KATEDRA INFORMATIKY
PŘÍRODOVĚDECKÁ FAKULTA
UNIVERZITA PALACKÉHO

ÚVOD DO INFORMATIKY

RADIM BĚLOHLÁVEK

Olomouc 2006

Abstrakt

Text je úvodem do informatiky. První část textu poskytuje informace o vybraných metodách diskrétní matematiky. Druhá část textu obsahuje základní informace o vybraných partiích informatiky. Text je psán matematickým stylem, tj. nové pojmy jsou definovány, o definovaných pojmech jsou vyslovována tvrzení a ta jsou pak dokazována. Důraz je kladen na motivaci pro zavedení nových pojmů a jejich vysvětlení. Text předpokládá jen základní středoškolské znalosti matematiky.

Cílová skupina

Text je určen pro studenty oborů Aplikovaná informatika a Informatika uskutečňovaných v prezenční formě na Přírodovědecké fakultě Univerzity Palackého v Olomouci.

Obsah

1 Základy logiky

Studijní cíle: Po prostudování kapitol 2.1 a 2.2 by student měl rozumět . . .

Klíčová slova: logika, pravdivostní hodnota.

1.1 Co a k čemu je logika?

Logika je věda o správném usuzování.

Logika je vědou o správném usuzování. V logice jde o to, aby usuzování mělo správnou *formu* bez ohledu na *obsah*. Uvažujme např. tvrzení „Prší.“ a „Jestliže prší, pak jsou silnice mokré“. Z nich lze odvodit tvrzení „Silnice jsou mokré.“ Uvažujme jinou dvojici tvrzení, např. „Petr má hlad.“ a „Jestliže má Petr hlad, pak se Petr snaží sehnat něco k jídlu.“ Z těchto tvrzení lze odvodit tvrzení „Petr se snaží sehnat něco k jídlu.“ V uvedených příkladech vyplývalo z dvojice tvrzení další tvrzení. Uvedené dvojice tvrzení měly zcela jistě jiný obsah, neboť „Prší.“ znamená něco jiného než „Petr má hlad.“ Způsob, jakým jsme odvodili třetí tvrzení byl však v obou případech stejný. Říkáme, že usuzování mělo stejnou formu. Tuto formu je možné znázornit *symbolicky* takto: z tvrzení A, a tvrzení $A \Rightarrow B$ (čteme „jestliže A, pak B“), plyne tvrzení B.

V logice jde o formu usuzování, ne o obsah usuzování.

Uvedené rysy jsou pro moderní logiku charakteristické, proto je zopakujme: logika studuje formy usuzování bez ohledu na obsah. Moderní logika má proto symbolický charakter, neboť jednotlivá tvrzení označujeme symboly (např. výše uvedenými symboly A a B), způsoby spojení tvrzení ve složitější tvrzení označujeme také symboly (např. výše uvedené “$\Rightarrow$”). Pro uvedené rysy bývá moderní logika označována jako *logika formální*, popř. *symbolická*. Symbolický charakter umožňuje logice snadněji odhlédnout od obsahu a soustředit se na formy usuzování.

Logika má symbolický charakter.

Slovo „logika“ má v běžném životě i jiné významy. Tyto významy jsou od původního významu, který jsme si právě vysvětlili, odvozené, ale jsou nepřesné a zavádějící. Měli bychom se proto snažit slovo „logika“ v těchto odvozených významech nepoužívat. Např. větou „Předložený návrh nemá žádnou logiku.“ chce autor říct, že návrh je nesrozumitelný, popř. špatně zdůvodněný, popř. neracionální. Větou „Logika našeho podnikání spočívá v maximálním uspokojování potřeb zákazníka.“ chce autor říct, že uspokojování potřeb zákazníků je hlavním rysem jeho podnikatelské strategie. „To je nelogické.“ znamená, že to nemá smysl. Podobných příkladů můžeme najít celou řadu.

Při studiu otázek, které v logice vznikají, se často používá matematických metod. Z tohto důvodu se někdy hovoří o *matematické logice*.

Budeme se zabývat klasickou logikou.

Dalším přívlastkem, který se v souvislosti s pojmem logika používá, je „klasická“, popř. „neklasická“. Zjednodušeně lze říci, že *klasickou logikou* se rozumí logika, která používá dvě pravdivostní hodnoty (pravda a nepravda) a tzv. klasické logické spojky. Mezi klasické logické spojky patří např. spojka “jestliže . . . , pak. . . ”, se kterou jsme se setkali výše. Logika, která se zabývá i jinými spojkami než klasickými, popř. dalšími aspekty, kterými se klasická logika nezabývá, se nazývá *neklasická logika*. Příkladem neklasické spojky je spojka “je možné, že . . . ”. Touto spojkou se zabývá modální logika. Dalším příkladem neklasické logiky je tzv. temporální logika (někdy nazývaná logikou času). Temporální logika, se zabývá tvrzeními, ve kterých hraje roli čas, např. „Po zelené naskočí na semaforu oranžová.“, „Každý den vychází Slunce.“ Dalším príkladem neklasické logiky je tzv. *fuzzy logika*. Ta se zabývá tvrzeními, které mohou mít kromě pravdivostních hodnot pravda a nepravda i jiné hodnoty. Např tvrzení „Zákazník je spokojený.“ může mít pravdivostní hodnotu 1 (pravda), pokud je spokojený bez výhrad, 0 (nepravda), pokud je nespokojený, ale i 0.8, pokud je např. spokojený, ale ne zcela. Fuzzy logika našla významné uplatnění v praxi a stále v ní probíhá intenzívní výzkum.

Existují i neklasické logiky, např. modální logika, temporální logika, fuzzy logika.

Vztah logiky a informatiky je bohatý a různorodý.

Vztah logiky a informatiky je bohatý a různorodý. Se základy logiky by měl být obeznámen každý informatik. Znalost základů logiky nám umožňuje srozumitelně a jednoznačně se vyjadřovat a argumentovat. To je pochopitelně užitečné pro každého, nejen pro informatika. Pro informatika je to však navýsost důležité proto, že svoje konstrukce a návrhy musí „sdělit počítači“, např. ve formě zdrojového kódu napsaného ve vhodném programovacím jazyku. Zdrojový kód obvykle obsahuje výrazy, které se vyhodnocují podle pravidel logiky (např. podmínky v příkazech větvení „if . . . then . . . else . . . “). Logika nás těmto pravidlům učí. Zdrojový kód musí být přesný, jinak je program chybný. Chyby mohou mít dalekosáhlé následky (pomysleme na program pro výpočet mezd, program pro řízení elektrárny apod.). Zdrojový program musí

být také srozumitelný, jinak mu nikdo jiný než jeho autor nebude rozumět (a po čase mu nebude rozumět ani jeho autor). Logika nás učí přesnosti i srozumitelnosti. To je další významný efekt studia logiky.

Logika nás učí přesnosti i srozumitelnosti.

Pokročilejší partie logiky jsou základem důležitých oblastí informatiky, pro příklad jmenujme logické programování, umělou inteligenci, expertní systémy, analýzu dat.

1.2 Výroky a logické spojky

Výrokem intuitivně rozumíme tvrzení (výpověď), u kterého má smysl uvažovat o jeho pravdivosti. Výroky jsou např. následující tvrzení.

Výrok je tvrzení, které může být pravdivé nebo nepravdivé.

Prší.

Byl jsem v obchodě a koupil jsem si knihu.

Když prší, jsou mokré silnice.

$2 + 2 = 4$ a $3 < 100$.

$2 + 2 = 6$.

Následující tvrzení ale nejsou výroky.

Kniha v obchodě.

$2 + 2$

Ať je pěkné počasí.

Z jednodušších výroků se vytvářejí složitější výroky pomocí tzv. *logických spojek*[1]. Logické spojky jsou speciální jazykové výrazy jako např.

Logické spojky jsou jazykové výrazy, kterými z jednodušších výroků vytváříme výroky složitější.

"... a ...", "... nebo ...", "jestliže ..., pak ...",
"..., právě když ...", "ne ..." (tj. "není pravda, že ...").

Např. z výroku "2+2=4" a výroku "Prší." můžeme vytvořit pomocí spojky "a" výrok "2+2=4 a Prší." Z výroku "Prší." vytvoříme pomocí spojky "ne" (tj. "není pravda, že ...") výrok "Neprší." (tj. "Není pravda, že prší."). Z výroků "Prší." a "Silnice jsou mokré." vytvoříme pomocí spojky "jestliže ..., pak ..." výrok "Jestliže prší, pak jsou silnice mokré."

Průvodce studiem

Všimněme si, že pojem spojka zde používáme v širším významu než bývá běžné: spojkou chápeme jazykový výraz, jehož použitím na výroky dostaneme nový výrok. Např. výrok "Jestliže prší, pak jsou silnice mokré." vznikl použitím spojky "jestliže..., pak ..." na výroky "Prší." a "Silnice jsou mokré." Z hlediska českého jazyka je výraz "jestliže" spojkou, jinou spojkou je výraz "pak".

Všimněme si také, že při použití spojek na výroky měníme pořadí větných členů. Např. v právě uvedeném příkladu by přísně vzato výsledným výrokem měl být výrok "Jestliže prší, pak silnice jsou mokré.". Tento výrok ale nezní pěkně. Podobné jazykové jevy budeme z hlediska logiky považovat za podružné a nebudeme se jimi zabývat. Ze stejného důvodu nebudeme rozlišovat např. tvrzení "Neprší." a "Není pravda, že prší."

Klasická logika (té se budeme věnovat) se zabývá tzv. klasickými spojkami. Mezi ně patří výše uvedené spojky, s dalšími klasickými spojkami se seznámíme později.

[1] Místo "logická spojka" říkáme často jen "spojka".

Průvodce studiem

Kromě klasických spojek se v běžném životě používají i další spojky, např. "je možné, že . . . ", "je nutné, že . . . ", "ví se, že . . . ", "věří se, že . . . ". Např. z výroku "Vesmír je nekonečný." vytvoříme pomocí spojky "věří se, že . . . " výrok "Věří se, že vesmír je nekonečný.", pomocí spojky "je možné, že . . . " pak výrok "Je možné, že vesmír je nekonečný." Spojkami "je možné, že . . . ", "je nutné, že . . . " se zabývá modální logika, spojkami "ví se, že . . . ", "věří se, že . . . " se zabývá epistemická logika. Tyto spojky jsou složitější než klasické spojky a my se jimi zabývat nebudeme.

Některé výroky jsou pravdivé (např. "2+2=4"), některé jsou nepravdivé (např. "2+2=6"). O tvrzení, které je pravdivé, řekneme, že má pravdivostní hodnotu 1 (pravda); o tvrzení, které je nepravdivé, řekneme, že má pravdivostní hodnotu 0 (nepravda).

Průvodce studiem

U některých tvrzení má smysl uvažovat o jejich pravdivosti (jsou tedy výroky), např. "Člověk s výškou 180cm je vysoký", přesto se však zdráháme říci, že dané tvrzení je pravdivé nebo, že není pravdivé (je nepravdivé). Pravdivostní hodnota, kterou bychom mu přiřadili, by byla někde mezi 0 a 1, např. řekneme-li, že "Člověk vysoký 180cm je vysoký" má pravdivostní hodnotu 0.8, říkáme tím, že je pravdivé ve stupni 0.8, tj. že je skoro pravdivé. V následujícím se omezíme na (tvrzení, které mohou mít jen) dvě pravdivostní hodnoty (0 a 1). Poznamenejme pouze, že studiem více pravdivostních hodnot se zabývá tzv. fuzzy logika (ta je v současné době intenzívně zkoumána).

U některých tvrzení závisí pravdivostní hodnota na čase, např. "Za týden bude pršet." Takovými tvrzeními se zabývá temporální logika (logika času). My se takovými tvrzeními zabývat nebudeme.

Klasická logika se tedy zabývá jen speciálními výroky. Nepokrývá všechny výroky, které v běžném životě používáme, pokrývá ale jejich významnou část. V dalším výkladu se zaměříme na to, jak se výrokům přiřazují pravdivostní hodnoty.

1.3 Pravdivostní hodnota výroku

Výrok může být pravdivý nebo nepravdivý.

V předchozí části jsme si řekli, že některé výroky jsou pravdivé, některé jsou nepravdivé. Je-li výrok V pravdivý, říkáme také, že má pravdivostní hodnotu "pravda". Místo "pravda" používáme symbolické označení 1, a říkáme tedy, že V má pravdivostní hodnotu 1. Je-li výrok V nepravdivý, říkáme, že má pravdivostí hodnotu "nepravda", popř. že má pravdivostní hodnotu 0. Že je výrok V pravdivý, resp. nepravdivý, pak zapisujeme také

$$||V|| = 1, \qquad ||V|| = 0,$$

tj. pravdivostní hodnotu výroku V označujeme $||V||$.

Jak ale zjistíme pravivostní hodnotu výroku? Podívejme se na následující výrok.

Prší a venkovní teplota je menší než 15°C.

Tento výrok vznikl použitím spojky "a" na výrok "Prší." a na výrok "Venkovní teplota je menší než 15°C." Výroky "Prší." a "Venkovní teplota je menší než 15°C." neobsahují žádné spojky. Takovým výrokům říkáme *atomické*. Pravdivostní hodnota výroku "Prší a venkovní teplota je menší než 15°C." závisí na pravdivostních hodnotách výroků "Prší." a "Venkovní teplota je menší než 15°C." Jsou-li oba výroky "Prší." i "Venkovní teplota je menší než 15°C." pravdivé, je i výrok "Prší a venkovní teplota je menší než 15°C." pravdivý. Jinak, tj. je-li některý z výroků "Prší." a "Venkovní teplota je menší než 15°C." nepravdivý, je výrok "Prší a venkovní teplota je menší než 15°C." nepravdivý.

Uvedený postup má obecnou platnost, a proto ho rozeberme podrobněji. Označme složený výrok "Prší a venkovní teplota je menší než 15°C." symbolem V. Atomické výroky "Prší." a "Venkovní teplota je menší

než 15°C.“ označmě symboly V_1 a V_2. Označme dále spojku “a” symbolem $\wedge\!\!\!\wedge$. Výrok V má tedy tvar (někdy říkáme formu)

$$V_1 \wedge\!\!\!\wedge V_2.$$

Pravdivostní hodnotu $||V_1 \wedge\!\!\!\wedge V_2||$ výroku $V_1 \wedge\!\!\!\wedge V_2$ vlastně “spočítáme” z pravdivostních hodnot $||V_1||$ a $||V_2||$ výroků V_1 a V_2 pomocí významu spojky “a”. Význam spojky “a” je dán následující tabulkou.

$\wedge$	0	1
0	0	0
1	0	1

Význam spojky “a” je tedy dán přiřazením pravdivostních hodnot dvojicím pravdivostních hodnot. Např. dvojici 0 a 0 je přiřazena hodnota 0, dvojici 0 a 1 hodnota 0, dvojici 1 a 0 hodnota 0, dvojici 1 a 1 hodnota 1, protože na průsečíku řádku označeného 0 a sloupce označeného 0 je hodnota 0 atd. Toto přiřazení (zobrazení, funkci) označme $\wedge$. Tabulka tedy říká $0 \wedge 0 = 0$, $0 \wedge 1 = 0$, $1 \wedge 0 = 0$, $1 \wedge 1 = 1$. Pravdivostní hodnota $||V_1 \wedge\!\!\!\wedge V_2||$ výroku $V_1 \wedge\!\!\!\wedge V_2$ je tedy dána vztahem

$$||V_1 \wedge\!\!\!\wedge V_2|| \;=\; ||V_1|| \wedge ||V_2||.$$

Tomuto vztahu je třeba rozumět takto: Pravdivostní hodnotu $||V_1 \wedge\!\!\!\wedge V_2||$ výroku $V_1 \wedge\!\!\!\wedge V_2$ (levá strana rovnice) spočítáme použitím funkce $\wedge$ na pravdivostní hodnoty $||V_1||$ a $||V_2||$ výroků V_1 a V_2. Tímto použitím získáme hodnotu $||V_1|| \wedge ||V_2||$ funkce $\wedge$ na pravdivostních hodnotách $||V_1||$ a $||V_2||$ (pravá strana rovnice). Hodnotu $||V_1|| \wedge ||V_2||$ zjistíme z výše uvedené tabulky: je to hodnota na průsečíku řádku označeného $||V_1||$ a sloupce označeného $||V_2||$.

Otázkou zůstává, jak zjistíme pravdivostní hodnoty $||V_1||$ a $||V_2||$ výroků V_1 a V_2. Zde musíme rozlišit dva případy.

1. Je-li výrok V_i atomický, tj. neobsahuje logické spojky, pak jeho pravdivostní hodnota musí být dána “zvenčí”. Např. v našem případě jsou oba výroky V_1 (“Prší.”) i V_2 (“Venkovní teplota je menší než 15°C.”) atomické. Jejich pravdivostní hodnotu nám někdo řekne, popř. ji sami zjistíme (podíváme se z okna, podíváme se na teploměr, najedeme na internetu apod.). Obecně budeme předpokládat, že existuje nějaký externí zdroj informací, označme ho e, pomocí kterého pravdivostní hodnotu $e(V_i)$ výroku V_i zjistíme.

2. Není-li výrok V_i atomický, tj. obsahuje logické spojky, pak je to složený výrok a jeho pravdivostní hodnotu spočítáme podobně jako jsme počítali pravdivostní hodnotu původního výroku V. Pokud je např. výrok V_1 složeným výrokem a má tvar $V_{11} \wedge\!\!\!\wedge V_{12}$, pak pravdivostní hodnotu $||V_1||$ výroku V_1, tj. hodnotu $||V_{11} \wedge\!\!\!\wedge V_{12}||$ výroku $V_{11} \wedge\!\!\!\wedge V_{12}$ spočítáme podle vztahu

   $$||V_{11} \wedge\!\!\!\wedge V_{12}|| \;=\; ||V_{11}|| \wedge ||V_{12}||.$$

   Výroky V_{11} a V_{12} mohou být opět složné nebo atomické a při určování jejich pravdivostních hodnot postupujeme obdobně.

Výrok V je jazykový výraz (tvrzení), např. “Prší a venkovní teplota je menší než 15°C.” Pravdivostní hodnota výroku V závisí na významu logických spojek a na pravdivostních hodnotách atomických výroků, ze kterých se výrok V skládá. V našem případě závisí pravdivostní hodnota výroku V na tabulce pravdivostních funkce $\wedge$ spojky “a” a na pravdivostních hodnotách atomického výroku “Prší.” a atomického výroku “Venkovní teplota je menší než 15°C.” Tabulky pravdivostních funkcí logických spojek považujeme za jednou provždy dané (pevné, konstantní). Jak jsme ale řekli, pravdivostní hodnoty atomických výroků jsou dány zvenčí. Někdo náme jde musí sdělit nebo je musíme zjistit. Obecně předpokládáme, že pravdivostní hodnoty e(“Prší.”) a e(“Venkovní teplota je menší než 15°C.”) výroků “Prší.” a “Venkovní teplota je menší než 15°C.” zjistíme z nějakého externího zdroje informací e. Na tomto zdroji tedy pravdivostní hodnota výroku V závisí. proto bychom přesněji měli psát

$$||V||_e \qquad \text{místo} \qquad ||V||,$$

abychom explicitně zdůraznili, že jde o pravdivostní hodnotu výroku V při e. Na e se vlastně můžeme dívat jako na přiřazení, které atomickým výrokům přiřazuje pravdivostní hodnoty. e se proto v logice nazývá pravdivostní ohodnocení (atomických výroků).

název	zápis v přirozeném jazyce	symbol	pravdivostní funkce	tabulka pravd. funkce
negace	"ne"	$\neg$	$\neg$	$\begin{array}{c\|c} a & \neg a \\ \hline 0 & 1 \\ 1 & 0 \end{array}$
konjunkce	"a"	$\wedge$	$\wedge$	$\begin{array}{c\|cc} \wedge & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$
disjunkce	"nebo"	$\vee$	$\vee$	$\begin{array}{c\|cc} \vee & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array}$
implikace	"jestliže . . . , pak . . . "	$\Rightarrow$	$\rightarrow$	$\begin{array}{c\|cc} \rightarrow & 0 & 1 \\ \hline 0 & 1 & 1 \\ 1 & 0 & 1 \end{array}$
ekvivalence	". . . , právě když . . . "	$\Leftrightarrow$	$\leftrightarrow$	$\begin{array}{c\|cc} \leftrightarrow & 0 & 1 \\ \hline 0 & 1 & 1 \\ 1 & 0 & 1 \end{array}$

Tabulka 1: Základní logické spojky.

Stejně jako v případě spojky "a" postupujeme i v případě ostatních logických spojek, např. "ne", "nebo", "jestliže . . . , pak . . . ", ". . . , právě když . . . ". Tyto spojky označujeme symboly $\neg$, $\vee$, $\Rightarrow$, $\Leftrightarrow$. Jejich významy, tj. zobrazení popisující přiřazení pravdivostních hodnot, pak označujeme $\neg$, $\vee$, $\rightarrow$, $\leftrightarrow$. Přehled právě uvedených logických spojek podává Tabulka 1.3.

Pravdivostní hodnota výroku se počítá z pravdivostních hodnot atomických výroků pomocí pravdivostních funkcí spojek.

Průvodce studiem

Každá logická spojka má své označení a svůj význam. Označením je symbol logické spojky. Významem je pravdivostní funkce logické spojky. Symboly a pravdivostní funkce základních logických spojek podává Tabulka 1.3.

Příklad 1.1. Máme za úkol určit pravdivostní hodnotu výroku "$2 + 2 = 5$ nebo číslo 10 je dělitelné číslem 6." Jde o složený výrok, který vznikl použitím spojky konjunkce ("a") na atomické výroky "$2 + 2 = 5$" a "Číslo 10 je dělitelné číslem 6." Označíme-li tyto atomické výroky symboly V_1 a V_2 a složený výrok symbolem V, můžeme výrok V zapsat symbolicky ve tvaru $V_1 \vee V_2$. Přitom víme, že "$2 + 2 = 5$" je nepravdivý výrok a "Číslo 10 je dělitelné číslem 6." je také nepravdivý výrok, tj. e("$2 + 2 = 5$") $= 0$ a e("Číslo 10 je dělitelné číslem 6.") $= 0$. Pro pravdivostní hodnotu výroku "$2 + 2 = 5$ nebo číslo 10 je dělitelné číslem 6." potom dostaneme

$$\begin{aligned} & ||\text{"}2 + 2 = 5 \text{ nebo číslo 10 je dělitelné číslem 6."}|| = \\ = \quad & ||V||_e = ||V_1 \vee V_2||_e = ||V_1||_e \vee V_2||_e = 0 \vee 0 = 0. \end{aligned}$$

Poznámka 1.2. V případě složených výroků často používáme závorky, abychom jednoznačně vyznačili strukturu výroku. Např. kdybychom napsali "$2 \cdot 3 = 5$ a $2 + 2 = 5$ nebo $2 + 2 = 4$", není jasné, jestli myslíme "$2 \cdot 3 = 5$ a ($2 + 2 = 5$ nebo $2 + 2 = 4$)" nebo "($2 \cdot 3 = 5$ a $2 + 2 = 5$) nebo $2 + 2 = 4$". Všimněme si, že při prvním uzávorkování dostaneme nepravdivý výrok, zatímco při druhém uzávorkování dostaneme výrok pravdivý. Závorky používáme i při symbolickém zápisu výroků. Píšeme např. $V_1 \wedge (V_2 \vee V_3)$, $(V_1 \wedge V_2) \vee V_3$.

Shrňme nyní, co víme o určování pravdivostní hodnoty výroku.

Průvodce studiem

Je-li dán výrok V v přirozeném jazyce a máme-li určit jeho pravdivostní hodnotu, postupujeme následovně.

1. Určíme atomické výroky $V_1, \ldots, V_n$, ze kterých se V skládá.
2. Určíme pravdivostní hodnoty $e(V_1), \ldots, e(V_n)$ atomických výroků $V_1, \ldots, V_n$. Hodnoty $e(V_i)$ jsou součástí zadání nebo je zjistíme nebo je známe.
3. Výrok V zapíšeme v symbolické podobě, dostaneme např. $V_1 \wedge (V_2 \Rightarrow V_3)$.
4. Je-li V atomický výrok, pak $||V||_e = e(V)$.
5. Je-li V složený výrok, tj. má jeden z tvarů $\neg\, V_1$, $V_1 \wedge V_2$, $V_1 \vee V_2$, $V_1 \Rightarrow V_2$, $V_1 \Leftrightarrow V_2$, pak jeho pravdivostní hodnotu určíme podle pravidel
   - $||\neg\, V_1||_e = \neg||V_1||_e$,
   - $||V_1 \wedge V_2||_e = ||V_1||_e \wedge ||V_2||_e$,
   - $||V_1 \vee V_2||_e = ||V_1||_e \vee ||V_2||_e$,
   - $||V_1 \Rightarrow V_2||_e = ||V_1||_e \rightarrow ||V_2||_e$,
   - $||V_1 \Leftrightarrow V_2||_e = ||V_1||_e \leftrightarrow ||V_2||_e$.

Poznámka 1.3. Poznamenejme, že ohodnocení e (náš externí zdroj informací, který říká, které atomické výroky jsou pravdivé a které jsou nepravdivé) někdy není popsán úplně. U některých atomických výroků se totiž předpokládá, že je známo, zda jsou pravdivé či nikoli. Naše zadání potom je např.

> Určete pravdivostní hodnotu výroku "$2 + 2 = 4$ a $2 \cdot 3 = 5$".

místo úplného

> Určete pravdivostní hodnotu výroku "$2 + 2 = 4$ a $2 \cdot 3 = 5$", víte-li, že "$2 + 2 = 4$" je pravdivý a "$2 \cdot 3 = 5$" je nepravdivý vyýrok.

U zkráceného zadání se předpokládalo, že víme $e(\text{"}2 + 2 = 4\text{"}) = 1$ a $e(\text{"}2 \cdot 3 = 5\text{"}) = 0$.

Příklad 1.4. Určeme pravdivostní hodnotu výroku "$2 + 2 = 4$ a číslo 10 je dělitelné číslem 6, právě když není pravda, že Čína je nejlidnatější stát světa.", víme-li, že "Čína je nejlidnatější stát světa." je pravdivý výrok.

Tento výrok se skládá ze tří atomických výroků, totiž z výroku "$2 + 2 = 4$", výroku "číslo 10 je dělitelné číslem 6" a výroku "Čína je nejlidnatější stát světa." Označíme-li tyto výroky V_1, V_2 a V_3, víme, že $e(V_1) = 1$, $e(V_2) = 0$, $e(V_3) = 1$. Symbolická podoba zadaného výroku je $(V_1 \wedge V_3) \Leftrightarrow (\neg\, V_4)$. Pravdivostní hodnota $||(V_1 \wedge V_3) \Leftrightarrow (\neg\, V_4)||$ je

$$||(V_1 \wedge V_3) \Leftrightarrow (\neg\, V_4)|| = ||V_1 \wedge V_3|| \leftrightarrow ||\neg\, V_4|| =$$
$$(||V_1|| \wedge ||V_3||) \leftrightarrow (\neg||V_4||) = (1 \wedge 0) \leftrightarrow (\neg 1) = 0 \leftrightarrow 0 = 1,$$

tedy výrok "$2 + 2 = 4$ a číslo 10 je dělitelné číslem 6, právě když není pravda, že Čína je nejlidnatější stát světa." je pravdivý.

1.4 Kvantifikátory a pravdivostní hodnoty výroků s kvantifikátory

Některé výrazy přirozeného jazyka obsahují proměnné. Příkladem jsou věty

Číslo x je větší nebo rovno 3.

$2 + y = 4$.

Jestliže je x dělitelné deseti, pak je x sudé.

$x + y \geq z$.

Tyto výrazy nejsou výroky. K tomu, aby se tyto výrazy staly výroky, bychom museli určit hodnotu proměnných, které se v těch výrazech vyskytují. Dosazením hodnot za proměnné vzniknou z těchto výrazů výroky. V našem případě, pokud dosadíme 1 za x, 2 za y, 103 za z, dostaneme výroky

Číslo 1 je větší nebo rovno 3.

$2 + 2 = 4$.

Jestliže je 1 dělitelné deseti, pak je 1 sudé.

$1 + 2 \geq 103$.

První a čtvrtý výrok je nepravdivý, druhý a třetí je pravdivý.

Výrazy, obsahující proměnné, ze kterých se po dosazení hodnot za proměnné stanou výroky, se nazývají výrokové formy.

Výrazy obsahující proměnné, které se po dosazení hodnot za proměnné stanou výroky, se nazývají *výrokové formy*.. Výroky jsme označovali písmeny, např. V. Výrokové formy bývá znakem označovat písmenem, za kterým jsou v závorce uvedeny všechny proměnné, které forma obsahuje. Např. "Číslo x je větší nebo rovno 3." bychom označili $V(x)$, "$x + y \geq z$" bychom označili $U(x, y, z)$ apod. Výraz, který vznikne z výrazu $U(x, y, z)$ dosazením hodnoty 6 za proměnnou y, označíme $U(x, 6, z)$ apod. Poznamenejme, že $U(x, 6, z)$ není výrok, neboť stále obsahuje proměnné. Výrokem bude např. výraz $U(1, 6, 100)$, tj. výraz "$1 + 6 \geq 100$".

Z výrokových forem můžeme tedy tvořit výroky dosazením hodnot za proměnné. Pro každou proměnnou x, která se v dané výrokové formě vyskytuje, bychom ale měli zadat její *obor hodnot*, tj. množinu D_x všech hodnot, kterých může proměnná x nabývat. Obor hodnot D_x se někdy nezadává, zvláště je-li z nějakého důvodu zřejmý. To však může vést k nedorozumění, a proto bychom obor hodnot každé proměnné měli vždy zadat. Např. u výrazu "x je větší nebo rovno 3" není jasné, co je oborem hodnot proměnné x. Tento obor musíme zadat. Musíme např. říct, že x může nabývat hodnot z množiny všech celých čísel, tj. $D_x = \{0, 1, -1, 2, -2, 3, -3, \dots\}$.

Kvantifikátory jsou jazykové výrazy, kterými s výrokových forem vznikají výroky. V klasické logice rozeznáváme obecný a existenční kvantifikátor.

Další způsob, jak tvořit z výrokových forem výroky představují *kvantifikátory*. V klasické logice rozeznáváme dva kvantifikátory, obecný a existenční.

Obecný kvantifikátor s proměnnou x je výraz

"Pro každý x platí, že . . . ",

popř. jen "Pro každý x . . . ". Symbolicky se obecný kvantifikátor s proměnnou x označuje výrazem $(\forall x)$. Použitím obecného kvantifikátoru na výraz "x je větší nebo rovno 1" dostaneme výraz

"Pro každý x platí, že x je větší nebo rovno 1",

Obecný kvantifikátor se značí symbolem $\forall$, existenční kvantifikátor se značí symbolem $\exists$.

což můžeme zapsat také symbolicky jako "$(\forall x)$ (x je větší nebo rovno 1)", popř. "$(\forall x)$ ($x \geq 1$)".

Existenční kvantifikátor s proměnnou x je výraz

"Existuje x tak, že platí . . . ",

popř. jen "Existuje x tak, že . . . ". Symbolicky se existenční kvantifikátor s proměnnou x označuje výrazem $(\exists x)$. Použitím existenčního kvantifikátoru na výraz "x je větší nebo rovno 1" dostaneme výraz

"Existuje x tak, že x je větší nebo rovno 1.",

což můžeme zapsat také symbolicky jako "$(\exists x)$ (x je větší nebo rovno 1).", popř. "$(\exists x)$ ($x \geq 1$)". Tento výraz je výrokem.

Průvodce studiem

Symboly $\forall$ a $\exists$ pro obecný a existenční kvantifikátor pocházejí z němčiny. Symbol $\forall$ vznikl otočením počátečního velkého „A“ ve slově „allgemein“, což je německý výraz pro „obecný“. Symbol $\exists$ vznikl otočením počátečního velkého „E“ ve slově „existentiell“, což je německý výraz pro „existenční“.

Obecně platí, že použitím obecného nebo existenčního kvantifikátoru s proměnnou x na výrokovou formu, jejíž jedinou proměnnou je proměnná x, získáme výrok. To je snadno vidět. Např. ve výše uvedeném příkladu vznikl výrok "Existuje x tak, že x je větší nebo rovno 1." použitím existenčního kvantifikátoru na výraz "x je větší nebo rovno 1."

Použitím kvantifikátorů na výrokové formy vznikají výroky.

Obecněji platí, že výrok vznikne použitím obecného nebo existenčního kvantifikátoru s proměnnou x na výraz, ve kterém je proměnná x jedinou proměnnou, která má v daném výrazu volný výskyt. Pojem volný výskyt proměnné zde nebudeme přesně definovat. Je to pojem intuitivně jasný, a proto zůstaneme v rovině intuice. Řekneme, že výskyt proměnné x v nějakém výrazu je volný, pokud se proměnná x v tomto výskytu nenachází v dosahu platnosti nějakého kvantifikátoru s proměnnou x. Uvažujme např. výraz

(Pro každé z je z vetší než 0) nebo (existuje y tak, že x je menší než y).

Dosah platnosti kvantifikátoru je ta část výrazu, na kterou se kvantifikátor vztahuje. Např. dosah platnosti kvantifikátoru "Pro každé z" je "z vetší než 0", dosah platnosti kvantifikátoru "existuje y" je "x je menší než y" apod. Proto výskyt proměnné z ve výrazu "z vetší než 0" není volným výskytem (z je totiž v dosahu platnosti kvantifikátoru "Pro každé z"), výskyt proměnné y ve výrazu "x je menší než y" není volným výskytem (y je totiž v dosahu platnosti kvantifikátoru "existuje y"), ale výskyt proměnné x ve výrazu "x je menší než y" je volným výskytem.

Podívejme se nyní, jak se vyhodnocují pravdivostní hodnoty výroků, které obsahují kvantifikátory. Předpokládejme, že je dána výroková forma $V(x)$, kde x je proměnná s oborem hodnot D_x. Pravdivostní hodnotu $||(\forall x)V(x)||$ výroku $(\forall x)V(x)$, tj. výroku "Pro každé x platí $V(x)$" definujeme pravidlem

Pravdivostní hodnoty výroků s kvantifikátory se určují podle jednoduchých pravidel.

$$||(\forall x)V(x)|| = \begin{cases} 1 & \text{pokud pro každé } m \in D_x \text{ je } ||V(m)|| = 1 \\ 0 & \text{jinak.} \end{cases}$$

Slovy: Výrok $(\forall x)V(x)$ je pravdivý, pokud pro každou hodnotu m z oboru D_x je výrok $V(m)$, který vznikne dosazením m do výrokové formy $V(x)$, pravdivý. Pravdivostní hodnotu $||(\exists x)V(x)||$ výroku $(\exists x)V(x)$, tj. výroku "Existuje x tak, že platí $V(x)$" definujeme pravidlem

$$||(\exists x)V(x)|| = \begin{cases} 1 & \text{pokud aspoň pro jedno } m \in D_x \text{ je } ||V(m)|| = 1 \\ 0 & \text{jinak.} \end{cases}$$

Slovy: Výrok $(\exists x)V(x)$ je pravdivý, pokud pro alespoň jednu hodnotu m z oboru D_x je výrok $V(m)$, který vznikne dosazením m do výrokové formy $V(x)$, pravdivý.

