Algebra a diskrétna matematika

VLADIMÍR KVASNIČKA
JIŘÍ POSPÍCHAL

Algebra a diskrétna matematika

Slovenská technická univerzita
v Bratislave
2008

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

PREDHOVOR

Cieľom tejto učebnice je poskytnúť študentom informatiky na Fakulte informatiky a informačných technológií STU ucelený text k prednáške „*Algebra a diskrétna matematika*“. Diskrétna 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 diskrétna 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 algebre. 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 diskrétnej matematiky patrí medzi študentmi k najobľúbenejšej časti predmetu.

V slovenskej a českej odbornej spisbe existuje mnoho učebných textov diskrétnej 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 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.

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 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 striktne deduktívne dokázateľné zo známych pojmov a reprezentujú akty kreatívnosti v matematike, ktoré taktiež znamenajú, že matematika nie je len veda deduktívneho charakteru, kde sa dá každý pojem odvodiť z iných jednoduchších poznatkov[1].

Ilustratívny príklad axiomatického systému

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

A_1. Každý vrchol leží aspoň na jednej hrane.

A_2. Pre každú hranu existujú práve dva vrcholy, ktoré na nej ležia.

[1] 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*[2], 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.

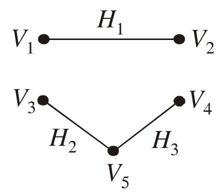
VETA 1.1. Každý graf má aspoň tri hrany.

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.

[2] Pojem grafu bude podrobne študovaný v kapitolách 10 až 13.

1.2 PRAVIDLÁ USUDZOVANIA VO VÝROKOVEJ LOGIKE

Pravidlá usudzovania vo výrokovej logike tvoria schému

$$\begin{array}{|l} predpoklad_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ predpoklad_n \\ \hline z\acute{a}ver \end{array} \tag{1.1}$$

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

$$\{predpoklad_1,\ldots,predpoklad_n\} \vdash z\acute{a}ver \tag{1.2a}$$

alebo formálne

$$\{\varphi_1,\ldots,\varphi_n\} \vdash \varphi \tag{1.2b}$$

Táto formula logického dôkazu môže byť prepísaná do formuly

$$\vdash \varphi_1 \wedge \ldots \wedge \varphi_n \Rightarrow \varphi \tag{1.3a}$$

alebo v ekvivalentnom tvare, kde konjunkcie sú nahradené implikáciami

$$\vdash \varphi_1 \Rightarrow \left(\varphi_2 \Rightarrow \left(\Rightarrow \ldots \left(\varphi_n \Rightarrow \varphi\right)\right)\right) \tag{1.3b}$$

Tabuľka 1.1. Schémy usudzovania výrokovej logiky

Schéma usudzovania	Teoréma výrokovej logiky	Názov schémy
$\begin{array}{\|l} p \\ \hline p \vee q \end{array}$	$p \Rightarrow (p \vee q)$	adícia
$\begin{array}{\|l} p \wedge q \\ \hline p \end{array}$	$(p \wedge q) \Rightarrow p$	simplifikácia (zjednodušenie)
$\begin{array}{\|l} p \\ q \\ \hline p \wedge q \end{array}$	$p \Rightarrow (q \Rightarrow (p \wedge q))$	konjunkcia
$\begin{array}{\|l} p \\ p \Rightarrow q \\ \hline q \end{array}$	$p \Rightarrow ((p \Rightarrow q) \Rightarrow q)$	modus ponens
$\begin{array}{\|l} \neg q \\ p \Rightarrow q \\ \hline \neg p \end{array}$	$\neg q \Rightarrow ((p \Rightarrow q) \Rightarrow \neg p)$	modus tollens
$\begin{array}{\|l} p \Rightarrow q \\ q \Rightarrow r \\ \hline p \Rightarrow r \end{array}$	$(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$	hypotetický sylogizmus

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

KONZISTENTNÉ PREDPOKLADY = ∃ 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[3] 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

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

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´*

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

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´*

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

[3] Nech *p, q, ..., r* sú atomické výrokové premenné, potom ***interpretácia*** (vzhľadom k týmto premenným) je označená symbolom $\tau = (p/1, q/0, ..., r/1)$. 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

$p =$ *´dnes prší´*

$q =$ *´kúpem sa´*

$r =$ *´navštívim príbuzného´*

potom schéma má tento formálny tvar mierne modifikovaného hypotetického sylogizmu

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

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. Obrátime našu pozornosť na formulu (1.2b) logického vyplývania výrokovej formuly φ z predpokladov, ktoré sú reprezentované formulami φ_1, φ_2,..., φ_n. Logické vyplývanie ilustrujeme jednoduchým príkladom.

PRÍKLAD 1.4. Postulujme, že množina predpokladov obsahuje tieto formuly – zložené výroky:

$\varphi_1 =$ *´dnes poobede nie je slnečno a je chladnejšie ako včera´*

$\varphi_2 =$ *´pôjdeme sa kúpať len vtedy, ak bude slnečno´*

$\varphi_3 =$ *´ak sa nepôjdeme kúpať, potom sa budeme člnkovať na rieke´*

$\varphi_4 =$ *´ak sa budeme člnkovať na rieke, potom sa vrátime domov podvečer´*

požadovaný záver má tvar

$\varphi =$ *´budem doma podvečer´*

Pomocou výrokových premenných

$p =$ *´dnes poobede je slnečno´*

$q =$ *´je chladnejšie ako včera´*

$r =$ *´ pôjdeme sa kúpať ´*

s = *´ budeme člnkovať na rieke´*

$t =$ *´ vrátime sa domov podvečer´*

vykonáme formalizáciu schémy logického vyplývania do tvaru

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

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$_1$
2.	$(r \Rightarrow p) \wedge (p \Rightarrow r)$	predpoklad$_2$
3.	$\neg r \Rightarrow s$	predpoklad$_3$
4.	$s \Rightarrow t$	predpoklad$_4$
5.	$\neg p$	simplifikácia predpokladu$_1$
6.	q	simplifikácia predpokladu$_1$
7.	$r \Rightarrow p$	simplifikácia predpokladu$_2$

8. $\neg r$ medzivýsledok 5 a modus tollens na predpoklad$_2$
9. s medzivýsledok 8 a modus ponens na predpoklad$_3$
10. t medzivýsledok 9 a modus ponens na predpoklad$_4$

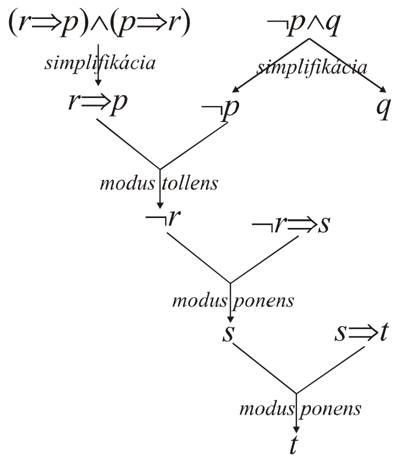
DÔKAZ AKO POSTUPNOSŤ FORMÚL

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

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

Túto postupnosť formúl 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:

φ_1 = *´ak mi pošleš email, potom program dokončím´*

φ_2 = *´ak mi nepošleš email, potom pôjdem spať skôr´*

φ_3 = *´ak pôjdem spať skôr, potom sa ráno zobudím odpočinutý´*

požadovaný záver má tvar

φ = *´ak nedokončím program, potom sa ráno zobudím odpočinutý´*

Pomocou výrokových premenných

p = *´pošleš mi email ´*

q = *´program dokončím´*

r = *´pôjdem spať skôr´*

s = *´ráno sa zobudím odpočinutý´*

vykonáme formalizáciu schémy logického vyplývania do tvaru

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

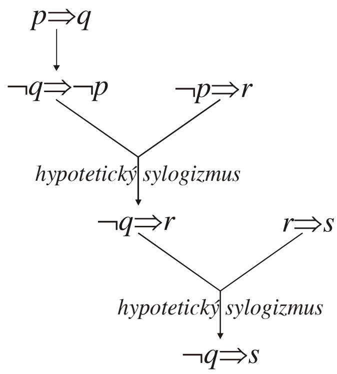
Pomocou postupnosti elementárnych krokov, kde budeme používať schémy usudzovania z tab. 1.1, ukážeme, že táto schéma je platná

1. $p \Rightarrow q$ predpoklad$_1$
2. $\neg p \Rightarrow r$ predpoklad$_2$
3. $r \Rightarrow s$ predpoklad$_3$

4.	$\neg q \Rightarrow \neg p$	inverzia implikácie na predpoklad$_1$
5.	$\neg q \Rightarrow r$	hypotetický sylogizmus na medzivýsledok 4 a predpoklad$_2$
6.	$\neg q \Rightarrow s$	hypotetický sylogizmus na medzivýsledok 5 a predpoklad$_3$

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.

