Množiny
Kombinatorika
Logické funkcie
Teória grafov

prof. RNDr. Martin Škoviera, PhD.

Katedra informatiky, FMFI UK

Bratislava 2023

Obsah

Kapitola 2

Množiny

2.1 Základné operácie

Pojem množiny je jedným zo základov súčasnej matematiky. Bez objasnenia základov teórie množín je dnes nepredstaviteľné hlbšie štúdium akéhokoľvek matematického predmetu – ani diskrétnej matematiky.

Teória množín pracuje s dvoma ústrednými pojmami, ktorými sú „množina“ a „byť prvkom“. Pod množinou si predstavujeme súbor objektov, ktoré (spravidla) majú nejakú spoločnú vlastnosť. Tieto objekty nazývame prvkami množiny. Súhrnom svojich prvkov je množina jednoznačne určená. Ak $\boldsymbol{A}$ je množina, skutočnosť, že x je jej prvkom zapisujeme takto: $x \in \boldsymbol{A}$. Opak zapisujeme $x \notin \boldsymbol{A}$. Treba povedať, že v čistej matematike prvkom množiny môže byť opäť jen množina. Vzťah $\in$, „byť prvkom“ je preto reláciou medzi množinami. Dve množiny $\boldsymbol{A}$ a $\boldsymbol{B}$ sa teda rovnajú práve vtedy, keď majú tie isté prvky:

$$\boldsymbol{A} = \boldsymbol{B} \;\Leftrightarrow\; (\forall x :\; x \in \boldsymbol{A} \Leftrightarrow x \in \boldsymbol{B})$$

Ako zadávame množiny? Jednou z možností je vymenovať všetky jej prvky. Zápis $\boldsymbol{A} = \{a,\ b,\ c,\ d\}$ označuje množinu, ktorej prvky sú (množiny) $a,\ b,\ c$ a d a žiadne iné. Druhou možnosťou je zadanie množiny pomocou vlastnosti, ktorú majú mať jej prvky. Zápisom $\boldsymbol{A} = \{x;\ P(x)\}$ vyjadrujeme skutočnosť, že množinu $\boldsymbol{A}$ tvoria tie a len tie prvky, ktoré majú vlastnosť P. Takto môžeme zadať napríklad niektoré významné číselné množiny:

$\mathbb{N}$ – množina prirodzených čísel

$\mathbb{Z}$ – množina celých čísel

$\mathbb{Q}$ – množina racionálnych čísel

$\mathbb{R}$ – množina reálnych čísel

Pri takomto spôsobe zadávania množín si však musíme dávať pozor na vlastnosť P: nie každá vlastnosť určuje množinu. Vyplýva to z nasledujúceho príkladu známeho ako Russelov paradox:

Uvažujme vlastnosť $R(x) : \ x \notin x$. Ako sme už spomenuli, prvkami množín sú opäť množiny. Zo skúsenosti vieme, že vyššie uvedená vlastnosť je často splnená. Napríklad $\mathbb{N} \notin \mathbb{N}$, lebo prvkami množiny $\mathbb{N}$ sú prirodzené čísla, no samotná množina $\mathbb{N}$ nie je prirodzené číslo. Zdá sa, že R je „rozumná vlastnosť“ a nič nám nebráni vytvoriť množinu $\boldsymbol{M} = \{x;\ R(x)\}$. Do množiny $\boldsymbol{M}$ patria napríklad známe číselné množiny $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ a mnohé ďalšie, ba aj všetky množiny, ktoré nám zídu na um. Čo však samotná množina $\boldsymbol{M}$?

Sú len dve možnosti: buďto $\boldsymbol{M}$ má vlastnosť R alebo ju nemá. Ak $\boldsymbol{M}$ má vlastnosť R, tak ju – podľa definície množiny $\boldsymbol{M}$ – musíme zaradiť medzi prvky množiny $\boldsymbol{M}$. Čiže $\boldsymbol{M} \in \boldsymbol{M}$ – no to je spor, lebo odporuje vlastnosti R.

Ostáva teda iba druhá možnosť: $\boldsymbol{M}$ nemá vlastnosť R. Z definície vlastnosti R teraz vyplýva, že $\boldsymbol{M} \in \boldsymbol{M}$. No každý prvok množiny $\boldsymbol{M}$, teda aj sama $\boldsymbol{M}$, spĺňa vlastnosť R, čiže $\boldsymbol{M} \notin \boldsymbol{M}$ – opäť spor.

Dôsledkom týchto úvah je, že $\boldsymbol{M} = \{x;\ R(x)\}$ nie je množinou. Inými slovami, vlastnosť R je taká, že nám nedovoľuje vytvoriť množinu. Príčina tohto paradoxu spočíva v tom, že sme pojem množiny zaviedli len intuitívne (ako „súbor“). Ak sa chceme vyhnúť Russelovmu paradoxu, musíme vybudovať základy teórie množín systematicky. Toto sa rieši pomocou axiomatickej výstavby teórie množín. My sa axiomatickou teóriou množín zaoberať nebudeme. Namiesto toho budeme pracovať len s takými súbormi, ktoré tvoria množiny a používať postupy, ktoré nám umožnia vytvoriť nové množiny z už známych východiskových množín.

Nech $\boldsymbol{A}$ a $\boldsymbol{B}$ sú množiny. Budeme hovoriť, že $\boldsymbol{A}$ je „podmnožinou“ množiny $\boldsymbol{B}$, ak každý prvok množiny $\boldsymbol{A}$ je zároveň prvkom množiny $\boldsymbol{B}$. Túto skutočnosť zapisujeme $\boldsymbol{A} \subseteq \boldsymbol{B}$. Symbolicky:

$$\boldsymbol{A} \subseteq \boldsymbol{B} \Leftrightarrow (\forall x :\ x \in \boldsymbol{A} \Rightarrow x \in \boldsymbol{B})$$

Ak $\boldsymbol{A} \subseteq \boldsymbol{B}$, ale $\boldsymbol{A} \neq \boldsymbol{B}$, tak hovoríme, že $\boldsymbol{A}$ je „vlastnou podmnožinou“ množiny $\boldsymbol{B}$ a píšeme $\boldsymbol{A} \subset \boldsymbol{B}$, prípadne – kvôli dôrazu – $\boldsymbol{A} \subsetneq \boldsymbol{B}$.

Porovnaním definícií uvidíme tiež to, že $\boldsymbol{A} = \boldsymbol{B}$ práve vtedy, keď $\boldsymbol{A} \subseteq \boldsymbol{B}$ a zároveň $\boldsymbol{B} \subseteq \boldsymbol{A}$. Toto pozorovanie často používame pri dokazovaní rovnosti dvoch množín $\boldsymbol{X}$ a $\boldsymbol{Y}$: najprv dokážeme $\boldsymbol{X} \subseteq \boldsymbol{Y}$ a potom $\boldsymbol{Y} \subseteq \boldsymbol{X}$ (alebo obrátene).

Nové množiny často vytvárame ako podmnožiny už jestvujúcich množín – do podmnožiny zahrnieme všetky prvky danej množiny, ktoré majú predpísanú vlastnosť. Napríklad môžeme vytvoriť množinu

$$\boldsymbol{F} = \{x \in \mathbb{N};\ x \text{ je deliteľné číslom } 5\}$$

všetkých prirodzených čísel, ktoré sú násobkami čísla 5.

Z daných množín $\boldsymbol{A}$ a $\boldsymbol{B}$ môžeme vytvoriť novú množinu $\boldsymbol{A} \cup \boldsymbol{B}$, ktorej prvky sú práve prvky množiny $\boldsymbol{A}$ a prvky množiny $\boldsymbol{B}$. Symbolicky:

$$\boldsymbol{A} \cup \boldsymbol{B} = \{x;\ (x \in \boldsymbol{A}) \vee (x \in \boldsymbol{B})\}$$

Množina $\boldsymbol{A} \cup \boldsymbol{B}$ sa nazýva „zjednotenie“ množín $\boldsymbol{A}$ a $\boldsymbol{B}$.

Axióma 1 (Axióma zjednotenia)**.**

$$\forall \boldsymbol{S}\ \exists \boldsymbol{U} \forall\ x\ :\quad (x \in \boldsymbol{U} \Leftrightarrow \exists\ \boldsymbol{A} \in \boldsymbol{S} :\ x \in \boldsymbol{A})$$

Množina $\boldsymbol{U} = \bigcup \boldsymbol{S}$ sa nazýva zjednotením množiny $\boldsymbol{S}$.

Príklad 2.1. $\bigcup\{\{a,b\},\{c,d\},\{e,f\}\} = \{a,b,c,d,e,f\}$, $\bigcup\{\boldsymbol{A},\boldsymbol{B}\} = \boldsymbol{A} \cup \boldsymbol{B}$, $\bigcup\{\boldsymbol{A},\boldsymbol{A}\} = \boldsymbol{A}$.

Ak $\boldsymbol{A}$ a $\boldsymbol{B}$ sú ľubovoľné množiny, môžeme vytvoriť ich „prienik“ $\boldsymbol{A} \cap \boldsymbol{B}$, množinu vštkých prvkov, ktoré patria súčasne do oboch množín $\boldsymbol{A}$ a $\boldsymbol{B}$:

$$\boldsymbol{A} \cap \boldsymbol{B} = \{x;\ (x \in \boldsymbol{A}) \wedge (x \in \boldsymbol{B})\}$$

Poznamenajme, že prienik môžeme vytvoriť aj ako podmnožinu každej z množín, ktoré prienik vytvárajú:

$$\boldsymbol{A} \cap \boldsymbol{B} = \{x \in \boldsymbol{A};\ x \in \boldsymbol{B}\} = \{x \in \boldsymbol{B};\ x \in \boldsymbol{A}\}$$

Môže sa stať, že množiny $\boldsymbol{A}$ a $\boldsymbol{B}$ nemajú žiadne spoločné prvky – potom množina $\boldsymbol{A} \cap \boldsymbol{B}$ nemá žiadne prvky. Množina bez prvkov sa nazýva „prázdna množina“ a označuje sa $\emptyset$ (niekedy tiez $\{\}$). Ak $\boldsymbol{A} \cap \boldsymbol{B} = \emptyset$, hovoríme, že množiny $\boldsymbol{A}$ a $\boldsymbol{B}$ sú „disjunktné“.

Je zrejmé, že existuje len jedna prázdna množina a že je podmnožinou každej množiny.

Zo všetkých podmnožín danej množiny $\boldsymbol{A}$ môžeme vytvoriť novú množinu $\mathcal{P}(\boldsymbol{A})$ – potenčnú množinu množiny $\boldsymbol{A}$:

$$\mathcal{P}(\boldsymbol{A}) = \{\boldsymbol{X};\ \boldsymbol{X} \subseteq \boldsymbol{A}\}$$

Niekedy sa táto množina označuje $2^{\boldsymbol{A}}$ – z dôvodov, ktoré budú zrejmé neskôr. Všimnime si, že potenčná množina je vždy neprázdna, lebo $\emptyset \in \mathcal{P}(\boldsymbol{A})$ pre každú množinu $\boldsymbol{A}$. Napríklad ak $\boldsymbol{A} = \{a, b\}$ tak $\mathcal{P}(\boldsymbol{A}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

Operácie zjednotenia a prieniku môžeme za istých podmienok zovšeobecniť na „systémy množín“. Ak $\boldsymbol{A}$ je neprázdna množina, jej prvky sú opäť množiny. Preto sa na ňu môžeme dívať aj ako na systém množín, ktoré môžeme zjednotiť alebo preniknúť. Nech $\boldsymbol{A} \neq \emptyset$. Definujme

$$\bigcup \boldsymbol{A} = \{x;\ \exists \boldsymbol{Z} \in \boldsymbol{A} :\ x \in \boldsymbol{Z}\}$$
$$\bigcap \boldsymbol{A} = \{x;\ \forall \boldsymbol{Z} \in \boldsymbol{A} :\ x \in \boldsymbol{Z}\}$$

Napríklad pre $\boldsymbol{A} = \{\emptyset, \{1, 2\}, \{1, 3\}\}$ máme $\cup\boldsymbol{A} = \{1, 2, 3\}$ a $\cap\boldsymbol{A} = \emptyset$, pre $\boldsymbol{A} = \{\emptyset\}$ dostávame $\cup\boldsymbol{A} = \cap\boldsymbol{A} = \emptyset$ a pre $\boldsymbol{A} = \{\{1, 2\}, \{1, 3\}\}$ máme $\cap\boldsymbol{A} = \{1\}$.

Veľmi často všetky operácie vykonáme vnútri nejakej „veľkej“ množiny $\boldsymbol{U}$, v ktorej sú ako podmnožiny obsiahnuté všetky množiny, ktoré potrebujeme. Množinu $\boldsymbol{U}$ v takom prípade nazývame „univerzum“.

V univerze $\boldsymbol{U}$ môžeme ku každej množine $\boldsymbol{A} \subseteq \boldsymbol{U}$ vytvoriť jej „doplnok“ (komplement)) ako množinu

$$\boldsymbol{A}^{\boldsymbol{C}} = \{x \in \boldsymbol{U};\ x \notin \boldsymbol{A}\}$$

Doplnok však môžeme vytvoriť nielen vzhľadom na univerzálnu množinu, ale aj vzhľadom na ľubovoľnú inú množinu. Na to nám slúži ďalšia operácia s množinami – rozdiel množín.

Nech $\boldsymbol{A}$ a $\boldsymbol{B}$ sú ľubovoľné množiny. „Rozdielom“ množín $\boldsymbol{A}$ a $\boldsymbol{B}$ rozumieme množiny všetkých tých prvkov množiny $\boldsymbol{A}$, ktoré nepatria do $\boldsymbol{B}$:

$$\boldsymbol{A} - \boldsymbol{B} = \{x \in \boldsymbol{A};\ x \notin \boldsymbol{B}\}$$

Doplnok množiny $\boldsymbol{A}$ v univerze $\boldsymbol{U}$ potom nie je nič iné ako množina $\boldsymbol{U} - \boldsymbol{A}$. Na druhej strame rozdiel množín $\boldsymbol{A}$ a $\boldsymbol{B}$ v univerze $\boldsymbol{U}$ môžeme vyjadriť pomocou doplnku:

$$\boldsymbol{A} - \boldsymbol{B} = \boldsymbol{A} \cap \boldsymbol{B}^{\boldsymbol{C}}$$

Poznamenajme, že pri práci v univerze $\boldsymbol{U}$ býva zvykom položiť $\cup\emptyset = \emptyset$ a $\cap\emptyset = \boldsymbol{U}$. Táto voľba má v istých situáciach svoje výhody. Stretneme sa s nimi často najmä v nasledujúcej kapitole.

V nasledujúcich dvoch tvrdeniach zhrnieme základné vzťahy medzi štyrmi operáciami na možinách, ktoré sme doposiaľ zaviedli.

