \text{ak som pekná, tak sa vydám} \end{array}}{\text{nevydám sa}}$$

Chyba v usudzovaní je podobná ako v predchádzajúcom príklade. O nekorrektnosti schém usudzovania (1.6a-b) sa ľahko presvedčíme tak, že im priradíme formuly výrokovej logiky

$$q \Rightarrow ((p \Rightarrow q) \Rightarrow p) \quad (1.7a)$$

$$\neg p \Rightarrow ((p \Rightarrow q) \Rightarrow \neg q) \quad (1.7b)$$

Pre prvú formulu existuje interpretácia premenných  $\tau = (p/0, q/0)$ , pre ktorú má prvá formula (1.7a) pravdivostnú hodnotu '0'. Táto interpretácia môže byť použitá aj pre druhú formulu (1.7b) aby sme ukázali, že formula má pravdivostnú hodnotu '0'. To znamená, že obe formuly (1.7a-b) nie sú tautológie, čiže nemôžu byť zákonmi výrokovej logiky.

Ako svedčia mnohé kognitívno-psychologické výskumy, obe tieto schémy, aj keď sú chybné, často sa využívajú v bežnom usudzovaní, možno ich teda pokladať za „klasické chyby“ nášho každodenného uvažovania.

## 1.3 PRAVIDLÁ USUDZOVANIA V PREDIKÁTOVEJ LOGIKE

Predikátová logika môže byť chápaná ako rozšírenie výrokovej logiky o tzv. kvantifikátory (všeobecný a existenčný) (pozri kapitoly 6 – 8 v Matematickej logike [11]). Základné schémy usudzovania v predikátovej logike sú uvedené v tab. 1.2.

**Tabuľka 1.2. Schémy usudzovania predikátovej logiky**

Schéma usudzovania	Teoréma predikátovej logiky	Názov schémy
$\frac{\forall x P(x)}{P(c)}$	$(\forall x P(x)) \Rightarrow P(c)$	Konkretizácia univerzálneho kvantifikátora
$\frac{P(c) \text{ pre každé } c}{\forall x P(x)}$	$P(c) \Rightarrow (\forall x P(x))$	Zovšeobecnenie pomocou univerzálneho kvantifikátora
$\frac{\exists x P(x)}{P(c) \text{ pre nejaký element } c}$	$(\exists x P(x)) \Rightarrow P(c)$	Konkretizácia existenčného kvantifikátora
$\frac{P(c) \text{ pre nejaký element } c}{\exists x P(x)}$	$P(c) \Rightarrow (\exists x P(x))$	Zovšeobecnenie pomocou existenčného kvantifikátora



KONKRETIZÁCIA  
UNIVERZÁLNEHO  
KVANTIFIKÁTORA

Ak nejakú vlastnosť  $P(x)$  má každý objekt (individuum) z univerza  $U$ ,  $\forall x P(x)$ , potom túto vlastnosť musí mať aj ľubovoľný konkrétny objekt  $c$  z tohto univerza,

$$(\forall x P(x)) \Rightarrow P(c) \quad (1.8)$$

Táto vlastnosť je priamym dôsledkom intuitívnej interpretácie univerzálneho kvantifikátora ako konjunkcie vlastnosti  $P(x)$  pre každý objekt  $x$  z konečného univerza

$$\forall x P(x) =_{\text{def}} \bigwedge_{x \in U} P(x) = P(a) \wedge P(b) \wedge \dots \wedge P(u) \quad (1.9)$$

Ak na túto formulu (predpoklad) použijeme schému usudzovania simplifikácie z tab. 1.1, potom vlastnosť  $P$  má menovite každý objekt z  $U$

$$\frac{\forall x P(x)}{\begin{array}{l} P(a) \\ P(b) \\ \dots \\ P(c) \\ \dots \end{array}} \quad (1.10)$$

Potom musí platiť aj implikácia (1.8). Ako ilustračný príklad tejto vlastnosti univerzálneho kvantifikátora uvidíme klasický príklad konkretizácie zo stredovekej logiky

$$\frac{\begin{array}{l} \textit{každý človek je smrteľný} \\ \textit{Sokrates je človek} \end{array}}{\textit{Sokrates je smrteľný}}$$

kde Sokrates patrí do univerza  $U$  (obsahujúceho všetkých ľudí) platnosti kvantifikátora  $\forall$ . Túto schému usudzovania môžeme zovšeobecniť takto

$$\frac{\begin{array}{l} \forall (x \in U) P(x) \\ c \in U \end{array}}{P(c)} \quad (1.11)$$

ZOVŠEOBECNENIE  
POMOCOU  
UNIVERZÁLNEHO  
KVANTIFIKÁTORA

Ak sa nám podarí dokázať, že vlastnosť  $P$  má každý objekt z nejakého univerza  $U$ , potom vzhľadom k tomuto univerzu môžeme definovať univerzálny kvantifikátor  $\forall$

$$P(a) \wedge \dots \wedge P(c) \wedge \dots = \bigwedge_{x \in U} P(x) =_{\text{def}} \forall x P(x) \quad (1.12)$$

Ak použijeme na túto formulu schému usudzovania konjunkcie z tab. 1.1, potom

$$\frac{\begin{array}{l} P(a) \\ \dots \\ P(c) \\ \dots \end{array}}{\forall x P(x)} \quad (1.13)$$

potom musí platiť aj

$$P(c) \Rightarrow (\forall x P(x)) \quad (1.14)$$

s poznámkou, že  $c$  je ľubovoľný objekt z univerza  $U$ . Zovšeobecnenie pomocou univerzálneho kvantifikátora sa často používa v matematike implicitne, pretože dôkaz vlastnosti  $P(c)$  bol vykonaný nielen pre určitý špecifický objekt, ale pre ľubovoľný objekt  $c$ .

INDUKTÍVNE  
ZOVŠEOBECNIE A  
FALZIFIKÁCIA

V mnohých prípadoch mimo matematiku, použitie zovšeobecnenia podľa schémy usudzovania (1.13) (alebo predikátovej formuly (1.14)) tvorí základ tzv. *induktívneho zovšeobecnia*, v ktorom sa snažíme parciálne poznatky zovšeobecniť pre každý objekt postulovaného univerza  $U$ . V tejto súvislosti potom vystupuje do popredia podľa rakúsko-anglického filozofa Karla Poppera problém falzifikácie všeobecného výroku  $\forall x P(x)$ . Stačí nájsť jeden objekt  $o \in U$ , pre ktorý neplatí vlastnosť  $P$ ,  $\neg P(o)$ , potom všeobecný výrok  $\forall x P(x)$  je neplatný,  $\neg \forall x P(x)$ .

Ako ilustračný príklad budeme študovať univerzum  $U$ , ktoré obsahuje všetky labute na našej planéte. Experimentálnym pozorovaním zistíme, že pre veľkú podmnožinu  $U' \subset U$  platí, že každá labuť z nej je biela (túto vlastnosť označíme predikátom  $B$ ). Túto skutočnosť môžeme „pochtivo“ zovšeobecniť pomocou univerzálneho kvantifikátora  $\forall'$  definovaného vzhľadom k „poduniverzu“  $U'$

$$\forall' x B(x) =_{\text{def}} \bigwedge_{x \in U'} B(x)$$

V dôsledku určitej netrpezlivosti, pozorovateľ zovšeobecni tento poznatok pre celé univerzum  $U$ , postuluje platnosť formuly  $\forall x B(x)$ . Falzifikácia tejto vlastnosti spočíva v tom, že nájdeme takú labuť (napr. pod skleneným mostom v Piešťanoch), ktorá je čierna, potom automaticky platí  $\neg \forall x B(x)$ .

ROZŠIROVANIE  
PLATNOSTI

V tejto súvislosti môžeme hovoriť aj o verifikácii vlastnosti  $\forall' x B(x)$ , ďalšími a ďalšími pozorovaniami rozširujeme univerzum  $U'$  o ďalšie objekty  $x$ , ktoré majú vlastnosť  $B(x)$ . Avšak je potrebné poznamenať, že toto rozširovanie platnosti  $\forall' x B(x)$  o ďalšie objekty nám neprináša nový poznatok, neustále platí, že „labute sú biele“, len máme stále rozsiahlejšie vedomosti o evidentnosti tohto poznatku. Preto falzifikácia, na rozdiel od verifikácie, je zásadne dôležitá pre indukzívne zovšeobecňovanie, napomáha nám pri vzniku nových poznatkov (čo ako prvý zdôraznil Karl Popper).

KONKRETIZÁCIA  
EXISTENČNÉHO  
KVANTIFIKÁTORA

Ak nejaká vlastnosť platí pre niektorý objekt  $c \in U$ , potom musí platiť aj implikácia

$$(\exists x P(x)) \Rightarrow P(c) \quad (1.15)$$

alebo pomocou schémy usudzovania

$$\frac{\exists x P(x)}{P(c) \text{ pre nejaký element } c} \quad (1.16)$$

Táto vlastnosť konkretizácie existenčného kvantifikátora vyplýva priamo z jeho intuitívnej interpretácie pomocou disjunkcie predikátov nad konečným univerzom

$$\exists x P(x) =_{\text{def}} \bigvee_{x \in U} P(x) = P(a) \vee \dots \vee P(c) \vee \dots \quad (1.17)$$

Disjunkcia výrokov je pravdivá vtedy a len vtedy, ak aspoň jeden jej výrok je pravdivý, potom existuje aspoň jeden objekt  $c$  pre ktorý je výrok  $P(c)$  pravdivý, t. j. platí implikácia (1.15).

ZOVŠEOBECNENIE  
POMOCOU  
EXISTENČNÉHO  
KVANTIFIKÁTORA

Podľa tejto „skromnej“ schémy usudzovania, ak nejaká vlastnosť  $P$  platí aspoň pre jeden objekt  $c$  z univerza  $U$ , potom túto skutočnosť môžeme zovšeobecniť pomocou existenčného kvantifikátora  $\exists$

$$P(c) \Rightarrow \bigvee_{x \in U} P(x) \stackrel{\text{def}}{=} \exists x P(x) \quad (1.18)$$

kde sme použili schému usudzovania s názvom adícia z tab. 1.1. Túto implikáciu môžeme vyjadriť pomocou schémy usudzovania

$$\frac{P(c) \text{ pre nejaký element } c}{\exists x P(x)} \quad (1.19)$$

Spojením (1.15) a (1.18) dostaneme

$$P(c) \equiv \exists x P(x) \quad (1.20)$$

Podľa tejto formuly, pravdivosť výroku  $P(c)$  je ekvivalentná pravdivosti výroku s existenčným kvantifikátorom  $\exists x P(x)$ .

**PRÍKLAD 1.8.**

Ukážte, že záver  $\varphi$  vyplýva z predpokladov  $\varphi_1$  a  $\varphi_2$ :

$\varphi_1$  = ‘každý kto navštevuje prednášky z diskkrétnej matematiky je študentom STU’

$\varphi_2$  = ‘Mária navštevuje prednášky z diskkrétnej matematiky’

$\varphi$  = ‘Mária je študentka STU’.

Tieto tri výroky prepíšeme do tvaru

$$\frac{\begin{array}{l} \varphi_1 = \forall x (DM(x) \Rightarrow STU(x)) \\ \varphi_2 = DM(Maria) \end{array}}{\varphi = STU(Maria)}$$

kde  $DM(x)$  je predikát ‘objekt  $x$  navštevuje prednášku z diskkrétnej matematiky’ a  $STU(x)$  je predikát ‘objekt  $x$  je študentom STU’. Korektnosť riešenia overíme postupnosťou formúl

1.	$\forall x (DM(x) \Rightarrow STU(x))$	predpoklad <sub>1</sub>
2.	$DM(Maria)$	predpoklad <sub>2</sub>
3.	$DM(Maria) \Rightarrow STU(Maria)$	konkretizácia 1
4.	$STU(Maria)$	modus ponens na 2 a 3

**PRÍKLAD 1.9.**

Ukážte, že záver  $\varphi$  vyplýva z predpokladov  $\varphi_1$  a  $\varphi_2$ :

$\varphi_1$  = ‘niektorí študenti navštevujúci prednášku nečítali predpísanú učebnicu’

$\varphi_2$  = ‘každý študent navštevujúci prednášku vykonal skúšku’

$\varphi$  = ‘niektorí študenti, ktorí vykonali skúšku, nečítali predpísanú učebnicu’.

Tieto tri výroky prepíšeme do tvaru



$$\left| \begin{array}{l} \varphi_1 = \exists x (P(x) \wedge \neg N(x)) \\ \varphi_2 = \forall x (P(x) \Rightarrow S(x)) \\ \hline \varphi = \exists x (S(x) \wedge \neg N(x)) \end{array} \right.$$

kde  $P(x)$  je predikát 'objekt  $x$  navštevuje prednášku',  $N(x)$  je predikát 'objekt  $x$  čítal predpísanú učebnicu',  $S(x)$  je predikát 'objekt  $x$  vykonal skúšku'. Korektnosť riešenia overíme postupnosťou formúl

1.	$\exists x (P(x) \wedge \neg N(x))$	predpoklad <sub>1</sub>
2.	$\forall x (P(x) \Rightarrow S(x))$	predpoklad <sub>2</sub>
3.	$P(c) \wedge \neg N(c)$	konkretizácia predpokladu <sub>1</sub>
4.	$P(c)$	simplifikácia 3
5.	$\neg N(c)$	simplifikácia 3
6.	$P(c) \Rightarrow S(c)$	konkretizácia predpokladu <sub>2</sub>
7.	$S(c)$	modus ponens na 4 a 6
8.	$S(c) \wedge \neg N(c)$	konjunkcia 5 a 7
9.	$\exists x (S(x) \wedge \neg N(x))$	zovšeobecnie 8 pomocou existenčného kvantifikátora

Ako vidieť z uvedených príkladov, dôkazy formúl obsahujúcich kvantifikátory sú zmesou aplikácií schém usudzovania tak z výrokovej, ako aj predikátovej logiky. Táto skutočnosť vyplýva z faktu, že predikátová logika je vlastne zovšeobecnením výrokovej logiky, ktorá je „vnorená“ do predikátovej logiky; všetky zákony výrokovej logiky sú aj zákonmi predikátovej logiky.

## 1.4 METÓDY DÔKAZU VIET

Dôkaz vety je vo všeobecnosti obtiažny a netriviálny problém, ktorý len v ojedinelých prípadoch môže byť vykonaný priamočiarym mechanickým postupom. Preto v matematike vznikli rôzne metódy dôkazu viet, z ktorých uvedieme najdôležitejšie: priamy dôkaz, nepriamy dôkaz, dôkaz sporom a dôkaz vymenovaním prípadov.

PRIAMY DÔKAZ



Implikácia  $p \Rightarrow q$  môže byť dokázaná tak, že ukážeme, že z predpokladu pravdivosti výroku  $p$  vyplýva taktiež aj pravdivosť výroku  $q$ . Túto jednoduchú formuláciu priameho dôkazu môžeme upresniť tak, že pri dôkaze vychádzame z axióm  $\{\varphi_1, \dots, \varphi_n\}$  a z už dokázaných viet  $\{\psi_1, \dots, \psi_m\}$ , potom dôkaz  $p \Rightarrow q$  môžeme charakterizovať vzťahom logického dôkazu

$$\{\varphi_1, \dots, \varphi_n\} \cup \{\psi_1, \dots, \psi_m\} \cup \{p\} \vdash q \quad (1.21)$$

V tejto schéme máme na ľavej strane všetky axiómy systému, dokázané potrebné

vety (tautológie) a predpoklad  $p$ . Použitím pravidiel odvodzovania (modus ponens, pravidlá substitúcie,...) z týchto „predpokladov“ odvodíme dôsledok  $q$ .

**PRÍKLAD 1.10.** Dokážte vetu „ak  $n$  je nepárne prirodzené číslo, potom  $n^2$  je taktiež nepárne číslo“.

Požadovanú vetu sformalizujeme pomocou implikácie

$$\underbrace{(n \text{ je nepárne číslo})}_p \Rightarrow \underbrace{(n^2 \text{ je nepárne číslo})}_q$$

Použijeme techniku priameho dôkazu, z predpokladu pravdivosti  $p$  dokážeme pravdivosť dôsledku  $q$ .

Nech  $n$  je nepárne prirodzené číslo, potom existuje také nezáporné celé číslo  $k$ , že  $n = 2k + 1$ . Pre kvadrát čísla  $n$  platí

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2 \underbrace{(2k^2 + 2k)}_l + 1 = 2l + 1$$

čiže aj kvadrát  $n^2$  je nepárne číslo. Týmto sme dokázali platnosť implikácie  $p \Rightarrow q$ .

NEPRIAMY  
DŮKAZ



Technika nepriameho dôkazu je založená na ekvivalencii (nazývanej zákon inverzie implikácie)  $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$ , podľa ktorej, ak v implikácii vymeníme poradie jej členov, potom musíme negovať aj jej jednotlivé členy. Z tohto zákona vyplýva, že dôkaz implikácie  $(p \Rightarrow q)$  je ekvivalentný dôkazu „inverznej“ implikácie  $\neg q \Rightarrow \neg p$ .

**PRÍKLAD 1.11.** Dokážte vetu „ak  $3n + 2$  je nepárne číslo, potom aj  $n$  je nepárne číslo“.

Vetu upravíme do tvaru implikácie

$$\underbrace{(3n + 2 \text{ je nepárne číslo})}_p \Rightarrow \underbrace{(n \text{ je nepárne číslo})}_q$$

Budeme dokazovať inverznú implikáciu

$$\underbrace{(n \text{ je párne číslo})}_{\neg q} \Rightarrow \underbrace{(3n + 2 \text{ je párne číslo})}_{\neg p}$$

Nech  $n$  je párne číslo, potom existuje také nezáporné celé číslo  $k$ , že  $n = 2k$ . Pre takto špecifikované číslo  $n$  dostaneme  $3n + 2 = 3(2k) + 2 = 2(3k + 1)$ , ktoré je párne. Týmto sme dokázali inverznú implikáciu  $\neg q \Rightarrow \neg p$ , čiže musí platiť aj „pôvodná“ implikácia  $p \Rightarrow q$ .

DŮKAZ SPOROM



Tento typ dôkazu je založený na schéme „reductio ad absurdum“ z tab. 1.1

$$\left| \begin{array}{l} p \Rightarrow q \\ p \Rightarrow \neg q \\ \hline \neg p \end{array} \right. \quad (1.22)$$

založenej na zákone výrokovej logiky

$$(p \Rightarrow q) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \neg p) \quad (1.23)$$

Túto schému usudzovania môžeme interpretovať tak, že ak z predpokladu  $p$  súčas-

ne odvodíme  $q$  a  $\neg q$ , potom musí byť pravdivá negácia  $\neg p$  východiskového predpokladu.

**PRÍKLAD 1.12.** Dokážte, že  $\sqrt{2}$  je iracionálne číslo.

Predpokladajme, že  $\sqrt{2}$  je racionálne číslo, tento výrok označíme

$$p = '\sqrt{2} \text{ je racionálne číslo}'$$

Z tohto výroku vyplýva, že číslo  $\sqrt{2}$  má tvar  $\alpha/\beta$ , kde  $\alpha$  a  $\beta$  sú celé nesúdeliteľné čísla, tento výrok označíme

$$q = '\sqrt{2} = \alpha/\beta, \text{ kde } \alpha, \beta \text{ sú celé nesúdeliteľné čísla}'$$

t. j. platí implikácia  $p \Rightarrow q$ . Úpravou matematického výrazu z výroku  $q$  dostaneme formulu  $\alpha^2 = 2\beta^2$ , z ktorej vyplýva, že číslo  $\alpha^2 = 2k$  je párne. V príklade 1.10 bola dokázaná veta, že ak celé číslo  $n$  je nepárne, potom aj jeho kvadrát  $n^2$  je nepárne číslo. Obrátením tejto implikácie dostaneme, že ak  $n^2$  je párne číslo, potom aj  $n$  je párne číslo. Z tejto vety vyplýva, že číslo  $\alpha$  je párne. Potom taktiež platí  $\beta^2 = 2p^2$ , t. j.  $\beta^2$  je párne číslo, čiže aj  $\beta$  je párne číslo. Týmto sme dokázali, že  $\alpha$ ,  $\beta$  sú párne čísla, čiže sú súdeliteľné

$$\neg q = '\sqrt{2} = \alpha/\beta, \text{ kde } \alpha, \beta \text{ sú celé súdeliteľné čísla}'$$

t. j. platí implikácia  $p \Rightarrow \neg q$ . Týmto sme dokázali, že súčasne platia implikácie  $p \Rightarrow q$  a  $p \Rightarrow \neg q$ , použitím schémy „reductio ad absurdum“ (1.22) dostaneme, že platí negácia ich predpokladu

$$\neg p = '\sqrt{2} \text{ je iracionálne číslo}'$$

čo bolo potrebné dokázať.

DŮKAZ  
VYMENOVANÍM  
PRÍPADOV

Naším cieľom je dokázať implikáciu

$$(p_1 \vee \dots \vee p_n) \Rightarrow q \tag{1.24}$$

Jednoduchými ekvivalentnými úpravami môžeme túto implikáciu prepísať do ekvivalentného tvaru

$$((p_1 \vee \dots \vee p_n) \Rightarrow q) \equiv ((p_1 \Rightarrow q) \wedge \dots \wedge (p_n \Rightarrow q)) \tag{1.25}$$



1.	$(p_1 \vee \dots \vee p_n) \Rightarrow q$	
2.	$\neg(p_1 \vee \dots \vee p_n) \vee q$	prepis 1 pomocou disjunktívneho tvaru implikácie
3.	$(\neg p_1 \wedge \dots \wedge \neg p_n) \vee q$	použitie De Morganovho zákona na 2
4.	$(\neg p_1 \vee q) \wedge \dots \wedge (\neg p_n \vee q)$	použitie distributívneho zákona na 3
5.	$(p_1 \Rightarrow q) \wedge \dots \wedge (p_n \Rightarrow q)$	prepis 4 s disjunktívnym tvarom implikácie

Formulu (1.25) môžeme prepísať do tvaru schémy usudzovania

$$\frac{\begin{array}{l} (p_1 \Rightarrow q) \\ \dots\dots\dots \\ (p_n \Rightarrow q) \end{array}}{(p_1 \vee \dots \vee p_n) \Rightarrow q} \quad (1.26)$$

Túto schému usudzovania (dôkaz vymenovaním prípadov) používame vtedy, ak výrok  $q$  je dôsledok rôznych prípadov  $p_1, \dots, p_n$ .

**PRÍKLAD 1.13.** Dokážte identitu

$$\max\{a, \min\{b, c\}\} = \min\{\max\{a, b\}, \max\{a, c\}\}$$

kde  $a, b$  a  $c$  sú rôzne čísla.

Dôkaz tejto identity vykonáme tak, že vykonáme verifikáciu identity pre všetkých 6 rôznych prípadov:

(1) Prípad  $a < b < c$

$$\begin{array}{l} \max\left\{a, \underbrace{\min\{b, c\}}_b\right\} = \min\left\{\underbrace{\max\{a, b\}}_b, \underbrace{\max\{a, c\}}_c\right\} \\ \underbrace{\max\{a, b\}}_b = \underbrace{\min\{b, c\}}_b \\ b = b \end{array}$$

(2) Prípad  $b < a < c$

$$\begin{array}{l} \max\left\{a, \underbrace{\min\{b, c\}}_b\right\} = \min\left\{\underbrace{\max\{a, b\}}_a, \underbrace{\max\{a, c\}}_c\right\} \\ \underbrace{\max\{a, b\}}_a = \underbrace{\min\{a, c\}}_a \\ a = a \end{array}$$

Podobným spôsobom preskúmame aj ostatné štyri možnosti vzájomného usporiadania čísel  $a, b$  a  $c$ . Týmto spôsobom sme dokázali 6 nezávislých implikácií

$$(a < b < c) \Rightarrow (\max\{a, \min\{b, c\}\} = b) \wedge (\min\{\max\{a, b\}, \max\{a, c\}\} = b)$$

$$(b < a < c) \Rightarrow (\max\{a, \min\{b, c\}\} = a) \wedge (\min\{\max\{a, b\}, \max\{a, c\}\} = a)$$

$$\dots\dots\dots (c < b < a) \Rightarrow (\max\{a, \min\{b, c\}\} = a) \wedge (\min\{\max\{a, b\}, \max\{a, c\}\} = a)$$

Týmto „enumeratívnym“ spôsobom sme dokázali danú algebraickú identitu tak, že sme separátne preskúmali všetky možné usporiadania čísel  $a, b$  a  $c$ .

**PRÍKLAD 1.14.** Dokážte identitu  $|a - b| \leq |a| + |b|$ , kde  $a, b$  sú ľubovoľné nenulové reálne čísla a  $|\cdot|$  je absolútna hodnota.

- (1)  $a < b < 0$ , potom  $a - b < 0$ ,  $a < 0$  a  $b < 0$ , dokazovaná nerovnosť má tvar  $-(a - b) \leq -a - b$ , alebo  $b \leq 0$ , čo je pravdivý výrok.
- (2)  $a < 0 < b$ , potom  $a - b < 0$ ,  $a < 0$  a  $b > 0$ , dokazovaná nerovnosť má tvar  $-(a - b) \leq -a + b$ , čo je pravdivý výrok.
- (3)  $0 < a < b$ , potom  $a - b < 0$ ,  $a > 0$  a  $b > 0$ , dokazovaná nerovnosť má tvar  $-(a - b) \leq a + b$ , alebo  $a \geq 0$ , čo je pravdivý výrok.

Podobným spôsobom by sa dokázali aj ostatné tri možnosti ( $b < a < 0$ ,  $b < 0 < a$  a  $0 < b < a$ ).

Nutnosť použitia metódy dôkazu vymenovaním všetkých prípadov sa môže stať v niektorých špeciálnych situáciách limitujúcim faktorom uskutočnenia dôkazu, keď počet možných prípadov je veľké číslo. Potom môžeme prenechať hlavnú ťarchu dôkazu počítaču, ktorý systematicky preverí všetky možné prípady. Podobná situácia sa vyskytla počiatkom 90. rokov minulého storočia, keď matematik Andrew Wiles po dlhoročnom úsilí dokázal Veľkú Fermatovu vetu<sup>5</sup>.

## 1.5 MATEMATICKÁ INDUKCIA

Stojíme pred problémom dokázať formulu  $\forall n P(n)$ , podľa ktorej vlastnosť  $P(n)$  platí pre každé prirodzené číslo. Dôkaz tejto formuly je možné vykonať metódou matematickej indukcie, ktorá je založená na dvoch východiskových predpokladoch  $P(1)$  a  $\forall n (P(n) \Rightarrow P(n+1))$ . Ukážeme, že z týchto dvoch predpokladov vyplýva formula  $\forall n P(n)$ .

1.	$P(1)$	
2.	$\forall n (P(n) \Rightarrow P(n+1))$	
<hr/>		
3.	$P(1) \Rightarrow P(2)$	konkretizácia 2 pre $n = 1$
4.	$P(2) \Rightarrow P(3)$	konkretizácia 2 pre $n = 2$
.....		
5.	$P(n) \Rightarrow P(n+1)$	konkretizácia 2 pre $n = n$
.....		

<sup>5</sup> Veľká Fermatova veta tvrdí, že rovnica  $x^n + y^n = z^n$  nemá celočíselné riešenie pre  $x, y$  a  $z$ , pričom  $xyz \neq 0$  a  $n$  je celé číslo, pričom  $n > 2$ . Wilesov článok, v ktorom podal dôkaz tejto vety, „Modular Elliptic Curves and Fermat's Last Theorem“ bol publikovaný v r. 1995 v časopise *Annals of Mathematics*. Článok je doprevádzaný vysoko technickou publikáciou jeho doktoranda Richarda Taylora, v ktorom boli enumeratívnym spôsobom preštudované na počítači vlastnosti špeciálnej Heckeho algebry, ktorej použitie hrá kľúčovú úlohu v celom dôkaze.

6.	$P(2)$	modus ponens na 1 a 3
7.	$P(3)$	modus ponens na 6 a 4
.....	.....	.....
8.	$P(n+1)$	modus ponens na predchádzajúci riadok a 5
.....	.....	.....
9.	$\forall n P(n)$	zovšeobecnenie pomocou $\forall$

Tento výsledok môže byť prezentovaný ako schéma usudzovania matematickej indukcie



$$\frac{\begin{array}{l} P(1) \\ \forall n (P(n) \Rightarrow P(n+1)) \end{array}}{\forall n P(n)} \quad (1.27)$$

PEANO

Metóda matematickej indukcie bola známa už počiatkom novoveku talianskemu matematikovi Francescovi Maurolicovi (1494 – 1575), ktorý ju používal na dôkaz niektorých vlastností celých čísel (napr. dokázal, že suma prvých  $n$  prirodzených nepárnych čísel sa rovná  $n^2$ ). V modernej matematike a logike matematická indukcia bola využitá talianskym matematikom a logikom Giuseppom Peanom (1858 – 1932) pri formulácii jeho axiomatického systému aritmetiky celých čísel.