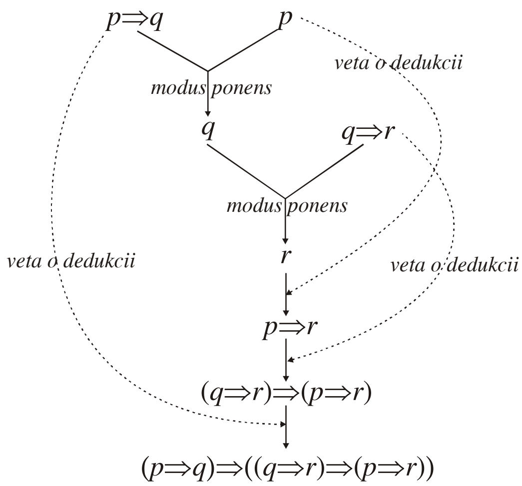
VETA O DEDUKCII

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

$$\left(\{\varphi_1,...,\varphi_n\} \cup \{\psi\} \vdash \varphi\right) \Rightarrow \left(\{\varphi_1,...,\varphi_n\} \vdash (\psi \Rightarrow \varphi)\right) \tag{1.4}$$

To znamená, že logický dôkaz formuly φ pomocou rozšírenej množiny predpokladov $\{\varphi_1,...,\varphi_n\} \cup \{\psi\}$ 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$_1$
2.	$q \Rightarrow r$	predpoklad$_2$
3.	p	pomocný predpoklad
4.	q	modus ponens na predpoklad$_1$ a pomocný predpoklad
5.	r	modus ponens na predpoklad$_2$ 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$_2$
8.	$(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$	použitie (1.4) na výsl. 7 a predpoklad$_1$

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

$$(\{\varphi_1,...,\varphi_n\} \vdash \varphi) \Rightarrow (\{\varphi_1,...,\varphi_n\} \cup \{\psi\} \vdash \varphi) \tag{1.5}$$

Význam tohto rozšírenia spočíva v tom, že zahrnutie vhodnej vety (tautológie) ψ môže podstatne zjednodušiť dôkaz vety.

PRÍKLAD 1.7. Dokážte zákon rezolventy[4]

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

pomocou zákona hypotetického sylogizmu

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

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

[4] V knihe Matematická logika [11] je rezolventa (alebo rezolučný princíp) formulovaná pomocou vety 5.2 ako formula $(B \vee l) \wedge (C \vee \neg l) \Rightarrow (B \vee C)$, 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$_1$
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 zámeny $p \leftrightarrow q$
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*)

$$\begin{array}{|l} q \\ p \Rightarrow q \\ \hline p \end{array} \qquad (1.6a)$$

POPRETIE PREDPOKLADU

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

$$\begin{array}{|l} \neg p \\ p \Rightarrow q \\ \hline \neg q \end{array} \qquad (1.6b)$$

Prvá schéma „popretie predpokladu“ je ilustrovaná príkladom

$$\begin{array}{|l} \textit{vydala som sa} \\ \textit{ak som pekná, tak sa vydám} \\ \hline \textit{som pekná} \end{array}$$

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

$$\begin{array}{|l} \textit{nie som pekná} \\ \textit{ak som pekná, tak sa vydám} \\ \hline \textit{nevydám sa} \end{array}$$

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

$$q \Rightarrow \big((p \Rightarrow q) \Rightarrow p\big) \tag{1.7a}$$

$$\neg p \Rightarrow \big((p \Rightarrow q) \Rightarrow \neg q\big) \tag{1.7b}$$

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
$\dfrac{\forall x\, P(x)}{P(c)}$	$\big(\forall x\, P(x)\big) \Rightarrow P(c)$	Konkretizácia univerzálneho kvantifikátora
$\dfrac{P(c)\ \textit{pre každé}\ c}{\forall x\, P(x)}$	$P(c) \Rightarrow \big(\forall x\, P(x)\big)$	Zovšeobecnenie pomocou univerzálneho kvantifikátora
$\dfrac{\exists x\, P(x)}{P(c)\ \textit{pre nejaký element}\ c}$	$\big(\exists x\, P(x)\big) \Rightarrow P(c)$	Konkretizácia existenčného kvantifikátora
$\dfrac{P(c)\ \textit{pre nejaký element}\ c}{\exists x\, P(x)}$	$P(c) \Rightarrow \big(\exists x\, P(x)\big)$	Zovšeobecnenie pomocou existenčného kvantifikátora

KONKRETIZÁCIA UNIVERZÁLNEHO KVANTIFIKÁTORA

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

$$\left(\forall x\, P(x)\right) \Rightarrow P(c) \tag{1.8}$$

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

$$\forall x\, P(x) =_{def} \bigwedge_{x\in U} P(x) = P(a) \wedge P(b) \wedge \ldots \wedge P(u) \tag{1.9}$$

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

$$\begin{array}{|l} \forall x\, P(x) \\ \hline P(a) \\ P(b) \\ \ldots\ldots\ldots \\ P(c) \\ \ldots\ldots\ldots \end{array} \tag{1.10}$$

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

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

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

$$\begin{array}{|l} \forall(x\in U)\, P(x) \\ c\in U \\ \hline P(c) \end{array} \tag{1.11}$$

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 $\forall$

$$P(a) \wedge \ldots \wedge P(c) \wedge \ldots = \bigwedge_{x\in U} P(x) =_{def} \forall x\, P(x) \tag{1.12}$$

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

$$\begin{array}{|l} P(a) \\ \ldots\ldots\ldots \\ P(c) \\ \ldots\ldots\ldots \\ \hline \forall x\, P(x) \end{array} \tag{1.13}$$

potom musí platiť aj

$$P(c) \Rightarrow \left(\forall x\, P(x)\right) \tag{1.14}$$

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 „poctivo“ zovšeobecniť pomocou univerzálneho kvantifikátora $\forall'$ definovaného vzhľadom k „poduniverzu“ U'

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

V dôsledku určitej netrpezlivosti, pozorovateľ zovšeobecní 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 induktívne 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

$$\left(\exists x\, P(x)\right) \Rightarrow P(c) \tag{1.15}$$

alebo pomocou schémy usudzovania

$$\frac{\exists x\, P(x)}{P(c)\ \textit{pre nejaký element } c} \tag{1.16}$$

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

$$\exists x\, P(x) =_{def} \bigvee_{x \in U} P(x) = P(a) \vee \ldots \vee P(c) \vee \ldots \tag{1.17}$$

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 $\exists$

$$P(c) \Rightarrow \bigvee_{x \in U} P(x) =_{def} \exists x\, P(x) \tag{1.18}$$

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

$$\begin{array}{|l} P(c)\ \textit{pre nejaký element c} \\ \hline \exists x\, P(x) \end{array} \tag{1.19}$$

Spojením (1.15) a (1.18) dostaneme

$$P(c) \equiv \exists x\, P(x) \tag{1.20}$$

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

PRÍKLAD 1.8. Ukážte, že záver φ vyplýva z predpokladov φ_1 a φ_2:

φ_1 = ‘každý kto navštevuje prednášky z diskrétnej matematiky je študentom STU‘
φ_2 = ‘Mária navštevuje prednášky z diskrétnej matematiky’
φ = ‘Mária je študentka STU’.

Tieto tri výroky prepíšeme do tvaru

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

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

1.	$\forall x\left(DM(x) \Rightarrow STU(x)\right)$	predpoklad$_1$
2.	$DM(Maria)$	predpoklad$_2$
3.	$DM(Maria) \Rightarrow STU(Maria)$	konkretizácia 1
4.	$STU(Maria)$	modus ponens na 2 a 3

PRÍKLAD 1.9. Ukážte, že záver φ vyplýva z predpokladov φ_1 a φ_2:

φ_1 = ‘*niektorí študenti navštevujúci prednášku nečítali predpísanú učebnicu* ‘
φ_2 = ‘*každý študent navštevujúci prednášku vykonal skúšku*’
φ = ‘*niektorí študenti, ktorí vykonali skúšku, nečítali predpísanú učebnicu*’.

Tieto tri výroky prepíšeme do tvaru

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

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.	$\exists x\left(P(x) \wedge \neg N(x)\right)$	predpoklad$_1$
2.	$\forall x\left(P(x) \Rightarrow S(x)\right)$	predpoklad$_2$
3.	$P(c) \wedge \neg N(c)$	konkretizácia predpokladu$_1$
4.	$P(c)$	simplifikácia 3
5.	$\neg N(c)$	simplifikácia 3
6.	$P(c) \Rightarrow S(c)$	konkretizácia predpokladu$_2$
7.	$S(c)$	modus ponens na 4 a 6
8.	$S(c) \wedge \neg N(c)$	konjunkcia 5 a 7
9.	$\exists x\left(S(x) \wedge \neg N(x)\right)$	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 $\{\varphi_1,...,\varphi_n\}$ a z už dokázaných viet $\{\psi_1,...,\psi_m\}$, potom dôkaz $p \Rightarrow q$ môžeme charakterizovať vzťahom logického dôkazu

$$\{\varphi_1,...,\varphi_n\} \cup \{\psi_1,...,\psi_m\} \cup \{p\} \vdash q \tag{1.21}$$

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

$$\underbrace{(n\ je\ nepárne\ číslo)}_{p} \Rightarrow \underbrace{(n^2\ \ je\ nepárne\ číslo)}_{q}$$

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 DÔKAZ

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

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

Budeme dokazovať inverznú implikáciu

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

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 $p \Rightarrow q$.

DÔKAZ SPOROM

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

$$\begin{array}{|l} p \Rightarrow q \\ p \Rightarrow \neg q \\ \hline \neg p \end{array} \tag{1.22}$$

založenej na zákone výrokovej logiky

$$(p \Rightarrow q) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \neg p) \tag{1.23}$$

Túto schému usudzovania môžeme interpretovať tak, že ak z predpokladu p súčasne 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

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

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

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

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 α je párne. Potom taktiež platí $\beta^2 = 2p^2$, t. j. β^2 je párne číslo, čiže aj β je párne číslo. Týmto sme dokázali, že α, β sú párne čísla, čiže sú súdeliteľné

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

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

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

čo bolo potrebné dokázať.