Tvrdenie 2.1. (a) $\boldsymbol{A} \cup \boldsymbol{A} = \boldsymbol{A}, \quad \boldsymbol{A} \cap \boldsymbol{A} = \boldsymbol{A}$ (idempotentnosť)

(b) $\boldsymbol{A} \cup \boldsymbol{B} = \boldsymbol{B} \cup \boldsymbol{A}, \quad \boldsymbol{A} \cap \boldsymbol{B} = \boldsymbol{B} \cap \boldsymbol{A}$ (komutatívnosť)

(c) $\boldsymbol{A} \cup (\boldsymbol{B} \cup \boldsymbol{C}) = (\boldsymbol{A} \cup \boldsymbol{B}) \cup \boldsymbol{C}, \quad \boldsymbol{A} \cap (\boldsymbol{B} \cap \boldsymbol{C}) = (\boldsymbol{A} \cap \boldsymbol{B}) \cap \boldsymbol{C}$ (asociatívnosť)

(d) $\boldsymbol{A} \cap (\boldsymbol{B} \cup \boldsymbol{C}) = (\boldsymbol{A} \cap \boldsymbol{B}) \cup (\boldsymbol{A} \cap \boldsymbol{C})$, $\boldsymbol{A} \cup (\boldsymbol{B} \cap \boldsymbol{C}) = (\boldsymbol{A} \cup \boldsymbol{B}) \cap (\boldsymbol{A} \cup \boldsymbol{C})$ (distributívnosť)

(e) $(\boldsymbol{A} \cup \boldsymbol{B})^{\boldsymbol{C}} = \boldsymbol{A}^{\boldsymbol{C}} \cap \boldsymbol{B}^{\boldsymbol{C}}, \quad (\boldsymbol{A} \cap \boldsymbol{B})^{\boldsymbol{C}} = \boldsymbol{A}^{\boldsymbol{C}} \cup \boldsymbol{B}^{\boldsymbol{C}}$ (de Morganove zákony)

(f) $\left(\boldsymbol{A}^{\boldsymbol{C}}\right)^{\boldsymbol{C}} = \boldsymbol{A}$

(g) $\boldsymbol{A} \cap \emptyset = \emptyset, \quad \boldsymbol{A} \cup \emptyset = \boldsymbol{A}$

(h) $\boldsymbol{A} \cap \boldsymbol{A}^{\boldsymbol{C}} = \emptyset, \quad \boldsymbol{A} \cup \boldsymbol{A}^{\boldsymbol{C}} = U$

(i) $\boldsymbol{A} \cap (\boldsymbol{A} \cup \boldsymbol{B}) = \boldsymbol{A}, \quad \boldsymbol{A} \cup (\boldsymbol{A} \cap \boldsymbol{B}) = \boldsymbol{A}$ (absorpcia)

Dôkaz. Vo všetkých prípadoch možno použiť priamy dôkaz a pridŕžať sa nasledujúcej schémy, napr.

(c)
1. $x \in \boldsymbol{A} \cup (\boldsymbol{B} \cup \boldsymbol{C})$ vyberieme ľubovoľný prvok $x \in \boldsymbol{A} \cup (\boldsymbol{B} \cup \boldsymbol{C})$
2. $(x \in \boldsymbol{A}) \vee x \in (\boldsymbol{B} \cup \boldsymbol{C})$ rozpíšeme podľa definície zjednotenia
3. $(x \in \boldsymbol{A}) \vee [(x \in \boldsymbol{B}) \vee (x \in \boldsymbol{C})]$ opäť rozpíšeme
4. $(x \in \boldsymbol{A}) \vee (x \in \boldsymbol{B}) \vee (x \in \boldsymbol{C})$ disjunkcia je asociatívna logická operácia
5. $x \in (\boldsymbol{A} \cup \boldsymbol{B}) \vee (x \in \boldsymbol{C})$ podľa definície zjednotenia
6. $x \in (\boldsymbol{A} \cup \boldsymbol{B}) \cup \boldsymbol{C}$ podľa definície zjednotenia

Na výber prvku x sme nekládli žiadne obmedzenia. Z toho vyplýva, že každý prvok z $\boldsymbol{A} \cup (\boldsymbol{B} \cup \boldsymbol{C})$ patrí aj do $(\boldsymbol{A} \cup \boldsymbol{B}) \cup \boldsymbol{C}$. Naviac pri dôkaze sme používali len ekvivalentné úpravy výrokov, a tým sme dokázali aj tvrdenie, že každý prvok z $(\boldsymbol{A} \cup \boldsymbol{B}) \cup \boldsymbol{C}$ patrí do množiny $\boldsymbol{A} \cup (\boldsymbol{B} \cup \boldsymbol{C})$. Dokázali sme teda

$$\begin{array}{lcll} \boldsymbol{A} \cup (\boldsymbol{B} \cup \boldsymbol{C}) & \subseteq & (\boldsymbol{A} \cup \boldsymbol{B}) \cup \boldsymbol{C} & \text{a} \\ (\boldsymbol{A} \cup \boldsymbol{B}) \cup \boldsymbol{C} & \subseteq & \boldsymbol{A} \cup (\boldsymbol{B} \cup \boldsymbol{C}), & \text{čiže} \\ (\boldsymbol{A} \cup \boldsymbol{B}) \cup \boldsymbol{C} & = & \boldsymbol{A} \cup (\boldsymbol{B} \cup \boldsymbol{C}). & \end{array}$$

Zhrnieme celý postup: vybrali sme ľubovoľný prvok x z množiny ležiacej na ľavej strane identity. Využili sme definície množinových operácií a výrok "x patrí do zloženej množiny" sme rozpísali na zložený výrok o príslušnosti x do množín $\boldsymbol{A}$, $\boldsymbol{B}$. Tento zložený výrok sme upravili využijúc poznatky z výrokovej logiky. (Pozor, tu si treba uvedomiť, či sme použili ekvivalentné úpravy, napr. $(p \vee q) \Leftrightarrow (q \vee p)$, alebo len "jednostranné", – napr. $(p \wedge q) \rightarrow p$.) Zložený výrok sme potom, použijúc definície množinových operácií, upravili na výrok o príslušnosti prvku do "zloženej" množiny z pravej strany identity. Ak sme pri úpravách výrokov použili ekvivalentné úpravy, dokázali sme týmto rovnosť množín; ak sme použili neekvivalentné úpravy, dokázali sme množinovú inklúziu.
Pri dôkaze ďalšieho tvrdenia budeme stručnejší:

(d)
1. $[x \in \boldsymbol{A} \cap (\boldsymbol{B} \cup \boldsymbol{C})] \Leftrightarrow [(x \in \boldsymbol{A}) \wedge x \in (\boldsymbol{B} \cup \boldsymbol{C})]$
2. $[(x \in \boldsymbol{A}) \wedge x \in (\boldsymbol{B} \cup \boldsymbol{C})] \Leftrightarrow [(x \in \boldsymbol{A}) \wedge ((x \in \boldsymbol{B}) \vee (x \in \boldsymbol{C}))]$
3. $[(x \in \boldsymbol{A}) \wedge ((x \in \boldsymbol{B}) \vee (x \in \boldsymbol{C}))] \Leftrightarrow$
   $\Leftrightarrow [((x \in \boldsymbol{A}) \wedge (x \in \boldsymbol{B})) \vee ((x \in \boldsymbol{A}) \wedge (x \in \boldsymbol{C}))]$
4. $[((x \in \boldsymbol{A}) \wedge (x \in \boldsymbol{B})) \vee ((x \in \boldsymbol{A}) \wedge (x \in \boldsymbol{C}))] \Leftrightarrow$
   $\Leftrightarrow [(x \in \boldsymbol{A} \cap \boldsymbol{B}) \vee x \in (\boldsymbol{A} \cap \boldsymbol{C})]$
5. $[(x \in \boldsymbol{A} \cap \boldsymbol{B}) \vee x \in (\boldsymbol{A} \cap \boldsymbol{C})] \Leftrightarrow [x \in (\boldsymbol{A} \cap \boldsymbol{B}) \cup (\boldsymbol{A} \cap \boldsymbol{C})]$.

V krokoch 1, 2, 4 a 5 sme použili definície prieniku a zjednotenia, v kroku 3, ktorý je kľúčový pre dôkaz identity, sme využili distributívny zákon pre konjunkciu a disjunkciu z výrokovej logiky.

□

Tvrdenie 2.2. *Nech $\boldsymbol{A}, \boldsymbol{B}$ a $\boldsymbol{C}$ sú ľubovoľné množiny. Potom platia nasledujúce rovnosti:*

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

(b) $(\boldsymbol{A} \cup \boldsymbol{B}) - \boldsymbol{C} = (\boldsymbol{A} - \boldsymbol{C}) \cup (\boldsymbol{B} - \boldsymbol{C})$

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

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

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

(f) $(\boldsymbol{A} - \boldsymbol{B}) - \boldsymbol{C} = \boldsymbol{A} - (\boldsymbol{B} \cup \boldsymbol{C})$

Dôkaz. Pri dôkazoch týchto identít nebudeme používať bezprostredne definície množinových operácií, ale využijeme už dokázané množinové identity. Budeme sa pridržiavať takejto taktiky: zoberieme tú stranu identity, ktorá vyzerá zložitejšie a snažíme sa ju ekvivalentnými úpravami upraviť na výraz ležiaci na druhej strane identity. Pri úpravách najprv nahradíme rozdiel množín $\boldsymbol{X} - \boldsymbol{Y}$ prienikom $\boldsymbol{X} \cap \boldsymbol{Y}^{\boldsymbol{C}}$. Ak je $\boldsymbol{Y}$ v tvare zjednotenia alebo prieniku množín, využijeme de Morganove zákony a upravíme výraz na taký tvar, v ktorom vystupujú už len doplnky „jednoduchých“ množín. Potom použijeme distributívny zákon, využijeme asociatívny, komutatívny a absorbčný zákon, resp. zákon idempotentnosti a upravíme výraz na potrebný tvar.

Tento postup ilustrujeme na dôkaze identít (c) a (e):

(c) $(\boldsymbol{C} - \boldsymbol{A}) \cap (\boldsymbol{C} - \boldsymbol{B}) = (\boldsymbol{C} \cap \boldsymbol{A}^{\boldsymbol{C}}) \cup (\boldsymbol{C} \cap \boldsymbol{B}^{\boldsymbol{C}}) = \boldsymbol{C} \cap (\boldsymbol{A}^{\boldsymbol{C}} \cup \boldsymbol{B}^{\boldsymbol{C}}) =$
$= \boldsymbol{C} \cap (\boldsymbol{A} \cap \boldsymbol{B})^{\boldsymbol{C}} = \boldsymbol{C} - (\boldsymbol{A} \cap \boldsymbol{B})$

(e) $\boldsymbol{A} - (\boldsymbol{B} - \boldsymbol{C}) = \boldsymbol{A} \cap (\boldsymbol{B} \cap \boldsymbol{C}^{\boldsymbol{C}})^{\boldsymbol{C}} = \boldsymbol{A} \cap (\boldsymbol{B}^{\boldsymbol{C}} \cup \boldsymbol{C}) = (\boldsymbol{A} \cap \boldsymbol{B}^{\boldsymbol{C}}) \cup (\boldsymbol{A} \cap \boldsymbol{C}) =$
$= (\boldsymbol{A} - \boldsymbol{B}) \cup (\boldsymbol{A} \cap \boldsymbol{C})$

□

Čitateľ si môže všimnúť rozdiely medzi dôkazmi identít z Tvrdenia 2.1 a Tvrdenia 2.2 Kým v prvých sme robili ekvivalentné úpravy výrokov, v druhých ekvivalentné úpravy množín. Častou chybou býva neuvedomenie si rozdielu medzi množinovými a logickými operáciami, čo vedie k nezmyselným tvrdeniam typu $(x \in \boldsymbol{A}) \vee (x \in \boldsymbol{B}) = (\boldsymbol{A} \cup \boldsymbol{B})$, kde na jednej strane rovnosti (ekvivalencie) stojí výrok, na druhej množina.

Ďalším pravidlom, ktoré nám umožňuje tvoriť nové množiny, je *pravidlo* (axióma) neusporiadanej dvojice:

Ak $\boldsymbol{A}$ a $\boldsymbol{B}$ sú ľubovoľné množiny, tak existuje množina $\{\boldsymbol{A}, \boldsymbol{B}\}$, ktorej prvky sú len $\boldsymbol{A}$ a $\boldsymbol{B}$.

Toto konštrukčné pravidlo je veľmi silné. Napríklad ak $\boldsymbol{A} = \emptyset$ a $\boldsymbol{B} = \emptyset$, tak dostávame množinu $\{\emptyset, \emptyset\} = \{\emptyset\}$, ktorá má práve jeden prvok, a to $\emptyset$. Z množín $\emptyset$ a $\{\emptyset\}$ môžeme vytvoriť $\{\emptyset, \{\emptyset\}\}$, ktorá má dva prvky. Zaveďme teraz takéto označenie: $\emptyset = 0$, $\{\emptyset\} = 1$, $\{\emptyset, \{\emptyset\}\} = \{0, 1\} = 2$. Z týchto množín môžeme teraz vytvoriť dvojice $\{0, 1\}$ a $\{1, 2\}$ a z nich pomocou pravidla zjednotenia aj množinu $\{0, 1\} \cup \{1, 2\} = \{0, 1, 2\}$, ktoré označíme 3. Analogickým spôsobom môžeme pokračovať ďalej a postupne vytvoriť všetky prirodzené čísla tak, že položíme $n = \{1, 2, \ldots, n - 1\}$; symbol $n - 1$ znamená číslo vytvorené v bezprostredne predchádzajúcom kroku.

Všimnime si, že na vytvorenie prirozdených čísel sme potrebovali len existenciu prázdnej množiny a možnosť vytvoriť z akýchkoľvek dvoch množín $\boldsymbol{A}$ a $\boldsymbol{B}$ dve nové množiny: $\boldsymbol{A} \cup \boldsymbol{B}$ a $\{\boldsymbol{A}, \boldsymbol{B}\}$

Ako uvidíme v nasledujúcej časti, pravidlo neusporiadanej dvojice umožňuje do „amorfných“ množín uviesť štruktúru – usporiadanie, rozklad a podobne – čo má rozhodujúci význam pre matematiku i jej aplikácie.

2.2 Karteziánsky súčin

V praxi neraz potrebujeme pracovať s usporiadanými súbormi objektov. Samotný pojem množiny na opis takýchto javov nestačí, lebo množina je jednoznačne určená svojimi prvkami – bez ohľadu na ich poradie: $\{0, 1, 2\} = \{1, 2, 0\}$. Na tento účel potrebujeme pojem usporiadanej n-tice $(a_1, a_2, \ldots, a_n)$, ktorá by mala tú základnú vlastnosť, že dve usporiadané n-tice $(a_1, a_2, \ldots, a_n)$ a $(b_1, b_2, \ldots, b_n)$ sa rovnajú práve vtedy, keď pre $i = 1, 2, \ldots, n$ platí $a_i = b_i$. Teraz ukážeme, ako sa dá takýto objekt zaviesť.

Nech a a b sú množiny. Potom množinu $\{\{a, b\}, \{a\}\}$ nazývame *usporiadanou dvojicou* prvkov a a b a označujeme (a, b):

$$\{\{a, b\}, \{a\}\} =: \ (a, b)$$

Prvok a sa nazýva prvou zložkou usporiadanej dvojice (a, b) a prvok b jej druhou zložkou.

(Myšlienka vyššie uvedenej definície je táto: v množine $\{\{a, b\}, \{a\}\}$ prvok $\{a, b\}$ špecifikuje zložky usporiadanej dvojice bez poradia a prvok {a} stanovuje jej prvú zložku.)

Je ľahké vidieť, že platí:

Tvrdenie 2.3. *Dve usporiadané dvojice (a, b) a (c, d) sa rovnajú práve vtedy, keď $a = c$ a $b = d$.*

Pomocou usporiadaných dvojíc môžeme už zaviesť usporiadané trojice, štvorice atď. Stačí postupne položiť

$$\begin{aligned} (a_1, a_2, a_3) &:= (a_1, (a_2, a_3)) \\ (a_1, a_2, \ldots, a_n) &= (a_1, (a_2, a_3, \ldots, a_n)) \end{aligned}$$

A požadovaná vlastnosť, aby sa usporiadané n-tice rovnali práve vtedy, keď sa rovnajú ich odpovedajúce zložky, bude splnená.

Je dobré si uvedomiť, že nič by sa nestalo, keby sme definíciu usporiadanej trojice zaviedli trebárs takto:

$$(a_1,\ a_2,\ a_3)\ := ((a_1,\ a_2),\ a_3)$$

a podobne by sme postupovali ďalej. Požadovaná vlastnosť o rovnosti by bola opäť splnená. S podobnými situáciami sa stretávame v matematike bežne: nie je podstatné ako sa presne daný objekt definuje; podstatné je aké má definovaný objekt vlastnosti.

Pomocou pojmu usporiadanej dvojice teraz zavedieme pojem karteziánskeho súčinu dvoch množín.