Příklad 1.5. (1) Je dán výrok "Pro každé x platí, že jestliže x je dělitelné 6, pak x je dělitelné 3". Oborem hodnot proměnné x je množina všech přirozených čísel, tj. $D_x = \{1, 2, 3, 4, \dots\}$. Určete pravdivostní hodnotu daného výroku.

Daný výrok můžeme symbolicky zapsat jako $(\forall x)(V(x))$, kde $V(x)$ je "Jestliže x je dělitelné 6, pak x je dělitelné 3." Podle výše uvedeného pravidla je $||(\forall x)(V(x))|| = 1$, právě když pro každé přirozené číslo m je $||V(m)|| = 1$. Přitom výrok $V(m)$ má tvar $V_1(m) \Rightarrow V_2(m)$, kde $V_1(m)$ je "m je dělitelné 6" a $V_2(m)$ je "m je dělitelné 3". Je zřejmé, že $||V_1(m) \Rightarrow V_2(m)|| = 1$, tj. že $||V(m)|| = 1$ (podrobněji: pro m dělitelná 6 je $||V_1(m) \Rightarrow V_2(m)|| = ||V_1(m)|| \rightarrow ||V_2(m)|| = 1 \rightarrow 1 = 1$; pro m nedělitelná 6 je $||V_1(m) \Rightarrow V_2(m)|| = ||V_1(m)|| \rightarrow ||V_2(m)|| = 0 \rightarrow ||V_2(m)|| = 1$). Ptoro je $||(\forall x)(V_1(x) \Rightarrow V_2(x))|| = 1$, tj. výrok "Pro každé x platí, že jestliže x je dělitelné 6, pak x je dělitelné 3" je pravdivý.

(2) Je dán výrok "Existuje x tak, že pro každé y platí, že $x \leq y$". Oborem hodnot proměnných x i y je množina všech přirozených čísel, tj. $D_x = D_y = \{1, 2, 3, 4, \dots\}$. Určete pravdivostní hodnotu daného výroku.

Daný výrok můžeme symbolicky zapsat jako $(\exists x)(\forall y)(V(x, y))$, kde $V(x, y)$ je "$x \leq y$". Přitom $(\forall y)(V(x, y))$ je výroková forma, kterou můžeme označit $U(x)$. Podle uvedených pravidel je $||(\exists x)(\forall y)(V(x, y))|| = 1$, tj. $||(\exists x)U(x)|| = 1$, právě když existuje přirozené číslo m tak, že $||U(m)|| = 1$. Zvolme za m číslo 1. $U(1)$ je výrok $(\forall y)(V(1, y))$. To je výrok tvaru $(\forall y)(W(y))$, kde $W(y)$ je výroková forma $V(1, y)$, tj. $W(y)$ je $1 \leq y$. Podle uvedených pravidel je $||(\forall y)(V(1, y))|| = 1$, tj. $||(\forall y)(W(y))|| = 1$, právě když pro každé přirozené číslo m je $||W(m)|| = 1$, tj. když pro každé přirozené číslo m je $||V(1, m)|| = 1$, tj. když pro každé přirozené číslo m je $1 \leq m$. To je evidentně pravda, a proto $||(\forall y)(V(1, y))|| = 1$, a tedy i $||(\exists x)(\forall y)(V(x, y))|| = 1$. Výrok "Existuje x tak, že pro každé y platí, že $x \leq y$" je tedy pravdivý.

Poznámka 1.6. Kvantifikátory se někdy objevují v následující podobě.

„Pro každé liché x platí, že $x^2 - 1$ je sudé." „Existuje sudé x tak, že x^2 je sudé.",

obecněji potom

„Pro každé x splňující $P(x)$ platí $V(x)$." „Existuje x splňující $P(x)$ tak, že $V(x)$."

Tato tvrzení jsou vlastně zkratkou za tvrzení

„Pro každé x platí, že jestliže $P(x)$, pak $V(x)$." „Existuje x tak, že $P(x)$ a $V(x)$."

1.5 Základy výrokové logiky

Úvod

Náš dosavadní výklad logiky ukázal několik základních pojmů a postupů, které jsou v logice důležité. Základní pojmy, se kterými jsme pracovali, tj. pojmy výrok a později výroková forma, však zůstaly jen neurčitě definované. Řekli jsme, že výrokem intuitivně rozumíme tvrzení, u kterého má smysl uvažovat o jeho pravdivosti. Tato definice, byť v řadě případů stačí, má dvě velké nevýhody. Za prvé, je nepřesná a ponechává prostor pro spekulace o tom, co to vlastně výrok je. Proto byly i další naše definice přísně vzato nepřesné a stavěné spíše na intuici[2]. Za druhé, je příliš široká, připouští i různá komplikovaná tvrzení, která mohou přinést zásadní problémy. Ukažme si to na příkladu, kterému se říká paradox lháře.

Náš pojem výroku je neurčitý a příliš široký.

Průvodce studiem

Představme si člověka C, který říká „Lžu". Podle našeho kritéria je to výrok. Je tento výrok pravdivý nebo ne?

Pojďme si to rozebrat. Jsou dvě možnosti. Buď je to pravdivý výrok nebo je to nepravdivý výrok.

Je-li výrok „Lžu." pravdivý, pak je pravda to, co C říká, tj. je pravda, že C lže. To, co C říká, je tedy nepravdivé, tedy i výrok „Lžu." je nepravdivý. Závěrem: Je-li výrok „Lžu." pravdivý, pak je tento výrok nepravdivý.

Je-li výrok „Lžu." nepravdivý, pak není pravda to, co C říká, tj. C nelže. To, co C říká, je tedy pravdivé, tedy i výrok „Lžu." je pravdivý. Závěrem: Je-li výrok „Lžu." nepravdivý, pak je tento výrok pravdivý.

Došli jsme k tomu, že výrok „Lžu." je pravdivý, právě když je nepravdivý. To je spor.

Přirozený jazyk je velmi bohatý. Obsahuje výroky, které vedou k logicky sporným situacím.

Paradox lháře ukazuje, že přirozený jazyk je natolik bohatý, že může vést k situacím, kdy nějaký výrok nemůže být ani pravdivý, ani nepravdivý, aniž by se porušila celková logická bezespornost. V případě paradoxu lháře je příčinou to, že výrok „Lžu." se odvolává sám na sebe, mluví sám o sobě, podobně jako výrok „Tento výrok je nepravdivý."

Má ale paradox lháře nějaké řešení? Jedním z možných řešení je vzdát se ambice pracovat se všemi možnými výroky přirozeného jazyka a namísto toho pracovat jen s určitými výroky, které ke sporům nevedou. Tak postupuje moderní matematická logika. Cílem Kapitoly 1.5 je ukázat si základy výrokové logiky. Výroková logika je nejjednodušší klasickou logikou. Umožní nám ale ukázat způsob, jakým se v moderní logice pracuje.

Jazyk výrokové logiky, formule, pravdivostní ohodnocení formulí

Na příkladu paradoxu lháře jsme viděli, že pokud nijak neomezíme množinu výroků, se kterými pracujeme, můžeme se dostat do sporu. Ve výrokové logice jsou výroky, se kterými se pracuje, omezené. Ve výrokové logice navíc nepracujeme s výroky samotnými, ale pracujeme s formami (tvary) výroků. Formy výroků se

nazývají formule a jsou to přesně definované řetězce symbolů. Definici formule uvedeme později. Příkladem formulí jsou řetězce $(p \wedge \neg q)$, $(p \Rightarrow (q \wedge r))$, $(p \wedge r) \vee q$. Formule je volně řečeno to, co je společné výrokům se stejným tvarem. Např. formule $(p \Rightarrow (q \wedge r))$ popisuje tvar mnoha konkrétních výroků, např. výroků „Jestliže prší, pak jsou silnice mokré a hrozí nebezpečí smyku.“, „Jestliže inflace roste, pak lidé méně spoří a více utrácejí.“ Tyto konkrétní výroky můžeme z formule $(p \Rightarrow (q \wedge r))$ dostat dosazením atomických výroků za symboly p, q, r, např. první výrok dostaneme dosazením „Prší.“ za p, „Silnice jsou mokré.“ za q a „Hrozí nebezpečí smyku.“ za r. Proto ze symbolům p, q, r, které se ve formulích výrokové logiky vyskytují, říká výrokové symboly. Tím, že ve výrokové logice pracujeme s formulemi, a ne s konkrétními výroky, se můžeme lépe odhlédnout od obsahu a soustředit se na formu. A o to nám v logice jde.

Formule výrokové logiky popisují tvar konkrétních výroků. Konkrétní výroky dostaneme z formulí nahrazením výrokových symbolů atomickými výroky.

Začneme definicí jaykza výrokové logiky.

Definice 1.7. *Jazyk výrokové logiky* se skládá z

Jazyk výrokové logiky obsahuje symboly, ze kterých se skládají formule výrokové logiky.

- *výrokových symbolů* $p, q, r, \ldots$, popř. s indexy, p_1, p_2; předpokládáme, že máme neomezeně mnoho (spočetně mnoho) výrokových symbolů;
- *symbolů výrokových spojek* $\neg$ (negace), $\Rightarrow$(implikace), popř. dále $\wedge$ (konjunkce), $\vee$ (disjunkce), $\Leftrightarrow$ (ekvivalence);
- *pomocných symbolů* (,), [,], atd. (různé druhy závorek).

Ze symbolů jazyka sestávají formule výrokové logiky.

Definice 1.8. Nechť je dán jazyk výrokové logiky. *Formule* daného jazyka výrokové logiky je definována následovně:

- každý výrokový symbol je formule (tzv. atomická formule);
- jsou-li φ a ψ formule, jsou i výrazy $\neg \varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \Rightarrow \psi)$, $(\varphi \Leftrightarrow \psi)$ formule.

Příklad 1.9. Formulemi jsou tedy jisté konečné posloupnosti symbolů jazyka výrokové logiky.

Formulemi jsou např. posloupnosti p, q_1, $\neg p$, $(p \Rightarrow q)$, $((p \wedge r) \vee p)$, $(\neg p \Rightarrow (q \wedge \neg r))$ jsou formule. Posloupnost $(\neg p \Rightarrow (q \wedge \neg r))$ je formule, protože: r je formule (atomická), tedy i $\neg r$ je formule, což spolu s tím, že q je formule, dává, že $(q \wedge \neg r)$ je formule; dále je p a tedy i $\neg p$ formule, a tedy konečně i $(\neg p \Rightarrow (q \wedge \neg r))$ je formule.

Formulemi nejsou posloupnosti $\wedge p$, $p \wedge \vee p$, $pp \Rightarrow (p \wedge))$, atd.

Všimněme si, že správně bychom měli říkat „formule daného jazyka výrokové logiky“. My však v případě, že jazyk je zřejmý z kontextu, popř. není důležitý, budeme říkat pouze „formule výrokové logiky“ nebo jen „formule“.

Poznámka 1.10 (konvence o vynechávání závorek)**.** Jak zná čtenář z aritmetiky, je pro zjednodušení zápisu a čtení užitečné vynechávat závorky tam, kde neutrpí jednoznačnost čtení. Podobně budeme postupovat i my. Např. místo $(p \Rightarrow q)$ budeme psát jen $p \Rightarrow q$. Dále se dohodneme na prioritách symbolů spojek: od největší po nejmenší je to $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$. To nám umožní vynechávat závorky. Tak např. místo $(p \wedge (q \wedge r))$ můžeme psát jen $p \wedge (q \wedge r)$, místo $(p \Rightarrow ((p \wedge q) \vee r))$ jen $p \Rightarrow p \wedge q \vee r$ apod.

Zatím jsme se věnovali jen tzv. syntaktické stránce výrokové logiky. Víme, co je to jazyk výrokové logiky, co jsou to formule. Zatím však nevíme, co to je pravdivá formule apod. Formule jsou jisté posloupnosti symbolů jazyka, samy o sobě však nemají žádný význam. Přiřazení významu syntaktickým objektům je záležitostí tzv. sémantiky. Právě sémantice výrokové logiky se v dalším budeme věnovat.

Definice 1.11. *(Pravdivostní) ohodnocení* je libovolné zobrazení e výrokových symbolů daného jazyka výrokové logiky do množiny $\{0, 1\}$, tj. ohodnocení e přiřazuje každému výrokovému symbolu p hodnotu 0 nebo 1.

[2] Přesto jsme se se základními principy klasické logiky poměrně dobře seznámili. Mohli jsme sice postupovat zcela přesně už od začátku, ale bylo by to na úkor srozumitelnosti.

Poznámka 1.12. (1) 0 a 1 reprezentují pravdivostní hodnoty nepravda a pravda. Hodnotu p5i5azenou ohodnocením e symbolu p označujeme $e(p)$. Je tedy $e(p) = 0$ neb $e(p) = 1$.

(2) Význam ohodnocení e můžeme chápat následovně. Jak jsme si řekli, výrokové symboly jsou pro nás symboly, které označují atomické výroky. Je-li $e(p) = 1$, znamená to pro nás, že atomický výrok označený symbolem p je pravdivý. Je-li $e(p) = 0$, znamená to, že atomický výrok označený symbolem p je nepravdivý.

Je-li dáno ohodnocení e, můžeme říci, co je to pravdivostní hodnota formule. Pravdivostní hodnota libovolné formule je pravdivostním ohodnocením jednoznačně určena a je definována následovně.

Definice 1.13. Nechť je dáno ohodnocení e. *Pravdivostní hodnota formule* φ při ohodnocení e, označujeme ji $\|\varphi\|_e$, je definována následovně:

- Je-li φ výrokovým symbolem p, pak

  $$\|p\|_e = e(p).$$

- Je-li φ složná formule, tj. jednoho z tvarů $\neg\ \psi$, $\psi \wedge \theta$, $\psi \vee \theta$, $\psi \Rightarrow \theta$, $\psi \Leftrightarrow \theta$, pak

  $$\begin{aligned}
  &\| \neg\ \psi\|_e = \neg\|\psi\|_e,\\
  &\|\psi \wedge \theta\|_e = \|\psi\|_e \wedge \|\theta\|_e,\\
  &\|\psi \vee \theta\|_e = \|\psi\|_e \vee \|\theta\|_e,\\
  &\|\psi \Rightarrow \theta\|_e = \|\psi\|_e \to \|\theta\|_e,\\
  &\|\psi \Leftrightarrow \theta\|_e = \|\psi\|_e \leftrightarrow \|\theta\|_e,
  \end{aligned}$$

  kde $\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$ jsou pravdivostní funkce logických spojek z Tabulky 1.3.

Poznámka 1.14. (1) Je-li $\|\varphi\|_e = 1$ ($\|\varphi\|_e = 0$), říkáme, že formule φ je při ohodnocení e pravdivá (nepravdivá). Uvědomme si, že nemá smysl říci "formule φ je pravdivá" nebo "nepravdivá" (musíme říci, při jakém ohodnocení!). Uvědomme si, že to přesně odpovídá situaci z Kapitoly 1.3, kdy jsme při určování pravdivostní hodnoty výroku museli znát pravdivostní hodnoty atomických výroků. Roli atomických výroků teď mají výrokové symboly.

(2) Část definice pravdivostní hodnoty formule, ve které se zavádí pravdivostní hodnota složené formule, můžeme alternativně uvést „slovně“:

$$\| \neg\ \psi\|_e = \begin{cases} 1 & \text{pokud } \|\psi\|_e = 1,\\ 0 & \text{jinak,}\end{cases}$$

$$\|\psi \wedge \theta\|_e = \begin{cases} 1 & \text{pokud } \|\psi\|_e = 1 \text{ a } \|\theta\|_e = 1,\\ 0 & \text{jinak,}\end{cases}$$

$$\|\psi \vee \theta\|_e = \begin{cases} 1 & \text{pokud } \|\psi\|_e = 1 \text{ nebo } \|\theta\|_e = 1,\\ 0 & \text{jinak,}\end{cases}$$

$$\|\psi \Rightarrow \theta\|_e = \begin{cases} 1 & \text{pokud } \|\psi\|_e = 0 \text{ nebo } \|\theta\|_e = 1,\\ 0 & \text{jinak,}\end{cases}$$

$$\|\psi \Leftrightarrow \theta\|_e = \begin{cases} 1 & \text{pokud } \|\psi\|_e = \|\theta\|_e,\\ 0 & \text{jinak.}\end{cases}$$

Snadno se vidí (ověřte si), že taková definice skutečně vede ke stejným pravdivostním hodnotám formulí.

Následující definice zavádí některé další užitečné pojmy.

Definice 1.15. Formule se nazývá

- *tautologie*, je-li při každém ohodnocení pravdivá,

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

Tabulka 2: Tabulka pro formuli $(p \Rightarrow q) \wedge (p \Rightarrow r)$.

- *kontradikce*, je-li při každém ohodnocení nepravdivá,
- *spnitelná*, je-li při aspoň jednom ohodnocení pravdivá.

Formule φ *sémanticky vyplývá* z množiny T formulí, označujeme $T \models \varphi$, jestliže φ je pravdivá pří každém ohodnocení, při kterém jsou pravdivé všechny formule z T.

Poznámka 1.16. Splnitelné formule jsou tedy právě ty, které nejsou kontradikcemi. Že je formule φ tautologie, se někdy zapisuje $\models \varphi$.

Příklad 1.17. (1) Formule $p \vee \neg p$ i $p \Rightarrow (p \vee q)$ jsou tautologie.

(2) Formule $p \wedge \neg p$ i $p \Leftrightarrow \neg p$ jsou kontradikce.

(3) Formule $p \Rightarrow \neg p$ je splnitelná, ale není to ani tautologie, ani kontradikce.

(4) Formule $p \Rightarrow q$ sémanticky vyplývá z množiny formulí $T = \{p \Rightarrow r, \neg q \Rightarrow \neg r\}$.

Příklad 1.18. Dokažme, že pro libovolnou množinu T formulí a formule φ, ψ platí

$$T, \varphi \models \psi \text{ právě když } T \models \varphi \Rightarrow \psi.$$

To je inutitivně poměrně jasné tvrzení. Přitom T, φ znamená $T \cup \{\varphi\}$, tj. T, φ označuje množinu T rozšířenou o formuli φ Důkaz je velmi snadný, stačí si rozmyslet, co máme dokázat. Předpokládejme tedy $T, \varphi \models \psi$ a dokažme $T \models \varphi \Rightarrow \psi$. Máme dokázat, že je-li e ohodnocení, při kterém jsou pravdivé všechny formule z T, je při e pravdivá i formule $\varphi \Rightarrow \psi$. Kdyby ale při e nebyla pravdivá formule $\varphi \Rightarrow \psi$, musela by být při e φ pravdivá a ψ nepravdivá (z definice pravdivostní funkce spojky implikace). Je-li ale při e pravdivá φ i všechny formule z T, pak je dle předpokladu $T, \varphi \models \psi$ pravdivá i ψ, což je spor s tím, že ψ je nepravdivá. Naopak, předpokládejme $T \models \varphi \Rightarrow \psi$ a dokažme $T, \varphi \models \psi$. Máme dokázat, že je-li e ohodnocení, při kterém je pravdivá φ i všechny formule z T, je při něm pravdivá i ψ. Dle předpokladu je ovšem při e pravdivá i $\varphi \Rightarrow \psi$ a protože je při e pravdivá i φ, je při e pravdivá i ψ, což jsme měli dokázat.

Tabulková metoda

Tabulková metoda představuje jednoduchý způsob, jak přehledně zapsat pravdivostní hodnoty dané formule při všech možných ohodnoceních. Jsou-li $p_1, \ldots, p_n$ všechny výrokové symboly, které se vyskytují ve formuli φ, budeme místo φ psát také $\varphi(p_1, \ldots, p_n)$.

Podstata tabulkové metody je následující. Pro zadanou formuli $\varphi(p_1, \ldots, p_n)$ vytvoříme tabulku. Tabulka 1.5 uazuje tabulku pro fromuli $(p \Rightarrow q) \wedge (p \Rightarrow r)$. Řádky tabulky odpovídají ohodnocením výrokových symbolů. Sloupce tabulky odpovídají symbolům $p_1, \ldots, p_n$ a formuli φ. Tabulka má tedy $n + 1$ sloupců, každý je v záhlaví označen příslušným výrazem, tj. buď p_i nebo φ. Obsah řádku, který odpovídá ohodnocení e je následující. Na místě odpovídajícímu sloupci tabulky s označením p_i je hodnota $e(p_i)$, tj. hodnota symbolu p_i při ohodnocení e. Na místě odpovídajícímu sloupci tabulky s označením φ je hodnota $||\varphi||_e$, tj.

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

Tabulka 3: Tabulka pro formule $\neg\neg\, p$, $(\neg\, q \Rightarrow \neg\, p)$ a q.

pravdivostní hodnota formule φ při ohodnocení e. Tabulka má tolik řádků, kolik je možností, jak ohodnotit symboly $p_1, \ldots, p_n$ hodnotami 0 a 1. Protože každému ze symbolů $p_1, \ldots, p_n$ můžeme přiřadit dvě možné hodnoty (tj. $e(p_i)$ může být 0 nebo 1), máme celkem 2^n možností (2 možnosti pro p_1 krát 2 možnosti pro p_1 krát $\cdots krt2monostipro\mathrm{p}_1$, tj. $2 \times \cdots \times 2 = 2^n$ možností). Tabulka má tedy 2^n řádků. To je potvrzeno v Tabulce 1.5. Zde máme tři výrokové symboly p, q, r, tabulka má tedy $2^3 = 8$ řádků. V každém řádku uvedeme příslušné ohodnocení symbolů $p_1, \ldots, p_n$ a hodnotu formule φ při tomto ohodnocení. Např. ve třetím řádku Tabulky 1.5 jsou uvedeny postupně hodnoty 0, 1, 0, 1, protože tento řádek odpovídá ohodnocení, které symbolům p, q a r přiřazuje postupně hodnoty 0, 1 a 0 a protože při tomto ohodnocení má formule $(p \Rightarrow q) \wedge (p \Rightarrow r)$ hodnotu 1. Je zvykem všechna možná ohodnocení symbolů uvádět přirozeně uspořádaná, tj. v prvních n sloupcích bude v prvním řádku $0 \ldots 0$ (n nul), ve druhém řádku pak $0 \ldots 01$ ($n-1$ nul a jedna jednička), atd. až v posledním řádku bude $1 \ldots 1$ (n jedniček). Tak je to také v Tabulce 1.5.

Poznámka 1.19. Řekli jsme, že v tabulce chceme zachytit hodnoty φ při všech možných ohodnoceních. Ohodnocení e je ale dáno tím, jaké hodnoty přiřazuje všem výrokovým symbolům, tedy nejen symbolům $p_1, \ldots, p_n$. My jsme ale při popisu tabulkové metody uvažovali jen hodnoty přiřazené symbolům $p_1, \ldots, p_n$. Dopustili jsme se tím jisté nepřesnosti, ale vcelku nepodstatné. Přesně řečeno se má situace takto. Pravdivostní hodnota $||\varphi||_e$ závisí jen na hodnotách $e(p_1), \ldots, e(p_n)$, tj. na ohodnocení výrokových symbolů $p_1, \ldots, p_n$, a nezávisí $e(p)$ pro $p \neq p_1, \ldots, p \neq p_n$, tj. ohodnocení výrokových symbolů jiných než $p_1, \ldots, p_n$. To je jasné proto, že $\varphi(p_1, \ldots, p_n)$ jiné výrokové symboly než $p_1, \ldots, p_n$ neobsahuje. Chceme-li v tabulce zachytit hodnoty φ při všech možných ohodnoceních, stačí tedy zachytit hodnoty φ pro všechna možná ohodnocení symbolů $p_1, \ldots, p_n$. Totiž, jak jsme řekli, hodnota $||\varphi||_e$ závisí jen na hodnotách $e(p_1), \ldots, e(p_n)$. Je-li e' jiné ohodnocení, které se s e shoduje v hodnotách přiřazených $p_1, \ldots, p_n$, tj. $e(p_1) = e'(p_1), \ldots, e(p_n) = e'(p_n)$, pak $||\varphi||_e = ||\varphi||_{e'}$, tj. hodnoty formule φ při ohodnoceních e a e' jsou stejné. V daném řádku uvedená hodnota formule $||||_e$ je tedy hodnotou formule φ při každém ohodnocení e, které symbolům $p_1, \ldots, p_n$ přiřazuje hodnoty uvedené v prvních n sloupcích tohoto řádku. Např. 3. řádek v Tabulce 1.5 udává hodnotu formule $(p \Rightarrow q) \wedge (p \Rightarrow r)$ při ohodnocení e, kde $e(p) = 0$, $e(q) = 1$, $e(r) = 0$, $e(p_1) = 0$, $e(p_2) = 0, \ldots$, ale i při ohodnocení e', $e'(p) = 0$, $e'(q) = 1$, $e'(r) = 0$, $e'(p_1) = 0$, $e'(p_2) = 0, \ldots$, a i při kazžém dalším ohodnocení e'', pro které je $e''(p) = 0$, $e''(q) = 1$, $e''(r) = 0$. Řádky tedy vlastně neodpovídají jednotlivým ohodnocením, ale celým třídám (skupinám) ohodnocení.

Tabulka vytvořená pro formuli φ umožňuje zjistit některé výše popsané vlastnosti formule φ: φ je tautologie, právě když ve sloupci odpovídajícím formuli φ jsou samé 1; φ je kontradikce, právě když ve sloupci odpovídajícím formuli φ jsou samé 0; φ je splnitelná, právě když ve sloupci odpovídajícím formuli φ je aspoň jedna 1.

Tabulkovou metodu můžeme jednoduše rozšířit pro více formulí. Předpokládejme, že máme formule $\varphi_1, \ldots, \varphi_m$, a že všechny proměnné vyskutující se v alespoň jedné z těchto formulí jsou právě $p_1, \ldots, p_n$. Odpovídající tabulka bude mít 2^n řádků a $n+m$ formulí, označených postupně $p_1, \ldots, p_n$ a $\varphi_1, \ldots, \varphi_m$. Do řádků píšeme ohodnocení e a hodnoty formulí $\varphi_1, \ldots, \varphi_m$ v těchto ohodnoceních: hodnoty $e(p_i)$ symbolů p_i v ohodnocení e píšeme do sloupců označených p_i. Příslušné hodnoty $||\varphi_{j}||_e$ formulí φ_j při ohodnocení e píšeme do sloupců označených φ_j. Příklad vidíme v Tabulce 1.5.

Rozšířenou tabulkovou meotdu můžeme použít ke zjištění, zda formule φ sémanticky plyne z formulí $\varphi_1, \ldots, \varphi_m$. Stačí vytvořit tabulku pro formule $\varphi_1, \ldots, \varphi_m$ a φ. Podle definice pak φ sémanticky plyne z $\varphi_1, \ldots, \varphi_m$, právě když v každém řádku, ve kterém mají formule $\varphi_1, \ldots, \varphi_m$ hodnotu 1, má také formule φ hodnotu 1. Z Tabulky 1.5 např. vidíme, že formule q vyplývá z formulí $\neg\neg\, p$ a $(\neg\, q \Rightarrow \neg\, p)$. Toitiž, jediný řádek, ve kterém mají obě formule $\neg\neg\, p$ a $(\neg\, q \Rightarrow \neg\, p)$ hodnotu 1, je čtvrtý řádek a v tomto řádku má

x_1	x_2	f
0	0	0
0	1	1
1	0	1
1	1	0

x_1	x_2	g
0	0	0
0	1	1
1	0	1
1	1	1

Tabulka 4: Tabulka booleovských funkcí dvou proměnných.

formule q také hodnotu 1. Naopak, formule $\neg\neg\, p$ nevyplývá z formulí $(\neg\, q \Rightarrow \neg\, p)$ a q, protože ve druhém řádku mají formule $(\neg\, q \Rightarrow \neg\, p)$ a q hodnotu 1, ale formule $\neg\neg\, p$ tam má hodnotu 0.

Průvodce studiem

Tabulková metoda slouží k vypsání (tabelaci) hodnot zadaných formulí $\varphi_1, \ldots, \varphi_m$ v tabulce. Tabulka má 2^n řádků a $n+m$ sloupců, kde n je počet všech výrokových symbolů, které se vyskytují ve formulích $\varphi_1, \ldots, \varphi_m$. Do řádků píšeme všechna možná ohodnocení těchto symbolů a hodnoty formulí $\varphi_1, \ldots, \varphi_m$.

Pomocí tabulkové metody můžeme zjistit, zda zadaná formule je tautologie, kontradikce, splnitelná, a také, zda zadaná formule sémanticky vyplývá z jiných zadaných formulí.

Booleovské funkce, úplná konjunktivní a disjunktivní normální forma

Booleovská funkce s n argumenty (někdy n-ární booleovská funkce) je libovolné zobrazení, které každé uspořádané n-tici hodnot 0 nebo 1 přiřadí hodnotu 0 nebo 1. Každou booleovskou funkci f s n argumenty lze zapsat v tabulce podobným způsobem jako jsme viděli u tabulkové metody. Předpokládejme, že argumenty funkce f označíme $x_1, \ldots, x_n$, pak píšeme také $f(x_1, \ldots, x_n)$. Odpovídající tabulka má 2^n řádků a $n+1$ sloupců. Sloupce označíme symboly $x_1, \ldots, x_n$ a f. Do každého řádku napíšeme hodnoty proměnných $x_1, \ldots, x_n$ a do posledního sloupce pak hodnotu, kterou funkce f nabývá při těchto hodnotách proměnných. Příkladem jsou booleovská funkce f a g dvou proměnných, které jsou zapsané v Tabulce 1.5. Funkce f např. přiřazuje dvojici hodnot 0 a 1 hodnotu 1, tj. $f(0,1) = 1$, dále $f(0,0) = 0$, $f(1,0) = 1$, $f(1,1) = 1$. Pro funkci g je $g(0,0) = 0$, $g(0,1) = 1$, $g(1,0) = 1$, $g(1,1) = 1$.

Všimněme si, že výše uvedená funkce g je shodná s pravdivostní funkcí $\vee$ spojky disjunkce. Pravdivostní funkce každé ze spojek, se kterými jsme se setkali, jsou booleovské funkce. Pravdivostní funkce spojek $\mathbb{\wedge}$, $\mathbb{\vee}$, $\Rightarrow$ a $\Leftrightarrow$, jsou funkce 2 argumentů, pravdivostní funkce spojky $\neg$ je booleovská funkce jednoho argumentu. Pravdivostní funkce logických spojek jsou vlastně booleovské funkce. Funkce f z Tabulky 1.5 ukazuje, že existují i jiné booleovské funkce než pravdivostní funkce $\wedge$, $\vee$, $\rightarrow$ a $\leftrightarrow$ logických spojek $\mathbb{\wedge}$, $\mathbb{\vee}$, $\Rightarrow$ a $\Leftrightarrow$. Každou booleovskou funkci 2 proměnných můžeme považovat za pravdivostní funkci logické spojky se dvěma argumenty. Z tohoto pohledu jsou tedy spojky $\mathbb{\wedge}$, $\mathbb{\vee}$, $\Rightarrow$ a $\Leftrightarrow$ jen některé z logických spojek se dvěma argumety. Skutečně, např. pravdivostní funkce spojky "buď ..., anebo ..." je právě funkce f z Tabulky 1.5 („Buď V_1, nebo V_2" je pravdivý výrok, právě když je pravdivý právě jeden z výroků V_1, V_2). Kolik je ale booleovských funkcí s n argumenty, tj. kolik je různých logických spojek s n argumenty?

Věta 1.20. *Existuje právě $2^{(2^n)}$ booleovských funkcí s n argumenty.*

Důkaz. Funkcí je tolik, kolika způsoby lze vyplnit příslušnou tabulku. Protože funkce mají n argumentů, má tabulka 2^n řádků. V každém řádku je jedno volné místo pro hodnotu funkce, a tu můžeme vyplnit libovolným způsobem (napsat tam 0 nebo 1). Protože volných míst je 2^n, lze je hodnotami 0 nebo 1 vyplnit $2^{(2^n)}$ způsoby. □

Příklad 1.21. Tabulka Přitom f_3 je pravdivostní funkce spojky negace.

Je jasné, že každá formule φ obsahující výrokové symboly $p_1, \ldots, p_n$ indukuje booleovskou funkci φ n argumentů. Je to právě funkce, jejíž tabulku získáme vytvořením tabulky pro formuli φ. Např. pro

x_1	f_1
0	0
1	0

x_1	f_2
0	0
1	1

x_1	f_3
0	1
1	0

x_1	f_3
0	1
1	1

Tabulka 5: Všechny booleovské funkce jedné proměnné.

funkci $f_{(p\Rightarrow q)\wedge(q\Rightarrow p)}$ indukovanou formulí $(p \Rightarrow q) \wedge (q \Rightarrow p)$ máme $f_{(p\Rightarrow q)\wedge(q\Rightarrow p)}(0,0,0) = 1, \ldots,$ $f_{(p\Rightarrow q)\wedge(q\Rightarrow p)}(1,0,1) = 1, \ldots, f_{(p\Rightarrow q)\wedge(q\Rightarrow p)}(1,1,1) = 1$, viz Tabulka 1.5.

Zajímavé ale je, že platí také opačné tvrzení. Ke každé booleovské funkci f s n argumenty existuje formule φ_f taková, že tato formule indukuje právě funkci f. Platí dokonce, že formuli φ_f můžeme vzít takovou, že obsahuje pouze spojky $\neg$, $\wedge$ a $\vee$. Postup, jak takovou formuli získat, si nyní podrobně popíšeme. Zaveďme nejprve následující pojmy.

Nechť V je množina výrokových symbolů. Pak

- *literál* nad V je libovolný výrokový symbol z V nebo jeho negace,
- *úplná elementární konjunkce* nad V je libovolná konjunkce literálů, ve které se každý výrokový symbol z V vyskytuje právě v jednom literálu;
- *úplná elementární disjunkce* nad V je libovolná disjunkce literálů, ve které se každý výrokový symbol z V vyskytuje právě v jednom literálu;
- *úplná konjunktivní normální forma* nad V je konjunkce úplných elementárních disjunkcí nad V.
- *úplná disjunktivní normální forma* nad V je disjunkce úplných elementárních konjunkcí nad V.

Příklad 1.22. Pro $V = \{p, q, r\}$

- literály: $p, q, r, \neg p, \neg q, \neg r$, (ne $\neg\neg p$)
- ÚEK: $p \wedge q \wedge r$, $\neg p \wedge q \wedge \neg r$, (ne $p \wedge r$)
- ÚED: $p \vee \neg q \vee r$
- ÚDNF $(p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r)$
- ÚKNF $(p \vee q \vee \neg r) \vee (p \vee \neg q \vee \neg r)$

Ke každé formuli výrokové logiky, která není kontradikcí (tautologií) existuje s ní (sémanticky) ekvivalentní formule, která je ve tvaru úplné konjunktivní normální formy (úplné disjunktivní normální formy).