**PRÍKLAD 1.15.**

Dokážte, že suma prvých  $n$  nepárnych prirodzených čísel sa rovná  $n^2$ .

Položíme

$$P(n): 1 + 3 + 5 + \dots + (2n-1) = \sum_{i=1}^n (2i-1) = n^2$$

Lahko sa presvedčíme, že platí  $P(1) = 1$ . Budeme študovať  $P(n+1)$

$$\begin{aligned} P(n+1): 1 + 3 + 5 + \dots + (2n-1) + (2(n+1)-1) &= \sum_{i=1}^{n+1} (2i-1) = \\ &= \sum_{i=1}^n (2i-1) + (2(n+1)-1) = n^2 + (2n+1) = (n+1)^2 \end{aligned}$$

Týmto sme dokázali, že platnosť formuly  $P(n)$  implikuje formulu  $P(n+1)$ , pre každé prirodzené číslo  $n$ , potom použitím zovšeobecnenia pomocou univerzálneho kvantifikátora dostaneme  $\forall n (P(n) \Rightarrow P(n+1))$ . Použitím schémy matematickej indukcie dostaneme

$$\forall n P(n): 1 + 3 + 5 + \dots + (2n-1) = \sum_{i=1}^n (2i-1) = n^2$$

čím sme zavšili dôkaz vety špecifikujúcej sumu prvých  $n$  nepárnych prirodzených čísel.

**PRÍKLAD 1.16.**

Dokážte, že pre každé prirodzené číslo  $n$  platí  $n < 2^n$ .

Nech  $P(n)$  je predikát ' $n < 2^n$ ', potom  $P(1)$  je pravdivý výrok. Budeme študovať  $P(n+1)$

$$n + 1 < 2^n + 1 \leq 2^n + 2^n = 2^{n+1}$$

kde sme k obidvom stranám nerovnice indukčného predpokladu  $n < 2^n$  pripočítali jednotku a taktiež sme použili jednoduchú vlastnosť  $1 \leq 2^n$ . Týmto sme dokázali, že pre každé prirodzené číslo  $n$  platí implikácia  $P(n) \Rightarrow P(n+1)$ , alebo inak vyjadrené  $\forall n (P(n) \Rightarrow P(n+1))$ , čo bolo potrebné dokázať.

SILNÁ  
MATEMATICKÁ  
INDUKCIA



Silná matematická indukcia je špeciálna forma „standardnej“ matematickej indukcie, v ktorej je vlastnosť  $P(n+1)$  implikovaná konjunkciou všetkých predchádzajúcich vlastností,  $P(1) \wedge P(2) \wedge \dots \wedge P(n) \Rightarrow P(n+1)$ . Predpokladajme, že táto vlastnosť je splnená pre každé  $n \geq 1$ , potom  $\forall n (P(1) \wedge \dots \wedge P(n) \Rightarrow P(n+1))$ . Zostrojme zovšeobecnenú schému usudzovania matematickej indukcie

$$\left| \begin{array}{l} P(1) \\ \forall n (P(1) \wedge P(2) \wedge \dots \wedge P(n) \Rightarrow P(n+1)) \\ \hline \forall n P(n) \end{array} \right.$$

Nebudeme dokazovať túto schému usudzovania, jej dôkaz je úplne analogický dôkazu schémy usudzovania matematickej indukcie (1.27).

#### PRÍKLAD 1.17.

Dokážte, že ľubovoľné prirodzené číslo  $n > 1$  môže byť vyjadrené ako súčin prvočísel.

Nech vlastnosť  $P(n)$  má tvar

$$P(n): \quad n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \quad p_k \leq n$$

kde  $p_1, p_2, p_3, \dots$  sú prvé prvočísla (2, 3, 5, ..., ktoré sú menšie ako  $n$ ) a  $\alpha_1, \alpha_2, \alpha_3, \dots$  sú nezáporné celé čísla. Táto formula je pravdivá pre  $P(2)$ , kde  $\alpha_1 = 1, k = 1$ , potom  $P(2): 2 = 2^1$ . Predpokladajme, že  $P(j)$  je pravdivé pre každé prirodzené  $j \leq n$ . Ukážeme, že z tohto predpokladu vyplýva platnosť  $P(n+1)$ . Bude rozlišovať dva prípady:

1. *prípado* –  $n+1$  je prvočíslo  $p_k$ , potom  $P(n+1): n+1 = p_1^0 p_2^0 \dots p_k^1$ .

2. *prípado* –  $n+1$  nie je prvočíslo, potom môže byť písané ako súčin dvoch prirodzených čísel  $a \cdot b$ , ktoré vyhovujú podmienke  $2 \leq a \leq b < n+1$ . Každé z týchto dvoch čísel môže byť vyjadrené ako súčin prvočísel (indukčný predpoklad)

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \quad p_k \leq n+1$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}, \quad p_k \leq n+1$$

potom ich súčin má tvar

$$P(n+1): \quad n+1 = a \cdot b = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \dots p_k^{\alpha_k+\beta_k}, \quad p_k \leq n+1$$

## ZHRNUTIE

### DÔKAZ

Dôkaz (deduktívny) v matematike a v informatike je špecifický postup konštrukcie nových viet (tautológií – teorém) pomocou súboru vybraných viet (axióm) a pravidiel odvodzovania (napr. pravidla modus ponens) tak, že zostrojíme postupnosť tautológií, pričom posledná tautológia z tejto postupnosti je dokazovaná veta. Komplikované dôkazy sú obvykle jasnejšie formulované, keď ich dôkaz je rozdelený na jednotlivé medzikroky, ktoré sú formulované ako samostatné vety.

### INDUKTÍVNE USUDZOVANIE

V matematike a v informatike sa v ojedinelých prípadoch používa aj *induktívne usudzovanie* (dôkaz), ktoré je založené na pozorovaní určitých skutočností, ktoré sa často opakujú v analogických situáciách. Tieto pozorované skutočnosti sú „induktívne“ zovšeobecnené. Nové pojmy, ktoré boli zavedené týmto „induktívnym“ spôsobom sa neskoršie buď dokážu deduktívne v rámci daného systému pojmov, alebo sa postulujú ako nové špeciálne axiómy. Tieto ojedinelé situácie v dejinách matematiky vždy znamenali vznik nových oblastí matematiky, ktoré nie sú striktné deduktívne dokázateľné zo známych pojmov.

### PRAVIDLÁ USUDZOVANIA

Pravidlá usudzovania vo výrokovvej logike tvoria schému (pozri tabuľku 1.1)

$$\frac{\begin{array}{l} \text{predpoklad}_1 \\ \dots\dots\dots \\ \text{predpoklad}_n \end{array}}{\text{záver}}$$

ktorá obsahuje  $n$  predpokladov a jeden záver. Táto schéma usudzovania je totožná so symbolom *logického dôkazu*

$$\{\text{predpoklad}_1, \dots, \text{predpoklad}_n\} \vdash \text{záver}$$

alebo

$$\{\varphi_1, \dots, \varphi_n\} \vdash \varphi$$

Použitie pravidiel usudzovania môže byť v niektorých prípadoch podstatne uľahčené aplikáciou vety o dedukcii. Množinu predpokladov  $\{\varphi_1, \dots, \varphi_n\}$  rozšírime o nový „pomocný“ predpoklad  $\psi$ , potom platí veta o dedukcii

$$(\{\varphi_1, \dots, \varphi_n\} \cup \{\psi\} \vdash \varphi) \Rightarrow (\{\varphi_1, \dots, \varphi_n\} \vdash (\psi \Rightarrow \varphi))$$

Dôkaz formuly  $\varphi$  pomocou rozšírenej množiny predpokladov  $\{\varphi_1, \dots, \varphi_n\} \cup \{\psi\}$  je rovnocenný dôkazu formuly  $\psi \Rightarrow \varphi$  pomocou pôvodnej množiny predpokladov.

### METÓDY DÔKAZU VIET

*Priamy dôkaz* implikácie  $p \Rightarrow q$  je uskutočnený tak, že ukážeme, že z predpokladu pravdivosti výroku  $p$  vyplýva taktiež aj pravdivosť výroku  $q$ .

*Nepriamy dôkaz* implikácie  $p \Rightarrow q$  spočíva v tom, že dôkaz tejto implikácie je ekvivalentný dôkazu „inverznej“ implikácie  $\neg q \Rightarrow \neg p$ .

*Dôkaz sporom* je založený na schéme „reductio ad absurdum“ z tab. 1.1



$$\frac{\begin{array}{l} p \Rightarrow q \\ p \Rightarrow \neg q \end{array}}{\neg p}$$

Ak z predpokladu  $p$  súčasne odvodíme  $q$  a  $\neg q$ , potom musí byť pravdivá negácia  $\neg p$  východzieho predpokladu, čo bolo potrebné dokázať.

Dôkaz vymenovaním prípadov implikácie  $(p_1 \vee \dots \vee p_n) \Rightarrow q$  je založený na jej ekvivalentnom tvare

$$((p_1 \vee \dots \vee p_n) \Rightarrow q) \equiv ((p_1 \Rightarrow q) \wedge \dots \wedge (p_n \Rightarrow q))$$

To znamená, že dôkaz sa redukuje na dôkazy všetkých implikácií  $p_i \Rightarrow q$ , pre  $i = 1, 2, \dots, n$ . Tento spôsob dôkazu je veľmi častý v diskkrétnej matematike.

MATEMATICKÁ  
INDUKCIA

Dôkaz vlastnosti  $\forall n P(n)$ , t. j.  $P(n)$  platí pre každé prirodzené číslo, je možné vykonať metódou matematickej indukcie, ktorá je založená na dvoch východiskových predpokladoch  $P(1)$  a  $\forall n (P(n) \Rightarrow P(n+1))$ , z ktorých vyplýva formula  $\forall n P(n)$ . Matematickú indukciu vyjadríme schémou usudzovania

$$\frac{\begin{array}{l} P(1) \\ \forall n (P(n) \Rightarrow P(n+1)) \end{array}}{\forall n P(n)}$$

## KLÚČOVÉ POJMY

deduktívny dôkaz  
matematická indukcia  
veta  
teoréma  
axióma  
lema  
pravidlá odvodzovania  
korektnosť  
konzistentnosť  
teória  
deduktívny dôkaz  
elementárny pojem  
induktívne usudzovanie  
axiomatický systém  
interpretácia  
model  
schéma usudzovania  
adícia  
simplifikácia

inverzia implikácie  
reductio ad absurdum  
strom odvodenia  
veta o dedukcii  
potvrdenie dôsledku  
popretie predpokladu  
predikátová logika  
konkretizácia univerzálneho kvantifikátora  
zovšeobecnenie pomocou univerzálneho kvantifikátora  
konkretizácia existenčného kvantifikátora  
zovšeobecnenie pomocou existenčného kvantifikátora  
induktívne zovšeobecnie  
falzifikácia  
priamy dôkaz  
nepriamy dôkaz

<i>konjunkcia</i>	<i>dôkaz sporom</i>
<i>modus ponens</i>	<i>dôkaz vymenovaním prípadov</i>
<i>modus tollens</i>	<i>F. Maurolico</i>
<i>hypotetický sylogizmus</i>	<i>G. Peano</i>
<i>disjunktívny sylogizmus</i>	<i>silná matematická indukcia</i>

## CVIČENIA

### 1.1. Aké pravidlo usudzovania bolo použité pri dôkaze záverov?

- Mária je študentka informatiky. Preto je Mária študentka informatiky alebo študentka telekomunikácií.
- Jaroslav študuje informatiku a elektrotechnológiu. Preto, Jaroslav študuje informatiku.
- Ak prší, potom plaváreň je zatvorená. Preto, ak plaváreň je otvorená, potom neprší.
- Ak dnes sneží, kino je dnes uzavreté. Kino dnes nie je uzavreté. Preto, dnes nesneží.
- Ak dnes pôjdem plávať, potom ráno skoro vstanem. Ak ráno skoro vstanem, potom pôjdem do obchodu kúpiť čerstvé pečivo. Preto, ak dnes pôjdem plávať, potom pôjdem do obchodu kúpiť čerstvé pečivo.

### 1.2. Aké pravidlo usudzovania bolo použité pri dôkaze záverov?

- Dnes bude teplo alebo bude smog v ovzduší. Dnes nebude teplo. Preto, dnes bude smog v ovzduší.
- Eva vynikajúco pláva. Ak Eva je vynikajúci plavec, potom môže pracovať ako plavčík. Preto, Eva môže pracovať ako plavčík.
- Stano bude pracovať v počítačovej firme ABC. Ak Stano dokončí štúdium na FIIT, potom nebude pracovať v počítačovej firme ABC. Preto, Stano nedokončil štúdium na FIIT.
- Ak budem intenzívne pracovať na projekte, potom zvládnem teóriu logických obvodov. Ak zvládnem teóriu logických obvodov, potom úspešne dokončím bakalárske štúdium. Preto, ak budem intenzívne pracovať na projekte, potom úspešne dokončím bakalárske štúdium.

### 1.3. Aké závery vyplývajú z množiny výrokov?

- „Ak jem korenenú stravu, potom mám hrozné sny“, „ak spím a pritom hrmí, potom mám hrozné sny“, „nemám hrozné sny“.
- „Ja som chytrý alebo mám šťastie“, „nemám šťastie“, „ak mám šťastie, potom zvíťazím v lotérii“.
- „Každý študent informatiky vlastní notebook“, „Rudo nevládni notebook“, „Anna vlastní notebook“.
- „Ak mám hlad, potom si kúpim bagetu“, „ak si kúpim bagetu, potom si kúpim aj kofolu“, „ak nepôjdem do bufetu, nekúpim si kofolu“.

- (e) „Všetky hlodavce hryzú potravu“, „myš je hlodavec“, „pes nehryzie potravu“, „netopier nie je hlodavec“.

**1.4.** Vysvetlite, ktorá schéma usudzovania bola použitá v ktorom kroku.

- (a) „Eva je študentka nášho krúžku a vlastní červené auto“, „každý, kto vlastní červené auto dostal aspoň jednu pokutu za prekročenie rýchlosti“, „preto, niekto z nášho krúžku dostal pokutu za prekročenie rýchlosti“.
- (b) „Všetci moji priatelia Mária, Adolf, Rudolf, Viera a Karol si zapísali do indexu prednášku z diskkrétnej matematiky“, „každý študent, ktorý si zapísal do indexu prednášku z diskkrétnej matematiky, môže si nasledujúci akademický rok zapísať aj prednášku z algoritmov“, „preto, všetci moji priatelia Mária, Adolf, Rudolf, Viera a Karol môžu si nasledujúci akademický rok zapísať do indexu prednášku z algoritmov“.
- (c) „Všetky filmy s Charlie Chaplinom sú vynikajúce“, „Charlie Chaplin hral v nemých filmoch“, „preto, niektoré vynikajúce filmy sú nemé“.

**1.5.** Vysvetlite prečo uvedené závery sú korektné alebo nekorektné.

- (a) „Všetci študenti v tomto krúžku ovládajú logiku“, „Jano je študent tohto krúžku“, „preto, Jano ovláda logiku“.
- (b) „Každý študent informatiky má zapísanú v indexe prednášku z diskkrétnej matematiky“, „Viera má zapísanú prednášku z diskkrétnej matematiky“, „preto, Viera je študentom informatiky“.
- (c) „Každý kôň má rád ovocie“, „môj pes nie je kôň“, „preto, môj pes nemá rád ovocie“.
- (d) „Každý, kto má rád ovsené vločky je zdravý“, „Lenka nie je zdravá“, „preto, Lenka nemá rada ovsené vločky“.

**1.6.** Určite, ktorá veta je pravdivá. Ak je uvedený záver korektný, určite, ktorá schéma usudzovania bola použitá pri jeho dôkaze.

- (a) Ak  $x$  je reálne číslo také, že  $x > 1$ , potom  $x^2 > 1$ . Predpokladajte, že  $x^2 > 1$ , potom  $x > 1$ .
- (b) Číslo  $\log_2 3$  je iracionálne vtedy, ak sa nedá vyjadriť ako podiel dvoch celých nesúdeliteľných čísel. Pretože číslo  $\log_2 3$  nie je vyjadriteľné ako  $p/q$ , kde  $p$  a  $q$  sú celé nesúdeliteľné čísla, potom je číslo  $\log_2 3$  iracionálne.
- (c) Ak  $x$  je reálne číslo, ktoré spĺňa podmienku  $x > 3$ , potom  $x^2 > 9$ . Nech  $x^2 \leq 9$ , potom  $x \leq 3$ .
- (d) Ak  $x$  je reálne číslo, ktoré spĺňa podmienku  $x > 2$ , potom  $x^2 > 4$ . Nech  $x \leq 2$ , potom  $x^2 \leq 4$ .

**1.7.** Určite, či uvedené výroky sú korektné, ak nie, prečo?

- (a) Ak  $x^2$  je iracionálne, potom  $x$  je iracionálne. Preto, ak  $x$  je iracionálne, potom  $x^2$  je iracionálne.

- (b) Ak  $x^2$  je iracionálne, potom  $x$  je iracionálne. Číslo  $x = \pi^2$  je iracionálne. Preto, číslo  $x = \pi$  je iracionálne.

**1.8.** Prečo tieto výroky sú nekorektné?

- (a) Nech  $H(x)$  je predikát s významom „ $x$  je šťastný“. Nech platí  $\exists x H(x)$ . Preto, Eva je šťastná.
- (b) Nech  $S(x, y)$  je predikát s významom „ $x$  je menší ako  $y$ “. Platí implikácia  $(\exists s S(s, Max)) \Rightarrow S(Max, Max)$ , kde  $Max$  je maximálne číslo z konečnej viacprvkovej množiny obsahujúcej prirodzené čísla.

**1.9.** Dokážte, keď sa dajú dokázať, tieto výroky:

- (a) Dokážte výrok  $P(0)$ , kde  $P(n)$  je výrok „ak  $n$  je kladné celé číslo väčšie ako 1, potom  $n^2 > n$ “. Ktorú schému usudzovania sme použili?
- (b) Dokážte výrok  $P(1)$ , kde  $P(n)$  je výrok „ak  $n$  je kladné celé číslo, potom  $n^2 > n$ “. Ktorú schému usudzovania sme použili?
- (c) Nech  $P(n)$  je výrok „ak  $a$  a  $b$  sú kladné reálne čísla, potom  $(a + b)^n \geq a^n + b^n$ “. Dokážte, že  $P(1)$  je pravdivý výrok.
- (d) Použitím priameho dôkazu dokážte, že kvadrát párneho čísla je párne číslo.
- (e) Použitím nepriameho dôkazu dokážte, že ak  $n$  je celé číslo a  $n^3 + 5$  je nepárne číslo, potom  $n$  je párne číslo.
- (f) Dokážte, že suma dvoch nepárnych čísel je párne číslo.
- (g) Dokážte, že súčin dvoch nepárnych čísel je nepárne číslo.
- (h) Dokážte, že ak  $x$  je iracionálne nenulové číslo, potom  $1/x$  je iracionálne číslo.

**1.10.** Dokážte metódou vymenovania prípadov tieto vlastnosti:

- (a)  $\max\{x, y\} + \min\{x, y\} = x + y$ , kde  $x, y$  sú reálne čísla.
- (b)  $\min\{a, \min\{b, c\}\} = \min\{\min\{a, b\}, c\}$ , kde  $a, b, c$  sú navzájom rôzne čísla a  $a < c$ .
- (c) Kvadráty celých čísel sú reprezentované dekadickými číslicami, ktoré končia 0, 1, 4, 5, 6, alebo 9.
- (d) Štvrté mocniny celých čísel sú reprezentované dekadickými číslami, ktoré končia 0, 1, 5, alebo 6.

**1.11.** Dokážte tieto vlastnosti:

- (a) Ak  $n$  je kladné celé číslo, potom  $n$  je párne vtedy a len vtedy, ak  $7n + 4$  je párne.
- (b) Ak  $n$  je kladné celé číslo, potom  $n$  je nepárne vtedy a len vtedy, ak  $5n + 6$  je nepárne.
- (c)  $m^2 = n^2$  platí vtedy a len vtedy, ak  $m = n$ , alebo  $m = -n$ .

- (d) Dokážte, že tieto tri výroky sú ekvivalentné: (1)  $a < b$ , (2) priemer  $a$  a  $b$  je väčší ako  $a$ ,  $(a+b)/2 > a$ , (3) priemer  $a$  a  $b$  je menší ako  $b$ ,  $(a+b)/2 < b$ .

**1.12.** Pomocou matematickej indukcie dokážte:

- (a) Suma prvých  $n$  prirodzených čísel je

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

- (b) Dokážte formulu

$$3 + 3 \cdot 5 + 3 \cdot 5^2 + \dots + 3 \cdot 5^n = \frac{1}{4}(5^{n+1} - 1)$$

- (c) Dokážte formulu

$$1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{1}{6}n(n+1)(2n+1)$$

- (d) Dokážte formulu

$$1^3 + 2^3 + 3^3 + \dots + n^3 = \frac{1}{4}n^2(n+1)^2$$

- (e) Dokážte formulu  $n! < n^n$ , pre  $n > 1$ .

- (f) Dokážte formulu pre prvú deriváciu funkcie  $f(x) = x^n$ ,  $f'(x) = nx^{n-1}$ .

- (g) Dokážte zovšeobecnené distributívne formuly z výrokovej logiky

$$(1) (p_1 \vee p_2 \vee \dots \vee p_n) \wedge q \equiv (p_1 \wedge q) \vee (p_2 \wedge q) \vee \dots \vee (p_n \wedge q)$$

$$(2) (p_1 \wedge p_2 \wedge \dots \wedge p_n) \vee q \equiv (p_1 \vee q) \wedge (p_2 \vee q) \wedge \dots \wedge (p_n \vee q)$$

- (h) Dokážte zovšeobecnené De Morganove formuly

$$(1) \neg(p_1 \wedge p_2 \wedge \dots \wedge p_n) \equiv (\neg p_1 \vee \neg p_2 \vee \dots \vee \neg p_n)$$

$$(2) \neg(p_1 \vee p_2 \vee \dots \vee p_n) \equiv (\neg p_1 \wedge \neg p_2 \wedge \dots \wedge \neg p_n)$$

**1.13.** Pomocou rozkladu na parciálne zlomky nájdite formulu pre

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \dots + \frac{1}{n(n+1)}$$



## 2 TEÓRIA MNOŽÍN I

MNOŽINA • OPERÁCIE NAD MNOŽINAMI •  
MNOŽINOVÁ ALGEBRA • MOHUTNOSŤ A ENUMERÁCIA •  
KARTEZIÁNSKY SÚČIN

*V tejto kapitole budeme študovať klasickú teóriu množín, ktorá patrí medzi základné matematické formálne prostriedky. Umožňuje formulovať prehľadným a jednotným spôsobom všetky oblasti matematiky prostredníctvom elementárnej štruktúry množiny a operáciami nad ňou. Teória množín vznikla koncom 19. storočia hlavne zásluhou nemeckého matematika Georga Cantora (1845 – 1918). Zásluhu na jej rozšírení má anglický logik a filozof Bertrand Russell (1872 – 1970), ktorý objavil vnútorné nekonzistentnosti jej intuitívnej formulácie, ktoré boli neskôr prekonané jej dôslednou axiomatickou výstavbou. V tejto kapitole budeme prezentovať pôvodnú intuitívnu (neaxiomatickú) výstavbu teórie množín. Budeme sa zaoberať algebrou teórie množín, problémom enumerácie elementov v množinách a na záver budeme špecifikovať dôležité množinové štruktúry – binárne relácie nad množinami.*

### 2.1 DEFINÍCIA MNOŽINY

---

CANTOR – VZNIK  
RUSSELL –  
AXIOMATICKÁ  
VÝSTAVBA

Koncepcia množiny patrí medzi základné formálne prostriedky matematiky. Umožňuje formulovať prehľadným a jednotným spôsobom všetky oblasti matematiky prostredníctvom elementárnej štruktúry množiny a operáciami nad ňou. Teória množín vznikla koncom 19. storočia hlavne zásluhou nemeckého matematika Georga Cantora (1845 – 1918). Zásluhu na jej rozšírení má anglický logik a filozof Bertrand Russell (1872 – 1970), ktorý objavil vnútorné nekonzistentnosti jej intuitívnej formulácie, ktoré boli neskôr prekonané jej dôslednou axiomatickou výstavbou. V tejto kapitole budeme prezentovať pôvodnú intuitívnu (neaxiomatickú) výstavbu teórie množín.

PRVOK (ELEMENT)

Elementárnym pojmom teórie množín je *prvok (element)*, pod ktorým budeme rozumieť nejaký reálny alebo abstraktný objekt, pričom postulujeme, že objekty medzi sebou sú dobre odlišiteľné.

**DEFINÍCIA 2.1.**MNOŽINA 

Množina je neusporiadaný súbor prvkov.

ODLIŠITELNÉ  
PRVKY

Ak sa nejaké dva prvky nachádzajú v tej istej množine, potom musia byť od seba odlišiteľné; v množine sa neopakuje výskyt dvoch rovnakých (neodlišiteľných) prvkov. V definícii množiny bol použitý elementárny pojem „súbor“, ktorý nebudeme bližšie špecifikovať. Pozorný čitateľ môže namietat', že pojem „súbor“ je vlastne len iný názov pre množinu. Táto skutočnosť naznačuje „osud“ všetkých definícií, pomocou ktorých špecifikujeme nové pojmy prostredníctvom iných elementárnych a intuitívne zrozumiteľných pojmov. Ak by sme pristúpili aj k špecifikácii elementárnych pojmov vyskytujúcich sa v definícii, potom by sme dospeli k nekonečnej rekurzii (opakovaniu) v definíciách, ktoré by takto stratili praktický význam a stali by sa bezcennými formálnymi prostriedkami.

 $a \in A$ 

Označme množinu písmenom  $A$ , potom skutočnosť, že prvok  $a$  *patrí* (*nepatrí*) do tejto množiny označíme výrazom  $a \in A$  ( $a \notin A$ ). Tento výraz chápeme ako výrok, ktorý je pravdivý (nepravdivý), ak prvok  $a$  patrí (nepatrí) do množiny  $A$ . Poznamenajme, že symbol  $\notin$  môžeme formálne definovať takto:  $x \notin A =_{def} \neg(x \in A)$ .

VYMENOVANIE A  
PREDIKÁT

Množinu môžeme špecifikovať dvoma rôznymi spôsobmi: **Prvý** spôsob určenia množiny je založený na **vymenovaní** všetkých prvkov, ktoré do nej patria

$$A = \{a, b, \dots, u\} \quad (2.1a)$$

Tento spôsob je vhodný len na špecifikácie množín, ktoré obsahujú konečný počet prvkov. Ak by sme takýmto spôsobom chceli napríklad definovať množinu párnych prirodzených čísel, potom tento spôsob je nepoužiteľný, pretože párnych prirodzených čísel je nekonečne mnoho. **Druhý** spôsob špecifikácie množiny je založený na použití **predikátu**  $P(x)$ , ktorý určuje, či prvok  $x \in U$  patrí do množiny  $A$  (predikát  $P(x)$  je pravdivý) alebo nepatrí do množiny  $A$  (predikát  $P(x)$  je nepravdivý)

$$A = \{x \in U; P(x)\} \quad (2.1b)$$

Tak napríklad, množina obsahujúca párne nezáporné celé čísla je definovaná takto

$$A = \{n \in U; P(n)\}$$

kde  $n$  sú nezáporné celé čísla z univerza  $U = \{0, 1, 2, \dots\}$  a predikát  $P(n)$  je špecifikovaný rovnosťou  $P(n) =_{def} \exists k (n = 2k)$ , kde  $k$  je nezáporné celé číslo, alebo

$$P(n) = \begin{cases} \text{pravda, } 1 & (n \text{ je párne číslo}) \\ \text{nepravda, } 0 & (n \text{ je nepárne číslo}) \end{cases}$$

Uvedený druhý spôsob špecifikácie množiny môže byť jednoducho pretransformovaný na koncepciu **charakteristických funkcií**. V tomto prístupe predikát  $P(x)$  z (2.1b) je určený takto



CHARAKTERIS-  
TICKÁ FUNKCIA

$$P(x) \stackrel{\text{def}}{=} (\mu_A(x) = 1) \quad (2.2)$$

kde

$$\mu_A(x) = \begin{cases} 1 & (x \in A) \\ 0 & (x \notin A) \end{cases} \quad (2.3)$$

UNIVERZUM  $U$ 

Pristúpme teraz k podrobnejšej diskusii špecifikácie množiny pomocou charakteristickej funkcie. Uvažujme **univerzum**  $U$ , nad ktorým sú definované všetky ostatné množiny.