Karteziánskym súčinom dvoch množín $\boldsymbol{A}$ a $\boldsymbol{B}$ nazveme množinu

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

Keďže $(x,\ y) \in \mathcal{P}(\mathcal{P}(\boldsymbol{A} \cup \boldsymbol{B}))$, máme $\boldsymbol{A} \times \boldsymbol{B} \subseteq \mathcal{P}(\mathcal{P}(\boldsymbol{A} \cup \boldsymbol{B}))$, čo zaručuje existenciu karteziánskeho súčinu na základe nám už známych konštrukčných princípov.

Ak $\boldsymbol{A} = \{a_1,\ a_2,\ \ldots,\ a_n\}$ a $\boldsymbol{B} = \{b_1,\ b_2,\ \ldots,\ b_n\}$, tak karteziánsky súčin môžeme reprezentovať obdĺžnikovou tabuľkou (maticou), ktorej riadky sú označené prvkami množiny $\boldsymbol{A}$, stĺpce prvkami množiny $\boldsymbol{B}$, pričom na priesčeníku i-teho riadku a j-teho stĺpca je umiestnený prvok $(a_i,\ b_j)$.

	b_1	b_2	$\ldots$	b_j	$\ldots$	b_n
a_1				$\vdots$		
a_2				$\vdots$		
$\vdots$				$\vdots$		
a_i	$\ldots$	$\ldots$	$\ldots$	(a_i, b_j)		
$\vdots$						
a_m						

Definíciu karteziánskeho súčinu môžeme ľahko rozšíriť na prípad n množín:

$$\boldsymbol{A}_1 \times \boldsymbol{A}_2 \times \cdots \times \boldsymbol{A}_n = \{(x_1,\ x_2, \ldots,\ x_n);\ \ x_i \in \boldsymbol{A}_i, \quad i = 1,\ 2,\ \ldots,\ n\}.$$

Uveďme teraz niektoré elementárne vlastnosti karteziánskeho súčinu. V prvom rade si všimnime, že karteziánsky súčin nie je komutatívny (môže sa stať, že $\boldsymbol{A} \times \boldsymbol{B} \neq \boldsymbol{B} \times \boldsymbol{A}$; kedy?) ani asociatívny (môže sa stať, že $(\boldsymbol{A} \times \boldsymbol{B}) \times \boldsymbol{C} \neq \boldsymbol{A} \times (\boldsymbol{B} \times \boldsymbol{C})$). Okrem toho platí

Tvrdenie 2.4. *Nech* $\boldsymbol{A}$, $\boldsymbol{B}$ *a* $\boldsymbol{C}$ *sú ľubovoľné množiny. Potom:*

(a) $\boldsymbol{A} \times \boldsymbol{B} \neq \emptyset$ *práve vtedy, keď* $\boldsymbol{A} \neq \emptyset$ *aj* $\boldsymbol{B} \neq \emptyset$.

(b) *Ak* $\boldsymbol{A} \times \boldsymbol{B} \neq \emptyset$ *a* $\boldsymbol{A} \times \boldsymbol{B} = \boldsymbol{C} \times \boldsymbol{D}$, *tak* $\boldsymbol{A} = \boldsymbol{C}$ *a* $\boldsymbol{B} = \boldsymbol{D}$.

(c) *Ak* $\boldsymbol{C} \neq \emptyset$ *a* $\boldsymbol{A} \times \boldsymbol{C} = \boldsymbol{B} \times \boldsymbol{C}$, *tak* $\boldsymbol{A} = \boldsymbol{B}$.

(d) *Ak* $\boldsymbol{A} \subseteq \boldsymbol{B}$, *tak* $\boldsymbol{A} \times \boldsymbol{C} \subseteq \boldsymbol{B} \times \boldsymbol{C}$.

(e) $(\boldsymbol{A} \cap \boldsymbol{B}) \times \boldsymbol{C} = (\boldsymbol{A} \times \boldsymbol{C}) \cap (\boldsymbol{B} \times \boldsymbol{C})$, $(\boldsymbol{A} \cup \boldsymbol{B}) \times \boldsymbol{C} = (\boldsymbol{A} \times \boldsymbol{C}) \cup (\boldsymbol{B} \times \boldsymbol{C})$.

(f) $(\boldsymbol{A} - \boldsymbol{B}) \times \boldsymbol{C} = (\boldsymbol{A} \times \boldsymbol{C}) - (\boldsymbol{B} \times \boldsymbol{C})$.

Dôkaz. Platnosť tvrdení (a) – (c) vyplýva priamo z definícií. Na ukážku urobíme dôkaz časti (f).

$$
\begin{aligned}
(x,\ y) \in (\boldsymbol{A} \times \boldsymbol{C}) - (\boldsymbol{B} \times \boldsymbol{C}) &\equiv [(x,\ y) \in \boldsymbol{A} \times \boldsymbol{C}] \wedge [\neg((x,\ y) \in \boldsymbol{B} \times \boldsymbol{C})] \equiv \\
&\equiv [(x \in \boldsymbol{A}) \wedge (y \in \boldsymbol{C})] \wedge \neg[(x \in \boldsymbol{B}) \wedge (y \in \boldsymbol{C})] \\
&\equiv [(x \in \boldsymbol{A}) \wedge (y \in \boldsymbol{C})] \wedge [\neg(x \in \boldsymbol{B}) \vee \neg(y \in \boldsymbol{C})] \equiv \\
&\equiv [(x \in \boldsymbol{A}) \wedge (y \in \boldsymbol{C}) \wedge \neg(x \in \boldsymbol{B})] \vee \\
&\vee [(x \in \boldsymbol{A}) \wedge (y \in \boldsymbol{C}) \wedge \neg(y \in \boldsymbol{C})] \equiv \\
&\equiv [(x \in \boldsymbol{A}) \wedge (x \in \boldsymbol{B}^c) \wedge (y \in \boldsymbol{C})] \equiv \\
&\equiv [(x \in \boldsymbol{A} - \boldsymbol{B}) \wedge (y \in \boldsymbol{C})] \equiv \\
&\equiv (x,\ y) \in (\boldsymbol{A} - \boldsymbol{B}) \times \boldsymbol{C}
\end{aligned}
$$

□

2.3 Binárne relácie

Medzi prvkami dvoch množín $\boldsymbol{A}$ a $\boldsymbol{B}$ môže existovať istý vzťah. Formálnym spôsobom takýto vzťah opisujeme pomocou pojmu binárna relácia.

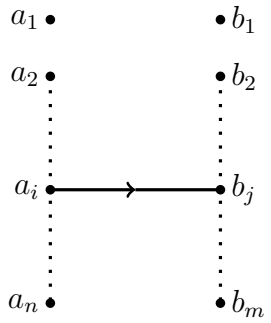
Binárna relácia z množiny $\boldsymbol{A}$ do množiny $\boldsymbol{B}$ je ľubovoľná podmnožina R karteziánskeho súčinu $\boldsymbol{A} \times \boldsymbol{B}$. Skutočnosť, že $(a, b) \in R$, v tomto kontexte spravidla zapisujeme aRb. Množinu $\boldsymbol{A}$ nazývame *oborom* a množinu $\boldsymbol{B}$ *kooborom* relácie R. Ak $a = b$, hovoríme, že R je *binárna relácia na množine* $\boldsymbol{A}$.

Analogicky definujeme aj *n-árnu reláciu* medzi množinami $\boldsymbol{A}_1,\ \boldsymbol{A}_2,\ \ldots,\ \boldsymbol{A}_n$, ako ľubovoľnú podmnožinu $R \subseteq \boldsymbol{A}_1 \times \boldsymbol{A}_1 \times \ldots \times \boldsymbol{A}_1$; 2-árna relácia je teda to isté ako binárna relácia.

Ak $\boldsymbol{A} = \{a_1,\ a_2, \ldots, a_m\}$ a $\boldsymbol{B} = \{b_1,\ b_2, \ldots, b_n\}$, tak binárnu reláciu medzi $\boldsymbol{A}$ a $\boldsymbol{B}$ môžeme reprezentovať maticou $m \times n$, kde riadky sú označené prvkami množiny $\boldsymbol{A}$, stĺpce prvkami množiny $\boldsymbol{B}$, pričom na priesečníku i-teho riadku a j-teho stĺpca je umiestnene číslo $\chi_R(i,\ j)$ (indikátor), také, že

$$\chi_R(i,\ j) = \begin{cases} 1, & \text{ak } (a_i, b_j) \in R \\ 0, & \text{ak } (a_i, b_j) \notin R \end{cases} \tag{2.1}$$

Ďalšou, veľmi názornou, reprezentáciou bineárnej relácie je reprezentácia pomocou grafu. Prvky množín $\boldsymbol{A}$ aj $\boldsymbol{B}$ znázorníme bodmi (malými krúžkami) v rovine, pričom body odpovedajúce množine $\boldsymbol{A}$ umiestnime do jedného stĺpca a body odpovedajúce množine $\boldsymbol{B}$ do druhého stĺpca. Od prvku a_i vedieme šípku k prvku b_j práve vtedy, keď $a_i\ R\ b_i$. Binárnej relácii takto zodpovedá systém bodov (ktoré nazývame *vrcholy*) a šípok (nazývaných *orientované hrany*) – *orientovaný graf*, nazývame tiež *grafom binárnej relácie*.



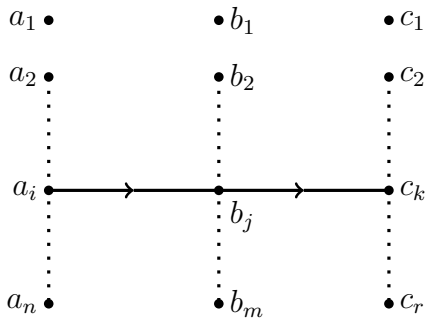
Binárne relácie sa dajú istým spôsobom kombinovať – skladať. Pojem kompozície (alebo skladania) relácií je podstatný pre pochopenie ich úlohy v matematike i v jej aplikáciách.

Nech R je binárna relácia z množiny $\boldsymbol{A}$ do množiny $\boldsymbol{B}$ a nech S je binárna relácia z množiny $\boldsymbol{B}$ do množiny $\boldsymbol{C}$. Potom môžeme vytvoriť novú reláciu RS z množiny $\boldsymbol{A}$ do množiny $\boldsymbol{C}$, ktorá je definovaná takto:

$$RS = \{(x, y) \in \boldsymbol{A} \times \boldsymbol{C};\ \text{existuje prvok } b \in \boldsymbol{B} \text{ taký, že } xRb \text{ a zároveň } bSy\}$$

Relácia RS sa nazýva *kompozícia* relácie R a relácie S (v tomto poradí) a niekedy sa označuje aj $S \circ R$.

Pozrime sa teraz na nasledujúci neformálny príklad.



Príklad 2.2. Nech $\boldsymbol{A}$ je množina všetkých obyvateľov Slovenska, ktorí majú priezvisko Kováč. Skúmajme dve relácie R a S na množine $\boldsymbol{A}$; to znamená $R, S \subseteq \boldsymbol{A} \times \boldsymbol{A}$. Nech aRb označuje, že Kováč b je synom Kováča a. Nech xSy znamená, že Kováč x je bratom Kováča y. Ak nastáva situácia, že aSb a bRc, zisťujeme, že Kováč c je synovcom Kováča a. Túto skutočnosť môžeme celkom prirodzene zapísať ako $aSRb$. To znamená, že SR je relácia „byť synovcom“. Ak však aRb a bSc, vidíme, že c je synom Kováča a. Inak povedané, ak pripustíme, že každý je sám svojím bratom, tak relácia RS je totožná s reláciou R. Záverom tohto príkladu môžeme povedať, že pomocou skladania relácií môžeme skúmať rozličné zaujímavé vzťahy, a že poradie v akom relácie skladáme je podstatné.

Kompozíciu binárnych relácií si ľahko môžeme názorne reprezentovať pomocou grafov relácií. Zoberieme graf relácie $R \subseteq \boldsymbol{A} \times \boldsymbol{B}$ a relácie $S \subseteq \boldsymbol{B} \times \boldsymbol{C}$, pričom množinu $\boldsymbol{B}$ reprezentujeme len raz – medzi množinami $\boldsymbol{A}$ a $\boldsymbol{C}$ (pozri obrázok2.3). Potom $aRSc$ práve vtedy, keď existuje postupnosť dvoch súhlasne orientovaných šípok vedúca z $\boldsymbol{A}$ do $\boldsymbol{C}$.

Relácie môžeme skladať aj opakovane.

Ak $R \subseteq \boldsymbol{A} \times \boldsymbol{B}$, $S \subseteq \boldsymbol{B} \times \boldsymbol{C}$ a $T \subseteq \boldsymbol{C} \times \boldsymbol{D}$, môžeme vytvoriť binárne operácie $(RS)T \times \boldsymbol{A} \times \boldsymbol{B}$ a $R(ST) \times \boldsymbol{A} \times \boldsymbol{D}$. Ukážeme, že tieto dve relácie sa vždy rovnajú – inými slovami: skladanie binárnych relácií je asociatívne. To nám pri skladaní binárnych relácií umožňuje vynechať zátvorky.

Tvrdenie 2.5. *Nech $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$ a $\boldsymbol{D}$ sú množiny a nech $R \subseteq \boldsymbol{A} \times \boldsymbol{B}, S \subseteq \boldsymbol{B} \times \boldsymbol{C}$ a $T \subseteq \boldsymbol{C} \times \boldsymbol{D}$ sú binárne relácie. Potom $(RS)T = R(ST)$.*

Dôkaz. Máme ukázať, že každá usporiadaná dvojica $(a,\ d)$, $a \in \boldsymbol{A}$, $d \in \boldsymbol{D}$, ktorá patrí do $(RS)T$, patrí aj do $R(ST)$ a obrátene: ak $(a, d) \in (RS)T$,

existuje $c \in \boldsymbol{C}$ také, že $(a,\ c) \in R \wedge (b, c) \in S \wedge (c,\ d) \in T$. Ale potom aj $(a,\ b) \in R \wedge (b,\ d) \in ST$ a $(a, d) \in R(ST)$ (Pozri obrázok 2.1). □

Opačné tvrdenie dokazujeme analogicky.

2.4 Ekvivalencie a rozklady

V tomto a nasledujúcom článku sa budeme venovať binárnym reláciam so špeciálnymi vlastnosťami a to takými, ktoré sa najčastejšie vyskytujú v rôzných aplikáciách.

Nech $\boldsymbol{A}$ je množina a $R \subseteq \boldsymbol{A} \times \boldsymbol{A}$ nech je binárna relácia na $\boldsymbol{A}$. Reláciu R nazveme

(a) *reflexívnou*, ak pre každý prvok $a \in \boldsymbol{A}$ platí aRa;

(b) *symetrickou*, ak zo vzťahu aRb vyplýa vždy bRa;

(c) *tranzitívnou*, ak zo vzťahov aRb a bRc vyplýa vždy aRc.

Nech $\mathrm{id}_{\boldsymbol{A}} = \{(a, a);\ a \in \boldsymbol{A}\} \subseteq \boldsymbol{A} \times \boldsymbol{A}$ označuje *identickú reláciu* a pre ľubovoľnú reláciu R nech R^- označuje binárnu reláciu $\{(b, a);\ (a, b) \in R\}$ – reláciu opačnú k R. Potom ľahko nahliadneme, že relácia R je reflexívna práve vtedy, keď $\mathrm{id}_{\boldsymbol{A}} \subseteq R$; je symetrická práve vtedy, keď $R^- \subseteq R$; a je tranzitívna práve vtedy, keď $R \circ R \subseteq R$.

Ak R je ľubovoľná relácia, $R \cup \mathrm{id}_{\boldsymbol{A}}$ je reflexívna relácia. Z ľubovoľnej relácie R je možné vyhotoviť aj symetrickú či tranzitívnu reláciu: relácia $R^{\pm} = R \cup R^-$ sa nazýva *symetrizáciou* relácie R a relácia $R^* = R \cup R^2 \cup R^3 \cup \cdots = \bigcup_{k \geq 0} R^k$, kde $R^k = R \circ R \circ \cdots \circ R$ (k-krát) sa nazýva *tranzitívnym uzáverom* relácie R. Symetrizácia relácie R je najmenšia symetrická relácia obsahujúca reláciu R. Podobne tranzitívny uzáver relácie R je najmenšia tranzitívna. relácia obsahujúca reláciu R. To znamená, že ak S je symetrická relácia obsahujúca R, tak $R^{\pm} \subseteq S$. Podobne ak S je tranzitívna relácia obsahujúca R, tak $(R^* \subseteq S)$.

