KATEDRA INFORMATIKY

PŘÍRODOVĚDECKÁ FAKULTA

UNIVERZITA PALACKÉHO

DISKRÉTNÍ MATEMATIKA PRO INFORMATIKY I

RADIM BĚLOHLÁVEK, VILÉM VYCHODIL

VÝVOJ TOHOTO UČEBNÍHO TEXTU JE SPOLUFINANCOVÁN
EVROPSKÝM SOCIÁLNÍM FONDEM A STÁTNÍM ROZPOČTEM ČESKÉ REPUBLIKY

Olomouc 2006

Abstrakt

Text je úvodem do vybraných partií diskrétní matematiky a souvisejících oblastí. Postupně seznamuje čtenáře s úvodem do logiky, množin, relací a funkcí, kombinatorikou, teorií grafů a vybranými pokročilejšími partiemi z teorie relací a logiky. 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 oboru Aplikovaná informatika uskutečňovaného v kombinované formě na Přírodovědecké fakultě Univerzity Palackého v Olomouci. Může být užitečný i studentům jiných informatických a matematických oborů a těm, kteří se chtějí seznámit se se základy diskrétní matematiky.

Obsah

1 Logika

Studijní cíle: Po prostudování kapitoly by student měl aktivně znát základy syntaxe a sémantiky výrokové logiky. Student by měl umět zapisovat výroky pomocí formulí a vyšetřovat pravdivost pomocí tabulkové metody.

Klíčová slova: disjunkce, ekvivalence, formule, implikace, jazyk výrokové logiky, konjunkce, kontradikce, logická operace, logická spojka, logika, negace, podformule, pravdivostní ohodnocení, sémantická ekvivalence, sémantika, syntaxe, tabelace, tautologie, výrok, výroková logika, výrokový symbol

Potřebný čas: 120 minut.

1.1 Co a k čemu je logika

Logika je věda zabývající se *usuzováním.* Zkoumá pojmy jako jsou *pravdivost, dokazatelnost, vyvratitelnost* a zabývá se jejich vzájemnými vztahy. Logika si klade otázky typu: „Je každé dokazatelné tvrzení pravdivé?“, „Co plyne z toho že jsme došli nějakou úvahou ke sporu?“. Hlavními rysy soudobé logiky jsou idealizace a formalizace – logika zkoumá pouze formu usuzování, nezabývá se obsahem tvrzení, psychologickými interpretacemi a podobně. Co se tím má na mysli? Vezmeme-li například dvojici tvrzení

„Jestliže prší, pak jsou silnice mokré“ a „Prší“,

pak z nich přirozenou úvahou odvozujeme „Silnice jsou mokré“. Vezmeme-li dvojici

„Pokud je Petr unavený, pak (Petr) spí“ a „Petr je unavený“,

pak odvodíme „Petr spí“. V těchto dvou příkladech vyplývalo z dvojice tvrzení další tvrzení. Ačkoliv měly obě dvojice tvrzení zcela jiný obsah (mokré silnice versus spánek), měly stejnou formu a z obou jsme vyvodili nový závěr stejným způsobem (úsudkem). Formu předchozích tvrzení lze symbolicky znázornit takto: $A \Rightarrow B$ („když A, pak B“) a A. Úsudek, který jsme použili k odvození závěrů byl: z $A \Rightarrow B$ a A odvodíme B. Pro uvedené rysy bývá moderní logika označována jako *formální logika* (*symbolická logika*).

Logika zkoumá formální aspekty usuzování.

Průvodce studiem

Důvod pro formalizaci tvrzení a úsudků plyne přímo povahy problémů, kterým se logika věnuje. Jelikož se logika zabývá aspekty usuzování, je zejména potřebné, aby byly pojmy jako je *tvrzení* či *úsudek* přesně a dostatečně jednoduše zavedené. Jedině tak budeme s to zkoumat jejich vlastnosti – například rozhodovat, zda-li je konkrétní úsudek správný či nikoliv, zda-li dané tvrzení vyplývá z jiných a podobně.

Logika, jako vědní disciplína, se vyvíjela během staletí a vyvíjely se i její cíle. Za zakladatele logiky je považován řecký filosof Aristotelés. Od svých počátků byly otázky logiky směrovány na podstatu lidského usuzování a byly tedy svou povahou hlavně filozofické – odtud pochází označení *filosofická logika*. Na přelomu 19. a 20. století došlo k výrazné formalizaci logiky – šlo především o formalizaci usuzování v matematice a v jiných vědách, filosofické aspekty byly úplně pominuty. V současnosti neexistuje žádná zřetelná hranice mezi formální a filosofickou logikou. Mnohé aspekty usuzování zkoumané filosofickou logikou se podařilo formalizovat a zkoumat je čistě matematickými metodami. Na druhou stranu, formální logika dokázala odpovědět na některé zásadní otázky, kterými se zabývali filosofové již od starověku.

Vztah logiky a informatiky je velmi těsný. Logika je důležitá v informatice (formální metody specifikace, verifikace, analýzy dat) a elektrotechnice (logika el. obvodů). Naopak, výsledky informatických disciplín (teorie informace, teorie jazyků) jsou nepostradatelné v logice. Logika se

Logika je základem formálních metod v informatice.

zabývá například algoritmickými aspekty usuzování a konstrukcí automatických dokazovacích systémů (jde o speciální algoritmy), které jsou schopny, byť omezeně, mechanicky odvozovat tvrzení z jiných.

Doposud jsme řekli, že logika formalizuje pojmy jako je tvrzení a úsudek, ale nespecifikovali jsme jak. Formalizace pojmů a práce s nimi je ve skutečnosti závislá na konkrétním *logickém kalkulu,* se kterým pracujeme. Logický kalkul lze zjednodušeně chápat jako soubor pravidel, která mimo jiné specifikují, jak „jemná“ formalizace se používá. Vše si ukažme na příkladu. Uvažujme tvrzení

„Pokud má Petr deset korun, pak si může koupit čokoládu.“

V případě, že si nebudeme všímat struktury sdělení v jednotlivých větách tohoto souvětí, se jedná o tvrzení ve tvaru „když A, pak B“. V druhé větě se však vyskytuje vazba „moci“, z tohoto úhlu pohledu se jedná o tvrzení tvaru „když A, pak může B“. Při ještě jemnější formalizaci bychom mohli zachytit i jednotlivé objekty („deset korun“, „čokoláda“, „Petr“) a vztahy mezi nimi („mít“, „koupit“). Zbytek úvodní kapitoly se věnuje *výrokové logice* (*výrokovému kalkulu*), která z pohledu formalizace zkoumá usuzování na úrovni vět v souvětích. V kapitole 6.3 představíme *predikátovou logiku,* která z pohledu formalizace zkoumá usuzování až na úrovni jednotlivých větných členů.

1.2 Výroková logika (úvod)

Výroková logika zkoumá usuzování o výrocích.

Výrokem intuitivně chápeme tvrzení, pro které má smysl ptát se, zda-li je pravdivé. Například „Prší.“ je výrok, „Byl jsem v obchodě a koupil jsem si knihu.“ je výrok, „$2 + 2 = 6$“ je výrok, ale „kniha v obchodě“ není výrok, „$2 + 2$“ není výrok. Je zcela v souladu s intuicí, že z výroků lze vytvářet výroky složitější tím, že je mezi sebou kombinujeme pomocí dodatečných slovních konstrukcí jako jsou „a“, „nebo“, „pokud, . . . pak . . . “, „ne“ (to jest „neplatí, že . . . “). Například výrok „Pokud prší a svítí slunce, pak je na obloze duha“ lze chápat jako výrok složený z výroků „Prší“, „Svítí slunce“, „Na obloze je duha“ pomocí vazeb „a“, „pokud . . . , pak . . . “. Výroková logika formalizuje tyto slovní vazby pomocí *logických spojek,* proto se někdy nazývá *logika výrokových spojek.* Formalizace ve výrokové logice nejde za hranici výroků, to jest výroková logika neformalizuje jednotlivé objekty a vztahy mezi nimi, nepracuje s časem, ani s vazbami typu „smět“, „moci“, „vědět“ a podobně.

Průvodce studiem

Výroková logika se soustředí na formu usuzování o výrocích – to jest nezajímá nás obsah výroků, ale pouze forma usuzovaného. Na jednu stranu tím v jistém smyslu ztratíme, neboť naše rozlišovací schopnost odhlédnutím od obsahu výroků klesne – výroky se stejnou formou, ale různým obsahem, pro nás budou nerozlišitelné. Na druhou stranu, soustředěním se pouze na formu nám umožní objevit zákonitosti, kterými se řídí usuzování nad jakýmikoli výroky, tedy výroky s libovolným obsahem. Výsledky, které získáme, budeme tedy moci použít na libovolné výroky.

1.2.1 Jazyk výrokové logiky, formule výrokové logiky

Nyní přikročíme k přesnému zavedení základních pojmů a vybudování formálního systému výrokové logiky (dále VL). Doposud jsme se o pojmech jako je „výrok“ bavili pouze na intuitivní úrovni, která byla nepřesná a neuchopitelná matematickými metodami. Intuitivní představu výroku je dobré mít neustále na paměti – je důležitá z hlediska vazby (formální) výrokové logiky na přirozené usuzování, pro naše další účely je však pouze intuitivní zavedení pojmů nedostačující kvůli vágnosti slovního popisu a přirozeného jazyka – v našem případě češtiny. Místo

Přirozený jazyk se pro formalizaci nehodí – je komplikovaný a nejednoznačný.

komplikovaného a nejednoznačného přirozeného jazyka nejprve zavedeme vhodný jednoduchý a přesný (*formální*) *jazyk výrokové logiky,* ve kterém budeme výroky popisovat.

Některé výroky jsou *složeny z jiných* užitím pomocných slovních konstrukcí („Prší *a* svítí slunce.“), jiné nikoliv („Prší.“) a jsou v tomto smyslu nedělitelné – *atomické.* Atomické výroky budeme v jazyku VL označovat speciálními symboly, kterým budeme říkat *výrokové symboly.* Slovní konstrukce, kterými se výroky spojují ve složené výroky, budeme v jazyku VL označovat *symboly výrokových spojek.* Výroky složené z jiných budeme v jazyku VL zapisovat pomocí výrokových symbolů a symbolů výrokových spojek, pro přehlednost a jednoznačnost je budeme vhodně oddělovat *závorkami.* Nyní můžeme pojem *jazyk VL* přesně zavést.

Formální jazyk odstraňuje nevýhody přirozeného jazyka.

Jazyk výrokové logiky se skládá z

- *výrokových symbolů*: $p, q, r, \dots,$
- *symbolů výrokových spojek*:
  $\neg$ (negace), $\Rightarrow$ (implikace), $\wedge$ (konjunkce), $\vee$ (disjunkce), $\Leftrightarrow$ (ekvivalence),
- *pomocných symbolů*: *závorek* (,).

Poznámka 1.1. (1) Výrokové symboly označujeme podle potřeby s indexy, to jest $p_1, p_2, \dots$ Dále budeme předpokládat, že výrokových symbolů máme k dispozici nekonečně mnoho – vezmeme-li konečně mnoho výrokových symbolů $p_1, p_2, \dots, p_n$, pak máme vždy k dispozici další výrokové symboly, které se mezi $p_1, p_2, \dots, p_n$ nenacházejí.

(2) Symboly výrokových spojek $\neg$ („neplatí, že . . . “), $\Rightarrow$ („když . . . , pak . . . “), $\wedge$ („. . . a . . . “), $\vee$ („. . . nebo . . . “), $\Leftrightarrow$ („. . . , právě když . . . “), zastupují pouze zlomek vazeb, které lze vyjádřit přirozeným jazykem – v tomto místě jsme oproti přirozenému jazyku provedli výrazné zjednodušení.