DÔKAZ VYMENOVANÍM PRÍPADOV

Naším cieľom je dokázať implikáciu

$$(p_1 \vee \ldots \vee p_n) \Rightarrow q \qquad (1.24)$$

Jednoduchými ekvivalentnými úpravami môžeme túto implikáciu prepísať do ekvivalentného tvaru

$$((p_1 \vee \ldots \vee p_n) \Rightarrow q) \equiv ((p_1 \Rightarrow q) \wedge \ldots \wedge (p_n \Rightarrow q)) \qquad (1.25)$$

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

Formulu (1.25) môžeme prepísať do tvaru schémy usudzovania

$$\begin{array}{|l} (p_1 \Rightarrow q) \\ \ldots\ldots\ldots\ldots\ldots \\ (p_n \Rightarrow q) \\ \hline (p_1 \vee \ldots \vee p_n) \Rightarrow q \end{array} \tag{1.26}$$

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

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 $a < b < c$

$$max\left\{a, \underbrace{min\{b,c\}}_{b}\right\} = min\left\{\underbrace{max\{a,b\}}_{b}, \underbrace{max\{a,c\}}_{c}\right\}$$

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

$$b = b$$

(2) Prípad $b < a < c$

$$max\left\{a, \underbrace{min\{b,c\}}_{b}\right\} = min\left\{\underbrace{max\{a,b\}}_{a}, \underbrace{max\{a,c\}}_{c}\right\}$$

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

$$a = a$$

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

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

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

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

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

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 $|a - b| \le |a| + |b|$, kde a, b sú ľubovoľné nenulové reálne čísla a $|\,.\,|$ je absolútna hodnota.

(1) $a < b < 0$, potom $a - b < 0$, $a < 0$ a $b < 0$, dokazovaná nerovnosť má tvar $-(a-b) \le -a - b$, alebo $b \le 0$, čo je pravdivý výrok.

(2) $a < 0 < b$, potom $a - b < 0$, $a < 0$ a $b > 0$, dokazovaná nerovnosť má tvar $-(a-b) \le -a + b$, čo je pravdivý výrok.

(3) $0 < a < b$, potom $a - b < 0$, $a > 0$ a $b > 0$, dokazovaná nerovnosť má tvar $-(a-b) \le a + b$, alebo $a \ge 0$, 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[5].

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.	$\forall n\,(P(n) \Rightarrow P(n+1))$	
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 $n = n$
...	....	

[5] 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

$$\begin{array}{|l} P(1) \\ \forall n\,\big(P(n) \Rightarrow P(n+1)\big) \\ \hline \forall n\, P(n) \end{array} \tag{1.27}$$

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

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

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

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

$$=\sum_{i=1}^{n}(2i-1)+\big(2(n+1)-1\big)=n^2+(2n+1)=(n+1)^2$$

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

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

čím sme zavŕšili 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 $\forall n \left(P(n) \Rightarrow P(n+1)\right)$, čo bolo potrebné dokázať.

SILNÁ MATEMATICKÁ INDUKCIA

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

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

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 prvočísiel.

Nech vlastnosť $P(n)$ má tvar

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

kde p_1, p_2, p_3, ... sú prvé prvočísla (2, 3, 5,..., ktoré sú menšie ako n) a α_1, α_2, α_3, ... 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. prípad – $n + 1$ je prvočíslo p_k, potom $P(n+1)$: $n+1 = p_1^0 p_2^0 ... p_k^1$.

2. prípad – $n + 1$ 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 prvočísiel (indukčný predpoklad)

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

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

potom ich súčin má tvar

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

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 striktne deduktívne dokázateľné zo známych pojmov.

PRAVIDLÁ USUDZOVANIA

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

$$\begin{array}{|l} predpoklad_1 \\ \ldots\ldots\ldots\ldots \\ predpoklad_n \\ \hline záver \end{array}$$

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

$$\{predpoklad_1,...,predpoklad_n\} \vdash záver$$

alebo

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

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

$$\left(\{\varphi_1,...,\varphi_n\} \cup \{\psi\} \vdash \varphi\right) \Rightarrow \left(\{\varphi_1,...,\varphi_n\} \vdash (\psi \Rightarrow \varphi)\right)$$

Dôkaz formuly φ pomocou rozšírenej množiny predpokladov $\{\varphi_1,...,\varphi_n\} \cup \{\psi\}$ 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

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

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 $(p_1 \vee ... \vee p_n) \Rightarrow q$ je založený na jej ekvivalentnom tvare

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

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

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

KĽÚČOVÉ 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

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

CVIČENIA

1.1. Aké pravidlo usudzovania bolo použité pri dôkaze záverov?

(a) Mária je študentka informatiky. Preto je Mária študentka informatiky alebo študentka telekomunikácií.
(b) Jaroslav študuje informatiku a elektrotechnológiu. Preto, Jaroslav študuje informatiku.
(c) Ak prší, potom plaváreň je zatvorená. Preto, ak plaváreň je otvorená, potom neprší.
(d) Ak dnes sneží, kino je dnes uzavreté. Kino dnes nie je uzavreté. Preto, dnes nesneží.
(e) 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?

(a) Dnes bude teplo alebo bude smog v ovzduší. Dnes nebude teplo. Preto, dnes bude smog v ovzduší.
(b) Eva vynikajúco pláva. Ak Eva je vynikajúci plavec, potom môže pracovať ako plavčík. Preto, Eva môže pracovať ako plavčík.
(c) 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.
(d) 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?

(a) „Ak jem korenenú stravu, potom mám hrozné sny“, „ak spím a pritom hrmí, potom mám hrozné sny“, „nemám hrozné sny“.
(b) „Ja som chytrý alebo mám šťastie“, „nemám šťastie“, „ak mám šťastie, potom zvíťazím v lotérii“.
(c) „Každý študent informatiky vlastní notebook“, „Rudo nevlastní notebook“, „Anna vlastní notebook“.
(d) „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 diskrétnej matematiky“, „každý študent, ktorý si zapísal do indexu prednášku z diskrétnej 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 diskrétnej matematiky“, „Viera má zapísanú prednášku z diskrétnej 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 $x^2 \le 9$, potom $x \le 3$.

(d) Ak x je reálne číslo, ktoré spĺňa podmienku $x > 2$, potom $x^2 > 4$. Nech $x \le 2$, potom $x^2 \le 4$.

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 $\left(\exists s\, S(s,Max)\right) \Rightarrow S(Max,Max)$, 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) Dokáže, 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

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

(b) Dokážte formulu

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

(c) Dokážte formulu

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

(d) Dokážte formulu

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

(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

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

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

(h) Dokážte zovšeobecnené De Morganove formuly

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

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

1.13. Pomocou rozkladu na parciálne zlomky nájdite formulu pre

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

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 odlíšiteľné.

DEFINÍCIA 2.1.
MNOŽINA ☞

Množina je neusporiadaný súbor prvkov.

ODLÍŠITEĽNÉ PRVKY

Ak sa nejaké dva prvky nachádzajú v tej istej množine, potom musia byť od seba odlíšiteľné; v množine sa neopakuje výskyt dvoch rovnakých (neodlíšiteľných) prvkov. V definícii množiny bol použitý elementárny pojem „súbor“, ktorý nebudeme bližšie špecifikovať. Pozorný čitateľ môže namietať, 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

$$A = \{a, b, ..., u\} \tag{2.1a}$$

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)

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

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

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

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

CHARAKTERISTICKÁ FUNKCIA

$$P(x) =_{def} \left(\mu_A(x) = 1\right) \tag{2.2}$$

kde

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

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 CHARAKTERISTICKEJ FUNKCIE

Každá množina A je pomocou charakteristickej funkcie vyjadrená takto

$$A = \left\{x \in U\ ;\ \mu_A(x) = 1\right\} \tag{2.4}$$

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

$$\mu_A : U \to \{0,1\} \tag{2.5}$$

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

PRÁZDNA MNOŽINA ∅
UNIVERZÁLNA MNOŽINA *U*

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

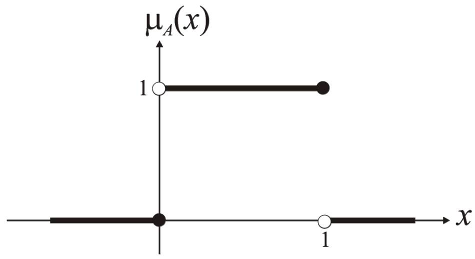
PRÍKLAD 2.1.

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

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

Grafické znázornenie tejto charakteristickej funkcie je na obr. 2.1.

OBRÁZOK 2.1.
CHARAKTERISTICKÁ 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 $A = \left\{x\ ;\ \mu_A(x) = 1\right\}$ sa ***rovná*** množine $B = \left\{x\ ;\ \mu_B(x) = 1\right\}$, $A = B$, vtedy a len vtedy, ak tieto množiny sú definované nad rovnakým univerzom U a charakteristické funkcie oboch množín sú rovnaké

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

Alternatívna definícia vzťahu rovnosti medzi množinami A a B je

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

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

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

VLASTNÁ PODMNOŽINA $A \subset B$

Alternatívna definícia podmnožiny je

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

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

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

kde

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

DEFINÍCIA 2.6.

$A \cap B$

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

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

kde

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

DEFINÍCIA 2.7.

$\overline{A}$

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

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

kde

$$\mu_{\overline{A}}(x) = 1 - \mu_A(x) \tag{2.10b}$$

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

DEFINÍCIA 2.8.