**DEFINÍCIA 2.2.**MNOŽINA  
POMOCOU  
CHARAKTERIS-  
TICKEJ FUNKCIE

Každá množina  $A$  je pomocou charakteristickej funkcie vyjadrená takto

$$A = \{x \in U ; \mu_A(x) = 1\} \quad (2.4)$$

kde **charakteristická funkcia**  $\mu_A(x)$  je zobrazenie

$$\mu_A : U \rightarrow \{0,1\} \quad (2.5)$$

ktoré binárne ohodnocuje každý prvok  $x$  univerza  $U$  binárnym číslom  $\mu_A(x) \in \{0,1\}$ , ktoré vyhovuje vlastnosti (2.3).

PRÁZDNA  
MNOŽINA  $\emptyset$   
UNIVERZÁLNA  
MNOŽINA  $U$ 

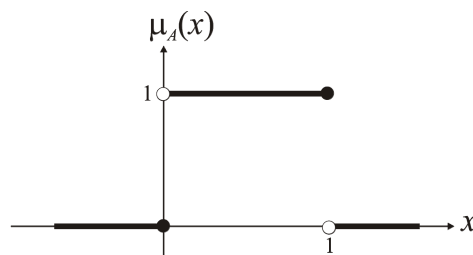
Pomocou charakteristickej funkcie môžeme definovať aj dve špeciálne množiny: **prázdnu množinu**  $\emptyset$ , ktorá nemá žiaden prvok,  $\emptyset = \{x ; \mu_\emptyset(x) = 0\}$  a **univerzálnu množinu**  $U$ ,  $U = \{x ; \mu_U(x) = 1\}$ , ktorá je totožná s univerzom.

**PRÍKLAD 2.1.**

Vyjadrite množinu – polootvorený interval  $A = (0,1]$  pomocou charakteristickej funkcie. V tomto prípade univerzum  $U$  je totožné s množinou reálnych čísel  $R$ . Charakteristická funkcia  $\mu_A(x)$  je definovaná takto

$$\mu_A(x) = \begin{cases} 1 & (\text{pre } 0 < x \leq 1) \\ 0 & (\text{ináč}) \end{cases}$$

Grafické znázornenie tejto charakteristickej funkcie je na obr. 2.1.

**OBRÁZOK 2.1.**  
CHARAKTERIS-  
TICKÁ FUNKCIA

Charakteristická funkcia množiny  $A$ , ktorá je určená ako polootvorený interval  $A = (0,1]$ .

Pomocou charakteristických funkcií môžeme definovať operácie nad množinami:

**DEFINÍCIA 2.3.**
 $A = B$ 

Hovoríme, že množina  $A = \{x ; \mu_A(x) = 1\}$  sa **rovná** množine  $B = \{x ; \mu_B(x) = 1\}$ ,  $A = B$ , vtedy a len vtedy, ak tieto množiny sú definované

nad rovnakým univerzom  $U$  a charakteristické funkcie oboch množín sú rovnaké

$$(A = B) =_{def} \forall (x \in U) (\mu_A(x) = \mu_B(x)) \quad (2.6a)$$

Alternatívna definícia vzťahu rovnosti medzi množinami  $A$  a  $B$  je

$$\begin{aligned} (A = B) &=_{def} \forall (x \in U) ((x \in A) \equiv (x \in B)) \\ &=_{def} \forall (x \in U) ((x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)) \end{aligned} \quad (2.6b)$$

**DEFINÍCIA 2.4.**



$A \subseteq B$

Hovoríme, že množina  $A = \{x; \mu_A(x) = 1\}$  je podmnožinou množiny  $B = \{x; \mu_B(x) = 1\}$ , čo píšeme  $A \subseteq B$ , vtedy a len vtedy, ak každý prvok z množiny  $A$  patrí aj do množiny  $B$

$$A \subseteq B =_{def} \forall (x \in U) ((\mu_A(x) = 1) \Rightarrow (\mu_B(x) = 1)) \quad (2.7a)$$

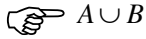
VLASTNÁ  
PODMNOŽINA  
 $A \subset B$

Alternatívna definícia podmnožiny je

$$A \subseteq B =_{def} \forall (x \in U) ((x \in A) \Rightarrow (x \in B)) \quad (2.7b)$$

V prípade, že  $A \neq B$ , potom formula  $A \subseteq B$  sa prepíše do tvaru  $A \subset B$ . Hovoríme, že  $A$  je **vlastnou podmnožinou**  $B$ , ak  $A \subset B$  a  $A \neq \emptyset$ . Rovnosť medzi množinami  $A = B$  platí vtedy a len vtedy, ak  $(A \subseteq B) \wedge (B \subseteq A)$ .

**DEFINÍCIA 2.5.**



$A \cup B$

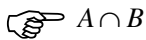
Hovoríme, že množina  $A \cup B$  je **zjednotenie množín**  $A$  a  $B$ , vtedy a len vtedy, ak

$$A \cup B =_{def} \{x; (x \in A) \vee (x \in B)\} = \{x; \mu_{A \cup B}(x) = 1\} \quad (2.8a)$$

kde

$$\mu_{A \cup B}(x) = \max\{\mu_A(x), \mu_B(x)\} \quad (2.8b)$$

**DEFINÍCIA 2.6.**



$A \cap B$

Hovoríme, že množina  $A \cap B$  je **prienik množín**  $A$  a  $B$ , vtedy a len vtedy, ak

$$A \cap B =_{def} \{x; (x \in A) \wedge (x \in B)\} = \{x; \mu_{A \cap B}(x) = 1\} \quad (2.9a)$$

kde

$$\mu_{A \cap B}(x) = \min\{\mu_A(x), \mu_B(x)\} \quad (2.9b)$$

**DEFINÍCIA 2.7.**



$\bar{A}$

Hovoríme, že množina  $\bar{A}$  je **doplňok (komplement)** množiny  $A$  (vzhľadom k univerzu  $U$ ), vtedy a len vtedy, ak

$$\bar{A} =_{def} \{x; x \notin A\} = \{x; \mu_{\bar{A}}(x) = 1\} \quad (2.10a)$$

kde

$$\mu_{\bar{A}}(x) = 1 - \mu_A(x) \quad (2.10b)$$

Poznamenajme, že platí jednoduchá ekvivalencia  $(x \notin A) \equiv (x \in \bar{A})$ , t. j. prvok  $x$  nie je z množiny  $A$  práve vtedy a len vtedy, ak patrí do komplementu  $\bar{A}$ .

**DEFINÍCIA 2.8.**

Hovoríme, že množina  $A - B$  (alebo  $A \setminus B$ ) je **rozdiel množín (relatívny doplňok množín)**  $A$  a  $B$ , vtedy a len vtedy, ak

$$A - B =_{def} \{x; (x \in A) \wedge (x \notin B)\} = \{x; \mu_{A-B}(x) = 1\} \quad (2.11a)$$

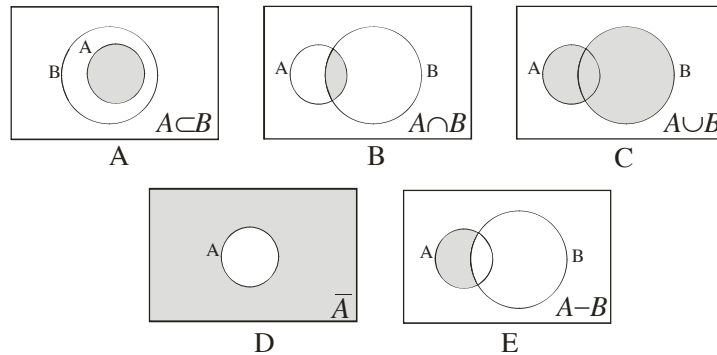
☞  $A \setminus B$

kde

$$\mu_{A-B}(x) = \min\{\mu_A(x), 1 - \mu_B(x)\} \quad (2.11b)$$

Takto definované operácie nad množinou  $U$  sú znázornené pomocou Vennových<sup>1</sup> diagramov (pozri obr. 2.2), ktoré reprezentujú rozšírený spôsob vizualizácie množinových operácií a ich formúl.

**OBRÁZOK 2.2.**  
OPERÁCIE NAD  
MNOŽINAMI  
POMOCOU  
VENNOVÝCH  
DIAGRAMOV



Znázornenie základných operácií nad množinami pomocou Vennových diagramov. Na týchto diagramoch obdĺžniková oblasť znázorňuje univerzum  $U$ , kde množiny  $A$  a  $B$  sú podmnožiny univerza. Diagram A znázorňuje reláciu „podmnožina“  $A \subset B$ , keď množina – oblasť  $A$  celá leží v množine – oblasti  $B$ . Diagram B znázorňuje operáciu „priek“  $A \cap B$ , kde vyšrafovaná oblasť reprezentuje priek množín  $A$  a  $B$ . Porovnaním diagramov A a B zistíme, že ak  $A \subset B$ , potom  $A \cap B = A$ . Diagram C znázorňuje operáciu zjednotenia množín  $A$  a  $B$ , vyšrafovaná je oblasť, ktorá sa nachádza v množine  $A$  alebo v množine  $B$ . Diagram D znázorňuje operáciu doplnok množiny  $A$  vzhľadom na univerzum  $U$ . Diagram E znázorňuje rozdiel množín  $A$  a  $B$ , vyšrafovaná je oblasť, ktorá sa nachádza v  $A$  a súčasne sa nenachádza v  $B$ .

Tab. 2.1 obsahuje základné formuly pre množinové operácie, ktoré tvoria tzv. **algebru teórie množín**. Každá formula z tejto tabuľky má pomerne jednoduchú vizualizáciu pomocou Vennových diagramov, ktoré v mnohých textoch o teórii množín slúžia aj ako podklad pre dôkaz ich korektnosti, pozri obr. 2.3.

☞

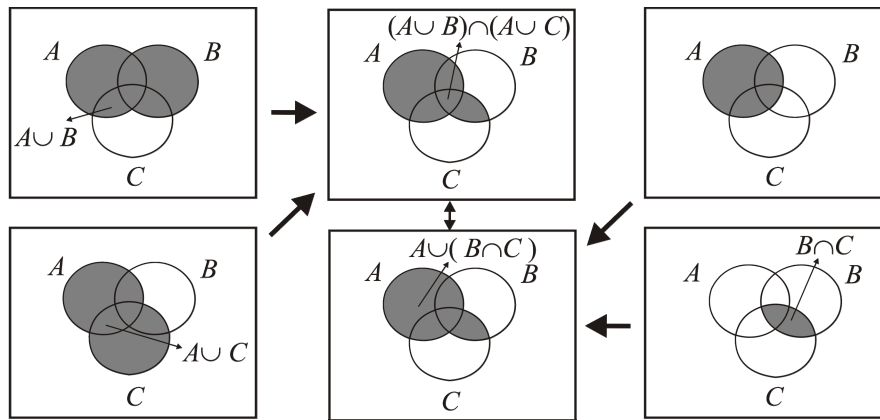
**Tabuľka 2.1.** Formuly teórie množín

vlastnosť	formula teórie množín
komutatívnosť	$A \cap B = B \cap A$ $A \cup B = B \cup A$
asociatívnosť	$A \cap (B \cap C) = (A \cap B) \cap C$ $A \cup (B \cup C) = (A \cup B) \cup C$
distributívnosť	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

<sup>1</sup> John Venn (1834–1923) je anglický matematik, ktorý sa zaslúžil o ďalší rozvoj Boolových algebraických snáh formalizovať výrokovú logiku.

De Morganove vzťahy	$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$
idempotentnosť	$A \cap A = A, A \cup A = A$
identita	$A \cap U = A, A \cup \emptyset = A$
dominancia	$A \cap \emptyset = \emptyset, A \cup U = U$
absorpcia	$A \cup (A \cap B) = A, A \cap (A \cup B) = A$
involúcia	$\overline{\overline{A}} = A$
zákon vylúčenia tretieho	$A \cup \overline{A} = U$
zákon sporu	$A \cap \overline{A} = \emptyset$
rozdiel množín	$A - B = A \cap \overline{B}$
distributívne zákony pre rozdiel	$A \cap (B - C) = (A \cap B) - (\overline{A} \cup C)$ $A \cup (B - C) = (A \cup B) - (\overline{A} \cap C)$

**OBRÁZOK 2.3.**  
VERIFIKÁCIA  
KOREKTNOSTI  
FORMULY  
 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$



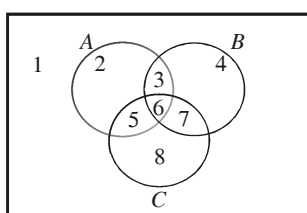
Verifikácia korektnosti formuly  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ . Prostredný Vennov diagram je zostrojený dvoma rôznymi nezávislými spôsobmi, v oboch prípadoch dostávame ten istý výsledok.

Na obr. 2.3 je znázornená pomocou Vennových diagramov verifikácia formuly  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ . Ľavá a pravá strana tejto formuly reprezentujú rôzne prístupy ku konštrukcii Vennovho diagramu, v oboch prípadoch dostávame ten istý výsledok, čiže verifikovaná formula je korektná. Tento postup môžeme „algebraizovať“ podobným štýlom, ako sa počítajú pravdivostné hodnoty formúl výrokovej logiky. Na obr. 2.4 je označených 8 oblastí univerza  $U$ , ktoré buď ležia alebo neležia v množinách  $A, B$  a  $C$ . Tak napr. oblasť 5 je taká, že existuje prvok, ktorý sa súčasne nachádza v množinách  $A$  a  $C$ , a nenachádza sa v množine  $B$ . Formula je korektná vtedy a len vtedy, ak pre každú oblasť obe strany formuly dávajú rovnaký výsledok, pozri tab. 2.2. V tejto tabuľke je každý riadok priradený jednej z ôsmich oblastí na obr. 2.4. Binárne hodnoty v jednotlivých riadkoch reprezentujú skutočnosť, či pre danú oblasť existuje

PRINCÍP  
KOMPOZICIONA-  
LITY

taký prvok, ktorý je v oblasti špecifikujúcej daný stĺpec. Tak napríklad, ôsmy stĺpec v tabuľke 2.2 obsahuje binárne hodnoty, ktoré špecifikujú, či  $A \cup B$  a  $A \cup C$  obsahujú spoločný prvok. Pri vytváraní tabuľky platí *princíp kompozicionality*, t. j. ohodnotenie zložitejších výrazov je vytvárané pomocou ich jednoduchších zložiek.

OBRÁZOK 2.4.  
OBLASTI V  
MNOŽINE UNIVERZA



Vyznačenie jednotlivých oblastí v množine univerza  $U$ . Oblasť 1 obsahuje prvky, ktoré nie sú obsiahnuté v množinách  $A$ ,  $B$  a  $C$ . Oblasť 2 obsahuje prvky, ktoré sú obsiahnuté v množine  $A$ , ale nie sú obsiahnuté v množinách  $B$  a  $C$ . Podobným spôsobom môžu byť charakterizované ostatné oblasti 3, 4, ..., 8.

TABUĽKOVÁ  
METÓDA PRE  
VERIFIKÁCIU

Tabuľka 2.2. Tabuľková metóda pre verifikáciu formúl teórie množín

oblasť	$A$	$B$	$C$	$A \cup B$	$A \cup C$	$B \cap C$	$(A \cup B) \cap (A \cup C)$	$A \cup (B \cap C)$
1	0	0	0	0	0	0	0	0
2	1	0	0	1	1	0	1	1
3	1	1	0	1	1	0	1	1
4	0	1	0	1	0	0	0	0
5	1	0	1	1	1	0	1	1
6	1	1	1	1	1	1	1	1
7	0	1	1	1	1	1	1	1

PRÍKLAD 2.2.

Pomocou tabuľkovej metódy verifikujte korektnosť De Morganových formúl  $\overline{(A \cup B)} = \bar{A} \cap \bar{B}$  a  $\overline{(A \cap B)} = \bar{A} \cup \bar{B}$ .

$A$	$B$	$A \cup B$	$\bar{A}$	$\bar{B}$	$A \cap B$	$\overline{A \cup B}$	$\bar{A} \cap \bar{B}$	$\overline{A \cap B}$	$\bar{A} \cup \bar{B}$
0	0	0	1	1	0	1	1	1	1
0	1	1	1	0	0	0	0	1	1
1	0	1	0	1	0	0	0	1	1

PRÍKLAD 2.3.

Dokážte De Morganovu formulu  $\overline{(A \cup B)} = \bar{A} \cap \bar{B}$

$$\mu_{\overline{A \cup B}}(x) = 1 - \mu_{A \cup B}(x) = 1 - \max\{\mu_A(x), \mu_B(x)\} \quad (2.12a)$$

$$\mu_{\bar{A} \cap \bar{B}}(x) = \min\{1 - \mu_A(x), 1 - \mu_B(x)\} \quad (2.12b)$$

Použitím algebraickej identity<sup>2</sup>

<sup>2</sup> Ktorá sa jednoducho dokáže použitím metódy vymenovania prípadov z kapitoly 1.4.

$$1 - \max\{a, b\} = \min\{1 - a, 1 - b\}$$

dokážeme, že formuly (2.12a-b) sú totožné pre ľubovoľné charakteristické funkcie, čiže platí

$$\forall (x \in U) (\mu_{\overline{A \cup B}}(x) = \mu_{\overline{A} \cap \overline{B}}(x)) \quad (2.13)$$

Použitím podmienky (2.6a) dostaneme, že množiny  $\overline{(A \cup B)}$  a  $\overline{A} \cap \overline{B}$  sa navzájom rovnajú.

**PRÍKLAD 2.4.**

Dokážte distributívnu formulu  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ .

$$\begin{aligned} \mu_{A \cup (B \cap C)}(x) &= \max\{\mu_A(x), \mu_{B \cap C}(x)\} = \max\{\mu_A(x), \min\{\mu_B(x), \mu_C(x)\}\} \\ \mu_{(A \cup B) \cap (A \cup C)} &= \min\{\mu_{A \cup B}(x), \mu_{A \cup C}(x)\} \\ &= \min\{\max\{\mu_A(x), \mu_B(x)\}, \max\{\mu_A(x), \mu_C(x)\}\} \end{aligned}$$

Použitím algebraickej identity (pozri príklad 1.13)

$$\max\{a, \min\{b, c\}\} = \min\{\max\{a, b\}, \max\{a, c\}\}$$

dostaneme, že vyššie uvedené charakteristické funkcie sa rovnajú

$$\forall (x \in U) (\mu_{A \cup (B \cap C)}(x) = \mu_{(A \cup B) \cap (A \cup C)})$$

čiže sa rovnajú aj množiny, ktoré určujú,  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ .

**PRÍKLAD 2.5.**

Dokážte distributívne zákony pre rozdiel množín.

K dôkazu použijeme formulu z Tabuľky 2.1 pre rozdiel množín,  $A - B = A \cap \overline{B}$ . Pristúpime k dôkazu prvej formuly  $A \cap (B - C) = (A \cap B) - (\overline{A} \cup C)$ , upravíme jej ľavú a pravú stranu

$$A \cap (B - C) = A \cap (B \cap \overline{C}) = A \cap B \cap \overline{C}$$

$$(A \cap B) - (\overline{A} \cup C) = (A \cap B) \cap \overline{(\overline{A} \cup C)} = (A \cap B) \cap (A \cap \overline{C}) = A \cap B \cap \overline{C}$$

Týmto sme dokázali, že ľavá a pravá strana sú si rovné, čiže platí prvý distributívny zákon pre rozdiel množín. Úplne analogickým spôsobom dokážeme aj platnosť druhej formuly  $A \cup (B - C) = (A \cup B) - (\overline{A} \cap C)$ , pomocou vzťahu

$A - B = A \cap \overline{B}$  upravíme ľavú a pravú stranu

$$A \cup (B - C) = A \cup (B \cap \overline{C}) = (A \cup B) \cap (A \cup \overline{C})$$

$$(A \cup B) - (\overline{A} \cap C) = (A \cup B) \cap \overline{(\overline{A} \cap C)} = (A \cup B) \cap (A \cup \overline{C})$$

Podobne ako aj v predchádzajúcom dôkaze, ľavá a pravá strana sú si rovné, čiže platí aj druhý distributívny zákon pre rozdiel množín.

MOHUTNOSŤ  
(KARDINALITA)  $|A|$

Ak množina  $A$  je **konečná** (obsahuje konečný počet prvkov), potom jej **mohutnosť** (**kardinalita**), označená  $|A|$ , je počet prvkov, ktoré obsahuje. V prípade, že množina  $A$  nie je konečná, potom jej mohutnosť je nekonečná,  $|A| = \infty$ .

**PRÍKLAD 2.6.**

Aká je mohutnosť množín?

(a)  $A = \{x; x \text{ je celé číslo ohraničené } 1/8 < x < 17/2\}$ ,  $|A| = 8$ ,

(b)  $A = \{x; \sqrt{x} \text{ je celé číslo}\} = \{0, 1, 4, 9, 16, \dots\}$ ,  $|A| = \infty$ ,

(c)  $A = \{x; x^2 = 1 \text{ alebo } 2x^2 = 1\} = \{1, -1, 1/\sqrt{2}, -1/\sqrt{2}\}$ ,  $|A| = 4$ ,

(d)  $A = \{a, \{a, b\}, \{a, b, c\}\}$ ,  $|A| = 3$ ,

(e)  $A = \{a, \{a\}, \{\{a\}\}\}$ ,  $|A| = 3$ .

(f)  $A = \{1, 2, 3, 4, 5, 6\}$ ,  $B = \{-2, -1, 0, 1, 2\}$ ,  $|A - B| = 4$ .

## 2.2 ENUMERÁCIA PRVKOV V KONEČNÝCH MNOŽINÁCH


V rôznych aplikáciách teórie množín vystupuje do popredia problém enumerácie prvkov danej konečnej množiny, čiže aká je mohutnosť danej množiny. Poznamenajme, že v tejto kapitole sa budeme zaoberať len konečnými množinami. Nech  $A$  a  $B$  sú disjunktné množiny (ich prienik je prázdna množina,  $A \cap B = \emptyset$ ), potom mohutnosť ich zjednotenia je určená súčtom mohutností jednotlivých množín

$$|A \cup B| = |A| + |B| \quad (2.14a)$$

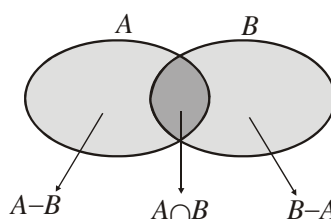
Tento výsledok môže byť jednoducho zovšeobecnený pomocou matematickej indukcie na mohutnosť zjednotenia  $n$  vzájomne disjunktných množín

$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n| \quad (2.14b)$$

Zovšeobecnenie formuly (2.14a) pre množiny, ktoré majú neprázdny prienik (ne-disjunktné množiny) je špecifikované vetou

**VETA 2.1.** Mohutnosť množiny  $A \cup B$  je určená formulou

$$|A \cup B| = |A| + |B| - |A \cap B| \quad (2.15)$$

**OBRÁZOK 2.5.**  
ROZKLAD MNOŽÍN

Rozklad množín  $A$  a  $B$  na tri disjunktné podmnožiny:  $A-B$ ,  $B-A$  a  $A \cap B$

## ROZKLAD MNOŽÍN

Formulu (2.15) ľahko dokážeme pomocou rozkladu množín  $A$  a  $B$  na disjunktné podmnožiny, pozri obr. 2.5, potom použitím (2.14) dostaneme

$$|A \cup B| = |A - B| + |B - A| + |A \cap B|$$

Mohutnosť samotných množín  $A$  a  $B$  je určená takto

$$|A| = |A - B| + |A \cap B|$$

$$|B| = |B - A| + |A \cap B|$$

Kombináciou týchto troch formúl dostaneme vzťah (2.15).

Podobne ako pre (2.14a), formula (2.15) môže byť zovšeobecnená pre mohutnosť zjednotenia 3 množín

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \quad (2.16)$$

Formulu (2.15) ľahko zovšeobecníme indukciou na

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{i=1}^n |A_i| - \sum_{\substack{i,j=1 \\ (i < j)}}^n |A_i \cap A_j| + \sum_{\substack{i,j,k=1 \\ (i < j < k)}}^n |A_i \cap A_j \cap A_k| + \dots \\ + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n| \quad (2.17)$$



### PRÍKLAD 2.7.

Každý zo 100 študentov Fakulty informatiky UGBM študuje aspoň jeden z týchto odborov: matematika, informatika a ekonómia. Nech  $U$  je množina všetkých študentov FI UGBM,  $M$  je množina študentov matematiky,  $I$  je množina študentov informatiky a  $E$  je množina študentov ekonómie. Počty študentov sú určené tabuľkou:

Študenti	symbol	počet
Všetci	$ U $	100
matematika	$ M $	65
informatika	$ I $	45
ekonómia	$ E $	42
matematika a informatika	$ M \cap I $	20
matematika a ekonómia	$ M \cap E $	25
informatika a ekonómia	$ I \cap E $	15

(i) Prvou úlohou je zistiť, koľko študentov súčasne študuje tri odbory,  $|M \cap I \cap E| = ?$

Použitím formuly (2.16) dostaneme

$$|U| = |M \cup I \cup E| = |M| + |I| + |E| - |M \cap I| - |M \cap E| - |I \cap E| + |M \cap I \cap E|$$

Táto formula nám špecifikuje počet študentov, ktorí súčasne študujú matematiku, informatiku a ekonómiu

$$100 = 65 + 45 + 42 - 20 - 25 - 15 + |M \cap I \cap E|$$

potom  $|M \cap I \cap E| = 8$ .

(ii) Druhou úlohou je zistiť, koľko študentov študuje matematiku a informatiku, ale nie ekonómiu,  $|M \cap I \cap \bar{E}| = ?$  Mohutnosť množiny  $M \cap I$  môžeme vyjadriť takto



$$|M \cap I| = |M \cap I \cap E| + |M \cap I \cap \bar{E}| \Rightarrow |M \cap I \cap \bar{E}| = -|M \cap I \cap E| + |M \cap I|$$

Použitím predchádzajúcich výsledkov dostaneme

$$|M \cap I \cap \bar{E}| = -|M \cap I \cap E| + |M \cap I| = 20 - 8 = 12.$$

(iii) Poslednou, treťou úlohou je zistiť, koľko študentov študuje len informatiku, ale nie matematiku a ekonómiu,  $|\bar{M} \cap I \cap \bar{E}| = ?$  Kardinalitu množiny  $I$  rozložíme na štyri časti

$$\begin{aligned} |I| &= |I \cap (M \cup \bar{M}) \cap (E \cup \bar{E})| = \\ &= |I \cap M \cap E| + |I \cap M \cap \bar{E}| + |I \cap \bar{M} \cap E| + |I \cap \bar{M} \cap \bar{E}| \end{aligned}$$

Platia tieto identity

$$\begin{aligned} |I \cap \bar{M} \cap E| &= |I \cap E| - |I \cap M \cap E| \\ |I \cap M \cap \bar{E}| &= |I \cap M| - |I \cap M \cap E| \end{aligned}$$

Dosadením týchto výsledkov do predošlého vzťahu dostaneme

$$|I| = -|I \cap M \cap E| + |I \cap E| + |I \cap M| + |I \cap \bar{M} \cap \bar{E}|$$

alebo

$$|I \cap \bar{M} \cap \bar{E}| = |I| + |I \cap M \cap E| - |I \cap E| - |I \cap M| = 45 + 8 - 15 - 20 = 18.$$

RUSSELL:

$$\begin{aligned} M &= \{A; A \notin A\} \\ M &\in M? \end{aligned}$$

AXIOMATIZÁCIA  
„RODINA MNOŽÍN“

Pojem množina môže byť zovšeobecnený tak, že prvky množiny môžu byť taktiež množiny (pozri príklad 2.6, zadanie d, e). Ak pristúpime na túto terminológiu, potom je korektný výrok „množina všetkých možných množín, ktoré neobsahujú samy seba ako prvky“. Označme túto množinu  $M$ , potom obsahuje také množiny  $A$  pre ktoré platí  $A \notin A$ , formálne  $M = \{A; A \notin A\}$ . Russell bol prvý, ktorý počiatkom 20. storočia poukázal na skutočnosť, že takto formulované výroky sú vnútorne rozporné. Položme si otázku, či táto množina obsahuje samu seba,  $M \in M$ ? Nech platí  $M \in M$ , potom podľa definície musí platiť  $M \notin M$ . Nech platí  $M \notin M$ , potom však z definície vyplýva taktiež  $M \in M$ . Tieto dva závery (implikácie) môžeme spojiť do jednej ekvivalencie,  $(M \in M) \equiv (M \notin M)$ , čo je evidentná kontradikcia. Russell navrhol prekonať túto vnútornú kontradikčnosť intuitívnej teórie množín tak, že pojem množina sa môže používať len na „prvej“ úrovni, t. j. keď prvkami tejto množiny sú prvky, ktoré nemajú svoju štruktúru. Na druhej úrovni používal termín „rodina množín“, jej prvky sú množiny z prvej úrovne. Na ďalšej tretej úrovni môžeme hovoriť o triede množín, jej prvky sú rodiny množín z predchádzajúcej druhej úrovne. Týmto spôsobom výrok „množina, ktorá obsahuje všetky možné množiny“ je nekorektný, jeho správna forma je „rodina všetkých možných množín“, potom už máme (hlavne zásluhou vhodnej terminológie) odstránený zmienený paradox, ktorý svojho času zohral fundamentálnu úlohu v teórii množín. Iný spôsob prekonania paradoxov Russellovho typu je dôsledná axiomatizácia teórie množín.