(3) V dalších kapitolách budeme někdy používat různé typy závorek (,), [,], . . . kvůli zvýšení přehlednosti. Přísně vzato bychom si ale vystačili pouze s jedním typem závorek.

Nyní již máme zaveden jazyk, ve kterém budeme výroky popisovat. Potřebujeme ještě jednoznačná pravidla zapisování výroků v tomto jazyku. Výroky budeme zapisovat jako konečné posloupnosti symbolů jazyka VL splňující další požadavky. Dostáváme se tak k následujícímu pojmu.

Formule jsou přesným zavedením intuitivního pojmu výrok.

Formule (daného jazyka) výrokové logiky jsou definovány následovně:

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

Nejprve nahlédněme, že definice formule je skutečně správná, nejedná se o definici kruhem, protože v druhém bodu definice se zavádějí formule složitější z formulí jednodušších. Všechny formule vznikají aplikací předchozích dvou bodů. Dále si všimněme, že pojem formule se vztahuje k jazyku VL, měli bychom tedy správně hovořit o „formulích daného jazyka VL“. Ve většině případů však bude jazyk zřejmý z kontextu proto budeme hovořit pouze o „formulích VL“ nebo jen o „formulích“.

Příklad 1.2. Pokud chceme rozhodnout, zda-li je daná posloupnost symbolů jazyka VL formule, stačí pouze mechanicky postupovat podle předchozí definice. Například p, q_1, $\neg p$, $(p \Rightarrow q)$, $\neg\neg(\neg p \Leftrightarrow p)$, $(\neg p \wedge (q \Rightarrow \neg r))$ jsou formule. Zdůvodníme podrobně pro $(\neg p \wedge (q \Rightarrow \neg r))$: každý z výrokových symbolů p, q, r je formule dle prvního bodu definice. Potom dle druhého bodu postupně dostáváme, že $\neg p$, $\neg r$ jsou také formule, dále $(q \Rightarrow \neg r)$ je formule, proto i $(\neg p \wedge (q \Rightarrow \neg r))$ je formule. Na druhou stranu $\neg(p)$, $(p\neg q)$, $(p \Rightarrow (q \wedge r)$, $p \Rightarrow r$, $(p \vee q \vee r)$, $\Rightarrow p$ nejsou formule.

Abychom zpřehlednili zápis formulí, přijmeme nyní konvenci o *vynechávání vnějších závorek.*

Vynecháním vnějších závorek zpřehledňujeme zápis formulí.

Formule tvaru $(\varphi \Rightarrow \psi)$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \Leftrightarrow \psi)$ budeme psát bez vnějších závorek, to jest $\varphi \Rightarrow \psi, \varphi \wedge \psi, \varphi \vee \psi, \varphi \Leftrightarrow \psi$. Závorky, které mohou být ve formulích φ a ψ, ale nevypouštíme.

Přepis tvrzení z přirozeného jazyka do jazyka VL a zpět není předmětem zkoumání formální logiky, protože je v mnoha ohledech zatížen psychologickými aspekty, vyžaduje znalost problémové domény, což je právě to, od čeho formální logika odhlíží. Přesto je potřebné mít v přepisu jistý cvik. Pokud na úrovni formalizovaného myšlení objevíme zákonitost, můžeme ji pak snadno porovnat s jejím protějškem přirozeného (intuitivního) usuzování – někdy tak můžeme objevit netušené zákonitosti v intuitivním usuzování, nebo můžeme naopak zjistit, že formalizace, kterou jsme zvolili, není vhodná – třeba se nechová dost přirozeně. Potřeba „umět číst formule" je nezbytná ve většině informatických a matematických disciplin, ve kterých se formalizované výroky používají k přesnému vyjadřování vztahů v definicích, algoritmech, větách a podobně. Nyní si uvedeme stručný návod, jak bychom při formalizaci výroků a čtení formulí měli postupovat, důraz je kladen na vhodné použití spojek.

- *negace* $\neg$ se na rozdíl od ostatních spojek váže pouze s jedním výrokem – o spojce říkáme, že je *unární.* Formuli $\neg\varphi$ čteme „neplatí, že φ". Pokud například výrokový symbol p formalizuje výrok „Venku prší", pak $\neg p$ formalizuje výrok „Venku *ne*prší", nebo kostrbatěji: „Neplatí, že venku prší". Je-li q formalizace výroku „5 je liché číslo", pak $\neg q$ je formalizací výroku „5 není liché číslo".

  Zde se prosím vyvarujme jakýchkoliv úvah o pravdivosti či nepravdivosti těchto výroků – – pořád zkoumáme výroky *pouze z hlediska jejich formy, nikoliv obsahu* nebo nějaké jejich *intuitivní či „přirozené" interpretace.* Kdybychom za negaci výroku „5 je liché číslo" považovali výrok „5 je sudé číslo", už bychom tím nepřípustně přihlédli k jeho obsahu!

Všechny dále uvedené spojky se vztahují vždy ke dvěma výrokům – říkáme jim *binární spojky.*

- *konjunkce* $\wedge$ vyjadřuje vazbu „a". Formuli $\varphi \wedge \psi$ čteme „φ a ψ". Podotkněme, že konjunkce se vztahuje k platnosti výroků, nikoliv k jejich obsahu ani k jejich časové návaznosti. Budou-li například výrokové symboly p, q formalizovat výroky „Egypťané postavili pyramidy" a „Člověk přistál na měsíci", pak $p \wedge q$ formalizuje výrok „Platí, že egypťané postavili pyramidy a platí, že člověk přistál na měsíci", nikoliv výrok „Platí, že egypťané postavili pyramidy a (současně) člověk přistál na měsíci".

- *disjunkce* $\vee$ vyjadřuje vazbu „nebo", nikoliv však ve smyslu „buď... a nebo... ", což je tak zvaná vylučovací disjunkce, ale ve smyslu platnosti alespoň jednoho z výroků. Formuli $\varphi \vee \psi$ čteme „φ nebo ψ". Pokud například výrokové symboly p a q vyjadřují výroky „Prší" a „Svítí slunce", pak $p \vee q$ vyjadřuje výrok „Prší nebo svítí slunce", ale zároveň nevylučuje platnost výroku „Prší a svítí slunce".

  I když jsme pro vylučovací disjunkci nezavedli samostatnou spojku, můžeme ji snadno vyjádřit třeba pomocí $\neg$, $\wedge$ a $\vee$. Jsou-li φ, ψ formule, pak $(\varphi \vee \psi) \wedge \neg(\varphi \wedge \psi)$ vyjadřuje, že platí φ nebo ψ, ale ne obě.

- *implikace* $\Rightarrow$ vyjadřuje výrokovou vazbu „když..., pak... " opět však ne ve smyslu času, ale ve smyslu „pokud platí..., pak platí... ". Formuli $\varphi \Rightarrow \psi$ lze číst mnoha způsoby, například „pokud φ, pak ψ", „ψ za předpokladu, že φ", „φ dostačuje pro ψ", „ψ je nutné pro φ", „φ, jen když ψ".

  Implikace obecně nelze obracet bez ztráty jejich významu, volně řečeno, nelze obracet příčinu a důsledek. Pokud například výrokové symboly p a q vyjadřují výroky „x je dělitelné šesti" a „x je dělitelné dvěma", pak $p \Rightarrow q$ vyjadřuje výrok „pokud je x dělitelné šesti, pak je x dělitelné dvěma", kdežto $q \Rightarrow p$ vyjadřuje výrok „pokud je x dělitelné dvěma, pak je x dělitelné šesti".

  Implikace $\varphi \Rightarrow \psi$ nic neříká o platnosti ψ za předpokladu, že φ není platná. Uvažujme například výrok „pokud je x přirozené číslo, pak je x celé číslo". Pokud výrok „x je přirozené číslo" není platný, pak o platnosti „x je celé číslo" nelze nic říct, což je zcela v souladu s intuitivní interpretací.

- *ekvivalence* $\Leftrightarrow$ vyjadřuje výrokovou vazbu „právě když“, to jest $\varphi \Leftrightarrow \psi$ čteme „φ, právě když ψ“. Ekvivalence $\varphi \Leftrightarrow \psi$ vyjadřuje, že φ je platná tehdy a jen tehdy, je-li platná ψ. Jinými slovy, buď jsou φ, ψ obě platné, nebo ani jedna z nich není platná. Vyjádřeno ještě jinak, pokud je platná φ, pak je platná i ψ a obráceně, pokud je platná ψ, pak je platná i φ. Pokud například výrokové symboly p a q vyjadřují výroky „$x = 2$“ a „x je sudé prvočíslo“, pak $p \Leftrightarrow q$ vyjadřuje výrok „$x = 2$, právě když je x sudé prvočíslo“.

  V přirozeném jazyku je někdy obtížné rozlišit implikaci a ekvivalenci. Někdy je typické sdělovat výroky ve tvaru ekvivalence pouze s důrazem na jednu její stranu, protože druhá strana je (v daném kontextu) platná triviálně. Například výrokem „Jestli budeš hodný, dostaneš čokoládu“ (zde je potřeba odhlédnout od časové souslednosti) mají rodiče obvykle na mysli „Čokoládu dostaneš, právě když budeš hodný“. To jest i přesto, že implikace „Čokoládu dostaneš, jen když budeš hodný“ je pro rodiče de facto hlavním předmětem sdělení, ve výchozím výroku není explicitně zahrnuta, protože plyne z kontextu.

Průvodce studiem

Rozdíl mezi výroky ve tvaru *implikace* a *ekvivalence* je nezbytně nutné pochopit, protože téměř veškerá tvrzení v informatice a matematice jsou buď ve tvaru implikace nebo ve tvaru ekvivalence. Záměna implikace za ekvivalenci je jednou z nejčastějších začátečnických chyb. Kdybychom ze středoškolské matematiky známé tvrzení: „Pokud má kvadratická rovnice dvě různá reálná řešení, pak nemá komplexně sdružený kořen“, reformulovali ve tvaru ekvivalence, dostali bychom tvrzení: „Kvadratická rovnice má dvě různá reálná řešení, právě když nemá komplexně sdružený kořen“, což neplatí například pro $x^2 = 0$.

Příklad 1.3. Následující výroky

„Petr nosí deštník, když je ráno mlha nebo prší“,
„Když jsou na obloze večer červánky, pak ráno není mlha“,
„Petr jezdí autem, jen když prší“.
„Ráno je mlha.“

formalizujeme formulemi VL. V předchozích výrocích se vyskytují tyto atomické výroky: „Petr nosí deštník“ (označíme d), „Ráno je mlha“ (označíme m), „Ráno prší“ (označíme p), „Na obloze jsou večer červánky“ (označíme c), „Petr jezdí autem“ (označíme a). Výroky můžeme nyní formalizovat formulemi $(m \vee p) \Rightarrow d$, $c \Rightarrow \neg m$, $a \Rightarrow p$, m. V prvním případě je diskutabilní, zda-li bychom neměli uvažovat spíše formuli $(m \vee p) \Leftrightarrow d$.

Při formalizaci výroků je nejprve vhodné najít atomické výroky.

V některých případech se nám bude hodit odkazovat se na části formulí, které jsou samy o sobě formulemi. Mějme formuli φ. Každá formule, která se ve φ nachází jako podřetězec (včetně celé φ), se nazývá *podformule* φ. Vezmeme-li například formuli $\neg(p \wedge q) \Rightarrow p$, pak všechny její podformule jsou p, q, $p \wedge q$, $\neg(p \wedge q)$ a $\neg(p \wedge q) \Rightarrow p$. ψ je *vlastní podformule* φ, pokud je ψ podformule φ a formule ψ, φ jsou vzájemně různé.