Relácia, ktorá je reflexívna, symetrická a tranzitívna sa nazýva *reláciou ekvivalencie* alebo jednoducho *ekvivalenciou*. Ak R je relácia a xRy, tak hovoríme, že prvky x a y sú ekvivalentné (vzhľadom na reláciu R).

Význam tohto typu relácie spočíva v tom, že predstavuje zovšeobecnenie rovnosti, akúsi rovnosť so „zmenenou rozlišovacou schopnosťou“. Všimnite si,

že $\mathrm{id}_{\boldsymbol{A}}$ je relácia ekvivalencie a že $a\,\mathrm{id}_{\boldsymbol{A}}\,b$ práve vtedy, keď $a = b$. Teda $\mathrm{id}_{\boldsymbol{A}}$ je vlastne reláciou rovnosti. Na označenie relácií ekvivalencie sa často používajú symboly pripomínajúce rovnosť: $\cong, \simeq, \equiv, \doteq, \approx, \asymp$ a podobne. Typické relácie ekvivalencie sú relácie, v ktorých dva prvky sú ekvivalentné práve vtedy, keď majú nejakú (špecifickú) rovnakú vlastnosť. Napríklad pre dve celé čísla x a y položíme $x \equiv y$ práve vtedy, keď x a y dávajú *rovnaký* zvyšok po delení daným prirodzeným číslom k. Menej formálne príklady:

Príklad 2.3. v množine všetkých občanov Slovenskej republiky je relácia ekvivalencie „mať rovnaký dátum narodenia“ alebo relácia „mať rovnaké číslo občianskeho preukazu bez ohľadu na sériu“ a podobne.)

Pojem relácie ekvivalencie veľmi úzko súvisí s pojmom rozkladu množiny. Rozklad množiny $\boldsymbol{A}$ je – voľne povedané – opačný proces ako vytvorenie množiny $\cup\boldsymbol{A}$. Systém množín $\mathcal{S} \subseteq \mathcal{P}(\boldsymbol{A})$ sa nazýva *rozklad množiny* $\boldsymbol{A}$, ak

(a) pre každý prvok $X \in \mathcal{S}$ platí $X \neq \emptyset$;

(b) pre ľubovoľné dva rôzne prvky $X \neq Y$ platí $X \cap Y = \emptyset$;

(c) zjednotenie všetkých prvkov systému $\mathcal{S}$ je $\boldsymbol{A}$, čiže $\bigcup \mathcal{S} = \{x \in \boldsymbol{A};\, \exists Y \in \mathcal{S} : x \in Y\} = \boldsymbol{A}$.

(Inými slovami – množina $\boldsymbol{A}$ je rozkladom množiny $\cup\boldsymbol{A}$ vo všeobecnosti len vtedy, keď $\emptyset \notin \boldsymbol{A}$. Teda $\boldsymbol{A} - \{\emptyset\}$ je rozkladom množiny $\cup\boldsymbol{A}$ vždy.) Špeciálne, ak $\mathcal{S} = \{\boldsymbol{A}_1, \boldsymbol{A}_2, \ldots, \boldsymbol{A}_n\}$, tak $\mathcal{S}$ je rozklad množiny $\boldsymbol{A}$, ak každá množina $\boldsymbol{A}_i$ je neprázdna, $\boldsymbol{A}_i \cap \boldsymbol{A}_j = \emptyset$ pre každé $i \neq j$ a $\boldsymbol{A}_1 \cup \boldsymbol{A}_2 \cup \cdots \cup \boldsymbol{A}_n = \boldsymbol{A}$.

Všimnime si, že z rozkladu $\mathcal{S} = \{\boldsymbol{A}_1, \boldsymbol{A}_2, \ldots, \boldsymbol{A}_n\}$ množiny $\boldsymbol{A}$ môžeme ľahko vytvoriť reláciu ekvivalencie $R_{\mathcal{S}}$ na $\boldsymbol{A}$ takto: dva prvky x a y množiny $\boldsymbol{A}$ budú ekvivalentné vtedy, keď patria do toho istého „rozkladanca“ $\boldsymbol{A}_i$. Na druhej strane môžeme pomocou akejkoľvek relácie ekvivalencie na množine $\boldsymbol{A}$ definovať rozklad množiny $\boldsymbol{A}$. Stačí pre prvok $x \in \boldsymbol{A}$ položiť

$$R[x] = \{y \in \boldsymbol{A} :\ yRx\}$$

a systém $\{R[x] :\ x \in \boldsymbol{A}\}$ bude tvoriť rozklad množiny $\boldsymbol{A}$. O tom sa presvedčíme v dôkaze nasledujúcej teorémy, ktorá ukazuje, že pojem rozkladu množiny $\boldsymbol{A}$ a pojem ekvivalencie na množine $\boldsymbol{A}$ sú dve strany tej istej mince.

Tvrdenie 2.6. *Nech $\mathcal{S}$ je rozklad množiny $\boldsymbol{A}$. Nech $R_{\mathcal{S}}$ je binárna relácia na $\boldsymbol{A}$ daná predpisom $aR_{\mathcal{S}}b$ práve vtedy, keď existuje množina $X \in \mathcal{S}$ taká,*

že $a \in X$ aj $b \in X$. Potom $R_{\mathcal{S}}$ je relácia ekvivalencie. Obrátene, ak binárna relácia $\boldsymbol{S}$ je ekvivalenciou na množine $\boldsymbol{A}$, tak systém

$$\mathcal{T}_{\boldsymbol{S}} = \{\boldsymbol{S}[x];\ x \in \boldsymbol{A}\}$$

je rozklad množiny $\boldsymbol{A}$. Naviac platí, že $\mathcal{T}_{(R_{\mathcal{S}})} = \mathcal{S}$ a $R_{(\mathcal{T}_{\boldsymbol{S}})} = \boldsymbol{S}$.

Dôkaz. Je ľahké priamo overiť, že relácia $R_{\mathcal{S}}$ je reflexívna, symetrická a tranzitívna. Aby sme ukázali, že systém $\mathcal{T}_{\boldsymbol{S}}$ je rozklad množiny $\boldsymbol{A}$ najprv overíme, že ľubovoľné dve množiny $\boldsymbol{S}[x]$ a $\boldsymbol{S}[y]$ sú buďto totožné alebo disjunktné. Ak $x\boldsymbol{S}y$, tak ľahko preveríme, že $\boldsymbol{S}[x] = \boldsymbol{S}[y]$. Naozaj ak $q \in \boldsymbol{S}[x]$, tak $q\boldsymbol{S}x$. Súčasne máme $x\boldsymbol{S}y$, takže z tranzitívnosti dostávame $q\boldsymbol{S}y$. To znamená, že $q \in \boldsymbol{S}[y]$. Keďže q bol ľubovoľný prvok množiny $\boldsymbol{S}[x]$, z uvedeného vyplýva $\boldsymbol{S}[x] \subseteq \boldsymbol{S}[y]$. Obrátená inklúzia sa dokáže analogicky. Preto $\boldsymbol{S}[x] = \boldsymbol{S}[y]$. Nech teraz $\boldsymbol{S}[x] \cap \boldsymbol{S}[y] \neq \emptyset$. Potom existuje prvok $z \in \boldsymbol{A}$ taký, že $z \in \boldsymbol{S}[x]$ a zároveň $z \in \boldsymbol{S}[y]$. Zo vzťahu $z \in \boldsymbol{S}[x]$ dostávame $z\boldsymbol{S}x$ a podobne zo vzťahu $z \in \boldsymbol{S}[y]$ dostávame, že $z \in \boldsymbol{S}y$ a teda (so symetrie relácie $\boldsymbol{S}$) aj $y \in \boldsymbol{S}[z]$. No teraz máme $y \in \boldsymbol{S}z$ a súčasne $z\boldsymbol{S}x$, takže z tranzitívnosti vyplýva $y \in \boldsymbol{S}[x]$. To však znamená $\boldsymbol{S}[y] = \boldsymbol{S}[x]$. Tým sme dokázali, že ak $\boldsymbol{S}[y] \neq \boldsymbol{S}[x]$, tak $\boldsymbol{S}[x] \cap \boldsymbol{S}[y] = \emptyset$. Napokon si uvedomme, že $x \in \boldsymbol{S}[x]$ na základe reflexívnosti, čo znamená, že $\boldsymbol{A} \subseteq \cup_{x \in \boldsymbol{A}} \boldsymbol{S}[x]$. Teda systém $\mathcal{T}_{\boldsymbol{S}}$ naozaj tvorí rozklad množiny $\boldsymbol{A}$.

Zvyšok dôkazu je ľahký: ak vyjdeme z rozkladu $\mathcal{S}$, skonštruujeme ekvivalenciu $R_{\mathcal{S}}$ a ňou indukujeme rozklad množiny $\boldsymbol{A}$, dostaneme očividne pôvodný rozklad $\mathcal{S}$. To je vyjadrené rovnosťou $\mathcal{T}_{(R_{\mathcal{S}})} = \mathcal{S}$. Ak vyjdeme z ekvivalencie $\boldsymbol{S}$, skonštruujeme rozklad $\mathcal{T}_{\boldsymbol{S}}$ a z toho rozkladu odvodíme reláciu ekvivalencie, dostávame opäť $\boldsymbol{S}$ – to je druhá rovnosť $R_{(\mathcal{T}_{\boldsymbol{S}})} = \boldsymbol{S}$. □

2.5 Usporiadania

Ďalším typom binárnej relácie na množine, ktorým sa budeme podrobnejšie zaoberať je relácia usporiadania. Tá nám umožňuje zoradiť prvky a určiť, či daný prvok je „predchodcom“ iného alebo nie.

Usporiadaním na množine $\boldsymbol{A}$ rozumieme ľubovoľnú binárnu reláciu, ktorá je reflexívna, tranzitívna a *antisymetrická*. Posledná vlastnosť znamená, že ak usporiadané dvojice (x, y) aj (y, x) sú súčasne v relácii, tak potom $x = y$. Reláciu usporiadania značíme obyčajne symbolom $\leq$ alebo jeho variantmi $\leqq, \subseteq, \preceq, \lesssim$ a podobne. Pre reláciu usporiadania $\leq$ na $\boldsymbol{A}$ teda platí:

(a) $x \leq x$ pre každý prvok $x \in \boldsymbol{A}$ (reflexívnosť);

(b) ak $x \leq y$ a $y \leq z$, tak $x \leq z$ pre všetky $x, y, z \in \boldsymbol{A}$ (tranzitívnosť);

(c) ak $x \leq y$ a $y \leq x$, tak $x = y$ pre všetky $x, y \in \boldsymbol{A}$ (antisymetria).

Zápis $x \leq y$ obyčajne čítame „x predchádza y“.

Usporiadaná dvojica $(\boldsymbol{A}, \leq)$, kde $\leq$ je relácia usporiadania na $\boldsymbol{A}$ sa nazýva *usporiadaná množina*. Samotná množina $\boldsymbol{A}$ sa v tejto súvislosti nazýva jej *nosičom*. Poznamenajme, že ak R je relácia usporiadania, aj R^- je reláciou usporiadania. Reláciu $(\leq)^-$ zapisujeme $\geq$. Okrem toho píšeme $x < y$, ak $x \leq y$ a $x \neq y$. Analogický význam majú aj symboly $\subset, \prec$ a podobne. Relácia $<$ však nie je reláciou usporiadania vo vyššie uvedenom zmysle, lebo nie je reflexívna. Niekedy sa takejto relácii hovorí relácia *ostrého usporiadania*.

Príklad 2.4. Potenčná množina $\mathcal{P}(\boldsymbol{A})$ je usporiadaná reláciou inklúzie $\subseteq$. Všimnime si, že v $(\mathcal{P}(\boldsymbol{A}), \subseteq)$ sa môžu nájsť dvojice prvkov $\boldsymbol{X}$ a $\boldsymbol{Y}$ také, že ani $\boldsymbol{X} \subseteq \boldsymbol{Y}$, ani $\boldsymbol{Y} \subseteq \boldsymbol{X}$. Napríklad v $\mathcal{P}(\{1,2,3\})$ sa to stane pre $\boldsymbol{X} = \{1,2\}$ a $\boldsymbol{Y} = \{2,3\}$. Inak povedané, tieto dva prvky nie sú porovnateľné. V usporiadanej množine $(\boldsymbol{A}, \leq)$ teda hovoríme , že x a y sú *porovnateľné* ak $x \leq y$ alebo $y \leq x$ a *neporovnateľné* v opačnom prípade.

Príklad 2.5. Číselné množiny $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ a $\mathbb{R}$ sú množiny usporiadané bežnou reláciou usporiadania podľa veľkosti. Ak sa vrátime k definícii prirodzeného čísla, pri ktorej 0 je totožná s prázdnou množinou a číslo n je totožné s množinou všetkých predchádzajúcich prirodzených čísel (čize $n = \{0, 1, \ldots, n-1\}$), tak vidíme, že nerovnosť prirodzených čísel $m \leq n$ je totožná s inklúziou $m \subseteq n$ chápanou ako medzi množinami. Zároveň však $m < n$ práve vtedy, keď $m \in n$.

Príklad 2.6. Nech $\boldsymbol{A} = \{0,1\} \times \{0,1\} \times \ldots \times \{0,1\} = \{0,1\}^n$. Pre dve usporiadané n-tice $x = (x_1, x_2, \ldots, x_n)$ a $y = (y_1, y_2, \ldots, y_n)$ položíme $x \leq y$ ak $x_i \leq y_i$ pre každé $i = 1, 2, \ldots, n$. Pritom berieme na množine $\{0,1\}$ prirodzené usporiadanie $0 \leq 1$. Napríklad $(0,0,1,1,0,1) \leq (0,1,1,1,0,1)$. Ľahko sa ukáže, že $(\{0,1\}^n, \leq)$ je usporiadaná množina. Aj tu ľahko nájdeme dvojice neporovnateľných prvkov. Tento príklad sa dá ľahko zovšeobecniť. Ak $(\boldsymbol{A}_1, \leq_1), (\boldsymbol{A}_2, \leq_2), \ldots, (\boldsymbol{A}_n, \leq_n)$ sú usporiadané množiny, na ich karteziánskom súčine $\boldsymbol{A} = \boldsymbol{A}_1 \times \boldsymbol{A}_2 \times \ldots \times \boldsymbol{A}_n$ môžeme definovať *súčinové usporiadanie* $\leq$ predpisom $(a_1, a_2, \ldots, a_n) \leq (b_1, b_2, \ldots, b_n)$ ak $a_i \leq_i b_i$ pre každé $i = 1, 2, \ldots, n$.

Ak v usporiadanej množine $(\boldsymbol{A}, \leq)$ neexistujú neporovnateľné dvojice prvkov, tak potom v $\boldsymbol{A}$ platí:

(d) pre každé $x \in \boldsymbol{A}$, $z \in \boldsymbol{A}$ buďto $x \leq z$ alebo $z \leq x$.

Tejto vlastnosti sa hovorí dichotómia. Usporiadaná množina $\boldsymbol{A}$ s vlastnosťou dichotómie sa nazýva *úplne usporiadaná*, no používajú sa tiež termíny *lineárne* či *totálne usporiadaná* množina. Ak chceme zdôrazniť, že množina $(\boldsymbol{A}, \leq)$ nie je úplne usporiadaná, hovoríme, že je *čiastočne usporiadaná*. Typickými príkladmi úplne usporiadaných množín sú číselné množiny $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.