Nech  $I = \{1, 2, \dots, n\}$  je množina indexov, ktorá obsahuje prvých  $n$  kladných celých čísel. Predpokladajme, že pre každý index  $i \in I$  má definovanú množinu  $A_i$ ,

potom rodina množín je definovaná takto

$$\mathcal{A} = \{A_i; i \in I\} = \{A_1, A_2, \dots, A_n\} \quad (2.18)$$

Pre rodinu množín  $\mathcal{A}$  môžeme definovať operáciu prieniku a zjednotenia jej množín

$$\bigcap_{i \in I} A_i = A_1 \cap A_2 \cap \dots \cap A_n = \{x; x \in A_i, \text{ pre každé } i \in I\} \quad (2.19a)$$

$$\bigcup_{i \in I} A_i = A_1 \cup A_2 \cup \dots \cup A_n = \{x; x \in A_i, \text{ pre nejaké } i \in I\} \quad (2.19b)$$

### PRÍKLAD 2.8.

Nech  $I = R$ , t. j. množina indexov je totožná s množinou reálnych čísel a nech

$$A_k = \{(x, kx); x \in R\}$$

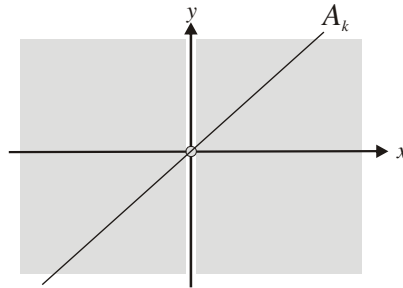
kde  $k \in R$ . Geometrická interpretácia množiny  $A_k$  je priamka so smernicou  $k$ , ktorá prechádza stredom súradnicového systému, pozri obr. 2.6. To znamená, že prienik množín  $A_k$  je jednoprvková množina, ktorá obsahuje stred súradnicového systému

$$\bigcap_{k \in R} A_k = \{(0, 0)\}$$

Zjednotenie týchto množín nám dáva celú rovinu bez osi  $o_y$ , doplnenú o stred súradnicového systému (pozri obr. 2.6)

$$\bigcup_{k \in R} A_k = \{(x, y); x, y \in R \text{ a } x \neq 0\} \cup \{(0, 0)\}$$

**OBRÁZOK 2.6.**  
GEOMETRICKÁ  
INTERPRETÁCIA  
MNOŽINY



Vytieňovaná oblasť znázorňuje zjednotenie všetkých množín  $A_k$ , ktoré reprezentuje celú rovinu, z ktorej je odstránená os  $o_y$ , plus počiatok súradnicového systému  $(0,0)$ . Množina  $A_k$  je reprezentovaná priamkou  $y=kx$ .

### DEFINÍCIA 2.9.

POTENČNÁ  
MNOŽINA

Množina  $\mathcal{P}(A)$  sa nazýva potenčná množina vzhľadom k množine (alebo jednoducho, množiny)  $A$  vtedy a len vtedy, ak obsahuje všetky možné podmnožiny množiny  $A$

$$\mathcal{P}(A) = \{B; B \subseteq A\} \quad (2.20)$$

Potenčná množina obsahuje prázdnu množinu  $\emptyset$  a taktiež aj množinu  $A$ , pretože obe tieto množiny sú podmnožinou množiny  $A$ . Vlastnosti potenčnej množiny sú určené vetou

### VELA 2.2.

Potenčná množina  $\mathcal{P}(A)$  spĺňa tieto vlastnosti

$$(A \subseteq B) \equiv (\mathcal{P}(A) \subseteq \mathcal{P}(B)) \quad (2.21a)$$

$$\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B) \quad (2.21b)$$

$$\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B) \quad (2.21c)$$

Dokážeme ekvivalenciu (2.21a), musíme dokázať dve nezávisle implikácie  $(A \subseteq B) \Rightarrow (\mathcal{P}(A) \subseteq \mathcal{P}(B))$  a  $(\mathcal{P}(A) \subseteq \mathcal{P}(B)) \Rightarrow (A \subseteq B)$ .

(1) Predpokladajme, že  $A \subseteq B$ , nech  $X \in \mathcal{P}(A)$ , potom  $X \subseteq A$ . Pretože predpokladáme platnosť  $A \subseteq B$ , potom musí platiť aj  $X \subseteq B$ , teda aj  $X \in \mathcal{P}(B)$ . Týmto sme dokázali, že z predpokladu  $A \subseteq B$  je odvoditeľná implikácia  $(X \in \mathcal{P}(A)) \Rightarrow (X \in \mathcal{P}(B))$ , z čoho priamo plynie  $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ .

(2) Predpokladajme, že  $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ , pretože  $A \in \mathcal{P}(A)$ , potom z predpokladu vyplýva, že musí platiť aj  $A \in \mathcal{P}(B)$ , čo je možné len vtedy, ak  $A \subseteq B$ .

Dôkaz vzťahu (2.21b) bude spočívať v dôkaze implikácie  $X \in (\mathcal{P}(A) \cup \mathcal{P}(B)) \Rightarrow X \in \mathcal{P}(A \cup B)$ . Predpokladajme  $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$ , potom

$$\begin{aligned} (X \in \mathcal{P}(A)) \vee (X \in \mathcal{P}(B)) &\Rightarrow (X \subseteq A) \vee (X \subseteq B) \Rightarrow \\ X \subseteq (A \cup B) &\Rightarrow X \in \mathcal{P}(A \cup B) \end{aligned}$$

Týmto sme dokázali  $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$ .

Dôkaz formuly (2.21c) je podobný poslednému dôkazu (v tomto prípade ide o množinovú rovnosť, t. j. musíme dokázať dve implikácie  $p \Rightarrow q$  a  $q \Rightarrow p$ ).

**PRÍKLAD 2.9.**

Niekoľko ilustračných príkladov potenčných množín:

(a)  $A = \emptyset$ ,  $\mathcal{P}(A) = \{\emptyset\}$ ,

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

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

(d)  $A = \{a, b, c\}$ ,  $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$ .

**PRÍKLAD 2.10.**

Pri práci s potenčnými množinami musíme veľmi starostlivo rozlišovať medzi symbolmi  $\in$  a  $\subseteq$ . Ak  $a \in A$ , potom  $\{a\} \subseteq A$  alebo  $\{a\} \in \mathcal{P}(A)$ . Študujme množinu  $A = \{1, 2, \{1\}\}$ , potom  $1 \in A$  a  $\{1\} \in A$ , preto  $\{1\} \in \mathcal{P}(A)$  a taktiež aj  $\{\{1\}\} \in \mathcal{P}(A)$ . Potenčná množina  $\mathcal{P}(A)$  je

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


Pripomínáme, že prvky 1,  $\{1\}$  a  $\{\{1\}\}$  sú rôzne. Prvý prvok z tejto trojice je číslo, druhý prvok je množina s jedným prvkom – číslom a tretí prvok je množina s jedným prvkom – množinou, ktorá obsahuje číslo 1.

Zostrojme postupnosť

$$1, \{1\}, \{\{1\}\}, \{\{\{1\}\}\}, \dots$$

každý prvok (s výnimkou prvého prvku) tejto postupnosti je množina, ktorá obsahuje predchádzajúci prvok. Táto vlastnosť rekurentnosti môže byť použitá na definíciu  $n$ -tého člena postupnosti

$$X_1 = 1 \quad \text{a} \quad X_{n+1} = \{X_n\}, \quad \text{pre } n = 1, 2, 3, \dots$$

**VETA 2.3.** 

Mohutnosť potenčnej množiny  $\mathcal{P}(A)$  konečnej množiny  $A$  je určená jednoduchým vzťahom

$$|\mathcal{P}(A)| = 2^{|A|} \quad (2.22)$$

Tento výsledok pre mohutnosť potenčnej množiny sa ľahko dokáže pomocou nasledujúcej úvahy: Nech konečná množina  $A$  obsahuje  $n$  prvkov,  $A = \{a_1, a_2, \dots, a_n\}$ , každá podmnožina  $A' \subseteq A$  môže byť charakterizovaná pomocou charakteristickej funkcie – binárneho vektora dĺžky  $n$ . Ak v  $i$ -tej polohe tohto vektora je 1 (0), potom  $a_i \in A'$  ( $a_i \notin A'$ ). To znamená, že každá podmnožina z potenčnej množiny  $\mathcal{P}(A)$  je jednoznačne špecifikovaná binárnym vektorom dĺžky  $n$ . Pretože v každej polohe binárneho vektora sú prípustné len dve hodnoty (1 a 0), potom celkový počet rôznych binárnych vektorov dĺžky  $n$  je  $2^n$ , toto číslo špecifikuje aj mohutnosť potenčnej množiny,  $|\mathcal{P}(A)| = 2^n$ , kde  $|A| = n$ . Tento jednoduchý výsledok viedol niektorých autorov k tomu, že potenčnú množinu označili symbolom  $2^A$ , jej mohutnosť sa rovná  $2^{|A|}$ .

## 2.3 KARTEZIÁNSKY SÚČIN MNOŽÍN

USPORIADANÉ  
DVOJICE PRVKOV

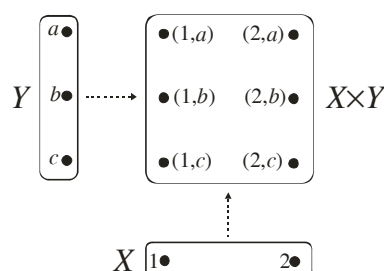
V mnohých matematických disciplínach alebo v ich aplikáciách vystupujú usporiadané dvojice prvkov. Tak napríklad, komplexné číslo môže byť charakterizované ako usporiadaná dvojica reálnych čísel  $z = (x, y)$ , kde  $x$  ( $y$ ) je reálna (komplexná) časť. Základná relácia pre usporiadané dvojice je rovnosť:  $(x, y) = (x', y')$ , ktorá platí vtedy a len vtedy, ak sú si rovné ich prvé a druhé časti,  $x = x'$  a  $y = y'$ . Táto podmienka rovnosti platí aj pre komplexné čísla, ktoré sú si rovné vtedy a len vtedy, ak sa rovnajú ich reálne a imaginárne časti. Ďalším ilustračným príkladom použitia usporiadanej dvojice v matematike je špecifikácia bodu ležiaceho v rovine, ktorý je taktiež plne určený usporiadanou dvojicou  $(x, y)$  svojich súradníc. Dva body (dve usporiadané dvojice)  $A = (x, y)$  a  $B = (x', y')$  sú rovné vtedy a len vtedy, ak sú rovné ich súradnice,  $x = x'$  a  $y = y'$ .

**DEFINÍCIA 2.10.**

Množina  $X \times Y$  sa nazýva **karteziánsky súčin**<sup>3</sup> dvoch množín  $X$  a  $Y$  vtedy a len vtedy, ak

$$X \times Y = \{(x, y); x \in X \text{ a } y \in Y\} \quad (2.23)$$

**OBRÁZOK 2.7.**  
KARTEZIÁNSKY  
SÚČIN POMOCOU  
VENNOVÝCH  
DIAGRAMOV



Znázornenie karteziánskeho súčinu pomocou Vennových diagramov.

V prípade, že  $X = Y$ , potom  $X \times X = X^2$ . Poznamenajme, že ak aspoň jedna z množín  $X$  alebo  $Y$  je prázdna množina, potom aj karteziánsky súčin  $X \times Y$  je prázdny. Ak množiny  $X$  a  $Y$  sú obe neprázdne, potom  $X \times Y = Y \times X$  vtedy a len vtedy, ak  $X = Y$  (táto vlastnosť je priamym dôsledkom podmienky rovnosti,  $(x, y) = (x', y')$ , medzi dvoma usporiadanými dvojicami).

**PRÍKLAD 2.11.**

Nech  $X = \{1, 2\}$  a  $Y = \{a, b, c\}$ , potom

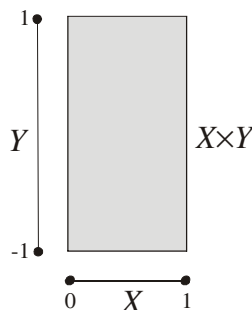
$$X \times Y = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$

reprezentácia tohto súčinu pomocou Vennovho diagramu je znázornená na obr. 2.7.

**PRÍKLAD 2.12.**

Nech  $X = [0, 1]$  a  $Y = [-1, 1]$  sú uzavreté intervaly reálnych čísel, karteziánsky súčin týchto dvoch intervalov môže byť znázornený pomocou obdĺžnika na obr. 2.8.

**OBRÁZOK 2.8.**  
KARTEZIÁNSKY  
SÚČIN DVOCH  
ÚSEČIEK

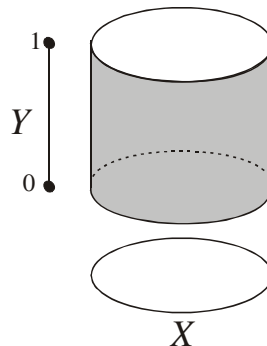


Znázornenie karteziánskeho súčinu dvoch úsečiek  $X$  a  $Y$ , výsledná oblasť je obdĺžnik.

<sup>3</sup> Pomenovanie je po francúzskom matematikovi a filozofovi René Descartesovi (1596 – 1650), ktorý sa pokladá za zakladateľa analytickej geometrie. Je tvorcom koncepcie ortogonálneho súradnicového systému, v ktorom je bod charakterizovaný usporiadanou dvojicou súradníc – reálnych čísel. Táto „matematizácia“ geometrie sa pokladá za jeden z najväčších úspechov matematiky 17. storočia, ktorý umožnil, okrem iného aj Leibnizovi zaviesť pojem derivácie funkcie ako smernicu dotyčnice ku grafu funkcie.

**PRÍKLAD 2.13.** Nech  $X = \{(x, y); x^2 + y^2 = 1\}$  je kružnica o polomere 1 so stredom v centre súradnicového systému a  $Y = [0, 1]$  je jednotková úsečka, karteziánsky súčin týchto dvoch oblastí produkuje povrch plášťa valca dĺžky 1 a s polomerom 1, pozri obr. 2.9.

**OBRÁZOK 2.9.**  
KARTEZIÁNSKY  
SÚČIN KRUŽNICE A  
ÚSEČKY



Znázornenie karteziánskeho súčinu kružnice  $X$  a úsečky  $Y$ , výsledná oblasť je valcová plocha.

KARTEZIÁNSKY  
SÚČIN PRE  $N$ -TICU

Koncepcia usporiadanej dvojice môže byť zovšeobecnená na usporiadanú  $n$ -ticu, pomocou karteziánskeho súčinu  $n$  množín. Hovoríme, že dve  $n$ -tice  $(x_1, x_2, \dots, x_n)$  a  $(x'_1, x'_2, \dots, x'_n)$  sa rovnajú vtedy a len vtedy, ak sú rovné ich zložky,  $x_1 = x'_1$ ,  $x_2 = x'_2$ , ...,  $x_n = x'_n$ .

**DEFINÍCIA 2.11.**  
KART. SÚČIN  $N$   
MNOŽÍN

Množina  $X_1 \times X_2 \times \dots \times X_n$  sa nazýva karteziánsky súčin  $n$  množín  $X_1, X_2, \dots, X_n$  vtedy a len vtedy, ak

$$X_1 \times X_2 \times \dots \times X_n = \{(x_1, x_2, \dots, x_n); x_1 \in X_1, x_2 \in X_2, \dots, x_n \in X_n\} \quad (2.24a)$$

Karteziánsky súčin môžeme taktiež vyjadriť symbolicky takto

$$X_1 \times X_2 \times \dots \times X_n = \prod_{i=1}^n X_i \quad (2.24b)$$

Ak všetky množiny z karteziánskeho súčinu sa rovnajú množine  $X$ , potom výraz  $X_1 \times X_2 \times \dots \times X_n$  je zjednodušený na  $X^n$ .


**PRÍKLAD 2.14.** Nech  $A = \{1, 2\}$ ,  $B = \{a, b\}$  a  $C = \{\alpha, \beta\}$ , potom karteziánsky súčin týchto množín má tvar

$$A \times B \times C = \{(1, a, \alpha), (1, a, \beta), (1, b, \alpha), (1, b, \beta), (2, a, \alpha), (2, a, \beta), (2, b, \alpha), (2, b, \beta)\}$$

**PRÍKLAD 2.15.** Nech  $X_1 = X_2 = \dots = X_n = R$ , kde  $R$  je množina reálnych čísel. Potom  $R^n$  je množina obsahujúca všetky  $n$ -tice reálnych čísel

$$R^n = \{(x_1, x_2, \dots, x_n); x_1, x_2, \dots, x_n \in R\}$$

a môže byť interpretovaná ako  **$n$ -rozmerný lineárny priestor**.

**VETA 2.4.** 


Mohutnosť karteziánskeho súčinu  $X \times Y$  dvoch konečných množín  $X$  a  $Y$  s mohutnosťami  $|X| = m$  a  $|Y| = n$ , sa rovná súčinu mohutností jeho zložiek

$$|X \times Y| = |X| \cdot |Y| = m \cdot n \quad (2.25a)$$

Tento výsledok môže byť jednoducho zovšeobecnený indukciou na  $n$ -násobný karteziánsky súčin konečných množín

$$|X_1 \times X_2 \times \dots \times X_n| = |X_1| \cdot |X_2| \cdot \dots \cdot |X_n| = m_1 \cdot m_2 \cdot \dots \cdot m_n \quad (2.25b)$$

kde  $m_i$  je mohutnosť množiny  $X_i$ .

**VETA 2.5.** 

Karteziánsky súčin množiny  $A$  s prienikom alebo zjednotením dvoch množín  $X$  a  $Y$  vyhovuje podmienkam distributívnosti

$$A \times (X \cap Y) = (A \times X) \cap (A \times Y) \quad (2.26a)$$

$$(X \cap Y) \times A = (X \times A) \cap (Y \times A) \quad (2.26b)$$

$$A \times (X \cup Y) = (A \times X) \cup (A \times Y) \quad (2.26c)$$

$$(X \cup Y) \times A = (X \times A) \cup (Y \times A) \quad (2.26d)$$


Dokážeme prvú rovnosť (2.26a), ostatné sa môžu dokázať analogickým spôsobom. Nech  $(a, x) \in A \times (X \cap Y)$ , potom  $a \in A$  a  $x \in (X \cap Y)$ . Z posledného výrazu vyplýva, že  $x$  sa súčasne vyskytuje v  $X$  a taktiež aj v  $Y$ . Potom  $(a, x) \in A \times X$  a taktiež aj  $(a, x) \in A \times Y$ , čiže  $(a, x) \in (A \times X) \cap (A \times Y)$ , čím sme dokázali  $A \times (X \cap Y) \subseteq (A \times X) \cap (A \times Y)$ . Predpokladajme, že  $(a, x) \in (A \times X) \cap (A \times Y)$ , potom  $(a, x) \in (A \times X)$  a  $(a, x) \in (A \times Y)$ . Tieto dva vzťahy môžeme prepísať takto:  $a \in A$  a  $x \in X \cap Y$ , alebo  $(a, x) \in A \times (X \cap Y)$ , čím sme dokázali  $(A \times X) \cap (A \times Y) \subseteq A \times (X \cap Y)$ . Spojením týchto dvoch relácií inklúzie dostaneme dokazovanú rovnosť  $A \times (X \cap Y) = (A \times X) \cap (A \times Y)$ , čo bolo potrebné dokázať.

**PRÍKLAD 2.16.**

Nech  $A = \{a, b, c\}$ ,  $X = \{x, y, z\}$  a  $Y = \{y, z, t\}$ .

$$\begin{aligned} A \times (X \cap Y) &= \{a, b, c\} \times (\{x, y, z\} \cap \{y, z, t\}) = \{a, b, c\} \times \{y, z\} \\ &= \{(a, y), (b, y), (c, y), (a, z), (b, z), (c, z)\} \\ (A \times X) \cap (A \times Y) &= (\{a, b, c\} \times \{x, y, z\}) \cap (\{a, b, c\} \times \{y, z, t\}) \\ &= \{(a, x), (a, y), (a, z), (b, x), (b, y), (b, z), (c, x), (c, y), (c, z)\} \cap \\ &\quad \{(a, y), (a, z), (a, t), (b, y), (b, z), (b, t), (c, y), (c, z), (c, t)\} \\ &= \{(a, y), (b, y), (c, y), (a, z), (b, z), (c, z)\} \end{aligned}$$

Ak porovnáme pravé strany oboch výrazov, dostaneme, že ľavé strany sú si rovné, t. j. platí (2.26a). Podobným spôsobom môžeme verifikovať formuly (2.26b-d).

**VETA 2.6.** 

Pre ľubovoľné tri množiny  $A, B$  a  $X$  platí implikácia

$$(A \subseteq B) \Rightarrow ((A \times X) \subseteq (B \times X)) \quad (2.27a)$$

Ak  $X$  je neprázdna množina, potom

$$((A \times X) \subseteq (B \times X)) \Rightarrow (A \subseteq B) \quad (2.27b)$$

Dôkaz tejto vety je pomerne jednoduchý, a preto ho prenecháme pozornému čitateľovi.

## 2.4 MNOŽINA AKO DÁTOVÁ ŠTRUKTÚRA V INFORMATIKE

### ALGORITMY TEÓRIE GRAFOV

V mnohých aplikáciách množinová dátová štruktúra podstatne uľahčuje implementáciu algoritmov, ktoré sú založené na formalizme teórie množín. Ako príklad takýchto algoritmov môže slúžiť teória grafov, ktorej jednoduchá a súčasne aj elegantná teória je založená na množinách. Mnohé algoritmy teórie grafov (napr. problém obchodného cestujúceho) patrí medzi základné algoritmy, preto je dôležité, hlavne z pedagogických dôvodov, mať možnosť využívať dátovú štruktúru množiny pre zjednodušenie a sprehl'adnenie týchto algoritmov.

### CHARAKTERIS- TICKÁ BINÁRNA FUNKCIA

Základný prístup k implementácii dátovej štruktúry množiny je jej charakteristická binárna funkcia, ktorá môže byť reprezentovaná binárnym vektorom. Maximálna dĺžka tohto vektora (napr.  $2^8 = 256$ ) špecifikuje maximálnu mohutnosť implementovanej množiny. Pre jednoduchosť uvažujme binárne vektory dĺžky  $2^3 = 8$ , ktoré určujú množiny v rámci univerzálnej množiny  $U = \{1, 2, 3, 4, 5, 6, 7, 8\}$ . Tak napr. binárny vektor  $(11001100)$  špecifikuje množinu  $A = \{1, 2, 5, 6\}$ . Ak binárny vektor obsahuje len nuly, potom množina  $A = \emptyset$ ; v opačnom prípade, ak binárny vektor obsahuje len jednotky, potom  $A = U$ . Pomocou binárnych vektorov môžeme pomerne jednoducho vykonávať algebraické operácie nad množinami.

### OPERÁCIA ZJEDNOTENIA

(1) **Operácia zjednotenia** množín  $A$  a  $B$ ,  $C = A \cup B$ , ktoré sú reprezentované binárnymi vektormi

$$\mu_A = (a_1, a_2, \dots, a_n)$$

$$\mu_B = (b_1, b_2, \dots, b_n)$$

je realizovaná pomocou binárnej operácie 'disjunkcie'

$$\mu_{A \cup B} = (c_1, c_2, \dots, c_n) = (a_1, a_2, \dots, a_n) \vee (b_1, b_2, \dots, b_n)$$

kde

$$c_i = \max\{a_i, b_i\}$$

### OPERÁCIA PRIENIKU

(2) **Operácia prieniku** množín  $A$  a  $B$ ,  $C = A \cap B$ , je realizovaná pomocou binárnej operácie 'konjunkcie'



$$\mu_{A \cap B} = (c_1, c_2, \dots, c_n) = (a_1, a_2, \dots, a_n) \wedge (b_1, b_2, \dots, b_n)$$

kde

$$c_i = \min\{a_i, b_i\}$$

OPERÁCIA  
KOMPLEMENTU

(3) **Operácia komplementu** množiny  $A$ ,  $C = \bar{A}$ , je realizovaná pomocou unárnej operácie 'komplementu'

$$\mu_{\bar{A}} = (c_1, c_2, \dots, c_n) = (1 - a_1, 1 - a_2, \dots, 1 - a_n)$$

PRÍKLAD 2.17.

Definujme dva binárne vektory dĺžky 8 (t. j. univerzum  $U = \{1, 2, 3, 4, 5, 6, 7, 8\}$ )  $\mu_A = (11001111)$  a  $\mu_B = (00011001)$ , ktoré reprezentujú množiny  $A = \{1, 2, 5, 6, 7, 8\}$  a  $B = \{4, 5, 8\}$ . Nad množinami  $A$  a  $B$  vykonáme základné operácie pomocou binárnych operácií nad vektormi. Zjednotenie  $A \cup B$  je určené pomocou binárnej operácie 'disjunkcie'

$$(11001111) \vee (00011001) = (11011111)$$

Výsledný vektor špecifikuje množinu  $C = \{1, 2, 4, 5, 6, 7, 8\}$ . Podobným spôsobom môžeme vykonať aj operáciu prieniku  $A \cap B$  pomocou operácie 'konjunkcie' pre binárne vektory

$$(11001111) \wedge (00011001) = (00001001)$$

Výsledný vektor špecifikuje množinu  $C = \{5, 8\}$ . Komplementy  $\bar{A}$  a  $\bar{B}$  sú zostrojené pomocou operácie „negácie“ binárnych vektorov

$$\mu_{\bar{A}} = \neg(11001111) = (00110000)$$

$$\mu_{\bar{B}} = \neg(00011001) = (11100110)$$

Výsledné vektory reprezentujú množiny  $C = \bar{A} = \{3, 4\}$  a  $C = \bar{B} = \{1, 2, 3, 6, 7\}$ .

## ZHRNUTIE

MNOŽINA

Koncepcia množiny je najrozšírenejšia elementárna štruktúra matematiky. V intuitívnom prístupe je definovaná ako súbor prvkov, ktoré sú navzájom odlíšiteľné. Symbol  $x \in A$  čítame tak, že prvok  $a$  patrí do množiny  $A$ . Množina je špecifikovaná dvoma rôznymi spôsobmi: (1) vymenovaním všetkých jej prvkov a (2) pomocou charakteristickej funkcie. Nad množinami môžeme definovať reláciu rovnosti ( $A = B$ ) a inklúzie ( $A \subseteq B$ ) a operácie prieniku ( $A \cap B$ ), zjednotenia ( $A \cup B$ ), rozdielu ( $A - B$ ) a komplementu  $\bar{A}$ . Tieto operácie sú vizualizované pomocou Vennových diagramov. Symbol  $|A|$  vyjadruje kardinalitu množiny  $A$ , t. j. počet jej prvkov.

ENUMERÁCIA  
PRVKOV  
V MNOŽINÁCH

Enumerácia prvkov v množinách je založená na formule, ktorá špecifikuje kardinalitu prieniku množín

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Túto formulu možno jednoducho zovšeobecniť indukciou pre prienik troch alebo

viac množín. Kardinalita zjednotenia dvoch množín množiny  $|A \cup B|$  sa interpretuje ako počet prvkov, ktoré buď patria do množiny  $A$  alebo patria do množiny  $B$  (t. j. majú buď vlastnosť  $A$  alebo vlastnosť  $B$ ). Podobným spôsobom interpretujeme aj kardinalitu prieniku množín  $|A \cap B|$ , ako počet prvkov, ktoré súčasne patria do množiny  $A$  a množiny  $B$  (t. j. majú vlastnosť  $A$  a vlastnosť  $B$ ).

#### POTENČNÁ MNOŽINA

Pre danú množinu  $A$  potenčná množina  $\mathcal{P}(A)$  obsahuje ako prvky všetky možné podmnožiny množiny  $A$ . Kardinalita potenčnej množiny je určená jednoduchou formulou  $|\mathcal{P}(A)| = 2^{|A|}$ .