Každá formule je podformule sebe sama.

1.2.2 Pravdivost formulí

Zatím jsme se formulím věnovali pouze z pohledu jejich tvaru, případně zápisu a čtení, ale doposud se nebavili o jejich pravdivosti či nepravdivosti. Část výrokové logiky, která se zabývá formulemi pouze jako řetězci symbolů jazyka, se nazývá *syntaxe*. Syntaxe VL nedefinuje pravdivost formulí ani význam spojek, ten jsme si v předchozí kapitole neformálně nastínili z důvodu nahlédnutí do vztahu výrok – formule. Formule samy o sobě nemají žádný význam. Přiřazení významu syntaktickým objektům je záležitostí další části výrokové logiky – *sémantiky*. Právě sémantikou výrokové logiky se nyní budeme zabývat.

Výroková logika má svou syntaxi a sémantiku.

	$\neg$
0	1
1	0

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

$\vee$	0	1
0	0	1
1	1	1

$\rightarrow$	0	1
0	1	1
1	0	1

$\leftrightarrow$	0	1
0	1	0
1	0	1

Tabulka 1: Logické operace

Dříve než začneme, si ještě na jednom příkladu ukážeme, proč je nezbytné formalizovat výroky i jejich význam. V přirozeném jazyku je možné snadno vytvářet „vazby na sebe sama“, tak zvané *autoreference*. Příkladem výroku, který v sobě obsahuje autoreferenci je výrok: „Tento výrok není pravdivý“ – jedná se tedy o výrok, který vypovídá o své vlastní pravdivosti. Kdybychom se zamysleli nad pravdivostí tohoto výroku, pak bychom se dostali do *paradoxní situace*: Pokud bychom předpokládali pravdivost výroku, pak by byla pravda, že on sám je nepravdivý. Kdybychom naopak vyšli z toho, že je nepravdivý, pak by nebyla pravda, že je nepravdivý, tudíž by měl být pravdivý. V přirozeném jazyku lze touto cestou snadno dospět k paradoxu, v jazyku VL nikoliv, protože tvrzení obsahující autoreferenci v něm nejsou formulovatelná.

Při zavedení pravdivosti formulí se budeme opět snažit odhlédnout od jejich obsahu. Výrokovým symbolům (atomickým formulím), budeme přidělovat *pravdivostní hodnoty* 0 nebo 1, přitom 0 bude mít význam „nepravda“ a 1 bude mít význam „pravda“. Tím se opět dopustíme významného zjednodušení, protože v mnoha situacích se lze setkat například s částečně pravdivými výroky. Samotné přiřazení pravdivostních hodnot výrokovým symbolům budeme nazývat *pravdivostní ohodnocení*. Dostáváme se tak k následujícímu pojmu.

0 značí nepravdu, 1 značí pravdu.

Pravdivostní ohodnocení (zkráceně *ohodnocení*) je předpis e, který každému výrokovému symbolu p jazyka VL přiřazuje *pravdivostní hodnotu* 0 (označujeme $e(p) = 0$), nebo 1 (označujeme $e(p) = 1$). Pokud $e(p) = 0$, pak říkáme, že p je *nepravdivý v ohodnocení e*, pokud $e(p) = 1$, pak říkáme, že p je *pravdivý v ohodnocení e*.

Průvodce studiem

Význam ohodnocení e můžeme chápat následovně. Výrokové symboly označují výroky. Zadáme-li ohodnocení e, pak výrokový symbol p označuje výrok, který má pravdivostní hodnotu $e(p)$. Na to lze nahlížet dvěma způsoby. V prvním případě „známe“ výrok označený symbolem p a považujeme jej za pravdivý nebo nepravdivý. V tom případě položíme $e(p) = 1$ nebo $e(p) = 0$. V druhém případě pravdivostní hodnotu výroku označeného p neznáme. Položíme-li pak $e(p) = 1$ nebo $e(p) = 0$, omezujeme se na situace, kdy je výrok označený p pravdivý nebo nepravdivý – pak se můžeme zabývat tím, co plyne z pravdivosti či nepravdivosti výroku p.

Zavedením pravdivostního ohodnocení definujeme pouze pravdivost výrokových symbolů, to jest atomických formulí. Pro stanovení pravdivosti formulí, které jsou složeny z jiných pomocí symbolů logických spojek je nutné nejprve přesně zavést *význam logických spojek*. Uveďme si nejprve neformální příklad. Pokud známe pravdivost výroků „Prší“ a „Svítí slunce“, pak přirozenou úvahou rozhodujeme, je-li výrok „Prší a svítí slunce“ pravdivý a to tak, že „Prší a svítí slunce“ je pravdivý (pouze) v případě, že „Prší“ a „Svítí slunce“ jsou oba pravdivé. Úplně stejnou úvahu provedeme, pokud budeme mít výroky „x je liché“ a „x je dělitelné třemi“. Při stanovení pravdivosti výroků „Prší a svítí slunce“ a „x je liché a dělitelné třemi“ vycházíme pouze z pravdivosti dílčích výroků (nikoliv jejich obsahu) a z toho, že přirozeně víme, jak interpretujeme spojku „a“. Stejnou úvahu lze udělat i pro ostatní spojky. Přirozené interpretace spojek budeme formalizovat *logickými operacemi* – ke každému symbolu logické spojky budeme uvažovat logickou operaci.

Logické operace formalizují význam logických spojek.

Logickou operaci negace označíme $\neg$, logickou operaci konjunkce označíme $\wedge$, logickou operaci disjunkce označíme $\vee$ a tak dále. Fakt, že „negací pravdy je nepravda“ vyjádříme $\neg 1 = 0$, naopak $\neg 0 = 1$ vyjadřuje, že „negace nepravdy je pravda". Jelikož je negace unární spojka, příslušná logická operace pracuje pouze s jednou pravdivostní hodnotou. U ostatních (binárních) spojek budou logické operace pracovat se dvěma pravdivostními hodnotami, u implikace bude navíc *záležet na jejich pořadí.* Například pro konjunkci položíme $0 \wedge 0 = 0$, $0 \wedge 1 = 0$, $1 \wedge 0 = 0$ a $1 \wedge 1 = 1$, což vyjadřuje naši intuitivní interpretaci konjunkce uvedenou v předchozím odstavci. Pro přehlednost si logické operace zadáme tabulkami, viz tabulku 1. Tabulku pro $\rightarrow$ je třeba číst nejprve po řádku, pak po sloupci, tedy $0 \rightarrow 0 = 1$, $0 \rightarrow 1 = 1$, $1 \rightarrow 0 = 0$ a $1 \rightarrow 1 = 1$.

Nyní nic nebrání tomu, abychom definovali pravdivost formulí VP při daném ohodnocení.

Definice 1.4. Pro každé pravdivostní ohodnocení e definujeme:

$$\begin{aligned} &\|p\|_e = e(p), && \|\varphi \curlywedge \psi\|_e = \|\varphi\|_e \wedge \|\psi\|_e, && \|\varphi \Rightarrow \psi\|_e = \|\varphi\|_e \rightarrow \|\psi\|_e, \\ &\|\neg\varphi\|_e = \neg\, \|\varphi\|_e, && \|\varphi \curlyvee \psi\|_e = \|\varphi\|_e \vee \|\psi\|_e, && \|\varphi \Leftrightarrow \psi\|_e = \|\varphi\|_e \leftrightarrow \|\psi\|_e, \end{aligned}$$

kde p je výrokový symbol a φ, ψ jsou formule jazyka VL. $\|\varphi\|_e$ se nazývá *pravdivostní hodnota formule φ při ohodnocení e.* Je-li $\|\varphi\|_e = 0$, pak říkáme, že φ *není pravdivá při ohodnocení e.* Pokud $\|\varphi\|_e = 1$, pak říkáme, že φ *je pravdivá při ohodnocení e.*

Pravdivost formule chápeme vždy vzhledem k nějakému ohodnocení.

Poznámka 1.5. Všimněte si, že logické operace tak, jak jsme je definovali v tabulkách 1 odpovídají zamýšlenému významu spojek, který jsme slovně popsali v kapitole 1.2.1. Logické operace bychom také mohli zavést analogickým slovním popisem. Například $\|\varphi \Rightarrow \psi\|_e = 1$, právě když $\|\varphi\|_e = 0$ nebo $\|\psi\|_e = 1$.

Průvodce studiem

V tomto okamžiku je potřebné, abyste se ujistili, že skutečně rozumíte rozdílu mezi symbolem logické spojky a jemu příslušnou logickou operací. Znovu připomeňme, že symbol spojky je zaveden v jazyku VL, jedná se tedy o *syntaktický* pojem. Naproti tomu logická operace je pojem *sémantický* a slouží k přesnému zavedení interpretace spojky – tedy jejího významu, který je na symbolu spojky nezávislý.

Vztahy z definice 1.4 nám dávají návod, jak zjistit hodnotu $\|\varphi\|_e$. Pokud je formule φ atomická, pak je φ některý z výrokových symbolů, řekněme p, a pak $\|\varphi\|_e = e(p)$. Pokud φ není atomická, pak je v některém ze tvarů $\neg\vartheta$, $\vartheta \curlywedge \chi$, $\vartheta \curlyvee \chi$, $\vartheta \Rightarrow \chi$ nebo $\vartheta \Leftrightarrow \chi$. Pokud je například ve tvaru $\vartheta \Rightarrow \chi$, pak stanovíme pravdivostní hodnoty $\|\vartheta\|_e$, $\|\chi\|_e$ a pomocí logické operace $\rightarrow$ snadno vypočteme $\|\varphi\|_e = \|\vartheta\|_e \rightarrow \|\chi\|_e$. Při vyšetřování pravdivosti navíc můžeme využít vlastností jednotlivých logických operací. Pokud například zjistíme, že $\|\varphi\|_e = 1$, pak platí $\|\varphi \curlyvee \psi\|_e = 1$ bez ohledu na hodnotu $\|\psi\|_e$, pokud je $\|\varphi\|_e = 0$, pak $\|\varphi \curlywedge \psi\|_e = 0$ opět bez ohledu na $\|\psi\|_e$.

Definice 1.6. Formule φ se nazývá *tautologie,* pokud $\|\varphi\|_e = 1$ při každém ohodnocení e. Formule φ se nazývá *kontradikce,* pokud $\|\varphi\|_e = 0$ při každém ohodnocení e. Formule φ se nazývá *splnitelná,* pokud $\|\varphi\|_e = 1$ při nějakém ohodnocení e. Formule φ, ψ jsou *sémanticky ekvivalentní,* pokud $\|\varphi\|_e = \|\psi\|_e$ pro každé ohodnocení e.

Poznámka 1.7. Pro tautologie, kontradikce a splnitelné formule platí několik vztahů, které vesměs plynou přímo z definice a z vlastností logických operací. Uveďme si některé z nich. Formule φ je tautologie (kontradikce), právě když je $\neg\varphi$ kontradikce (tautologie). Formule φ je kontradikce, právě když není splnitelná. Pokud máme stanovit, zda-li je nějaká formule splnitelná, stačí najít alespoň jedno ohodnocení, při kterém je pravdivá. Každá tautologie je splnitelná formule. Formule φ, ψ jsou sémanticky ekvivalentní, právě když je $\varphi \Leftrightarrow \psi$ tautologie.

Sémanticky ekvivalentní formule od sebe nelze rozlišit pravdivostí.