Pro ÚDNF:

-pro $\varphi(p_1, \ldots, p_n)$ uvaž. tabulku pr. hodnot

-pro řádky s hodnotou 1 sestroj ÚEK z p_i (pro 1) a $\neg\, p_i$ (pro 0)

-výsledná ÚDNF je disjunkcí takových ÚEK

Pro ÚKNF duálně: (řádky s nulou; k nim ÚED z p_i (pro 1) a $\neg\, p_i$ (pro 0); ÚKNF je konjunkcí takových ÚED)

ÚDNF, ÚKNF: příklad

Sestrojte ÚDNF a ÚKNF k $(p \Rightarrow q) \wedge (p \Rightarrow r)$.

p	q	r	$(p \Rightarrow q) \wedge (p \Rightarrow r)$	ÚEK	ÚED
0	0	0	1	$\neg\, p \wedge \neg\, q \wedge \neg\, r$	
0	0	1	1	$\neg\, p \wedge \neg\, q \wedge r$	
0	1	0	1	$\neg\, p \wedge q \wedge \neg\, r$	
0	1	1	1	$\neg\, p \wedge q \wedge r$	
1	0	0	0		$\neg\, p \vee q \vee r$
1	0	1	0		$\neg\, p \vee q \vee \neg\, r$
1	1	0	0		$\neg\, p \vee \neg\, q \vee r$
1	1	1	1	$p \wedge q \wedge r$	

Tedy: ÚDNF je $(\neg\, p \wedge \neg\, q \wedge \neg\, r) \vee (\neg\, p \wedge \neg\, q \wedge r) \vee (\neg\, p \wedge q \wedge \neg\, r) \vee (\neg\, p \wedge q \wedge r) \vee (p \wedge q \wedge r)$

ÚKNF je: $(\neg\, p \vee q \vee r) \wedge (\neg\, p \vee q \vee \neg\, r) \wedge (\neg\, p \vee \neg\, q \vee r)$

Ke každé formuli výrokové logiky existuje s ní (sémanticky) ekvivalentní formule, která je ve tvaru úplné konjunktivní normální formy (úplné disjunktivní normální formy); viz přednášky (literál je výrokový symbol nebo jeho negace; úplná elementární konjunkce (disjunkce) na danou množinou V výrokových symbolů je konjunkce (disjunkce) literálů, ve které se každý výrokový symbol z V vyskytuje právě v jednom literálu; úplná disjunktivní (konjunktivní) normální forma (nad V) je disjunkce (konjunkce) úplných elementárních konjunkcí (disjunkcí) (nad V); konstrukce ÚDNF dané formule φ: z tabulky pravdivostních hodnot φ se vyberou řádky, pro které je formule pravdivá a pro každý takový řádek se vytvoří úplná elementární konjunkce takto: pro každý výrokový symbol p formule φ se vytvoří odpovídající literál, přitom má-li p v ohodnocení příslušném tomuto řádku hodnotu 1, je tím literálem přímo p, má-li hodnotu 0, je tím literálem $\neg\, p$; takto vybrané literály se spojí konjunkcí; takto vytvořené konjunkce se spojí disjunkcí — zdůvodněte, proč takto skutečné vznikne formule ekvivalentní původní formuli φ; duálně se vytvoří úplná disjunktivní normální forma).

Vyjadřování spojek jinými spojkami

Úplné systémy spojek VL

Booleovská funkce (n-ární) je libovolné zobrazení $f : \{0,1\}^n \to \{0,1\}$.

Každému symbolu logické spojky odpovídá booleovská funkce, např. $\Rightarrow$ odpovídá $\to$.

Množina $\{f_1, \ldots, f_k\}$ booleovských funkcí je funkčně úplná, pokud každou $f : \{0,1\}^n \to \{0,1\}$ lze vyjádřit jako složení některých funkcí z $\{f_1, \ldots, f_k\}$.

Množina výrokových spojek je úplná, jestliže je úplná množina jim odpovídajících booleovských funkcí.

$\{\neg, \vee, \wedge\}$ je funkčně úplná.

Plyne z věty o ÚDNF.

Je-li možné každou z $\{f_1, \ldots, f_k\}$ vyjádřit jako složení některých z $\{g_1, \ldots, g_l\}$, pak je-li $\{f_1, \ldots, f_k\}$ úplná, je i $\{g_1, \ldots, g_l\}$ úplná.

Snadný.

Zaveďme operace $\mathrm{sh}(a, b) = \neg(a \wedge b)$ (Shefferova); $\mathrm{pe}(a, b) = \neg a \wedge \neg b)$ (Peirceova nebo Nicodova . . . "ani . . . , ani . . . ");

$\{\neg, \wedge\}$, $\{\neg, \vee\}$, $\{\neg, \rightarrow\}$, $\{\mathrm{sh}\}$, $\{\mathrm{pe}\}$ jsou úplné systémy.

Plyne z úplnosti $\{\neg, \vee, \wedge\}$, uvedeného Lemma a

$$\begin{aligned} a \vee b &= \neg(\neg a \wedge \neg b) \\ a \wedge b &= \neg(\neg a \vee \neg b) \\ a \wedge b &= \neg(a \vee \neg b) \\ \neg a &= \mathrm{sh}(a, a) \\ (a \wedge b) &= \mathrm{sh}(\mathrm{sh}(a, b), \mathrm{sh}(a, b)) \\ \neg a &= \mathrm{pe}(a, a) \\ (a \vee b) &= \mathrm{pe}(\mathrm{pe}(a, b), \mathrm{pe}(a, b)) \end{aligned}$$

Úplnost $\{f_1, \ldots, f_k\}$ . . . k realizaci logických obvodů vystačím s hradly realizující $\{f_1, \ldots, f_k\}$.

Kolik existuje n-árních Booleovských funkcí?

Jsou systémy $\{\leftrightarrow\}$ a $\{\neg, \leftrightarrow\}$ úplné?

Shrnutí

Logika je věda o správném usuzování. V logice jde o formu usuzování, nikoli o obsah.

Pojmy k zapamatování

- logika,
- logická spojka,
- výrok,
- pravdivostní hodnota výroku,
- symbol logické spojky a pravdivostní funkce logické spojky,
- kvantifikátor.

Kontrolní otázky

1. *Jaké znáte logické spojky?*
2. *Co to je klasická a nelasická logika?*
3. *Jaký je vztah mezi obecným a existenčním kvantifikátorem?*
4. *Co to je formule výrokové logiky?*
5. *Vysvětlete, co to je tabulková metoda a k čemu slouží.*
6. *Vysvětlete pojem sémantické vyplývání.*

Cvičení

1. Určete pravdivostní hodnotu výroku "Jestliže Čína je nejlidnatější stát světa, pak Petr je synem Marie.". Přitom "Petr je synem Marie." je pravdivý výrok.
2. Je dán výrok "Pro každé x platí, že jestliže $2x + 1$ je sudé, pak x je násobkem 5". Přitom D_x je množina všech přirozených čísel. Je daný výrok pravdivý?
3. Jsou dány výroky "Pro každé x existuje y tak, že platí $x \leq y$" a "Existuje y tak, že pro každé x platí $x \leq y$". Oborem hodnot proměnných x i y je množina všech celých čísel, tj. $D_x = D_y = \{0, 1, -1, 2, -2, 3, -3, \dots\}$. Určete pravdivostní hodnoty daných výroků.
4. U každé z následujících formulí zjistěte, zda je tautologie, kontradikce, splnitelná.

$\varphi \vee \neg\, \varphi$	zákon vyloučeného třetího
$\neg\, (\varphi \wedge \neg\, \varphi)$	zákon sporu
$\neg\, (\varphi \wedge \varphi) \Leftrightarrow (\neg\, \varphi \vee \neg\, \varphi)$	De Morganův zákon
$\neg\, (\varphi \vee \varphi) \Leftrightarrow (\neg\, \varphi \wedge \neg\, \varphi)$	De Morganův zákon
$(\varphi \Rightarrow \psi) \Leftrightarrow (\neg\, \psi \Rightarrow \neg\, \varphi)$	zákon kontrapozice

5. Zjistěte, zda formule ψ sémanticky plyne z φ: (a) φ je $(p \wedge q) \vee r$, ψ je $p \Rightarrow (q \vee r)$; (b) φ je $(p \wedge q) \vee r$, ψ je $p \Rightarrow (q \vee \neg\, r)$.
6. Přesvědčte se, že je-li $\psi \models \varphi$ a $\varphi \models \chi$, pak $\psi \models \chi$.

Úkoly k textu

1. Vypište všechny binární logické spojky.
2. Uveďte příklady výrokových forem $V(x, y)$ tak, že $(\forall x)(\exists y)(V(x, y))$ je pravdivý výrok a $(\exists y)(\forall x)(V(x, y))$ je nepravdivý výrok. Lze najít příklad formy $V(x, y)$ tak, aby $(\forall x)(\exists y)(V(x, y))$ byl nepravdivý výrok a aby $(\exists y)(\forall x)(V(x, y))$ byl pravdivý výrok?
3. Ukažte, že je-li $V(x)$ výroková forma, pak $||(\forall x)(V(x))|| = \min_{x \in D_x} ||V(m)||$ a $||(\exists x)(V(x))|| = \max_{x \in D_x} ||V(m)||$.
4. Ukažte, že je-li $V(x)$ výroková forma, pak $||(\forall x)(V(x))|| = || \neg\, (\exists x)(\neg\, V(x))||$ a $||(\exists x)(V(x))|| = || \neg\, (\forall x)(\neg\, V(x))||$.
5. Někdy se uvádí následující varianta paradoxu lháře: Kréťan říká „Všichni Kréťani lžou." Je to paradox, tj. vede tato situace ke sporu podobně jako vede ke sporu paradox lháře?
6. Zdůvodněte podle definice, že formule φ je tautologie, právě když φ sémanticky vyplývá z prázdné množiny formulí.

Řešení

1. Výrok je pravdivý.
2. Výrok je pravdivý. Nápověda: Pro každé přirozené číslo m je $2m + 1$ liché, tedy "Jestliže $2m + 1$ je sudé, pak m je násobkem 5" je pravdivý výrok, viz tabulka pravdivostní funkce spojky implikace.
3. Výrok "Pro každé x existuje y tak, že platí $x \leq y$." je pravdivý. Výrok "Existuje y tak, že pro každé x platí $x \leq y$." je nepravdivý.
4. DOPLNIT ODPOVEDI
5. Zjistěte, zda formule ψ sémanticky plyne z φ: (a) φ je $(p \wedge q) \vee r$, ψ je $p \Rightarrow (q \vee r)$; (b) φ je $(p \wedge q) \vee r$, ψ je $p \Rightarrow (q \vee \neg\, r)$.
6. Jednoduchou úvahou přímo z definice: Nechť e je libovolné ohodnocení, při kterém je ψ pravdivá. Protože předpokládáme $\psi \models \varphi$, je při ohodnocení e pravdivá také φ, a tedy protože předpokládáme $\varphi \models \chi$, je při e pravdivá i χ, což jsme měli dokázat.

2 Množiny, relace, funkce

Studijní cíle: Po prostudování kapitol 2.1 a 2.2 by student měl rozumět pojmu množina. Měl by znát základní operace a vztahy definované nad množinami. Student by měl tyto pojmy znát aktivně, měl by umět samostatně dokázat jednoduchá tvrzení, hledat příklady a protipříklady.

Klíčová slova: množina, prvek, podmnožina, průnik, sjednocení, rozdíl.

Potřebý čas: 180 minut.

2.1 Co a k čemu jsou množiny, relace a funkce

Množiny, relace a funkce jsou matematickými protějšky jevů, se kterými se setkáváme v každodenním životě. Množina je protějškem *souboru* (či *seskupení*). Relace je protějškem *vztahu*. Funkce je protějškem *přiřazení*. Pojmy množina, relace a funkce patří k základním stavebním prvkům diskrétní matematiky a matematiky vůbec. Umožňují přesné, srozumitelné a jednoduché vyjadřování. Používají se v matematice (bez jejich znalosti nemůžeme číst žádný matematický text) a v řadě aplikovaných oborů včetně informatiky (funkcionální programování, relační databáze, informační systémy, znalostní inženýrství a další).

Množina, relace a funkce jsou základní pojmy matematiky. V informatice se bez nich neobejdeme.

Průvodce studiem

S pojmy množina, relace a funkce se podrobně seznamte. Jsou to jednoduché pojmy. Byly zavedeny, abychom mohli přesně mluvit o souborech, seskupeních, systémech, vztazích, přiřazeních apod. Nenechte se svést tím, že přeci víte, co je to seskupení nebo vztah. Když formalismus množin, relací a funkcí dobře zvládnete, ušetříte si spoustu práce v dalším studiu. Navíc budete umět praktické problémy dobře „uchopit“ a popsat. Když naopak formalismus množin, relací a funkcí nezvládnete, budete s tím i v dalších oblastech neustále bojovat.

2.2 Množiny

2.2.1 Pojem množiny

Pojem množina je matematickým protějškem běžně používaných pojmů *soubor*, *seskupení*, apod. *Množina* je objekt, který se skládá z jiných objektů, tzv. *prvků* té množiny. Tak například množina (označme ji S) všech sudých čísel, které jsou větší než 1 a menší než 9, se skládá z čísel 2, 4, 6, 8. Tato čísla jsou tedy prvky množiny S. Fakt, že S se skládá právě z prvků 2, 4, 6, 8 zapisujeme

Množina je objekt, který se skládá z jiných objektů, tzv. prvků množiny.

$$S = \{2, 4, 6, 8\}.$$

Množiny zpravidla označujeme velkými písmeny ($A, B, \ldots, Z$), jejich prvky pak malými písmeny ($a, b, \ldots, z$). Fakt, že x je prvkem množiny A označujeme

$$x \in A$$

a říkáme také, že x patří do A (popř. x je v A, A obsahuje x apod.). Není-li x prvkem A, píšeme $x \notin A$.

Daný objekt do dané množiny buď patří, nebo nepatří. Množina je jednoznačně dána svými prvky, tj. tím, které prvky do ní patří a které ne. Nemá tedy smysl hovořit o pořadí prvků v množině (tj. pojmy „první prvek množiny“, „druhý prvek množiny“ atd. nemají smysl). Nemá také smysl uvažovat, kolikrát je daný prvek v dané množině (tj. říci „prvek x je v dané množině A třikrát“).

Množina je jednoznačně dána tím, jaké prvky obsahuje.

Speciální množinou je tzv. *prázdná množina*. Označuje se $\emptyset$. Tato množina neobsahuje žádný prvek, tj. pro každý prvek x platí $x \notin \emptyset$.

Příklad 2.1. Význačné množiny čísel mají svá speciální označení.

- $\mathbb{N}$ označuje množinu všech *přirozených čísel*. $\mathbb{N}$ tedy sestává z prvků $1, 2, 3, 4, 5, \ldots$.
- $\mathbb{Z}$ označuje množinu všech *celých čísel*. $\mathbb{Z}$ tedy sestává z prvků $0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots$.
- $\mathbb{Q}$ označuje množinu všech *racionálních čísel*. $\mathbb{Q}$ tedy sestává z celočíselných zlomků, tj. z čísel $\frac{m}{n}$, kde $m \in \mathbb{Z}$, $n \in \mathbb{N}$.
- $\mathbb{R}$ označuje množinu všech *reálných čísel*. Ta obsahuje i iracionální čísla, např. $\sqrt{2}, \pi$ apod.

Množiny se dělí na konečné a nekonečné. Množina A se nazývá *konečná*, právě když existuje přirozené číslo n tak, že prvky této množiny lze jednoznačně očíslovat čísly $1, 2, \ldots n$. Číslo n se přitom nazývá počet prvků množiny A a značíme ho $|A|$, tj. $|A| = n$. Říkáme také, že A má n prvků. Např. množina $\{2, 4, 6, 8\}$ je konečná. Zvolíme-li totiž $n = 4$, můžeme její prvky očíslovat např. následovně: prvku 2 přiřadíme číslo 1, prvku 4 číslo 2, prvku 6 číslo 3, prvku 8 číslo 4. Máme tedy $|\{2, 4, 6, 8\}| = 4$, tj. počet prvků množiny $\{2, 4, 6, 8\}$ je 4. Množina A se nazývá *nekonečná*, není-li konečná. Pak píšeme $|A| = \infty$ a říkáme, že A má nekonečně mnoho prvků. Např. množina $\mathbb{N}$ všech přirozených čísel je nekonečná.

Prvky konečných množin lze očíslovat čísly 1, . . . , n. Pokud to nelze, je množina nekonečná.

2.2.2 Zápisování množin

Množiny zapisujeme dvěma základními způsoby. Prvním je zápis tzv. *výčtem prvků*. Množina sestávající právě z prvků $a_1, \ldots, a_n$ se označuje $\{a_1, \ldots, a_n\}$. Příkladem je výše uvedený zápis $\{2, 4, 6, 8\}$. Zápis výčtem prvků můžeme použít u konečných množin. Druhým je zápis udáním tzv. *charakteristické vlastnosti*. Množina sestávající právě z prvků, které splňují vlastnost $\varphi(x)$, se označuje $\{x \mid \varphi(x)\}$.

$\{a_1, \ldots, a_n\}$ je množina, která obsahuje právě prvky $a_1, \ldots, a_n$.

Vlastnost $\varphi(x)$ může být popsaná třeba i v přirozeném jazyce, ale musí mít jednoznačný smysl. Např. je-li $\varphi(x)$ vlastnost „x je sudé přirozené číslo větší než 1 a menší než 9“, můžeme uvažovat množinu označenou $\{x \mid \varphi(x)\}$. Ta je shodná s množinou označenou $\{2, 4, 6, 8\}$.

$\{x \mid \varphi(x)\}$ je množina, která obsahuje právě prvky x splňující vlastnost $\varphi(x)$.

Místo „množina označená zápisem $\{\ldots\}$“ budeme říkat jen „množina $\{\ldots\}$“. Např. říkáme „množina $\{a, b, c\}$ má tři prvky“, „uvažujme množinu $\{x \mid x$ je sudé celé číslo$\}$“ apod.

Někdy se používá i pro zápis nekonečných množin způsob, který je podobný zápisu výčtem. Například množinu všech kladných sudých čísel zapíšeme $\{2, 4, 6, 8, \ldots\}$. Obecně tedy můžeme použít zápis $\{a_1, a_2, a_3, a_4, \ldots\}$, pokud je z prvků a_1, a_2, a_3, a_4 zřemá vlastnost charakterizující prvky popisované množiny. Poznamenejme také, že prázdná množina se někdy zapisuje $\{\}$.

Poznámka 2.2. Zápis výčtem prvků svádí k tomu mluvit o prvním prvku množiny, druhém prvku množiny, atd. Např. u množiny $\{2, 4, 6, 8\}$ máme tendenci říci, že 2 je prvním prvkem, 4 druhým prvkem atd. My však víme, že výrazy „první prvek množiny“, „druhý prvek množiny“ atd. nemají smysl. Množina je totiž dána jen tím, jaké prvky obsahuje, ne jejich pořadím. Při zápisu výčtem se ale pořadí objevuje. Správně bychom měli říci, že $\{2, 4, 6, 8\}$ označuje množinu, v jejímž zápise výčtem, který jsme použili, je prvek 2 na prvním místě, prvek 4 na druhém místě atd. Stejnou množinu můžeme zapsat výčtem a např. $\{4, 6, 2, 8\}$. V tomto zápise je prvek 2 na třetím místě.

Zápis výčtem svádí dále k tomu mluvit o tom, kolikrát se prvek v dané množině vyskytuje. Z technickým důvodů je výhodné připustit, aby se prvky v zápisu výčtem opakovaly. Můžeme např. napsat $\{2, 4, 6, 8, 2, 2, 4\}$. Takový zápis označuje stejnou množinu jako $\{2, 4, 6, 8\}$. Stejnou množinu označuje i $\{6, 6, 6, 2, 4, 8\}$. Záleží tedy jen na tom, které prvky se v zápise vyskytují, nezáleží na počtu jejich výskytu. Nelze tedy např. říci, že množina $\{2, 4, 6, 8, 2, 2, 4\}$ obsahuje tři prvky 2. Můžeme jen říci, že v zápise $\{2, 4, 6, 8, 2, 2, 4\}$ se prvek 2 vyskytuje třikrát.

Poznámka 2.3. (1) Zápis $\{x \in A \mid \varphi(x)\}$ označuje množinu $\{x \mid x \in A$ a $\varphi(x)\}$. Je to tedy zápis pomocí charakteristické vlastnosti. Označíme-li totiž $\psi(x)$ vlastnost, kterou prvek x splňuje, právě když patří do A a splňuje $\varphi(x)$, pak množina $\{x \in A \mid \varphi(x)\}$ je rovna množině $\{x \mid \psi(x)\}$. Např. množina $\{x \in \mathbb{Z} \mid x \leq 2\}$ je množina $\{x \mid x \in \mathbb{Z}$ a $x \leq 2\}$, tj. množina všech celých čísel, která jsou nejvýše rovna 2.

(2) Často se také používá zápis $\{a_i \mid i \in I\}$. Přitom I je nějaká množina (říká se jí *indexová*) a pro každý (index) $i \in I$ je a_i nějaký prvek. Pak $\{a_i \mid i \in I\}$ je množina

$$\{x \mid \text{existuje } i \in I \text{ tak, že } x = a_i\}.$$

$\{a_i \mid i \in I\}$ je tedy vlastně zápis pomocí charakteristické vlastnosti, neboť označuje množinu $\{x \mid \varphi(x)\}$, kde $\varphi(x)$ je „existuje $i \in I$, tak, že $x = a_i$“. Je-li každý prvek a_i množinou, nazývá se $\{a_i \mid i \in I\}$ indexovaný systém množin.

(3) Při zápise pomocí charakteristické vlastnosti se při popisu vlastnosti $\varphi(x)$ často používají obraty „pro každé y platí, že ...“ a „existuje y tak, že platí ...“. Jak je běžné, budeme tyto obraty zkráceně zapisovat (po řadě) pomocí „$\forall y \ldots$“ a „$\exists y \ldots$“ s případnými závorkami, které zajistí jednoznačný způsob čtení, popř. větší srozumitelnost. „$\forall y \in Y \ldots$“ a „$\exists y \in Y \ldots$“ znamenají „pro každé y z množiny Y platí, že ...“ a „existuje y z množiny Y tak, že platí ...“. Např. množina $\{x \mid \exists y \in \mathbb{N} : x = y^2\}$ je množina prvků x takových, že existuje přirozené číslo y tak, že $x = y^2$. Je to tedy množina všech druhých mocnin přirozených čísel. V Kapitole **??** se s kvantifikátory a jejich vlastnostmi seznámíme podrobněji.

Příklad 2.4. Podívejte se na následující množiny a jejich zápisy.

- $\{k \mid \exists n \in \mathbb{N} : k = 2^n\}$ označuje množinu všech kladných mocnin čísla 2. Stejnou množinu označuje $\{2, 4, 8, 16, \ldots\}$.
- $\{k \in \mathbb{N} \mid k \neq 1$ a jestliže $\exists m, n \in \mathbb{N} : m \cdot n = k,$ pak $m = 1$ nebo $n = 1\}$ označuje množinu všech prvočísel.
- $\{\{a, b\}, \{a\}, \{1, 2, 3, \{a, b\}\}\}$ je množina, která má tři prvky. Tyto prvky samy, tj. $\{a, b\}$, $\{a\}$, a $\{1, 2, 3, \{a, b\}\}$, jsou opět množiny. $\{a, b\}$ má dva prvky (a a b), $\{a\}$ má jeden prvek (a), $\{1, 2, 3, \{a, b\}\}$ má tři prvky (jsou to 1, 2, 3 a $\{a, b\}$). Vidíme tedy, že množina může obsahovat prvek, který je sám množinou. Tento prvek-množina sám může obsahovat prvky, které jsou množinami atd.
- $\{\emptyset\}$ je jednoprvková množina. Jejím jediným prvkem je $\emptyset$ (prázdná množina). Uvědomte si, že $\{\emptyset\}$ a $\emptyset$ jsou různé množiny ($\{\emptyset\}$ obsahuje jeden prvek, $\emptyset$ neobsahuje žádný). $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$ je čtyřprvková množina. Její prvky jsou $\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}\}$.
- Nechť $a_1 = p$, $a_2 = q$, $a_3 = r$, $a_4 = x$, $a_5 = y$, $a_6 = z$, $a_7 = 1$, $a_8 = r$, $I = \{1, 2, 3, 4\}$, $J = \{1, 2, 3, 7, 8\}$. Pak $\{a_i \mid i \in I\}$ je množina $\{p, q, r, x\}$, $\{a_i \mid i \in J\}$ je množina $\{p, q, r, 1\}$.
- $\{2^i \mid i \in \mathbb{N}\}$ je zápis typu $\{a_i \mid i \in I\}$ (máme $a_i = 2^i$, $I = \mathbb{N}$). Je to množina všech kladných mocnin čísla 2.

Pouhý množinový zápis umožňuje přehledně vyjádřit strukturu, kterou chceme zachytit.

Množina je pojem, který intuitivně používáme v běžném životě, chceme-li označit několik objektů najednou („dát je do jednoho pytle“). Např. řekneme-li „ekonomické oddělení“, myslíme tím vlastně množinu zaměstnanců ekonomického odělení. Množinový zápis také umožňuje jednoduše vyjádřit hierarchickou strukturu. Předpokládejme pro jednoduchost, že v nemocnici pracuje ředitel (R), tři údržbáři (U_1, U_2, U_3), na oddělení chirurgie dva lékaři (C_1, C_2) a tři sestry (CS_1, CS_2, CS_3), na anesteziologicko-resuscitačním oddělení dva lékaři (A_1, A_2) a dvě sestry (AS_1, AS_2), na oddělení interním tří lékaři (I_1, I_2, I_3) a čtyři sestry (IS_1, IS_2, IS_3, IS_4). Pak strukturu zaměstnanců nemocnice popisuje jistým způsobem např. množina

$$\{\{R\}, \{U_1, U_2, U_3\}, \\ \{\{C_1, C_2, CS_1, CS_2, CS_3\}, \{A_1, A_2, AS_1, AS_2\}, \{I_1, I_2, I_3, IS_1, IS_2, IS_3, IS_4\}\}\}.$$

Při tomto pohledu se díváme takto: Zaměstnanci nemocnice jsou rozděleni do třech skupin, a to $\{R\}$ (vedení), $\{U_1, U_2, U_3\}$ (technický personál), $\{\{C_1, C_2, CS_1, CS_2, CS_3\}, \{A_1, A_2, AS_1, AS_2\}, \{I_1, I_2, I_3, IS_1, IS_2, IS_3, IS_4\}$ (zdravotnický personál). Zdravotnický personál se dále dělí na $\{C_1, C_2, CS_1, CS_2, CS_3\}$ (chirurgické oddělení), $\{A_1, A_2, AS_1, AS_2\}$ (anesteziologicko-resuscitační oddělení) a $\{I_1, I_2, I_3, IS_1, IS_2, IS_3, IS_4\}$ (interní oddělení). Jiným způsobem (vedení, technický personál, lékaři, sestry) popisuje strukturu zaměstnanců množina

$$\{\{R\}, \{U_1, U_2, U_3\}, \\ \{C_1, C_2, A_1, A_2, I_1, I_2, I_3\}, \{CS_1, CS_2, CS_3, AS_1, AS_2, IS_1, IS_2, IS_3, IS_4\}\}.$$

Pokud mluvíme o množině, jejíž prvky jsou opět množiny, říká se někdy místo „množina množin“ spíše „systém množin“ nebo „soubor množin“. Důvody k tomu jsou však jen estetické (zvukomalebné, „množina množin“ nezní dobře).

Poznámka 2.5. (1) Ne každou slovně popsanou vlastnost lze použít k zápisu množiny. Uvažujme např. zápis $\{x \mid x$ je číslo udávající ve stupních Celsia vysokou letní teplotu v Česku$\}$. Problém je v tom, že pojem „vysoká letní teplota v Česku“ není vymezen tak, že by pro každá teplota buď byla nebo nebyla vysoká. Např. by teploty 30 stupňů a více byly vysoké a teploty menší než 30 stupňů vysoké nebyly. Pojem „vysoká letní teplota v Česku“ je totiž vágní, určité teploty mu vyhovují lépe, určité hůře. Vágností se zabývá tzv. fuzzy logika a fuzzy množiny. Fuzzy množina se od (klasické, tj. „nefuzzy“) množiny liší v zásadě v tom, že objekt do fuzzy množiny může patřit v určitém stupni, např. 0 (vůbec nepatří), 0.2 (patří jen trochu), . . . , 1 (úplně patří). Klasické množiny lze chápat jako hraniční přípdad fuzzy množin, kdy používáme pouze stupně 0 a 1. Zájemce odkazujeme např. na [KlYu95].

Je-li vlastnost $\varphi(x)$ popsaná slovně, nemusí být určitá, a pak $\{x\varphi(x)\}$ nepopisuje množinu.

(2) Přístup k množinám, který zde představujeme, je tzv. naivní (popř. intuitivní). Může však vést k zvláštním situacím, tzv. paradoxům. Začátkem 20. stol. na ně upozornil Bertrand Russel. Aby paradoxy odstranil, navrhl tzv. teorii typů a na ní vybudobal přístup k množinám, ve kterém se paradoxy neobjevují. Jiný, později mnohem rozšířenější přístup k množinám, ve kterém se paradoxy nevyskytují, nabízí tzv. axiomatická teorie množin. Pro naše účely a i v řadě jiných situací však postačuje naivní přístup. Protože je také mnohem jednodušší, zůstaneme u něj.

(3) Jedním z nejznámějších paradoxů naivního přístupu k množinám je tzv. Russellův paradox. Vypadá takto: Prvky množin mohou být opět množiny. Dále lze jistě uvažovat vlastnost „$x \notin x$“ a množiny objektů, které ji splňují. Označme ji N a nazvěme ji množinou všech normálních množin, tj. $x \in N$, právě když $x \notin x$. Poznamenejme na okraj, že všechny množiny, které jsme zatím viděli, byly normální. Protože N sama o sobě množina, můžeme se zeptat, zda platí $N \in N$, tj. zda N sama je normální. Je jasné, že musí být buď (a) $N \in N$, nebo (b) $N \notin N$. Zkusme ty možnosti rozebrat: (a) Když $N \in N$, pak N splňuje vlastnost prvků množiny N, tedy splňuje $x \notin x$, tedy $N \notin N$. Naopak, když (b) $N \notin N$, pak protože N splňuje vlastnost $x \notin x$, je dle definice normální a tedy patří do množiny všech normálních množin, tedy patří do N, tedy $N \in N$. Vidíme tedy, že z $N \in N$ plyne $N \notin N$ a z $N \notin N$ plyne $N \in N$, tedy $N \in N$ platí, právě když $N \notin N$. To je spor. Z přirozených předpokladů jsme přirozenými úvahami došli ke sporu, odtud název paradox. Russellův paradox má řadu populárních podob. Jednou z nich je tzv. paradox holiče: Ve městě je holič, který holí právě ty lidi, kteří neholí sami sebe. Otázka: Holí holič sám sebe?

Russellův paradox ukazuje meze našeho přístupu k množinám.

2.2.3 Vztahy mezi množinami

Základní vztahy mezi množinami jsou *rovnost* (označujeme ji symbolem $=$) a *inkluze* (označujeme ji symbolem $\subseteq$). Jsou-li A a B množiny, pak $A = B$ čteme „(množina) A se rovná (množině) B“ a $A \subseteq B$ čteme „(množina) A je podmnožinou (množiny) B“. Přitom

Základní vztahy mezi množinami jsou rovnost a inkluze.

$$A = B \quad \text{znamená, že} \quad \text{pro každý } x : x \in A \text{ právě když } x \in B$$

a

$$A \subseteq B \quad \text{znamená, že} \quad \text{pro každý } x : \text{ jestliže } x \in A, \text{ pak } x \in B.$$

Jinými slovy, $A = B$ znamená, že množiny A a B obsahují stejné prvky (neexistuje prvek, který by do jedné patřil ale do druhé ne). $A \subseteq B$ znamená, že všechny prvky množiny A jsou také prvky množiny B. $A \neq B$ znamená, že neplatí $A = B$. $A \not\subseteq B$ znamená, že neplatí $A \subseteq B$.

Všimněme si, že $A = B$ platí, právě když platí zároveň $A \subseteq B$ a $B \subseteq A$. Někdy je výhodné psát $A \subset B$, abychom označili, že $A \subseteq B$ a $A \neq B$. Dále si uvědomme, že pro všechny množiny A, B, C je $\emptyset \subseteq A$, $A \subseteq A$ a že jestliže $A \subseteq B$ a $B \subseteq C$, pak $A \subseteq C$.

Dokažme poslední tvrzení. Předpokládejme, že $A \subseteq B$ a $B \subseteq C$. Máme dokázat $A \subseteq C$, tedy že pro každý x platí, že když $x \in A$, pak $x \in C$. Zvolme tedy libovolný x a předpokládejme, že $x \in A$. Chceme ukázat $x \in C$. Uděláme to následovně. Z $x \in A$ a z předpokladu $A \subseteq B$ plyne, že $x \in B$. Dále z $x \in B$ a z předpokladu $B \subseteq C$ plyne $x \in C$. Důkaz je hotov.

Právě dokázané tvrzení je velmi jednoduché. Je tak jednoduché, že má člověk sklon říci „to je přece jasné, to není třeba dokazovat“. Tvrzení však mohou být složitější a složitější (viz dále) tak, že už nebudou „přece jasná“. Dokázat dané tvrzení, tj. vyjít z předpokladů a pomocí jednoduchých úvah (a popř. i pomocí známých tvrzení) dojít z předpokladů k závěru daného tvrzení, je pak jediným způsobem, jak se přesvědčit, že tvrzení platí. Ostatně uvědomme si, že i u velmi jednoduchých tvrzení je jediným korektním zdůvodněním důkaz.

Říci „to je přece jasné“ nemá jako argument žádnou váhu. Za prvé, člověk se může splést (co, co se mu zdá jasné, tak ve skutečnosti nemusí být). Za druhé, a to je snad ještě důležitější, argumentujeme-li pomocí „to je jasné“, může se nám stát, že pojmy, o kterých mluvíme, vlastně pořádně nechápeme, že je chápeme jen povrchně, intuitivně. Umět dokázat i jednoduchá tvrzení (a tvrzení vůbec) je tedy i dobrý test, jestli věci rozumíme (u složitějších tvrzení je dobré alespoň důkaz si přečíst a pochopit). Tedy naše doporučení: Čtěte důkazy a pokoušejte se je sami vymýšlet. To je užitečný zvyk nejen pro diskrétní matematiku. Naše zkušenost je následuící: Osvojit si důkazy (číst je, ty jednoduché i sami formulovat) vyžaduje počáteční časovou investici. Ta se ale vyplatí. Věcem lépe porozumíte, začnou se zdát jednoduché a začnete vidět souvislosti. Platí to nejen pro matematiku a informatiku, ale i pro každou oblast, ve které ze základních kamenů (pojmů, konstruktů, principů, . . .) budujeme složitější systém.

Příklad 2.6. Platí např.

- $\{2\} = \{n \in \mathbb{N} \mid n \text{ je sudé prvočíslo}\}$,
- $\emptyset = k \in \mathbb{Z} \mid \exists n \in \mathbb{N} : 2k = 2n + 1$,
- $\{a, b, c, d\} = \{b, d, c, a\}$, $\{a, b, 1\} = \{1, a, a, b, b, b, 1\}$,
- $\{a, b\} \subseteq \{a, b, c, d\}$, $\{a, b\} \subseteq \{1, 2, a, b\}$,
- $\{a, \{a, b\}, \{\{a, 1\}, b\}\} \subseteq \{\{a, b, \{a, b\}, \{a, b, 1\}, \{\{a, 1\}, b\}\}\}$,
- $\{a, b\} \not\subseteq \{\{a, b, c\}\}$, $\{\{a, 1\}\} \not\subseteq \{a, b, 1, \{a\}, \{1\}\}$.