#### KARTEZIÁNSKY SÚČIN MNOŽÍN

Pre dve množiny  $X$  a  $Y$  karteziánsky súčin  $X \times Y$  je množina, ktorá obsahuje všetky možné usporiadané dvojice  $(x, y)$ , pre  $x \in X$  a  $y \in Y$ . Význam karteziánskeho súčinu spočíva v tom, že pomocou vhodných množín  $A_1, A_2, \dots, A_n$  môžeme vytvárať súčiny  $A_1 \times A_2 \times \dots \times A_n$ , ktoré majú názornú geometrickú interpretáciu pomocou rôznych telies. Tak napríklad nech  $A$  je úsečka a  $B$  je kružnica, potom  $A \times B$  je plášť valca (pozri obr. 2.9).

## KLÚČOVÉ POJMY

*množina*  
*operácie nad množinami*  
*množinová algebra*  
*mohutnosť (kardinalita)*  
*enumerácia*  
*karteziánsky súčin*  
*Georg Cantor*  
*Bertrand Russell*  
*axiomatická výstavba*  
*prvok (element)*  
*odlišiteľné prvky*  
*vymenovanie prvkov*  
*predikát*  
*charakteristická funkcia*  
*univerzum  $U$*   
*prázdna množina  $\emptyset$*   
*rovnosť množín*

*podmnožina*  
*vlastná podmnožina  $A \subset B$*   
*zjednotenie množín*  
*prienik množín*  
*doplnok (komplement) množiny*  
*rozdiel množín (relatívny doplnok)*  
*Vennove diagramy*  
*algebra teórie množín*  
*princíp kompozicionality*  
*oblasti v množine univerza*  
*tabuľková metóda pre verifikáciu*  
*rodina množín*  
*axiomatizácia*  
*geometrická interpretácia množiny*  
*potenčná množina*  
*René Descartes*

---

## CVIČENIA

---

**2.1.** Ktoré prvky patria do množiny:

- (a)  $\{x; (x \in \mathbb{R}) \wedge (x^2 = 1)\}$ , (kde  $\mathbb{R}$  je množina reálnych čísel)
- (b)  $\{x; (x \in \mathbb{R}) \wedge (x^2 - 3x + 2 = 0)\}$ ,
- (c)  $\{x; (x \in \mathbb{N}) \wedge (x < 12)\}$ , (kde  $\mathbb{N}$  je množina nezáporných celých čísel)
- (d)  $\{x; (x \in \mathbb{N}) \wedge (x^2 < 100)\}$ ,
- (e)  $\{x; (x \in \mathbb{N}) \wedge (x^2 = 2)\}$ .

**2.2.** Vyjadrite tieto množiny pomocou predikátu (pozri (2.1b)):

- (a)  $A = \{0, 3, 6, 9, 12\}$ ,
- (b)  $A = \{-3, -2, -1, 0, 1, 2, 3\}$ ,
- (c)  $A = \{m, n, o, p\}$ .

**2.3.** Zistite, či množiny z každej dvojice sú navzájom rovné:

- (a)  $A = \{1, 2, 2, 3, 3, 3, 4, 4, 4, 4\}$ ,  $B = \{1, 2, 3, 4\}$ ,
- (b)  $A = \{\{1\}\}$ ,  $B = \{1, \{1\}\}$ ,
- (c)  $A = \emptyset$ ,  $B = \{\emptyset\}$ .

**2.4.** Nech  $A = \{2, 4, 6\}$ ,  $B = \{2, 6\}$ ,  $C = \{4, 6\}$ ,  $D = \{4, 6, 8\}$ . Zistite, ktoré množiny sú podmnožiny ktorých množín.

**2.5.** Pre každú množinu  $A$  určite, či platí  $2 \in A$ :

- (a)  $A = \{x \in \mathbb{R}; x < 2\}$ ,
- (b)  $A = \{x \in \mathbb{R}; \exists (n \in \mathbb{N})(x = n^2)\}$ ,
- (c)  $A = \{2, \{2\}\}$ ,
- (d)  $A = \{\{2\}, \{\{2\}\}\}$ ,
- (e)  $A = \{\{2\}, \{2, \{2\}\}\}$ .

**2.6.** Pre každý príklad z cvičenia 2.5 rozhodnite, či prvok  $\{2\}$  je prvkom množiny  $A$ .

**2.7.** Rozhodnite, či výroky sú pravdivé alebo nepravdivé:

- (a)  $0 \in \emptyset$ ,
- (b)  $\emptyset \in \{0\}$ ,
- (c)  $\{0\} \subset \emptyset$ ,

- (d)  $\emptyset \subset \{0\}$ ,
- (e)  $\{0\} \in \{0\}$ ,
- (f)  $\{0\} \subset \{0\}$ ,
- (g)  $\{0\} \subseteq \{0\}$ .

**2.8.** Rozhodnite, či výroky sú pravdivé alebo nepravdivé:

- (a)  $\emptyset \in \{\emptyset\}$ ,
- (b)  $\emptyset \in \{\emptyset, \{\emptyset\}\}$ ,
- (c)  $\{\emptyset\} \in \{\emptyset\}$ ,
- (d)  $\{\emptyset\} \in \{\{\emptyset\}\}$ ,
- (e)  $\{\emptyset\} \subset \{\emptyset, \{\emptyset\}\}$ ,
- (f)  $\{\{\emptyset\}\} \subset \{\emptyset, \{\emptyset\}\}$ .

**2.9.** Nech  $A \subseteq B$  a  $B \subseteq C$ , dokážte  $A \subseteq C$ .

**2.10.** Nájdite také dve množiny  $A$  a  $B$ , aby platilo

- (a)  $A \in B$ ,
- (b)  $A \subseteq B$ .

**2.11.** Aká je mohutnosť týchto množín:

- (a)  $\{a\}$ ,
- (b)  $\{\{a\}\}$ ,
- (c)  $\{a, \{a\}\}$ ,
- (d)  $\{a, \{a\}, \{a, \{a\}\}\}$ .

**2.12.** Aká je mohutnosť týchto množín:

- (a)  $\emptyset$ ,
- (b)  $\{\emptyset\}$ ,
- (c)  $\{\emptyset, \{\emptyset\}\}$ ,
- (d)  $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ .

**2.13.** Zostrojte potenčnú množinu  $\mathcal{P}(A)$  pre

- (a)  $A = \{a\}$ ,
- (b)  $A = \{a, b\}$ ,
- (c)  $A = \{\emptyset, \{\emptyset\}\}$ .

**2.14.** Dokážte alebo vyvráťte implikáciu  $(\mathcal{P}(A) = \mathcal{P}(B)) \Rightarrow (A = B)$ .

**2.15.** Určite, ktorá z množín je potenčná množina

- (a)  $\emptyset$ ,
- (b)  $\{\emptyset, \{a\}\}$ ,
- (c)  $\{\emptyset, \{a\}, \{\emptyset, a\}\}$ ,
- (d)  $\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ .

**2.16.** Nech  $A = \{a, b, c\}$ ,  $B = \{x, y\}$ , zostrojte

- (a)  $A \times B$ ,
- (b)  $B \times A$ .

**2.17.** Aký význam má karteziánsky súčin  $A \times B$ , kde  $A$  je množina prednášok, ktoré poskytuje Ústav aplikovanej informatiky a  $B$  je množina pedagógov Fakulty informatiky?

**2.18.** Aký je význam karteziánskeho súčinu  $A \times B \times C$ , kde  $A$  je množina všetkých leteckých spoločností,  $B$  a  $C$  sú množiny letísk na svete.

**2.19.** Nech  $A$  je množina študentov FIIT, ktorí sú z Bratislavy a  $B$  je množina študentov FIIT, ktorí jazdia na fakultu autom. Opíšte študentov, ktorí patria do množiny

- (a)  $A \cap B$ ,
- (b)  $A \cup B$ ,
- (c)  $A - B$ ,
- (d)  $B - A$ .

**2.20.** Nech  $A$  je množina prvákov na našej fakulte a  $B$  je množina študentov navštevujúcich diskretnú matematiku. Vyjadrite pomocou množín  $A$  a  $B$  tvrdenia:

- (a) Množina prvákov, ktorí navštevujú prednášku z diskretnéj matematiky.
- (b) Množina prvákov, ktorí nenavštevujú prednášku z diskretnéj matematiky.
- (c) Množina študentov, ktorí sú prváci alebo navštevujú prednášku z diskretnéj matematiky.
- (d) Množina študentov, ktorí nie sú prváci alebo nenavštevujú prednášku z diskretnéj matematiky.

**2.21.** Nech  $A$  a  $B$  sú množiny, dokážte

- (a)  $(A \cap B) \subseteq A$ ,
- (b)  $(A \cap B) \subseteq B$ ,
- (c)  $A \subseteq (A \cup B)$ ,
- (d)  $B \subseteq (A \cup B)$ ,
- (e)  $A - B \subseteq A$ ,
- (f)  $A \cap (B - A) = \emptyset$ .

**2.22.** Nech  $A$ ,  $B$  a  $C$  sú množiny, dokážte  $(A - B) - C = (A - C) - (B - C)$ .

**2.23.** Čo môžeme povedať o množinách  $A$  a  $B$ , ak platí

- (a)  $A \cup B = A$ ,
- (b)  $A \cap B = A$ ,
- (c)  $A - B = A$ ,
- (d)  $A \cap B = B \cap A$ ,
- (e)  $A - B = B - A$ .

**2.24.** Nech  $A$ ,  $B$  a  $C$  sú množiny, zistite, či sú pravdivé implikácie:

- (a)  $(A \cup C = B \cup C) \Rightarrow (A = B)$ ,
- (b)  $(A \cap C = B \cap C) \Rightarrow (A = B)$ .

**2.25.** Nech  $A$  a  $B$  sú množiny, dokážte vlastnosť  $(A \subseteq B) \Rightarrow (\bar{B} \subseteq \bar{A})$ .

**2.26.** Nech  $A_i = \{1, 2, \dots, i\}$ , pre  $i=1, 2, \dots, n$ . Nájdite

- (a)  $A_1 \cap A_2 \cap \dots \cap A_n$ ,
- (b)  $A_1 \cup A_2 \cup \dots \cup A_n$ .

**2.27.** Nech  $A_i$  je množina binárnych reťazcov, ktorých dĺžka nie je väčšia ako  $i$ , pre  $i=1, 2, \dots, n$ . Nájdite

- (a)  $A_1 \cap A_2 \cap \dots \cap A_n$ ,
- (b)  $A_1 \cup A_2 \cup \dots \cup A_n$ .

**2.28.** Dokážte pomocou matematickej indukcie vzťahy

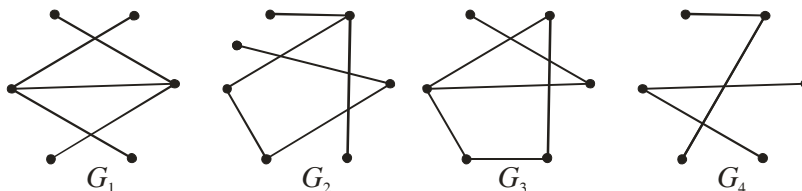
$$(a) \overline{\bigcup_{i=1}^n A_i} = \bigcap_{i=1}^n \bar{A}_i$$

$$(b) \overline{\bigcap_{i=1}^n A_i} = \bigcup_{i=1}^n \bar{A}_i$$

# RIEŠENÉ CVIČENIA Z KAPITOLY 12

**12.1.** Ktoré z nasledujúcich grafov na obr. 12.19 nie sú stromy a prečo?

**OBRÁZOK 12.19.**  
KTORÉ NIE SÚ  
STROMY?



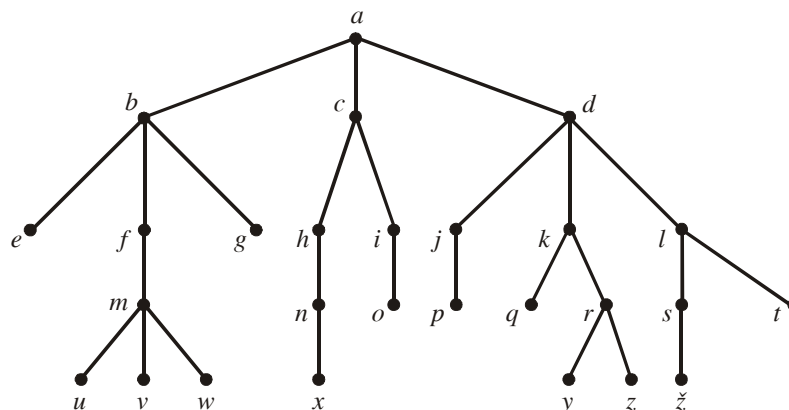
Ktoré nie sú stromy?

Grafy  $G_1$  a  $G_2$  sú stromy, neobsahujú cyklus a sú súvislé, graf  $G_3$  nie je strom, obsahuje cyklus, graf  $G_4$  nie je strom, nie je súvislý.

**12.2.** Odpovedzte pre graf na obr. 12.20 nasledujúce dotazy:

- Ktorý z vrcholov je koreň? Koreň je  $a$ .
- Ktoré vrcholy sú vnútorné? Vnútorné vrcholy sú  $\{a, b, c, d, f, h, i, j, k, l, m, n, r, s\}$ .
- Ktoré vrcholy sú listy? Listy sú  $\{e, u, v, w, g, x, o, p, q, y, z, ž, t\}$ .
- Ktoré vrcholy sú nasledovníci (synovia) vrcholu  $k$ ? Nasledovníci vrcholu  $k$  sú vrcholy  $q$  a  $r$ .
- Ktoré vrcholy sú rodičia vrcholu  $k$ ? Rodič vrcholu  $k$  je  $d$ .
- Ktoré vrcholy sú predkovia  $k$ ? Predkovia vrcholu  $k$  sú vrcholy  $d$  a  $a$ .
- Ktoré vrcholy sú potomkovia vrcholu  $k$ ? Potomkovia vrcholu  $k$  sú vrcholy  $q, r, y, z$ .

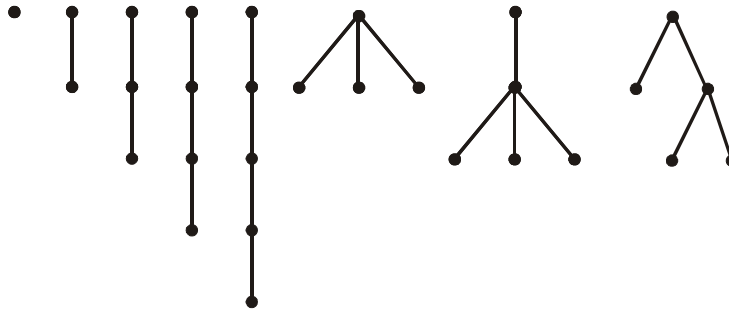
**OBRÁZOK 12.20.**  
KOREŇOVÝ  
STROM



Koreňový strom.

**12.3.** Koľko neizomorfných podstromov do 5 vrcholov obsahuje graf na obr. 12.20?

Neizomorfných podstromov je 8, všetky stromy, ktoré do 5 vrcholov existujú.



**12.4.** Majme  $n$  nenulových prirodzených čísel  $s_1, s_2, s_3, \dots, s_n$ , kde  $n \geq 2$ . Nutná a postačujúca podmienka, aby existoval strom na  $n$  vrchoch taký, že  $s_1, s_2, s_3, \dots, s_n$ , sú po poriadku stupne jeho vrcholov, je

$$\sum_{i=1}^n s_i = 2n - 2$$

Dokážte.

Keď existuje strom so stupňami  $s_1, s_2, s_3, \dots, s_n$ , potom zo vzorca (10.1)  $\sum_{i=1}^n s_i = 2|E|$  a zo vzorca vety 12.2 pre stromy  $|E| = |V| - 1$  vychádza vzorec, ktorý máme dokázať.

V opačnom prípade, keď platí dokazovaný vzorec, postupujeme matematickou indukciou, aby sme dokázali, že existuje strom so stupňami  $s_1, s_2, s_3, \dots, s_n$ . Pre  $n = 2$  je  $s_1 = s_2 = 1$  a strom existuje. Nech  $n > 2$  a predpokladáme existenciu stromu pre každú  $(n-1)$ ticu čísel  $s_i$ , ktoré spĺňajú dokazovaný vzorec. Keď zvolíme  $n$  čísel  $s_i$ , ktoré spĺňajú dokazovaný vzorec, je vidno, že aspoň dve z nich (povedzme  $s_1, s_2$ ) sa rovnajú 1 a aspoň jedno ďalšie (povedzme  $s_3$ ) je väčšie ako 1. Čísla  $s_2, s_3-1, s_4, \dots, s_n$  spĺňajú indukčný predpoklad a existuje teda strom o  $n-1$  vrchoch s príslušnými stupňami. Označme v ňom  $x$  vrchol  $(s_3-1)$ ého stupňa a nech  $y$  je ďalší vrchol nepatriaci do uvedeného stromu o  $n-1$  vrchoch. Teraz doplníme tento strom vrcholom  $y$  a hranou  $xy$ .

**12.5.** Nech  $G$  je jednoduchý graf o  $n$  vrchoch. Ukážte, že  $G$  je strom vtedy a len vtedy, keď je súvislý a má  $n - 1$  hrán.

Dokážeme toto tvrdenie indukciou pre  $n$ , počet vrcholov grafu  $G$ . Keď  $n = 1$ , ide o izolovaný vrchol, ktorý je formálne strom, je súvislý a má  $1 - 1 = 0$  hrán. Tvrdenie je teda pravdivé. Teraz predpokladajme, že tvrdenie je pravdivé pre obyčajné grafy o  $n$  vrchoch, a nech  $G$  je obyčajný graf o  $n + 1$  vrchoch.

Po prvé predpokladajme, že  $G$  je strom; musíme ukázať že  $G$  je súvislý a že má  $(n + 1) - 1 = n$  hrán. Samozrejme,  $G$  je súvislý podľa definície. Aby sme dokázali, že  $G$  má požadovaný počet hrán, potrebujeme nasledujúcu skutočnosť: strom s aspoň jednou hranou musí obsahovať vrchol stupňa 1. (Aby sme to ukázali, stačí si zobrať najdlhšiu jednoduchú cestu. Nejaká cesta maximálnej dĺžky musí v konečnom grafe existovať. Konce tejto cesty musia byť v strome



vrcholy stupňa 1, pretože inak by táto cesta mohla byť predĺžená.) Nech  $v$  je vrchol stupňa 1 v  $G$ , a nech  $G'$  je  $G$  s  $v$  a s ním incidentnou hranou odstránený. Nový graf  $G'$  je stále strom, nemá žiadne kružnice (graf  $G$  nemal žiadne) a je stále súvislý (odstránená hrana nie je potrebná na vytvorenie cesty medzi vrcholmi rozdielnymi od  $v$ ). Preto podľa indukčnej hypotézy,  $G'$ , ktorý má  $n$  vrcholov, má  $n-1$  hrán; keďže  $G$  má o hranu viac ako  $G'$ , má teda  $n$  hrán.

Z druhej strany, predpokladajme, že  $G$  je súvislý a má  $n$  hrán a  $(n+1)$  vrcholov. Keď  $G$  nie je strom, potom musí obsahovať kružnicu. Keď z tejto kružnice odstránime jednu hranu, výsledný graf  $G'$  bude stále súvislý. Keď je  $G'$  strom, potom s odstraňovaním hrán končíme; v opačnom prípade proces opakujeme. Pretože  $G$  má konečný počet hrán, tento proces musí skončiť pre nejaký strom o  $n+1$  vrcholoch (strom má rovnaký počet vrcholov ako pôvodný graf  $G$ ). Podľa predchádzajúceho odseku má tento strom  $n$  hrán. To je ale v protiklade s tým, že sme odstránili najmenej jednu hranu. Preto náš predpoklad, že  $G$  nie je strom, je zlý. ■

- 12.6.** Predpokladajme, že 1024 ľudí sa účastní šachového turnaja. Použite koreňový strom ako model turnaja na určenie, koľko hier musí byť odohraných, aby sa určil víťaz, pokiaľ je hráč eliminovaný po jednej prehre a turnaj pokračuje, dokiaľ iba jeden účastník neprehral. Predpokladáme, že nebudú žiadne remízy.

Turnaj môžeme modelovať ako úplný binárny strom. Každý vnútorný vrchol reprezentuje výhercu hry hranej jeho dvoma deťmi. Máme 1024 listov, jeden pre každého hráča. Koreň je víťaz turnaja. Podľa vety 12.3, pre  $m=2$  a  $l=1024$ ,  $n=i+l=m \times i+1$ ; z toho dostávame  $i=(l-1)/(m-1)=1023$ . Preto musí byť odohraných presne 1023 hier na určenie víťaza.

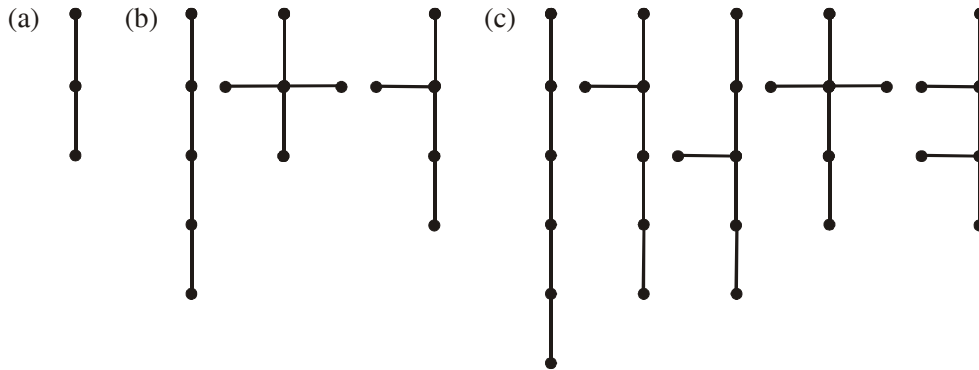
- 12.7.** Reťazový list začína človekom posielajúcim list desiatim ďalším ľuďom. Každý príjemca je požiadaný, aby poslal list ďalším desiatim a každý list obsahuje zoznam predchádzajúcich šiestich ľudí v reťazci. Pokiaľ zoznam neobsahuje menej ako šesť mien, každý príjemca pošle dvadsať korún prvému človeku v zozname, odstráni jeho meno zo zoznamu a pridá svoje vlastné meno na koniec zoznamu. Keď všetci takto odpovedia na list a nikto nedostane viac ako jeden list, koľko peňazí človek zapojený do reťazca nakoniec dostane?

Nech  $P$  je človek rozposielajúci list. Potom 10 ľudí dostane jeho list na konci zoznamu (na 6. pozícii). Potom 100 ľudí dostane list s jeho menom na piatej pozícii atď., až 1 000 000 ľudí dostane list s menom  $P$  na prvej pozícii. Preto by  $P$  mal dostať 20 000 000. Model je tu úplný strom s vetvením stupňa 10.

- 12.8.** Koľko rôznych izomérov majú nasledujúce nasýtené uhľovodíky?

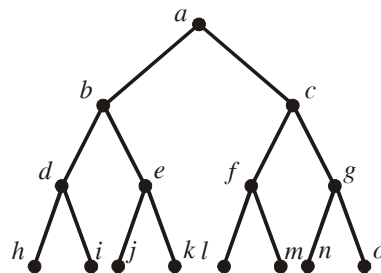
- (a)  $C_3H_8$   
 (b)  $C_5H_{12}$   
 (c)  $C_6H_{14}$

Z definície alkánov (nasýtených uhľovodíkov) vyplýva, že alkány majú štruktúru stromov. Stačí si všimnúť iba stromy z uhľíkových atómov týchto uhľovodíkov, hrany s vodíkovými atómami stupňa vrcholov 1 potom iba automaticky dopĺňajú počet incidentných hrán s každým uhľíkovým atómom na stupeň 4. Ak chceme teda spočítať alkány s daným počtom  $n$  atómov uhlíka, stačí spočítať všetky typy stromov s  $n$  vrcholmi, v ktorých sa nevyskytujú vrcholy stupňa väčšieho ako 4. Pre prípad (a) je to iba jeden graf, pre prípad (b) 3 a pre (c) 5, ako je vidno na nasledujúcom obrázku.



**12.9.** Ukážte, ako môže byť 16 čísel sčítaných pomocou 15 procesorov v priebehu 4 časových krokov potrebných na sčítanie dvojice čísel (vstup a prenos informácie neuvažujeme za časovo náročné kroky a ich čas zanedbávame v porovnaní so sčítaním).

Vytvoríme kompletný binárny strom o 15 vrcholoch, ktorý reprezentuje sieť so stromovou štruktúrou o 15 procesoroch. V prvom kroku sčítame prvých 8 dvojíc čísel v procesoroch  $h, \dots, o$ . V druhom časovom okamihu sčítame výsledky týchto súčtov v procesoroch  $d, \dots, g$ , v treťom časovom okamihu sú to súčty výsledkov procesorov  $d, e$  v  $b$  a  $f, g$  v  $c$  a v poslednom štvrtom časovom okamihu sčítame výsledky z  $b, c$  v  $a$ .



**12.10.** Nech  $n$  je mocnina dvoch. Ukážte, že  $n$  čísel môže byť sčítaných v  $\log_2 n$  krokoch pri použití siete so stromovou štruktúrou o  $n - 1$  procesoroch.

Predpokladajme, že  $n = 2^k$ , kde  $k$  je kladné celé číslo. Chceme ukázať ako sčítať  $n$  čísel za  $\log_2 n$  krokov pri použití siete so stromovou štruktúrou o  $n - 1$  procesoroch. Dokážme to matematickou indukciou na  $k$ . Keď  $k = 1$ , potom  $n = 2$  a  $n - 1 = 1$  a v  $\log_2 2 = 1$  kroku dokážeme sčítať 2 čísla jedným procesorom. Predpokladajme ako induktívnu hypotézu, že môžeme sčítať  $n = 2^k$  v  $\log_2 n$  krokoch pri použití siete so stromovou štruktúrou o  $n - 1$  procesoroch. Predpokladajme teraz, že máme  $2n = 2^{k+1}$  čísel na sčítanie,  $x_1, x_2, \dots, x_{2n}$ . Sieť so stromovou štruktúrou o  $2n - 1$  procesoroch vytvoríme zo siete so stromovou štruktúrou o  $n - 1$  procesoroch spolu s dvoma novými procesormi ako deťmi každého listu v  $(n - 1)$ -procesorovej sieti. V jednom kroku môžeme použiť listy rozšírenej siete pre sčítanie  $x_1 + x_2, x_3 + x_4, x_{2n-1} + x_{2n}$ . To nám dáva  $n$  čísel. Podľa induktívnej hypotézy teraz môžeme použiť zvyšok siete na sčítanie týchto čísel v  $\log_2 n$  krokoch. Dovedna sme použili  $1 + \log_2 n$  krokov a ako sme potrebovali ukázať  $\log_2(2n) = \log_2 2 + \log_2 n = 1 + \log_2 n$ . ■

- 12.11.** Koľko vážení na rovníramenných váhach je potrebné na nájdenie ľahšej falošnej mince spomedzi štyroch mincí? Opíšte algoritmus na nájdenie tejto ľahšej mince pri použití tohto počtu vážení.

Mince rozdelíme na dve dvojice a tie porovnáme, zoberieme ľahšiu dvojicu a tú porovnáme. Potrebujeme teda dve porovnaní.

- 12.12.** Koľko vážení na rovníramenných váhach je potrebné na nájdenie falošnej mince spomedzi štyroch mincí, ktorá môže byť ľahšia alebo ťažšia ako ostatné tri?

Pretože sú 4 rôzne výsledky na túto testovaciu procedúru, potrebujeme aspoň dve vážení, pretože jedno váženie nám môže dať iba 3 možné výsledky (ternárny rozhodovací strom výšky 1 má iba 3 listy). Označme si mince písmenami  $A, B, C, D$ . Porovnáme mince  $A$  a  $B$ . Pokiaľ sú v rovnováhe, falošná minca je medzi druhými dvoma. V tom prípade, porovnajme  $C$  s  $A$ , pokiaľ sú v rovnováhe,  $D$  je falošná minca, keď nie,  $C$  je falošná. Na druhej strane, keď  $A$  a  $B$  nie sú v rovnováhe, jedna z nich je falošná. Opäť porovnajme  $C$  s  $A$ . Keď sú v rovnováhe,  $B$  je falošná, v opačnom prípade je  $A$  falošná.

- 12.13.** Koľko vážení na rovníramenných váhach je potrebné na nájdenie falošnej mince, ktorá je ľahšia ako ostatné, spomedzi 12 mincí?