Jak můžeme zjistit, zda-li je daná formule tautologie? Pokud bychom chtěli mechanicky ověřit $\|\varphi \Rightarrow \psi\|_e = 1$ pro každé ohodnocení e, narazíme na problém, že pravdivostních ohodnocení je *nekonečně mnoho,* protože v jazyku VL předpokládáme (a potřebujeme) nekonečně mnoho výrokových symbolů. Na druhou stranu, v každé formuli se vyskytuje pouze konečně mnoho výrokových symbolů. Pro přehlednost tedy zavedeme

Označení 1.8. Výraz $\varphi(p_1, \ldots, p_n)$ označuje, že φ je formule jazyka VL a $p_1, \ldots, p_n$ jsou právě všechny výrokové symboly vyskytující se v φ.

Je téměř evidentní, že pokud vezmeme dvě obecně různá ohodnocení e a e' taková, že $e(p_1) = e'(p_1), \ldots, e(p_n) = e'(p_n)$, pak pro $\varphi(p_1, \ldots, p_n)$ máme $\|\varphi\|_e = \|\varphi\|_{e'}$. To jest, platí

Důsledek 1.9. *Pravdivost formule φ při daném pravdivostním ohodnocení závisí pouze na ohodnocení výrokových symbolů vyskytujících se ve formuli φ.* □

Aplikací předchozí úvahy je již zřejmé, že k tomu, abychom vyšetřili tautologičnost formule φ, se lze omezit pouze na ověření její pravdivosti v konečně mnoha ohodnoceních, která se od sebe vzájemně liší v pravdivostních hodnotách přiřazených výrokovým symbolům vyskytujících se ve φ. Pro $\varphi(p_1, \ldots, p_n)$ je třeba vzít v úvahu právě 2^n ohodnocení. Na tomto pozorování je založena *tabulková metoda* neboli *tabelace.*

Tabelací formule $\varphi(p_1, \ldots, p_n)$ rozumíme vyšetření, ve kterých ohodnoceních je φ pravdivá, přitom se omezíme na ohodnocení, která výrokovým symbolům $p_1, \ldots, p_n$ přiřazují vzájemně různé pravdivostní hodnoty. Při tabelaci vytváříme tabulku, jejíž *řádky reprezentují pravdivostní ohodnocení* a *sloupce reprezentují podformule φ,* které jsou psány zleva doprava tak, aby vždy platilo, že pokud aktuální sloupec odpovídá formuli ψ, pak sloupce odpovídající všem vlastním podformulím ψ jsou uvedeny před aktuálním sloupcem. V tabulce tedy bude na posledním místě sloupec odpovídající φ. Rovněž je praktické do prvních n sloupců zapsat výrokové symboly $p_1, \ldots, p_n$. Například pro formuli $p \Leftrightarrow ((p \Rightarrow \neg q) \wedge r)$ bychom mohli sloupce zapsat v pořadí

Tabelace slouží k přehlednému vyšetření pravdivosti.

p	q	r	$\neg q$	$p \Rightarrow \neg q$	$(p \Rightarrow \neg q) \wedge r$	$p \Leftrightarrow ((p \Rightarrow \neg q) \wedge r)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

.

V tabulce je na daném poli 0 (případně 1), pokud je v ohodnocení reprezentovaném řádkem formule příslušná sloupci nepravdivá (případně pravdivá). V tabulce nejprve vyplňujeme hodnoty u sloupců reprezentujících výrokové symboly – s ohledem na to, aby byly každé dva řádky různé. Poté můžeme vyplňovat zbylé sloupce zleva doprava pomocí logických operací – pokud postupujeme zleva doprava, máme vždy k dispozici hodnoty pravdivostí podformulí při ohodnocení reprezentovaném řádkem. Pro formuli $p \Leftrightarrow ((p \Rightarrow \neg q) \wedge r)$ tedy budeme mít tabulku:

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

Z ní je jasné, že $p \Leftrightarrow ((p \Rightarrow \neg q) \wedge r)$ je splnitelná formule (aspoň v jednom řádku v posledním sloupci tabulky je 1), tím pádem není kontradikce, ale není tautologie (například na druhém řádku v posledním sloupci je 0, to jest pro ohodnocení e, kde $e(p) = 0$, $e(q) = 0$, $e(r) = 1$ máme $\|p \Leftrightarrow ((p \Rightarrow \neg q) \wedge r)\|_e = 0$).

Příklad 1.10. Rozhodneme, zda-li jsou formule

$$p \vee (p \Rightarrow \neg q), \qquad (p \wedge q) \Leftrightarrow p, \qquad \neg(p \Rightarrow p).$$

splnitelné, tautologie, nebo kontradikce. Provedeme tabelaci:

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

Formule $p \vee (p \Rightarrow \neg q)$ je tautologie, $(p \wedge q) \Leftrightarrow p$ je splnitelná, $\neg(p \Rightarrow p)$ je kontradikce.

Ve výrokovém kalkulu je obvyklé uvažovat pouze dva základní symboly logických spojek $\neg$, $\Rightarrow$ a nikoliv pět $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, jak jsme učinili my. Důvody pro snížení počtu symbolů jsou dva. První důvod je čistě technický – zjednodušení důkazů. Druhým důvodem je fakt, že konjunkci, disjunkci a ekvivalenci je možné vyjádřit pouze pomocí negace a implikace – v tomto smyslu jsou i symboly spojek $\wedge$, $\vee$, $\Leftrightarrow$ nadbytečné. Vskutku, formule $p \vee q$, $p \wedge q$ a $p \Leftrightarrow q$ (v tomto pořadí) jsou sémanticky ekvivalentní formulím

$$\neg p \Rightarrow q, \qquad \neg(p \Rightarrow \neg q), \qquad \neg((p \Rightarrow q) \Rightarrow \neg(q \Rightarrow p)),$$

o čemž se můžeme přesvědčit tabelací:

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

To jest $\|\neg p \Rightarrow q\|_e = \|p \vee q\|_e$ a $\|\neg(p \Rightarrow \neg q)\|_e = \|p \wedge q\|_e$ při každém pravdivostním ohodnocení e. O sémantické ekvivalenci $\neg((p \Rightarrow q) \Rightarrow \neg(q \Rightarrow p))$ s $p \Leftrightarrow q$ nechť se čtenář přesvědčí sám. Pokud bychom v jazyku VL měli pouze symboly spojek $\neg$, $\Rightarrow$, pak $\varphi \vee \psi$ již není formule takového jazyka, ale můžeme ji chápat jako zkratku za formuli $\neg\varphi \Rightarrow \psi$.

V jazyku VL bychom si vystačili pouze se symboly spojek $\neg$ a $\Rightarrow$.

Shrnutí

Logika je věda zkoumající usuzování, přitom odhlíží od obsahu a zabývá se pouze formou usuzování. Výroková logika se zabývá formálním usuzováním o výrocích.
Výroková logika má svou syntaxi a sémantiku. Syntaxe výrokové logiky definuje pojmy jako je jazyk a formule, ale formulemi (i ostatními syntaktickými pojmy) se zabývá čistě z pohledu jejich tvaru. Sémantika výrokové logiky zavádí pojem pravdivostní ohodnocení a pravdivost formule při daném ohodnocení. Sémantika přiřazuje význam syntaktickým pojmům.
Z hlediska pravdivosti lze každou formuli klasifikovat jako splnitelnou, kontradikci, nebo tautologii. K ověření, do které kategorie formule patří můžeme použít tabulkovou metodu.

Pojmy k zapamatování

- výrok, logická spojka, výrokový symbol,
- jazyk výrokové logiky,
- formule, podformule,
- pravdivostní ohodnocení, logická operace,
- sémantická ekvivalence, kontradikce, tautologie,
- tabelace

Kontrolní otázky

1. *Čím se zabývá logika a čím se nezabývá?*
2. *Jaký je vztah mezi výrokem a formulí?*
3. *Jaký je vztah mezi symbolem logické spojky a logickou operací?*

4. *Existují tautologie, které nejsou splnitelné?*
5. *Čím se odlišuje implikace od ekvivalence?*

Cvičení

1. Rozhodněte, zda-li jsou následující výrazy formule VL a rozhodněte proč.

$$\begin{array}{lll} p, & \neg p, & (\neg q \wedge q) \Leftrightarrow r, \\ \neg(\neg\neg p), & \neg q \vee \neg p, & p \Rightarrow q \wedge r. \end{array}$$

   Ke každé formuli navíc vypište všechny její podformule.

2. Zjistěte, které z následujících formulí jsou splnitelné, tautologie, nebo kontradikce.

$$\begin{array}{lll} p \Rightarrow (\neg p \Rightarrow q), & p \Rightarrow (\neg q \Rightarrow (q \wedge \neg p)), & p \vee (\neg q \wedge \neg r), \\ (q \wedge \neg p) \Leftrightarrow \neg(\neg q \vee p), & r \Rightarrow (\neg(p \Rightarrow p) \Rightarrow q), & \neg q \wedge ((p \Rightarrow q) \wedge p). \end{array}$$

Úkoly k textu

1. Vraťte se k příkladu 1.3 na straně 9. Vhodně formalizujte následující výroky v souladu s formalizací výroků v příkladu 1.3:

   „Pokud má Petr deštník, pak nejede autem“,
   „Večer nejsou na obloze červánky“,
   „Ráno je mlha, když neprší“,
   „K tomu aby Petr jel autem stačí aby byly na obloze červánky“.

   Pokud je možné některý z výroků formalizovat několika způsoby, uveďte všechny, které jsou podle vás „rozumné“ a proveďte diskusi nad jejich případnými rozdíly. Jsou vaše odlišné formalizace výroků sémanticky ekvivalentní?

Řešení

1. p je formule (podformule: p); $\neg p$ je formule (podformule: $p, \neg p$); $(\neg q \wedge q) \Leftrightarrow r$ je formule když přijmeme konvenci o vynechání vnějších závorek (podformule: $q, r, \neg q, \neg q \wedge q, (\neg q \wedge q) \Leftrightarrow r$); $\neg(\neg\neg p)$ není formule; $\neg q \vee \neg p$ je formule když přijmeme konvenci o vynechání vnějších závorek (podformule: $p, q, \neg p, \neg q, \neg q \vee \neg p$); $p \Rightarrow q \wedge r$ není formule.
2. $p \Rightarrow (\neg p \Rightarrow q)$ je tautologie, $p \Rightarrow (\neg q \Rightarrow (q \wedge \neg p))$ je splnitelná ale není tautologie, $p \vee (\neg q \wedge \neg r)$ je splnitelná ale není tautologie, $(q \wedge \neg p) \Leftrightarrow \neg(\neg q \vee p)$ je tautologie, $r \Rightarrow (\neg(p \Rightarrow p) \Rightarrow q)$ je tautologie, $\neg q \wedge ((p \Rightarrow q) \wedge p)$ je kontradikce.

Studijní cíle: Po prostudování kapitoly by student měl umět znát pojem sémantického vyplývání formulí z množin formulí. Dále by měl umět vyšetřovat sémantické vyplývání pomocí tabulkové metody a měl by umět najít normální formy formulí.

Klíčová slova: DNF, KNF, booleovská funkce, elementární disjunkce, elementární konjunkce, funkční úplnost, literál, normální forma, sémantické vyplývání, úplný systém spojek

Potřebný čas: 120 minut.

1.3 Sémantické vyplývání ve výrokové logice

V předchozím úvodu do výrokové logiky jsme přesně zavedli intuitivní pojmy *výrok* a *pravdivost* pomocí formulí výrokové logiky a pravdivosti formulí při daném ohodnocení výrokových symbolů. Přesné zavedení těchto pojmů nám umožnilo pracovat s nimi jako s matematickými objekty, o kterých můžeme dokazovat různá tvrzení (třeba, že každá formule je podformule sebe sama, že pravdivost formule při daném ohodnocení záleží pouze na ohodnocení výrokových symbolů vyskytujících se v této formuli a podobně). Nyní se zaměříme na přesné zavedení pojmu *vyplývání*, který má v logice ústřední význam.