Proč platí $\{a, b\} \not\subseteq \{\{a, b, c\}\}$, tj. proč $\{a, b\}$ není podmnožinou $\{\{a, b, c\}\}$? Vždyť v $\{\{a, b, c\}\}$ jsou všechny prvky, které jsou v $\{a, b\}$ (pokušení které může plynout z povrchního chápání $\subseteq$). Zdůvodnění: Např. pro prvek a je $a \in \{a, b\}$, ale $a \notin \{\{a, b, c\}\}$.

Průvodce studiem

Podívejte se znovu na Příklad 2.6. Vztahy mezi množinami, které jsou v něm uvedené, a další podobné vztahy byste měli umět bez problémů zdůvodnit. Tak si ověříte, že těm úplně základním věcem rozumíte. Tady i na jiných místech v textu platí, že skoro nemá smysl číst text dál, dokud vám nebude jasné (tj. dokud nebudete umět pomocí definic zdůvodnit), proč např. platí $\{\{a\}\} \subseteq \{\{a\}, \{b\}\}$ a proč neplatí $\{\{a\}\} \subseteq \{\{a, b\}\}$. Než tyto věci začnete jasně chápat a vidět, může to chvíli trvat. Ten čas se vám ale vrátí. Zdůvodněte např., proč je $x \in A$, právě když $\{x\} \subseteq A$.

Množina, jejímiž prvky jsou právě všechny podmnožiny dané množiny X, se nazývá *potenční množina* množiny X a značí se 2^X. Tedy

$$2^X = \{A \mid A \subseteq X\}.$$

Potenční množina množiny X je množina všech podmnožin množiny X.

Vezměme např. $X = \{a, b\}$. X má čtyři podmnožiny. Jsou to $\emptyset$ (ta je podmnožinou každé množiny), $\{a\}$, $\{b\}$ a $\{a, b\}$ (množina je podmnožino sebe samé). Tedy $2^X = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

Příklad 2.7.
- Pro $X = \{a\}$ je $2^X = \{\emptyset, \{a\}\}$,
- pro $X = \{1, 2, 3\}$ je $2^X = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$,
- pro $X = \emptyset$ je $2^X = \{\emptyset\}$ (to si promyslete: jedinou podmnožinou množiny $\emptyset$ je $\emptyset$),
- pro $X = \{a, \{a\}\}$ je $2^X = \{\emptyset, \{a\}, \{\{a\}\}, \{a, \{a\}\}\}$.

2.2.4 Operace s množinami

Se skupinami objektů provádíme v běžném životě různé operace. Např. řekneme „samostatnost a logické uvažování jsou společné vlastnosti Jany a Aleny“. Z množinového pohledu tím myslíme následující. Jana i Alena mají nějaké vlastnosti. Množinu rysů Jany označme J, množinu rysů Aleny označme A. Množiny J a A jsou různé, např. označuje-li m vlastnost „je dobrá v matematice“, může být $m \in J$ (Jana je dobrá v matematice), ale $m \notin A$ (Alena není dobrá v matematice). Označme s a l vlastnosti „samostatnost“ a

„logické uvažování“. Označme dále $J \cap A$ množinu vlastností, které patří do J i do A. Pak „samostatnost a logické uvažování jsou společné vlastnosti Jany a Aleny“ vlastně znamená $s \in J \cap A$ a $l \in J \cap A$.

Základní operace s množinami jsou průnik, sjednocení a rozdíl.

Mezi základní operace s množinami, se kterými se seznámíme, patří *průnik* (značí se $\cap$), *sjednocení* (značí se $\cup$) a *rozdíl* (značí se $-$). Jsou-li A a B množiny, definujeme množiny $A \cap B$, $A \cup B$ a $A - B$ předpisy

$$\begin{aligned} A \cap B &= \{x \mid x \in A \text{ a } x \in B\}, \\ A \cup B &= \{x \mid x \in A \text{ nebo } x \in B\}, \\ A - B &= \{x \mid x \in A \text{ a } x \notin B\}. \end{aligned}$$

Tedy x patří do $A \cap B$, právě když x patří do A i do B; x patří do $A \cup B$, právě když x patří do A nebo do B; x patří do $A - B$, právě když x patří do A, ale nepatří do B.

Příklad 2.8.
- Pro $A = \{a, b, e\}$, $B = \{b, c, d\}$ je $A \cap B = \{b\}$, $A \cup B = \{a, b, c, d, e\}$, $A - B = \{a, e\}$,
- pro $A = \{1, 2, a, b\}$, $B = \{1, a\}$ je $A \cap B = \{1, a\}$, $A \cup B = \{1, 2, a, b\}$, $A - B = \{2, b\}$, $B - A = \emptyset$,
- Pro $A = \{a\}$, $B = \{b, \{a\}\}$ je $A \cap B = \emptyset$, $A \cup B = \{a, b, \{a\}\}$,
- pro $A = \{\emptyset, a, \{a\}, \{a, b\}\}$, $B = \{b, \{a, \{b\}\}\}$ je $a \cap B = \emptyset$, $A \cup B = \{\emptyset, a, \{a\}, \{a, b\}, b, \{a, \{b\}\}\}$, $A - B = A$, $B - A = B$.

Množiny A a B se nazývají (navzájem) *disjunktní*, právě když $A \cap B = \emptyset$. Např. množiny $\{a, b, c, d\}$ a $\{1, 2, 3\}$ jsou disjunktní, množiny $\{a, b, 1\}$ a $\{1, 2, a\}$ disjunktní nejsou.

Často uvažujeme jednu množinu X, které říkáme *univerzum* (obor našich úvah) a pracujeme jen s množinami, které jsou podmnožinami X. Např. uvažujeme univerzum X všech občanů České republiky a potom pracujeme s jeho podmnožinami (např. množina dětí z X, množina zaměstnaných, množina důchodců apod.). Je-li dáno nějaké univerzum X a množina $A \subseteq X$, pak *doplněk* (někdy také *komplement*) množiny A je množina $X - A$ a značíme ji $\overline{A}$. Např. pro $X = \{a, b, c, d, e\}$ je $\overline{\{a, c\}} = \{b, d, e\}$.

Je-li $A = \{B_i \mid i \in I\}$ množina, jejíž prvky jsou opět množiny, definujeme

$$\bigcup A = \{x \mid \exists i \in I : x \in B_i\},$$

tedy $x \in \bigcup A$, právě když x patří do nějaké množiny, která je prvkem A. Např. $\bigcup\{\{a, b, c\}, \{a, 1\}, \{1, 2\}\} = \{a, b, c, 1, 2\}$.

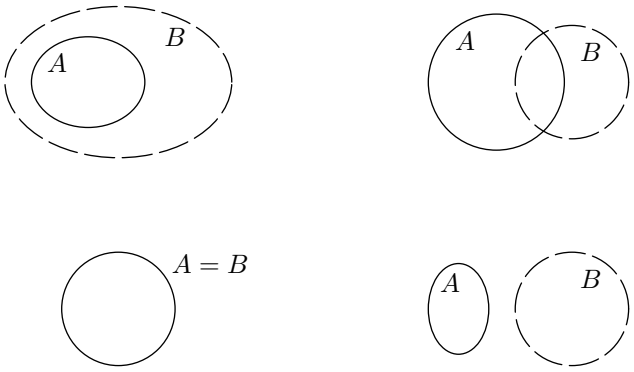
Vennovy diagramy slouží ke grafické ilustraci množin.

Průvodce studiem

Operace a základní vztahy mezi množinami můžeme ilustrovat pomocí tzv. *Vennových diagramů*[3]. Množiny se znázorňují (jsou reprezentovány) v rovině jako obrazce ohraničené uzavřenými křivkami (kružnice, ovály apod.). Přitom jedna množina může být reprezentována několika obrazci, které se neprotínají, popř. se jen dotýkají. Prvky množiny jsou ty body roviny, které se nacházejí uvnitř odpovídajícího obrazce (popř. se některé prvky v obrazci explicitně vyznačí křížkem). Ke každému obrazci se napíše symbol odpovídající množiny. Podívejte se na Obr. 1. Každá ze čtyř situací (vlevo dole, vpravo dole, vpravo nahoře, vlevo nahoře) znázorňuje dvě množiny, A a B. Pro situaci vlevo dole je $A = B$, vpravo dole jsou A a B disjunktní, vpravo nahoře A a B disjunktní nejsou, vlevo nahoře je $A \subseteq B$. Množina $A \cap B$ je reprezentována obrazcem, který je roven společné části obrazce reprezentujícího A a obrazce reprezentujícího B. Množina $A \cup B$ je reprezentována obrazcem, který je dán sloučením obrazce reprezentujícího A a obrazce reprezentujícího B. Fakt $A \subseteq B$ odpovídá situaci, kdy obrazec reprezentující A je obsažen v obrazci reprezentujícím B.

Vennovy diagramy umožňují názornou představu. Lze pomocí nich znázornit množiny, jejichž prvky můžeme chápat jako dvourozměrné. Některé množiny tak znázornit nemůžeme.

Podívejme se teď na některé základní vlastnosti.



Obrázek 1: Vennovy diagramy.

Věta 2.9. *Pro množiny A, B, C platí*

$$\begin{aligned}
A \cap \emptyset = \emptyset, &\qquad A \cup \emptyset = A \\
A \cup A = A, &\qquad A \cap A = A \\
A \cup B = B \cup A, &\qquad A \cap B = B \cap A \\
(A \cup B) \cup C = A \cup (B \cup C), &\qquad (A \cap B) \cap C = A \cap (B \cap C) \\
A \cap (B \cup C) = (A \cap B) \cup (A \cap C), &\qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \\
A \cup (A \cap B) = A, &\qquad A \cap (A \cup B) = A
\end{aligned}$$

Před důkazem si uvědomme následující. Máme-li dokázat $A = B$, máme podle definice dokázat, že pro libovolný prvek x je $x \in A$, právě když $x \in B$. To lze dále rozložit na ověření toho, že z $x \in A$ plyne $x \in B$ a že z $x \in B$ plyne $x \in A$. Pojďme na důkaz Věty 2.9.

Důkaz. $A \cap \emptyset = \emptyset$: Zvolme libovolný x. Je $x \in A \cap \emptyset$, právě když (podle definice $\cap$) $x \in A$ a $x \in \emptyset$. Protože $x \in \emptyset$ je vždy nepravdivé, je vždy nepravdivý i výrok $x \in A$ a $x \in \emptyset$. Máme tedy dále $x \in A$ a $x \in \emptyset$, právě když $x \in \emptyset$. Celkem tedy máme $x \in A \cap \emptyset$, právě když $x \in \emptyset$, což dokazuje $A \cap \emptyset = \emptyset$.

$A \cup \emptyset = A$: $x \in A \cup \emptyset$, právě když (podle definice $\cup$) $x \in A$ nebo $x \in \emptyset$, právě když (protože $x \in \emptyset$ je vždy nepravdivé) $x \in A$.

$A \cup A = A$: $x \in A \cup A$, právě když $x \in A$ nebo $x \in A$, právě když $x \in A$.

$A \cap A = A$: Podobně jako předchozí, $x \in A \cap A$, právě když $x \in A$ a $x \in A$, právě když $x \in A$.

$A \cup B = B \cup A$: $x \in A \cup B$, právě když $x \in A$ nebo $x \in B$, právě když $x \in B$ nebo $x \in A$, právě když $x \in B \cup A$.

$A \cap B = B \cap A$: Podobně jako předchozí.

$(A \cup B) \cup C = A \cup (B \cup C)$: $x \in (A \cup B) \cup C$, právě když $x \in (A \cup B)$ nebo $x \in C$, právě když ($x \in A$ nebo $x \in B$) nebo $x \in C$, právě když (podle pravidel výrokové logiky) $x \in A$ nebo ($x \in B$ nebo $x \in C$), právě když $x \in A$ nebo $x \in B \cup C$, právě když $x \in A \cup (B \cup C)$.

$(A \cap B) \cap C = A \cap (B \cap C)$: Podobně jako předchozí.

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$: $x \in A \cap (B \cup C)$, právě když $x \in A$ a $x \in B \cup C$, právě když $x \in A$ a ($x \in B$ nebo $x \in C$), což je podle pravidel výrokové logiky právě když ($x \in A$ a $x \in B$) nebo ($x \in A$ a $x \in C$), právě když $x \in A \cap B$ nebo $x \in A \cap C$, právě když $x \in (A \cap B) \cup (A \cap C)$.

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$: Podobně jako předchozí.

$A \cup (A \cap B) = A$: $x \in A \cup (A \cap B)$, právě když $x \in A$ nebo ($x \in A$ a $x \in B$)), což je podle pravidel výrokové logiky právě když $x \in A$.

$A \cap (A \cup B) = A$: Podobně jako předchozí. □

Vidíme tedy, že řadu vlastností operací s množinami dostaneme jednoduše z odpovídajících pravidel výrokové logiky. Podívejme se ještě jednou na důkaz tvrzení $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Z výrokové logiky víme, že formule $p \wedge (q \vee r)$ je ekvivalentní formuli $(p \wedge q) \vee (p \wedge r)$, tj. tyto formule mají při každém ohodnocení stejnou pravdivostní hodnotu. Vezmeme-li ohodnocení, které výrokovým symbolům p, q a r přiřazují po řadě pravdivostní hodnoty tvrzení $x \in A$, $x \in B$, $x \in C$, pak při tomto ohodnocení má formule $p \wedge (q \vee r)$ stejnou pravdivostní hodnotu jako tvrzení $x \in A \cap (B \cup C)$ (podívejte se do výše napsaného důkazu) a formule $(p \wedge q) \vee (p \wedge r)$ má stejnou pravdivostní hodnotu jako tvrzení $x \in (A \cap B) \cup (A \cap C)$. Proto je $x \in A \cap (B \cup C)$, právě když $x \in (A \cap B) \cup (A \cap C)$, tedy $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Průvodce studiem

Jedním z jednoduchých ale užitečných přínosů teorie množin je, že nám dává prostředky jednoduše a jednoznačně se vyjadřovat. Bez množinového formalismu bychom vše museli vyjadřovat opisem. K jednoduchosti: Zkuste např. opisem (tj. v přirozenémjazyku, bez množinového formalismu) popsat množinu $(A \cap (B \cup (A \cap D))) \cup (B \cup E)$. K jednoznačnosti: Řekneme-li „seskupení sudých a lichých čísel“, máme nejspíš na mysli sjednocení množiny sudých a množiny lichých čísel. Řekneme-li ale „soubor malých a zelených mužíčků“, máme asi na mysli soubor těch mužíčků, kteří jsou zároveň malí a zelení (průnik množiny malých mužíčků a množiny zelených mužíčků), ale můžeme mít namysli i soubor těch mužíčků, kteří jsou malí nebo zelení (sjednocení množiny malých mužíčků a množiny zelených mužíčků). Co přesně máme na mysli, vyplývá z kontextu nebo to musíme upřesnit. Množinový formalismus je naproti tomu jednoznačný.

Shrnutí

Množiny, relace a funkce patří k základním pojmům matematiky. Množina je matematický pojem, který je protějškem běžně používaného pojmu soubor, seskupení apod. Relace je protějškem pojmu vztah. Funkce je protějškem pojmu přiřazení.
Množina je dána tím, jaké prvky obsahuje. Speciální množinou je prázdná množina, ta neobsahuje žádný prvek. S množinami můžeme provádět různé operace. Mezi základní patří průnik, sjednocení a rozdíl. Základní vztah mezi množinami je vztah inkluze (být podmnožinou). Množiny zapisujeme nejčastěji výčtem prvků nebo udáním charakteristické vlastnosti.

Pojmy k zapamatování

- množina,
- inkluze,
- průnik, sjednocení, rozdíl,
- potenční množina.

Kontrolní otázky

1. *Může množina obsahovat daný prvek více než jedenkrát? Proč? Jsou množiny $\{a, b\}$ a $\{b, a\}$ různé? Proč?*
2. *Jaké znáte způsoby zápisu množin? Jsou množiny $\{x \in \mathbb{R} \mid x^2 < 0\}$ a $\{x \in \mathbb{N} \mid x^4 < 0\}$ stejné? Je některá z nich rovna $\emptyset$?*
3. *Platí, že když $A \subseteq B$, pak $|A| = |B|$? Co je to potenční množina dané množiny? Existuje množina, jejíž potenční množina je prázdná?*
4. *Jaké znáte množinové operace? Jaká je nutná a postačující podmínka pro to, aby $A \cap X = A$? Jaká pro $A \cup X = A$?*

Cvičení

1. Platí následující tvrzení?
   a) $\emptyset \subseteq \emptyset$
   b) $\emptyset \in \emptyset$
   c) $\{a\} \in \{a, b, c\}$
   d) $\{a\} \in \{\{a, b\}, c\}$
   e) $\{a, b\} \subseteq \{a, \{a, b\}\}$
   f) $\{a, b\} \subseteq \{a, b, \{a, b\}\}$
   g) $A \in P(A)$
2. Nechť $A = \{a, 1, \{a, b\}\}$, $B = \{2, a, \{a\}, \}$, $C = \{\emptyset, 2, 3, \{a, b\}\}$. Určete $A \cup B$, $A \cap C$, $C - A$, $A \times B$, $P(B)$.
3. Nechť $A = \{a, \{b\}\}$, $B = \{a, b, \{a, b\}\}$. Určete $B \cap P(A)$, $(A \times B) \cap (B \times A)$.
4. Určete $P(\emptyset)$, $P(\{\emptyset\})$, $P(\{1\})$, $P(\{\{\emptyset\}\})$, $P(\{\emptyset, \{\emptyset\}\})$.
5. Definujme operaci $\oplus$ vztahem

$$A \oplus B = (A \cup B) - (A \cap B).$$

   Zjistěte, zda platí následující vztahy (vztahy dokažte nebo nalezněte protipříklady.)
   a) $A \oplus A = A$
   b) $A \oplus (B \cap C) = (A \oplus B) \cap (A \oplus C)$
   c) $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$
   d) $A \oplus (A \oplus A) = A$
   e) $A \subseteq B \Rightarrow A \oplus C \subseteq B \oplus C$
6. Najděte nutnou a postačující podmínku pro to, aby a) $A \oplus B = A \cup B$, b) $A \oplus B = A$.
7. Najděte příklady množin A, B, C tak, aby platilo
   a) $A \cap B = C \cap B$, ale $A \neq C \neq \emptyset$
   b) $A \cap B \subset A \cap C$, ale $B \not\subseteq C$
   c) $A \cup B = C \cup B$, ale $A \neq C$
   d) $A \cup B \subset A \cup C$, ale $B \not\subseteq C$
8. Nechť pro množiny A, B, C platí $B \subset A \subset C$. Určete množinu X, pro kterou $A - X = B$ a $A \cup X = C$.

Úkoly k textu

1. Zdůvodněte (přesně podle definice), proč je prázdná množina podmnožinou každé množiny.
2. Může mít potenční množina množiny A méně prvků než množina A? Může jich mít stejně? Může jich mít více?
3. Jaké vztahy platí mezi množinou A a 2^X?

Řešení

1. a) ano, b) ne, c) ne, d) ne, e) ne, f) ano, g) ano.
2. $A \cup B = \{a, 1, 2, \{a\}, \{a, b\}\}$, $A \cap C = \{\{a, b\}\}$, $C - A = \{\emptyset, 2, 3\}$, $A \times B = \{\langle a, 2\rangle, \langle a, a\rangle, \langle a, \{a\}\rangle, \langle 1, 2\rangle, \langle 1, a\rangle, \langle 1, \{a\}\rangle, \langle \{a, b\}, 2\rangle, \langle \{a, b\}, a\rangle, \langle \{a, b\}, \{a\}\rangle, \}$, $P(B) = \{\emptyset, \{2\}, \{a\}, \{\{a\}\}, \{2, a\}, \{2, \{a\}\}, \{a, \{\}\}, \{2, a, \{a\}\}\}$.
3. $B \cap P(A) = \emptyset$, $(A \times B) \cap (B \times A) = \{\langle a, a\rangle\}$.
4. $P(\emptyset) = \{\emptyset\}$, $P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$, $P(\{1\}) = \{1, \{1\}\}$, $P(\{\{\emptyset\}\}) = \{\{\{\emptyset\}\}, \emptyset\}$, $P(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$.

5. a) ne, b) ano, c) ano, d) ano, e) ne
6. a) $A \cap B = \emptyset$, b) $B = \emptyset$.
7. a) $A = \{a, b, c\}$, $B = \{a, c, d\}$, $C = \{a\}$, b) $A = \{a\}$, $B = \{a, b\}$, $C = \{a, c\}$, c) $A = \{a\}$, $B = \{a, b, c\}$, $C = \{c\}$, d) $A = \{a, b\}$, $B = \{a, c\}$, $C = \{b, c, d\}$.
8. $X = C - B$ (jiné nejsou).

Studijní cíle: Po prostudování kapitol 2.3 a 2.5 by student měl rozumět pojmům relace a funkce. Měl by znát základní operace a vztahy definované nad těmito pojmy. Student by měl tyto pojmy znát aktivně, měl by umět samostatně dokázat jednoduchá tvrzení, hledat příklady a protipříklady.

Klíčová slova: kartézský součin, relace, reprezentace relací, inverzní relace, skládání relací, funkce, injekce, surjekce, bijekce, princip indukce.

Potřebý čas: 180 minut.

2.3 Relace

2.3.1 Pojem relace

Pojem relace je matematickým protějškem běžně používaného pojmu *vztah*. Různé objekty jsou nebo nejsou v různých vztazích. Např. číslo 3 je ve vztahu „být menší“ s číslem 5, ne však s číslem 2. Karel Čapek byl ve vztahu „být bratrem“ s Josefem Čapkem. Tři body v rovině mohou být ve vztahu „ležet na jedné přímce“.

Všimněme si, čím je vztah určen. Za prvé je to tzv. arita vztahu, tj. číslo udávající počet objektů, které do vztahu vstupují. Např. do vztahu „být bratrem“ vstupují dva objekty, ten vztah je binární, do vztahu „ležet na jedné přímce“ vstupují tři objekty, ten vztah je ternární. Za druhé jsou to množiny, jejichž prvky do vztahu vstupují. Např. do vztahu „být bratrem“ vstupují dva objekty, první je z množiny X_1 lidí, druhý je z množiny X_2 lidí. V tomto případě jsou X_1 a X_2 stejné, tj. $X_1 = X_2$. To tak ale nemusí být. Uvažujme např. vztah „mít“ mezi množinou X_1 nějakých objektů a množinou X_2 nějakých atributů. V tomto případě je obecně $X_1 \neq X_2$, např. $X_1 = \{$pes, kočka, běhat, stůl, rychlý, zelený, číst$\}$ a $X_2 = \{$„je podstatné jméno“, „je sloveso“$\}$. Je-li dána arita n a příslušné množiny $X_1, \ldots, X_n$, vztah je potom určen tím, které prvky x_1 z $X_1, \ldots, x_n$ z X_n v tom vztahu jsou a které ne. To nás přivádí k pojmu relace.

Základním pojmem je pojem uspořádané n-tice prvků. *Uspořádaná n-tice* objektů $x_1, \ldots, x_n$ (v tomto pořadí) se označuje $\langle x_1, \ldots, x_n \rangle$. Prvek x_i ($1 \leq i \leq n$) se nazývá i-tá složka dané n-tice. Rovnost definujeme tak, že $\langle x_1, \ldots, x_n \rangle = \langle y_1, \ldots, y_m \rangle$, právě když $n = m$ a $x_1 = y_1$, …, $x_n = y_n$. n-tice a m-tice jsou si tedy rovny, právě když mají stejný počet složek a odpovídající si složky jsou stejné.

Definice 2.10. *Kartézský součin* množin $X_1, \ldots, X_n$ je množina $X_1 \times \cdots \times X_n$ definovaná předpisem

$$X_1 \times \cdots \times X_n = \{\langle x_1, \ldots, x_n \rangle \mid x_1 \in X_1, \ldots, x_n \in X_n\}.$$

Kartézský součin n množin je množina všech uspořádaných n-tic prvků z těchto množin.

Je-li $X_1 = \cdots = X_n = X$, pak $X_1 \times \cdots \times X_n$ značíme také X^n (n-tá kartézská mocnina množiny X). Uspořádanou 1-tici $\langle x \rangle$ obvykle ztotožňujeme s prvkem x (tj. $\langle x \rangle = x$). Potom tedy X^1 je vlastně množina X.

Příklad 2.11.
- Pro $A = \{a, b, c\}$, $B = \{1, 2\}$ je $A \times B = \{\langle a, 1\rangle, \langle a, 2\rangle, \langle b, 1\rangle, \langle b, 2\rangle, \langle c, 1\rangle, \langle c, 2\rangle\}$, $B^2 = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle\}$,
- pro $A = \{\{a\}, b\}$, $B = \{1\}$ je $A \times B = \{\langle \{a\}, 1\rangle, \langle b, 1\rangle\}$,
- pro $A = \{1, 2\}$, $B = \{b\}$ je $A \times B \times A = \{\langle 1, b, 1\rangle, \langle 1, b, 2\rangle, \langle 2, b, 1\rangle, \langle 2, b, 2\rangle\}$,
- pro $A = \emptyset$, $B = \{1, 2, 3\}$ je $A \times B = \emptyset$ (neexistuje totiž uspořádaná dvojice $\langle x, y \rangle$ tak, aby $x \in A$ a $y \in B$).

Můžeme přistoupit k definici pojmu relace.

Definice 2.12. Nechť $X_1, \ldots, X_n$ jsou množiny. *Relace* mezi $X_1, \ldots, X_n$ je libovolná podmnožina kartézského součinu $X_1 \times \cdots \times X_n$.

Relace mezi množinami $X_1, \ldots, X_n$ je podmnožina kartézského součinu $X_1 \times \cdots \times X_n$.

Poznámka 2.13. (1) Číslu n říkáme arita relace R, R se nazývá n-ární. Je-li $X_1 = \cdots = X_n = X$, nazývá se R také n-ární relace v množině X. Pro $n = 1, 2, 3, 4$ se místo n-ární používá také unární, binární, ternární, kvaternární. To, že R je unární relace v X, vlastně znamená, že $R \subseteq X$.

(2) O prvcích $x_1 \in X_1, \ldots, x_n \in X_n$ říkáme, že jsou (v tomto pořadí) v relaci R, pokud $\langle x_1, \ldots, x_n \rangle \in R$.

Relace je tedy množina sestávající z n-tic prvků příslušných množin. Obsahuje ty n-tice $\langle x_1, \ldots, x_n \rangle$, které mezi sebou mají zamýšlený vztah. Ty, které zamýšlený vztah nemají, neobsahuje. Běžně používaný, avšak jen intuitivně chápaný, pojem vztah je tedy pojmem relace matematizován. Pojem relace je přitom založen na pojmech množina a uspořádaná n-tice.

Příklad 2.14. (1) Pro $X = \{a, b, c\}$, $Y = \{1, 2, 3, 4\}$ jsou $\{\langle a, 2\rangle, \langle a, 3\rangle, \langle b, 1\rangle, \langle c, 1\rangle\}$, $\{\langle a, 2\rangle\}$, $\emptyset$, $X \times Y$ binární relace mezi X a Y. $\{\langle a, b, 2, 4, c\rangle, \langle a, a, 2, 2, a\rangle\}$ je relace mezi X, X, Y, Y, X. $\{\langle a, 1\rangle, \langle 2, c\rangle\}$ není binární relace mezi X a Y, protože dvojice $\langle 2, c\rangle$ nepatří do kartézského součinu $X \times Y$.

(2) Předpokládejme, že na rodinné oslavě jsou Adam (A), Bedřich (B), Cyril (C), Dominik (D), Egon (E), Marta (M), Naďa (N), Olga (O), Pavla (P) a Radka (R). Přitom A je synem Cyrila a Marty, C je synem Egona a Olgy, P je dcerou Dominka, E je synem Adama a Radky. Určete binární relaci R, která odpovídá vztahu „X je dítětem Y“, a ternární relaci S, která odpovídá vztahu „X je dítětem Y a Z“, kde Y je otec a Z je matka.

Jde o relace na množině {A, B, C, D, E, M, N, O, P, R}. R bude obsahovat všechny uspořádané dvojice $\langle x, y\rangle$ takové, že x je dítětem y. Tedy

$$R = \{\langle \mathrm{A}, \mathrm{C}\rangle, \langle \mathrm{A}, \mathrm{M}\rangle, \langle \mathrm{C}, \mathrm{E}\rangle, \langle \mathrm{C}, \mathrm{O}\rangle, \langle \mathrm{P}, \mathrm{D}\rangle, \langle \mathrm{E}, \mathrm{A}\rangle, \langle \mathrm{E}, \mathrm{R}\rangle\}$$

a

$$S = \{\langle \mathrm{A}, \mathrm{C}, \mathrm{M}\rangle, \langle \mathrm{C}, \mathrm{E}, \mathrm{O}\rangle, \langle \mathrm{E}, \mathrm{A}, \mathrm{R}\rangle\}.$$

(3) Platí-li navíc, že C je manželem M, E je manželem O a A je manželem R, můžeme uvažovat binární relaci T mezi množinou $X = \{\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{E}\}$ mužů a množinou $Y = \{\mathrm{M}, \mathrm{N}, \mathrm{O}, \mathrm{P}, \mathrm{R}\}$ žen, tj. $T \subseteq X \times Y$, která odpovídá vztahu „být manželem“. Pak bude

$$T = \{\langle \mathrm{C}, \mathrm{M}\rangle, \langle \mathrm{E}, \mathrm{O}\rangle, \langle \mathrm{A}, \mathrm{R}\rangle\}.$$

(4) Zapište jako binární relaci vztah dělitelnosti (tj. „x dělí y“ znamená, že existuje celé číslo k tak, že $x \cdot k = y$) na množině $X = \{2, \ldots, 10\}$.

Označme příslušnou relaci D. Je tedy $D \subseteq X \times X$, konkrétně

$$D = \{\langle 2, 2\rangle, \langle 2, 4\rangle, \langle 2, 6\rangle, \langle 2, 8\rangle, \langle 2, 10\rangle, \langle 3, 6\rangle, \langle 3, 9\rangle, \langle 4, 8\rangle, \langle 5, 10\rangle\}.$$

Průvodce studiem

Zastavme se u pojmu relace. Podle Definice 2.12 je relace podmnožina kartézského součinu. Dává to smysl? Relace má být matematickým protějškem pojmu vztah, který je přece každému jasný. Naproti tomu „podmnožina kartézského součinu“ zní nepřístupně a zbytečně komplikovaně. Pokud souhlasíte s předchozími dvěma větami, bude nejlepší, když si zkusíte sami narvhnout definici pojmu relace. Uvidíte, jestli přijdete na něco lepšího než je Definice 2.12. Přitom ale dodržte „pravidla hry“: Vaše definice musí být jednoznačná (tj. musí být založana na jednoznačně definovaných pojmech) a musí být tak obecná, aby odpovídala pojmu vztah (tj. nemůžete se např. omezit jen na binární relace). Např. definice „Relace je dána tím, které prvky jsou v relaci se kterými.“ neobstojí. Je značně neurčitá a navíc je to definice kruhem (v definici pojmu relace se odkazujeme na pojme relace). Zkuste si představit, že podle této definice máte rozhodnout, zde něco je nebo není relace. Že je třeba, aby definice relace byla jednoznačná a jednoduchá vynikne nejlépe, když si uvědomíme, že relace můžeme chtít zpracovávat počítačem (a počítačových aplikací založených na relacích je celá řada). Předkládáme-li nejednoznačnou definici člověku, může nám to projít, ten člověk si definici třeba domyslí. U počítače nám to neprojde,

příjmení	jméno	narození	vzdělání	funkce
Adam	Jiří	1976	SŠ	prodejce
Kos	Jan	1961	VŠ	projektant
Malá	Magda	1955	SŠ	sekretářka
Rychlý	Karel	1967	VŠ	ředitel
⋮	⋮	⋮	⋮	⋮
Zahradník	Milan	1950	ZŠ	technik

Tabulka 6: Databáze z Příkladu 2.15.

počítač si nic nedomyslí. Kromě toho, jednoznačnost a jednoduchost definice patří k základům kultury vyjadřování nejen v matematice. Nejste-li tedy spokojeni s Definicí 2.12, zkuste teď sami navrhnout lepší a pak pokračujte ve čtení.

Porovnejte nyní váš návrh s Definicí 2.12 (nejlépe s kolegy nebo učitelem). Pokud jste lepší definici nevymysleli, vraťte se k Definici 2.12 a znovu ji posuďte.

Příklad 2.15. Pojem relace má ústřední roli v tzv. relačním databázovém modelu, který navrhl E. F. Codd.[4] Tzv. relační pohled na databáze spočívá v tom, že databázi chápeme jako relaci. Např. databázi znázorněnou Tab. 6, která obsahuje v řádcích informace o zaměstnancích, můžeme chápat jako 5-ární relaci R mezi množinami (těm se v databázích říká domény) $D_1 = \{\text{Adam, Kos, Malá, Rychlý, } \dots\}$, $D_2 = \{\text{Jiří, Jan, Magda, Karel, } \dots\}$, $D_3 = \{n \in \mathbb{N} \mid 1900 \leq n \leq 2004\}$, $D_4 = \{\text{ZŠ, SOU, SŠ, VŠ}\}$, $D_5 = \{\text{prodejce, projektant, sekretářka, ředitel, } \dots\}$, tedy $R \subseteq D_1 \times D_2 \times D_3 \times D_4 \times D_5$. Relace je dána záznamy (řádky) v databázi, takže např. $\langle$ Adam, Jiří, 1976, SŠ, prodejce$\rangle \in R$, $\langle$ Kos, Jan, 1961, VŠ, projektant$\rangle \in R$. V relačních databázích jsou zavedeny i jiné operace než ty, které zavedeme my. Tyto operace slouží k manipulaci a zpřístupňování dat v databázi a čtenář se s nimi může seznámit téměř v každé učebnici databázových systémů.

2.3.2 Vztahy a operace s relacemi

Relace jsou množiny (relace je podmnožina kartézského součinu). Proto s nimi lze provádět množinové operace ($\cap$, $\cup$, $-$) a lze na ně aplikovat vztah inkluze ($\subseteq$).

Relace jsou speciální množiny, a proto s nimi můžeme provádět všechny množinové operace.

Příklad 2.16. (1) Mějme $X = \{a, b, c\}$, $Y = \{1, 2, 3, 4\}$ a uvažujme binární relace $R = \{\langle a, 1\rangle, \langle a, 4\rangle, \langle c, 2\rangle, \langle c, 3\rangle, \langle c, 4\rangle\}$, $S = \{\langle a, 2\rangle, \langle a, 3\rangle, \langle a, 4\rangle, \langle b, 1\rangle, \langle b, 3\rangle\}$, $T = \{\langle a, 4\rangle, \langle c, 4\rangle\}$ mezi X a Y. Pak je např.

$$\begin{aligned} R \cap S &= \{\langle a, 4\rangle\}, \\ R \cup S &= \{\langle a, 1\rangle, \langle a, 2\rangle, \langle a, 3\rangle, \langle a, 4\rangle, \langle b, 1\rangle, \langle b, 3\rangle, \langle c, 2\rangle, \langle c, 3\rangle, \langle c, 4\rangle\}. \end{aligned}$$

Dále je $T \subseteq S$, $R \not\subseteq S$ apod.