Pretože existuje 12 rozdielnych výsledkov testovacej procedúry, potrebujeme aspoň 3 vážení, pretože 2 vážení by nám dali 9 možných výsledkov (rozhodovací strom hĺbky 2 má iba 9 listov). Rozdeľte mince na 3 skupiny po 4 minciach, a porovnajme dve skupiny. Keď sú vyvážené, falošná minca je medzi ostatnými štyrmi mincami. Keď nie sú v rovnováhe, falošná minca je medzi ľahšou štvoricou. Teraz môžeme využiť cvičenie 12.11, pomocou dvoch ďalších vážení určíme falošnú mincu.

- 12.14.** Ktorý z nasledujúcich kódov je prefixový kód?

(a)  $a: 11, e: 00, t: 10, s: 01$

Je prefixový kód, žiaden z kódov nie je začiatkom iného kódu.

(b)  $a: 0, e: 1, t: 01, s: 001$

Nie je prefixový kód, napríklad kód pre  $a$  je začiatkom kódu pre  $s$ .

(c)  $a: 101, e: 11, t: 001, s: 011, n: 010$

Je prefixový kód, žiaden z kódov nie je začiatkom iného kódu.

(d)  $a: 010, e: 11, t: 011, s: 1011, n: 1001, p: 10101$

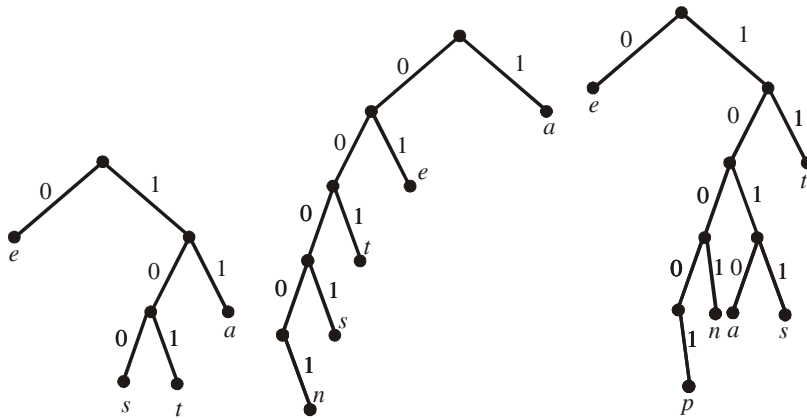
Je prefixový kód, žiaden z kódov nie je začiatkom iného kódu.

- 12.15.** Skonstruujte binárny strom s prefixovými kódmi reprezentujúcimi tieto kódové schémy:

(a)  $a: 11, e: 0, t: 101, s: 100$

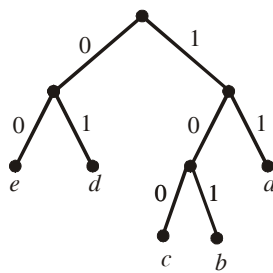
(b)  $a: 1, e: 01, t: 001, s: 0001, n: 00001$

(c)  $a: 1010, e: 0, t: 11, s: 1011, n: 1001, p: 10001$



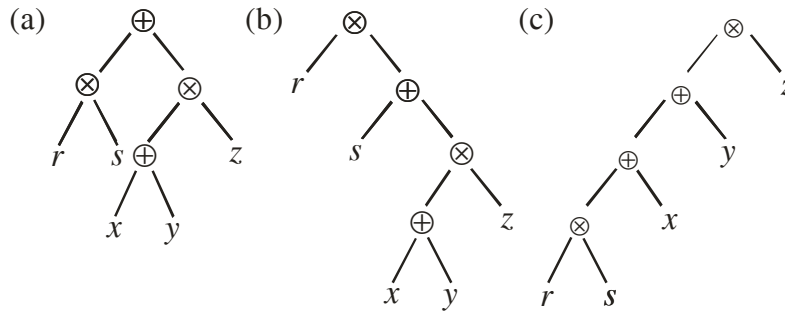
- 12.16.** Skonstruujte binárny strom reprezentujúci Huffmanove kódovanie pre nasledujúce symboly s frekvenciami:  $a: 0,2$ ;  $b: 0,1$ ;  $c: 0,15$ ;  $d: 0,25$ ;  $e: 0,3$ .

Riadime sa algoritmom pre Huffmanove kódovanie. Pretože  $b$  a  $c$  sú symboly s najmenšou váhou, skombinujeme ich do podstromu, ktorý tu budeme volať T1, s váhou  $0,1 + 0,15 = 0,25$ , so symbolom s väčšou váhou naľavo. Teraz dva stromy o najmenšej váhe sú samostatný symbol  $a$  a buď T1 alebo samostatný symbol  $d$ , oba o váhe  $0,25$ . Náhodne si zvolíme T1, a dostávame tak strom T2 s ľavým podstromom T1 a pravým podstromom  $a$  (mohli sme zvoliť aj druhú možnosť, výsledkom by bol odlišný, no rovnako kvalitný strom v ohľade priemerného počtu bitov na zakódovanie). Ďalším krokom je kombinácia  $e$  a  $d$  do podstromu T3 s váhou  $0,55$ . Konečným krokom je kombinácia T2 a T3.



- 12.17.** Reprezentujte nasledujúce výrazy ako binárne stromy

- $(r \otimes s) \oplus ((x \oplus y) \otimes z)$
- $r \otimes (s \oplus ((x \oplus y) \otimes z))$
- $((r \otimes s) \oplus x) \oplus y \otimes z$



**12.18.** Koľko rozdielnych možných interpretácií má každý z nasledujúcich výrazov, keď predpokladáme asociatívnosť operácie  $\otimes$  a keď ju nepredpokladáme?

- (a)  $x \otimes y \otimes z$   
 (b)  $t \oplus x \otimes y \otimes z$   
 (c)  $t \otimes x \oplus y \otimes z$

Keď predpokladáme asociatívnosť operácie  $\otimes$ :

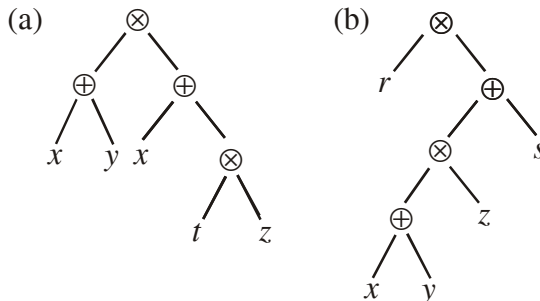
- (a) 1 interpretácia,  $x \otimes y \otimes z$   
 (b) 3 interpretácie,  $(t \oplus x) \otimes y \otimes z$ ,  $t \oplus (x \otimes y \otimes z)$ ,  $(t \oplus (x \otimes y)) \otimes z$   
 (c) 4 interpretácie,  $(t \otimes x) \oplus (y \otimes z)$ ,  $((t \otimes x) \oplus y) \otimes z$ ,  $(t \otimes (x \oplus y)) \otimes z$ ,  $t \otimes (x \oplus (y \otimes z))$

Keď nepredpokladáme asociatívnosť operácie  $\otimes$ :

- (a) 2 interpretácie,  $(x \otimes y) \otimes z$ ,  $x \otimes (y \otimes z)$   
 (b) 5 interpretácií,  $(t \oplus x) \otimes (y \otimes z)$ ,  $t \oplus ((x \otimes y) \otimes z)$ ,  $t \oplus (x \otimes (y \otimes z))$ ,  $(t \oplus (x \otimes y)) \otimes z$ ,  $((t \oplus x) \otimes y) \otimes z$   
 (c) 5 interpretácií,  $(t \otimes x) \oplus (y \otimes z)$ ,  $((t \otimes x) \oplus y) \otimes z$ ,  $(t \otimes (x \oplus y)) \otimes z$ ,  $t \otimes (x \oplus (y \otimes z))$ ,  $t \otimes ((x \oplus y) \otimes z)$

**12.19.** Zostrojte infixovú, prefixovú a postfixovú formu výrazov reprezentovaných nasledujúcimi binárnymi stromami na obr. 12.21.

**OBRÁZOK 12.21.**  
 ZOSTROJTE  
 INFIXOVÚ,  
 PREFIXOVÚ A  
 POSTFIXOVÚ  
 FORMU STROMOV

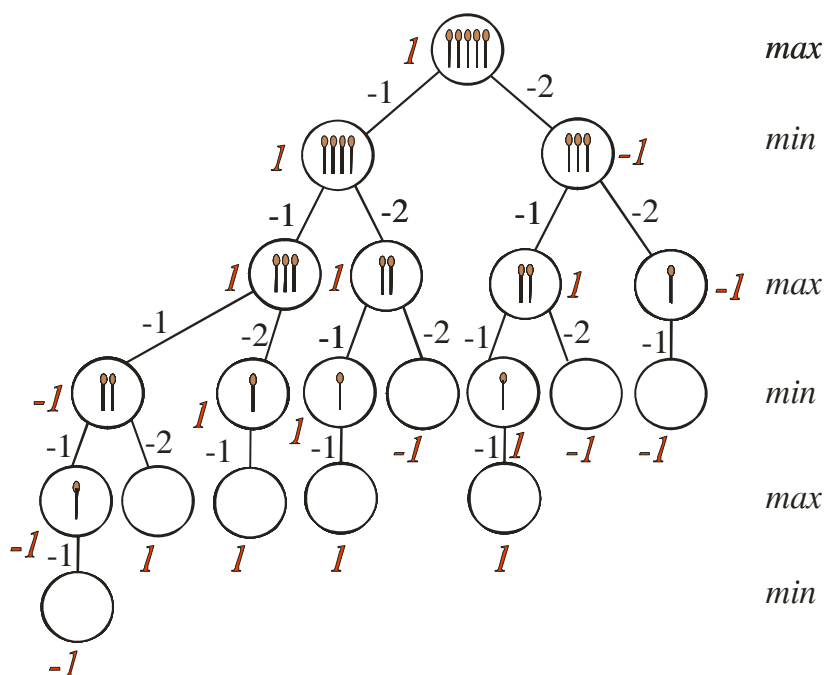


Zostrojte infixovú, prefixovú a postfixovú formu stromov.

- (a) Infix  $(x \oplus y) \otimes (x \oplus (t \otimes z))$ , prefix  $\otimes \oplus xy \oplus x \otimes tz$ , postfix  $xy \oplus xtz \otimes \oplus \otimes$   
 (b) Infix  $r \otimes (((x \oplus y) \otimes z) \oplus s)$ , prefix  $\otimes r \oplus \otimes \oplus xyzs$ , postfix  $rx y \oplus z \otimes s \oplus \otimes$

- 12.20.** Zostrojte strom riešení hry odoberania zápalkiek, keď máte na začiatku hry 5 zápalkiek, každý hráč môže odobrať jednu, alebo 2 zápalky a kto odoberie poslednú zápalku, tak prehral. Vrcholy z jednotlivých vrstiev stromu ohodnot'te pomocou minimax princípu.

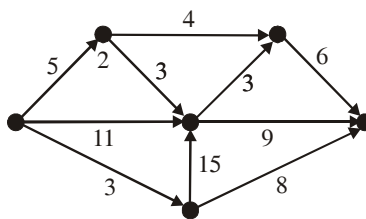
Na obrázku sú vrcholy s počtom zápalkiek na hromádke, jednotka označená kurzívou znamená, že ide o podstrom, kde vyhráva 1. hráč (voliaci stratégiu max, teda vyberajúci pre seba ako ideálnu stratégiu maximálne ohodnotený zo svojich podstromov),  $-1$  označená kurzívou znamená, že ide o podstrom, kde vyhráva 2. hráč (min). Ohodnotenia hrán  $-1$  a  $-2$  znamenajú odobratie jednej alebo dvoch zápalkiek hráčom. Z ohodnotenia koreňa je zrejmé, že pre prvého hráča existuje víťazná stratégia. Existuje aj trochu zložitejšia populárnejšia verzia tejto hry, volaná **nim**, kde sú zápalky na niekoľkých hromádkach a hráč môže odobrať 1 alebo 2 iba z jednej z hromádok.



# RIEŠENÉ CVIČENIA Z KAPITOLY 13

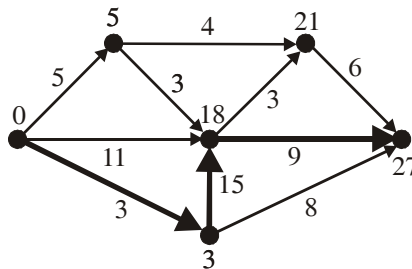
**13.1.** Pre siete projektu na obr. 13.17 a 13.18 určite minimálny celkový čas, ktorý zaberie dokončenie projektu, minimálne časové ohodnotenie  $E(v)$  u jednotlivých vrcholov a kritickú cestu. Každá z hrán je ohodnotená časom potrebným na splnenie úlohy jej priradené.

**OBRÁZOK 13.17.** (a)  
ČASOVÝ PLÁN  
PROJEKTU

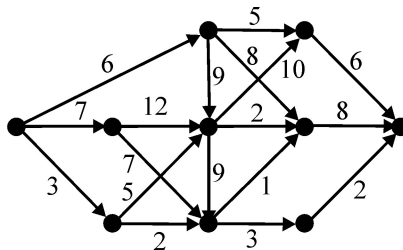


Časový plán projektu, určite kritickú cestu

Minimálny celkový čas je 27, ohodnotenie  $E(v)$  je uvedené u vrcholov, kritická cesta je tučne vyznačená.

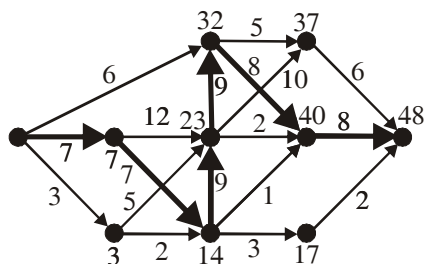


**OBRÁZOK 13.18.** (b)  
ČASOVÝ PLÁN  
PROJEKTU



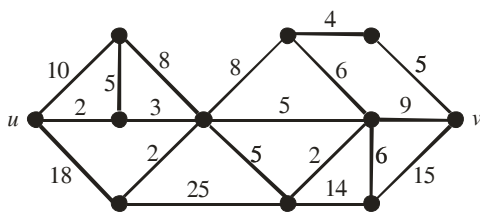
Časový plán projektu, určite kritickú cestu

Minimálny celkový čas je 48, ohodnotenie  $E(v)$  je uvedené u vrcholov, kritická cesta je tučne vyznačená.



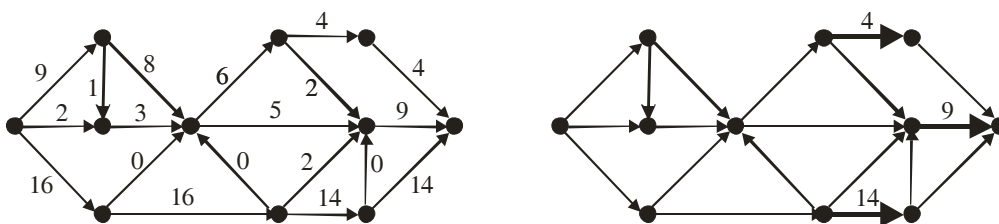
13.2. Pre nasledujúce kapacitné siete na obr. 13.19 a 13.20 s ohodnotením hrán ich kapacitami (namiesto dvojice opačne orientovaných hrán je vždy vykreslená iba neorientovaná hrana) nájdite maximálny tok z  $u$  do  $v$  a dokážte, že je tok maximálny nájdením minimálneho rezu, ktorého kapacita sa rovná hodnote vami nájdeného toku.

OBRÁZOK 13.19. (a)  
MAXIMÁLNY TOK A  
MINIMÁLNY REZ?

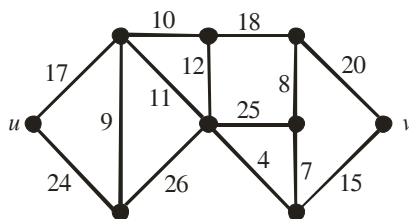


Nájdite maximálny tok a minimálny rez siete.

Maximálny tok je 27, minimálny rez je zobrazený v druhom grafe.



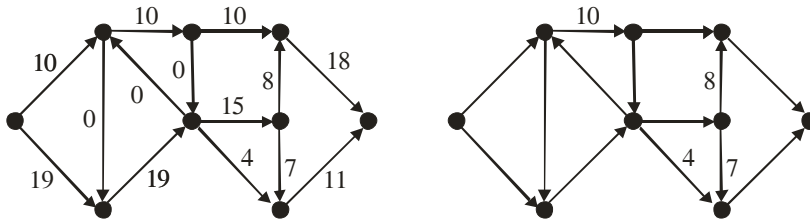
OBRÁZOK 13.20. (b)  
MAXIMÁLNY TOK A  
MINIMÁLNY REZ?



Nájdite maximálny tok a minimálny rez siete.

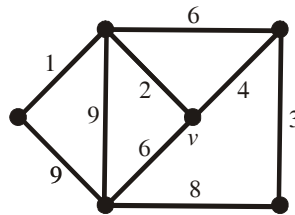
Maximálny tok je 29, minimálny rez je zobrazený v druhom grafe.





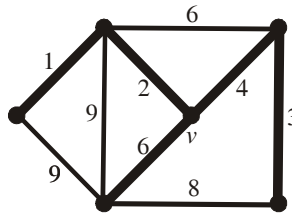
13.3. Pre grafy z obr. 13.21 a 13.22 použite Primov algoritmus, začínajúci na vyznačenom vrchole  $v$ , na nájdenie minimálnej kostry a určite jej váhu.

**OBRÁZOK 13.21.** (a)  
MINIMÁLNA  
KOSTRA?

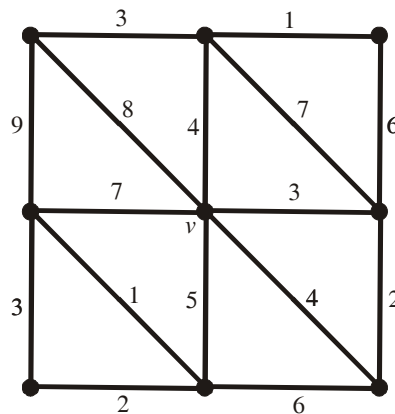


Nájdite minimálnu kostru.

Váha minimálnej kostry je 16, kostra je zvýraznená tučnými hranami v grafe.

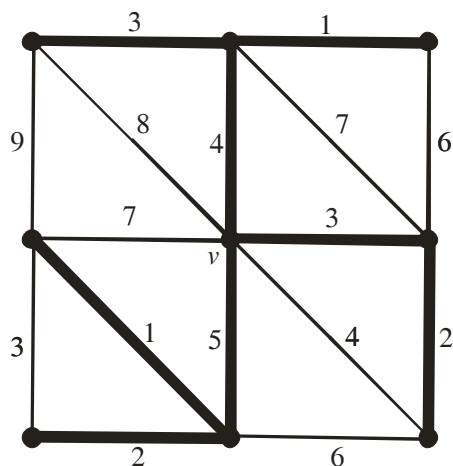


**OBRÁZOK 13.22.** (b)  
MINIMÁLNA  
KOSTRA?



Nájdite minimálnu kostru.

Váha minimálnej kostry je 21, kostra je zvýraznená tučnými hranami v grafe.

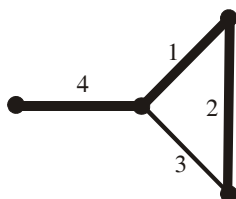


- 13.4.** Použite Kruskalov algoritmus na nájdenie minimálnej kostry pri grafoch z príkladu 13.3 a určite jej váhu.

Riešenie: Nájdené kostry sú rovnaké, ale keby niektoré z hrán s vyššími váhami mali rovnaké váhy, potom tak Kruskalov, aj Primov algoritmus by mohli viesť k rozdielnym kostrám kvôli náhodnosti výberu u rovnako ohodnotených hrán.

- 13.5.** Nech  $T$  je minimálna kostra ohodnoteného grafu  $G$ . Určte, či nasledujúce tvrdenia sú pravdivé:  
(a) Váha každej hrany patriacej do  $T$  je menšia alebo rovná váhe ľubovoľnej hrany z  $G$  nepatriacej do  $T$ .

Kontrapríklad



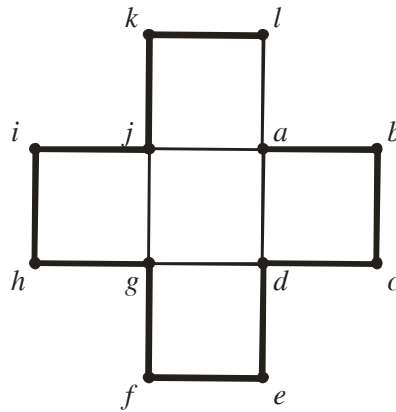
- (b) Keď žiadne dve hrany nemajú rovnakú váhu, potom Kruskalov algoritmus vyberie kostru  $T$  jednoznačne.

Tvrdenie je pravdivé, Kruskalov algoritmus potom pri výbere hrán nemá voľbu, postup je striktno deterministický.

- 13.6.** Použite prehľadávanie do hĺbky na nájdenie kostry daného jednoduchého grafu z obr. 13.23. Zvoľte vrchol  $a$  ako koreň tejto kostry a predpokladajte, že vrcholy sú usporiadané abecedne (namiesto typického postupu prehľadávania vykresleného grafu „zľava doprava“).

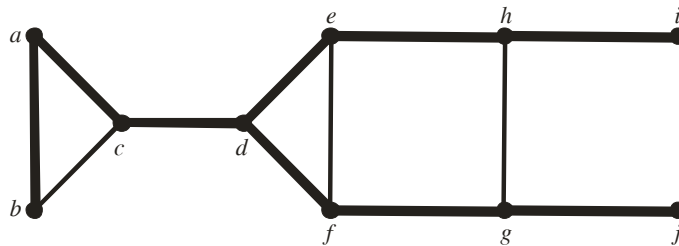


Keď začneme vo vrchole  $a$  a ideme v abecednom poradí, potom je kostra nájdená pomocou prehľadávania do hĺbky jednoznačne definovaná. Začneme vo vrchole  $a$  a vytvoríme cestu vyznačenú tučnými hranami až do bodu  $l$ .



- 13.8.** Použite prehľadávanie do šírky na nájdenie kostry daného jednoduchého grafu zadaného v cvičení 13.6. Zvoľte vrchol  $a$  ako koreň tejto kostry a predpokladajte, že vrcholy sú usporiadané abecedne (namiesto typického postupu prehľadávania vykresleného grafu „zľava doprava“).

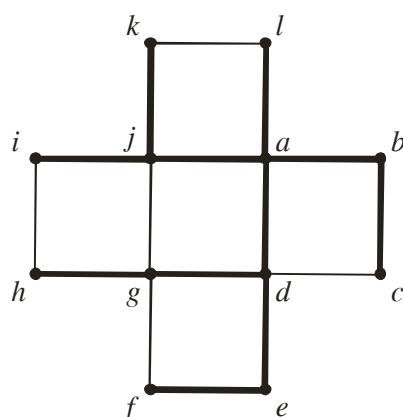
Postup pridávania hrán do kostry  $T$  by bol  $\{a, b\}, \{a, c\}, \{c, d\}, \{d, e\}, \{d, f\}, \{e, h\}, \{f, g\}, \{h, i\}, \{g, j\}$



- 13.9.** Použite prehľadávanie do šírky na nájdenie kostry daného jednoduchého grafu zadaného v cvičení 13.7. Zvoľte vrchol  $a$  ako koreň tejto kostry a predpokladajte, že vrcholy sú usporiadané abecedne (namiesto typického postupu prehľadávania vykresleného grafu „zľava doprava“).

Postup pridávania hrán do kostry  $T$  by bol

$\{a, b\}, \{a, d\}, \{a, j\}, \{a, l\}, \{b, c\}, \{d, e\}, \{d, g\}, \{j, i\}, \{j, k\}, \{e, f\}, \{g, h\}$



**13.10.** Čo musí platiť pre danú hranu jednoduchého súvislého grafu, aby bola v každej kostre tohto grafu?

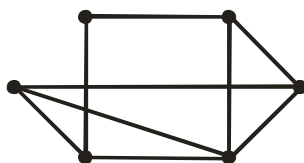
Platí v prípade, že je táto hrana mostom.

**13.11.** Kedy má jednoduchý súvislý graf práve jednu kosťu?

Vtedy, keď je graf stromom a kosťu je s týmto grafom totožná. V prípade, že graf obsahuje kružnicu o  $k$  hranách, potom existujú kostre obsahujúce akúkoľvek podmnožinu o  $k-1$  týchto hranách.

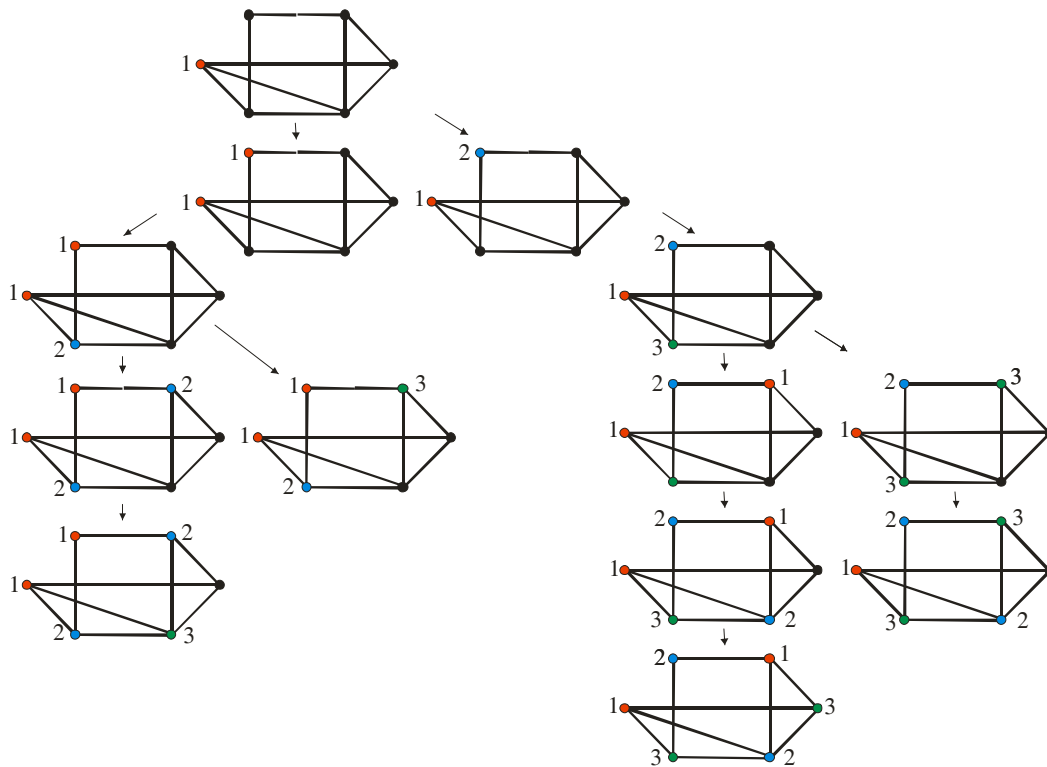
**13.12.** Použite prehľadávanie do hĺbky na nájdenie priradenia farieb vrcholom grafu z obr. 13.25 s využitím iba troch farieb.

**OBRÁZOK 13.25.**  
FARBENIE  
PREHĽADÁVANÍM  
DO HĽBKY?



Nájdite farbenie 3 farbami prehľadávaním do hĺbky.

Uvádzame strom prehľadávania, kedy v prípade ešte nepoužitých farieb pokladáme všetky farby za ekvivalentné a preto neuvádzame permutácie nájdeného riešenia s výmenou farieb medzi množinami vrcholov rovnakej farby. V takom prípade existuje iba jedno riešenie. Farby sú označené prirodzenými číslami



**13.13.** Použite prehľadávanie do hĺbky na nájdenie riešenia problému  $n$  dám na šachovnici pre zadané hodnoty  $n$ .

(a)  $n = 3$

Pre  $3 \times 3$  šachovnicu začneme prehľadávanie umiestnením dámy na pozícii (1,1). Jediná možnosť na umiestnenie dámy v druhom stĺpci je pozícia (3,2). Teraz neexistuje pozícia, na ktorú umiestniť dámu v treťom stĺpci. Preto sa vrátíme v prehľadávaní naspäť a pokúsime sa umiestniť prvú dámu na pozíciu (2,1). Potom nie je možné umiestniť dámu do druhého stĺpca. Na základe symetrie nepotrebujeme uvažovať pozíciu prvej dámy v štvorci (3,1), bola by ekvivalentná pozícii (1,1) cez stredovú čiaru. Tým sme ukázali, že riešenie neexistuje.

(b)  $n = 5$

Začneme s umiestnením dámy v pozícii (1,1). Prvá pozícia, kam sa dá umiestniť dáma v druhom stĺpci, je (3,2). Jediná možná pozícia v treťom stĺpci je (5,3), podobne vo štvrtom stĺpci (2,4) a v piatom (4,5). Na nájdenie tohto riešenia sme našťastie vôbec nepotrebovali použiť prehľadávanie do hĺbky.