Definice 1.11. Mějme formule $\psi_1, \ldots, \psi_n$, kde $n \geq 0$. Formule φ *sémanticky plyne* z formulí $\psi_1, \ldots, \psi_n$ (značíme $\psi_1, \ldots, \psi_n \vDash \varphi$), jestliže $\|\varphi\|_e = 1$ pro každé pravdivostní ohodnocení e takové, že $\|\psi_1\|_e = 1, \ldots, \|\psi_n\|_e = 1$.

Poznámka 1.12. Formule $\psi_1, \ldots, \psi_n$ z předchozí definice někdy nazýváme *předpoklady,* formuli φ nazýváme *sémantický důsledek* formulí $\psi_1, \ldots, \psi_n$. Definice 1.11 zahrnuje i případ vyplývání z nulového počtu formulí, tedy $\vDash \varphi$. V tomto případě dle definice 1.11 máme, že $\vDash \varphi$, právě když pro každé pravdivostní ohodnocení e platí $\|\varphi\|_e = 1$, což je právě když φ je tautologie.

φ je tautologie, právě když $\vDash \varphi$.

Příklad 1.13. Rozhodněte, které z následujících formulí

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

sémanticky plynou z formulí $p \Rightarrow \neg(r \vee q)$, $\neg r$.

Nechť φ označuje $p \Rightarrow \neg(r \vee q)$ a nechť ψ označuje $\neg r$. Provedeme tabelaci:

	p	q	r	φ	ψ
e_1:	0	0	0	1	1
	0	0	1	1	0
e_2:	0	1	0	1	1
	0	1	1	1	0

	p	q	r	φ	ψ
e_3:	1	0	0	1	1
	1	0	1	0	0
	1	1	0	0	1
	1	1	1	0	0

Z předchozí tabulky je vidět, že stačí vyšetřovat pravdivost formulí v ohodnoceních, která jsou v tabulce reprezentována řádky označenými e_1, e_2, e_3, protože to jsou řádky reprezentující právě ta ohodnocení, při nichž jsou obě formule pravdivé. Nyní zřejmě $\varphi, \psi \vDash q \Rightarrow \neg p$, protože formule $q \Rightarrow \neg p$ je pravdivá v každém z ohodnocení e_1, e_2, e_3. Dále $\|(p \Rightarrow q) \vee r\|_{e_3} = 0$, to jest formule $(p \Rightarrow q) \vee r$ sémanticky neplyne z φ, ψ – ohodnocení e_3 nám slouží jako *protipříklad.* Stejně tak třetí formule $(s \wedge q) \Rightarrow p$ neplyne z φ, ψ, uvažujeme-li například ohodnocení e, kde $e(p) = e_2(p)$, $e(q) = e_2(q)$, $e(r) = e_2(r)$ a $e(s) = 1$, pak e je ohodnocení, při kterém jsou obě formule φ i ψ pravdivé, ale $\|(s \wedge q) \Rightarrow p\|_e = 0$. Konečně formule $r \Rightarrow ((p \Rightarrow \neg q) \Rightarrow r)$ sémanticky plyne z φ, ψ, protože se jedná o tautologii (tautologie je pravdivá při každém ohodnocení, tedy i ve všech ohodnoceních, při kterých jsou obě φ i ψ pravdivé).

Tautologie sémantický plynou z libovolných formulí.

Průvodce studiem

Sémantické vyplývání jsme přesně zavedli a můžeme se dál zabývat jeho vlastnostmi. V kapitole 6.1 si například nastíníme otázku, zda-li je možné o sémantickém vyplývání rozhodnout i bez použití pravdivostních ohodnocení, to jest pouze manipulací s formulemi. Podobné otázky jsou ve středu zájmu formální logiky.

Nyní si pro ukázku dokážeme jednoduché tvrzení o sémantickém vyplývání:

Věta 1.14. *$\chi_1, \ldots, \chi_n \vDash \varphi \Rightarrow \psi$, právě když $\chi_1, \ldots, \chi_n, \varphi \vDash \psi$.*

Důkaz. Nejprve předpokládejme $\chi_1, \ldots, \chi_n \models \varphi \Rightarrow \psi$ a dokážeme $\chi_1, \ldots, \chi_n, \varphi \models \psi$. Stačí ověřit, že pro každé ohodnocení e, při kterém jsou všechny formule z $\chi_1, \ldots, \chi_n, \varphi$ pravdivé, máme $\|\psi\|_e = 1$. Jsou-li ale $\chi_1, \ldots, \chi_n, \varphi$ při ohodnocení e pravdivé, pak dostáváme $\|\varphi \Rightarrow \psi\|_e = 1$ dle předpokladu $\chi_1, \ldots, \chi_n \models \varphi \Rightarrow \psi$. Rovněž platí $\|\varphi\|_e = 1$. To jest

$$\|\varphi \Rightarrow \psi\|_e = \|\varphi\|_e \to \|\psi\|_e = 1 \to \|\psi\|_e = 1.$$

Z vlastností $\to$ pak plyne, že $\|\psi\|_e = 1$. To jest $\chi_1, \ldots, \chi_n, \varphi \models \psi$.

Naopak, předpokládejme $\chi_1, \ldots, \chi_n, \varphi \models \psi$. Stačí ověřit, že pro každé ohodnocení e, při kterém jsou všechny formule $\chi_1, \ldots, \chi_n$ pravdivé, je $\|\varphi \Rightarrow \psi\|_e = 1$. Mohou nastat dvě situace. V prvním případě je $\|\varphi\|_e = 0$ a tím pádem $\|\varphi \Rightarrow \psi\|_e = 0 \to \|\psi\|_e = 1$. V druhém případě $\|\varphi\|_e = 1$, to jest při ohodnocení e jsou pravdivé všechny formule z $\chi_1, \ldots, \chi_n, \varphi$ a tím pádem dostáváme $\|\psi\|_e = 1$ z předpokladu $\chi_1, \ldots, \chi_n, \varphi \models \psi$. Odtud $\|\varphi \Rightarrow \psi\|_e = 1 \to 1 = 1$, v důsledku čehož $\chi_1, \ldots, \chi_n \models \varphi \Rightarrow \psi$. $\square$

Věta 1.14 má následující význam: k tomu abychom prokázali, že $\varphi \Rightarrow \psi$ sémanticky plyne ze $\chi_1, \ldots, \chi_n$ stačí ukázat, že ψ sémanticky plyne z $\chi_1, \ldots, \chi_n, \varphi$ a obráceně, k tomu abychom prokázali, že ψ sémanticky plyne z $\chi_1, \ldots, \chi_n, \varphi$, stačí ukázat, že implikace $\varphi \Rightarrow \psi$ sémanticky plyne z $\chi_1, \ldots, \chi_n$. Aplikací tohoto tvrzení můžeme například okamžitě tvrdit, že $\models \varphi \Rightarrow \varphi$, protože φ sémanticky plyne z φ triviálně. Dvojnásobnou aplikací tvrzení na zřejmý fakt $\varphi, \psi \models \varphi \mathbin{\&} \psi$ dostáváme $\models \varphi \Rightarrow (\psi \Rightarrow (\varphi \mathbin{\&} \psi))$ a tak podobně. Věta 1.14 rovněž dává další návod pro ověření sémantického vyplývání: k tomu, abychom ověřili, že φ sémanticky plyne z $\chi_1, \ldots, \chi_n$, stačí ověřit, že formule $\chi_1 \Rightarrow (\chi_2 \Rightarrow (\cdots(\chi_n \Rightarrow \varphi)\cdots))$ je tautologie.

1.4 Normální formy formulí

V kapitole 1.2.2 jsme pro formuli φ sestrojovali tabulku, kterou jsme vyšetřovali pravdivost formule v závislosti na ohodnocení výrokových symbolů. Nabízí se přirozená otázka, zdali není možné provést opačný proces. To jest k libovolné tabulce o 2^n řádcích (vyplněných nulami a jedničkami) najít formuli $\varphi(p_1, \ldots, p_n)$ tak, že její tabelací získáme výchozí tabulku pravdivostních hodnot. V této kapitole si ukážeme, že je tomu vskutku tak. Nalezená formule bude navíc ve speciálním tvaru – *normální formě.* Postup uvedený v této kapitole lze aplikovat například v situaci kdy známe pravdivostní výstupy nějakého systému, které jsme získali jeho pozorováním nebo jako informaci od experta, a potřebujeme je vyjádřit (popsat) pomocí výrokové formule. Místo pojmu „řádek v tabulce" nyní zavedeme o něco přesnější pojem.

Definice 1.15. *n-ární booleovská funkce* je předpis f, který každým n pravdivostním hodnotám $a_1, \ldots, a_n$ (v tomto pořadí) přiděluje pravdivostní hodnotu $f(a_1, \ldots, a_n)$. Pro každou $\varphi(p_1, \ldots, p_n)$ budeme uvažovat n-ární booleovskou funkci f^φ takovou, že

$$f^\varphi(\|p_1\|_e, \ldots, \|p_n\|_e) = \|\varphi\|_e$$

pro každé ohodnocení e.

Příklad 1.16. Nejprve si uvědomte, že f^φ je díky důsledku 1.9 vždy dobře definovaná booleovská funkce. Vezmeme-li například formuli $p \mathbin{\&} q$, pak příslušná booleovská funkce $f^{p \& q}$ je binární a máme $f^{p\& q}(0,0) = f^{p\& q}(0,1) = f^{p\& q}(1,0) = 0$ a $f^{p\& q}(1,1) = 1$. Jinými slovy, $f^{p\& q}$ bychom mohli vyjádřit pomocí logické operace $\wedge$ jako $f^{p\& q}(a,b) = a \wedge b$. Analogicky třeba $f^{p \Leftrightarrow (q \& r)}(a,b,c) = a \leftrightarrow (b \wedge c)$ a tak dále. Předchozí úvahu lze zobecnit pro libovolnou formuli φ o čemž se můžete snadno přesvědčit. Booleovské funkce tedy v jistém smyslu zobecňují logické operace – v jistém smyslu je to totéž jak uvidíme dále.

Booleovské funkce lze chápat jako obecné logické operace.

Nyní si zavedeme dvě normální formy formulí VP. Nejprve jedno upřesnění. Tabulkovou metodou se lze snadno přesvědčit, že například formule $p \mathbin{\&} (q \mathbin{\&} r)$ a $(p \mathbin{\&} q) \mathbin{\&} r$ jsou sémanticky ekvivalentní, to jest u formulí ve tvaru konjunkce nezáleží na uzávorkování. To samé platí pokud bychom nahradili konjunkci disjunkcí. V dalším tedy budeme psát stručně $p_1 \mathbin{\&} \cdots \mathbin{\&} p_n$ místo $p_1 \mathbin{\&} (p_2 \mathbin{\&} (\cdots(p_{n-1} \mathbin{\&} p_n)\cdots))$. Analogicky pro disjunkci.

Definice 1.17. Každý výrokový symbol p a jeho negaci $\neg p$ nazveme *literál.* Nechť $l_1, \ldots, l_k$ jsou literály. Formuli ve tvaru $l_1 \wedge \cdots \wedge l_k$ nazveme *elementární konjunkce literálů,* formuli ve tvaru $l_1 \vee \cdots \vee l_k$ nazveme *elementární disjunkce literálů.*

Formule φ je v

– *disjunktivní normální formě* (DNF), pokud je ve tvaru $\vartheta_1 \vee \cdots \vee \vartheta_n$ a $\vartheta_1, \ldots, \vartheta_n$ jsou elementární konjunkce literálů,

– *konjunktivní normální formě* (KNF), pokud je ve tvaru $\vartheta_1 \wedge \cdots \wedge \vartheta_n$ a $\vartheta_1, \ldots, \vartheta_n$ jsou elementární disjunkce literálů.