Teraz si ukážeme jeden významný príklad úplného usporiadania, ktorému hovoríme *lexikologické usporiadanie* a s ktorým sa bežne stretávame v slovníkoch. Nech $(\boldsymbol{A}, \leq)$ je úplne usporiadaná množina. Na množinu $\boldsymbol{A}$ sa budeme dívať ako na *abecedu* (je dané poradie znakov). Utvorme teraz všetky karteziánske mocniny $\boldsymbol{A}^n = \boldsymbol{A} \times \boldsymbol{A} \times \ldots \times \boldsymbol{A}$ (n-krát) vrátane $\boldsymbol{A}^0 = \{\emptyset\}$ a z nich ďalej vytvorme množinu $\boldsymbol{A}^* = \cup_{i \geq 0} \boldsymbol{A}^i$. Prvky množiny $\boldsymbol{A}^n$ budeme nazývať *slová dĺžky* n. Slovo dĺžky 0 sa nazýva *prázdne slovo*. Množina $\boldsymbol{A}^*$ je *množina všetkých slov* nad abecedou $\boldsymbol{A}$. Na $\boldsymbol{A}^*$ zavedieme úplné usporiadanie $\leq_L$, ktoré nazývame *lexikologickým usporiadaním*, a to takto: $\boldsymbol{x} = (x_1, x_2, \ldots, x_m) \leq (y_1, y_2, \ldots, y_n) = \boldsymbol{y}$ ak je splnená niektorá z nasledujúcich podmienok:

(1) existuje index i taký, že $x_i < y_i$ a súčasne $x_j = y_j$ pre všetky indexy j také, že $1 \leq j < i$. (Inými slovami – slová x a y majú zhodný začiatočný úsek až po index $i-1$ a na i-tom mieste nastáva „správna“ ostrá nerovnosť.)

(2) $m \leq n$ a zároveň $x_i = y_i$ pre $i = 1, 2, \ldots, m$. (To znamená, že slovo x je *podslovom* slova y.)

Tieto podmienky zabezpečujú, že v $\{0,1\}^*$ platí $(0,0) \leq (0,0,1)$ (podľa podmienky (2)) a „palica“ $\leq$ „polica“ v Slovníku slovenského jazyka (podľa pravidla (1), lebo $a \leq o$).

Podľa podmienky (2) prázdne slovo $\emptyset$ predchádza všetky ostatné slová, je teda *prvým*, či *najmenším* prvkom množiny $\boldsymbol{A}^*$. Túto terminológiu podrobnejšie rozvedieme.

Nech $(\boldsymbol{A}, \leq)$ je ľubovoľná usporiadaná množina. Prvok $x \in \boldsymbol{A}$ nazveme *minimálnym*, ak pre každý prvok y, pre ktorý $y \leq x$, platí $y = x$ (t.j. od prvku x neexistuje menší). Analogicky definujeme *maximálny* prvok (stačí použiť $\geq$ namiesto $\leq$). Prvok $x \in \boldsymbol{A}$ nazveme *najmenším* prvkom, ak pre všetky $y \in \boldsymbol{A}$ platí $x \leq y$. Analogicky definujeme *najväčší* prvok.

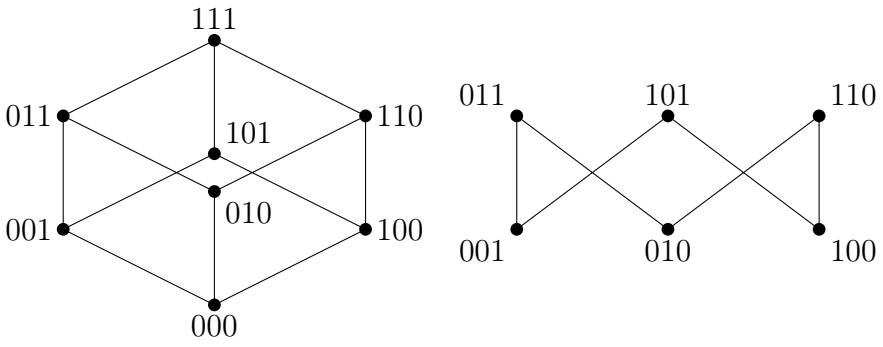
Všimnime si, že množina $(\boldsymbol{A}, \leq)$ môže mať najviac jeden najmenší prvok, a ak ho má, musí byť porovnateľný so všetkými ostatnými prvkami. Naproti tomu množina $(\boldsymbol{A}, \leq)$ môže mať niekoľko minimálnych prvkov – tie však budú navzájom neporovnateľné. Najmenší prvok usporiadanej množiny, ak existuje, je jeho jediným minimálnym prvkom.

Skonštruujeme prípad usporiadanej množiny, ktorá má veľa minimálnych a maximálnych prvkov. Na to použijeme všeobecnú konštrukciu indukovaného usporiadania. Nech $(\boldsymbol{A}, \leq)$ je usporiadaná množina a nech $\boldsymbol{B} \subseteq \boldsymbol{A}$. položme $\leq_{\boldsymbol{B}} =: \leq \cap(\boldsymbol{B} \times \boldsymbol{B})$. To znamená, že pre dva prvky $b, c \in \boldsymbol{B}$ platí $b \leq_{\boldsymbol{B}} c$ práve vtedy, keď $b \leq c$.

Ľahko sa overí, že $\leq_{\boldsymbol{B}}$ je usporiadanie na $\boldsymbol{B}$; naviac, ak $\leq$ je úplné usporiadanie na $\boldsymbol{A}$, tak $\leq_{\boldsymbol{B}}$ je úpné usporiadanie na $\boldsymbol{B}$. Usporiadanie $\leq_{\boldsymbol{B}}$ sa nazýva *indukovaným usporiadaním*. Niekedy tiež hovoríme, že usporiadanie $\leq_{\boldsymbol{B}}$ množiny $\boldsymbol{B}$ je *zúžením* usporiadania $\leq$ množiny $\boldsymbol{A}$.

Ako príklad zoberme usporiadanú množinu $\boldsymbol{A} = \{0,1\}^n$ so súčinovým usporiadaním zavedeným vyššie. Táto množina má najmenší prvok $\mathbf{0} = (0, 0, \ldots, 0)$ a najväčší prvok $\mathbf{1} = (1, 1, \ldots, 1)$ a pritom je čiastočne usporiadaná. Zoberme teraz množinu $\boldsymbol{B} = \{0,1\}^n - \{\mathbf{0}, \mathbf{1}\}$ s indukovaným usporiadaním. Jej minimálne prvky sú $(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots (0, \ldots, 0, 1)$ a maximálne vzniknú z minimálnych zámenou núl a jednotiek.

Usporiadané množiny je niekedy výhodné graficky znázorniť. Nech $(\boldsymbol{A}, \leq)$ je usporiadaná množina. Nech x a y sú také dva jej prvky, že $x \leq y$, ale neexistuje $z \in \boldsymbol{A}$, pre ktoré by platilo $x \leq z \leq y$. V takom prípade hovoríme, že x *bezprostredne nasleduje* y (alebo tiež y *pokrýva* x), čo značíme symbolom $x \leq \ \cdot y$. Usporiadanej množine $(\boldsymbol{A}, \leq)$ priradíme teraz grafickú reprezentáciu nazývanú *Hasseho diagram*, takto. Prvky množiny budeme reprezentovať bodmi roviny a nazývame ich *vrcholmi* diagramu. Ak $x \leq \cdot\ y$, zakreslíme tieto body neďaleko od seba, pričom bod z umiestnime vyššie ako x (nie nevyhnutne priamo nad x). Body x a y spojíme krivkou, najlepšie úsečkou; túto spojnicu nazveme *hranou* diagramu. Ako príklad uvádzame na obrázku 1.3 Hasseho diagram usporiadanej množiny $(\{0,1\}^3, \leq)$ so súčinovým usporiadaním a množiny $(\{0,1\}^3 - \{0,1\}, \leq)$ s indukovaným usporiadaním (namiesto $(x_1, x_2, \ldots, x_n)$ tu aj v ďalšom budeme písať $x_1 x_2 \ldots x_n$).



Obr. 2.1: Hasseho diagramy

2.6 Zobrazenia

Pojem zobrazenia patrí medzi najdôležitejšie pojmy celej matematiky. Intuitívne povedané, zobrazenie je "pravidlo", podľa ktorého každému prvku jednej množiny, povedzme $\boldsymbol{A}$, jednoznačne priradíme prvok akejsi množiny, povedzme $\boldsymbol{B}$. Rôznym prvkom množiny $\boldsymbol{A}$ pritom môžeme, no nemusíme, priradiť ten istý prvok množiny $\boldsymbol{B}$. Ako jednoduchý príklad zobrazenia nám môže poslúžiť priradenie priezviska každému občanovi Slovenskej republiky.

Formálne je zobrazenie špeciálnym druhom binárnej relácie. Ak máme binárnu reláciu $R \subseteq \boldsymbol{A} \times \boldsymbol{B}$, označíme

$$\mathrm{pr}_1(R) = \{a \in \boldsymbol{A};\ \text{existuje } b \in \boldsymbol{B} \text{ také, že } (a,b) \in R\}.$$

Analogicky,

$$\mathrm{pr}_2(R) = \{b \in \boldsymbol{B};\ \text{existuje } a \in \boldsymbol{A} \text{ také, že } (a,b) \in R\}.$$

Tieto množiny *prvou projekciou* relácie R (alebo tiež *nosičom* relácie R) a *druhou projekciou* relácie R (alebo tiež *obrazom* relácie R). Reláciu $R \subseteq \boldsymbol{A} \times \boldsymbol{B}$ nazveme *všade definovanou*, ak jej nosičom je celá množina $\boldsymbol{A}$. Zaveďme ďalej takáto označenie: pre každý prvok $x \in \boldsymbol{A}$ nech $R[x] = \{y \in \boldsymbol{B};\ (x,y) \in R\}$. Túto množinu nazveme *obrazom prvku* $x \in \boldsymbol{A}$ v relácii R. Reláciu R nazveme *jednoznačnou*, ak pre každý prvok $x \in \boldsymbol{A}$ má množina $R[x]$ najviac jeden prvok.

Zobrazenie f z množiny $\boldsymbol{A}$ do množiny $\boldsymbol{B}$ je binárna relácia $f \subseteq \boldsymbol{A} \times \boldsymbol{B}$, ktorá je všade definovaná a jednoznačná. Teda pre každý prvok $a \in \boldsymbol{A}$ existuje jediný prvok $b \in \boldsymbol{B}$ taký, že afb. Tento prvok b spravidla označujeme

$f(a)$ a nazývame ho obrazom prvku a. Z druhej strany, ak $b \in \boldsymbol{B}$, tak každý prvok $a \in \boldsymbol{A}$ taký, že $b = f(a)$ sa nazýva *vzor* prvku b. Množinu $\boldsymbol{A}$ nazývame *oborom* alebo *definičným oborom* a množinu $\boldsymbol{B}$ *kooborom* alebo *oborom hodnôt* zobrazenia f (tieto pojmy sme zaviedli už pre relácie). Na vyjadrenie skutočnosti, že $f \subseteq \boldsymbol{A} \times \boldsymbol{B}$ je zobrazenie, štandardne používame označenie $f\colon \boldsymbol{A} \to \boldsymbol{B}$ alebo $\boldsymbol{A} \xrightarrow{f} \boldsymbol{B}$. (Skutočnosť, že f prvku $a \in \boldsymbol{A}$ priraďuje prvok $b \in \boldsymbol{B}$ (t.j. že $f(a) = b$), označujeme priraďovacou šípkou: $a \overset{f}{\mapsto} b$, alebo jednoducho $a \mapsto b$, na rozdiel od zobrazovacej šípky, ktorú používame na označenie samotného zobrazenia $f\colon \boldsymbol{A} \to \boldsymbol{B}$ s oborom $\boldsymbol{A}$ a kooborom $\boldsymbol{B}$.)

Ešte raz zhrňme: v zobrazení $f\colon \boldsymbol{A} \to \boldsymbol{B}$ má každý prvok $a \in \boldsymbol{A}$ jediný obraz $f(a)$, naproti tomu prvok $b \in \boldsymbol{B}$ môže mať viacero vzorov, no nemusí mať ani jeden.

Príklady zobrazení:

1. Ak $\boldsymbol{A}$ je ľubovoľná množina, tak identická relácia $\mathrm{id}_{\boldsymbol{A}}$ na množine $\boldsymbol{A}$ je zobrazením $\mathrm{id}_{\boldsymbol{A}}\colon \boldsymbol{A} \to \boldsymbol{A}$, kde $a \mapsto a$ pre každý prvok $a \in \boldsymbol{A}$.

2. Nech $\boldsymbol{A}$ a $\boldsymbol{B}$ sú množiny, pričom $\boldsymbol{B}$ je neprázdna, a nech $b \in \boldsymbol{B}$ je pevne zvolený prvok (konštanta). Potom existuje *konštantné zobrazenie* $f\colon \boldsymbol{A} \to \boldsymbol{B}$, $x \mapsto b$, ktoré každému prvku $x \in \boldsymbol{A}$ priradí prvok b.

3. $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto ax + b$, kde $a, b \in \mathbb{R}$ sú konštanty, sa nazýva *lineárne zobrazenie* (lineárna funkcia).

4. Ak $\boldsymbol{A} \times \boldsymbol{B}$ je karteziánsky súčin dvoch neprázdnych množín, tak $\pi_1\colon \boldsymbol{A} \times \boldsymbol{B} \to \boldsymbol{A}$, $(x, y) \mapsto x$ je zobrazenie, ktoré sa nazýva *projekciou* karteziánskeho súčinu na prvého činiteľa (alebo *prvou projekciou*). Analogicky definujeme *druhú projekciu* (prípadne ďalšie projekcie, ak uvažujeme karteziánsky súčin viac ako dvoch množín). Nech $\boldsymbol{A}$ je ľubovoľná množina. Zobrazenie, ktoré každému prvku $x \in \boldsymbol{A}$ priraďuje ten istý prvok, t.j. $f\colon \boldsymbol{A} \to \boldsymbol{A}$, $x \mapsto x$, sa nazýva *identickým zobrazením* a označuje sa $\mathrm{id}_{\boldsymbol{A}}$.

5. Ak $f\colon \boldsymbol{A} \to \boldsymbol{B}$ je ľubovoľné zobrazenie a $\boldsymbol{C} \subseteq \boldsymbol{A}$ tak môžeme skonštruovať *zúženie zobrazenia* f na množinu $\boldsymbol{C}$, čo je zobrazenie $f|\boldsymbol{C}\colon \boldsymbol{C} \to \boldsymbol{B}$ definované takto: $(f|\boldsymbol{C})(x) = f(x)$ pre každý prvok $x \in \boldsymbol{C}$.

6. Pomocou zobrazení môžeme opisovať aj podmnožiny nejakej množiny. Nech $\boldsymbol{U}$ je universum a $\boldsymbol{A} \subseteq \boldsymbol{U}$. Definujme zobrazenie$\chi_{\boldsymbol{A}}\colon \boldsymbol{U} \to \{0, 1\}$

takto:

$$\chi_{\boldsymbol{A}}(x) = \begin{cases} 1 & \text{ak } x \notin \boldsymbol{A}; \\ 0 & \text{pre } x \in \boldsymbol{B}. \end{cases} \tag{2.2}$$

Toto zobrazenie sa nazýva *charakteristická funkcia* množiny $\boldsymbol{A}$.

7. Ľubovoľné zobrazenie $a\colon \mathbb{N} \to \boldsymbol{X}$ množiny prirodzených čísel do množiny $\boldsymbol{X}$ sa nazýva *postupnosťou* v množine $\boldsymbol{X}$. Niekedy sa pod (konečnou) postupnosťou rozumie aj zobrazenie $b\colon \{0, 1, \ldots, n-1\} \to \boldsymbol{X}$. Pre postupnosť však používame odlišné označenie. Namiesto zápisu pomocou šípky spravidla používame zápis $a = (a_i)_{i\in\mathbb{N}} = (a_i)_{i=0}^{\infty} = (a_i)_{i\geq 0}$ alebo $b = (b_i)_{i=0}^{n-1}$. Používajú sa aj označenia $a = (a_1, a_2, \ldots)$ a $b = (b_1, b_2, \ldots, b_{n-1})$, $a = (a(i))_{i\in\mathbb{N}}$ a podobne. Konečné postupnosti $b = (b_1, b_2, \ldots, b_{n-1})$, kde $b_i \in \boldsymbol{X}$ sa tiež zvyknú nazývať *slová* nad abecedou $\boldsymbol{X}$. V tom prípade sa používa označenie $b_0 b_1 \ldots b_{n-1}$ bez zátvoriek a čiarok[1].