(c)  $n = 6$

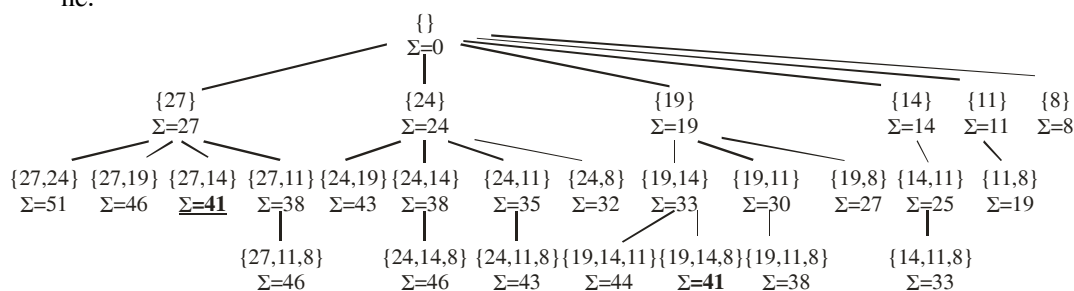
Časť stromu riešení odpovedajúca umiestneniu prvej dámy na pozíciu (1,1) je dosť veľká a nevedie k riešeniu. (Druhá dáma môže byť na pozíciách (3,2), (4,2), (5,2), alebo (6,2).) Keď je druhá dáma na pozícii (3,2), potom tretia môže byť na pozíciách (5,3) alebo (6,3). Po ďalšom preskúmaní a návratoch zistíme, že pre pozíciu začínajúcu na (1,1) neexistuje

riešenie. Ako ďalšiu začneme pozíciu (2,1) pre prvú dámu. Po niekoľkých návratoch v strome riešeni nájde umiestnenie zvyšných dám na pozíciách (4,2), (6,3), (1,4), (3,5), a (5,6).

**13.14.** Použite prehľadávanie do hĺbky na nájdenie podmnožiny, pokiaľ existuje, pre množinu {27, 24, 19, 14, 11, 8} so súčtom rovným

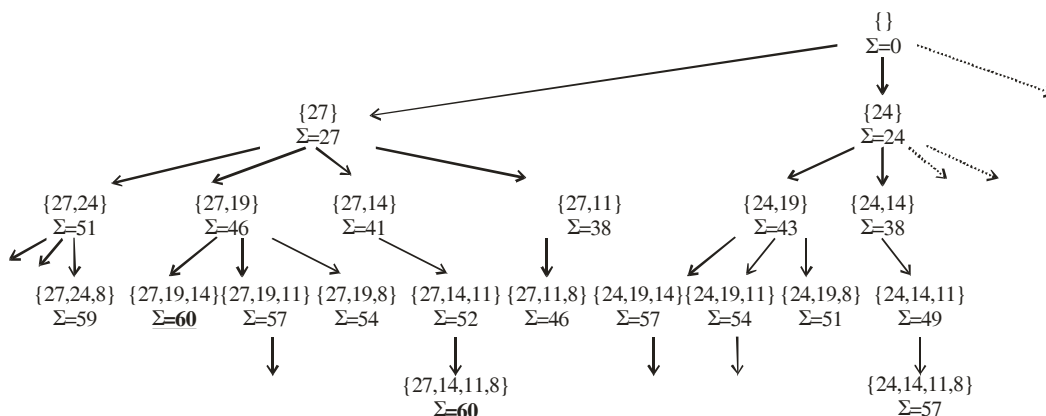
(a) 41

Po prekročení hľadaného súčtu sa už nepokračuje hlbšie do stromu prehľadávania a pridávajú sa vždy iba menšie čísla, ako je už najmenšie obsiahnuté vo vytváranej podmnožine.



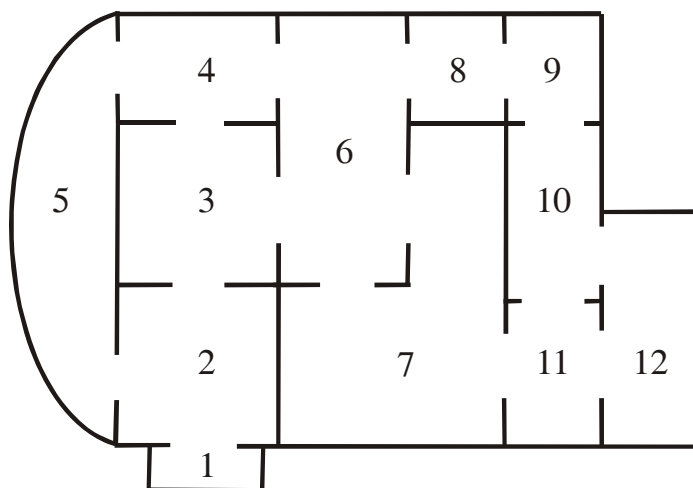
(b) 60

Po prekročení hľadaného súčtu sa už nepokračuje hlbšie do stromu prehľadávania a pridávajú sa vždy iba menšie čísla, ako je už najmenšie obsiahnuté vo vytváranej podmnožine. Pre prípady, ktoré by prekročili 60, uvádzame kvôli úspore miesta iba šípky. Bodkované šípky značia, že celková suma pre akúkoľvek kombináciu zloženú zo zvyšných čísel nemôže dosiahnuť 60 a preto už podstrom riešeni nie je uvádzaný (aj keď do prehľadávania do hĺbky by sa takéto osekávanie stromu muselo špeciálne zaviesť).



**13.15.** Vysvetlite, ako je možné prehľadávanie do hĺbky využiť na nájdenie cesty v múzeu, pri zadanej štartovnej pozícii a cieľovej pozícii. Múzeum má plán poschodia nakreslený na obr. 13.26.

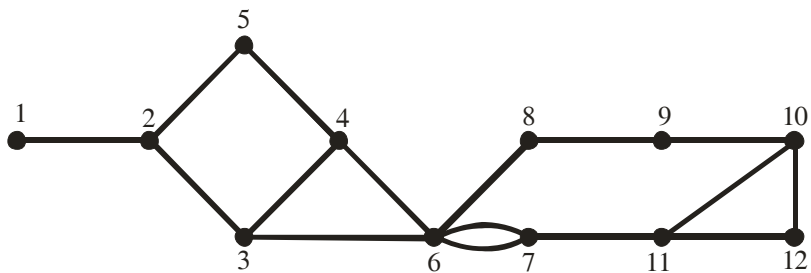
**OBRÁZOK 13.26.**  
 PLÁN MÚZEA  
 PREROBIŤ NA  
 GRAF



Plán múzea reprezentovať grafom.

- (a) Nakreslite graf reprezentujúci plán poschodia, kde každá miestnosť bude ako vrchol a každé dvere ako hrana.

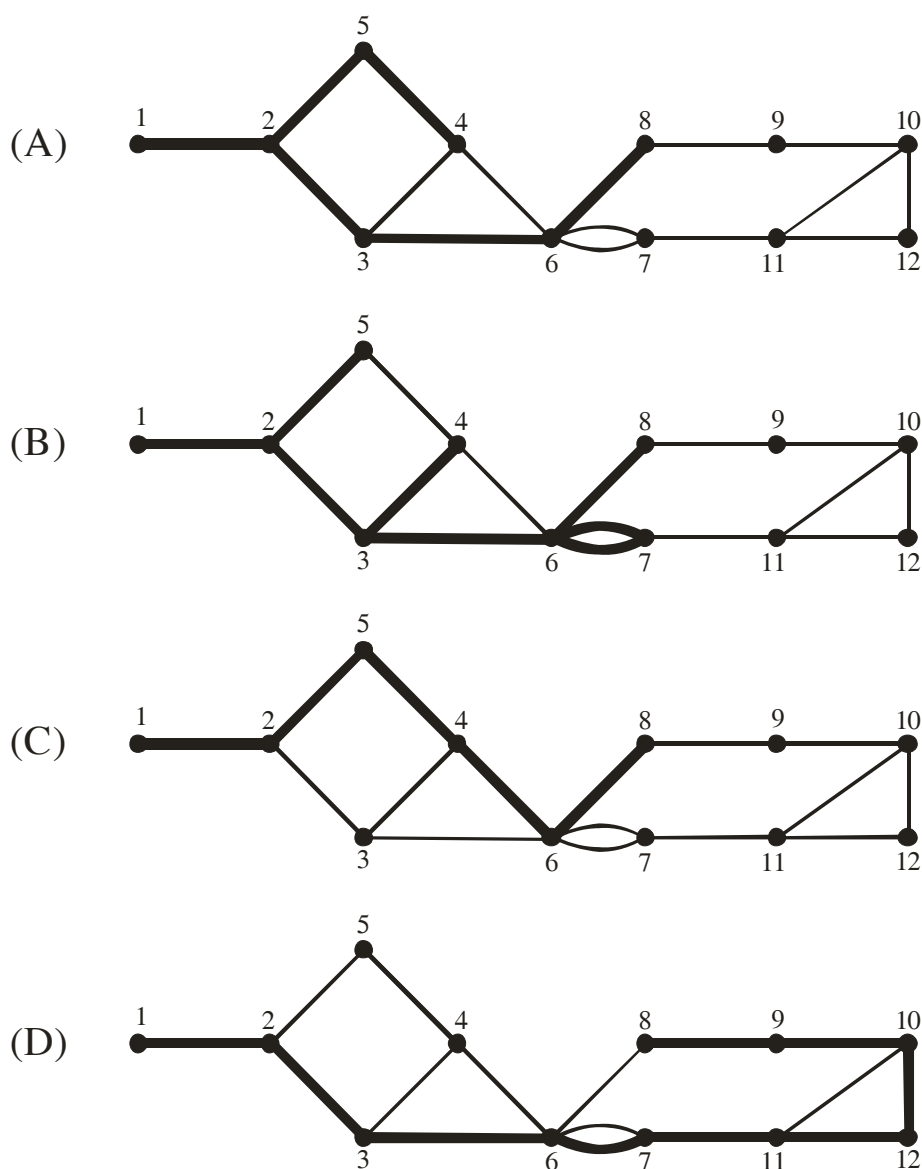
Graf reprezentujúci plán poschodia:



- (b) Urobte prehľadávanie do šírky a do hĺbky, so štartom v miestnosti 1 a cieľom v miestnosti 8.

Grafy prehľadávania do šírky a do hĺbky, so štartom v miestnosti 1, keď cieľom je prísť do miestnosti 8. Uvádžeme kostru vytváranú pri prehľadávaní. Pri prehľadávaní do šírky – grafy (A), (B) aj do hĺbky – grafy (C), (D) uvádzame najprv graf, kedy prehľadáваме miestnosti podľa poradia „najprv vľavo“, ako druhý uvádzame graf pre poradie „najprv vpravo“:





(c) Porovnajete, ktorý zo spôsobov prehľadávania by ste odporučili.

Pokiaľ meriame iba počet nových dverí, ktorými sme prešli, najvýhodnejšie je prehľadávanie do hĺbky podľa poradia „najprv vľavo“, potom ide prehľadávanie do šírky podľa poradia „najprv vľavo“, za ním ide prehľadávanie do šírky podľa poradia „najprv vpravo“, a nakoniec ide prehľadávanie do hĺbky podľa poradia „najprv vpravo“. Samozrejme, pri prehľadávaní neznámeho grafu sa nedá vopred odporučiť najlepšia stratégia.

# LITERATÚRA

- [1] Bečvář, J.: *Lineární algebra*. Matfyzpress, Praha, 2000.
- [2] Bučko, M.; Klešč, M.: *Diskrétna matematika*. Elfa, Košice, 2006.
- [3] Čada, R.; Kaiser, T.; Ryjáček, T.: *Diskrétní matematika*. Západočeská univerzita v Plzni. Plzeň, 2004.
- [4] Galanová, J.; Kaprálik, P.: *Diskrétna matematika*. STU, Bratislava, 1997.
- [5] Garnier, R.; Taylor, J.: *Discrete Mathematics for New Technology*. Institute of Physics Publishing, Bristol and Philadelphia, 1999.
- [6] Hein, J. L.: *Discrete Structures, Logic, and Computability*. Jones and Bartlett Publishers, Sudbury, MA, 2002.
- [7] Jablonskij, S. V.: *Úvod do diskrétnej matematiky*. Alfa, Bratislava, 1984.
- [8] Knor, M.: *Kombinatorika a teória grafov I*. Univerzita Komenského, Bratislava, 2000.
- [9] Knor, M.; Niepel, L.: *Kombinatorika a teória grafov II*. Univerzita Komenského, Bratislava, 2000.
- [10] Kolář, J.; Štěpánková, O.; Chytil, M.: *Logika, algebry a grafy*. SNTL, Praha, 1989.
- [11] Kvasnička, V.; Pospíchal, J.: *Matematická logika*. STU, Bratislava, 2006.
- [12] Matoušek J.; Nešetřil, J.: *Kapitoly z diskrétní matematiky*. Matfyzpress, Praha, 1996.
- [13] Preparata, F. P.; Yeh, R. T.: *Úvod do teórie diskrétnych matematických štruktúr*. Alfa, Bratislava, 1982.
- [14] Rosen, K. H.: *Discrete Mathematics and Its Applications*. McGraw Hill, Boston, 2003.

# REGISTER

- $\neg$  negácia, 6, 47, 144, 160
  - $\vee$  disjunktia, 5, 13, 46, 47, 144, 146, 160, 187
  - $\oplus$  exkluzívna disjunktia, XOR, 174
  - $\otimes$  súčin binárnych matíc, **187-189**
  - $\exists$  existenčný kvantifikátor, 11-14
  - $\Rightarrow$  implikácia, 4, 5, 9, 12-13, 15-16
  - $\wedge$  konjunktia, 4, 12, 21, 46-47, 144, 160, 187
  - $\forall$  univerzálny (všeobecný) kvantifikátor, 11-13
  - $U$  univerzum, 11-13, 30-35, 113, 119
  - $\emptyset$  prázdna množina, **31**, 128, 145
  - $\subset$ , vlastná podmnožina  $A \subset B$ , **32**
  - $\subseteq$ , podmnožina, tiež podgrupa,  $A \subseteq B$ , **32**, 40, 113, 131, podmonoid 142
  - $\cup$  zjednotenie množín, **32-33**, 37-38, **46**, 113, 124, 144, 168, zjednotenie relácií **54**, zjednotenie grafov, **234**
  - $\cap$  prienik množín, **32-33**, **46**, 113-114, 124, 144, prienik relácií **54**, prienik grafov, **234**
  - $\bar{A}$  doplnok (komplement) množiny, **32**, **47**, **113**, 144, doplnok relácie, **54**, doplnkový graf, **252**
  - $\bar{x}$  komplement premennej Boolovej algebry, **144-148**
  - $\setminus$  rozdiel množín (relatívny doplnok),  $A \setminus B$ , **32-34**
  - $\in$  prvok  $a$  patrí do množiny,  $a \in A$ , **30-32**
  - $\notin$  prvok  $a$  nepatrí do množiny,  $a \notin A$ , **30-32**
  - $\exists!x$  existuje práve jeden prvok  $x$ , ktorý spĺňa dané podmienky, 66, 70, 123
  - $\lceil x \rceil, \lfloor x \rfloor$  horná, dolná celá časť, 62, 84, 116
  - $\mathbb{Z}$  množina celých čísel, 60, 129
  - $\mathcal{P}(A)$  potenčná množina množiny  $A$ , **40**, 124, 137
  - $\mathbb{R}_+$  množina kladných reálnych čísel, 129, 136
  - $e$  neutrálny prvok, **124-126**, 128, 145
  - $E$  jednotková matica, **179**, 183, 194
  - $a^{-1}$  inverzný prvok (v grupe), **124-126**, 129
  - $A^{-1}$  inverzná matica, **194-197**
  - $R^{-1}$  inverzná relácia, **53**
  - $f^{-1}$  inverzná funkcia, **69-70**
  - $A^T$  transponovaná matica, **179**
  - $\equiv$  ekvivalentnosť, 144, 146, **149**
  - $\#'$  „prázdny“ symbol, 166
  - $\varepsilon$  prázdny znak, 128, prázdny reťazec 137
  - $\chi(G)$  chromatické číslo grafu, **266**, **269**
  - $C_n$  kružnica (graf), **233**, 237, 244
  - $K_n$  kompletný graf, **233**
  - $K_{n,m}$  kompletný bipartitný graf, 234
  - $W_n$  graf typu koleso, 251
  - $Q_n$  hyperkocka, 246, 260-261
- ## A
- Abel, Niels Henrik, **127**
  - Abelova pologrupa, **127**
  - absorpcia, **34**, **147**
  - adícia, **4**, **5**
  - aktivačná (alebo sigmoidová prechodová) funkcia, **71**
  - algebra 19, 244
    - teórie množín, **33**, 46
    - Boolova, **143-147**, 155-156
    - maticová, **177-226**
  - algebraické štruktúry, **123-176**
  - algebraický výraz, strom, **287-288**
  - algoritmus
    - 4.1., náhodne generovanie permutácie, **88**
    - 4.2., systematické generovanie všetkých permutácií, **89**
    - 5.1., rekurzívny pre výpočet faktoriálu, **100**
    - 5.2., Hanojské veže, **106-107**
    - 5.3., rekurzívne delenie intervalu pri hľadaní minimálneho prvku, **110**

- 5.4., Eratostenovo sito, **116**
- 8.1., násobenie matíc, **184**
- 10.1., konštrukcia uzavretého eulerovského ťahu prehl'adávaním do hĺbky, **240**
- 10.2., konštrukcia otvoreného eulerovského ťahu prehl'adávaním do hĺbky, **241**
- 10.3., pre konštrukciu všetkých možných hamiltonovských ciest, **248**
- 11.1., Dijkstrov, **259**
- 11.2., greedy, zafarbenie obyčajného grafu, **267**, greedy Quinova a McCluskeyho metóda, 169, greedy konštrukcia zátvorkovania pri násobení matíc, 186
- 12.1., prehl'adávanie binárneho stromu, resp. priradenie nového záznamu, **282**
- 12.2., Huffmanove kódovanie, **286-287**
- 13.1., minimálne časové ohodnotenie v sieti, **302-304**
- 13.2., maximálne časové ohodnotenie v sieti, **304-305**
- 13.3., určenie maximálneho toku v sieti, **305-307**
- 13.4., Primov, na minimálnu kostru, **308-309**
- 13.5., Kruskalov, na minimálnu kostru, **309**, 322
- 13.6., prehl'adávanie do hĺbky s rekurziou, **310-311**
- 13.7., prehl'adávanie do hĺbky pomocou zásobníka, **311-312**
- 13.8., prehl'adávanie do hĺbky s výpisom cesty od koreňa, **313-314**
- 13.9., prehl'adávanie do šírky s radom, **319-321**
- Ford-Fulkersonov, **306-307**
- polynomiálny, 260, 284
- „rozdeľuj a panuj“, **108-113**
- usporiadania so spájaním (merge sort), **111-113**
- binárne prehl'adávanie, **108-109**

algoritmus, zložitost', 100, 108-109, 112, 169, 184, 237, 259, 267, **284**, 295, 309, 310, 319

alkány, 277-278

antisymetrická relácia, **58**

argument, 1-2, **66**

artikulácia, **238**

asociatívna binárna operácia, **124**, 127, 129

asociatívnot', **33**, **145**, 183

axióma, 1-3, 15, 20

axiomatická výstavba teórie množín, 29, 39

axiomatický systém, 2-4, 20

axiomatizácia, 39

## B

backtracking, **310-311**

bijekcia, **70**, 136, 215, 236

bijektívne zobrazenie, 71, 88, 133, 137

binárna matica, 55, **187**

- , disjunkcia, 187
- , konjunkcia, 187
- , mocnina, 188
- , súčin, 187

binárna relácia, **53-55**

binárne prehl'adávanie, **108-109**, **282-283**

binárny strom, **280**, **282-283**, 286

binomická veta, **82**

binomický koeficient, **81-82**, 83-84, 91, 185

bipartitný graf, **233-234**, 260

Boole, George, **143**

Boolova algebra, 33, **143-147**

Boolova formula, **148**

Boolova premenná, **148**

Boolova funkcia, 143-144, 148, **149-155**, 159, 164, 172

Brooks, Rowland Leonard, 266

## C

Cantor, Georg, 29

Cayley, Arthur, **277**

Cayleyho (multiplikačná) tabuľka, 124

cesta, 3, **237-238**, 279, 307, 310

- , dĺžka, **79**, **242**, 243, 248, **257-259**, 280, 302, 312, 321
- hamiltonovská, **244**, 260
- minimálnej dĺžky, 243, 257-259, 312-313
- optimálna (alebo minimálna), 79-80, 248
- orientovaná, 58, 242
- kritická, **301-305**

Cramer, Gabriel, **222**

Cramerovo pravidlo, **222**  
 cyklomatické číslo grafu, **281**  
 cyklus, okruh, **237, 242**  
 časové ohodnotenie earliest a latest, **302**  
 čiastočne usporiadaná množina (poset), **63**  
 čiastočné usporiadanie, **62-65**, 167-168  
 číslo grafu  
 – cyklomatické, **281**  
 – hranové chromatické  $\chi_{\text{hranové}}(G)$ , **269**  
 – chromatické  $\chi(G)$ , **266-267**  
 – priesečníkové (crossing number), **274**  
 – vrcholovej nezávislosti, **269-270**

**D**

dámy, problém  $n$  dám, 269-270, **316**  
 De Morgan, August, 267  
 De Morganove zákony, 17, 27, **34**, 113, **144**,  
**147**  
 dedukcia, veta o, **8**  
 deduktívny dôkaz, **2**  
 definícia, obor definície funkcie, **66**  
 derangementálna permutácia, **117-118**  
 Descartes, René, **43**  
 determinant, 194, **214-222**  
 –, výpočet, 217, 220-221, 222  
 diagonálna matica, **179**  
 diagonálny prvok, **179**, 192, 219, 221  
 diagram Hasseho, **64-65**, 168, 170  
 diagram Vennov, 33-34, 43  
 dihedrálna grupa, **133**, 135  
 Dijkstra, Edsger, 258-259, 308  
 Dijkstrov algoritmus, **258-259**  
 Diracova teoréma, **245**  
 disjunkcia binárnych matíc, 187  
 disjunkcia, logická brána, 160  
 disjunktívna normálna forma (DNF), 151-154,  
 165  
 disjunktívny sylogizmus, **5**  
 disjunktívny rozklad, 37, 60, **61-62**  
 distributívne zákony pre rozdiel množín, **34**, 36  
 distributívnosť, **33**, 45, 57, **145**  
 dĺžka cesty, **79**, **242**, 243, 248, **257-259**, 280,  
 302, 312, 321  
 dĺžka oblasti (stupeň steny), **262**

dodekaéder (dodekahedron), **244**  
 dominujúca množina, **269**  
 dominancia, **34**, 230  
 doplnkový (príp. komplementárny, comple-  
 mentary) graf, **252**  
 doplnok (komplement) množiny, **32**, 33  
 doplnok relácie, **54-55**  
 doplnok, relatívny (rozdiel množín), **32-33**, **34**,  
 36  
 dôkaz „kombinatorický“, **91**, 92-93  
 dôkaz nepriamy, **16**  
 dôkaz priamy, **15**, 106  
 dôkaz sporom, **16**, **22-23**  
 dôkaz vymenovaním prípadov, **17-19**, 57  
 dôkaz deduktívny, **2**  
 dôsledok, potvrdenie, 16, 18  
 „dualizmus“ výrokovej logiky a teórie množín,  
**144**  
 duálna forma rovnosti, **146**  
 duálny graf k mape, **264-265**  
 dvojité sumátor, **162-163**

**E**

ekvivalencia, 144, relácia **60**, 146  
 –, trieda, **61-62**  
 – Boolových formúl, **149-150**  
 ekvivalentné matice, **191-192**  
 elektronický obvod, 143, 172, 228, 261, 274  
 – spínací **155-159**  
 – logický **159-163**  
 element (prvok), 11, **29-30**, 63, 123-124, 171,  
 178, 182, 197  
 elementárny pojem, 2, 29, 30  
 enumerácia, **37-42**, 103, 105, 107, 115  
 Eratosthenes, **115**  
 Eratostenovo sito, **115-116**  
 Euler, Leonhard, **227-228**  
 Eulerova formula, **262**  
 eulerovský ťah, **237-238**, 240-241  
 existenčný kvantifikátor, konkretizácia, 11, 13  
 existenčný kvantifikátor, zovšeob., 11, 14  
 existuje práve jeden prvok  $x, \exists!x$ , 66, 123  
 exklúzia a inklúzia, metóda, **113-118**  
 exkluzívna disjunkcia,  $\oplus$ , XOR, 174

**F**

- faktoriál, 100
- rekurzívne, **100**
- falzifikácia, **13**
- farbenie **264-269**
- “k-tuple”, **268**
- grafu, 266-267
- grafu pomocou prehľadávania do hĺbky, 316
- grafu pomocou greedy algoritmu, **267**
- mapy, 264-265
- Fermatova veta, Veľká, **19**
- Fibonacci, vlastným menom Leonardo Pisano, **102**
- Fibonacciho čísla, **102**, 104
- Ford, Lester Randolph, 306
- Ford-Fulkersonov algoritmus, **306-307**
- forma, disjunktívna normálna (DNF), 151-154, 165
- forma, konjunktívna normálna (KNF), 154
- formula
- Boolova, **148-149**, 150, 165
- Eulerova, **262-263**
- Stirlingova, 285
- , ekvivalentnosť Boolových formúl, **149-150**
- rekurentná, **99-108**
- Frobeniova veta, **208**, 212
- Frobenius, Ferdinand Georg, **208**
- Fulkerson, Delbert Ray, 306
- funkcia
- Boolova, 143-144, 148, **149-155**, 159, 164, 172
- charakteristická, **31-32**, 36, 42, **46**, 53, 55-56
- inverzná, **69-72**
- jedno-jednoznačná (injekcia), **69**, 136, 137, 139
- jednotková, **67**, 70-72
- sigmoidová prechodová (alebo aktivačná), **71**
- spínacia, **156-157**
- zložená, **67-69**
- funkcie, rovnosť, **67**
- funkčná hodnota (obraz), **66**, 152-155
- , obor, **66-67**

**G**

- Gauss, Carl Friedrich, **210**
- Gaussova eliminačná metóda, **210-212**
- generovanie permutácií, **88-89**
- genetické programovanie, 288
- geometrická interpretácia rovnice, **206-208**
- graf, 228
- bipartitný, **233-234**, 260
- doplnkový (príp. komplementárny, complementary), **252**
- duálny k mape, **264-265**
- kompletný, **233**, 261, 266
- kompletný bipartitný, 233-234, 260-261
- neorientovaný, **228**, 231, 236-237, 278
- obyčajný, 229, 235-236, 245, 253, 262, 308
- ohodnotený, 258, 283, 293, 301
- orientovaný, 59, **228-229**, 230, 231, 235-236, 242, 302, 305
- ovplyvňovania, 250
- Petersenov, **264**, 266
- planárny, **260-264**, 267, 274
- plánovania udalostí, **230**
- pravidelný (regular), **252**
- prienikový (intersection graph), **250**
- riedky, 259, 309
- samokomplementárny (selfcomplementary), **253**
- silno/slabo súvislý, **242**
- súvislý, **237-243**, 262-263, 277, 308
- zmiešaný, 228
- , farbenie, 266-267
- , hranové chromatické číslo  $\chi_{\text{hranové}}(G)$ , 269
- , chromatické číslo  $\chi(G)$ , **266-267**
- , multigraf, **228-229**, 236
- , pseudograf, 229, 235
- , rovinná (planárna) reprezentácia, **260-262**
- grafová postupnosť, **231-232**
- grafy Kuratowského, **263**
- grafy, zjednotenie, **234**, 237
- Gray, Frank, 246
- Grayov kód, **246**
- greedy algoritmus, 169, 186, 187, 267, 308

grupa, **129**

- dihedrálna, **133**, 135
- permutácií, **133-135**, 215
- symetrická, 133-135, 215
- , rád, **129**, 131
- , stred, **142**
- grupoid, **123**