(2) Nechť $\leq$ je relace uspořádání a $|$ relace dělitelnosti na množině $\mathbb{N}$ přirozených čísel. Tedy $\langle k, l\rangle \in \leq$, právě když k je menší nebo rovno l, a $\langle k, l\rangle \in |$, právě když l je dělitelné číslem k (v tomto případě, jako i u jiných případů binárních relací, běžně používáme tzv. infixovou notaci, tj. píšeme $k \leq l$ a $k|l$). Pak $| \subseteq \leq$, tj. relace $|$ je podmnožinou relace $\leq$. To vlastně znamená, že pro všechna přirozená čísla $k, l \in \mathbb{N}$ platí, že když $k|l$, pak $k \leq l$.

(3) Jsou-li R_1 a R_2 relace popisující nějaké databáze (viz Příklad 2.15), pak $R_1 \cup R_2$ je relace popisující databázi, která vznikne sloučením výchozích databází, tj. zřetězením databázových tabulek (přesně vzato, sloučením a vymazáním duplicitních výskytů databázových řádků). $R_1 \cap R_2$ je relace, která popisuje společné položky obou databází.

[4] Pěkně je o tom napsáno v knize C. J. Date: *The Database Relational Model: A Retrospective Analysis*. Addison Wesley, Reading, MA, 2001.

R	1	2	3	4
a	×	×		×
b		×		×
c	×			

Tabulka 7: Tabulka popisující binární relaci R mezi $X = \{a, b, c\}$ a $Y = \{1, 2, 3, 4\}$.

R	b	h	k	o	r	s	v	z
1		×			×			
2		×						
3	×	×	×	×	×	×	×	×
4							×	
5		×			×		×	
6	×	×	×		×			
7	×	×				×		×

S	C	M	N	S	Za
b	×	×			
h	×	×		×	
k	×				
o					×
r	×			×	
s		×			
v			×	×	×
z		×			

Tabulka 8: K Příkladu 2.18: Tabulky popisující binární relaci R mezi pacienty a příznaky nemocí (vlevo) a relaci S příznaky nemocí a nemocemi (vpravo).

2.3.3 Operace s binárními relacemi

S relacemi však lze díky jejich speciální struktuře provádět i další operace. Zaměříme se na binární relace. Ty lze znázorňovat tabulkami. Např. relace $R = \{\langle a, 1\rangle, \langle a, 2\rangle, \langle a, 4\rangle, \langle b, 2\rangle, \langle b, 4\rangle, \langle c, 1\rangle\}$ mezi množinami $X = \{a, b, c\}$ a $Y = \{1, 2, 3, 4\}$ je znázorněna v Tab. 8. Tedy, je-li $\langle x, y\rangle \in R$, je v průsečíku řádku x a sloupce y symbol $\times$, jinak tam není nic.

S binárními relacemi lze navíc provádět operace inverze a skládání.

Začneme tzv. inverzní relací. *Inverzní relací* k relaci $R \subseteq X \times Y$ je relace R^{-1} mezi Y a X definovaná předpisem

$$R^{-1} = \{\langle y, x\rangle \mid \langle x, y\rangle \in R\}.$$

Příklad 2.17. Nechť relace R mezi $X = \{a, b, c\}$ a $Y = \{1, 2, 3\}$ je $R = \{\langle a, 1\rangle, \langle a, 2\rangle, \langle b, 2\rangle\}$. Pak inverzní relace k R je relace R^{-1} mezi Y a X daná $R^{-1} = \{\langle 1, a\rangle, \langle 2, a\rangle, \langle 2, b\rangle\}$.

Další operací je tzv. skládání. Je-li R relací mezi množinami X a Y a S relací mezi množinami Y a Z, pak *složením* relací R a S je relace $R \circ S$ mezi X a Z definovaná předpisem

$$R \circ S \;=\; \{\langle x, z\rangle \mid \text{existuje } y \in Y : \langle x, y\rangle \in R \text{ a } \langle y, z\rangle \in S\}.$$

Tedy $\langle x, z\rangle$ patří do relace $R \circ S$, právě když existuje prvek $y \in Y$ tak, že $\langle x, y\rangle$ jsou v relaci R a $\langle y, z\rangle$ jsou v relaci S.

Uvažujme následující příklad. Nechť X je množina pacientů, Y množina příznaků nemocí a Z množina nemocí. Nechť $R \subseteq X \times Y$ je relace „mít příznak“, tj. $\langle x, y\rangle \in R$ znamená, že pacient x má příznak y, a $S \subseteq Y \times Z$ je relace „být příznakem“, tj. $\langle y, z\rangle \in S$ znamená, že y je příznakem nemoci z (např. zvýšená teplota je příznakem chřipky). Pak pro pacienta $x \in X$ a nemoc $z \in Z$ znamená $\langle x, z\rangle \in R \circ S$, že existuje příznak $y \in Y$ tak, že pacient x má tento příznak a zároveň je tento příznak příznakem nemoci z. Tedy $\langle x, z\rangle \in R \circ S$ můžeme interpretovat jako „pacient x může mít nemoc z“.

Příklad 2.18. Nechť $X = \{1, 2, 3, 4, 5, 6, 7\}$ (X reprezentuje pacienty 1–7), $Y = \{b, h, k, o, r, s, v, z\}$ (b ... bolest hlavy, h ... horečka, k ... bolest končetin, o ... oteklé žlázy na krku, r ... rýma, s ... strnulý krk, v ... vyrážka, z ... zvracení), $Z = \{C, M, N, S, Za\}$ (C ... chřipka, M ... meningitida, N ... plané neštovice, S ... spalničky, Za ... zarděnky). Vztah „mít příznak“ mezi pacienty a příznaky je popsán relací $R \subseteq X \times Y$ znázorněnou v Tab. 8 vlevo, vztah „být příznakem nemoci“ mezi příznaky a nemocemi je popsán relací $S \subseteq Y \times Z$ znázorněnou v Tab. 8 vpravo. Složení relací R a S je relace $R \circ S \subseteq X \times Z$ znázorněná v Tab. 9. Protože $\langle x, z\rangle \in R \circ S$ můžeme chápat tak, že pacient x může mít nemoc z, můžeme se na přílad dívat následovně. Ze vstupních informací R (dáno lékařským vyšetřením) a S (dáno znalostí lékaře) jsme odvodili nové informace reprezentované relací $R \circ S$. Ty říkají, že např. pacient 1 může

$R \circ S$	C	M	N	S	Za
1	×	×		×	
2	×	×			
3	×	×	×	×	×
4			×	×	×
5	×	×	×	×	×
6	×	×		×	
7	×	×		×	

Tabulka 9: Tabulka popisující binární relaci $R \circ S$ mezi pacienty a nemocemi (viz Příklad 2.18).

mít chřipku, meningitidu nebo spalničky, že pacient 5 může mít libovolnou z uvažovaných nemocí (má všechny sledované příznaky), pacient 6 může mít libovolnou z uvažovaných nemocí (přestože nemá všechny sledované příznaky) atd.

Věta 2.19. *Pro relace $R \subseteq X \times Y$, $S \subseteq Y \times Z$, $T \subseteq Z \times U$ platí.*

$$\begin{aligned} R \circ (S \circ T) &= (R \circ S) \circ T \\ (R \circ S)^{-1} &= S^{-1} \circ R^{-1} \\ (R^{-1})^{-1} &= R \end{aligned}$$

Důkaz. $R \circ (S \circ T) = (R \circ S) \circ T$: Máme $\langle x, u\rangle \in R \circ (S \circ T)$, právě když existuje $y \in Y$ tak, že $\langle x, y\rangle \in R$ a $\langle y, u\rangle \in S \circ T$, právě když právě když existuje $y \in Y$ tak, že $\langle x, y\rangle \in R$ a existuje $z \in Z$ tak, že $\langle y, z\rangle \in S$ a $\langle z, u\rangle \in T$, právě když existují $y \in Y$ a $z \in Z$ tak, že $\langle x, y\rangle \in R$, $\langle y, z\rangle \in S$, $\langle z, u\rangle \in T$, právě když existuje $z \in Z$ tak, že $\langle x, z\rangle \in R \circ S$ a $\langle z, u\rangle \in T$, právě když $\langle x, y\rangle \in (R \circ S) \circ T$.

$(R \circ S)^{-1} = S^{-1} \circ R^{-1}$: $\langle z, x\rangle \in (R \circ S)^{-1}$, právě když $\langle x, z\rangle \in (R \circ S)$, právě když existuje $y \in Y$ tak, že $\langle x, y\rangle \in R$ a $\langle y, z\rangle \in S$, právě když existuje $y \in Y$ tak, že $\langle z, y\rangle \in S^{-1}$ a $\langle y, x\rangle \in R^{-1}$, právě když $\langle z, x\rangle \in S^{-1} \circ R^{-1}$.

$(R^{-1})^{-1} = R$: $\langle x, y\rangle \in (R^{-1})^{-1}$, právě když $\langle y, x\rangle \in R^{-1}$, právě když $\langle x, y\rangle \in R$. □

Způsobů, jak skládat relace, existuje více.

Existují však i další přirozené způsoby, jak skládat relace. Předpokládejme opět, že $R \subseteq X \times Y$, $S \subseteq Y \times Z$. Pak $R \lhd S$, $R \rhd S$ a $R \square S$ jsou relace mezi X a Z definované předpisy

$$\begin{aligned} R \lhd S &= \{\langle x, z\rangle \mid \text{pro každé } y \in Y : \text{ pokud } \langle x, y\rangle \in R, \text{ pak } \langle y, z\rangle \in S\}, \\ R \rhd S &= \{\langle x, z\rangle \mid \text{pro každé } y \in Y : \text{ pokud } \langle y, z\rangle \in S, \text{ pak } \langle x, y\rangle \in R\}, \\ R \square S &= \{\langle x, z\rangle \mid \text{pro každé } y \in Y : \langle x, y\rangle \in R, \text{ právě když } \langle y, z\rangle \in S\}. \end{aligned}$$

Vraťme se k příklady s pacienty, příznaky a nemocemi. $\langle x, z\rangle \in R \lhd S$ znamená, že všechny příznaky, které má pacient x, jsou příznaky nemoci z. $\langle x, z\rangle \in R \rhd S$ znamená, že pacient x má všechny příznaky nemoci y. $\langle x, z\rangle \in R \square S$ znamená, že pacient x má právě příznaky nemoci y. Uvědomme si, že relace R může vzniknout na základě lékařského vyšetření (lékař zjišťuje, jaké příznaky pacienti mají) a že relace S je „učebnicová znalost“ (lékařské knihy popisují příznaky jednotlivých nemocí). Obě R i S tedy mohou být dostupné např. v databázi. Všechna složení $R \circ S$, $R \lhd S$, $R \rhd S$ i $R \square S$ je pak možné z R a S jednoduše spočítat. Tyto relace poskytují netriviální informace o tom, kteří pacienti mohou mít které nemoci. Přitom pro daného pacienta x a danou nemoc y má každý z faktů $\langle x, z\rangle \in R \circ S$, $\langle x, z\rangle \in R \lhd S$, $\langle x, z\rangle \in R \rhd S$ i $\langle x, z\rangle \in R \square S$ přesně stanovený význam. Přitom nejslabší indikací toho, že pacient x má nemoc z je fakt $\langle x, z\rangle \in R \circ S$ (x má aspoň jeden příznak nemoci z), nejsilnější naopak fakt $\langle x, z\rangle \in R \square S$ (x má právě všechny příznaky nemoci z). Jak je vidět přímo z definice (rozmyslete si), relace $\lhd$ i $\rhd$ jsou podmnožinami relace $\square$, ta je jejich průnikem.

Příklad 2.20. Vraťme se k Příkladu 2.18. Relace $R \lhd S$, $R \rhd S$ a $R \square S$ jsou znázorněny v Tab. 10.

$R \lhd S$	C	M	N	S	Za
1	×			×	
2	×	×		×	
3					
4			×	×	×
5				×	
6	×				
7		×	×	×	×

$R \rhd S$	C	M	N	S	Za
1					
2					
3	×	×	×	×	×
4			×		
5			×	×	
6	×				
7		×			

$R \square S$	C	M	N	S	Za
1					
2					
3					
4			×		
5				×	
6	×				
7		×			

Tabulka 10: Tabulka popisující binární relace $R \lhd S$, $R \rhd S$ a $R \square S$ mezi pacienty a nemocemi (viz Příklad 2.20).

2.3.4 Binární relace a jejich reprezentace

Průvodce studiem

Chceme-li matematické pojmy zpracovávat v počítači, je třeba je vhodným způsobem v počítači reprezentovat. Musíme tedy navrhnout, jak by měl být matematický pojem (množina, relace apod.) v počítači (tj. v paměti počítače) uložen. Nejde ale jen o samotné uložení v paměti, nýbrž také o to, aby výpočty, které budou s danými pojmy prováděny, byly rychlé.

Matematické pojmy je třeba umět vhodně reprezentovat. Zvlášť důležitá je reprezentace v paměti počítače.

V této kapitole si ukážeme základní způsoby reprezentace binárních relací. Předpokládejme, že je dána binární relace R mezi konečnými množinami X a Y.

Reprezentace maticí (tabulkou)

Připomeňme, že matice typu $m \times n$ je obdélníkové schéma o m řádcích a n sloupcích, ve kterém se na každém místě odpovídajícím nějakému řádku a nějakému sloupci nachází nějaká (zpravidla číselná) hodnota. Označme takovou matici $\mathbf{M}$. Pro každé $i \in \{1, \ldots, m\}$ a $j \in \{1, \ldots, n\}$ označme m_{ij} prvek matice z průsečíku řádku i a sloupce j.

Průvodce studiem

Matice typu $m \times n$ je to samé co tabulka o m řádcích a n sloupcích. Rozdíl je jen v tom, že matice mají specifický způsob zápisu a že s maticemi jsou definovány různé standardní operace. Pojem matice používají matematici a inženýři, zvlášť když se s údaji zanesenými v matici budou provádět další operace. Pojem tabulka používá každý, kdo chce přehledným způsobem zapsat údaje o nějakých položkách (viz tabulkové procesory, nabídkové katalogy apod.).

Tabulky a matice představují základní způsob reprezentace binárních relací. Nechť R je relace mezi množinami $X = \{x_1, \ldots, x_m\}$ a $Y = \{y_1, \ldots, y_n\}$. Relaci R reprezentujeme tabulkou/maticí, ve které se na místě odpovídajícím řádku i a sloupci j nachází hodnota, která určuje, zda dvojice $\langle x_i, y_j \rangle$ je v relaci R. Obvykle se používá 1 (popř. ×) k označení $\langle x_i, y_j \rangle \in R$ a 0 (popř. prázdné místo) k označení $\langle x_i, y_j \rangle \notin R$. Matice $\mathbf{M}_R$ reprezentující relaci $R \subseteq \{x_1, \ldots, x_m\} \times \{y_1, \ldots, y_n\}$ je definována předpisem

Relaci lze reprezentovat maticoví (tabulkou).

R	1	2	3	4
a	×	×		×
b		×		×
c	×			

$$\mathbf{M}_R = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Tabulka 11: Tabulka (vlevo) a matice (vpravo) popisující binární relaci R mezi $X = \{a, b, c\}$ a $Y = \{1, 2, 3, 4\}$.

$$m_{ij} = \begin{cases} 1 & \text{je-li } \langle x_i, y_j \rangle \in R, \\ 0 & \text{je-li } \langle x_i, y_j \rangle \notin R. \end{cases} \tag{2.1}$$

$\mathbf{M}_R$ se nazývá *matice relace* R. Naopak také, každá binární matice $\mathbf{M}$ typu $m \times n$, tj. matice s hodnotami 0 a 1, reprezentuje relaci mezi $X = \{x_1, \ldots, x_m\}$ a $Y = \{y_1, \ldots, y_n\}$.

Příklad 2.21. V Tab. 11 vidíme tabulkovou a maticovou reprezentaci relace

$$R = \{\langle a, 1\rangle, \langle a, 2\rangle, \langle a, 4\rangle, \langle b, 2\rangle, \langle b, 4\rangle, \langle c, 1\rangle\}$$

mezi $X = \{a, b, c\}$ a $Y = \{1, 2, 3, 4\}$.

Maticová reprezentace je názorná. Její nevýhodou je velká paměťová náročnost.

Výhodou této reprezentace je přehlednost a to, že zjistit, zda $\langle x_i, y_j \rangle \in R$, lze rychle. Nevýhodou je paměťová náročnost. Např. pro reprezentaci relace na množině X s 1000 prvky zabírá je odpovídající matice rozměru 1000×1000 a má tedy 1000000 políček. V případě, že každý prvek z X je v relaci s (průměrně) 3 prvky z Y, obsahuje matice 3 tisíce jedniček a zbytek (997 tisíc) jsou nuly. Přitom uchovávat nuly je zbytečné, stačilo by uchovat informaci o tom, kde mají být jedničky. Pro takové případy se používají jiné reprezentace.

Pro binární matice můžeme zavést operace, které odpovídají operacím s relacemi. Mějme binární matice $\mathbf{M}, \mathbf{N}$ typu $m \times n$ a matici $\mathbf{K}$ typu $n \times k$. Definujme následující operace.

$$\begin{aligned}
&\mathbf{M} \vee \mathbf{N} = \mathbf{P}, && p_{ij} = \max\{m_{ij}, n_{ij}\} \\
&\mathbf{M} \wedge \mathbf{N} = \mathbf{P}, && p_{ij} = \min\{m_{ij}, n_{ij}\} \\
&\mathbf{M} - \mathbf{N} = \mathbf{P}, && p_{ij} = \max\{0, m_{ij} - n_{ij}\} \\
&\mathbf{M} \cdot \mathbf{K} = \mathbf{P}, && p_{ij} = \max\{m_{il} \cdot k_{lj};\ l = 1, \ldots, n\} \\
&\mathbf{M}^T, && m^T_{ij} = m_{ji}\,.
\end{aligned}$$

Například operace $\vee$ přiřazuje maticím $\mathbf{M}$ a $\mathbf{N}$ matici $\mathbf{P}$, jejíž každý prvek p_{ij} je roven minimu z hodnot m_{ij} a n_{ij}.

Operace s relacemi lze provádět pomocí vhodných operací s maticemi.

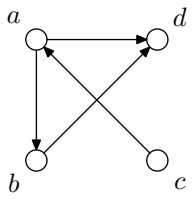
Věta 2.22. *Pro relace $R, S \subseteq X \times Y$, $U \subseteq Y \times Z$ je*

$$\begin{aligned}
\mathbf{M}_{R \cup S} &= \mathbf{M}_R \vee \mathbf{M}_S \\
\mathbf{M}_{R \cap S} &= \mathbf{M}_R \wedge \mathbf{M}_S \\
\mathbf{M}_{R - S} &= \mathbf{M}_R - \mathbf{M}^S \\
\mathbf{M}_{R \circ U} &= \mathbf{M}_R \cdot \mathbf{M}_U \\
\mathbf{M}_{R^{-1}} &= (\mathbf{M}_R)^T
\end{aligned}$$

Důkaz. Důkaz je jednoduchý. Stačí porovnat definice operací s maticemi a definice operací s relacemi. □

Příklad 2.23. Na množině $X = \{a_1, a_2, a_3, a_4\}$ uvažujme relace $R = \mathrm{id}_X \cup \{\langle a_1, a_2\rangle, \langle a_1, a_3\rangle, \langle a_3, a_2\rangle\}$ a $S = \{\langle a_1, a_1\rangle, \langle a_2, a_4\rangle, \langle a_3, a_4\rangle, \langle a_4, a_1\rangle\}$. Přitom $\mathrm{id}_X = \{\langle a_1, a_1\rangle, \ldots, \langle a_6, a_6\rangle\}$. Matice těchto relací jsou

$$\mathbf{M}_R = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{a} \quad \mathbf{M}_S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$



Obrázek 2: Graf relace k Příkladu 2.24.

Matice relace $R \cup S$ je

$$\mathbf{M}_R \vee \mathbf{M}_S = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} .$$

Matice relace $R \cap S$ je

$$\mathbf{M}_R \wedge \mathbf{M}_S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} .$$

Matice relace $R \circ S$ je

$$\mathbf{M}_R \cdot \mathbf{M}_S = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} .$$

Matice relace R_{-1} je

$$(\mathbf{M}_R)^T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

Reprezentace grafem

Grafy představují další způsob reprezentace binárních relací, který je názorný. Graf binární relace R na množině X dostaneme tak, že každý prvek $x \in X$ znázorníme v rovině jako kroužek s označením daného prvku. Pokud $\langle x, y\rangle \in R$, nakreslíme z kroužku odpovídajícího x do kroužku odpovídajícího y orientovanou čáru s šipkou.

Relace na množině lze graficky znázornit pomocí tzv. grafů.

Příklad 2.24. Na Obr. 2 vidíme graf reprezentující binární relaci $R = \{\langle a, b\rangle, \langle a, d\rangle, \langle c, a\rangle, \langle b, d\rangle\}$ na množině $X = \{a, b, c, d\}$.

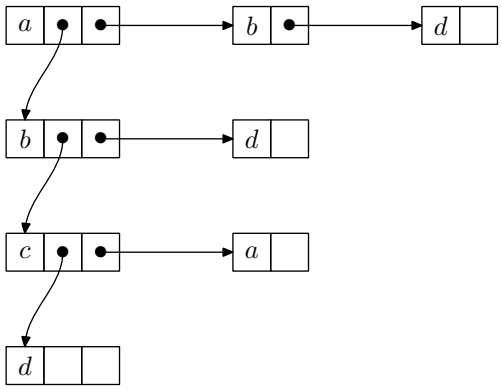
Upozorněme už teď, že graf je jedním ze základních pojmů diskrétní matematiky. Grafy se budeme zabývat v Kapitole **??**. V tomto smyslu používáme v této kapitole pojem graf nepřesně. Podobně jak jsme ukázali, je možné reprezentovat i relace R *mezi* X a Y. Čtenář nechť si detaily rozmyslí sám.

Reprezentace seznamem seznamů

Tento způsob reprezentace je vhodný pro uložení binární relace R na množině X v paměti počítače. Na Obr. 3 je znázorněna reprezentace relace R z Příkladu 2.24 seznamem seznamů. Reprezentaci tvoří hlavní (spojový) seznam[5], ve kterém jsou uloženy všechny prvky množiny X. Na Obr. 3 je hlavní seznam znázorněn shora dolů spojenými čtverečky, které obsahují $a, \ldots, d$. Z každého prvku $x \in X$ hlavního seznamu vede seznam obsahující právě ty $y \in X$, pro které $\langle x, y\rangle \in R$. Na Obr. 3 jsou tyto seznamy znázorněny vodorovně. Např. z prvku a hlavního seznamu vede seznam obsahující b a d. To proto, že $\langle a, b\rangle \in R$ a $\langle a, d\rangle \in R$. Z prvku d nevede žádný seznam (tj. z d vede prázdný seznam), protože neexistuje $y \in X$ tak, že $\langle d, y\rangle \in R$.

Reprezentace seznamem seznamů je paměťově úsporná a je vhodná pro počítačové zpracování.

[5] Spojový seznam je jednou ze základních datových struktur. Blíže viz jakoukoli učebnici algoritmů a datových struktur.



Obrázek 3: Relace R z Příkladu 2.24 reprezentovaná seznamem seznamů.

Vraťme se k relaci na množině X s 1000 prvky, kde každý prvek je v relaci s průměrně 3 prvky. Při reprezentaci seznamem seznamů budeme potřebovat 1000 políček pro prvky hlavního seznamu a pro každý z těchto prvků 3 další políčka pro prvky seznamu, který z tohoto prvky vede. To je celkem 4000 políček. Započítáme-li, že v každém políčku je třeba mít nejen označní prvku, ale i ukazatel na další políčko, je třeba zhruba 2×4000 paměťových buněk. Připomeňme, že maticová reprezentace takové relace vyžaduje 1000000 paměťových buněk[6].

2.4 Binární relace na množině

PODROBNE INFORMACE KE KAPITOLE 2.5 LZE NAJIT V TEXTU Bělohlávek R., Vychodil V.: Diskrétní matematika 1, který je dostupný na http://phoenix.inf.upol.cz/esf/ucebni/DM1.pdf.

2.4.1 Vlastnosti binárních relací na množině

reflexivita, symetrie, antisymetrie, tranzitivita

2.4.2 Ekvivalence

ekvivalence a rozklady

2.4.3 Uspořádání

(částečné) uspořádání, základní pojmy, Hasseovy diagramy

2.5 Funkce (zobrazení)

2.5.1 Pojem funkce

Funkce je matematickým protějškem běžně používaného pojmu *přiřazení*. Objektům jsou často jednoznačným způsobem přiřazovány další objekty. Např. funkce sinus přiřazuje každému reálnému číslu x hodnotu $\sin(x)$, zaměstnancům jsou v rámci společnosti, kde pracují, přiřazována identifikační čísla apod. Takové přiřazení je možné chápat jako množinu dvojic $\langle x, y\rangle$, kde y je objekt přiřazený objektu x. Přiřazení je tedy možné chápat jako binární relaci mezi množinou X objektů, kterým jsou přiřazovány objekty, a množinou Y objektů, které jsou objektům z X přiřazovány. Taková relace R má díky jednoznačnosti přiřazení následující speciální vlastnost: je-li $\langle x, y_1\rangle \in R$ (objektu x je přiřazen objekt y_1) a $\langle x, y_2\rangle \in R$ (objektu x je přiřazen

[6]Celá tato úvaha je zjednodušená, ale ilustruje podstatu věci.

objekt y_2), pak $y_1 = y_2$ (jednoznačnost přiřazeného objektu, objektu x nemohou být přiřazeny dva různé objekty). To vede k následující definici.

Definice 2.25. Relace R mezi X a Y se nazývá *funkce* (někdy také *zobrazení*) množiny X do množiny Y, právě když pro každé $x \in X$ existuje $y \in Y$ tak, že

$$\langle x, y\rangle \in R,$$

a pro každé $x \in X$ a $y_1, y_2 \in Y$ platí, že

$$\langle x, y_1\rangle \in R \text{ a } \langle x, y_2\rangle \in R \text{ implikuje } y_1 = y_2.$$

Fakt, že R je funkce X do Y, označujeme $R : X \to Y$. Pro funkce používáme spíš $f, g, \ldots$ než $R, S, \ldots$. Je-li $f : X \to Y$ funkce a $x \in X$, pak ten $y \in Y$, pro který je $\langle x, y\rangle \in f$, označujeme $f(x)$, píšeme také $x \mapsto y$, popř. $x \mapsto f(x)$.

Příklad 2.26. Uvažujme množiny $X = \{a, b, c\}$, $Y = \{a, b, 1, 2\}$.

- Relace $R = \{\langle a, a\rangle, \langle b, b\rangle\}$ není funkce X do Y, protože k prvku $c \in X$ neexistuje prvek $y \in Y$ tak, že $\langle x, y\rangle \in R$.
- Relace $R = \{\langle a, a\rangle, \langle b, 2\rangle, \langle c, a\rangle, \langle c, 2\rangle\}$ není funkce X do Y, protože k prvku $c \in X$ existují dva různé prvky, které jsou s ním v relaci R. Máme totiž $\langle c, a\rangle \in R$, $\langle c, 2\rangle \in R$, ale $a \neq 2$.
- Relace $R = \{\langle a, 2\rangle, \langle b, b\rangle, \langle c, 2\rangle\}$ je funkce X do Y.

Relace $R \subseteq X \times Y$, která splňuje když $\langle x, y_1\rangle \in R$ a $\langle x, y_2\rangle \in R$, pak $y_1 = y_2$ se někdy nazývá *parciální* (částečná) *funkce*.

Někdy se používá obrat „uvažujme funkci $y = f(x)$“, kde $f(x)$ je nějaký výraz, např. $y = x^2$ apod. Přitom se má za to, že je jasné, o jaké množiny X a Y se jedná (často je $X = Y = \mathbb{R}$, popř. $X \subseteq \mathbb{R}$). Pak jde vlastně o funkci $\{\langle x, y\rangle \mid x \in X, y \in Y, y = f(x)\}$.

2.5.2 Typy funkcí

Definice 2.27. Funkce $f : X \to Y$ se nazývá

- *prostá* (někdy také *injektivní*), právě když pro každé $x_1, x_2 \in X$, že z $x_1 \neq x_2$ plyne $f(x_1) \neq f(x_2)$,
- funkce množiny X *na* množinu Y (někdy také *surjektivní*), právě když pro každé $y \in Y$ existuje $x \in X$ tak, že $f(x) = y$,
- *vzájemně jednoznačná* (někdy také *bijektivní*), právě když je prostá a je to funkce na množinu Y (tj. injektivní a surjektivní).

Funkce je tedy prostá, právě když z $f(x_1) = f(x_2)$ plyne $x_1 = x_2$.

Příklad 2.28.
- Pro $X = \{a, b, c, d\}$ a $Y = \{1, 2, 3, 4\}$ je $f = \{\langle a, 1\rangle, \langle b, 1\rangle, \langle c, 4\rangle, \langle d, 3\rangle\}$ funkce X do Y. f není injektivní (protože $f(a) = f(b)$, ale $a \neq b$), ani surjektivní (neexistuje $x \in X$ tak, aby $f(x) = 2$), a tedy ani bijektivní.
- Pro $X = \{a, b\}$ a $Y = \{1, 2, 3\}$ je $f = \{\langle a, 1\rangle, \langle b, 3\rangle\}$ funkce X do Y, která je injektivní, ale není surjektivní (neexistuje $x \in X$ tak, aby $f(x) = 2$), a tedy ani bijektivní.
- Pro $X = \{a, b, c\}$ a $Y = \{1, 2\}$ je $f = \{\langle a, 2\rangle, \langle b, 2\rangle, \langle c, 1\rangle\}$ funkce X do Y, která není injektivní (protože $f(a) = f(b)$, ale $a \neq b$), ale je surjektivní, a tedy není bijektivní.
- Pro $X = \{a, b, c\}$ a $Y = \{1, 2, 3\}$ je $f = \{\langle a, 2\rangle, \langle b, 1\rangle, \langle c, 3\rangle\}$ funkce X do Y, která je injektivní i surjektivní, a i bijektivní.

Příklad 2.29. Podívejte se na následující funkce.

- $f = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$ je funkce $\mathbb{R}$ do $\mathbb{R}$, která není injekce (např. $(-2)^2 = 2^2$) ani surjekce (např. neexistuje $x \in \mathbb{R}$ tak, že $x^2 = -1$). Uvažujeme-li ji však jako funkci množiny $\mathbb{R}$ do množiny $\{a \in \mathbb{R} \mid a \geq 0\}$ (nezáporná reálná čísla), je to surjekce.
- $f = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} \mid y = x^3\}$ je funkce $\mathbb{R}$ do $\mathbb{R}$, která je injekcí i surjekcí, tj. je bijekcí.
- $f = \{\langle x, y\rangle \in \mathbb{N} \times \mathbb{N} \mid y = x!\}$ je funkce $\mathbb{N}$ do $\mathbb{N}$ (faktoriál, tj. $x! = x \cdot (x-1) \cdots 2 \cdot 1$). Je to injekce, ale ne surjekce (např. číslo 3 není faktoriálem žádného čísla, tj. neexistuje $x \in \mathbb{N}$ tak, že $x! = 3$).

Podívejme se na některé vlastnosti funkcí.

Věta 2.30. *Pro funkce $f, f_1, f_2 : X \to Y$, $g, g_1, g_2 : Y \to Z$ platí*

a) $f \circ g$ je funkce.
b) Jsou-li f, g injekce, je $f \circ g$ injekce.
c) Jsou-li f, g surjekce, je $f \circ g$ surjekce.

Důkaz. Dokažme *a*). Nejprve musíme ukázat, že pro každé $x \in X$ existuje $z \in Z$ tak, že $\langle x, z\rangle \in f \circ g$. Protože je f funkce, existuje k $x \in X$ prvek $y \in Y$ tak, že $\langle x, y\rangle \in f$, a protože je g funkce, existuje k tomu y prvek $z \in Z$ tak, že $\langle y, z\rangle \in g$. Podle definice je tedy $\langle x, z\rangle \in f \circ g$. Nyní musíme ukázat, že když $\langle x, z_1\rangle \in f \circ g$ a $\langle x, z_2\rangle \in f \circ g$, pak $z_1 = z_2$. Když $\langle x, z_1\rangle \in f \circ g$ a $\langle x, z_2\rangle \in f \circ g$, pak podle definice pro nějaké $y_1, y_2 \in Y$ je $\langle x, y_1\rangle \in f$, $\langle y_1, z_1\rangle \in g$, a $\langle x, y_2\rangle \in f$, $\langle y_2, z_2\rangle \in g$. Protože f je funkce, musí být $y_1 = y_2$, a protože g je funkce, musí být $z_1 = z_2$. Tedy *a*) platí.

Dokažme *b*). Je-li $\langle x_1, z\rangle \in f \circ g$, $\langle x_2, z\rangle \in f \circ g$, existují $y_1, y_2 \in Y$ tak, že $\langle x_1, y_1\rangle \in f$, $\langle x_2, y_2\rangle \in f$, $\langle y_1, z\rangle \in g$, $\langle y_2, z\rangle \in g$. Protože g je injekce, platí $y_1 = y_2$. Platí tedy $\langle x_1, y_1\rangle \in f$, $\langle x_2, y_1\rangle \in f$, a protože f je injekce, je $x_1 = x_2$, tedy $f \circ g$ je injekce.

c) se dokáže podobně. □

2.5.3 Princip indukce

Princip (matematické) indukce umožňuje dokazovat tvrzení tvaru „pro každé přirozené číslo n platí $V(n)$“, kde $V(n)$ je nějaké tvrzení, které závisí na n (např. $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$).

Věta 2.31 (princip indukce)**.** *Nechť je pro každé $n \in \mathbb{N}$ dáno tvrzení $V(n)$. Předpokládejme, že platí*

- *$V(1)$ (indukční předpoklad),*
- *pro každé $n \in \mathbb{N}$: z $V(n)$ plyne $V(n+1)$ (indukční krok).*

Pak $V(n)$ platí pro každé $n \in \mathbb{N}$.

Princip indukce je jednou ze základních vlastností přirozených čísel. Z předpokladu, že každá neprázdná podmnožina $K \subseteq \mathbb{N}$ má nejmenší prvek (což je pravdivý a intuitivně jasný předpoklad) lze princip indukce dokázat.

Důkaz. Princip indukce dokážeme sporem. Předpokládejme, že princip indukce neplatí, tj. existují tvrzení $V(n)$ ($n \in \mathbb{N}$), které splňují oba předpoklady principu indukce, ale pro nějaké $n' \in \mathbb{N}$ tvrzení $V(n')$ neplatí. Označme $K = \{m \in \mathbb{N} \mid V(m) \text{ neplatí}\}$ množinu všech takových n'. K je tedy neprázdná (neboť $n' \in K$). K má tedy nejmenší prvek k (viz poznámka před důkazem) a ten je různý od 1 (protože podle indukčního předpokladu $1 \notin K$). Pak tedy $k - 1 \notin K$, tedy $V(k-1)$ platí. Z indukčního kroku plyne, že platí i $V(k)$, tedy $k \notin K$, což je spor s $k \in K$. □

Příklad 2.32. Dokažme už uvedený vztah $1+2+\cdots+n = \frac{n(n+1)}{2}$. Tedy $V(n)$ je tvrzení $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$. Podle principu indukce stačí ověřit indukční předpoklad a indukční krok.

Indukční předpoklad: $V(1)$ je tvrzení $1 = \frac{1 \cdot (1+1)}{2}$, a to evidentně platí.