Formule $\psi(p_1, \ldots, p_n)$ se nazývá *disjunktivní* (*konjunktivní*) *normální forma n-ární booleovské funkce f,* pokud je ψ v DNF (KNF) a $f(a_1, \ldots, a_n) = f^{\psi}(a_1, \ldots, a_n)$ při všech pravdivostních hodnotách $a_1, \ldots, a_n$. Formule ψ se nazývá *disjunktivní* (*konjunktivní*) *normální forma formule φ,* pokud je ψ v DNF (KNF) a ψ je sémanticky ekvivalentní φ.

Algoritmus nalezení DNF a KNF pro zadanou n-ární booleovskou funkci si nejprve neformálně ukážeme na příkladu. Mějme tabulku, která nám definuje binární booleovskou funkci f:

a	b	$f(a,b)$
0	0	1
0	1	0
1	0	1
1	1	1

Normální formy hledáme jako „předpis“ pro booleovskou funkci.

Kdybychom měli slovně vyjádřit „jakou informaci tabulka zachycuje“, mohli bychom to vyjádřit například obratem: „$f(a, b) = 1$, právě když $a = 0$ a $b = 0$, nebo když $a = 1$ a $b = 0$, nebo když $a = 1$ a $b = 1$“, nebo kratším obratem „$f(a, b) = 1$, právě když neplatí $a = 0$ a $b = 1$“. Pokud přepíšeme první (druhé) vyjádření pomocí formule, najdeme tak DNF (KNF) pro f. Dále budeme používat výrokové symboly p, q, přitom p bude označovat výrok „$a = 1$“ a q bude označovat výrok „$b = 1$“. Nalezení DNF je intuitivně jasné: $(\neg p \wedge \neg q) \vee (p \wedge \neg q) \vee (p \wedge q)$ – – znovu srovnejte s uvedeným slovním popisem.

Při nalezení KNF se snažíme formalizovat popis, který nezachycuje, kdy je booleovská funkce pravdivá, ale naopak zároveň vylučuje všechny situace, kdy je nepravdivá. Přímým přepisem výše uvedeného popisu bychom dostali formuli $\neg(\neg p \wedge q)$, která ale není v KNF. $\neg(\neg p \wedge q)$ je ale sémantický ekvivalentní $p \vee \neg q$, což už je formule v KNF. Čtenář se může tabulkovou metodou přesvědčit, že obě zkonstruované formy jsou skutečně předpisem výchozí funkce f. Nyní si algoritmy nalezení DNF a KNF podrobně popíšeme.

Algoritmus 1.18 (Nalezení DNF).
Vstup: n-ární booleovská funkce f
Výstup: formule φ v DNF

Zvolíme n vzájemně různých výrokových symbolů $p_1, \ldots, p_n$, jména symbolů obvykle volíme podle potřeby. Pro pravdivostní hodnoty $a_1, \ldots, a_n$ (v tomto pořadí) můžeme uvažovat elementární konjunkci $a_1^\circ \wedge \cdots \wedge a_n^\circ$, kde a_i° je buďto literál p_i, pokud je $a_i = 1$, nebo literál $\neg p_i$ v opačném případě (to jest $a_i = 0$). Pokud neexistují žádné $a_1, \ldots, a_n$ tak, aby $f(a_1, \ldots, a_n) = 1$, pak položíme $\varphi = p \wedge \neg p$, kde p je některý ze symbolů $p_1, \ldots, p_n$. V opačném případě položíme $\varphi = \vartheta_1 \vee \cdots \vee \vartheta_k$, kde ϑ_i $(i = 1, \ldots, k)$ jsou právě všechny formule ve tvaru $a_1^\circ \wedge \cdots \wedge a_n^\circ$, pro které platí $f(a_1, \ldots, a_n) = 1$. □

Algoritmus 1.19 (Nalezení KNF).
Vstup: n-ární booleovská funkce f
Výstup: formule φ v KNF

Zvolíme n vzájemně různých výrokových symbolů $p_1, \ldots, p_n$, jména symbolů obvykle volíme podle potřeby. Pro pravdivostní hodnoty $a_1, \ldots, a_n$ (v tomto pořadí) můžeme uvažovat elementární disjunkci $a_1^\bullet \vee \cdots \vee a_n^\bullet$, kde $a_i^\bullet$ je buďto literál p_i, pokud je $a_i = 0$, nebo literál $\neg p_i$ v opačném případě (to jest $a_i = 1$). Pokud neexistují žádné $a_1, \ldots, a_n$ tak, aby $f(a_1, \ldots, a_n) = 0$, pak položíme $\varphi = p \vee \neg p$, kde p je některý ze symbolů $p_1, \ldots, p_n$. V opačném případě položíme $\varphi = \vartheta_1 \wedge \cdots \wedge \vartheta_k$, kde ϑ_i $(i = 1, \ldots, k)$ jsou právě všechny formule ve tvaru $a_1^\bullet \vee \cdots \vee a_n^\bullet$, pro které platí $f(a_1, \ldots, a_n) = 0$. □

Poznámka 1.20. Za pozornost stojí, že formule vytvořené předcházejícími algoritmy, až na formule $p \wedge \neg p$ a $p \vee \neg p$, obsahují v každé elementární konjunkci (disjunkci) libovolný výrokový symbol z $p_1, \ldots, p_n$ jako literál *právě jednou.* Takovým formulím říkáme, že jsou v *úplné* DNF, případně *úplné* KNF. KNF a DNF dané booleovské funkce není určena jednoznačně a to ani v případě, kdybychom zanedbali použití různých výrokových symbolů či jiné uzávorkování výrazů. Například formule $(p \vee q) \wedge (q \vee \neg q)$ a $(p \vee q)$ jsou obě v KNF a jsou sémanticky ekvivalentní – tudíž se jedná o KNF téže booleovské funkce.

Příklad 1.21. K následující tabulkou zadané booleovské funkci najdeme DNF a KNF. Tabulka je z úsporných důvodů rozdělena na dvě části:

a	b	c	$f(a,b,c)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1

a	b	c	$f(a,b,c)$
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Máme $f(0,0,0) = f(0,1,0) = f(0,1,1) = f(1,0,1) = f(1,1,1) = 1$, to jest DNF má tvar

$$(\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge r),$$

dále máme $f(0,0,1) = f(1,0,0) = f(1,1,0) = 0$, to jest KNF má tvar

$$(p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee \neg q \vee r).$$

Nyní je jasné, jak najít DNF (KNF) k $\varphi(p_1, \ldots, p_n)$. Stačí najít formuli $\psi(p_1, \ldots, p_n)$, která je disjunktivní (konjunktivní) normální forma booleovské funkce f^φ. Pokud zachováme identické značení výrokových symbolů, pak budou formule φ, ψ sémanticky ekvivalentní.

Příklad 1.22. Najdeme DNF a KNF formule $p \Leftrightarrow q$. Tabelací dostáváme

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

To jest DNF má tvar $(\neg p \wedge \neg q) \vee (p \wedge q)$, KNF má tvar $(p \vee \neg q) \wedge (\neg p \vee q)$.

V příkladu 1.22 jsme našli KNF a DNF formule $p \Leftrightarrow q$, přitom booleovská funkce $f^{p \Leftrightarrow q}(a, b)$ odpovídá logické operaci příslušné ekvivalenci, to jest $f^{p \Leftrightarrow q}(a, b) = a \leftrightarrow b$. Jinými slovy, obě nalezené normální formy je možné chápat jako vyjádření *ekvivalence* pouze pomocí konjunkce, disjunkce a negace. Stejnou úvahu bychom mohli provést i pro symbol spojky $\Rightarrow$ a logickou operaci $\rightarrow$. To nás přímo dovede k úvaze, že za základní symboly spojek jazyka VL bychom mohli vzít pouze $\neg$, $\wedge$ a $\vee$ a na sémantické úrovni bychom je interpretovali příslušnými logickými operacemi. To je možná poněkud překvapující, protože tím pádem známe již třetí systém logických spojek, který je dostačující z hlediska popisu všech ostatních spojek. Připomeňme, že náš výchozí systém obsahoval všechny symboly: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ a dále jsme uvedli, že se lze bez újmy omezit pouze na $\neg, \Rightarrow$. Nyní jsme zjistili, že stačí $\neg, \wedge, \vee$. Nejsou to však jediné systémy spojek, které jsou z hlediska popisu ostatních dostačující.

$\neg, \curlywedge, \curlyvee, \Rightarrow, \Leftrightarrow$	$\neg, \Rightarrow$	$\Uparrow$
$\neg(p \Rightarrow p)$	$\neg(p \Rightarrow p)$	$(p \Uparrow (p \Uparrow p)) \Uparrow (p \Uparrow (p \Uparrow p))$
$p \curlywedge q$	$\neg(p \Rightarrow \neg q)$	$(p \Uparrow q) \Uparrow (p \Uparrow q)$
$\neg(p \Rightarrow q)$	$\neg(p \Rightarrow q)$	$(p \Uparrow (p \Uparrow p)) \Uparrow (p \Uparrow (p \Uparrow q))$
p	p	p
$\neg(q \Rightarrow p)$	$\neg(q \Rightarrow p)$	$(p \Uparrow (p \Uparrow p)) \Uparrow (q \Uparrow (p \Uparrow p))$
q	q	q
$\neg(p \Leftrightarrow q)$	$(p \Rightarrow q) \Rightarrow \neg(q \Rightarrow p)$	$(p \Uparrow (p \Uparrow q)) \Uparrow (q \Uparrow (p \Uparrow p))$
$p \curlyvee q$	$\neg p \Rightarrow q$	$(p \Uparrow p) \Uparrow (q \Uparrow q)$
$\neg(p \curlyvee q)$	$\neg(\neg p \Rightarrow q)$	$(p \Uparrow (p \Uparrow p)) \Uparrow ((p \Uparrow p) \Uparrow (q \Uparrow q))$
$p \Leftrightarrow q$	$\neg((p \Rightarrow q) \Rightarrow \neg(q \Rightarrow p))$	$(p \Uparrow q) \Uparrow ((p \Uparrow p) \Uparrow (q \Uparrow q))$
$\neg q$	$\neg q$	$q \Uparrow q$
$q \Rightarrow p$	$q \Rightarrow p$	$q \Uparrow (p \Uparrow p)$
$\neg p$	$\neg p$	$p \Uparrow p$
$p \Rightarrow q$	$p \Rightarrow q$	$p \Uparrow (p \Uparrow q)$
$\neg(p \curlywedge q)$	$p \Rightarrow \neg q$	$p \Uparrow q$
$p \Rightarrow p$	$p \Rightarrow p$	$p \Uparrow (p \Uparrow p)$

Tabulka 2: Tři úplné systémy spojek

Systémy logických spojek, pomocí nichž lze vyjádřit libovolnou další spojku nazýváme *úplné systémy spojek*. Na úrovni sémantiky spojek (to jest příslušných logických operací) to znamená, že libovolnou logickou operaci lze zkonstruovat pouze ze základních logických operací – této vlastnosti se říká *funkční úplnost*. Čím větší je systém základních spojek, které uvažujeme v jazyku VL, tím jednodušší je vyjadřování ostatních spojek, naopak, pokud je systém spojek malý, vyjadřování ostatních spojek může být komplikované a formule sloužící k vyjádření zbývajících spojek jsou obvykle dlouhé.