Podobne ako relácie môžeme skladať aj zobrazenia. Ak $f\colon \boldsymbol{A} \to \boldsymbol{B}$ a $g\colon \boldsymbol{B} \to \boldsymbol{C}$ sú zobrazenia, môžeme vytvoriť zloženú reláciu fg s oborom $\boldsymbol{A}$ a kooborom $\boldsymbol{C}$. Je ľahké presvedčiť sa o tom, že táto relácia je zobrazením. Ak $a \overset{f}{\mapsto} b$ a $b \overset{g}{\mapsto} c$, tak $a \overset{fg}{\mapsto} c$. Na rozdiel od bežných binárnych relácií, pri zobrazeniach zápis $a(fg)c$ nepoužívame. Keďže $b = f(a)$ a $c = g(b)$, máme $c = g(b) = g(f(a))$. Preto v tejto súvislosti dávame prednosť označeniu $g \circ f$ pre zložené zobrazenie, pričom správanie tohto zloženého zobrazenia je jednoznačne charakterizované vzťahom

$$g \circ f(a) = g(f(a)).$$

Tento zápis neznamená nič iné, že hodnotu zobrazenia $g \circ f\colon \boldsymbol{A} \to \boldsymbol{C}$ zistíme tak, že najprv určíme hodnotu zobrazenia $f\colon \boldsymbol{A} \to \boldsymbol{B}$ na prvku $a \in \boldsymbol{A}$ a následne hodnotu zobrazenia $g\colon \boldsymbol{B} \to \boldsymbol{C}$ na prvku $f(a) \in \boldsymbol{B}$.

Pri definícii zobrazenia sa nič nehovorilo o tom, koľko prvkov z množiny $\boldsymbol{A}$ sa môže zobraziť na ten istý prvok množiny $\boldsymbol{B}$ ani či každý prvok množiny $\boldsymbol{B}$ je obrazom nejakého prvku z množiny $\boldsymbol{A}$. Ak takéto podmienky pridáme k definícii, dostaneme dôležité typy zobrazení.

Zobrazenie $f\colon \boldsymbol{A} \to \boldsymbol{B}$ nazývame *injektívne* alebo *injekcia*, ak pre každé $a, c \in \boldsymbol{A}$ a $b \in \boldsymbol{B}$ z rovností $f(a) = b$ $f(c) = b$ vyplýva, že $a = c$. Inými

[1] Slová „zobrazenie“ a „funkcia“ používame ako synonymá. Niektorí autori však pod funkciou rozumejú zobrazenie, ktorého kooborom je nejaká číselná množina. Slovo „postupnosť“ používame aj v zmysle konečnej postupnosti.

slovami, v injekcii nemôže nastať, žeby dva rôzne prvky množiny $\boldsymbol{A}$ mali ten istý obraz.

Zobrazenie $f\colon \boldsymbol{A} \to \boldsymbol{B}$ je *surjektívne* alebo *surjekcia*, ak pre každý prvok $b \in \boldsymbol{B}$ existuje aspoň jeden prvok $a \in \boldsymbol{A}$ taký, že $f(a) = b$. Inak povedané, v surjekcii je každý prvok množiny $\boldsymbol{B}$ obrazom nejakého prvku množiny $\boldsymbol{A}$.

Zobrazenie $f\colon \boldsymbol{A} \to \boldsymbol{B}$ je *bijektívne* alebo *bijekcia*, ak je injekcia a zároveň surjekcia.

Na označenie injekcie sa tiež používa názov *prosté zobrazenie* a surjektívne zobrazenie sa tiež zvykne nazývať *zobrazením na* množinu $\boldsymbol{B}$. Bijektívne zobrazenie sa tiež nazýva *vzájomne jednoznačné*, lebo sprostredkuje vzájomne jednoznačnú korešpondenciu medzi prvkami množiny $\boldsymbol{A}$ a prvkami množiny $\boldsymbol{B}$.

Vyššie uvedené triedy zobrazení môžeme výhodne opísať pomocou pojmu inverznej relácie. Ak $R \subseteq \boldsymbol{A} \times \boldsymbol{B}$ je binárna relácia, symbolom R^- označme reláciu z množiny $\boldsymbol{B}$ do množiny $\boldsymbol{A}$ definovanú takto:

$$R^- = \{(b, a) \in \boldsymbol{B} \times \boldsymbol{A};\ (a, b) \in R\}.$$

Relácia R^- sa nazýva *inverznou reláciou* k relácii R.

Je zrejmé, že inverzná relácia k zobrazeniu nemusí byť zobrazenie. Platí však nasledujúce jednoduché tvrdenie:

Tvrdenie 2.7. *Nech $f\colon \boldsymbol{A} \to \boldsymbol{B}$ je zobrazenie. Potom:*

(a) *f je injektívne práve vtedy, keď f^- je jednoznačná relácia;*

(b) *f je surjektívne práve vtedy, keď f^- je všade definovaná relácia;*

(c) *f je bijektívne práve vtedy, keď f^- je zobrazenie.*

Ak zobrazenie $f\colon \boldsymbol{A} \to \boldsymbol{B}$ je bijektívne, tak – ako sme práve spomenuli – f^- je zobrazenie. No nielen to: f^- je dokonca bijektívne zobrazenie. Označujeme ho $f^{-1}\colon \boldsymbol{B} \to \boldsymbol{A}$ a nazývame *inverzným zobrazením* k bijekcii f.

Platí naviac takéto tvrdenie:

Tvrdenie 2.8. *Nech $f\colon \boldsymbol{A} \to \boldsymbol{B}$ a $g\colon \boldsymbol{B} \to \boldsymbol{C}$ sú zobrazenia. Potom:*

(a) ak f a g sú injekcie, tak aj $g \circ f\colon \boldsymbol{A} \to \boldsymbol{C}$ je injekcia;

(b) ak f a g sú surjekcie, tak aj $g \circ f\colon \boldsymbol{A} \to \boldsymbol{C}$ je surjekcia;

(c) ak f a g sú bijekcie, tak aj $g \circ f\colon \boldsymbol{A} \to \boldsymbol{C}$ je bijekcia.

Presvedčiť sa o tom, že zobrazenie $f\colon \boldsymbol{A} \to \boldsymbol{B}$ je bijekcia, môže byť niekedy dosť pracné. Pri riešení tohto problému býva preto vhodné nasledujúce tvrdenie.

Tvrdenie 2.9. *Zobrazenie $f\colon \boldsymbol{A} \to \boldsymbol{B}$ je bijekcia práve vtedy, keď existuje zobrazenie $g\colon \boldsymbol{B} \to \boldsymbol{A}$ také, že $g \circ f = id_{\boldsymbol{A}}$ a zároveň $f \circ g = id_{\boldsymbol{B}}$*

Dôkaz. Ak f je bijekcia, stačí položiť $g = f^{-1}$ a identity $g \circ f = id_{\boldsymbol{A}}$ a $f \circ g = id_{\boldsymbol{B}}$ sú splnené.

Obrátene, predpokladajme, že tieto identity sú splnené. Najprv ukážeme, že z prvej vyplýva, že f je injekcia. Nech $f(x) = z = f(y)$ pre nejaké $x, y \in \boldsymbol{A}$ a $z \in \boldsymbol{B}$. Potom $x = id_{\boldsymbol{A}}(x) = g \circ f(x) = g(f(x)) = g(z) = g(f(y)) = g \circ f(y) = id_{\boldsymbol{A}}(y) = y$. Naozaj, táto rovnosť znamená, že f je injekcia.

Ďalej sa presvedčíme o tom, že z druhej identity vyplýva, že f je surjekcia. Nech b je ľubovoľný prvok množiny $\boldsymbol{B}$. Keďže $f \circ g = id_{\boldsymbol{B}}$ je bijekcia, prvok $b \in \boldsymbol{B}$ má vzhľadom na zobrazenie $id_{\boldsymbol{B}}$ vzor v množine $\boldsymbol{B}$ – totiž samého seba, prvok b. Tento teraz zobrazíme do množiny $\boldsymbol{A}$ zobrazením g. Položme $g(b) = a$. Keďže $f \circ g = id_{\boldsymbol{B}}$, máme $b = id_{\boldsymbol{B}}(b) = f \circ g(b) = f(g(b)) = f(a)$. Znamená to, že k prvku $b \in \boldsymbol{B}$ sme našli prvok $a \in \boldsymbol{A}$ taký, že $f(a) = b$ – jeho vzor zvhľadom na zobrazenie f. Keďže prvok $b \in \boldsymbol{B}$ bol ľubovoľný, zisťujeme, že každý prvok množiny $\boldsymbol{B}$ má nejaký vzor vzhľadom na zobrazenie f. Inými slovami, že f je surjekcia. □

Nasledujúce tvrdenie vyjadruje vzťah medzi injekciami a surjekciami.

Tvrdenie 2.10. *Nech $\boldsymbol{A}$ a $\boldsymbol{B}$ sú neprázdne množiny. Potom injekcia $\boldsymbol{A} \to \boldsymbol{B}$ existuje práve vtedy, keď existuje surjekcia $\boldsymbol{B} \to \boldsymbol{A}$.*

Dôkaz. Nech $f\colon \boldsymbol{A} \to \boldsymbol{B}$ je injektívne zobrazenie. Z definície injektívnosti vyplýva, že pre každý prvok $y \in B$ existuje najviac jeden prvok $x \in \boldsymbol{A}$ taký, že $f(x) = y$. Zvoľme si teraz ľubovoľný pevný prvok $a^* \in \boldsymbol{A}$ a definujme zobrazenie $g\colon \boldsymbol{B} \to \boldsymbol{A}$ nasledovne. Nech $b \in \boldsymbol{B}$ je ľubovoľný prvok. Ak pre toto b existuje $a \in A$ také, že $f(a) = b$, tak položíme $g(b) = a$, inak položíme $g(b) = a^*$. Je zrejmé, že takto definované zobrazenie $g\colon \boldsymbol{B} \to \boldsymbol{A}$ je surjektívne.

Nech teraz $f\colon \boldsymbol{A} \to \boldsymbol{B}$ je surjekcia. Z definície vyplýva, že každý prvok $y \in B$ je množina $f^{-1}(\{y\})$ neprázdna. Inými slovami, existuje prvok $x_y \in \boldsymbol{A}$ taký, že $f(x_y) = y$. Ak takých prvkov existuje viac, vyberieme jeden z nich a označíme ho x_y. Definujme zobrazenie $g\colon \boldsymbol{B} \to \boldsymbol{A}$ tak, že položíme $g(y) = x_y$. Je zjavné, že toto zobrazenie je injektívne. □

Poznámka. Dôkaz implikácie "$\Leftarrow$" využíva tzv. *axiómu výberu*, ktorá umožňuje pre daný systém množín $\mathcal{S}$ vytvoriť množinu $\boldsymbol{A}$ takú, že pre ľubovoľný prvok $X \in \mathcal{S}$ je prienik $X \cap \boldsymbol{A}$ jednoprvková množina. Názov axiómy pochádza zo skutočnosti, že novú množinu môžeme vytvoriť, ak v nejakom systéme množín z každej množiny vyberieme po jednom prvku. Na prvý pohľad vyzerá táto axióma prirodzene, no jej použitie môže viesť k dôkazu tvrdení, ktoré sa vzpierajú intuícii. Jedným z nich je napr. Banachov-Tarského paradox, ktorý tvrdí, že trojrozmernú guľu s polomerom 1 môžeme rozbiť na konečný počet podmnožín, z ktorých len pootočením a posunutím na iné miesto 3-rozmerného priestoru dokážeme poskladať guľu s akokoľvek veľkým polomerom. Napriek takýmto paradoxom je axióma výberu veľmi užitočná a v modernej matematike sa bežne používa. V hierarchii axióm teórie množín má však osobitné postavenie.

Na záver tejto časti zavedieme ešte jedno označenie, ktoré býva niekedy veľmi užitočné: Pre množiny $\boldsymbol{A}$ a $\boldsymbol{B}$ označme symbolom $\boldsymbol{B}^{\boldsymbol{A}}$ množinu všetkých zobrazení $f\colon \boldsymbol{A} \to \boldsymbol{B}$. Ponechávame čitateľovi, aby sa presvedčil o tom, že pre každú množinu $\boldsymbol{B}$ je množina $\boldsymbol{B}^{\emptyset}$ neprázdna, no ak $\boldsymbol{A} \neq \emptyset$, tak množina $\emptyset^{\boldsymbol{A}}$ je prázdna. Totiž $\emptyset$ je (jediným!) zobrazením $\emptyset \to \boldsymbol{B}$, čiže $\boldsymbol{B}^{\emptyset} = \{\emptyset\}$, no naproti tomu neprázdnu množinu nemožno zobraziť do $\emptyset$. Presvedčte sa o tom starostlivým preverením príslušných definícií.

2.7 Mohutnosti množín

Pojem bijekcie teraz využijeme na spresnenie a zovšeobecnenie intuitívneho pojmu počtu prvkov množiny.

Budeme hovoriť, že dve množiny $\boldsymbol{A}$ a $\boldsymbol{B}$ sú *ekvivalentné*, alebo že majú *rovnakú mohutnosť*, ak existuje bijekcia $f\colon \boldsymbol{A} \to \boldsymbol{B}$. Budeme tiež hovoriť, že majú rôznu mohutnosť, ak taká bijekcia neexistuje. Je zrejmé, že tento vzťah je symetrický, lebo $f^{-1}\colon \boldsymbol{B} \to \boldsymbol{A}$ je bijekcia. Keďže bijekcia medzi množinami $\boldsymbol{A}$ a $\boldsymbol{B}$ predstavuje vzájomne jednoznačnú korešpondenciu medzi prvkami týchto množín, znamená to, že ich prvky sa líšia síce menami, ale je ich „rovnako veľa“. Pojem mohutnosti teda zovšeobecňuje pojem počtu prvkov.

Všimnime si, že ak množiny $\boldsymbol{A}$ a $\boldsymbol{B}$ majú rovnakú mohutnosť a množiny $\boldsymbol{B}$ a $\boldsymbol{C}$ majú tiež rovnakú mohutnosť, tak aj množiny $\boldsymbol{A}$ a $\boldsymbol{C}$ majú rovnakú mohutnosť – ako by sme prirodzene očakávali. Ak totiž $f\colon \boldsymbol{A} \to \boldsymbol{B}$ je bijekcia zabezpečujúca rovnakú mohutnosť množín $\boldsymbol{A}$ a $\boldsymbol{B}$ a $g\colon \boldsymbol{B} \to \boldsymbol{C}$ je bijekcia

zabezpečujúca rovnakú mohutnosť množín $\boldsymbol{B}$ a $\boldsymbol{C}$, tak $g \circ f \colon \boldsymbol{A} \to \boldsymbol{C}$ zabezpečuje rovnakú mohutnosť množín $\boldsymbol{A}$ a $\boldsymbol{C}$. Môžeme teda povedať, že všetky tri mnoziny $\boldsymbol{A}$, $\boldsymbol{B}$ a $\boldsymbol{C}$ majú rovnakú mohutnosť. To nás oprávňuje zaviesť zápis $|\boldsymbol{A}| = |\boldsymbol{B}|$ pre skutočnosť, že množiny $\boldsymbol{A}$ a $\boldsymbol{B}$ majú rovnakú mohutnosť.

Budeme hovoriť, že množina $\boldsymbol{A}$ má n prvkov (alebo že má mohutnosť n), ak existuje bijekcia $f : \boldsymbol{A} \to \{0, 1, 2, \ldots, n-1\} = n$. Symbolicky to zapíšeme takto: $|\boldsymbol{A}| = n$.