Indukční krok: Předpokládejme, že platí $V(n)$ a dokažme $V(n+1)$. $1 + \cdots + n + n + 1$ se rovná $(1 + \cdots + n) + n + 1$, což se dle předpokladu rovná $\frac{n(n+1)}{2} + n + 1$. Dále je $\frac{n(n+1)}{2} + n + 1 = \frac{n(n+1)+2(n+1)}{2} = \frac{n^2+3n+2}{2} = \frac{(n+1)\cdot(n+1)}{2}$. Celkem tedy $1 + \cdots + n + n + 1 = \frac{(n+1)\cdot(n+1)}{2}$, což je právě tvrzení $V(n+1)$.

Podle principu indukce je tedy tvrzení dokázané.

2.5.4 Konečné, spočetné a nespočetné množiny

Množina A se nazývá *konečná*, právě když prázdná ($A = \emptyset$) nebo existuje přirozené číslo n a bijekce $f : A \to \{1, 2, \ldots, n\}$. V prvním případě říkáme, že počet prvků množiny A je 0. Ve druhém případě říkáme, že počet prvků množiny A je n.

Příklad 2.33. Je tedy $|\emptyset| = 0$. Množiny $A = \{2, 4, 6\}$, $B = \{n \in \mathbb{N} \mid n \leq 10000000 \text{ a } n \text{ je sudé}\}$ jsou konečné a je $|A| = 3$, $|B| = 5000000$.

Množina A se nazývá *nekonečná*, právě když není konečná. Množina A se nazývá *spočetná*, právě když bijekce $f : A \to \mathbb{N}$. Množina A se nazývá *nespočetná*, právě když je nekonečná a není spočetná.

Poznámka 2.34. (1) Protože pro žádné $n \in \mathbb{N}$ neexistuje bijekce $f : \{1, \ldots, n\} \to \mathbb{N}$, je každá spočetná množina nekonečná.

(2) Z definice plyne, že každá nekonečná množina je buď spočetná, nebo nespočetná.

Příklad 2.35. Množiny $A = \{2, 4, 6, 8, \ldots\}$, $B = \{2, 2^2, 2^{(2^2)}, 2^{(2^{(2^2)})}, \cdots\}$, $B = \mathbb{Z}$, $C = \mathbb{Q}$, $D = \mathbb{R}$, $E = [0, 1]$ jsou nekonečné. Přitom A, B, C jsou spočetné a D a E jsou nespočetné.

Shrnutí

Kartézský součin množin $X_1, \ldots, X_n$ je množina všech uspořádaných n-tic prvků z těchto množin. Relace mezi množinami $X_1, \ldots, X_n$ je libovolná podmnožina kartézského součinu těchto množin. S relacemi lze provádět všechny množinové operace. S binárními relacemi lze provádět operace inverze a skládání. Binární relace se nejčastěji reprezentují tabulkou nebo grafem, v paměti počítače pak maticí nebo seznamem seznamů.
Funkce je zvláštní typ relace. Injekce, surjekce a bijekce jsou speciální typy funkcí.
Princip indukce slouží k prokázání toho, že daný výrok platí pro všechna přirozená čísla.

Pojmy k zapamatování

- kartézský součin,
- relace, binární relace, inverzní relace, skládání binárních relací, reprezentace binárních relací,
- funkce, injekce, surjekce, bijekce,
- princip indukce.

Kontrolní otázky

1. *Je pravda, že každá neprázdná n-ární relace má aspoň n prvků? Proč?*
2. *Jaká je inverzní relace k relaci „být otcem“ na množině všech lidí (slovně ji popište)? Je-li R výše uvedená relace „být otcem“, co je relací $R \circ R$? Co jsou relace $R \lhd R$, $R \rhd R$?*
3. *Jaký je rozdíl mezi tabulkovou a maticovou reprezentací binární relace?*
4. *Nechť X a Y jsou množiny. Jaký vztah musí platit mezi $|X|$ a $|Y|$ pro to, aby existovala funkce $f : X \to Y$, která je injekcí, surjekcí, bijekcí?*
5. *Může být prázdná množina funkcí X do Y? Rozeberte v závislosti na mnžinách X a Y.*

Cvičení

1. Dokažte následující vztahy.

$$\begin{aligned}
A \times B = \emptyset, \text{ právě když } A = \emptyset \text{ nebo } B = \emptyset \\
A \times B = B \times A, \text{ právě když } A \times B = \emptyset \text{ nebo } A = B \\
A \times (B \cup C) = (A \times B) \cup (A \times C) \\
(A \cup B) \times C = (A \times C) \cup (B \times C) \\
A \times (B \cap C) = (A \times B) \cap (A \times C) \\
(A \cap B) \times C = (A \times C) \cap (B \times C) \\
A \times (B - C) = (A \times B) - (A \times C) \\
(A - B) \times C = (A \times C) - (B \times C)
\end{aligned}$$

2. Najděte příklady relací, pro které platí (neplatí) $R \circ S = S \circ R$, $R^{-1} = R$.
3. Dokažte, že pro relace $R, R_1, R_2, U \subseteq X \times Y,\ S, S_1, S_2, V \subseteq Y \times Z,\ T \subseteq Z \times W$ platí

$$\begin{aligned}
(R^{-1})^{-1} = R \\
(R \circ S) \circ T = R \circ (S \circ T) \\
(R \circ S)^{-1} = S^{-1} \circ R^{-1} \\
\text{Je-li } R \subseteq U, S \subseteq V, \text{ pak } R \circ S \subseteq U \circ V \\
(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1} \\
(R_1 \cap R_2)^{-1} = R_1^{-1} \cap R_2^{-1} \\
R \circ (S_1 \cup S_2) = R \circ S_1 \cup R \circ S_2 \\
R \circ (S_1 \cap S_2) = R \circ S_1 \cap R \circ S_2 \\
(R_1 \cup R_2) \circ S = R_1 \circ S \cup R_2 \circ S \\
(R_1 \cap R_2) \circ S = R_1 \circ S \cap R_2 \circ S
\end{aligned}$$

4. Které z následujících relací R jsou funkce X do Y?
   a) $X = Y = \mathbb{N}$, $R = \{\langle m, n\rangle \mid m \neq n\}$,
   b) $X = Y = \{a, b, c\}$, $R = \{\langle a, a\rangle, \langle a, b\rangle, \langle a, c\rangle\}$,
   c) $X = Y = \{a, b, c\}$, $R = \{\langle a, a\rangle, \langle b, a\rangle, \langle c, a\rangle\}$,
   d) X je množina všech českých slov, Y je množina všech písmen české abecedy $\{\langle w, l\rangle \mid w$ je české slovo s posledním písmenem $l\}$,
   e) $X = Y = \mathbb{R}$, $R = \{\langle x, y\rangle \mid x^2 + y^2 = 1\}$,
   f) $X = Y = \mathbb{R}$, $R = \{\langle x, y\rangle \mid x^2 = y\}$,
   g) $X = Y = \mathbb{R}$, $R = \{\langle x, y\rangle \mid x = y^2\}$.
5. Které z následujících funkcí jsou injektivní? Které jsou surjektivní?
   a) $f : N \to N$, $f(n) = n + 1$,
   b) $f : Z \to Z$, $f(i) = i + 1$,
   c) $f : K \to K$, kde $K = \{1, 2, \ldots, k\}$,

$$f(i) = \begin{cases} i + 1 & \text{pro } 1 \leq i < k \\ 1 & \text{pro } i = k \end{cases}$$

   d) $f : N \to \{0, 1, 2, 3\}$, kde

$$f(i) = \begin{cases} 0 & \text{jestliže } i \text{ je dělitelné 5, ale ne 11,} \\ 1 & \text{jestliže } i \text{ je dělitelné 11, ale ne 5,} \\ 2 & \text{jestliže } i \text{ je dělitelné 55,} \\ 3 & \text{v ostatních případech,} \end{cases}$$

   e) $f : Q \to Q$, $f(i) = i^3$.
6. Najděte příklady funkcí f a g tak, aby

a) g nebyla injekce, ale $f \circ g$ ano,

b) f nebyla surjekce, ale $f \circ g$ ano.

7. Pro množinu U nechť je $\mathrm{id}_U = \{\langle u, u\rangle \mid u \in U\}$ relace identita. Ukažte, že pro relaci $f \subseteq X \times Y$ platí

   a) f splňuje, že z $\langle x, y_1\rangle \in f$ a $\langle x, y_2\rangle \in f$ plyne $y_1 = y_2$, právě když $f^{-1} \circ f \subseteq \mathrm{id}_Y$,

   b) je-li f funkce X do Y, pak je injektivní, právě když $f \circ f^{-1} = \mathrm{id}_X$.

   c) Je-li f funkce X do Y, pak je surjektivní, právě když $f^{-1} \circ f = \mathrm{id}_Y$.

8. Mějme $f : X \to Y$. Pro $A \subseteq X$ a $B \subseteq Y$ označme $f(A) = \{f(x) \mid x \in A\}$ a $f_{-1}(B) = \{x \in X \mid f(x) \in B\}$. Ukažte, že

   a) f je injektivní, právě když f^{-1} splňuje, že z $\langle x, y_1\rangle \in f$ a $\langle x, y_2\rangle \in f$ plyne $y_1 = y_2$,

   b) je-li f injektivní, pak pro každé $A, B \subseteq X$ platí $f(A \cap B) = f(A) \cap f(B)$, $f(A - B) = f(A) - f(B)$.

   c) pro každé $A, B \subseteq Y$ $f_{-1}(A \cap B) = f_{-1}(A) \cap f_{-1}(B)$, $f_{-1}(A - B) = f_{-1}(A) - f_{-1}(B)$.

9. Ukažte, že není-li f injektivní, neplatí bod b) z předchozího cvičení.
10. Dokažte, že pro funkce $f, f_1, f_2 : X \to Y$, $g, g_1, g_2 : Y \to Z$ platí, že

    a) je-li $f \circ g$ injekce, je f injekce,

    b) je-li $f \circ g$ surjekce, je g surjekce,

    c) je-li g injekce $f_1 \circ g = f_2 \circ g$, je $f_1 = f_2$,

    d) je-li f surjekce $f \circ g_1 = f \circ g_2$, je $g_1 = g_2$.

11. Dokažte indukcí, že $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.
12. Dokažte indukcí, že $\sum_{k=1}^{n} k^3 = [\frac{n(n+1)}{2}]^2$.
13. Dokažte indukcí, že pro $n \in \mathbb{N}$ je $2^{n+2} + 3^{2n+1}$ dělitelné 7.
14. Dokažte, že pro $n \in \mathbb{N}$ je $(1 + \frac{1}{3})^n \geq 1 + \frac{n}{3}$.
15. Kde je chyba v následujícím „důkazu“ indukcí? *Tvrzení.* V pro každou posloupnost n prvků $a_1, \ldots, a_n$ platí, že všechny prvky v ní jsou stejné.
    Důkaz. Pro číslo 1 je tvrzení triviálně splněno. Předpokládejme, že tvrzení platí pro k prvků. Uvažujme posloupnost libovolných $k + 1$ prvků $a_1, \ldots, a_{k+1}$. Pak $a_1, \ldots, a_k$ je posloupnost k prvků a $a_2, \ldots, a_{k+1}$ je posloupnost k prvků, a podle předpokladu tedy $a_1 = \cdots = a_k$ a $a_2 = \cdots = a_{k+1}$. Odtud plyne $a_1 = \cdots = a_{k+1}$.

Úkoly k textu

1. Vraťme se k pojmu uspořádaná dvojice prvků. Tento pojem jsme chápali jako základní, tj. nedefinovaný. Je ho však možné definovat pomocí pojmu množina tak, že bude mít všechny požadované vlastnosti. Řekněme, že uspořádaná dvojice prvků a, b je množina $\langle a, b\rangle = \{a, \{a, b\}\}$. Ukažte, že $\langle a, b\rangle = \langle c, d\rangle$, právě když $a = c$ a $b = d$.
2. Dokažte zbývající části Věty 2.9
3. Dokažte Větu 2.22.
4. Ukažte, že pro konečné množiny X a Y existuje bijekce X do Y, právě když X a Y mají stejný počet prvků.
5. Dokažte bod c) z Věty 2.30.

Řešení

1. Vztahy se dokážou jednoduše, rozepsáním přímo podle definice.
2. Mějme např. $X = Y = \{x, y, z\}$. $R \circ S = S \circ R$ platí pro $R = \{\langle x, y\rangle, \langle z, y\rangle\}$, $S = \{\langle y, x\rangle, \langle y, z\rangle\}$, neplatí pro $R = \{\langle x, y\rangle\}$, $S = \{\langle y, z\rangle\}$.
   $R^{-1} = R$ platí např. pro $R = \{\langle x, y\rangle, \langle y, x\rangle\}$, neplatí např. pro $R = \{\langle x, z\rangle\}$.

3. Vztahy se dokážou jednoduše, rozepsáním přímo podle definice.
4. Funkcemi jsou relace R z c), d), f).
5. Injekce: a), b), c), e), surjekce: b), c), d).
6. Vezměme $X = \{x\}$, $Y = \{y_1, y_2\}$, $Z = \{z\}$. $f = \{\langle x, y_1\rangle\}$, $g = \{\langle y_1, z\rangle, \langle y_2, z\rangle\}$ splňují a) i b).
7. a) Nechť f splňuje, že z $\langle x, y_1\rangle \in f$ a $\langle x, y_2\rangle \in f$ plyne $y_1 = y_2$. Když $\langle y_1, y_2\rangle \in f^{-1} \circ f$, pak existuje $x \in X$ tak, že $\langle y_1, x\rangle \in f^{-1}$ a $\langle x, y_2\rangle \in f$, tj. $\langle x, y_1\rangle \in f$ a $\langle x, y_2\rangle \in f$. Z předpokladu plyne $y_1 = y_2$, tj. $f^{-1} \circ f \subseteq \mathrm{id}_Y$.
Naopak, nechť $f^{-1} \circ f \subseteq \mathrm{id}_Y$. Nechť $\langle x, y_1\rangle \in f$ a $\langle x, y_2\rangle \in f$. Pak $\langle y_1, y_2\rangle \in f^{-1} \circ f \subseteq \mathrm{id}_Y$. Protože $f^{-1} \circ f \subseteq \mathrm{id}_Y$, je $\langle y_1, y_2\rangle \in \mathrm{id}_Y$, tj. $y_1 = y_2$. Tedy z z $\langle x, y_1\rangle \in f$ a $\langle x, y_2\rangle \in f$ plyne $y_1 = y_2$.
b) a c) se dokážou podobnými úvahami.
8. a) přímo z definice.
b) $f(A \cap B) = f(A) \cap f(B)$: Protože $A \cap B \subseteq A$ i $A \cap B \subseteq B$, je dle definice $f(A \cap B) \subseteq f(A)$ i $f(A \cap B) \subseteq f(B)$. Z toho plyne $f(A \cap B) \subseteq f(A) \cap f(B)$. Naopak, pokud $y \in f(A) \cap f(B)$, pak existují $x_1 \in A$ a $x_2 \in B$ tak, že $f(x_1) = y$ a $f(x_2) = y$. Protože je f injekce, musí být $x_1 = x_2$. Tedy $x_1 \in A \cap B$, a proto $y \in f(A \cap B)$. Proto je $f(A) \cap f(B) \subseteq f(A \cap B)$.
$f(A - B) = f(A) - f(B)$: Nechť $y \in f(A - B)$, tj. existuje $x \in A - B$ tak, že $f(x) = y$. Proto je $y \in f(A)$. Kdyby $y \in f(B)$, pak existoval $x' \in B$ tak, že $f(x') = y$. Protože $x \in A - B$, je $x \neq x'$. To je ale spor s injektivitou f, protože máme $x \neq x'$ a $f(x) = y = f(x')$. Tedy je $y \in f(A) - f(B)$. Naopak, nechť $y \in f(A) - f(B)$. Pak $y = f(x)$ pro nějaký $x \in A$ a neexistuje $x' \in B$ tak, že $f(x') = y$. Proto je $x \in A - B$, a tedy $y \in f(A - B)$.
c) se dokáže podobnými úvahami.
9. Vezměme např. $X = \{x_1, x_2\}$, $Y = \{y\}$, funkci f danou předpisy $f(x_1) = y$, $f(x_2) = y$, množiny $A = \{x_1\}$, $B = \{x_2\}$. Pak $f(A \cap B) = \emptyset$ a $f(A) \cap f(B) = \{y\}$. Pro množiny $A = \{x_1, x_2\}$ a $B = \{x_2\}$ je $f(A - B) = f(\{x_1\}) = \{y\}$ a $f(A) = f(B) = \emptyset$.
10. Dokažme b). Kdyby g nebyla surjekce, pak by existoval $z \in Z$, kte kterému neexistuje $y \in Y$ tak, že $g(y) = z$. Proto nemůže existovat $x \in X$ tak, aby $f \circ g(x) = z$ (jinak by pro $y = f(x)$ bylo $g(y) = z$).
Dokažme d). Protože f je surjekce, existuje pro libovolný prvek $y \in Y$ prvek $x \in X$ tak, že $\langle x, y\rangle \in f$. Platí tedy $g_1(y) = g_1(f(x)) = f \circ g_1(x) = f \circ g_2(x) = g_2(f(x)) = g_2(y)$. Dokázali jsme, že pro libovolný prvek $y \in Y$ je $g_1(y) = g_2(y)$, tedy $g_1 = g_2$.
a) a c) se dokážou podobnými úvahami.
11. $V(n)$ je tvrzení $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$. $V(1)$ platí, protože je to tvrzení $1^2 = \frac{1(1+1)(2+1)}{6}$. Předpokládejme, že platí $V(n)$ a dokažme $V(n+1)$, tj. dokažme $\sum_{k=1}^{n+1} k^2 = \frac{(n+1)(n+2)(2(n+1)+1)}{6}$. Je $\sum_{k=1}^{n+1} k^2 = \sum_{k=1}^{n} k^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + \frac{6(n+1)^2}{6} = \frac{2n^3+9n^2+13n+6}{6} = \frac{(n+1)(n+2)(2(n+1)+1)}{6}$.
12. Jednoduché, standardně použitím jednoduchých úprav.
13. Jednoduché, standardně použitím jednoduchých úprav.
14. Jednoduché, standardně použitím jednoduchých úprav.
15. Chyba je v tom, že úvaha, kterou se z $V(k)$ dokáže $V(k+1)$, není správná pro $k = 1$, tj. neplatí, že z $V(1)$ plyne $V(2)$. Projděte si úvahu podrobně: tvrdí se v ní, že z toho, že v posloupnosti a_1 jsou všechny prvky stejné, a z toho, že v posloupnosti a_2 jsou všechny prvky stejné, plyne, že $a_1 = a_2$, což není pravda.

3 Čísla

Studijní cíle: Po prostudování kapitol by student měl rozumět základním pojmům které se týkají čísel a číselných oborů.

Klíčová slova: přirozená čísla, celá čísla, racionální čísla, reálná čísla, princip indukce, dělitelnost, prvočísla, číselné soustavy.

3.1 Přirozená, celá, racionální a reálná čísla

Předpokládáme, že čtenář má základní znalosti o číselných oborech. Budeme vycházet z geometrické představy o číslených oborech, která je dána rozmístěním čísel na číselné ose. Budeme pracovat s následujícími množinami čísel:

- *Přirozená čísla*. Jsou to čísla $1, 2, 3, 4, \ldots$. Množinu všech přirozených čísel označujeme $\mathbb{N}$.
- *Přirozená čísla*. Jsou to čísla $0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots$. Množinu všech přirozených čísel označujeme $\mathbb{Z}$.
- *Racionální čísla*. Jsou to čísla, která lze vyjádřit ve tvaru zlomku $\frac{m}{n}$, kde m je celé číslo a n je přirozené číslo. Množinu všech racionálních čísel označujeme $\mathbb{Q}$. Racionální čísla jsou tedy např. $\frac{1}{3}$, $-\frac{2}{5}$, $-\frac{20}{341}$, $-\frac{4}{10}$, atd. $\frac{1}{3}$, $\frac{2}{6}$, $\frac{6}{18}$ jsou různé zápisy téhož racionálního čísla. Rovněž $-\frac{4}{2}$, $\frac{10}{-5}$, -2 jsou různé zápisy téhož racionálního čísla. Raconální čísla zapisujeme také pomocí tzv. desetinného rozvoje. Např. číslo $\frac{3}{2}$ zapisujeme jako 1.5. Číslo $\frac{1}{3}$ má tzv. nekonečný desetinný rozvoj a jej jím $0.3333\ldots$, což také zapisujeme jako $0.\overline{3}$.
- *Reálná čísla*. Jsou to všechna čísla, která se nacházejí na číselné ose. Kromě racionálních čísel zahrnují reálná čísla i čísa tzv. iracionální. To jsou čísla, která nelze vyjádřit ve tvaru zlomku. Příkladem iracionálních čísel jsou $\sqrt{2}, \sqrt{2}, \pi, e$. Množinu všech reálnýchch čísel označujeme $\mathbb{R}$.

Je tedy

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Předpokládáme, že čtenář má základní znalosti o uspořádání čísel. Např. $1 < 2.8$ označuje, že číslo 1 je menší než číslo 2.8.

3.2 Princip indukce

Viz přednášky.

Princip dobrého uspořádání (každá neprázná podmnožina přirozených čísel má nejmenší prvek), důkaz matematickou indukcí, definice matematickou indikcí.

Základní informace a příklady lze najít v Kapitole 2.5.

3.3 Konečné, spočetné a nespočetné množiny

Viz přednášky.

Konečné množiny, nekonečné množiny, spočetné a nespočetné množiny, základní pravidla, nespočetnost množiny reálných čísel diagonální metodou.

Základní informace a příklady lze najít v Kapitole 2.5.

3.4 Dělitelnost a prvočísla

Definice 3.1. Pro $m, n \in \mathbb{Z}$ říkáme, že m *dělí* n, píšeme $m|n$, právě když existuje $k \in \mathbb{Z}$ tak že $m \cdot k = n$.

Když $m|n$, říkáme také, že m je dělitelem n nebo n je dělitelné m.

Příklad 3.2. $1|3$, $2|6$, $3|-6$, $-3|-6$, ale $4 \not| 2$, $-2 \not| 3$.

Věta 3.3. *Pro $a, b, c \in \mathbb{Z}$ platí*

1. *Jestliže $a|b$ a $b|c$, pak $a|c$.*
2. *Jestliže $a|b$ a $a|c$, pak pro každé $x, y \in \mathbb{Z}$ platí $a|(bx + cy)$.*

Důkaz. Viz přednášky. □

Věta 3.4 (o jednoznačnosti dělění se zbytkem)**.** *Pro $a, b \in \mathbb{Z}$ existují jednoznačně určená $q, r \in \mathbb{Z}$ tak, že*

$$a = b \cdot q + r \qquad a \qquad 0 \leq r < b.$$

Důkaz. Viz přednášky. □

Číslo r se nazývá zbytek po celočíselném dělení čísla a číslem b. Píšeme také $(a \mod b) = r$.

Příklad 3.5. Pro $a = 10, b = 3$ je $q = 3, r = 1$, tj. $(10 \mod 3) = 1$. Pro $a = 35, b = 5$ je $q = 7, r = 0$, tj. $(35 \mod 5) = 0$. Pro $a = -16, b = 8$ je $q = -2, r = 0$, tj. $(-16 \mod 8) = 0$. Pro $a = -15, b = 4$ je $q = -5, r = 2$, tj. $(-18 \mod 4) = 2$.

Definice 3.6. Přirozené číslo n se nazývá *prvočíslo*, jestliže $n \neq 1$ a jestliže n je dělitelné jen čísly 1 a n.

Příklad 3.7. $2, 3, 5, 7, 11, 13, 17, 19, \ldots$ jsou prvočísla. 6 není prvočíslo, protože je dělitelné 2 a 3.

Věta 3.8. *Existuje nekonečně mnoho prvočísel.*

Důkaz. Viz přednášky. □

Věta 3.9 (základní věta aritmetiky)**.** *Každé přirozené číslo lze vyjádřit jednoznačně až na pořadí činitelů jako součin prvočísel.*

Důkaz. Viz přednášky. □

Příklad 3.10. $15 = 3 \cdot 5$, $20 = 2 \cdot 2 \cdot 5$, $980220 = 2^2 \cdot 3 \cdot 5 \cdot 17 \cdot 31^2$.

3.5 Číselné soustavy

Viz přednášky.

Základní fakta:

Věta 3.11 (věta o jednoznačnosti zápisu přirozeného čísla v soustavě o základu b)**.** *Nechť $b > 1$ je přirozené číslo. Pro každé $x \in \mathbb{N}$ existují jednoznačně určená čísla $a_n, \ldots, a_1, a_0$ tak, že $0 \leq a_i < b$, $a_n \neq 0$, tak, že*

$$x = a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + \cdots + a_1 \cdot b + a_0.$$

Důkaz. Viz přednášky. □

Zápis čísla x v soustavě o základu b je dán čísly $a_n, \ldots, a_1, a_0$. Pro zápis čísel a_i používáme dohodnuté symboly. Např. pro $b = 10$ (soustava o základu 10, desítková soustava) používáme pro čísla nula, jedna, dvě, ..., devět, symboly $0, 1, 2, \ldots, 9$. Použijeme-li pro označení čísel $0, \ldots, b-1$ symboly $s_0, \ldots, s_{b-1}$ pak zápisem čísla x v soustavě o základu b je řetězec

$$s_{a_n} s_{a_{n-1}} \ldots s_{a_1} s_{a_0},$$

píšeme také $(s_{a_n} s_{a_{n-1}} \ldots s_{a_1} s_{a_0})_b$. Je-li $b = 10$ nebo je-li b zřejmé z kontextu, zpravidla b vynecháváme.

Pro zápisy čísel ve dvojkové soustavě ($b = 2$) používáme symboly 0 a 1. Pro zápisy čísel v šestnáctkové (hexadecimální) soustavě ($b = 16$) používáme symboly $0, 1, \ldots, A, B, C, D, E, F$.

Příklad 3.12. 1. Pro $x = 8965$ je $x = 8 \cdot 10^3 + 9 \cdot 10^2 + 6 \cdot 10 + 5$, tedy zápisem čísla osm tisíc devět set šedesát pět s soustavě o základu 10 je řetězec 8965, tj. $x = (8965)_{10}$.

2. Pro $x = 7$ a $b = 2$ je
$$x = 1 \cdot 2^2 + 1 \cdot 2^1 + 1,$$
tj. $x = (110)_2$ neboli $(7)_{10} = (110)_2$.

3. Pro $x = 75$ a $b = 2$ je
$$x = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0,$$
tj. $(75)_{10} = (1001011)_2$.

4. Pro $x = 37$ a $b = 16$ je
$$x = 2 \cdot 16^1 + 5 \cdot 16^0,$$
tj. $(37)_{10} = (25)_{16}$.

5. Pro $x = 31$ a $b = 16$ je
$$x = 1 \cdot 16^1 + 15 \cdot 16^0,$$
tj. $(31)_{10} = (1F)_{16}$.

Převody mezi zápisy čísel v různých číselných soustavách.

Shrnutí

DOPLNIT

Pojmy k zapamatování

- DOPLNIT

Kontrolní otázky

1. *DOPLNIT*

Cvičení

1. DOPLNIT

Úkoly k textu

1. DOPLNIT

Řešení

1. DOPLNIT

4 Kombinatorika

Studijní cíle: Po prostudování kapitol 4.1, 4.2 a 4.3 by student měl být znát základy kombinatorického počítání. Měl by znát pravidla součtu a součinu, pojmy permutace, variace a kombinace. Student by měl umět v základních úlohách samostatně provést správnou kombinatorickou úvahu. Měl by být schopen použít pravidla součtu a součinu k rozložení složitější úlohy na jednodušší.

Klíčová slova: kombinatorika, pravidlo součtu, pravidlo součinu, permutace, permutace s opakováním, variace, variace s opakováním, kombinace, kombinace s opakováním

Potřebý čas: 180 minut.

4.1 Co a k čemu je kombinatorika

Kombinatorika se zabývá určováním počtu možností, které mohou nastat za předepsaných podmínek.

Kombinatorika je jednou z nejužitečnějších oblastí diskrétní matematiky. Zabývá se určováním počtu možností (konfigurací), které existují za určitých předepsaných podmínek. Může nás například zajímat, kolika způsoby je možné vyjádřit přirozené číslo n ve tvaru součtu $n_1+\cdots+n_k$ přirozených čísel $n_1,\ldots,n_k$ přičemž nezáleží na pořadí čísel v součtu. Zde se jednou možností rozumí čísla $n_1,\ldots,n_k$. Předepsané podmínky v tomto případě říkají, že musí platit $n_1+\cdots+n_k=n$ a dále že možnosti $n_1,\ldots,n_k$ a $n'_1,\ldots,n'_k$ se považují za shodné (počítají se jako jedna možnost), pokud se liší jen pořadím čísel (např. možnosti $1,1,2$ a $1,2,1$ se považují za shodné, $1,1,2$ a $1,2,2$ nikoli). Tak například pro číslo 3 existují 3 možnosti (ty možnosti jsou $1+1+1$, $1+2$, 3), pro číslo 4 existuje 5 možností ($1+1+1+1$, $1+1+2$, $1+3$, $2+2$, 4) atd.

Průvodce studiem

V časopise BYTE Magazine kdysi vyšla následující zpráva. "According to ... WEB Technologies' vice president of sales and marketing, the compression algorithm used by DataFiles/16 is not subject to the laws of information theory" (BYTE Magazine 17(6):45, June 1992). Představitelé WEB Technologies tvrdili, že jejich kompresní program DataFiles/16 komprimuje všechny typy souborů na přibližně jednu šestnáctinu jejich původní velikosti a že pro soubory velikosti aspoň 64KB je tato komprese bezeztrátová. Jednoduchá kombinatorická úvaha však ukazuje, že to není možné.

Uvažujme např. délku souboru $16n$ bitů. Existuje celkem 2^{16n} různých souborů délky $16n$ bitů. Každý takový soubor by podle WEB Technologies mělo být možné zkomprimovat na výsledný soubor délky nejvýše n bitů. Přitom existuje právě 2^k různých souborů délky k bitů. Tedy navzájem různých souborů délky nejvýše n bitů existuje $2^0+2^1+2^2+\cdots+2^n=2^{n+1}-1$. Protože ale $2^{n+1}-1<2^{16n}$, není taková komprese možná. Kompresí totiž vyrobíme z daného souboru délky $16n$ bitů (těch je 2^{16n}) některý ze souborů délky nejvýše rovné n (těch je $2^{n+1}-1$). Proto musí existovat různé soubory délky $16n$, které se kompresí převedou na stejný soubor délky nejvýše rovné n. Taková komprese tedy není bezeztrátová.

Kombinatorika má použití v mnoha praktických oblastech našeho života.

Příklad 4.1. Předpokládejme, že heslo pro přístup do databáze je posloupnost sestávající z právě 5 povolených znaků. Mezi povolené znaky patří písmena `a`,..., `z`, `A`, ..., `Z`, číslice 0, 1, ..., 9. Platí přitom, že heslo musí začínat písmenem. Kolik existuje různých hesel?

Protože písmen je 52 (26 malých a 26 velkých) a číslic je 10, použitím pravidla součinu (viz dále) zjistíme, že hesel je $52\cdot 62^4=768.369.472$. Neznáme-li heslo, musíme tedy to spávné „uhodnout" z cca 768 miliónů možných hesel. Úvahy tohoto typu musí umět provádět každý, kdo se zabývá bezpečností počítačových systémů.

Příklad 4.2. Uvažujme následující variantu hazardní hry. Z osudí obsahujícího míčky s čísly 1,..., 20 jsou vylosovány 3 míčky. Hra spočívá v tom, že si před losováním můžeme vsadit na námi vybraná 3 čísla. Za vsázku zaplatíme 10 Kč. V případě, že uhodneme všechna 3 později vylosovaná čísla, dostaneme 20.000 Kč, jinak nedostaneme nic. Vyplatí se vsadit si, tj. budeme-li dlouhodobě vsázet, budeme celkově prohrávat nebo vyhrávat?

Vybrat 3 míčky z 20 je možné 2.280 způsoby (je to počet kombinací 3 z 20, viz dále). My si vsadíme na 1 takový výběr. Pravděpodobnost, že trefíme ten správný, je tedy $\frac{1}{2280}$. Z dlouhodobého hlediska tedy vyhrajeme v 1 z 2280 případů. V takových 2280 případech tedy vyhrajeme $1 \times 20.000 = 20.000$ Kč, přitom za vsázení utratíme $2.280 \times 10 = 22.800$ Kč. Vsadit si se tedy nevyplatí.

Příklad 4.3. Předpokládejme, že kódujeme elementární zprávy (zpráva může být znak nebo nějaká posloupnost znaků) tak, že každou zprávu zakódujeme jako posloupnost n symbolů 0 a 1, tzv. kódové slovo. Takovému kódu se říká binární kód délky n. Binární kód délky n tedy můžeme považovat za nějakou množinu posloupností délky n, které sestávají z 0 a 1. Např. $\{100, 010, 001\}$ je binární kód délky 3. Ten může být použit např. pro kódování výsledků nějakého procesu, kde výsledek je jeden z tří možných typů (prohra, remíza, výhra; rychlost ≤ 50 km/h, rychlost > 50, ale < 70 km/h, rychlost ≥ 70 km/h), tak, že např. prohra je kódována posloupností 100, remíza posloupností 010, výhra posloupností 001.

První otázka: Chceme-li kódovat k znaků binárním kódem délky n, jaké nejmenší n musíme zvolit, abychom zaručili možnost jednoznačného dekódování? Aby byl kód jednoznačně dekódovatelný, musí obsahovat aspoň k posloupností. Přitom posloupností z 0 a 1, které mají délku n, je právě 2^n (podle pravidla součinu, viz dále). Délka n musí tedy splňovat $k \leq 2^n$, tj. $\log_2 k \leq n$.

Druhá otázka: Předpokládejme, že na kódující posloupnosti 0 a 1 působí rušivé vlivy a že se proto může 0 změnit na 1 a 1 změnit na 0. Takové chyby jsou ale málo časté. Přijmeme-li posloupnost v délky n, může být zatížena chybami, a nemusí to tedy nutně být nějaké kódové slovo. Protože předpokládáme, že chyby jsou málo časté, je intuitivně přirozené chápat v jako chybou změněné kódové slovo w, a to takové w, které se ze všech kódových slov od v nejméně liší. Ve výše uvedeném případě např. 110 není kódovým slovem a jemu nejbližší kódová slova jsou 100 a 010. Vzdáleností posloupností přitom rozumíme počet pozic, na kterých se liší, tj. vzdálenost posloupností $a_1 \cdots a_n$ a $b_1 \cdots b_n$ je počet prvků množiny $\{i \mid a_i \neq b_i\}$. Vzdálenost 110 a 100 je tedy rovna 1 (liší se právě jednou pozicí). Pokud je kód dobře navržený, může dekódování probíhat tak, že přijatá posloupnost w délky n se opraví a výsledkem bude nejbližší kódové slovo. Jak jsme viděli, výše uvedený kód není dobře navržený, protože ke slovu 110 existují dvě kódová slova (100 a 010) se stejnou vzdáleností od 110. Jaký je největší počet k kódových posloupností binárního kódu délky n, který umožňuje opravu jednoduchých chyb? Přitom jednoduchá chyba je ta, která vznikne změnou právě jednoho symbolu posloupnosti (jednoduchou chybou vznikne z 001 např. 101, ale už ne 110). Uvažujme takto: Nechť takový kód obsahuje právě k kódových slov. Vezměme libovolné z nich a označme ho v. Slovem v bude interpretována nejen posloupnost v, ale i každá posloupnost, jejíž vzdálenost od v je 1 (tyto posloupnosti budou opraveny na v). Posloupností, které mají od v vzdálenost 1, je právě n (chyba může být na libovolné z n pozic). Slov, které připadají na kódové slovo v v tom smyslu, že budou po případné opravě jedné chyby převedeny na v, je tedy celkem $1 + n$. Protože na každé z k kódových slov takto připadá $n + 1$ navzájem různých posloupností délky n a protože počet všech posloupností nul a jedniček délky n je 2^n, musí být $k \cdot (n + 1) \leq 2^n$, tedy $k \leq \frac{2^n}{n+1}$. Největší počet kódových posloupností binárního kódu délky n, který umožňuje opravu jednoduchých chyb, je tedy $\frac{2^n}{n+1}$. Pro $n = 3$ je tedy největší počet $\frac{2^3}{3+1} = 2$. Kód s 3 kódovými slovy opravující jednoduché chyby tedy musí mít délku n aspoň 4 (protože pro délku $n = 3$ je největší počet kódových slov 2). Výše uvedený příklad tedy nelze spravit tím, že vybereme jiná kódová slova délky 3.