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

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

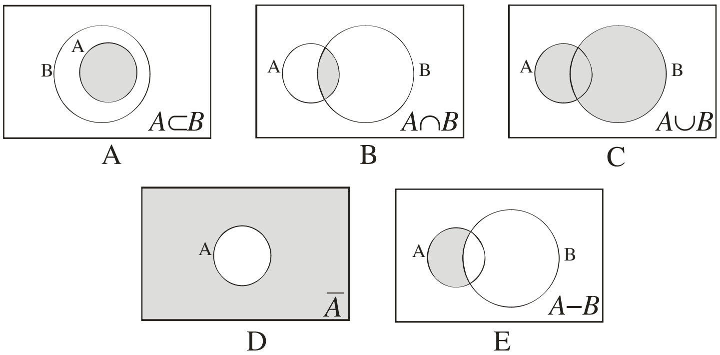
☞ $A \setminus B$

kde

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

Takto definované operácie nad množinou U sú znázornené pomocou Vennových[1] 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 „prienik“ $A \cap B$, kde vyšrafovaná oblasť reprezentuje prienik 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 k univerzu 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.

☞

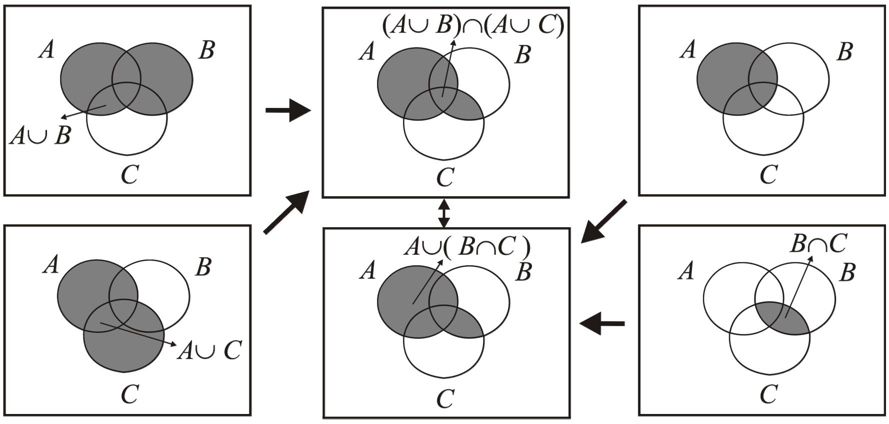
Tabuľka 2.1. Formuly teórie množín

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	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

[1] 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 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

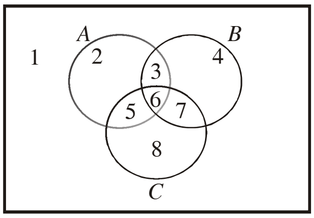


Verifikácia korektnosti formuly $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. Prostredný Vennov diagram je zostrojený dvoma rôznymi nezávislými spôsobmi, v oboch prípadoch dostávame ten istý výsledok.

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 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.

PRINCÍP KOMPOZICIONALITY

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

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

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

Použitím algebraickej identity[2]

[2] 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

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

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 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

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

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

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

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

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

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

(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

$$|A\cup B|=|A|+|B| \tag{2.14a}$$

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

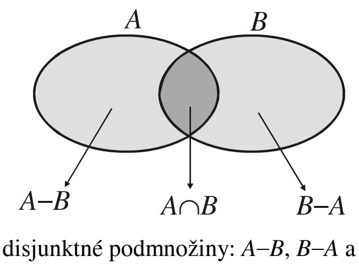
$$|A_1\cup A_2\cup ...\cup A_n|=|A_1|+|A_2|+...+|A_n| \tag{2.14b}$$

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

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

$$|A\cup B|=|A|+|B|-|A\cap B| \tag{2.15}$$

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

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

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 formulu 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, $|M \cap I \cap \overline{E}| = ?$ 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

$$|I| = |I \cap (M \cup \bar{M}) \cap (E \cup \bar{E})| =$$
$$|I \cap M \cap E| + |I \cap M \cap \bar{E}| + |I \cap \bar{M} \cap E| + |I \cap \bar{M} \cap \bar{E}|$$

Platia tieto identity

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

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:
$M = \{A; A \notin A\}$
$M \in M$?

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 $I = \{1, 2, ..., n\}$ 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

$$\mathcal{A}=\{A_i; i\in I\}=\{A_1, A_2, ..., A_n\} \tag{2.18}$$

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

$$\bigcap_{i\in I} A_i = A_1 \cap A_2 \cap ... \cap A_n = \{x;\ x\in A_i,\ pre\ každé\ i\in I\} \tag{2.19a}$$

$$\bigcup_{i\in I} A_i = A_1 \cup A_2 \cup ... \cup A_n = \{x;\ x\in A_i,\ pre\ nejaké\ i\in I\} \tag{2.19b}$$

PRÍKLAD 2.8.

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

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

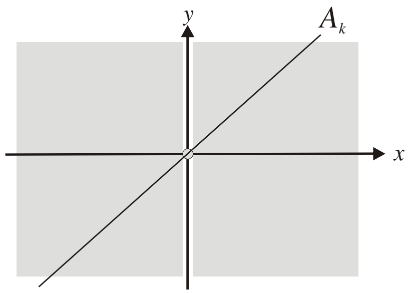
kde $k\in R$. Geometrická interpretácia množiny A_k je priamka so smernicou k, ktorá prechádza stredom súradnicového systému, pozri obr. 2.6. To znamená, že prienik množín A_k je jednoprvková množina, ktorá obsahuje stred súradnicového systému

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

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 $y=k\,x$.

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

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

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

VETA 2.2. ☞

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

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

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

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

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

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

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

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

Pripomíname, 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

$$1,\{1\},\{\{1\}\},\{\{\{1\}\}\},...$$

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

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

VETA 2.3. Mohutnosť potenčnej množiny $\mathcal{P}(A)$ konečnej množiny A je určená jednoduchým vzťahom

$$\left|\mathcal{P}(A)\right| = 2^{|A|} \tag{2.22}$$

Tento výsledok pre mohutnosť potenčnej množiny sa ľahko dokáže pomocou nasledujúcej úvahy: Nech konečná množina A obsahuje n prvkov, $A = \{a_1, a_2, ..., a_n\}$, 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, $\left|\mathcal{P}(A)\right| = 2^n$, 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

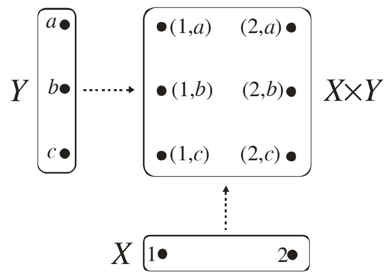
V mnohých matematických disciplínach alebo v ich aplikáciách vystupujú usporiadané dvojice prvkov. Tak napríklad, komplexné číslo môže byť charakterizované ako usporiadaná dvojica reálnych čísel $z = (x,y)$, kde x (y) je reálna (komplexná) časť. Základná relácia pre usporiadané dvojice je rovnosť: $(x,y) = (x',y')$, 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***[3] dvoch množín X a Y vtedy a len vtedy, ak

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

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).

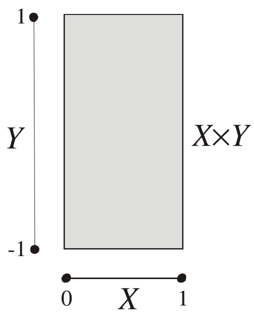
PRÍKLAD 2.11. Nech $X = \{1,2\}$ a $Y = \{a,b,c\}$, potom

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

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



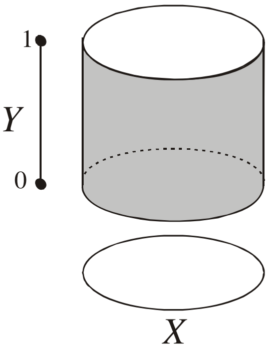
Znázornenie karteziánskeho súčinu dvoch úsečiek X a Y, výsledná oblasť je obdĺžnik.

---

[3] 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 $(x_1, x_2, ..., x_n)$ a $(x_1', x_2', ..., x_n')$ 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 $X_1 \times X_2 \times ... \times X_n$ sa nazýva karteziánsky súčin n množín X_1, X_2, ..., X_n vtedy a len vtedy, ak

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

Karteziánsky súčin môžeme taktiež vyjadriť symbolicky takto

$$X_1 \times X_2 \times ... \times X_n = \mathop{\times}_{i=1}^{n} X_i \quad (2.24b)$$

Ak všetky množiny z karteziánskeho súčinu sa rovnajú množine X, potom výraz $X_1 \times X_2 \times ... \times X_n$ 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 $X_1 = X_2 = ... = X_n = R$, kde R je množina reálnych čísel. Potom R^n je množina obsahujúca všetky n-tice reálnych čísel

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

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

$$|X \times Y| = |X| \cdot |Y| = m \cdot n \tag{2.25a}$$

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

$$|X_1 \times X_2 \times ... \times X_n| = |X_1| \cdot |X_2| \cdot ... \cdot |X_n| = m_1 \cdot m_2 \cdot ... \cdot m_n \tag{2.25b}$$

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

$$A \times (X \cap Y) = (A \times X) \cap (A \times Y) \tag{2.26a}$$

$$(X \cap Y) \times A = (X \times A) \cap (Y \times A) \tag{2.26b}$$

$$A \times (X \cup Y) = (A \times X) \cup (A \times Y) \tag{2.26c}$$

$$(X \cup Y) \times A = (X \times A) \cup (Y \times A) \tag{2.26d}$$

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 obidvoch 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

$$(A \subseteq B) \Rightarrow ((A \times X) \subseteq (B \times X)) \tag{2.27a}$$

Ak X je neprázdna množina, potom

$$((A \times X) \subseteq (B \times X)) \Rightarrow (A \subseteq B) \tag{2.27b}$$

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 sprehľadnenie týchto algoritmov.