Množina, ktorá má mohutnosť niektorého prirodzeného čísla je *konečná množina*; ostatné množiny sú *nekonečné*.

Intuitívne je zrejmé, že množina všetkých prirodzených čísel $\mathbb{N} = \{0, 1, 2, \ldots\}$ nie je konečná. Dokázať toto tvrdenie exaktne je možné napríklad takýmto postupom:

Ak m a n sú rôzne prirodzené čísla, tak ich mohutnosti sú rôzne, čoho dôsledkom je, že žiadna vlastná podmnožina konečnej množiny nie je s celou množinou ekvivalentná. (Vypracovať podrobnosti tohto postupu dá istú prácu.) Naproti tomu množina $\mathbb{N}$, ako o chvíľu uvidíme, obsahuje vlastnú podmnožinu, ktorá je ekvivalentná s $\mathbb{N}$. Preto $\mathbb{N}$ nemôže byť konečná. Za požadovanú vlastnú podmnožinu rovnakej mohutnosti ako $\mathbb{N}$ môžeme zobrať napríklad množinu $2\mathbb{N} = \{0,\ 2,\ 4, \ldots\}$ všetkých párnych prirodzených čísel. Naozaj, zobrazenie

$$\begin{aligned} h :\ \mathbb{N} &\to 2\mathbb{N} \\ x &\mapsto 2x \end{aligned}$$

je injektívne rovnako ako zobrazenie

$$\begin{aligned} k :\ 2\mathbb{N} &\to \mathbb{N} \\ x &\mapsto \frac{x}{2} \end{aligned}$$

Ľahko sa presvedčíme, že $k \circ h = id_{\mathbb{N}}$ a $h \circ k = id_{2\mathbb{N}}$, takže $k = h^{-1}$, čiže obe zobrazenia sú bijekcie. Teda $|2\mathbb{N}| = |\mathbb{N}|$, no $2\mathbb{N} \subsetneqq \mathbb{N}$.

Množinu $\boldsymbol{A}$ nazveme *nekonečne spočítateľnou*, ak má rovnakú mohutnosť ako množina prirodzených čísel $\mathbb{N}$. Mohutnosť nekonečne spočítateľnej množiny sa zvykne označovať symbolom $\aleph_0$, ktorý je odvodený od prvého písmena $\aleph$ hebrejskej abecedy (alef) a číta sa „alef-nula“. Teda $|\mathbb{N}| = \aleph_0$. Množinu nazveme *spočítateľnou*, ak je konečná alebo nekonečne spočítateľná, a *nespočítateľnou*, ak nie je spočítateľná.

Teraz ukážeme, že množina $(0, 1)$ všetkých reálnych čísel na otvorenom intervale medzi 0 a 1 je nespočítateľná. Prvým krokom bude, že každé reálne číslo reprezentujeme pomocou nekonečnej postupnosti nôl a jednotiek.

Pod *postupnosťou* v množine $\boldsymbol{A}$ rozumieme ľubovoľné zobrazenie $f\colon \mathbb{N} \to \boldsymbol{A}$. Namiesto $f(i)$ často píšeme f_i a namiesto $f\colon \mathbb{N} \to \boldsymbol{A}$ často píšeme $(f_i)_{i=0}^{\infty}$ alebo $(f_0, f_1, f_2, \dots)$. Ak $\boldsymbol{A} = \{0,1\}$, postupnosť sa nazýva *binárnou*.

Naznačíme proces, akým je možné číslu $c \in (0,1)$ jednoznačne priradiť nekonštantnú binárnu postupnosť – čiže skonštruovať bijekciu $(0,1) \to \{0,1\}^{\mathbb{N}} - \{\mathbf{0},\mathbf{1}\} =: \boldsymbol{B}$ (kde $\mathbf{0} = (0,0,\dots)$ a $\mathbf{1} = (1,1,\dots)$).

Nech $c \in (0,1)$. Interval $(0,1)$ teraz rozdelíme na dva (takmer) rovnaké polovice – podintervaly $\left(0,\frac{1}{2}\right)$ a $\left\langle\frac{1}{2},1\right)$. Ak $c \in \left(0,\frac{1}{2}\right)$, položíme $f_0 = 0$. Ak $c \in \left(\frac{1}{2},1\right)$, položíme $f_0 = 1$. Ak $c = \frac{1}{2}$, položíme $f_0 = 1$ a $f_1 = f_2 = \dots = 0$, čím sme v tomto prípade určili už celú postupnosť. Ak hľadaná postupnosť f ešte nie je úplne určená, pokračujeme v procese ďalej. Povedzme, že $c \in \left(\frac{1}{2},1\right)$. Teraz rozdelíme tento interval na dva: $\left(\frac{1}{2},\frac{3}{4}\right)$ a $\left\langle\frac{3}{4},1\right)$. Ak $c \in \left(\frac{1}{2},\frac{3}{4}\right)$, položíme $f_1 = 0$ (pričom máme $f_0 = 1$). Ak $c \in \left(\frac{3}{4},1\right)$, položíme $f_1 = 1$. Ak $c = \frac{3}{4}$ položíme $f_1 = 1$ a $f_2 = f_3 = \dots = 0$, čím sme opäť určili celú postupnosť. Analogicky postupujeme v ďalších krokoch.

Nie je veľmi ťažké sa presvedčiť, že takto priradíme každému číslu $c \in (0,1)$ nejakú binárnu postupnosť a že taká postupnosť nie je konštantná (lebo $0,1 \notin (0,1)$). Obrátene, ak je zadaná nekonštantná binárna postupnosť f, pomocou postupného delenia intervalu $(0,1)$ na polovice a vyberaním ľavého či pravého podintervalu podľa toho, či skúmaný člen f_i našej postupnosti f je 0 alebo 1 môžeme postupne „polohu“ čísla c vymedziť. (Presný dôkaz tu však vyžaduje poznatky z topológie reálnych čísel, čo je ďaleko nad rámec tohto textu). Takýmto spôsobom môžeme ukázať, že existuje bijekcia $\varphi\colon (0,1) \to \boldsymbol{B}$.

Ďalším krokom je ukázať, že množina $\boldsymbol{B}$ nie je spočítateľná. Na to použijeme techniku, ktorá sa nazýva *diagonálna metóda* a rôzne jej variácie majú široké použitie.

Predpokladajme kvôli sporu, že množina $\boldsymbol{B}$ je spočítateľná. To znamená, že existuje bijekcia $\mathbb{N} \to \boldsymbol{B}$. Táto bijekcia definuje „očíslovanie“ prvkov množiny $\boldsymbol{B}$ prirodzenými číslami, alebo – inak povedané zoradenie jej prvkov do nekonečnej postupnosti $(b^0, b^1, b^2, \dots)$. Každý člen b^i je sám nekonečnou postupnosťou $b^i = (b^i_0, b^i_1, b^i_2, \dots)$. Zapíšeme teraz tieto postupnosti do tabuľky 2.7 tak, že každá postupnosť b^i bude v jednom riadku, a členy rovnakého poradia budú v jednom stĺpci.

Hoci táto tabuľka 2.7 obsahuje všetky prvky množiny $\boldsymbol{B}$, ľahko skonštruujeme binárnu postupnosť, ktorá v tejto tabuľke nie je. Naozaj, definujeme binárnu postupnosť $c = (c_0,\ c_1,\ c_2, \dots)$ tak, že od postupnosti b^0 sa bude odlišovať členom b^0_0, od b^1 členom $b^1_1, \dots$, od b^n členom b^n_n a tak ďalej. Stačí

$$\begin{array}{lcccccccc}
b^0 & = & (\boxed{b_0^0}, & b_1^0\,, & b_2^0\,, & \ldots, & b_n^0\,, & \ldots) \\
b^1 & = & (b_0^1, & \boxed{b_1^1}, & b_2^1\,, & \ldots, & b_n^1\,, & \ldots) \\
\vdots & = & & & \square & & \ldots & \\
b^n & = & (b_0^n, & b_1^n\,, & b_2^n\,, & \ldots, & \boxed{b_n^n}\,, & \ldots) \\
\vdots & & & & & \ldots & & \square
\end{array}$$

teda položiť

$$c_i = 1 - b_i^i.$$

Je teraz zrejmé, že $c \in \boldsymbol{B}$, no c sa líši od každej z postupností b^i, $i = 0{,}1{,}\ldots$, čo je spor. Toto dokazuje, že množina $\boldsymbol{B}$ nie je spočítateľná.

Keďže množina $\boldsymbol{B}$ je ekvivalentná s intervalom (0,1), aj on je nespočítateľnou množinou. Keďže $(0,1) \subseteq \mathbb{R}$, množina všetkých reálnych čísel je tiež nespočítateľná. V skutočnosti majú množiny (0,1) a $\mathbb{R}$ rovnakú mohutnosť. Funkcia *arcus tangens* $\arctan\colon \mathbb{R} \to (-\frac{\pi}{2}, \frac{\pi}{2})$ je bijekcia, lineárna funkcia $f\colon (-\frac{\pi}{2}, \frac{\pi}{2}) \to (0,1)$, $x \mapsto \frac{1}{\pi}x + \frac{1}{2}$ je tiež bijekcia a ich zložením získavame požadovanú bijekciu $\mathbb{R} \to (0,1)$.

Vráťme sa teraz k spočítateľným množinám. Zatiaľ vieme, že $\mathbb{N}$ je spočítateľná množina. Vieme tiež, že aj každá podmnožina spočítateľnej množiny je spočítateľná. Spočítateľná je aj množina $\mathbb{Z}$ všetkých celých čísel. Stačí ju totiž zoradiť do postupnosti , a to je ľahké: 0, 1, −1, 2, −2, 3, −3, ... O niečo náročnejšie je ukázať, že množina $\mathbb{Q}$ všetkých racionálnych čísel je spočítateľná. Prv než se o tom presvedčíme, dokážeme nasledujúce tvrdenia.

Tvrdenie 2.11. *Nech $\boldsymbol{A}_0, \boldsymbol{A}_1, \ldots, \boldsymbol{A}_i, \ldots$ sú spočítateľné množiny (môže byť ich konečne aj nekonečne-spočítateľne-veľa). Potom aj množina $\boldsymbol{A}_0 \cup \boldsymbol{A}_1 \cup \ldots \cup \boldsymbol{A}_i \cup \ldots$ je spočítateľná.*

Poznámka. Zatiaľ sme definovali zjednotenie iba dvoch množín (a tým aj zjednotenie ľubovoľného konečného počtu množín). Tu však hovoríme aj o nekonečnom zjednotení množín. To sa definuje takto:

$$\bigcup_{i=0}^{\infty} \boldsymbol{A}_i = \boldsymbol{A}_0 \cup \boldsymbol{A}_1 \cup \ldots \cup \boldsymbol{A}_i \cup \ldots = \{x;\ \text{existuje index } i \text{ taký, že } x \in \boldsymbol{A}_i\}.$$

Podobne definujeme aj prienik:

$$\bigcap_{i=0}^{\infty} \boldsymbol{A}_i = \boldsymbol{A}_0 \cap \boldsymbol{A}_1 \cap \ldots \cap \boldsymbol{A}_i \cap \ldots = \{x;\quad x \in \boldsymbol{A}_i \text{ pre každý index } i\}.$$

Dôkaz. Keďže každá z množín $\boldsymbol{A}_i$ je spočítateľná, môžeme jej prvky zoradiť do postupnosti $(a_0^i, a_1^i, \ldots)$. Zapíšeme teraz tieto postupnosti do tabuľky tak, že každá postupnosť $(a_0^i, a_1^i, \ldots)$ bude v jednom riadku a členy rovnakého poradia budú tom istom stĺpci. Teraz stačí prepísať túto tabuľku do jedného riadka, čo sa dá urobiť viacerými spôsobmi. Jeden je označený na nasledujúcom obrázku.

$$\begin{array}{cccccc} a_0^0, & a_1^0, & a_2^0, & \ldots, & a_n^0, & \ldots \\ a_0^1, & a_1^1, & a_2^1, & \ldots, & a_n^1, & \ldots \\ a_0^2, & a_1^2, & a_2^2, & \ldots, & a_n^2, & \ldots \end{array}$$

Tým sme dostali nasledujúcu postupnosť obsahujúcu všetky prvky množiny $\boldsymbol{A}_0 \cup \boldsymbol{A}_1 \cup \ldots$: $a_0^0, a_0^1, a_1^0, a_0^2, a_1^1, a_2^0, a_0^3, a_1^2, \ldots$. Takto sme ukázali, že množina $\boldsymbol{A}_0 \cup \boldsymbol{A}_1 \cup \ldots$ je spočítateľná. □

Teraz je už ľahké dokázať, že množina $\mathbb{Q}$ je spočítateľná. Každé racionálne číslo si najprv vyjadríme zlomkom v základnom tvare; tento zápis je jednoznačný. Nech $\boldsymbol{R_n}$ označuje množinu všetkých racionálnych čísel, ktoré majú v základnom tvare menovateľ n. Potom $\boldsymbol{R_1} = \mathbb{Z}$ a existuje prirodzená bijekcia $\boldsymbol{R_n} \to \mathbb{Z}$, totiž zobrazenie $\pm\frac{a}{n} \mapsto \pm a$. Teda každá z množín $\boldsymbol{R_n}$ je spočítateľná. Podľa predchádzajúceho tvrdenia musí byť spočítateľná aj množina $\boldsymbol{R_1} \cup \boldsymbol{R_2} \cup \ldots \cup \boldsymbol{R_n} \cup \ldots = \bigcup_{n=1}^{\infty} \boldsymbol{R_n} = \mathbb{Q}$.

Podobným trikom môžeme dokázať nasledujúci dôsledok Tvrdenia 1.8.

Tvrdenie 2.12. *Ak $\boldsymbol{A}$ a $\boldsymbol{B}$ sú spočítateľné množiny, tak aj ich karteziánsky súčin $\boldsymbol{A} \times \boldsymbol{B}$ je spočítateľná množina.*

2.8 Kardinálne čísla

V tejto časti ukážeme, že na mohutnosť množiny – zovšeobecnenie počtu jej prvkov – sa môžeme dívať aj ako na nejaké číslo, ktoré v tejto súvislosti budeme nazývať *kardinálne číslo*. Nepovieme, čo sú kardinálne čísla; povieme len aké vlastnosti majú a ako sa dajú sčitovať, násobiť a mocniť.

Hovoríme, že dve množiny majú rovnaké *kardinálne číslo*, ak sú ekvivalentné, čiže ak majú rovnakú mohutnosť. Kardinálne číslo je teda to, čo je spoločné všetkým navzájom ekvivalentným množinám – je to akési stelesnenie ekvivalencie množín. Kardinálne číslo množiny $\boldsymbol{A}$ označujeme $|\boldsymbol{A}|$.

Niektoré kardinálne čísla už poznáme: v časti 1.5 sme si už povedali, že množina je n-prvková ak je ekvivalentná s množinou $n = \{0, 1, \ldots, n-1\}$.

Za kardinálne číslo všetkých n-prvkových množín môžeme preto zobrať prirodzené číslo n, teda množinu $\{0, 1, \ldots, n-1\}$. Ďalej sme si povedali, že množina je nekonečne spočítateľná, ak je ekvivalentná s množinou $\mathbb{N}$. Mohutnosť množiny $\mathbb{N}$ sme označovali symbolom $\aleph_0$ (alef-nula), čo budeme považovať za kardinálne číslo všetkých nekonečne spočítateľných množín. Teda $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$. Napokon vieme, že množina $\mathbb{R}$ nie je spočítateľná; jej kardinálne číslo sa označuje c a nazýva sa *mohutnosť kontinua*. Uvidíme, že $c = 2^{\aleph_0}$ a že aj nespočítateľné množiny môžu mať rôzne kardinálne čísla.

Zo skúsenosti vieme, že zjednotením dvoch disjunktných konečných množín, pričom jedna má m prvkov a druhá má n prvkov, dostaneme $(m+n)$-prvkovú konečnú množinu. V nasledujúcej kapitole venovanej kombinatorike sa s týmto pozorovaním stretneme ako s pravidlom súčtu.