Úplný systém spojek stačí k popisu všech ostatních spojek.

Speciální význam mají Pierceova spojka (význam: „ani . . . , ani . . . “, označujeme symbolem $\Downarrow$) a Shefferova spojka (význam: „pokud . . . , pak neplatí . . . “, označujeme symbolem $\Uparrow$), které samy o sobě tvoří úplný systém spojek. Obě dvě spojky jsou interpretovány následujícími logickými operacemi:

$\downarrow$	0	1
0	1	0
1	0	0

$\uparrow$	0	1
0	1	1
1	1	0

Příklad 1.23. V tabulce 2 je uveden souhrn všech binárních booleovských funkcí, které jsou popsány formulemi pomocí tří různých systémů spojek. Každá binární booleovská funkce nabývá právě 2^2 hodnot, to jest vzájemně různých binárních booleovských funkcí je $2^{2^2} = 16$.

Shrnutí

Sémantické vyplývání formalizuje intuitivní pojem „vyplývání“ z množin formulí. Sémantické vyplývání je zavedeno pomocí pojmu ohodnocení. Pro ověření sémantického vyplývání je možné použít tabelaci. Booleovské funkce představují obecné logické operace. Pro každou booleovskou funkci můžeme najít výrokovou formuli, která jej jejím předpisem. Formule v disjunktivní (konjunktivní) normální formě jsou výrokové formule ve speciálních tvarech. Ke každé výrokové formuli lze najít logicky ekvivalentní formuli, která je v disjunktivní nebo konjunktivní normální formě. K nalezení normálních forem lze opět použít tabelaci.

Pojmy k zapamatování

- sémantické vyplývání,

- booleovská funkce,
- elementární disjunkce (konjunkce),
- disjunktivní (konjunktivní) normální forma,
- funkční úplnost, úplný systém spojek,

Kontrolní otázky

1. *Co jsou to literály?*
2. *Může být někdy kontradikce sémantickým důsledkem?*
3. *Čím se liší postup nalezení DNF a KNF dané formule?*
4. *Co je to funkční úplnost?*

Cvičení

1. Formuli $(q \Leftrightarrow \neg(r \Rightarrow p)) \vee p$ převeďte do DNF a KNF.
2. Rozhodněte, které z formulí

$$r \Rightarrow (\neg r \Rightarrow (q \Rightarrow r)), \quad p \Rightarrow (q \wedge r), \quad p \Rightarrow (q \Rightarrow \neg(p \Rightarrow q)),$$
$$(p \Rightarrow q) \Rightarrow \neg r, \quad (r \Rightarrow p) \Rightarrow (\neg q \Rightarrow \neg r), \quad \neg((p \vee q) \Rightarrow r),$$

   sémanticky plynou z formulí $p \Rightarrow \neg q, r \Rightarrow (p \vee r), r \Rightarrow \neg(p \Rightarrow q)$.
3. Dokažte následující tvrzení.
   (a) Pokud $\chi_1, \ldots, \chi_n \models \varphi$, pak $\vartheta_1, \ldots, \vartheta_k, \chi_1, \ldots, \chi_n \models \varphi$.
   (b) $\chi_1, \ldots, \chi_n, \neg\varphi \models p \wedge \neg p$, právě když $\chi_1, \ldots, \chi_n \models \varphi$.
   (c) Pokud $\chi_1, \ldots, \chi_n \models \varphi$ a $\chi_1, \ldots, \chi_n \models \varphi \Rightarrow \psi$, pak $\chi_1, \ldots, \chi_n \models \psi$.
   (d) φ a ψ jsou logicky ekvivalentní, právě když $\varphi \models \psi$ a $\psi \models \varphi$.

Úkoly k textu

1. Vraťte se k příkladu 1.3 na straně 9 a k úkolu k textu z minulé kapitoly. Pro vaši formalizaci již uvedených výroků

   „Pokud má Petr deštník, pak nejede autem“,
   „Večer nejsou na obloze červánky“,
   „Ráno je mlha, když neprší“,
   „K tomu aby Petr jel autem stačí aby byly na obloze červánky“,

   zjistěte, které z formulí příslušných výše uvedeným výrokům sémanticky plynou z formulí uvedených v příkladu 1.3 a přesvědčte se, zda-li výsledek koresponduje s intuitivním usuzováním.

2. Předpokládejme, že jisté zařízení je ovládáno člověkem – expertem, který na základě pozorování tří čidel A, B, C ovládá zařízení pomocí dvou spínačů P, Q. Čidla i spínače nabývají dvou stavů (nesvítí/svítí, případně vypnuto/zapnuto), které označíme $0/1$. Při každé konfiguraci čidel pracovník jistým způsobem nastaví spínače tak, aby zařízení vykonávalo požadovanou činnost. V následující tabulce je uvedena závislost nastavení spínačů na hodnotách čidel.

A	B	C	P	Q
0	0	0	1	0
0	0	1	1	1
0	1	0	0	1
0	1	1	1	0

A	B	C	P	Q
1	0	0	1	1
1	0	1	0	0
1	1	0	1	1
1	1	1	0	1

   Popište řídící činnost experta pomocí formulí.

Řešení

1. DNF: $(\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r)$; KNF: $(p \vee q \vee \neg r) \wedge (p \vee \neg q \vee r)$.
2. Sémantické důsledky: $r \Rightarrow (\neg r \Rightarrow (q \Rightarrow r))$, $p \Rightarrow (q \Rightarrow \neg(p \Rightarrow q))$, $(p \Rightarrow q) \Rightarrow \neg r$.
3. (a) Přímý důsledek faktu: pokud jsou při pravdivostním ohodnocení e pravdivé všechny formule $\vartheta_1, \ldots, \vartheta_k, \chi_1, \ldots, \chi_n$, pak jsou pravdivé i $\chi_1, \ldots, \chi_n$.
(b) Plyne z faktu, že formule $p \wedge \neg p$ je kontradikce, tudíž $\chi_1, \ldots, \chi_n, \neg\varphi \models p \wedge \neg p$, právě když neexistuje žádné pravdivostní ohodnocení, při kterém by byly všechny formule z $\chi_1, \ldots, \chi_n, \neg\varphi$ pravdivé.
(c) Vezměme pravdivostní ohodnocení e, při kterém jsou $\chi_1, \ldots, \chi_n$ pravdivé. Pak pokud $\|\varphi\|_e = 1$, pak z předpokladu $\|\varphi \Rightarrow \psi\|_e = 1 \rightarrow \|\psi\|_e = 1$, tedy $\|\psi\|_e = 1$.
(d) Plyne přímo z definice logické ekvivalence a sémantického vyplývání.

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.

Potřebný 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 $1, 2, 3, 4, 5, \dots$.
- $\mathbb{Z}$ označuje množinu všech *celých čísel*. $\mathbb{Z}$ tedy sestává z prvků $0, 1, -1, 2, -2, 3, -3, 4, -4, \dots$.
- $\mathbb{Q}$ 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 $1, 2, \dots n$. 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 $a_1, \dots, a_n$ se označuje $\{a_1, \dots, a_n\}$. 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 $\{x \mid \varphi(x)\}$.

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

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

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

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

Někdy se používá i pro zápis nekonečných množin způsob, který je podobný zápisu výčtem. Například množinu všech kladných sudých čísel zapíšeme $\{2, 4, 6, 8, \dots\}$. Obecně tedy můžeme použít zápis $\{a_1, a_2, a_3, a_4, \dots\}$, 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 $\{x \mid x \in A \text{ a } \varphi(x)\}$. 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 $\{x \mid x \in \mathbb{Z} \text{ a } x \leq 2\}$, 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 6 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 $\{2, 4, 8, 16, \ldots\}$.
- $\{k \in \mathbb{N} \mid k \neq 1 \text{ a jestliže } \exists m, n \in \mathbb{N} : m \cdot n = k, \text{ pak } m = 1 \text{ nebo } n = 1\}$ 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.

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

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

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 případ 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 následující: 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

Potenční množina množiny X je množina všech podmnožin množiny X.

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

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 $l \in J \cap A$.

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

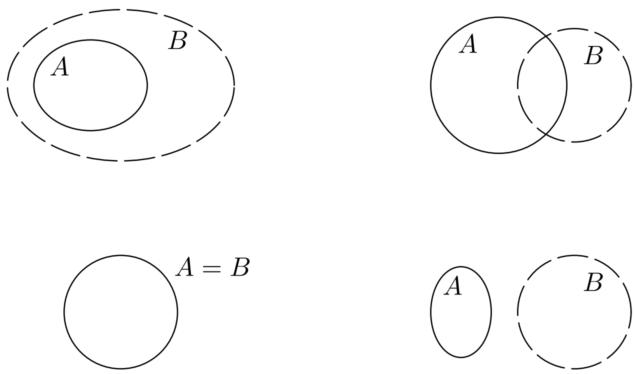
Základní operace s množinami jsou průnik, sjednocení a rozdíl.

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

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 $A \cap B = \emptyset$, $A \cup B = \{a,b,\{a\}\}$,



Obrázek 1: Vennovy diagramy.

- 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*[1]. 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.

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. $\square$

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 2.4 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.

Potřebný 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 $x_1 = y_1, \ldots,$ $x_n = y_n$. 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 $X_1, \dots, X_n$ jsou množiny. *Relace* mezi $X_1, \dots, X_n$ je libovolná podmnožina kartézského součinu $X_1 \times \cdots \times X_n$.

Relace mezi množinami $X_1, \dots, X_n$ 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 $x_1 \in X_1, \dots, x_n \in X_n$ říkáme, že jsou (v tomto pořadí) v relaci R, pokud $\langle x_1, \dots, x_n \rangle \in R$.

Relace je tedy množina sestávající z n-tic prvků příslušných množin. Obsahuje ty n-tice $\langle x_1, \dots, x_n \rangle$, 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 $X = \{2, \dots, 10\}$.

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

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 3: Databáze z Příkladu 2.15.

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, 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.[2] Tzv. relační pohled na databáze spočívá v tom, že databázi chápeme jako relaci. Např. databázi znázorněnou Tab. 3, která obsahuje v řádcích informace o zaměstnancích, můžeme chápat jako 5-ární relaci R mezi množinami (těm se v databázích říká domény) $D_1 = \{$Adam, Kos, Malá, Rychlý, $\dots\}$, $D_2 = \{$Jiří, Jan, Magda, Karel, $\dots\}$, $D_3 = \{n \in \mathbb{N} \mid 1900 \leq n \leq 2004\}$, $D_4 = \{$ZŠ, SOU, SŠ, VŠ$\}$, $D_5 = \{$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] 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	$\times$	$\times$		$\times$
b		$\times$		$\times$
c	$\times$			

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

(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.

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. 5. Tedy, je-li $\langle x, y\rangle \in R$, je v průsečíku řádku x a sloupce y symbol $\times$, jinak tam není nic.

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

S binárními relacemi lze navíc provádět operace inverze a skládání.

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

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. 5 vlevo, vztah „být příznakem nemoci“ mezi příznaky a nemocemi je popsán relací $S \subseteq Y \times Z$ znázorněnou v Tab. 5 vpravo. Složení relací R a S je relace $R \circ S \subseteq X \times Z$ znázorněná v

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

S	C	M	N	S	Za
b	$\times$	$\times$			
h	$\times$	$\times$		$\times$	
k	$\times$				
o					$\times$
r	$\times$			$\times$	
s		$\times$			
v			$\times$	$\times$	$\times$
z		$\times$			

Tabulka 5: K Příkladu 2.18: Tabulky popisující binární relaci R mezi pacienty a příznaky nemocí (vlevo) a relaci S příznaky nemocí a nemocemi (vpravo).