CHARAKTERISTICKÁ 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 $A = \varnothing$; 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

$$\mu_A = (a_1, a_2, ..., a_n)$$
$$\mu_B = (b_1, b_2, ..., b_n)$$

je realizovaná pomocou binárnej operácie ´disjunkcie´

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

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´

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

kde

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

OPERÁCIA KOMPLEMENTU

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

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

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 $\overline{A}$ a $\overline{B}$ sú zostrojené pomocou operácie „negácie“ binárnych vektorov

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

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

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

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 $\overline{A}$. 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 $A_1, A_2, ..., A_n$ môžeme vytvárať súčiny $A_1 \times A_2 \times ... \times A_n$, 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).

KĽÚČOVÉ POJMY

množina
operácie nad množinami
množinová algebra
mohutnosť (kardinalita)
enumerácia
karteziánsky súčin
Georg Cantor
Bertrand Russell
axiomatická výstavba
prvok (element)
odlíšiteľné 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 diskrétnu matematiku. Vyjadrite pomocou množín *A* a *B* tvrdenia:

(a) Množina prvákov, ktorí navštevujú prednášku z diskrétnej matematiky.

(b) Množina prvákov, ktorí nenavštevujú prednášku z diskrétnej matematiky.

(c) Množina študentov, ktorí sú prváci alebo navštevujú prednášku z diskrétnej matematiky.

(d) Množina študentov, ktorí nie sú prváci alebo nenavštevujú prednášku z diskrétnej 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 $(A \subseteq B) \Rightarrow (\overline{B} \subseteq \overline{A})$.

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

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

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

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

2.28. Dokážte pomocou matematickej indukcie vzťahy

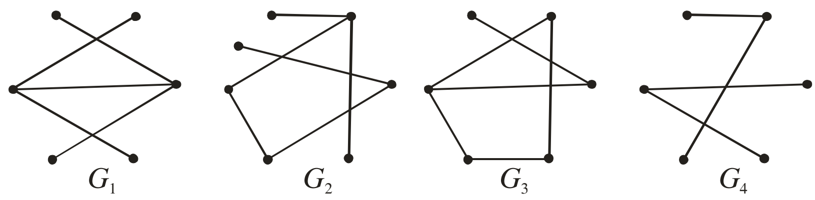
(a) $\overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A_i}$

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

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?

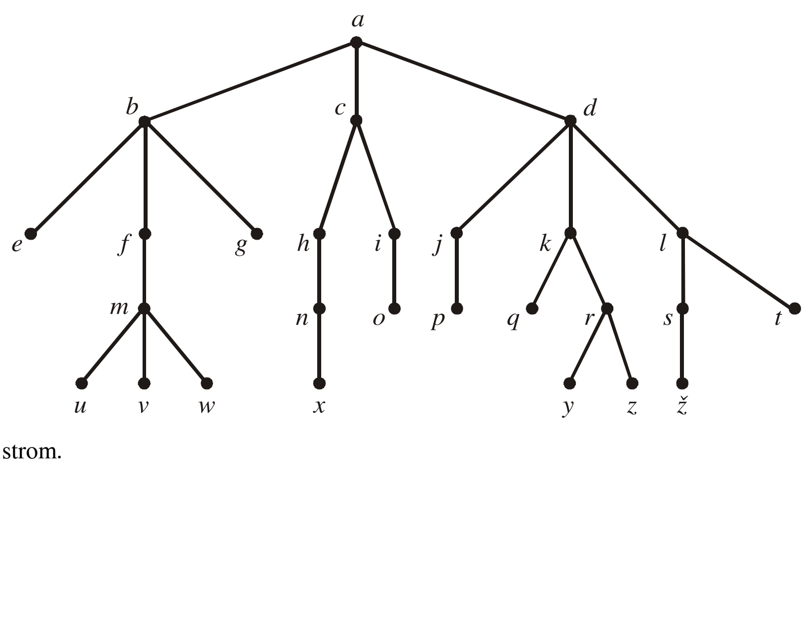


Ktoré nie sú stromy?

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

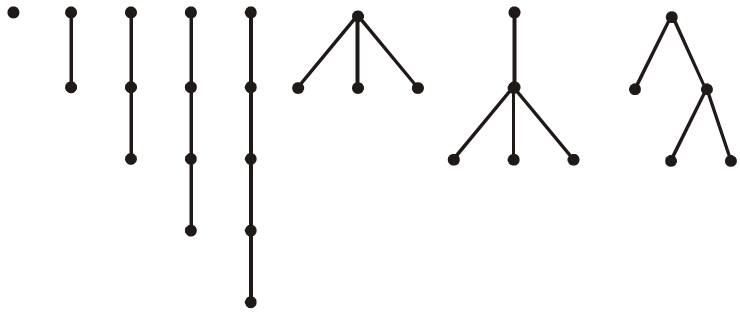
OBRÁZOK 12.20. KOREŇOVÝ STROM



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 $s_1, s_2, s_3, \ldots, s_n$, kde $n \geq 2$. Nutná a postačujúca podmienka, aby existoval strom na n vrcholoch taký, že $s_1, s_2, s_3, \ldots, s_n$, sú po poriadku stupne jeho vrcholov, je

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

Dokážte.

Keď existuje strom so stupňami $s_1, s_2, s_3, \ldots, s_n$, 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 $s_1, s_2, s_3, \ldots, s_n$. 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, $s_4, \ldots, s_n$ spĺňajú indukčný predpoklad a existuje teda strom o n-1 vrcholoch 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 vrcholoch. Teraz doplníme tento strom vrcholom y a hranou xy.

12.5. Nech G je jednoduchý graf o n vrcholoch. 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 vrcholoch, a nech G je obyčajný graf o $n + 1$ vrcholoch.

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.

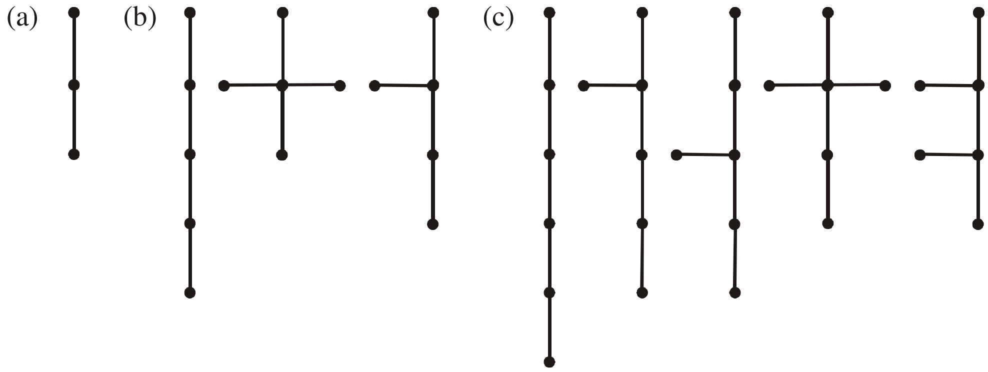
Turnaj môžeme modelovať ako úplný binárny strom. Každý vnútorný vrchol reprezentuje výhercu hry hranej jeho dvoma deťmi. Máme 1024 listov, jeden pre každého hráča. Koreň je víťaz turnaja. Podľa vety 12.3, pre $m = 2$ a $l = 1024$, $n = i + l = m \times i + 1$; z toho dostávame $i = (l - 1)/(m - 1) =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

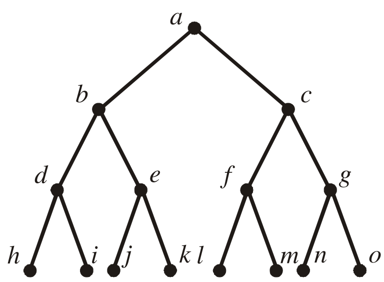
12.8. Koľko rôznych izomérov majú nasledujúce nasýtené uhľovodíky?
(a) C_3H_8
(b) C_5H_{12}
(c) C_6H_{14}

Z definície alkánov (nasýtených uhľovodíkov) vyplýva, že alkány majú štruktúru stromov. Stačí si všímať iba stromy z uhlíkových atómov týchto uhľovodíkov, hrany s vodíkovými atómami stupňa vrcholov 1 potom iba automaticky dopĺňajú počet incidentných hrán s každým uhlíkovým 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 $h,...,o$. V druhom časovom okamihu sčítame výsledky týchto súčtov v procesoroch d, ...,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, $x_1, x_2, ..., x_{2n}$. 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 rovnoramenných 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 porovnania.

12.12. Koľko vážení na rovnoramenných 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 váženia, 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, porovnajte 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 porovnajte C s A. Keď sú v rovnováhe, B je falošná, v opačnom prípade je A falošná.

12.13. Koľko vážení na rovnoramenných 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 váženia, pretože 2 váženia by nám dali 9 možných výsledkov (rozhodovací strom hĺbky 2 má iba 9 listov). Rozdeľte mince na 3 skupiny po 4 minciach, a porovnajte 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.

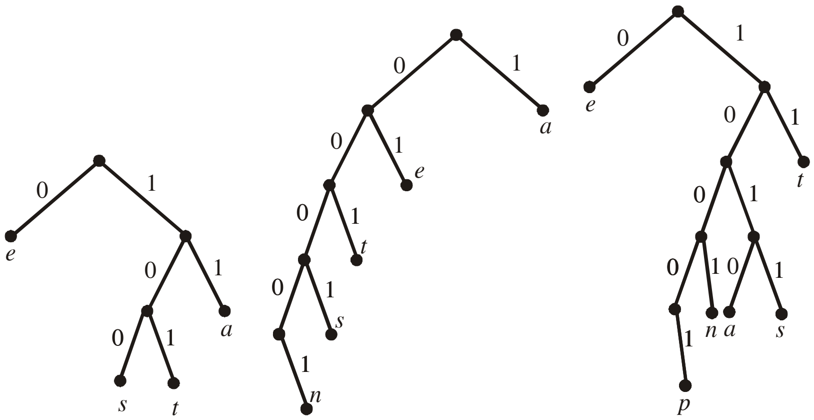
(d) a: 010, e: 11, t: 011, s: 1011, n: 1001, p: 10101
Je prefixový kód, žiaden z kódov nie je začiatkom iného kódu.