Uvedené příklady představují typické problémy, kterými se kombinatorika zabývá. Přesněji řečeno, kombinatorika se, jako každá oblast matematiky, zabývá obecnými principy, které je potom možné na konkrétní situace z praktického života použít. Tak například předpokládejme, že víme, kolika způsoby je možné vybrat dvouprvkovou podmnožinu $\{x, y\}$ z daných n prvků. Označme počet těchto způsobů $D(n)$. Víme tedy, že $D(n) = \frac{n(n-1)}{2}$ (vyzkoušejte nebo to přímo odvoďte). Pak je snadné spočítat, že z 30 studentů je možné vybrat dvojici studentů 435 způsoby (neboť $435 = \frac{30 \cdot 29}{2}$), že existuje právě 499 500 způsobů jak vybrat dva míčky z tisíce ($499\,500 = \frac{1000 \cdot 999}{2}$) atd.

Upozorníme nyní na důležitou věc. I v kombinatorice se setkáme s tím, že pro různé situace odvodíme různé vzorce (jako výše uvedený vzorec $D(n) = \frac{n(n-1)}{2}$). Včas však varujme: Střežme se mechanického používání vzorců! V kombinatorice snad více než kde jinde platí, že k tomu, abychom byli vůbec schopni vybrat pro danou situaci "správný vzorec", musíme situaci rozebrat a dokonale jí porozumět. Přitom toto porozumění je často netriviální záležitost (tomu tak není např. u derivování funkcí: máme-li například spočítat derivaci funkce $x^2 \cdot \sin(x)$, stačí znát vzorce pro derivování x^2, $\sin(x)$ a vzorec pro derivování

součinu funkcí; použití vzorce pro úlohu spočítání derivace dané funkce je tedy téměř triviální). Řešení kombinatorické úlohy se spíše podobá řešení "slovní úlohy": neexistuje obecný předpis pro řešení. Situaci musíme nejdříve dobře porozumět, pokud možno rozložit ji na jednodušší situace a ty potom vyřešit pomocí základních kombinatorických pravidel. Tato základní pravidla mohou mít podobu vzorců. Nesrovnatelně důležitější než naučit se vzorce, je ale naučit se používat základní kombinatorická pravidla (tato pravidla jsou pravým smyslem kombinatorických vzorců). Bez porozumění kombinatorickým pravidlům nejsme schopni řešit jiné než triviální kombinatorické úlohy.

4.2 Pravidla součtu a součinu

Pravidlo součtu a pravidlo součinu jsou dvě základní kombinatorická pravidla. Mnoho dalších pravidel vzniká jejich kombinováním.

Základní kombinatorická pravidla jsou pravidlo součtu a pravidlo součinu.

Průvodce studiem

Pravidlo součtu: Lze-li úkol A provést m způsoby a lze-li úkol B provést n způsoby, přičemž žádný z m způsobů provedení úkolu A není totožný s žádným z n způsobů provedení úkolu B, pak provést úkol A nebo úkol B lze provést $m + n$ způsoby.

Pravidlo součtu je zjevné. Ukážeme, jak ho lze použít.

Příklad 4.4. V knihovně je 5 knih, jejichž autorem je A. C. Doyle (?), a 10 knih, jejichž autorkou je A. Christie. Čtenář si tedy může vybrat 15 způsoby knihu, kterou napsali A. C. Doyle nebo A. Christie. Je-li A úkol "vybrat knihu, jejíž autorem je A. C. Doyle" a B úkol "vybrat knihu, jejíž autorem je A. Christie", pak je $m = 5$ a $n = 10$. Přitom přitom provést úkol A nebo úkol B znamená vybrat knihu, kterou napsali A. C. Doyle nebo A. Christie. Podle pravidla součtu to lze právě $m + n = 15$ způsoby. Použití pravidla součtu je oprávněné, protože žádná kniha, kterou napsal A. C. Doyle, není totožná s žádnou knihou, kterou napsala A. Christie.

Příklad 4.5. Množiny M a N jsou disjunktní (tj. nemají společné prvky) a platí $|M| = m$ a $|N| = n$. Kolika způsoby lze vybrat prvek, který patří do M nebo do N? Jsou-li A a B po řadě úkoly "vybrat prvek z množiny M" a 'vybrat prvek z množiny N", pak předpoklady pravidla součtu jsou splněny (M a N nemají společné prvky), a proto existuje $m + n$ způsobů, jak vybrat prvek z M nebo N. Jinými slovy, jsou-li M a N disjunktní množiny, je $|M \cup N| = |M| + |N|$.

Poznamenejme, že předpoklad pravidla součtu, která říká, že žádný z m způsobů provedení úkolu A není totožný s žádným z n způsobů provedení úkolu B, je podstatná. Uvažujme Příklad 4.5, ale vezměme množiny, které nejsou disjunktní, např. $M = \{a, b, c\}$, $N = \{b, c, d, e\}$. Jak snadno vidíme, existuje 5 způsobů, jak vybrat prvek z M nebo N, přitom $5 \neq 3 + 4 = m + n$.

Pravidlo součtu lze zobecnit na konečný počet úkolů: Lze-li úkol C rozložit na po sobě následující úkoly $A_1, \ldots, A_n$ a lze-li úkol A_i provést m_i způsoby (pro každé $i = 1, \ldots, n$), pak lze úkol C provést $m_1 + \cdots + m_n$ způsoby.

Pokud úkol A_1 lze provést m_1 způsoby, úkol A_2 lze provést m_2 způsoby, ..., úkol A_k lze provést m_k způsoby, přičemž po každou dvojici A_i a A_j ($i \neq j$) žádný z m_i způsobů provedení úkolu A_i není totožný s žádným z m_j způsobů provedení úkolu A_j, pak provést úkol A_1 nebo úkol A_2 nebo úkol A_k lze provést $m_1 + m_2 + \cdots + m_k$ způsoby.

Příklad 4.6. Nechť $M_1, \ldots, M_k$ jsou konečné po dvou disjunktní množiny. Kolik prvků má sjednocení $M_1 \cup \cdots \cup M_k$? Pomocí zobecněného pravidla součtu můžeme podobně jako v Příkladě 4.5 ukázat, že $|M_1 \cup \cdots \cup M_k| = |M_1| + \cdots + |M_k|$.

Průvodce studiem

Pravidlo součinu: Lze-li úkol C rozložit na po sobě následující úkoly A a B (tj. provést C znamená provést nejdřív A a potom B) a lze-li úkol A provést m způsoby a úkol B lze provést n způsoby, pak lze úkol C provést $m \cdot n$ způsoby.

Také pravidlo součinu je zjevné. Ukážeme ho na konkrétních příkladech.

Příklad 4.7. Kolik prvků má kartézský součin $M \times N$ dvou konečných množin M a N? Připomeňme, že $M \times N = \{\langle x, y\rangle \mid x \in M, y \in N\}$. Určit libovolný prvek $\langle x, y\rangle \in M \times N$ znamená totéž, co splnit úkol "zvol x a zvol y". Tento úkol lze rozložit na úkol "zvol x" a úkol "zvol y". Prvek x lze přitom zvolit $|M|$ způsoby, prvek y lze zvolit $|N|$ způsoby. Podle pravidla součinu lze tedy úkol "zvol x a zvol y" provést $|M| \cdot |N|$ způsoby. Proto $|M \times N| = |M| \cdot |N|$.

Podobně jako pravidlo součtu lze i pravidlo součinu zobecnit na na konečný počet úkolů: Lze-li úkol C rozložit na po sobě následující úkoly $A_1, \ldots, A_k$ a lze-li úkol A_i provést m_i způsoby (pro každé $i = 1, \ldots, k$), pak lze úkol C provést $m_1 + \cdots + m_k$ způsoby.

Příklad 4.8. Registrační značka vozidla má tvar PKC CCCC, kde P, K, a C jsou symboly a přitom P je některá z číslic 1–9, K je písmeno, určující příslušnost ke kraji (např. T označuje Moravskoslezský kraj, H označuje hradecký apod.) a C je některá z číslic 0–9. Kolik lze v rámci jednoho kraje přidělit registračních značek?

První symbol lze zvolit 9 způsoby, druhý symbol nelze volit, protože je v rámci kraje pevně daný, třetí symbol lze zvolit 10 způsoby, stejně tak lze 10 způsoby zvolit čtvrtý, pátý, šestý i sedmý symbol. Podle zobecněného pravidla součinu tedy existuje v rámci jednoho kraje $9 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 9 \cdot 10^5$ (devět set tisíc) možných různých registračních značek.

Pravidla součtu a součinu se často v jedné úloze kombinují. Ukažme jednoduchý příklad.

Příklad 4.9. Nechť A, B, C jsou konečné množiny, přičemž A a B jsou disjunktní. Kolik prvků má množina $(A \cup B) \times C$?

Úkol vybrat libovolně prvek z $(A \cup B) \times C$ lze rozložit na dva následující úkoly "vyber prvek z $A \cup B$" a "vyber prvek z C" (viz Příklad 4.7). Přitom úkol "vyber prvek z $A \cup B$" znamená "vyber prvek z A nebo vyber prvek z B" a lze ho podle pravidla součtu provést $|A| + |B|$ způsoby (viz Příklad 4.5). Proto lze podle pravidla součtu prvek z $(A \cup B) \times C$ vybrat $(|A| + |B|) \cdot |C|$ způsoby, tedy $|(A \cup B) \times C| = (|A| + |B|) \cdot |C|$.

4.3 Permutace, variace, kombinace

Kolika způsoby lze seřadit určitý počet objektů? Kolika způsoby lze vybrat určitý počet objektů z daných objektů, když na pořadí výběru záleží? Co když na pořadí výběru nezáleží? Co když se prvky ve výběru nemohou opakovat? Co když se opakovat mohou? Tyto a podobné otázky se často objevují v různých kombinatorických úlohách. Odpovědi na ně lze nalézt použitím pravidel součtu a součinu. Protože se však tyto otázky objevují opravdu často, odvodíme si vzorce, které na některé tyto otázky odpovídají. Vzorce, které odvodíme, patří k základům kombinatorického počítání. Nejprve však ještě jednou varování.

Průvodce studiem

Při používání kombinatorických vzorců, které uvedeme, je důležité vzorci dobře rozumět, "vidět do něj", umět ho kdykoli odvodit. Důležitější než vzorce samotné jsou totiž úvahy, které k nim vedou. Vzorec je jen symbolickým vyjádřením závěru kombinatorické úvahy. Osvojíme-li si odpovídající úvahy, potřebné vzorce si nakonec můžeme odvodit sami (nebo je někde najdeme). Když si odpovídající úvahy neosvojíme, budou nám nejspíš vzorce k ničemu, neboť je u jen trochu složitějších úloh nebudeme umět používat. Čtenáři proto následující doporučení: Nesnažte se učit vzorce. Snažte se pochopit a naučte se sami provádět úvahy. Uvidíte, že věci jsou ve skutečnosti jednoduché.

4.3.1 Permutace

Student si u zkoušky vybere tři otázky. Může si vybrat, v jakém pořadí na ně bude odpovídat. Kolik má možností? Označme otázky A, B a C. Možná pořadí odpovídání jsou ABC, ACB, BAC, BCA, CAB, CBA. Je jich tedy šest. Tak přicházíme k pojmu permutace.

Permutace nějakých prvků je jejich seřazení.

Definice 4.10 (permutace)**.** *Permutace* n (navzájem různých) objektů je libovolné seřazení těchto objektů, tj. seřazení od prvního k n-tému. Počet permutací n objektů budeme značit $P(n)$.

Věta 4.11. $P(n) = n!$.

Důkaz. Jedno ale libovolné seřazení dostaneme tak, že vybereme 1. prvek (to lze provést n způsoby), poté vybereme 2. prvek (to lze provést $n-1$ způsobem, protože jeden prvek jsme již vybrali), poté vybereme 3. prvek (to lze provést $n-2$ způsoby), ..., nakonec vybereme n-tý prvek (to lze provést jedním způsobem, $n-1$ prvků totiž již bylo vybráno a zbývá poslední prvek). Podle pravidla součinu lze takový výběr provést $n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 1 = n!$ způsoby. Tedy $P(n) = n!$. □

Seřazujeme-li objekty, z nichž některé jsou stejné, provádíme tzv. permutace s opakováním.

U permutací s opakováním mohou být některé seřazované prvky stejné.

Definice 4.12 (permutace s opakováním)**.** Je dáno n objektů rozdělených do r skupin, které mají po řadě $n_1, \ldots, n_r$ objektů, tj. $n_1 + \cdots + n_r = n$. Objekty v každé ze skupin jsou navzájem nerozlišitelné. Každé seřazení těchto n objektů se nazývá *permutace s opakováním* (daným parametry $(n_1, \ldots, n_r)$). Počet takových permutací značíme $P(n_1, \ldots, n_r)$.

Věta 4.13. *Pro* $n_1 + \cdots + n_r = n$ *je* $P(n_1, \ldots, n_r) = \frac{n!}{n_1! \cdot \cdots \cdot n_r!}$.

Důkaz. Uvažujme libovolnou permutaci s opakováním. Očíslujme objekty v rámci každé z r skupin tak, aby se staly rozlišitelnými. Pak dané permutaci s opakováním odpovídá několik permutací očíslovaných objektů v tom smyslu, že na pozici i ($1 \leq i \leq n$) je v permutaci s opakováním objekt z j-té skupiny ($1 \leq i \leq n$), právě když je na pozici i v permutaci očíslovaných objektů objekt, který vznikl očíslováním z některého objektu z j-té skupiny.

Pro příklad: Mějme $n = 5$, $r = 2$, $n_1 = 3$, $n_2 = 2$, objekty první skupiny značíme A, objekty druhé skupiny značíme B. Po očíslování budeme mít objekty A_1, A_2, A_3, B_1, B_2. Permutaci s opakováním ABAAB odpovídá např. permutace $\mathrm{A}_3\mathrm{B}_1\mathrm{A}_2\mathrm{A}_1\mathrm{B}_2$, ne však permutace $\mathrm{A}_3\mathrm{A}_2\mathrm{A}_1\mathrm{B}_1\mathrm{B}_2$.

Kolik permutací očíslovaných objektů odpovídá každé permutaci s opakováním? Objekty první skupiny můžeme na jejich pozicích (ty jsou pro danou permutaci s opakováním dány pevně a je jich n_1) seřadit $n_1!$ způsoby (tolik je permutací n_1 prvků), ..., objekty r-té skupiny můžeme na jejich pozicích seřadit $n_r!$ způsoby. Protože seřazování objektů každé skupiny provádíme nezávisle na seřazování objektů libovolné jiné skupiny. Proto je celkový počet permutací očíslovaných objektů, které odpovídají libovolné permutaci s opakováním roven $n_1! \cdot \cdots \cdot n_r!$. Dostali jsme tedy

$$P(n_1, \ldots, n_r) \cdot n_1! \cdot \cdots \cdot n_r! = P(n),$$

odkud plyne $P(n_1, \ldots, n_r) = \frac{n!}{n_1! \cdot \cdots \cdot n_r!}$. □

Příklad 4.14. Kolik slov (i nesmyslných) lze sestavit přerovnáním písmen ve slově POSTOLOPRTY? Počet slov je roven počtu seřazení písmen slova POSTOLOPRTY. Jde o permutace objektů s opakováním. Máme $n = 11$ objektů (písmen), které jsou rozděleny do $r = 7$ skupin odpovídajících jednotlivým písmenům P, O, S, T, L, R, Y. Počty objektů v jednotlivých skupinách jsou $n_{\mathrm{P}} = 2$, $n_{\mathrm{O}} = 3$, $n_{\mathrm{S}} = 1$, $n_{\mathrm{T}} = 2$, $n_{\mathrm{L}} = 1$, $n_{\mathrm{R}} = 1$, $n_{\mathrm{Y}} = 1$. Počet slov je tedy $P(2, 3, 1, 2, 1, 1, 1) = \frac{11!}{2!3!2!}$.

4.3.2 Variace

Na lodi jsou čtyři důstojníci. Z nich je třeba jmenovat kapitána a jeho zástupce. Kolika způsoby to lze provést? Označme důstojníky písmeny A, B, C, D. Pak existuje těchto 12 způsobů: AB (A je kapitán, B jeho zástupce), AC, AD, BA, BC, BD, CA, CB, CD, DA, DB, DC.

Variace je výběr, u kterého záleží na pořadí vybíraných prvků.

Definice 4.15 (variace)**.** Je dáno n (navzájem různých) objektů a číslo $r \leq n$. *Variace* r (objektů) z n (objektů) je libovolný výběr r objektů z daných n objektů, ve kterém záleží na pořadí vybíraných objektů. Počet takových variací značíme $V(n, r)$.

Ve výše uvedeném příkladu je $n = 4$ (máme 4 objekty) a $r = 2$ (vybíráme dva objekty). Variace BA je výběr, ve kterém je jako první vybrán objekt B a jako druhý objekt A. Variace BA a AB jsou různé (záleží na pořadí). Celkem existuje 12 takových variací, tj. $V(4, 2) = 12$.

Věta 4.16. $V(n, r) = n \cdot (n-1) \cdot \cdots \cdot (n-r+1)$.

Důkaz. Každá variace je dána tím, jaké objekty jsou na 1., 2., . . . , r-tém místě. Objekt na 1. místě lze zvolit n způsoby (vybíráme z n objektů), objekt na 2. místě pak $n-1$ způsoby (vybíráme z $n-1$ objektů, protože jeden objekt je už na 1. místě), . . . , objekt na r-tém místě lze vybrat $n-r+1$ způsoby (tolik objektů je3tě k výběru zbývá). Podle pravidla součinu je tedy celkový počet takto provedených výběrů, tj. počet všech variací, $n \cdot (n-1) \cdot \cdots \cdot (n-r+1)$. □

Všimněme si, že $V(n, r) = \frac{n!}{(n-r)!}$. Skutečně,

$$\frac{n!}{(n-r)!} = \frac{n \cdot (n-1) \cdot \cdots \cdot (n-r+1) \cdot (n-r) \cdot \cdots \cdot 1}{(n-r) \cdot \cdots \cdot 1} = n \cdot (n-1) \cdot \cdots \cdot (n-r+1) = V(n, r)$$

Příklad 4.17. Zámek na kolo s kódem má pro nastavení kódu tři otáčecí kolečka. Na každém z nich lze nastavit číslice 0, 1, . . . , 9. Předpokládejme, že nastavení a zkouška jedné číselné kombinace trvá 2 sekundy. Jak dlouho trvá v průměrném případě otevření zákmu, neznáme-li správnou číselnou kombinaci (průměrný případ definujeme jako aritmetický průměr nejlepšího a nejhoršího případu)?

Číselné kombinace jsou 000 až 999. Jsou to tedy variace 3 z 10 s opakováním (3 pozice, 10 číslic). Těch je $10^3 = 1000$. V nejlepším případě nastavíme správnou kombinaci už v 1. pokusu (to trvá 2 sekundy), vnejhorším až v 1000. pokusu (to trvá 2000 sekund). V průměrném případě je to tedy $\frac{1000}{2} = 500$ sekund (což je 8 minut a 20 sekund).

Poznámka 4.18. Všimněte si, že $V(n, n) = n! = P(n)$, tj. počet variací n a n je stejný jako počet permutací n objektů. To není náhoda. Variace n a n je vlastně výběr n prvků z n prvků, ve kterém záleží na pořadí. Je to tedy uspořádání, tj. permutace, n prvků (první vybraný prvek je v daném uspořádání na prvním místě, . . . , n-tý vybraný prvek je v daném uspořádání na n-tém místě).

Výběry, ve kterých se prvky mohou opakovat, nazýváme variace s opakováním.

U variací s opakováním může být každý prvek vybrán několikrát.

Definice 4.19 (variace s opakováním)**.** Jsou dány objekty n různých typů. Objektů každého typu je neomezeně mnoho a jsou navzájem nerozlišitelné. *Variace* r (objektů) z n (objektů) *s opakováním* je libovolný výběr r objektů z daných objektů n typů, ve kterém záleží na pořadí vybíraných objektů. Počet takových variací značíme $\overline{V}(n, r)$.

Protože jsou prvky jednotlivých typů nerozlišitelné, jsou dvě variace s opakováním stejné, právě když mají na odpovídajících si místech (prvním až r-tém) objekty stejných typů.

Věta 4.20. $\overline{V}(n, r) = n^r$.

Důkaz. První prvek můžeme vybrat n způsoby, druhý prvek můžeme vybrat n způsoby, . . . , r-tý můžeme vybrat n způsoby. Podle pravidla součinu lze tedy výběr provést $n \cdot \cdots \cdot n = n^r$ způsoby. □

Poznámka 4.21. Variace s opakováním bychom mohli definovat jinak, a to následovně: Je dáno n (navzájem různých) objektů a číslo r. Variace r (objektů) z n (objektů) s opakováním (definovaná alternativně) je libovolný výběr r objektů z daných n objektů, ve kterém záleží na pořadí vybíraných objektů a ve kterém se prvky po výběru vracejí mezi prvky, ze kterých se vybírá. Uvědomme si, že způsob výběru zde je jiný, než v Definici 4.19. Důležité však je, že počet variací s opakováním je i v tomto případě $\overline{V}(n, r)$ (ověřte).

Příklad 4.22. Z místa A je třeba předávat na místo B zprávu o tom, jak dopadla akce konaná v místě A. Přitom existuje celkem 20 000 možných výsledků té akce. Předpokládejme, že pro zakódování výsledku se použije posloupnost $k = 2$ různých symbolů (např. 0 a 1), která má délku d. Jaká je nejmenší délka takové posloupnosti? Jak to bude při jiných počtech symbolů $k = 3, 4, 5$?

Jde o to, najít nejmenší délku d tak, aby posloupností k symbolů bylo aspoň 20000, tj. aby každý výsledek mohl být nějakou posloupností zakódován. Vybíráme-li z k symbolů posloupnost délky d, vybíráme vlastně variaci d z k s opakováním. Takových posloupností je tedy $\overline{V}(k, d) = k^d$. Chceme tedy najít nejmenší d tak, aby $k^d \geq 20000$. Pro $k = 2$ je $d = 15$, pro $k = 3$ je $d = 10$, pro $k = 4$ je $d = 8$, pro $k = 5$ je $d = 7$.

4.3.3 Kombinace

V táboře jsou 4 muži (označme je A, B, C, D). Kolika způsoby z nich lze vybrat dvoučlennou hlídku? Výběr hlídky je dán výběrem dvou z nich, tedy dvouprvkovou podmnožinou množiny $\{\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}\}$. Hlídky tedy mohou být $\{\mathrm{A}, \mathrm{B}\}$, $\{\mathrm{A}, \mathrm{C}\}$, $\{\mathrm{A}, \mathrm{D}\}$, $\{\mathrm{B}, \mathrm{C}\}$, $\{\mathrm{B}, \mathrm{D}\}$, $\{\mathrm{C}, \mathrm{D}\}$, je jich tedy 6.

Kombinace je výběr, u kterého nezáleží na pořadí vybíraných prvků.

Definice 4.23 (kombinace)**.** Je dáno n (navzájem různých) objektů a číslo $r \leq n$. *Kombinace* r (objektů) z n (objektů) je libovolný výběr r objektů z daných n objektů, ve kterém nezáleží na pořadí vybíraných objektů. Počet takových kombinací značíme $\binom{n}{r}$.

Čísla $\binom{n}{r}$ se nazývají *kombinační čísla* a označují se také $C(n, r)$ (čte se "en nad er").

Ve výše uvedeném příkladu je $n = 4$ (máme 4 objekty) a $r = 2$ (vybíráme dva objekty). Kombinace $\{\mathrm{A}, \mathrm{C}\}$ je výběr, ve kterém jsou vybrány A a C. Celkem existuje 6 takových kombinací, tj. $\binom{4}{2} = 6$.

Věta 4.24. $\binom{n}{r} = \frac{n!}{(n-r)!r!}$.

Důkaz. Víme, že $V(n, r) = \frac{n!}{(n-r)!}$. Uvědomme si, že každé kombinaci r z n odpovídá tolik variací r z n, kolika způsoby lze uspořádat r vybraných objektů (u kombinace záleží jen na vybraných objektech, ne na jejich uspořádání, kdežto u variace záleží i na jejich uspořádání). Např. kombinaci $\{\mathrm{A}, \mathrm{B}, \mathrm{C}\}$ odpovídají variace ABC, ACB, BAC, BCA, CAB, CBA. Existuje $r!$ způsobů, jak uspořádat r objektů. Je tedy

$$\text{počet kombinací } r \text{ z } n \text{ krát počet uspořádání } r \text{ objektů = počet variací } r \text{ z } n,$$

tj.

$$\binom{n}{r} \cdot r! = V(n, r).$$

Odtud $\binom{n}{r} = \frac{V(n,r)}{r!} = \frac{n!}{(n-r)!r!}$. □

Přímo z odvozeného vzorce plyne

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

Skutečně, $\binom{n}{n-r} = \frac{n!}{(n-(n-r))!(n-r)!} = \frac{n!}{(n-r)!r!} = \binom{n}{r}$. Dále platí, že

$$\binom{n}{n} = 1 \quad \text{a} \quad \binom{n}{0} = 1.$$

Poznámka 4.25. Vzorec pro $\binom{n}{r}$ lze odvodit také takto. Očíslujme n objektů, ze kterých vybíráme, čísly 1 až n. Kombinaci r z n můžeme vyjádřit jako řetězec n nul a jedniček, který obsahuje právě r jedniček, přičemž na i-tém místě toho řetězce je 1, právě když se v dané kombinaci nachází i-tý prvek. Např. jsou-li a, b, c, d první až čtvrtý prvek a, pak řetězci 0110 odpovídá kombinace $\{b, c\}$. Takový řetězců existuje právě tolik, kolik existuje permutací n prvků s opakováním, které jsou rozděleny do dvou skupin obsahujících r prvků (jedničky) a $n - r$ prvků (nuly). Takových permutací je podle Věty 4.13 $\frac{n!}{(n-r)!r!}$.

Příklad 4.26. Kolika způsoby lze vybrat 4 předměty z nabídky 10 volitelných předmětů? Výběr předmětů je kombinace 4 z 10. Výběr lze tedy provést $\binom{10}{4} = \frac{10!}{6!\cdot 4!} = \frac{10\cdot 9\cdot 8\cdot 7}{4\cdot 3\cdot 2} = 210$ způsoby.

Řekneme si teď dva užitečné vztahy. Prvním z nich je, že pro $k < n$ platí

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}. \tag{4.1}$$

Odvoďme to: $\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!} = \frac{k\cdot(n-1)!+(n-k)\cdot(n-1)!}{k!(n-k)!} = \frac{(k+(n-k))\cdot(n-1)!}{k!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$.

Druhým je tzv. *binomická věta*.

Věta 4.27 (binomická věta)**.** *Pro reálné číslo x a nezáporné celé n je*

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k. \tag{4.2}$$

Důkaz. Dokážeme to indukcí přes n.

Indukční předpoklad: Pro $n = 0$ je tvrzení zřejmé. Např. pro $n = 0$ je $(1+x)^0 = 1$ a $\sum_{k=0}^{0} \binom{n}{k} x^k = \binom{0}{0} x^0 = 1$.

Indukční krok: Předpokládejme, že tvrzení platí pro $n-1$, tj. $(1+x)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} x^k$, a dokažme ho pro n. Máme

$$\begin{aligned}
(1+x)^n &= (1+x)(1+x)^{n-1} = (1+x)\sum_{k=0}^{n-1} \binom{n-1}{k} x^k = \\
&= \sum_{k=0}^{n-1} \binom{n-1}{k} x^k + \sum_{k=0}^{n-1} \binom{n-1}{k} x^{k+1} = \sum_{k=0}^{n-1} \binom{n-1}{k} x^k + \sum_{k=1}^{n} \binom{n-1}{k-1} x^k = \\
&= \binom{n-1}{0} x^0 + \sum_{k=1}^{n-1} \left(\binom{n-1}{k-1} x^k + \binom{n-1}{k-1} x^k\right) + \binom{n-1}{n-1} x^n = \\
&= x^0 + \sum_{k=1}^{n-1} \left(\binom{n-1}{k-1} + \binom{n-1}{k-1}\right) x^k + x^n = \\
&= \binom{n}{0} x^0 + \sum_{k=1}^{n-1} \binom{n}{k} x^k + \binom{n}{n} x^n = \sum_{k=0}^{n} \binom{n}{k} x^k.
\end{aligned}$$

Přitom jsme použili vzorec (4.1). □

Binomická věta má řadu použití.

Příklad 4.28 (počet podmnožin n-prvkové množiny)**.** Dosazením $x = 1$ dostáváme

$$2^n = \sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}.$$

Protože $\binom{n}{k}$ je počet všech k-prvkových podmnožin n-prvkové množiny, udává součet vpravo počet 0-prvkových plus počet 1-prvkových plus ... plus počet n-prvkových, tj. počet všech podmnožin n-prvkové množiny. Pomocí binomické věty tedy vidíme, že je roven 2^n.

K tomu lze ale dojít i takto: Seřaďme prvky dané n-prvkové množiny za sebe. Představme si n pozic, které odpovídají 1., 2.,..., n. prvku. Do pozic budeme umísťovat 0 a 1. Podmnožiny jednoznačně odpovídají umístěním 0 a 1 do těchto pozic: je-li na i-té pozici 1, pak i-tý prvek patří do dané podmnožiny, je-li tam 0, pak do ní nepatří. Podmnožin n-prvkové množiny je tedy právě tolik, kolika způsoby lze do n pozic umístit nuly a jedničky. Tento počet je roven počtu variací n ze 2 (vybíráme z $\{0,1\}$), tedy je to $\overline{V}(n,2) = 2^n$.

Způsobů, jak vyřešit kombinatorický problém, bývá několik.

Průvodce studiem

Počet všech podmnožin n-prvkové množiny je 2^n. Lze k tomu dojít několika způsoby. Dva z nich jsme ukázali v Příkladu 4.28. Taková situace, kdy k jednomu výsledku můžeme dojít několika způsoby, je pro kombinatoriku typická. Různé způsoby odpovídají různým pohledům na věc. Například u počtu všech podmnožin byl první způsob "sečti počty všech 0-prvkových, 1-prvkových, ..., n-prvkových podmnožin", druhý způsob byl "představ si podmnožiny jako posloupnosti nul a jedniček a urči počet těchto posloupností". Obecný návod, jak si problém vhodně představit, není. Záleží jen na naší představivosti.

Výběr, ve kterém nezáleží na pořadí prvků a ve kterém se prvky mohou opakovat, se nazývá kombinace s opakováním. Vede k tomu následující úloha. V obchodě mají 4 typy zákusků (věnečky, řezy, špičky a trubičky). Máme koupit 6 zákusků. Kolika způsoby to lze provést? Jeden možný způsob je koupit 6 věnečků, další je koupit 6 větrníků, další je koupit 2 větrníky a 4 řezy, další je koupit věneček, řez, špičku a 3 větrníky atd. Důležité je, zaprvé, že pořadí zákusků v nákupu je nepodstatné, a zadruhé, že v nákupu mohou být zákusky stejného typu (zákusky se mohou opakovat).

U kombinací s opakováním může být každý prvek vybrán několikrát.

Definice 4.29 (kombinace s opakováním)**.** Jsou dány objekty n různých typů. Objektů každého typu je neomezeně mnoho a jsou navzájem nerozlišitelné. *Kombinace* r (objektů) z n (objektů) *s opakováním* je libovolný výběr r objektů z daných objektů n typů, ve kterém nezáleží na pořadí vybíraných objektů. Počet takových kombinací značíme $\overline{C}(n, r)$.

Že jsou objekty jednotlivých typů nerozlišitelné, znamená, že dvě kombinace s opakováním považujeme za stejné, právě když pro každý z n typů obsahují stejné počty objektů toho typu. U příkladu se zákusky to např. znamená, že každé dva nákupy obsahující dva větrníky a čtyři špičky, považujeme za stejné (byť v jednom nákupu mohou být jiné dva věnečky než ve druhém).

Věta 4.30. $\overline{C}(n, r) = \binom{n+r-1}{n-1}$.

Důkaz. Podívejme se na výběr takhle. Máme n přihrádek, které odpovídají typům objektů. Vybrat kombinaci r z n s opakováním znamená umístit do těchto přihrádek celkem r kuliček. Počet kuliček v i-té přihrádce můžeme totiž chápat jako počet objektů typu i, které jsme vybrali. Hledaný počet kombinací $\overline{C}(n, r)$ je tedy stejný jako počet umístění r kuliček do n přihrádek.

Abychom určili počet takových umístění, budeme každé umístění reprezentovat posloupností nul (reprezentují přepážky mezi přihrádkami) a 1 (reprezentují kuličky). Např. pro $n = 4$ a $r = 6$ řetězec 101100111 reprezentuje umístění, kdy je v první přihrádce 1 kulička, ve druhé 2 kuličky, ve třetí 0 kuliček, ve čtvrté 3 kuličky. Tedy: první jednička reprezentuje 1 kuličku v první přihrádce; následující nula reprezentuje přepážku; následující dvě jedničky reprezentují 2 kuličky ve druhé přihrádce; následující nula reprezentuje přihrádku mezi druhou a třetí přihrádkou; pak nenásleduje žádná jednička (tj. třetí přihrádka neobsahuje žádnou kuličku), ale hned další nula reprezentující přepážku mezi třetí a čtvrtou přihrádkou; následují tři jedničky reprezentující 3 kuličky ve čtvrté příhrádce. Protože máme $n - 1$ přepážek a r kuliček, je každé umístění reprezentováno řetězcem délky $n + r - 1$, ve kterém je $n - 1$ nul a r jedniček. Každý takový řetězec je určen tím, na kterých jeho $n - 1$ pozicích z 1.,. . . ,$(n + r - 1)$-té pozice jsou nuly (na ostatních pozicích jsou totiž jedničky). Výběr $n - 1$ pozic pro nuly z celkového počtu $n + r - 1$ pozic je kombinace $n - 1$ z $n + r - 1$, a těch je podle Věty 4.24 $\binom{n+r-1}{n-1}$. □

Příklad 4.31. Vraťme se k zákuskům (viz výše). Výběr 6 zákusků ze 4 druhů zákusků je kombinace 6 z 4 s opakováním. Těch je podle Věty 4.30 $\overline{C}(n, r) = \binom{n+r-1}{n-1} = \binom{4+6-1}{4-1} = \binom{9}{3} = \frac{9!}{6!3!} = 84$.