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

Tabulka 6: Tabulka popisující binární relaci $R \circ S$ mezi pacienty a nemocemi (viz Příklad 2.18).

Tab. 6. 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 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 $\langle x, y\rangle \in R$. $\square$

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 $R \Box S$ jsou relace mezi X a Z definované předpisy

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

$R \lhd S$	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 7: Tabulka popisující binární relace $R \lhd S$, $R \rhd S$ a $R \square S$ mezi pacienty a nemocemi (viz Příklad 2.20).

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. 7.

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.

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

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

R	1	2	3	4
a	$\times$	$\times$		$\times$
b		$\times$		$\times$
c	$\times$			

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

Tabulka 8: Tabulka (vlevo) a matice (vpravo) popisující binární relaci R mezi $X = \{a, b, c\}$ a $Y = \{1, 2, 3, 4\}$.

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. $\times$) 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).

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

$\mathbf{M}_R$ 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. 8 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.

$$\mathbf{M} \vee \mathbf{N} = \mathbf{P}, \qquad p_{ij} = \max\{m_{ij}, n_{ij}\}$$

$$\mathbf{M} \wedge \mathbf{N} = \mathbf{P}, \qquad p_{ij} = \min\{m_{ij}, n_{ij}\}$$

$$\mathbf{M} - \mathbf{N} = \mathbf{P}, \qquad p_{ij} = \max\{0, m_{ij} - n_{ij}\}$$

$$\mathbf{M} \cdot \mathbf{K} = \mathbf{P}, \qquad p_{ij} = \max\{m_{il} \cdot k_{lj};\, l = 1, \ldots, n\}$$

$$\mathbf{M}^T, \qquad m^T_{ij} = m_{ji}\,.$$

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

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

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

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

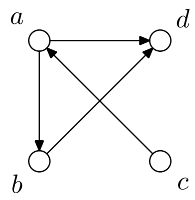
Matice relace R_{-1} je

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

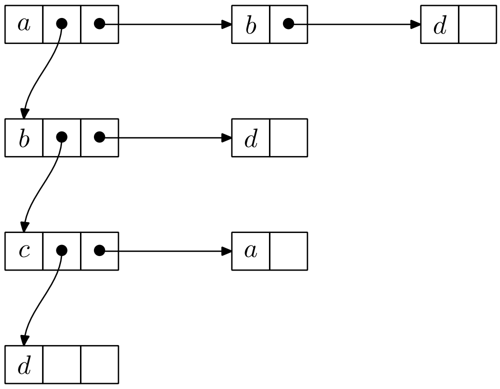
Reprezentace grafem

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.



Obrázek 2: Graf relace k Příkladu 2.24.



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

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 4. 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[3], ve kterém jsou uloženy všechny prvky množiny X. Na Obr. 3 je hlavní seznam znázorněn shora dolů spojenými čtverečky, které obsahují a, $\dots$, 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.

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[4].

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

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

2.4 Funkce (zobrazení)

2.4.1 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 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 $f, g, \dots$ než $R, S, \dots$. 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 $\{\langle x, y\rangle \mid x \in X, y \in Y, y = f(x)\}$.

2.4.2 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. □

2.4.3 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 $k \in K$. $\square$

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.

2.4.4 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 $A = \{2, 4, 6\}$, $B = \{n \in \mathbb{N} \mid n \leq 10000000$ a n 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 $A = \{2, 4, 6, 8, \ldots\}$, $B = \{2, 2^2, 2^{(2^2)}, 2^{(2^{(2^2)})}, \ldots\}$, $B = \mathbb{Z}$, $C = \mathbb{Q}$, $D = \mathbb{R}$, $E = [0, 1]$ 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. *Necht' 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 $a_1, \dots, a_n$ 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 $a_1, \dots, a_{k+1}$. Pak $a_1, \dots, a_k$ je posloupnost k prvků a $a_2, \dots, a_{k+1}$ 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 Kombinatorika

Studijní cíle: Po prostudování kapitol 3.1, 3.2 a 3.3 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

Potřebný čas: 180 minut.

3.1 Co a k čemu je kombinatorika

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.

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

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 3.1. 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 3.2. 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 3.3. 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.

3.2 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 3.4. 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 3.5. 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 3.5, 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 3.6. 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 3.5 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 3.7. 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 3.8. 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 3.9. 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 3.7). 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 3.5). Proto lze podle pravidla součtu prvek z $(A \cup B) \times C$ vybrat $(|A| + |B|) \cdot |C|$ způsoby, tedy $|(A \cup B) \times C| = (|A| + |B|) \cdot |C|$.

3.3 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.

3.3.1 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 3.10 (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 3.11. $P(n) = n!$.

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 $n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 1 = n!$ 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 3.12 (permutace s opakováním). Je dáno n objektů rozdělených do r skupin, které mají po řadě $n_1, \dots, n_r$ objektů, tj. $n_1 + \dots + n_r = n$. Objekty v každé ze skupin jsou navzájem nerozlišitelné. Každé seřazení těchto n objektů se nazývá *permutace s opakováním* (daným parametry $(n_1, \dots, n_r)$). Počet takových permutací značíme $P(n_1, \dots, n_r)$.

Věta 3.13. *Pro* $n_1 + \dots + n_r = n$ *je* $P(n_1, \dots, n_r) = \frac{n!}{n_1! \cdot \dots \cdot n_r!}$.

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 $(1 \le i \le n)$ je v permutaci s opakováním objekt z j-té skupiny $(1 \le i \le n)$, 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 $A_3B_1A_2A_1B_2$, ne však permutace $A_3A_2A_1B_1B_2$.

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 $n_1! \cdot \dots \cdot n_r!$. Dostali jsme tedy

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

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

Příklad 3.14. 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 $P(2, 3, 1, 2, 1, 1, 1) = \frac{11!}{2!3!2!}$.

3.3.2 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 3.15 (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 3.16. $V(n, r) = n \cdot (n-1) \cdot \dots \cdot (n-r+1)$.

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, $n \cdot (n-1) \cdot \dots \cdot (n-r+1)$. □

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

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

Příklad 3.17. 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 3.18. 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 3.19 (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 3.20. $\overline{V}(n,r) = n^r$.

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 $n \cdot \dots \cdot n = n^r$ způsoby. $\square$

Poznámka 3.21. 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 3.19. Důležité však je, že počet variací s opakováním je i v tomto případě $\overline{V}(n,r)$ (ověřte).

Příklad 3.22. 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 $d = 7$.

3.3.3 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 3.23 (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 nazývájí *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 3.24. $\binom{n}{r} = \frac{n!}{(n-r)!r!}$.

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

počet kombinací r z n krát počet uspořádání r objektů = počet variací r 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 3.25. 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 3.13 $\frac{n!}{(n-r)!r!}$.

Příklad 3.26. 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

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}. \tag{3.1}$$

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

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k. \tag{3.2}$$

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

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

Přitom jsme použili vzorec (3.1). □

Binomická věta má řadu použití.

Příklad 3.28 (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 3.28. 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 3.29 (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 3.30. $\overline{C}(n,r) = \binom{n+r-1}{n-1}$.

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 3.24 $\binom{n+r-1}{n-1}$. $\square$

Příklad 3.31. Vraťme se k zákuskům (viz výše). Výběr 6 zákusků ze 4 druhů zákusků je kombinace 6 z 4 s opakováním. Těch je podle Věty 3.30 $\overline{C}(n,r) = \binom{n+r-1}{n-1} = \binom{4+6-1}{4-1} = \binom{9}{3} = \frac{9!}{6!3!} = 84$.

Poznámka 3.32. 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.

3.3.4 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 3.33. 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 3.34. 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. židi, ..., 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 3.35. 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 3.1, 3.2, 3.3 zdůvodněte použité kombinatorické úvahy.
2. Vraťme se k Příkladu 3.3. 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 3.3 tedy dává odpověď pro $t = 1$. [Odpověď: $\frac{2^n}{1+n+\binom{n}{2}+\cdots+\binom{n}{r}}$.]
3. Vraťme se k Příkladu 3.8. 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 3.13.
5. Zdůvodněte podrobně Větu 3.16.
6. Zdůvodněte podrobně Větu 3.24.

   Promyslete si a zdůvodněte důkaz Věty 3.30.

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 $|P^n(X)| = 2^{2^{\cdot^{\cdot^{\cdot^{k}}}}}$ (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 3.35 $\binom{n-k+1}{k}$.

Studijní cíle: Po prostudování kapitol 3.4 a 3.5 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

Potřebný čas: 160 minut.

3.4 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 3.36 (princip inkluze a exkluze). *Pro množiny $A_1, \dots, A_n$ platí*

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

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 $A_1, \dots, A_n$. Na pravé straně je součet výrazů $(-1)^{|I|+1}|\cap_{i \in I} A_i|$, kde I probíhá přes všechny neprázdné podmnožiny množiny $\{1, \dots, n\}$. $|\cap_{i \in I} A_i|$ 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 $A_1, \dots, A_n$, 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 3.36.

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 $A_1, \dots, A_k$. Můžeme předpokládat, že to jsou množiny $A_1, \dots, A_k$ (kdyby ne, množiny přeznačíme). Pak x patří do nějakého průniku, který je na pravé straně rovnosti, právě když je to průnik nějakých množin z $A_1, \dots, A_j$. 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 $A_1, \dots, A_k$ 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 (3.2) $x = -1$. Dostaneme

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

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 3.37. 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

$$A_1 = \{n \in \mathbb{N} \mid 1 \leq n \leq 100,\ n \text{ je dělitelné } 2\}, \tag{3.3}$$
$$A_2 = \{n \in \mathbb{N} \mid 1 \leq n \leq 100,\ n \text{ je dělitelné } 3\}, \tag{3.4}$$
$$A_3 = \{n \in \mathbb{N} \mid 1 \leq n \leq 100,\ n \text{ je dělitelné } 5\}. \tag{3.5}$$

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 $|A| = 100 - |A_1 \cup A_2 \cup A_3| = 26$.

3.5 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 3.38. 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 3.39. 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 3.39. 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 číla padla. Tedy hod můžeme chápat jako kombinaci 2 z 6 s opakováním a těch je podle Věty 3.30 $\overline{C}(6,2) = \binom{6+2-1}{6-1} = \binom{7}{5} = 21$. 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 3.39! 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 3.40. Jaká je pravděpodobnost, že při rozdávání 4 karet z balíčku 32 hracíh 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 3.40.
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 3.1, 3.2, 3.3 zdůvodněte použité kombinatorické úvahy.
2. Vraťme se k Příkladu 3.3. 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 3.3 tedy dává odpověď pro $t = 1$. [Odpověď: $\frac{2^n}{1+n+\binom{n}{2}+\cdots+\binom{n}{r}}$.]
3. Vyřešte podrobně Příklad 3.37.
4. Na základě Příkladu 3.37 dokažte následující tvrzení: Jsou-li podmnožiny $A_1, \dots, A_n$ nějaké k-prvkové množiny X, pak počet prvků množiny X, které nepatří ani jedné z množin $A_1, \dots, A_n$ je $k - \sum_{\emptyset \neq I \subseteq \{1,2,\dots,n\}} (-1)^{|I|+1} |\bigcap_{i \in I} A_i|$.
5. Vysvětlete podrobně chybu popsanou v odstavci na Příkladem 3.39.

Řešení

1. 534.
2. 458.
3. 76.
4. $15!\left(\binom{14}{10} - \binom{5}{1}\binom{10}{6} + \binom{5}{2}\binom{6}{2}\right)$.
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