12.15. Skonštruujte binárny strom s prefixovými kódmi reprezentujúcimi tieto kódové schémy:

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

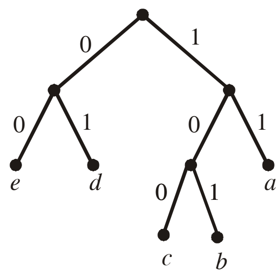
(b) a: 1, e: 01, t: 001, s: 0001, n: 00001

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



12.16. Skonštruujte 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.

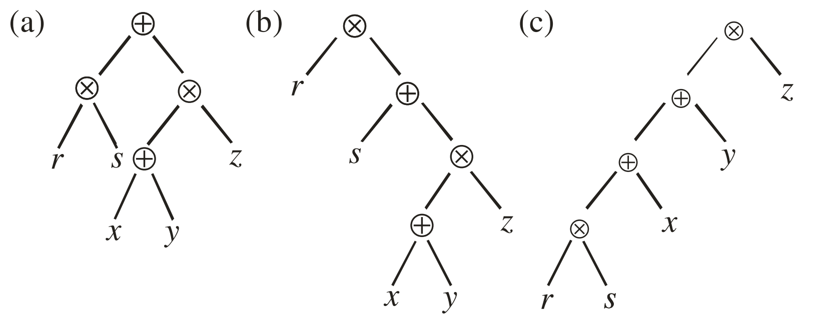


12.17. Reprezentujte nasledujúce výrazy ako binárne stromy

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

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

(c) $(((\mathrm{r}\otimes\mathrm{s})\oplus\mathrm{x})\oplus\mathrm{y})\otimes\mathrm{z}$



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 $\otimes$:

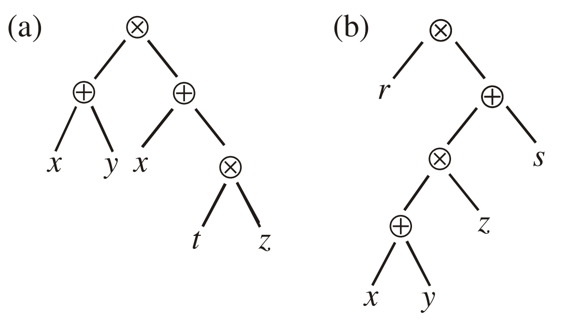
(a) 1 interpretácia, $x\otimes y\otimes z$
(b) 3 interpretácie, $(t\oplus x)\otimes y\otimes z$, $t\oplus(x\otimes y\otimes z)$, $(t\oplus(x\otimes y))\otimes z$
(c) 4 interpretácie, $(t\otimes x)\oplus(y\otimes z)$, $((t\otimes x)\oplus y)\otimes z$, $(t\otimes(x\oplus y))\otimes z$, $t\otimes(x\oplus(y\otimes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

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

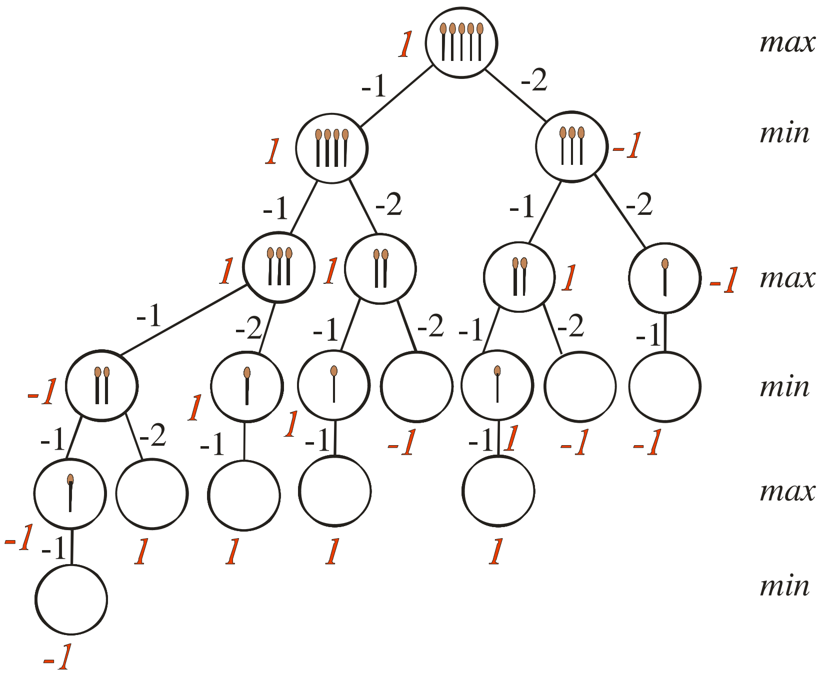


Zostrojte infixovú, prefixovú a postfixovú formu stromov.

(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 $rxy\oplus\ z\otimes s\oplus\otimes$

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

Na obrázku sú vrcholy s počtom zápaliek 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 zápaliek hráčom. Z ohodnotenia koreňa je zrejmé, že pre prvého hráča existuje víťazná stratégia. Existuje aj trocha 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.

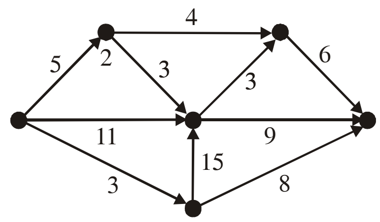


RIEŠENÉ CVIČENIA Z KAPITOLY 13

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.

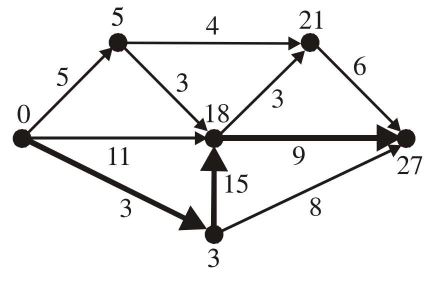
OBRÁZOK 13.17. ČASOVÝ PLÁN PROJEKTU

(a)



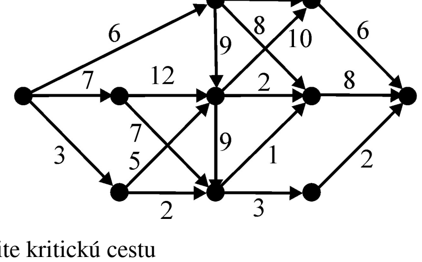
Časový plán projektu, určite kritickú cestu

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



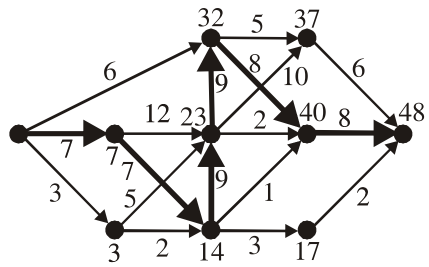
OBRÁZOK 13.18. ČASOVÝ PLÁN PROJEKTU

(b)



Časový plán projektu, určite kritickú cestu

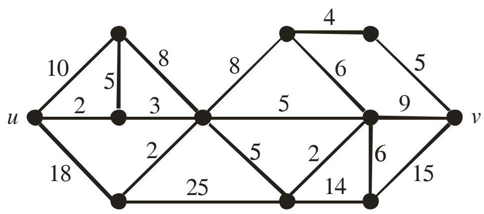
Minimálny celkový čas je 48, ohodnotenie $E(v)$ je uvedené u vrcholov, kritická cesta je tučne vyznačená.



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.

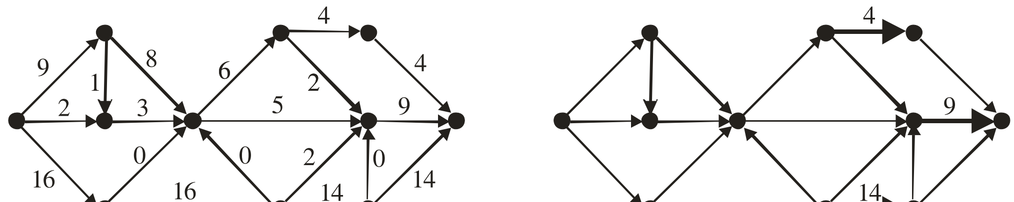
OBRÁZOK 13.19. MAXIMÁLNY TOK A MINIMÁLNY REZ?

(a)



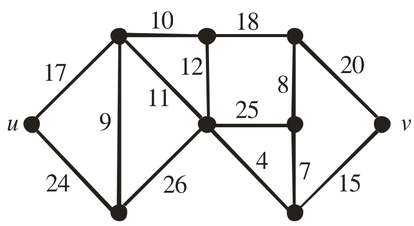
Nájdite maximálny tok a minimálny rez siete.

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



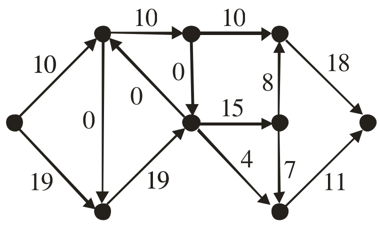
OBRÁZOK 13.20. MAXIMÁLNY TOK A MINIMÁLNY REZ?

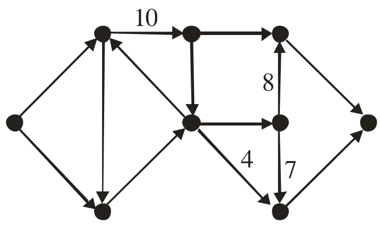
(b)



Nájdite maximálny tok a minimálny rez siete.