## H

- Hamilton, William Rowan, **244**, 267
- hamiltonovská cesta, **244**, 245-246, 248
- hamiltonovská kružnica, **244-248**, 259-260, 319
- Hammingova vzdialenosť, **165**, 166
- Hanojské veže, **104-107**
- Hasseho diagram, **64-65**, 168, 170
- Havlova a Hakimiho veta, **232**
- hierarchicky usporiadané pravidlá, **289**
- hlavná diagonála, **179**
- hlúbka stromu, **280**, 281, 284, 285, 289, 318
- hodnosť matice, **189-194**, 209, 213-214, 218
- homogénna sústava lineárnych rovníc, **212-214**
- homomorfizmus, **137-138**
- hra, 104, 118, 244, 288
- , stav, 288-290, **292**, 315
  - , stavový priestor, **292**
- hrana, 2-3, 58-60, 64, 227, **228**
- incidentná s vrcholmi, **230**
  - násobná, **229**, 235
  - orientovaná, **229**, 231, 236
  - , váha, **257**, **301**
  - , zafarbenie, **269**
- hranové chromatické č. grafu  $\chi_{\text{hranové}}(G)$ , **269**
- hrúbka (thickness) jednoduchého grafu, **274**
- Huffman, David, 286
- Huffmanove kódovanie, **286-287**
- hviezda (topológia grafu), 234, 251
- hyperkocka, 246, 260-261
- hypotetický sylogizmus, **4-5**

## CH

- charakteristická funkcia, **31-32**, 36, 42, **46**, 53, 55-56

chemický vzorec, 277-278

chromatické číslo grafu  $\chi(G)$ , **281**

## I

- idempotentnosť, **34**, **147**
- idempotentný prvok, 142
- identita
- Pascalova, **82**, 86
  - Vandermondeova, **86**
- implikácia, inverzia, **5**, **16**
- incidenčná matica, **236**
- incidentná hrana s vrcholmi, **230**
- indexový register, farbenie, 268
- indukcia, matematická, **19-21**, 37-38, 45, 82, 101, 106, 108, 151, 243, 262, 280, 281
- indukcia, silná matematická, **21**
- induktívne usudzovanie, **2**
- induktívne zovšeobecnie, **2**, **13**
- infixová notácia, **288**
- injekcia (jedno-jednoznačná funkcia), **69**, 136, 137, 139
- inklúzia a exklúzia, metóda, **113-118**
- interpretácia, 3, 5, 8, 11, 58-60, 146, 188
- interpretácia množiny, geometrická, **206-208**
- invariant vzhľadom na izomorfizmus, 236
- invarianty, 269
- inverzia implikácie, **5**, **16**
- inverzia permutácie, 134-135, 215
- inverzná funkcia, **69-72**
- inverzná matica, **194-197**
- , konštrukcia, **195-197**
- inverzná relácia, **53**
- inverzný prvok, **124-126**, 129, 136, 147
- involúcia, **34**
- involutívnosť komplementu, **147**
- izolovaný vrchol, **231**
- izomorfizmus, **136-137**, **234-237**

## J

- Jarník, Vojtěch, 308
- jedno-jednoznačná funkcia (injekcia), **69**, 136, 137, 139
- jednotková funkcia, **67**, 70-72

jednotková matica  $E$ , **179**, 183, 194  
 „jednotkový“ prvok, 125, 128  
 jednoznačnosť neutrálnych a inverzných prvkov, **126**, **129**, 130, 147

## K

„kanonická“ reprezentácia Boolovej funkcie, 150, 152  
 kapacita rezu, **305-307**  
 kapacita spojenia (priepustnosť), **305**  
 kapacitná sieť, **305**  
 kardinalita (mohutnosť), **36**, 37, 42, 45, 48, 113, 129, 134  
 Karnaughove mapy, 164  
 karteziánsky súčin, **42-46**, 53-54, 58, 127  
 klauzula, **150**  
 – minimálna, 168-170  
 – súčinová, **150**, 152, 165-166  
 – súčtová, **150**, 152  
 –, „pokrytie“, **167-171**  
 kocka, ( $n$ -kocka), 246, 251, 261  
 kód Grayov, **246**  
 kód prefixový, **285-287**, 288  
 kódovanie Huffmanove, **286-287**  
 kódovanie nestratové, 285  
 koleso, 251  
 kombinácie, 91, 93, 246  
 „kombinatorický dôkaz“, **91**, 92-93  
 komplement (doplnok) množiny, **32**, 33  
 –, involutívnosť, **147**  
 komplement grafu, **252**  
 komplementy konštánt, **147**  
 kompletný bipartitný graf, 233-234, 260-261  
 kompletný graf, **233**, 261, 266  
 komponent grafu, 3, **237-238**, 262, 281  
 kompozícia relácií, **56-58**, 188  
 kompozicionalita, princíp, **35**  
 komunikačná sieť, 255, 278  
 komutatívna  
 – binárna operácia, **124**  
 – operácia, 129, 146, 152, 183  
 – pologrupa, **127**  
 – grupa, **129**, 136-137  
 komutatívnosť, **33**, 137, **144**

konjunkcia, **4**, 12, 21, 46, 144, 146  
 – binárnych matíc, **187**  
 –, logická brána, **160**  
 konjunktívna normálna forma (KNF), 154  
 konkretizácia  
 – existenčného kvantifikátora, 11, 13  
 – univerzálneho kvantifikátora, 11, 12  
 konštanta 0 a 1, **144-145**, 148  
 konštrukcia inverznej matice, **195-197**  
 kontradikcia, 5, 16-17, 39, 146  
 konzistentnosť, 2, 5, 29  
 koobor, **66**  
 korektnosť, 1-2, 33-34, 39  
 koreň  
 – algebraickej rovnice, 86  
 – stromu, **279**, 282  
 koreňový strom, **279-281**, 287-288  
 kostra (spanning tree), 308, 310-313, 321  
 kostra, minimálna, 308-309  
 kôň, problém knight tour, **245-246**, **318-319**, **321-322**  
 krátenie sprava a zľava, 130  
 kritická cesta siete, **301-305**  
 Kruskal, Joseph, 309  
 Kruskalov algoritmus, **309**, 322  
 kružnica  
 – v grafe, **233**, 237-239, 242, 263, 278, 281  
 – hamiltonovská, **244-248**, 259-260, 319  
 Kuratowského grafy, **263**  
 Kuratowského veta, **263**  
 Kuratowski, Kazimierz, **263**  
 kvantifikátor  
 – existenčný, konkretizácia, 11, 13  
 – existenčný, zovšeobecnenie, 11, 14  
 – univerzálny, konkretizácia, 11, 12  
 – univerzálny, zovšeobecnenie, 11, 12, 13, 20

## L

Lagrangeova veta, **131**  
 ľavý nasledovník, **280**, 282  
 Leibniz, Gottfried Wilhelm, 43  
 lema, 1  
 les, 278, 281, 286-287  
 lineárna kombinácia vektorov, **190**, 192



lineárna závislosť vektorov, **189-190**, 193,  
218-219  
lineárne rovnice, sústava, **205-214**, 221-222  
lineárny priestor, **44**, 219  
list, **279**, 280-281, 288  
literál, **148**, 150, 163-164  
logické brány disjunkcie, konjunkcie a negácie  
160  
logický obvod, **159-163**  
logický obvod, optimalizácia, **163-171**  
logické siete, **172**  
logika, predikátová, 11-15  
Lucas, Édouard, 104

## M

mapa 258  
– Karnaughova, 164  
– politická, 264-265  
– rovinná, 262  
–, farbenie, 264-265  
matematická indukcia, **19-21**, 37-38, 45, 82,  
101, 106, 108, 151, 243, 262, 280, 281  
matica  
–,  $\alpha$ -násobok, **182**  
– binárna, 55, **187**  
–, definícia, **177-181**  
–, determinant, **214**  
– diagonálna, **179**  
–, hlavná diagonála, **179**, 219, 235  
–, hodnosť, **189-194**  
– incidenčná, **236**  
– inverzná, **194**  
– inverzná, konštrukcia, **195-197**  
– jednotková, **179**  
– koeficientov (m. sústavy), **205**, 209, 213  
– nulová, **179**  
– obdĺžniková, **179**  
– regulárna, **194**, 221  
– relácie, 55  
– susednosti, **235-236**, 243  
– sústavy (m. koeficientov), **205**, 209, 213  
– sústavy, rozšírená, **208**  
– symetrická, **180**  
– štvorcová, **179**

– transponovaná, **179-180**  
– trojuholníková, **180**  
–, typ, **178**  
matice, ekvivalentné, **191**  
matice, rovnosť, **182**  
matice, súčet, **182**  
matice, súčin, **182**, **187**  
matice, zložitost' násobenia, 184  
maticová algebra, **177-226**  
Maurolico, Francisco, 20  
maximálny prvok, **63**, 65  
maximálny tok, **305-307**  
McCluskey, Edward J., **165**  
McCulloch, Warren, a Pitts, Walter, 159  
merge sort - usporiadanie so spájaním, **111-113**  
metóda inklúzie a exklúzie, **113-118**  
metóda kritickej cesty, CPM Critical path met-  
hod, **301-305**  
metóda Gaussova eliminačná, **210-212**  
metrika, **79**, 165  
minimalizácia Boolových výrazov, **164-171**  
minimálna dominujúca množina, **269**  
minimálna kostra, 308-309  
minimálne klauzuly, 168-170  
minimálny prvok, **63**, 65  
minimálny rez, **305-307**  
minimax princíp, 293-294  
množina  
– dominujúca, **269**  
–, doplnok, **32**, 33  
–, komplement, **32**, 33  
– minimálna dominujúca, **269**  
–, mohutnosť, **36**, 37, 42, 45, 103, 113-114,  
129, 134, 178  
–, operácie, 31-33, 46-47, 123-124, 144-146  
– potenčná, **40-42**, 63-64, 124-125, 128, 137  
– prázdna, **31**, 125, 128  
– prípustných akcií, 292  
–, prvok (element), 11, **29-30**, 63, 123-124,  
171, 178, 182, 197  
–, rodina, **39-40**  
– vlastná, **32**  
množinová algebra, **33**, 46

množiny  
 –, karteziánsky súčin, **42-46**, 53-54, 58, 127  
 –, prienik, **32-33**, 40, 46-47, 54, 68, 113-114, 124, 128, 144  
 –, rovnosť, **31-32**, 42, 144  
 –, rozdiel, **32-33**, 34  
 –, zjednotenie, **32-33**, 38, 40, 46, 54, 113, 124, 144  
 mocnina binárnych matíc, 188  
 mocniny relácie  $R$ , 188  
 model, 3, 144, 290  
 modus ponens, **4-5**  
 modus tollens, **4-5**  
 Mohamedova šabl'a, **239**  
 mohutnosť (kardinalita), **36**, 37, 42, 45, 48, 113, 129, 134  
 monoid, **128-129**, 137, 142  
 Montmort, de, Pierre Raymond, 118  
 morfizmy, **135-138**, **234-237**  
 most grafu, **238**, 262  
 mosty Královca, 227-228  
 multigraf, 228, 229, 236  
 multimnožina, 92-93  
 multinomická veta, **87**  
 multiplicita, 229  
 multiplikačná (Cayleyho) tabuľka, 124

## N

$n$ -árny strom, **280**  
 nasledovník, 279-280, 282  
 $\alpha$ -násobok matice, **182**  
 násobenie matíc, **182**, **187**  
 –, zložitost', 184  
 násobná hrana, 227, 228, **229**, 235-236  
 negácia, logická brána, 160  
 neorientovaný graf, **228**, 231, 237  
 nepriamy dôkaz, **16**  
 nerovnosť, „trojuholníková“, **79**, 260  
 nestratové kódovanie, 285  
 neurónové siete, 71, 159, 172  
 neutrálny prvok, **124-126**, 128, 129, **145**, 147  
 notácia  
 – Omega, 284  
 – Omikron, 284

– infixová, **288**  
 – postfixová (reverzná poľská), **288**  
 – prefixová (poľská), **288**  
 – Theta, **284**  
 notácie Boolovej algebry, 145, 148  
 NP-úplný problém, 260, 284  
 $n$ -uholník, **233**, 234, 237  
 nulitnosť, **147**  
 nulová matica, **179**  
 „nulový“ prvok, **125**

## O

obchodný cestujúci, problém, **248**, 258-260  
 oblasť, dĺžka (stupeň steny), **262**  
 oblasti v množine univerza, 35  
 obor definície, **66**  
 obor funkčných hodnôt, **66-67**  
 obraz, funkčná hodnota, **66**, 152-155  
 obvod elektronický, 143, 172, 228, 261, 274  
 obvod logický, **159-163**  
 obvod spínací, **155-159**  
 obyčajný graf, 229, 235-236, 245, 253, 262, 308  
 odlišiteľné prvky, **29-30**, 92-93  
 odvodenie, strom, 7-8  
 ohodnotený graf, 258, 283, 293, 301  
 okruh, cyklus, **237**, **242**  
 Omega notácia, 284  
 Omikron notácia, 284  
 operácia  
 – symetrie, 132-133  
 – asociatívna binárna, **124**, 127, 129  
 – binárna, **123-124**  
 – komutatívna, 129, 146, 152, 183  
 – komutatívna binárna, **124**  
 – nad množinami, **31-34**, **46-47**  
 – nad reláciami, **54-56**  
 optimalizácia logických obvodov, **163-171**  
 optimálna (alebo minimálna) cesta, 79-80, 243, 248, 257-259, 312-313  
 Oreho teoréma, **245**  
 orientovaná cesta, 58, 242  
 orientovaný graf, 59, **228-229**, 230, 231, 235-236, 242, 302, 305

**P**

- paralelné zapojenie – súčet premenných, 156  
 paralelné spracovanie, 230, 301  
 Pascal, Blaise, **81**  
 Pascalov trojuholník, **81**, 82-83, 85  
 Pascalova identita, 82  
 Peano, Giuseppe, 20  
 permutácia, **88**, 152, 216, 260, 317  
 – ako bijekcia, 88, **215**  
 – ako postupnosť ťahov piškvoriek, 294  
 – derangementálna, **117-118**  
 –, generovanie, **88, 89**  
 –, grupa, **133-135**  
 – s opakovaním, **92, 93**  
 –, strom konštrukcie, **90**  
 –, súčin, 134-135  
 Petersen, Julius, 264  
 Petersenov graf, 264, 266  
 Pisano, Leonardo, nazývaný Fibonacci, **102**  
 piškvoriky, 288-295  
 planárna (rovinná) reprezentácia grafu, 260-261  
 planárny graf, **260-264**, 267, 274  
 plánovanie udalostí, graf, **230**  
 plne  $n$ -árny strom, **280-281**  
 počet riešení sústavy lineárnych rovníc, 206-208  
 –, 1 riešenie, 206-208  
 –, nekonečne veľa riešení, 206-208  
 –, nemá riešenie, 206-208  
 počítačové, transportné siete, 228, 237, 257, 305, 308  
 podgraf, **234**, 237, 263, 266, 279, 308, 310  
 podgrupa, **131-132**, 135, 136, 142  
 podgrupa, triviálna, **131**  
 podmnožina, 13, **32-33**, 37, 40, 53-54, 67, 91, 131, 132, 142, 233  
 podmonoid, **142**  
 podstrom, **279**  
 pohyb v stavovom priestore hry, 292  
 pojem, elementárny, 2, 29, 30  
 „pokrytie“ klauzúl, **167-171**  
 pokrytie prvku, **64, 167**  
 politická mapa, 264-265  
 pologrupa, **127-128**  
 – Abelova, **127**  
 – komutatívna, **127**  
 polosumátor, **161-163**  
 polynomiálny algoritmus, 260, 284  
 Popper, Karl 13  
 popretie predpokladu, **10**  
 poset (čiastočne usporiadaná množina), **63**  
 postfixová (reverzná poľská) notácia, **288**  
 postupnosť stupňov vrcholov grafu, **231-232**  
 postupnosť ťahov piškvoriek – permutácia, 294  
 potenčná množina, **40-42**, 63-64, 124-125, 128, 137  
 potomok, **279-280**  
 potvrdenie dôsledku, 16, 18  
 pravidelný (regular) graf, **252**  
 pravidlá odvodzovania, 2, 16  
 pravidlo  
 – Cramerovo, **222**  
 – Sarrusovo, **216-217**  
 pravý nasledovník, 279-280, 282  
 prázdna množina  $\emptyset$ , **31**, 128, 145  
 „prázdny“ symbol '#', 166  
 predchodca, **279-280**  
 predikát, 13, **30**  
 predikátová logika, 11-15  
 predok, **279-280**  
 predpoklad, popretie, **10**  
 prefixová (poľská) notácia, **288**  
 prefixový kód, **285-287**, 288  
 prehľadávanie  
 – binárne, **108-109, 282-283**  
 – binárneho stromu, **282**  
 – do hĺbky (Depth-First Search, DFS), spätné, backtracking, **310-311**  
 – do šírky (Breadth-First Search, BFS), **319-322**  
 – stromu riešení, 89, 186, **289-290**, 293, 317  
 premenná, Boolova, **148**  
 priamy dôkaz, **15**, 106  
 prienik množín, **32-33**, 40, 46-47, 54, 68, 113-114, 124, 128, 144  
 prienik relácií, **54**

- prienikový graf (intersection graph), **250**  
 priepustnosť (kapacita spojenia), **305**  
 priesečníkové číslo (crossing number) obyčajného grafu, **274**  
 priestor, lineárny, **44**, 219  
 Prim, Robert, 308  
 Primov algoritmus, **309**, 322  
 princíp  
 – kompozicionality, **35**  
 – minimax, 293-294  
 – duality, **144**, **146**  
 prípustné akcie, množina, 292  
 priradenie frekvencií, farbenie, 267-268  
 problém  
 – knight tour, **245-246**, **318-319**, **321-322**  
 –  $n$  dám, 269-270, **316**  
 – NP-úplný, 260, 284  
 – obchodného cestujúceho, **248**, 258-260  
 – sumy podmnožín, 317-318  
 projekt, sieť, 301-305  
 prvok (element), 11, **29-30**, 63, 123-124, 171, 178, 182, 197  
 – idempotentný, 142  
 – inverzný, **124-126**, 129, 136, 147  
 – „jednotkový“, 125, 128  
 – maximálny, **63**, 65  
 – minimálny, **63**, 65  
 – neutrálny, **124-126**, 128, 129, **145**, 147  
 – „nulový“, **125**  
 –, pokrytie, **64**, **167**  
 pseudograf, **229**, 235
- Q**
- Quine, Willard Van Orman, **165**  
 Quinova a McCluskeyho metóda, **164-171**
- R**
- rad – queue, 319-321  
 rád grupy, **129**, 131  
 recontres, 118  
 reductio ad absurdum, **5**, 16, 22  
 reflexívna relácia, **58**, 59-60, 62  
 regulárna matica, **194**, 221  
 rekurentná formula, **99-108**  
 rekurzia, **100**, 311  
 relácia, 42, **53-65**  
 – ako orientovaný graf, **59-60**  
 – antisymetrická, **58**  
 – binárna, **53-55**  
 –, doplnok, **54-55**  
 – inverzná, **53**  
 –, mocnina, 188  
 – reflexívna, **58**, 59-60, 62  
 – symetrická, **58**, 59-60  
 – tranzitívna, **58**, 60, 63  
 relácie  
 –, kompozícia, **56-58**, 188  
 –, operácie, **54-56**  
 –, prienik, **54**  
 –, zjednotenie, **54**  
 reprezentácia grafu rovinná (planárna), 260-261  
 rez  
 –, kapacita, **305-307**  
 – minimálny, **305-307**  
 rezolventa, 9-10  
 riadkový vektor, 178, **180**, 189-190, 192, 219  
 riedky graf, 259, 309  
 riešenie sústavy, **206-208**, 201, 214, 222  
 $r$ -kombinácia, **91**  
 $r$ -kombinácie z  $k$  znakov, **93**  
 rodina množín, **39-40**  
 rovinná (planárna) reprezentácia grafu, 260-261  
 rovinná mapa, 262  
 rovnosť  
 – funkcií, **67**  
 – matíc, **182**  
 – množín, **31-32**, 42, 144  
 rozdiel množín (relatívny doplnok), **32-33**, 34  
 rozhodovací strom, **283-285**, 314  
 rozklad disjunktný, 37, 60, **61-62**  
 rozšírená matica sústavy, **208**  
 rozvrh, farbenie, 267  
 $r$ -permutácie, **88**, **90**  
 $r$ -permutácie pre  $k$  znakov, **93**  
 $r$ -permutácie s opakovaním, **92**  
 Russell, Bertrand, 29, 39

## S

- samokomplementárny (selfcomplementary)  
 graf, **253**
- Sarrusovo pravidlo, **216-217**
- separátor, 93-94
- sériové zapojenie – súčin premenných, 155
- Shannon, Claude Elwood, 269
- schéma usudzovania, **4-6, 11-14, 20**
- sieť
- kapacitná, **305**
  - komunikačná, 255, 278
  - , metóda kritickej cesty, **301-305**
  - neurónová, 71, 159, 172
  - počítačová, transportná, 228, 237, 257, 305, 308
  - projektu, 301-305
  - logická, **172**
- sieťová analýza, **302**
- sigmoidová prechodová (alebo aktivačná)  
 funkcia, **71**
- silná matematická indukcia, **21**
- silno súvislý graf, **242**
- simplifikácia, **4, 12**
- sito, Eratostenovo, **115-116**
- slabo súvislý graf, **242**
- sled, **237-238, 243**
- uzavretý, **237-238**
- spätne prehľadávanie, do hĺbky (Depth-First Search, DFS), backtracking, **310-311**
- spínací obvod, **155-159**
- spínacia funkcia, **156-157**
- spínač, **155**
- spoj, tlačný, 228, 260
- spor, dôkaz, **16, 22-23**
- spor, zákon, **34**
- stack, zásobník, 310, **311-312, 314, 321**
- stav hry, 288-290, **292, 315**
- stavový priestor hry, **292, 318**
- stena, stupeň (dĺžka oblasti), **262**
- Stirlingova formula, 285
- stĺpcová (riadková) hodnosť, **190**
- stĺpcový vektor, **180-181, 190, 208, 212**
- stred grupy, **142**
- strom, 277-296
- ako model, 277-278
  - algebraického výrazu, **287-288**
  - binárny, **280, 282-283, 286**
  - binárny, prehľadávanie, **282**
  - , hĺbka, **280, 281, 284, 285, 289, 318**
  - konštrukcie permutácií, **90**
  - koreňový, **279-281, 287-288**
  - $n$ -árny, **280**
  - odvodenia, 7-8
  - plne  $n$ -árny, **280-281**
  - riešení pre uzavretý eulerovský ťah, 240-241
  - rozhodovací, **283-285, 314**
  - ternárny, **280**
  - usporiadaný koreňový, **280, 282**
  - vyvážený koreňový, **281, 283**
- stupeň steny (dĺžka oblasti), **262**
- stupeň vrcholu, **230-231**
- súčet matíc, **182**
- súčin
- karteziánsky, **42-46, 53-54, 58, 127**
  - matíc, **182, 187**
  - permutácií, 134-135
- súčinová klauzula, **150, 152, 165-166**
- súčtová klauzula, **150, 152**
- suma podmnožín, 317-318
- sumátor binárnych čísel, **161-163**
- susedia, zoznam, **235**
- susedné vrcholy, **230**
- susednosť, matica, **235-236, 243**
- sústava lineárnych rovníc, **205-214, 221-222**
- homogénna, **212-214**
- sústava
- , matica, **205, 208-209, 213**
  - , riešenie, **206-208, 201, 214, 222**
- súvislý graf, **237-243, 262-263, 277, 308**
- sylogizmus
- disjunktívny, **5**
  - hypotetický, **4-5**
- symetrická
- grupa, 133-135, 215
  - matica, **180**
  - relácia, **58, 59-60**
- systém, axiomatický, 2-4, 20

šabl'a Mohamedova, **239**  
 špeciálne matice, 179-180  
 štruktúry, algebraické, **123-176**  
 štvorcová a obdĺžniková matica, **179**

## T

tabuľková metóda pre verifikáciu, 35  
 ťah, 237  
 – eulerovský, **237-238**, 240-241  
 – uzavretý, 228, **237**, 238-240  
 – uzavretý eulerovský, **238**, 239-241, 247  
 tautológia, 5, 9  
 teoréma  
 – Diracova, **245**  
 – Oreho, **245**  
 teória, 2, 29, 33, 39, 123, 144, 227  
 ternárny strom, **280**  
 Theta notácia, **284**  
 tlačný spoj, 228, 260  
 tok, maximálny v sieti, **305-307**  
 torus, 274, 437  
 transformácia, **66**, 133, 143, 193  
 transformácia stavu akciou, 105, **292**  
 transponovaná matica, **179-180**  
 tranzitívna relácia, **58**, 60, 63  
 trieda ekvivalencie, **61-62**  
 triviálna podgrupa, **131**  
 trojuholník Pascalov, **81**, 82-83, 85  
 trojuholníková matica, **180**  
 „trojuholníková“ nerovnosť, **79**, 260  
 typ matice, **178**

## U

umelá inteligencia, 2, **159**, 290  
 univerzálny kvantifikátor  
 –, konkretizácia, 11, 12  
 –, zovšeobecnenie, 11, 12, 13, 20  
 univerzum  $U$ , 11-14, **31**, 113  
 úrokovanie, zložitý, **101**  
 úroveň vrcholu, 186, **280**, 281, 290, 294, 317,  
 320  
 usporiadanie, 18, 42  
 – so spájaním-merge sort, **111-113**

– čiastočné, **62-65**, 167-168  
 usporiadaný koreňový strom, **280**  
 ústie, 301, 302, 305-306  
 usudzovanie, induktívne, **2**, **13**  
 usudzovanie, schéma, **4-6**, **11-14**, 20  
 uzavretý eulerovský ťah, **238**, 239-241, 247  
 uzavretý sled, **237-238**  
 uzavretý ťah, 228, **237**, 238-240

## V

váha hrany, **257**, **301**  
 Vandermonde, Alexandre Théophile, **86**  
 Vandermondeova identita, **86**  
 variácia, 88  
 vektor neznámych, **205**  
 vektor pravých strán (vektor konštantných členov), **205**, 209, 212, 222  
 vektor, riadkový, 178, **180**, 189-190, 192, 219  
 vektor, stĺpcový, **180-181**, 190, 208, 212  
 vektory, lineárna kombinácia vektorov, **190**, 192  
 vektory, lineárna závislosť, **189-190**, 193, 218-219  
 Veľká Fermatova veta, **19**  
 veľkosť toku, **305-306**  
 Vennove diagramy, 33-34, 43  
 Venn, John, **33**  
 verifikácia, tabuľková metóda, 35  
 veta  
 – binomická, **82**  
 – Frobeniova, **208**, 212  
 – Havlova a Hakimiho, **232**  
 – Kuratowského, **263**  
 – Lagrangeova, **131**  
 – multinomická, **87**  
 – o štyroch farbách, **267**  
 – o dedukcii, **8**  
 – Veľká Fermatova, **19**  
 Vizing, Vadim Georgievich, 269  
 vlastná podmnožina  $A \subset B$ , **32**  
 vlastnosť konštanty 0, **145**, 147, 148  
 vlastnosť konštanty 1, **145**, 147, 148  
 vnútorný vrchol, **279-281**

vrchol  
– izolovaný, **231**  
– vnútorný, **279**  
–, stupeň, **230-231**  
–, úroveň, 186, **280**, 281, 290, 294, 317, 320  
–, vstupný stupeň, **231**, 302  
–, výstupný stupeň, **231**, 302  
vrcholová nezávislosť, číslo, **269-270**  
vrcholy susedné, **230**, 235  
vstupný stupeň vrcholu, **231**, 302  
vymenovanie prípadov, dôkaz, **17-19**, 57  
vymenovanie prvkov, 30  
výpočet determinantov, 217, 220-221, 222  
výstupný stupeň vrcholu, **231**, 302  
vyvážený koreňový strom, **281**, 283  
vzdialenosť Hammingova, **165**, 166  
vzťah rekurentnej formuly a rekurzcie, 100

## W

Wiles, Andrew, 19

## X

XOR, exkluzívna disjunkcia,  $\oplus$ , 174

## Z

zafarbenie hranové, **269**  
zákon sporu, **34**  
zákon vylúčenia tretieho, **34**  
zákony De Morganove, 17, 27, **34**, 113, **144**,  
**147**  
zásobník, 310, **311-312**, 314, 321  
zátvorkovanie súčinu matíc, **184-187**  
zdroj, **301-302**, 305  
zjednotenie  
– dvoch grafov, **234**, 237  
– množín, **32-33**, 38, 40, 46, 54, 113, 124, 144  
– relácií, **54**  
zložená funkcia, **67-69**  
zložité úrokovanie, **101**  
zložitosť algoritmu, 100, 108-109, 112, 169,  
184, 237, 259, 267, **284**, 295, 309, 310, 319  
zložitosť násobenia matíc, 184  
zmiešaný graf, 228

zobrazenie  
– bijektívne, 71, 88, 133, 137  
zovšeobecnenie  
– pomocou existenčného kvantifikátora, 11, 14  
– pomocou univerzálneho kvantifikátora, 11,  
12, 13, 20  
– induktívne, **2**, **13**  
zoznam susedov, **235**