Poznámka 4.32. Zastavme se u pojmů permutace s opakováním, variace s opakováním a kombinace s opakováním. Ve všech případech máme vlastně objekty rozděleny do několika typů. Zatímco však u permutací s opakováním je objektů každého typu předepsaný počet a tyto počty mohou být pro různé typy různé, u variací i kombinací s opakováním je objektů každého typu neomezeně mnoho.

4.3.4 Další výběry

Permutace, variace a kombinace jsou základní typy výběrů. Ukázali jsme si základní typy úvah, které vedou ke stanovení jejich počtu. Prakticky se však můžeme setkat s příklady složitějšími, ve kterých úvahy o permutacích, variacích a kombinacích můžeme využít.

Příklad 4.33. Ligu hraje 14 týmů. Výsledek ligy je dán tím, které týmy obsadí 1., 2. a 3. místo a které 2 týmy sestoupí do nižší soutěže. Kolik je možných výsledků ligy?

Výsledek ligy je dán výběrem týmů na 1.-3. místě a výběrem týmů, které sestupují. Týmy na 1.-3. místě jsou tři a vybíráme je z 14 týmů, přitom na pořadí výběru záleží. Jde tedy o variace 3 z 14 a je jich $V(14,3)$. Po jejich výběru vybereme ze zbývajících 11 týmů dva, které sestoupí. Zde na pořadí nezáleží. Jde tedy o kombinace 2 z 11 a je jich $\binom{11}{2}$. Podle pravidla součinu je celkově $V(14,3) \cdot \binom{11}{2}$ možných výsledků ligy.

Můžeme ale také postupovat obráceně, tj. nejdřív vybrat ze 14 dva sestupující týmy a pak ze zbylých 12 vybrat 3 medailisty. Tak dostaneme $\binom{14}{2} \cdot V(12,3)$ možností. Výsledek je ale stejný jako u první úvahy, protože

$$\begin{aligned}\binom{14}{2} \cdot V(12,3) &= \frac{14 \cdot 13}{2} \cdot 12 \cdot 11 \cdot 10 = \frac{14 \cdot 13 \cdot 12 \cdot 11 \cdot 10}{2} = \\ &= 14 \cdot 13 \cdot 12 \cdot \frac{11 \cdot 10}{2} = V(14,3) \cdot \binom{11}{2}.\end{aligned}$$

Příklad 4.34. Kolika různými způsoby lze kolem kulatého stolu se 6 židlemi posadit 6 osob? Přitom dvě posazení, která se liší jen pootočením, považujeme za shodná.

Označmě osoby A, B, C, D, E, F. Kdyby i dvě posazení lišící se pootočením, byla považována za různá, pak by počet všech posazení byl stejný jako počet všech permutací 6 objektů, tj. $P(6) = 6!$. Kruhové uspořádání kolem stolu by totiž nehrálo roli. Kolem stolu je 6 míst, můžeme jim říkat 1., 2., . . . , 6. místo. Otázka by pak byla, kolika způsoby můžeme umístit 6 osob na 6 míst, tj. vlastně kolika způsoby lze uspořádat 6 osob. Odpověď je pak zjevně $P(6)$. Považujeme-li však posazení za shodná, právě když lze z jednoho do druhého přejít pootočením, bude celkový počet posazení menší. Dojdeme k němu např. následovně. Kruhové posazení kolem stolu "roztrhneme" a zapíšeme lineárně. Např. ABCFDE je zápis, kdy A sedí na 1. židli, . . . , E sedí na 6. židli. Postupným otáčením tohoto posazení o 0 až 5 židlí dostaneme celkem 6 jeho zápisů: ABCFDE, BCFDEA, CFDEAB, FDEABC, DEABCF, EABCFD. Celkový počet zápisů je tedy 6 krát větší než počet posazení. Protože zápisů je $P(6)$, je hledaný počet posazení $\frac{P(6)}{6} = \frac{6!}{6} = 5!$.

Příklad 4.35. Kolik existuje posloupností n nul a k jedniček, ve kterých žádné dvě jedničky nejsou vedle sebe?

Představme si posloupnost n nul. Na začátku, mezi nulami a na konci této posloupnosti je celkem $n + 1$ míst (např. pro posloupnost 000 jsou to místa _0_0_0_). Libovolnou posloupnost n nul a k jedniček, která splňuje požadované podmínky, tak, že na vzniklých $n + 1$ míst umístíme k jedniček. Takových možností je právě tolik, kolika způsoby můžeme z $n + 1$ míst (mezi nulami) vybrat k míst (na každé z nich dáme jedničku), tedy právě $\binom{n+1}{k}$. Počet hledaných posloupností je tedy $\binom{n+1}{k}$.

Shrnutí

Kombinatorika se zabývá zjišťováním počtu možností, které mnohou nastat za předem daných podmínek. Základní kombinatorická pravidla jsou pravidlo součtu a pravidlo součinu. Pomocí nich se dají určit např. počty možností různých typů výběrů. Mezi základní typy výběrů patří permutace, variace a kombinace. Permutace n prvků je jejich libovolné uspořádání. Variace k prvků z n prvků je libovolný výběr k prvků z n prvků, ve kterém na pořadí vybíraných prvků záleží. Kombinace k prvků z n prvků je libovolný výběr k prvků z n prvků, ve kterém na pořadí vybíraných prvků nezáleží. Variace a kombinace s opakováním jsou podobné výběry, ve kterých se vybírané prvky mohou opakovat.

Pojmy k zapamatování

- pravidla součtu a součinu,
- permutace a permutace s opakováním,
- variace a variace s opakováním,
- kombinace a kombinace s opakováním.

Kontrolní otázky

1. *Co říká pravidlo součtu? Co říká pravidlo součinu?*
2. *Čím se liší permutace a variace? Čím se liší variace a kombinace?*
3. *Čím se liší permutace a permutace s opakováním? Čím se liší variace a variace s opakováním? Čím se liší kombinace a kombinace s opakováním?*
4. *Čím se liší aspekt opakování u permutací s opakováním, variací s opakováním a kombinací s opakováním?*

Cvičení

1. Kolik existuje v soustavě o základu n nezáporných čísel, které mají právě k číslic?
2. Kolik různých slov lze získat z akronymu WYSIWYG?
3. Dokažte matematickou indukcí, že $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ pro všechna $n \in N$ a $k = 0, 1, \ldots, n$.
4. Definujme indukcí $P^1(X) = P(X)$ a pro $n > 1$ $P^n(X) = P(P^{n-1}(X))$. Je-li množina X konečná, kolik prvků má $P^n(X)$?
5. Kolik má n-prvková množina m-prvkových podmnožin ($m < n$)?
6. Kolik existuje funkcí m prvkové do n prvkové množiny?
7. Kolik existuje injektivních funkcí z m prvkové do n prvkové množiny?
8. Kolik existuje n-árních operací na m-prvkové množině? Kolik z nich je injektivních? Kolik jich je surjektivních?
9. Krotitel má do arény přivést za sebou jdoucích 5 lvů a 4 tygry. Přitom žádní dva tygři nesmí jít bezprostředně za sebou (musí mezi nimi být lev). Kolika způsoby to lze provést? Na pořadí tygrů i lvů záleží.
10. Rozeberte předchozí cvičení pro případ n lvů a k tygrů.
11. Na poličce je 12 knih. Kolika způsoby lze vybrat 5 z nich tak, aby žádné dvě z vybraných nestály vedle sebe? Jak je to při výběru k knih z n?

Úkoly k textu

1. U Příkladů 4.1, 4.2, 4.3 zdůvodněte použité kombinatorické úvahy.

2. Vraťme se k Příkladu 4.3. Jaký je největší počet k kódových posloupností binárního kódu délky n, který umožňuje opravu až t-násobných chyb? t-násobnou chybou vznikne z daného slova slovo, které se od daného liší právě v t pozicích. Příklad 4.3 tedy dává odpověď pro $t = 1$. [Odpověď: $\frac{2^n}{1+n+\binom{n}{2}+\cdots+\binom{n}{r}}$.]

3. Vraťme se k Příkladu 4.8. Navrhněte různé tvary registračních značek a pro každý tvar spočítejte odpovídající počet značek, které lze přidělit. Jaké pravidlo pro návrh tvaru registračních značek plyne?

4. Zdůvodněte podrobně Větu 4.13.

5. Zdůvodněte podrobně Větu 4.16.

6. Zdůvodněte podrobně Větu 4.24.

   Promyslete si a zdůvodněte důkaz Věty 4.30.

Řešení

1. $(n-1)\cdot n^{k-1}$.
   Návod: Jako první číslici lze použít $n-1$ číslic (nelze 0), na každou z dalších $k-1$ pozic pak n číslic. Podle principu součinu to lze celkem $(n-1)\cdot n^{k-1}$ způsoby.
2. 1260.
   Návod: Je to $P(2,2,1,1,1)$.
3. Dokažte matematickou indukcí, že $\binom{n}{k}+\binom{n}{k-1}=\binom{n+1}{k}$ pro všechna $n\in N$ a $k=0,1,\ldots,n$.
4. Označme $k=|X|$. Pak $|P^1(X)|=2^k$, $|P^2(X)|=2^{2^k}$, atd. Obecně je $|P^n(X)|=2^{\overset{k}{\overset{\vdots}{2^{2^{\cdot}}}}}$ (dvojka je tam k krát).
5. $\binom{n}{m}$, je to právě počet kombinací m z n.
6. $\overline{V}(n,m)=n^m$.
   Návod: Mějme $X=\{x_1,\ldots,x_m\}$, $Y=\{y_1,\ldots,y_n\}$. Libovolná funkce f je dána uspořádanou m-ticí $\langle f(x_1),\ldots,f(x_m)\rangle$ hodnot $f(x_i)\in Y$. Výběr každé takové m-tice je variace m z n s opakováním. Těch je $\overline{V}(n,m)=n^m$.
7. Pro $m\leq n$ existuje $V(n,m)$ injektivních funkcí, pro $m>n$ žádná.
   Návod: Viz předchozí cvičení, jde o variace bez opakování.
8. m^{m^n}.
   Návod: Pro $|X|=m$ je to počet zobrazení množiny X^n do množiny X. Protože $|X^n|=m^n$, je jich n^{m^n} (viz předchozí cvičení).
9. Existuje 43200 způsobů.
   Návod: Lvy lze rozmístit $P(5)=5!=120$ způsoby. Zbývá 6 míst pro umístění tygrů (na začátku, mezi lvy a na konci). Do nich lze tygry umístit $V(6,4)=360$ způsoby. Podle pravidla součinu existuje celkem $120\cdot 360=43200$ způsobů.
10. Pro $k\leq n+1$ existuje $P(n)\cdot V(n+1,k)$ způsobů. Pro $k>n+1$ takový způsob neexistuje.
11. Existuje 56 možností. V obecném případě existuje $\binom{n+k-1}{k}$ možností (pokud $2k-1\leq n$, jinak žádná možnost neexistuje).
    Návod: Každý každý takový výběr k knih z n knih můžeme reprezentovat posloupností k jedniček (na pozicích vybraných knih) a $n-k$ nul (na pozicích nevybraných knih), ve které se nevyskytují sousedící jedničky (vybrané knihy nestojí vedle sebe). Těch je podle Příkladu 4.35 $\binom{n-k+1}{k}$.

Studijní cíle: Po prostudování kapitol 4.4 a 4.5 by student měl být znát princip inkluze a exkluze a umět ho použít. Dále by měl znát základy počítání pravděpodobností. Student by měl umět v základních úlohách samostatně provést správnou kombinatorickou úvahu.

Klíčová slova: princip inkluze a exkluze, pravděpodobnost, počítání pravděpodobnosti

Potřebý čas: 160 minut.

4.4 Princip inkluze a exkluze

V nabídce volitelných předmětů je němčina a angličtina. Němčinu si zvolilo 15 studentů, angličtinu 30 studentů. 5 studentů si zvolilo nemčinu i angličtinu. Kolik studentů si jako volitelný předmět vybralo cizí jazyk (tj. němčinu nebo angličtinu)? Označme N a A po řadě množiny studentů, kteří si zapsali němčinu a angličtinu. Sečteme-li $|N|$ (počet těch, kteří si zapsali němčinu) a $|A|$ (počet těch, kteří si zapsali anličtinu), počítáme dvakrát ty, kteří si zapsali němčinu i angličtinu (těch je $|N\cap A|$). Ty tedy musíme od $|N|+|A|$ odečíst. Počet $|N\cup A|$ těch, teří si zapsali němčinu nebo angličtinuje tedy

$$|N\cup A|=|N|+|A|-|N\cap A|=15+30-5=40.$$

Jiný příklad: Na jisté univerzitě je 56 učitelů členy americké informatické společnosti ACM (Association for Computing Machinery). Členové ACM si mohou přikoupit členství v některé z tzv. special interest

group (SIG, SIG jsou součásti ACM). Ze zmíněných 56 učitelů jich je 20 členy SIMOD (Special Interest Group on Management of Data), označme jejich množinu A_1; 15 členy SIGIR (Special Interest Group on Information Retrieval), označme jejich množinu A_2; 20 členy SIGKDD (Special Interest Group on Knowledge Discovery in Data), označme jejich množinu A_3. Dále je známo, že 10 jich je členy SIMOD i SIGIR, 8 jich je členy SIGMOD i SIGKDD, 7 jich je členy SIGIR i SIGKDD, 4 jsou členy SIGMOD, SIGIR i SIGKDD. Kolik z 56 členů ACM je členem některé z SIGMOD, SIGIR, SIGKDD? Ptáme se vlastně, kolik prvků má množina $A_1 \cup A_2 \cup A_3$, přitom známe $|A_1|$, $|A_2|$, $|A_3|$, $|A_1 \cap A_2|$, $|A_1 \cap A_3|$, $|A_2 \cap A_3|$ a $|A_1 \cap A_2 \cap A_3|$. Pokud bychom pouze sečetli $|A_1| + |A_2| + |A_3|$, pak jsou dvakrát započítáni ti z $A_1 \cap A_2$, z $A_1 \cap A_3$ a z $A_2 \cap A_3$, a dokonce třikrát jsou započítáni ti z $A_1 \cap A_2 \cap A_3$. To svádí k tomu říci, že $|A_1 \cup A_2 \cup A_3|$ se rovná

$$|A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| - 2|A_1 \cap A_2 \cap A_3|.$$

To je ale špatně. Odečteme-li totiž od $|A_1| + |A_2| + |A_3|$ počty $|A_1 \cap A_2|$, $|A_1 \cap A_3|$ i $|A_2 \cap A_3|$, odečítáme v každém z $|A_1 \cap A_2|$, $|A_1 \cap A_3|$ a $|A_2 \cap A_3|$ i počet těch, kteří jsou v $A_1 \cap A_2 \cap A_3$ (nakreslete si obrázek). Tedy od $|A_1| + |A_2| + |A_3|$ jsme odečetli $3|A_1 \cap A_2 \cap A_3|$. K tomu jsme pak ještě odečetli $2|A_1 \cap A_2 \cap A_3|$. Celkově jsme tedy od $|A_1| + |A_2| + |A_3|$ odečetli $|A_1 \cap A_2 \cap A_3|$ pětkrát a měli jsme to odečíst jen dvakrát. Správný výsledek tedy je

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + \\ &\quad + |A_1 \cap A_2 \cap A_3| = 20 + 15 + 20 - 10 - 8 - 7 + 4 = 24. \end{aligned}$$

Úvahy ukázané na výše uvedených příkladech jsou předmětem tzv. principu inkluze a exkluze (tj. zapojování a vylučování).

Věta 4.36 (princip inkluze a exkluze)**.** *Pro množiny $A_1, \ldots, A_n$ platí*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{\emptyset \neq I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|+1} |\bigcap_{i \in I} A_i|.$$

Zastavme se nejdřív nad tím, co princip inkluze a exkluze říká. Na levé straně rovnosti je počet prvků, které patří do sjednocení $A_1 \cup \cdots \cup A_n$, tj. alespoň do jedné z $A_1, \ldots, A_n$. Na pravé straně je součet výrazů $(-1)^{|I|+1} |\cap_{i \in I} A_i|$, kde I probíhá přes všechny neprázdné podmnožiny množiny $\{1, \ldots, n\}$. $|\cap_{i \in I} A_i|$ je počet prvků průniku množin, jejichž index patří do I, tj. např. pro $I = \{2, 3, 5\}$ je to $|A_2 \cap A_3 \cap A_5|$. Výraz $(-1)^{|I|+1}$ je roven 1, pokud I obsahuje lichý počet prvků, a je roven -1, pokud I obsahuje sudý počet prvků. Tedy: v součtu na pravé straně jsou počty prvků všech možných průniků (jednočlenných, dvoučlenných,. . . , až po n-členný) utvořené z $A_1, \ldots, A_n$, přitom počet prvků daného průniku je se znaménkem $+$ pro průniky lichého počtu množin a se znaménkem $-$ pro průniky lichého počtu množin. Zkontrolujte, že vzorec pro $n = 2$ i $n = 3$ dává právě dva vzorce, ke kterým jsme došli i příkladů s volitelnými předměty a s členstvím v SIG ACM. Přejděme nyní k důkazu Věty 4.36.

Důkaz. Vezměme libovolný prvek z $A_1 \cup \cdots \cup A_n$ a porovnejme, jakým číslem x "přispívá" na levé a na pravé straně dokazované rovnosti. Na levé straně přispívá zřejmě jedničkou. Pro pravou stranu je to složitější. Prvek x patří právě do, řekněme, k množin z množin $A_1, \ldots, A_k$. Můžeme předpokládat, že to jsou množiny $A_1, \ldots, A_k$ (kdyby ne, množiny přeznačíme). Pak x patří do nějakého průniku, který je na pravé straně rovnosti, právě když je to průnik nějakých množin z $A_1, \ldots, A_j$. Je-li to průnik lichého počtu množin, x do odpovídajícího výrazu $(-1)^{|I|+1} |\bigcap_{A_i}|$ přispívá číslem 1, je-li to průnik sudého počtu množin, x do výrazu $(-1)^{|I|+1} |\bigcap_{A_i}|$ přispívá číslem -1. Z $A_1, \ldots, A_k$ lze vytvářet jednoprvkové, . . . , k-prvkové průniky. Počet l-prvkových průniků je přitom $\binom{k}{l}$. Vidíme tedy, že x přispívá celkem na pravou stranu číslem

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

Jaká je hodnota tohoto součtu? Vezměme binomickou větu a dosaďme do (4.2) $x = -1$. Dostaneme

$$\begin{aligned} 0 = 0^k = (1-1)^k = (1+x)^k = \sum_{i=0}^{k} \binom{n}{k} x^i = 1 + \sum_{i=1}^{k} (-1)^i \binom{k}{i} = \\ = \quad 1 - (\binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \cdots + (-1)^{k+1} \binom{k}{k}). \end{aligned}$$

Odtud tedy vidíme, že hledaná hodnota součtu je 1. Prvek x tedy i nalpravou stranu přispívá jedničkou. Protože x byl libovolný, výrazy na levé a pravé straně dokazované rovnosti mají stejné hodnoty. □

Příklad 4.37. Kolik je přirozených čísel mezi 1 a 100 (včetně 1 i 100), která nejsou dělitelná ani dvěma, ani třemi nebo pěti? Princip inkluze a exkluze můžeme použít následovně. Označme

$$A_1 = \{n \in \mathbb{N} \mid 1 \leq n \leq 100,\ n \text{ je dělitelné } 2\}, \tag{4.3}$$
$$A_2 = \{n \in \mathbb{N} \mid 1 \leq n \leq 100,\ n \text{ je dělitelné } 3\}, \tag{4.4}$$
$$A_3 = \{n \in \mathbb{N} \mid 1 \leq n \leq 100,\ n \text{ je dělitelné } 5\}. \tag{4.5}$$

Pak přirozená čísla mezi 1 a 100 (včetně 1 i 100), která nejsou dělitelná ani dvěma, ani třemi nebo pěti, jsou právě prvky množiny $A = \overline{A_1} \cap \overline{A_2} \cap \overline{A_3}$. Protože

$$\overline{A_1} \cap \overline{A_2} \cap \overline{A_3} = \overline{A_1 \cup A_2 \cup A_3},$$

je $|A| = |\overline{A_1 \cup A_2 \cup A_3}| = 100 - |A_1 \cup A_2 \cup A_3|$. Podle principu inkluze a exkluze je

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

Zbývá tedy určit $|A_1|$, $|A_2|$, $|A_3|$, $|A_1 \cap A_2|$, $|A_1 \cap A_3|$, $|A_2 \cap A_3|$, $|A_1 \cap A_2 \cap A_3|$, což je snadné. Ukažme to na příkladu množiny $A_1 \cap A_2$. $A_1 \cap A_2$ je množina přirozených čísel mezi 1 a 100, která jsou dělitelná dvěma i třemi. To jsou ale právě ta čísla, která jsou dělitelná 6 (číslo je dělitelné 6, právě když je dělitelné 2 i 3). Těch je $\lfloor \frac{100}{6} \rfloor = 16$ (dolní celá část čísla $\frac{100}{6}$), tj. $|A_1 \cap A_2| = 16$. Podobně dostaneme $|A_1| = 50$, $|A_2| = 33$, $|A_3| = 20$, $|A_1 \cap A_3| = 10$, $|A_2 \cap A_3| = 6$, $|A_1 \cap A_2 \cap A_3| = 3$. Dosazením pak dostaneme $|A| = 100 - |A_1 \cup A_2 \cup A_3| = 26$.

4.5 Počítání pravděpodobnosti

Počítání pravděpodobností jednoduchých jevů je jednou z aplikací kombinatorického počítání, která je v praktickém životě velmi užitečná. Představme si, že házíme kostkou. Může padnout jednička, dvojka, trojka, čtyřka, pětka nebo šestka. Přitom každý z těchto výsledků má stejnou šanci (kostka je férová). Jaká je pravděpodobnost, že při hodu padne číslo dělitelné třemi? Jinými slovy, jaká je pravděpodobnost, že při hodu padne trojka nebo šestka? Celkový existuje 6 možných výsledků hodu kostkou. Z těchto právě dva výsledky (trojka a šestka) odpovídají jevu „padne trojka nebo šestka“. Chápeme-li pravěpědobnost jako počet kladných výsledků ku počtu všech možných výsledků, je to dvě ku šesti, tedy $\frac{2}{6} = 0.33333\ldots$.

Průvodce studiem

Otázkami o pravděpodobnostech a usuzování za nejistoty se zabývá teorie pravděpodobnosti. Velké množství případů, se kterými se prakticky setkáváme, má následující podobu.

Představme si, že se koná nějaký pokus, který skončí jedním z výsledků $e_1, \ldots, e_n$. Výsledkům $e_1, \ldots, e_n$ se říká *elementární jevy*. Předpokládáme, že každý z výsledků $e_1, \ldots, e_n$ má stejnou šanci, tj. elementární jevy jsou stejně pravděpodobné. Pokusem může být hod kostkou, elementární jevy jsou pak $1, 2, 3, 4, 5, 6$ (výsledky hodu). *Jev* je každá podmnožina $A \subseteq E = \{e_1, \ldots, e_n\}$. Jevem u hodu kostkou je např. množina $A = \{3, 6\}$ (padne číslo dělitelné třemi) nebo $B = \{2, 3, 4, 5, 6\}$ (padne číslo různé od 1). *Pravděpodobnost* $P(A)$ jevu A je dána vztahem

$$P(A) = \frac{|A|}{|E|},$$

tj. je to počet všech výsledků příznivých jevu A ku počtu všech možných výsledků. Např. pravděpodobnost toho, že padne číslo dělitelné 3 je tedy $P(A) = \frac{|\{3,6\}|}{|\{1,2,3,4,5,6\}|} = \frac{1}{3}$, pravděpodobnost, že padne číslo různé od 1 je $P(A) = \frac{|\{2,3,4,5,6\}|}{|\{1,2,3,4,5,6\}|} = \frac{5}{6}$.

Pravděpodobnost může nabývat hodnot od 0 do 1. 0 je pravděpodobnost nemožného jevu, např. že padne číslo, které je sudé i liché. 1 je pravděpodobnost jistého jevu, např. že padne číslo menší než 9.

Chceme-li určit pravděpodobnost nějaké události, můžeme jednoduše použít vzorec $P(A) = \frac{|A|}{|E|}$. K tomu je ale třeba učinit následující:

1. Určit množinu E všech elementárních jevů (výsledků) a ověřit, že jsou všechny stejně pravděpodobné,
2. určit jev $A \subseteq E$, který odpovídá dané události,
3. určit počet prvků množiny E, tj. určit $|E|$,
4. určit počet prvků množiny A, tj. určit $|A|$.

V krocích 1. a 2. si koncepčně ujasníme situaci (1. a 2. odpovídá nalezení správného pohledu na věc), v krocích 3. a 4. obvykle provedeme určité kombinatorické úvahy.

Začneme jednoduchými příklady.

Příklad 4.38. Házíme modrou a červenou kostkou. Jaká je pravděpodobnost, že na modré kostce padne sudé a na červené liché číslo?

Na sitaci se můžeme dívat takto: Výsledek, tj. elementární jev, je dán dvojicí čísel $\langle m, c\rangle$, kde $m, c \in \{1, 2, 3, 4, 5, 6\}$ a m a c jsou po řadě výsledek na modré a červené kostce. Tedy máme

$$E = \{\langle m, c\rangle \mid m, c \in \{1, 2, 3, 4, 5, 6\}\}.$$

Elementární jev $\langle m, c\rangle$ je příznivý události „na modré kostce padne sudé a na červené liché číslo“, právě když $m \in \{2, 4, 6\}$ a $c \in \{1, 3, 5\}$. Tedy

$$A = \{\langle m, c\rangle \mid m \in \{2, 4, 6\},\ c \in \{1, 3, 5\}\}.$$

Vidíme, že $|E| = 6 \cdot 6 = 36$ (přímo podle pravidla součinu) a že $|A| = 3 \cdot 3 = 9$ (podle pravidla součinu). Tedy hledaná pravděpodobnost $P(A)$ je $P(A) = \frac{|A|}{|E|} = \frac{9}{36} = 0.25$.

Příklad 4.39. Házíme dvěma kostkami, které jsou nerozlišitelné. Jaká je pravděpodobnost, že aspoň na jedné z nich padne dvojka?

Vezměme opět $E = \{\langle m, c\rangle \mid m, c \in \{1, 2, 3, 4, 5, 6\}\}$. Zajímá nás teď jev $A = \{\langle m, c\rangle \in E \mid m = 2 \text{ nebo } c = 2\}$ a jeho počet prvků. K němu můžeme dojít tak: Pro jevy $A_1 = \{\langle m, c\rangle \in E \mid m = 2\}$ (na modré padne dvojka) a $A_2 = \{\langle m, c\rangle \in E \mid c = 2\}$ (na červené padne dvojka) zřejmě platí $A = A_1 \cup A_2$. Protože $A_1 \cap A_2 = \{\langle 2, 2\rangle\}$, je podle principu inkluze a exkluze

$$|A| = |A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = 6 + 6 - 1 = 11.$$

Pravděpodobnost, že aspoň na jedné z kostek padne dvojka je tedy $P(A) = \frac{|A|}{|E|} = \frac{11}{36}$.

Při hledání vhodného pohledu na věc (viz bod 1.) musíme být opatrní. Podívejme se znovu na Příklad 4.39. Příklad svádí k následujícímu pohledu. Na hody se můžeme dívat jako na kombinace 2 z 6 s opakováním. Pro to, zda padne dvojka, totiž není důležité, jestli padne na jedné nebo druhé kostce. Důležité je vědět, že např. padla trojka a čtyřka, nezáleží na tom, na které z kostek ta čísla padla. Tedy hod můžeme chápat jako kombinaci 2 z 6 s opakováním a těch je podle Věty 4.30 $\overline{C}(6, 2) = \binom{6+2-1}{6-1} = \binom{7}{5} = 21$. Máme tedy 21 elementárních jevů. Kolik z nich je příznivých jevu A, který popisuje, že padla aspoň jedna dvojka? Je jich 6. Skutečně, v kombinaci, která do jevu patří, musí být jeden z prvků dvojka a ten druhý může být libovolný z 1, 2, 3, 4, 5, 6. To je celkem 6 možností. Hodnota pravděpodobnosti $P(A)$ je tedy $P(A) = \frac{|A|}{|E|} = \frac{6}{21}$. To je ale jiný výsledek než ten, který jsme dostali v Příkladu 4.39! Kde je chyba (zkuste na to přijít nejdřív sami)? Je v tom, že když se na elementární jevy díváme jako na kombinace s opakováním, nejsou všechny stejně pravděpodobné. Např. kombinace, ve které jsou dvě trojky (padnou dvě trojky) je (dvakrát) méně pravděpodobná než kombinace, ve které je trojka a šestka. Výsledek „dvě trojky“ totiž může nastat právě jedním způsobem: na modré i červené padne trojka. Výsledek „trojka a šestka“ může naproti tomu padnout dvěma způsoby: na modré trojka a na červené šestka, nebo na modré šestka a na červené trojka. Vzorec $P(A) = \frac{|A|}{|E|}$ tedy nemůžeme použít.

Příklad 4.40. Jaká je pravděpodobnost, že při rozdávání 4 karet z balíčku 32 hracích karet dostaneme čtyři sedmičky? Jaká je pravděpodobnost, že dostaneme 2 krále a a dvě esa?

V tomto případě můžeme za elementární jevy považovat čtyřprvkové množiny karet (podmnožiny 32-prvkové množiny všech karet). Každému rozdání totiž odpovídá jedna čtyřprvková množina karet (na pořadí nezáleží). Pravděpodobnosti, že dostaneme čtyři sedmičky je $1/\binom{32}{4}$. Pravděpodobnost, že dostaneme 2 krále a 2 esa je $\binom{4}{2}\binom{4}{2}/\binom{32}{4}$.

Shrnutí

Princip inkluze a exkluze je často používaným kombinatorickým principem. Udává počet prvků sjednocení několika množin pomocí počtu prvků průniků jednotlivých množin.
Počítání pravděpodobností jednoduchých jevů patří mezi základní aplikace kombinatorického počítání. Pravděpodobnost jevu je dána podílem počtu možností příznivých danému jevu ku počtu všech možností. Kombinatorické úvahy se uplatní při určování počtu množností.

Pojmy k zapamatování

- princip inkluze a exkluze,
- elementární jev, jev,
- pravděpodobnost.

Kontrolní otázky

1. *Co říká princip inkluze a exkluze?*
2. *Jak se zjednoduší vzorec z principu inkluze a exkluze, jsou-li množiny $A_1, \ldots, A_n$ po dvou disjunktní?*
3. *Jaký je rozdíl mezi pojmy jev a elementární jev?*
4. *Co je to pravděpodobnost jevu a jak je definována?*

Cvičení

1. Určete počet přirozených čísel mezi 1 a 2000 (včetně 1 i 2000), která nejsou dělitelná ani 2, ani 3, ani 5.
2. Určete počet přirozených čísel mezi 1 a 2000 (včetně 1 i 2000), která nejsou dělitelná ani 2, ani 3, ani 5, ani 7.
3. Určete počet přirozených čísel mezi 1 a 2000 (včetně 1 i 2000), která nejsou dělitelná ani 2, ani 3, ani 5, ale jsou dělitelná 7.
4. Kolika způsoby můžeme rozmístit 15 různých knih do 5 přihrádek tak, aby v každé přihrádce byla aspoň jedna kniha, ale nejvýše 4 knihy?
5. Házíme dvěma kostkami. Máme si vsadit na číslo, které vzejde jako součet výsledků na jednotlivých kostkách. Na jaké číslo vsadíme?
6. Rozveďte výpočet u Příkladu 4.40.
7. Házíme třikrát po sobě kostkou. Jaká je pravděpodobnost, že výsledek při druhém i při třetím hodu je větší než výsledek při prvním hodu?
8. Házíme třikrát po sobě kostkou. Jaká je pravděpodobnost, že výsledek při druhém hodu je větší než výsledek při prvním hodu a že výsledek při třetím hodu je větší než výsledek při druhém hodu?

Úkoly k textu

1. U Příkladů 4.1, 4.2, 4.3 zdůvodněte použité kombinatorické úvahy.

2. Vraťme se k Příkladu 4.3. Jaký je největší počet k kódových posloupností binárního kódu délky n, který umožňuje opravu až t-násobných chyb? t-násobnou chybou vznikne z daného slova slovo, které se od daného liší právě v t pozicích. Příklad 4.3 tedy dává odpověď pro $t = 1$. [Odpověď: $\frac{2^n}{1+n+\binom{n}{2}+\cdots+\binom{n}{r}}$.]

3. Vyřešte podrobně Příklad 4.37.

4. Na základě Příkladu 4.37 dokažte následující tvrzení: Jsou-li podmnožiny $A_1, \ldots, A_n$ nějaké k-prvkové množiny X, pak počet prvků množiny X, které nepatří ani jedné z množin $A_1, \ldots, A_n$ je $k - \sum_{\emptyset \neq I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|+1} |\bigcap_{i \in I} A_i|$.

5. Vysvětlete podrobně chybu popsanou v odstavci na Příkladem 4.39.

Řešení

1. 534.
2. 458.
3. 76.
4. $15!\dot{(}\binom{14}{10} - \binom{5}{1}\binom{10}{6} + \binom{5}{2}\binom{6}{2})$.
5. 6, 7 nebo 8.
6. Návod: Počet všech čtyřprvkových podmnožin 32-prvkové množiny je $\binom{32}{4}$; existuje jediná z nich, která obsahuje samé sedmičky; $\binom{4}{2}\binom{4}{2}$ z nich obsahuje 2 krále a 2 esa.
7. $55/216$.
8. $5/54$.

Reference

[Goo98] Goodaire E. G., *Parmenter M. M.: Discrete Mathematics with Graph Theory*. Prentice-Hall, Inc., 1998.

[Gri99] Grimaldi R.: *Discrete and Combinatorial Mathematics. An Applied Introduction. 4th ed.* Addison Wesley, Reading, MA, 1999.

[KlYu95] Klir G. J., Yuan B.: *Fuzzy Sets and Fuzzy Loic. Theory and Applications.* Prentice Hall, Upper Saddle River, NJ, 1995.

[MaNe00] Matoušek J., Nešetřil J.: *Kapitoly z diskrétní matematiky.* Karolinum, Praha, 2000.

[Mau91] Maurer S. B., Ralston A.: *Discrete Algorithmic Mathematics*. Addison Wesley, 1991. DOPLNIT NOVEJSI REF.?

[PrYe73] Preparata F. P., Yeh R. T.: *Introduction to Discrete Structures. For Computer Science and Engineering.* Addison Wesley, Reading, MA, 1973.

[Soch01] Sochor A.: Klasická matematická logika. Karolinum, Praha, 2001 (v prodeji, velmi dobře psaná s řadou doplňujících informací).

[Šve02] Švejdar V.: Logika, neúplnost a složitost. Academia, Praha, 2002.

[Vil77] Vilenkin N. J.: *Kombinatorika.* SNTL, Praha, 1977.

A Seznam obrázků

B Seznam tabulek