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

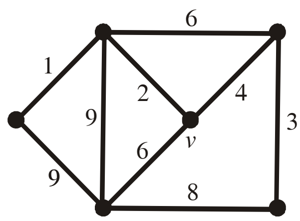




13.3. Pre grafy z obr. 13.21 a 13.22 použite Primov algoritmus, začínajúci na vyznačenom vrchole *v*, na nájdenie minimálnej kostry a určite jej váhu.

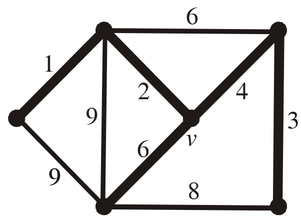
OBRÁZOK 13.21. MINIMÁLNA KOSTRA?

(a)



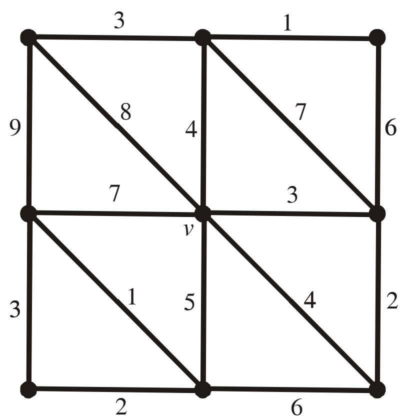
Nájdite minimálnu kostru.

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



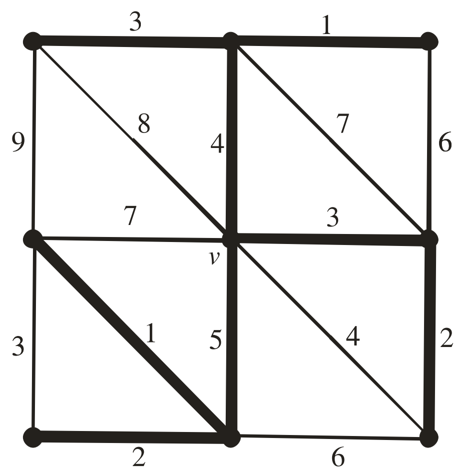
OBRÁZOK 13.22. MINIMÁLNA KOSTRA?

(b)



Nájdite minimálnu kostru.

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



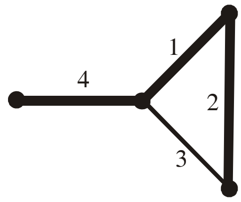
13.4. Použite Kruskalov algoritmus na nájdenie minimálnej kostry pri grafoch z príkladu 13.3 a určite jej váhu.

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

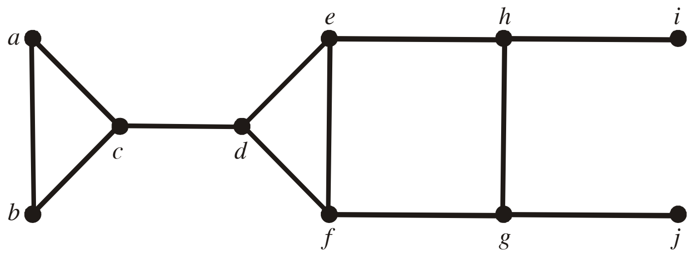


(b) Keď žiadne dve hrany nemajú rovnakú váhu, potom Kruskalov algoritmus vyberie kostru T jednoznačne.

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

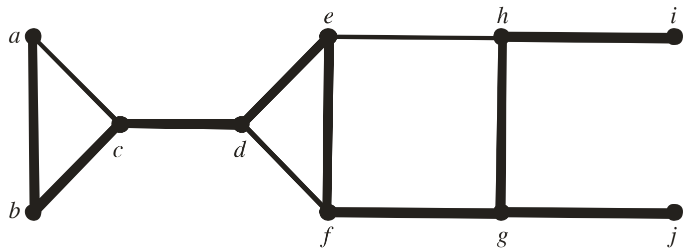
13.6. Použite prehľadávanie do hĺbky na nájdenie kostry daného jednoduchého grafu z obr. 13.23. Zvoľte vrchol a ako koreň tejto kostry a predpokladajte, že vrcholy sú usporiadané abecedne (namiesto typického postupu prehľadávania vykresleného grafu „zľava doprava“).

Obrázok 13.23. Kostra prehľadávaním do hĺbky?



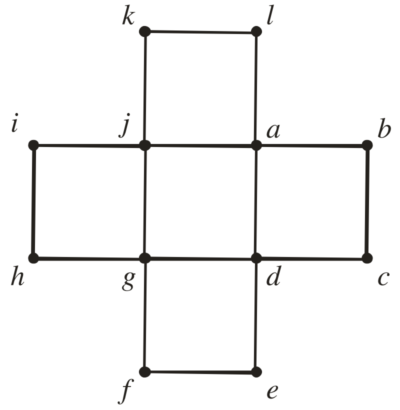
Nájdite kostru prehľadávaním do hĺbky.

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 i predtým, ako sme nútení sa vrátiť. Z vrcholu h nejde cesta na žiaden ešte nenavštívený vrchol, ale z vrcholu g ide cesta na nenavštívený vrchol j. Dostávame kostru vyznačenú tučnými hranami.



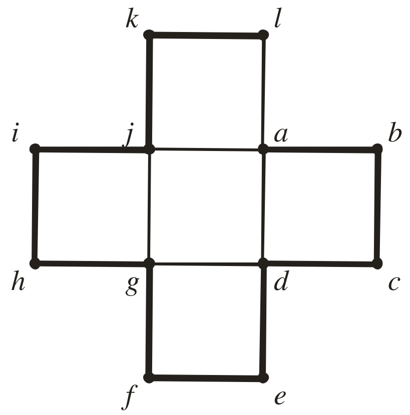
13.7. Použite prehľadávanie do hĺbky na nájdenie kostry daného jednoduchého grafu z obr. 13.24. Zvoľte vrchol a ako koreň tejto kostry a predpokladajte, že vrcholy sú usporiadané abecedne (namiesto typického postupu prehľadávania vykresleného grafu „zľava doprava“).

Obrázok 13.24. Kostra prehľadávaním do hĺbky?



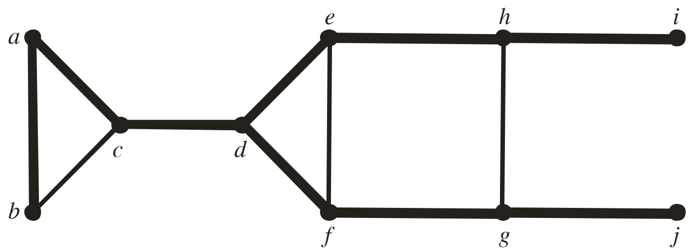
Nájdite kostru prehľadávaním do hĺbky.

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").

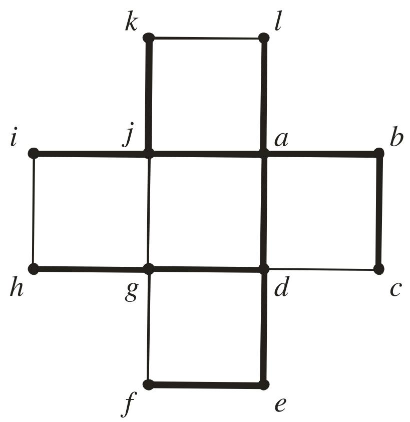
Postup pridávania hrán do kostry T by bol $\{a, b\}$, $\{a, c\}$, $\{c, d\}$, $\{d, e\}$, $\{d, f\}$, $\{e, h\}$, $\{f, g\}$, $\{h, i\}$, $\{g, j\}$



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?

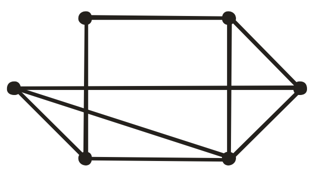
Platí v prípade, že je táto hrana mostom.

13.11. Kedy má jednoduchý súvislý graf práve jednu kostru?

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

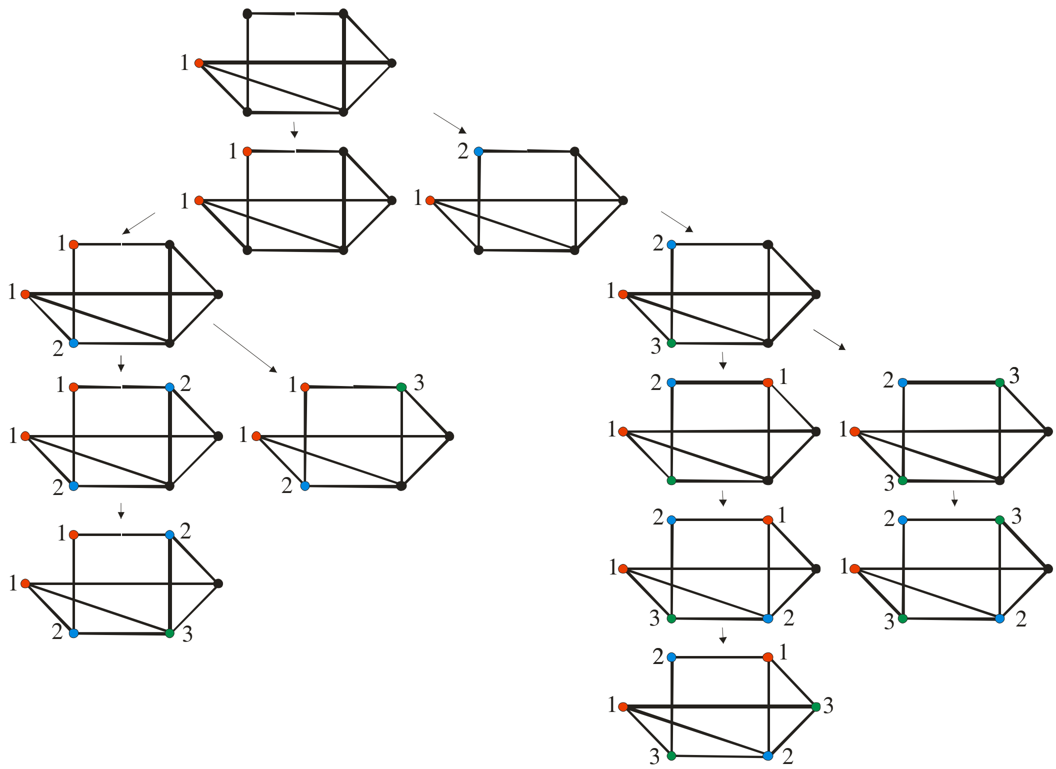
13.12. Použite prehľadávanie do hĺbky na nájdenie priradenia farieb vrcholom grafu z obr. 13.25 s využitím iba troch farieb.

OBRÁZOK 13.25. FARBENIE PREHĽADÁVANÍM DO HĹBKY?



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 3×3 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 vrátime 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.

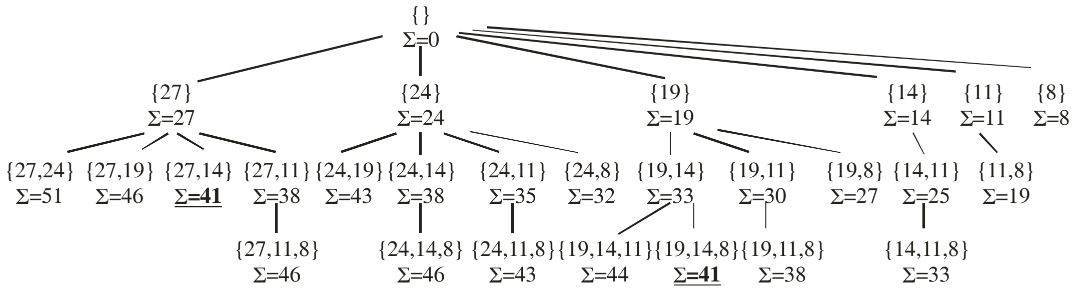
(c) $n = 6$

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 riešení nájdeme 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

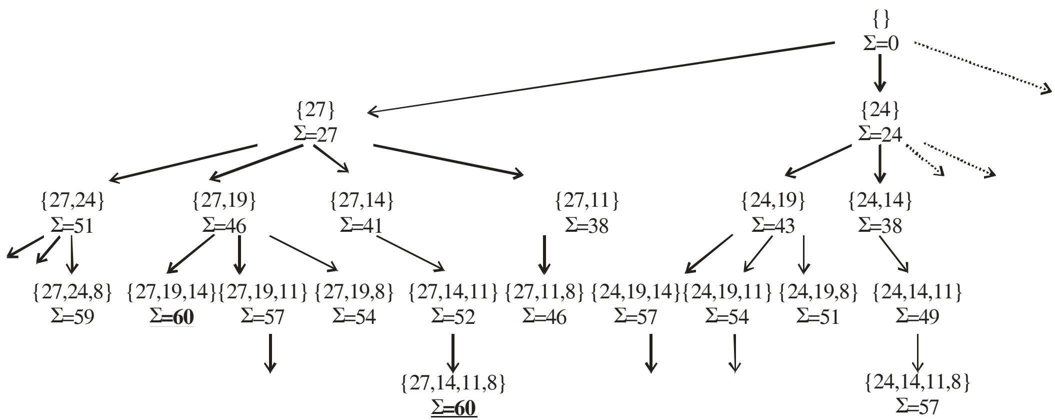
(a) 41

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.



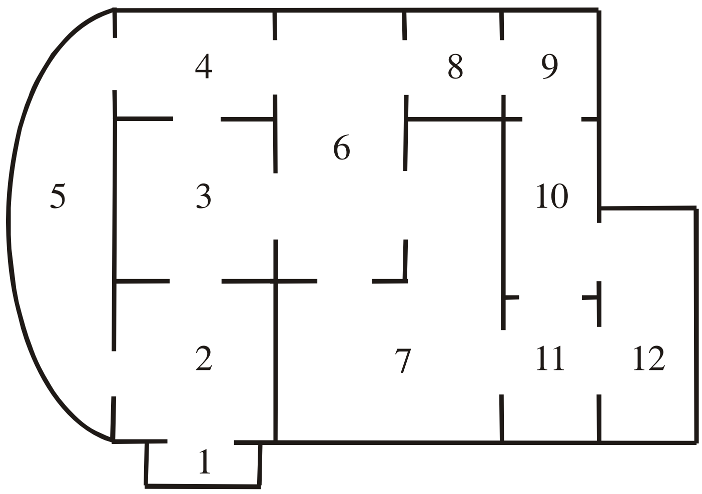
(b) 60

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 riešení nie je uvádzaný (aj keď do prehľadávania do hĺbky by sa takéto osekávanie stromu muselo špeciálne zaviesť).



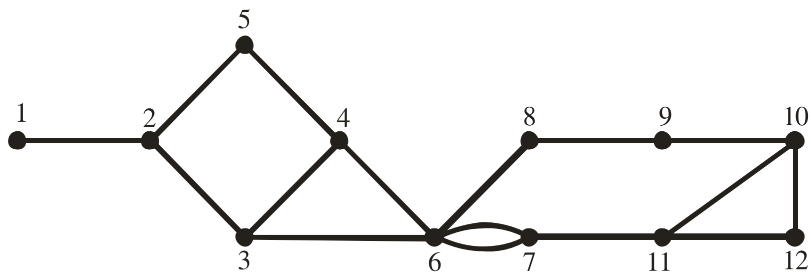
13.15. Vysvetlite, ako je možné prehľadávanie do hĺbky využiť na nájdenie cesty v múzeu, pri zadanej štartovnej pozícii a cieľovej pozícii. Múzeum má plán poschodia nakreslený na obr. 13.26.

OBRÁZOK 13.26. PLÁN MÚZEA PREROBIŤ NA GRAF



Plán múzea reprezentovať grafom.

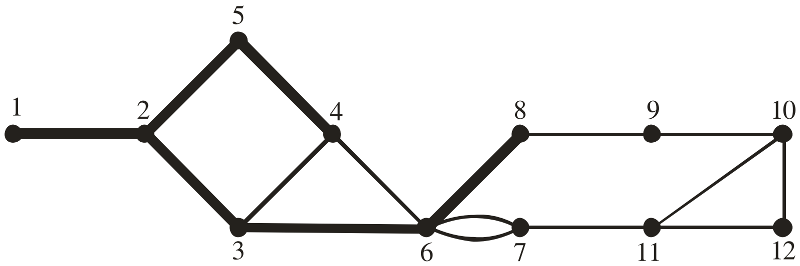
(a) Nakreslite graf reprezentujúci plán poschodia, kde každá miestnosť bude ako vrchol a každé dvere ako hrana.
Graf reprezentujúci plán poschodia:



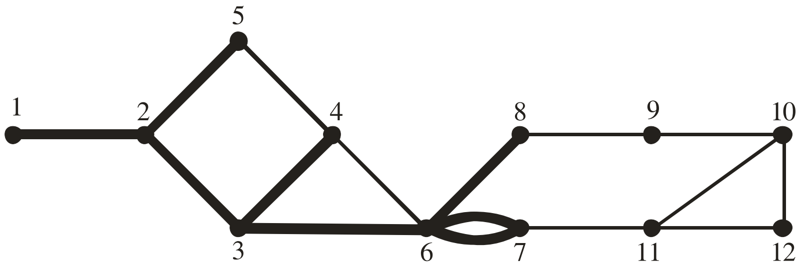
(b) Urobte prehľadávanie do šírky a do hĺbky, so štartom v miestnosti 1 a cieľom v miestnosti 8.

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

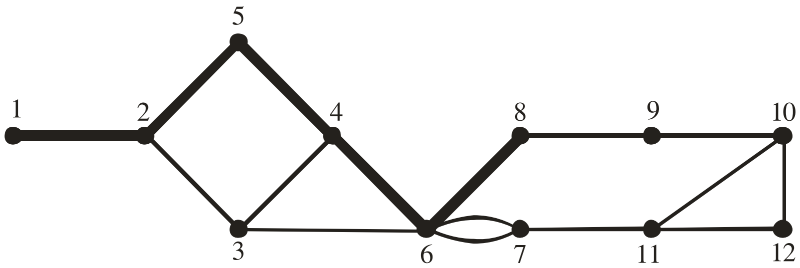
(A)



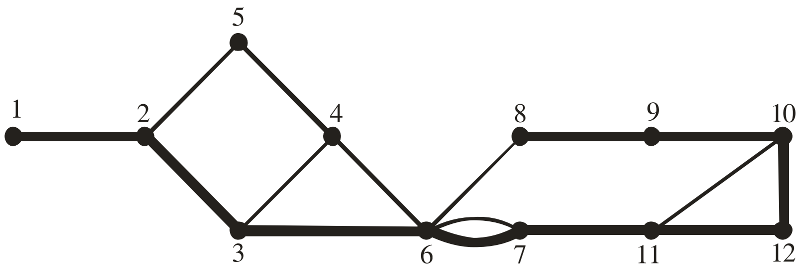
(B)



(C)



(D)



(c) Porovnajte, 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, Ľ.: *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

A

F

G

N

O

P

Q

R

S