Definícia 1. Nech α a β sú ľubovoľné kardinálne čísla. Nech $\boldsymbol{A}$ a $\boldsymbol{B}$ sú disjunktné množiny také, že $|\boldsymbol{A}| = \alpha$ a $|\boldsymbol{B}| = \beta$. Definujme

$$\alpha + \beta \ := |\boldsymbol{A} \cup \boldsymbol{B}|$$

Poznamenajme, že táto definícia nezávisí od konkrétnej voľby množín $\boldsymbol{A}$ a $\boldsymbol{B}$. Ak totiž $\boldsymbol{A'}$ a $\boldsymbol{B'}$ sú disjunktné množiny, pre ktoré $|\boldsymbol{A'}| = |\boldsymbol{A}| = \alpha$ a $|\boldsymbol{B'}| = |\boldsymbol{B}| = \beta$, tak $|\boldsymbol{A'} \cup \boldsymbol{B'}| = |\boldsymbol{A} \cup \boldsymbol{B}|$.

Pri definícii súčinu kardinálnych čísel vychádzame z toho, že karteziánsky súčin m-prvkovej množiny a n-prvkovej množiny má $m \cdot n$ prvkov. V kombinatorike sa tento fakt nazýva pravidlom súčinu.

Definícia 2. Nech α a β sú ľubovoľné kardinálne čísla. Nech $\boldsymbol{A}$ a $\boldsymbol{B}$ sú ľubovoľné množiny také, že $|\boldsymbol{A}| = \alpha$ a $|\boldsymbol{B}| = \beta$. Definujeme

$$\alpha \cdot \beta := |\boldsymbol{A} \times \boldsymbol{B}|.$$

Podobne ako v predchádzajúcej definícii, súčin kardinálnych čísel nezávisí od konkrétnej voľby množín: ak $|\boldsymbol{A'}| = |\boldsymbol{A}|$ a $|\boldsymbol{B'}| = |\boldsymbol{B}|$, tak $|\boldsymbol{A'} \times \boldsymbol{B'}| = |\boldsymbol{A} \times \boldsymbol{B}|$.

Mocnenie kardinálnych čísel sa zakladá na nasledujúcom porovnaní, ktoré – ako uvidíme v nasledujúcej kapitole – súvisí s počtom variácií s opakovaním. Ak $\boldsymbol{A}$ je m-prvková množina a $\boldsymbol{B}$ je n-prvková množina, tak množina $\boldsymbol{B}^{\boldsymbol{A}}$ všetkých zobrazení $\boldsymbol{A} \to \boldsymbol{B}$ má n^m (teda $|\boldsymbol{B}|^{|\boldsymbol{A}|}$) prvkov.

Definícia 3. Nech α a β sú ľubovoľné kardinálne čísla.Nech $\boldsymbol{A}$ a $\boldsymbol{B}$ sú množiny také, že $|\boldsymbol{A}| = \alpha$ a $|\boldsymbol{B}| = \beta$. Definujme

$$\beta^\alpha = |\boldsymbol{B}^{\boldsymbol{A}}|.$$

Čitateľ sa opäť môže presvedčiť, že ani táto definícia nezávisí od konkrétnej voľby množín: ak $|\boldsymbol{A}'| = |\boldsymbol{A}|$ a $|\boldsymbol{B}'| = |\boldsymbol{B}|$, tak $|\boldsymbol{B}^{\boldsymbol{A}'}| = |\boldsymbol{B}^{\boldsymbol{A}}|$.

Z definícii ľahko odvodíme nasledujúce tvrdenia.

Tvrdenie 2.13. *Nech α, β a γ sú ľubovoľné kardinálne čísla. Potom platí:*

(a) $\alpha + \beta = \beta + \alpha, \quad \alpha \cdot \beta = \beta \cdot \alpha$ (komutatívnosť)

(b) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma), \quad (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$ (asociatívnosť)

O niečo ťažšie sa dokáže nasledujúce tvrdenie (hlavne jeho tretia časť):

Tvrdenie 2.14. *Nech α, β a γ sú ľubovoľné kardinálne čísla. Potom platí:*

(a) $\alpha^{\beta} \cdot \alpha^{\gamma} = \alpha^{\beta+\gamma}$

(b) $(\alpha \cdot \beta)^{\gamma} = \alpha^{\gamma} \cdot \beta^{\gamma}$

(c) $(\alpha^{\beta})^{\gamma} = \alpha^{\beta \cdot \gamma}$

Prejdime teraz k niektorým dôsledkom predchádzajúcich tvrdení. Z tvrdení 2.8 a 2.9 ľahko odvodíme, že $\aleph_0 + \aleph_0 = \aleph_0 = \aleph_0 \cdot \aleph_0$. Dá sa tiež ukázať, že pre každé prirodzené číslo n platí $n \cdot \aleph_0 = \aleph_0 = {\aleph_0}^n$ a že ${\aleph_0}^{\aleph_0} = 2^{\aleph_0}$.

Veľkosti kardinálnych čísel môžeme porovnávať podobne ako veľkosti prirodzených čísel.

Definícia 4. Nech α a β sú kardinálne čísla. Nech $\boldsymbol{A}$ a $\boldsymbol{B}$ sú ľubovoľné množiny, pre ktoré $|\boldsymbol{A}| = \alpha$ a $|\boldsymbol{B}| = \beta$. Budeme hovoriť, že α je *menšie alebo rovnaké* ako β (alebo, že α *neprevyšuje* β) a písať $\alpha \leq \beta$, ak existuje injekcia $\boldsymbol{A} \to \boldsymbol{B}$. Ďalej budeme hovoriť, že α je menšie ako β a písať $\alpha < \beta$ ak $\alpha \leq \beta$ a zároveň $\alpha \neq \beta$. Symboly $\alpha \geq \beta$ a $\alpha > \beta$ budú mať zrejmý význam.

Predchádzajúca definícia sa nám hneď na prvý pohľad zdá byť plne v súhlase s našou intuíciou. Zároveň však kladie prirodzenú otázku: ak α a β sú kardinálne čísla také, že $\alpha \leq \beta$ a súčasne $\alpha \geq \beta$, musí platiť aj $\alpha = \beta$? Preložené do jazyka zobrazení: ak $\boldsymbol{A}$ a $\boldsymbol{B}$ sú množiny a $f\colon \boldsymbol{A} \to \boldsymbol{B}$ a $g\colon \boldsymbol{B} \to \boldsymbol{A}$ sú injekcie, musí už existovať aj bijekcia $\boldsymbol{A} \to \boldsymbol{B}$? Táto otázka je obzvlášť zaujímavá v súvise s nekonečnými množinami. Napr. $|\mathbb{N}| = |\mathbb{Q}| = \aleph_0$, pritom však prirodzené vloženie $\mathbb{N} \to \mathbb{Q}$, $x \mapsto x$, je injekcia, ktorá nie je bijekciou. Našťastie naše otázky majú kladnú odpoveď, a tá je obsahom nasledujúcej netriviálnej teorémy:

Teoréma 2.15 (Cantorova-Bernsteinova)**.** *Nech $\boldsymbol{A}$ a $\boldsymbol{B}$ sú ľubovoľné množiny. Ak existuje injektívne zobrazenie $f\colon \boldsymbol{A} \to \boldsymbol{B}$ a injektívne zobrazenie $g\colon \boldsymbol{B} \to \boldsymbol{A}$, tak množiny $\boldsymbol{A}$ a $\boldsymbol{B}$ sú ekvivalentné.*

Dôkaz. Každý prvok $y \in \boldsymbol{B}$ je obrazom najviac jedného prvku $x \in \boldsymbol{A}$ v zobrazení f. Ak taký prvok x jestvuje, nazveme ho *rodičom* prvku y. Podobne je každý prvok $x \in \boldsymbol{A}$ obrazom najviac jedného prvku $y \in \boldsymbol{B}$ v zobrazení g. Tento prvok y, ak existuje, sa tiež bude nazývať *rodičom* prvku x.

Pre každý prvok t z množiny $\boldsymbol{A}$ alebo z množiny $\boldsymbol{B}$ budeme sledovať reťazec jeho predkov. Formálne prvok z nazveme *predkom* prvku t, ak existuje postupnosť $z = z_n, z_{n-1}, \ldots, z_1, z_0 = t$ prvkov množiny $\boldsymbol{A} \cup \boldsymbol{B}$ taká, že pre každé $i \in \{0, \ldots, n-1\}$ je prvok z_{i+1} rodičom prvku z_i. Pre ľubovoľný $t \in \boldsymbol{A} \cup \boldsymbol{B}$ môžu nastať tri navzájom sa vylučujúce prípady.

(1) každý predok prvku t má rodiča;

(2) existuje taký predok z prvku t, ktorý už nemá rodiča, pričom $z \in \boldsymbol{A}$;

(3) existuje taký predok z prvku t, ktorý nemá rodiča, pričom $z \in \boldsymbol{B}$.

(Aj keď pre ďalší beh dôkazu to nie je podstatné, bude užitočné, ak si čitateľ uvedomí, že prípad (1) môže nastať dvoma rozličnými spôsobmi: buďto je prvok t sám svojím predkom – a teda t má iba konečne veľa predkov – alebo každý predok prvku t je rôzny od t.)

Nech teraz $\boldsymbol{A}_i$, kde $i = 1, 2, 3$, je množina všetkých $t \in \boldsymbol{A}$, ktoré majú vyššie uvedenú vlastnosť i. Podobne definujme aj množiny $\boldsymbol{B}_i$ pre $i = 1, 2, 3$. Keďže sa prípady vylučujú, sú množiny $\boldsymbol{A}_i$ ako aj $\boldsymbol{B}_i$ po dvoch disjunktné.

Ľahko nahliadneme, že predok prvku $t \in \boldsymbol{A}$ patriaci do $\boldsymbol{A}_i$ tiež leží v $\boldsymbol{A}_i$. Podobné tvrdenie platí aj o $t \in \boldsymbol{B}$. Preto $f|\boldsymbol{A}_1\colon \boldsymbol{A}_1 \to \boldsymbol{B}_1$ je bijekcia, $f|\boldsymbol{A}_2\colon \boldsymbol{A}_2 \to \boldsymbol{B}_2$ je bijekcia a $g|\boldsymbol{B}_3\colon \boldsymbol{B}_3 \to \boldsymbol{A}_3$ je bijekcia. Napokon vidíme, že zobrazenie $h:\ \boldsymbol{A} \to \boldsymbol{B}$ definované predpisom

$$h(x) = \begin{cases} f(x), & \text{ak } x \in \boldsymbol{A}_1 \cup \boldsymbol{A}_2 \\ g^{-1}(x), & \text{ak } x \in \boldsymbol{A}_3 \end{cases}$$

je bijekcia. □

Pri dôkaze naspočítateľnosti množiny $(0, 1)$ sme zároveň vlastne ukázali, že $|(0,1)| = |\{0,1\}^{\mathbb{N}}| = |\{0,1\}|^{|\mathbb{N}|} = 2^{\aleph_0}$. Hneď potom sme nahliadli, že $|\mathbb{R}| = |(0,1)|$. Odtiaľ dostávame vzťah pre mohutnosť kontinua c:

$$c = |\mathbb{R}| = |(0,1)| = 2^{\aleph_0}.$$

Keďže množina $\mathbb{N}$ je spočítateľná, ale $\mathbb{R}$ nie je (a $\mathbb{N} \subseteq \mathbb{R}$), dostávame, že $2^{\aleph_0} > \aleph_0$. Analogická nerovnosť (notoricky známa pre prirodzené čísla) platí všeobecne. Vyplýva to z nasledujúcich dvoch tvrdení.

Tvrdenie 2.16. *Pre ľubovoľnú množinu $\boldsymbol{A}$ platí:*

$$|\mathcal{P}| = 2^{|\boldsymbol{A}|}$$

Dôkaz. Ľahko nahliadneme, že zobrazenie $\Phi : \mathcal{P}(\boldsymbol{A}) \to \{0,1\}^{\boldsymbol{A}}$, ktoré podmnožine $X \subseteq \boldsymbol{A}$ priradí jej charakteristickú funkciu $\chi_x : \boldsymbol{A} \to \{0,1\}$ (pozri príklad 4 v článku 1.4) je bijekcia. Preto $|\mathcal{P}(\boldsymbol{A})| = |\{0,1\}^{\boldsymbol{A}}| = 2^{|\boldsymbol{A}|}$. □

Ako dôsledok tohto tvrdenia dostávame, že mohutnosť kontinua c je totožná s mohutnosťou množiny všetkých podmnožín množiny $\mathbb{N}$:

$$c = |\mathbb{R}| = 2^{\aleph_0} = 2^{|\mathbb{N}|} = |\mathcal{P}(\mathbb{N})|.$$

Teoréma 2.17 (Cantorova)**.** *Pre každú množinu $\boldsymbol{A}$ platí*

$$|\mathcal{P}(\boldsymbol{A})| > |\boldsymbol{A}|.$$

Dôkaz. Je zrejmé, že $|\boldsymbol{A}| \leq |\mathcal{P}(\boldsymbol{A})|$, lebo zobrazenie $\boldsymbol{A} \to \mathcal{P}(\boldsymbol{A})$, $x \mapsto \{x\}$ je injektívne. Aby sme ukázali, že $|\boldsymbol{A}| \neq |\mathcal{P}(\boldsymbol{A})|$ stačí sa presvedčiť o tom, že neexistuje surjekcia $\boldsymbol{A} \to \mathcal{P}(\boldsymbol{A})$. Predpokladajme, kvôli sporu, že zobrazenie $f\colon \boldsymbol{A} \to \mathcal{P}(\boldsymbol{A})$ je surjektívne. Keďže pre každý prvok $x \in \boldsymbol{A}$ je $f(x) \subseteq \boldsymbol{A}$, má zmysel sa spýtať, či $x \in f(x)$ alebo $x \notin f(x)$. Zoberme teda množinu $\boldsymbol{B} = \{x \in \boldsymbol{A};\ x \notin f(x)\} \subseteq \boldsymbol{A}$. Táto množina musí mať vzhľadom na zobrazenie f vzor v množine $\boldsymbol{A}$; nech je to prvok $y \in \boldsymbol{A}$. Patrí prvok y do množiny $\boldsymbol{B}$?

Keby $y \in \boldsymbol{B}$, tak y by spĺňal vlastnosť definujúcu množinu $\boldsymbol{B}$, totiž y by nepatril do $f(y)$. No $f(y) = \boldsymbol{B}$ a dostali by sme, že $y \notin \boldsymbol{B}$ – spor. Preto $y \notin \boldsymbol{B}$. No $\boldsymbol{B} = f(y)$, takže $y \notin f(y)$. Tým je prvok y splnená podmienka príslušnosti do množiny $\boldsymbol{B}$, takže $y \in \boldsymbol{B}$ – čo je spor. Tento spor dokazuje, že surjekcia $\boldsymbol{A} \to \mathcal{P}(\boldsymbol{A})$ nemôže existovať. Teoréma je dokázaná. □

Poznámka. 1. Stojí za povšimnutie, že predchádzajúci dôkaz je založený na myšlienke veľmi podobnej tej, ktorá leží v jadre Russelovho paradoxu.

2. Z Cantorovej teorémy 2.17 vyplýva, že medzi nespočítateľnými množinami existujú množiny rôznych mohutností, ba dokonca ľubovoľne veľkých mohutností. Môžeme totiž zobrať nespočítateľnú množinu $\mathbb{R}$ mohutnosti $c = 2^{\aleph_0}$ a postupne brať množiny $\mathcal{P}(\mathbb{R})$, $\mathcal{P}(\mathcal{P}(\mathbb{R}))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{R})))$ atď. Tým dostaneme neobmedzene rastúci sled nespočítateľných mohutností $2^{\aleph_0} < 2^{(2^{\aleph_0})} < 2^{(2^{(2^{\aleph_0})})} < \dots$

Napokon bez dôkazu uvedieme niekoľko užitočných nerovností medzi kardinálnymi číslami.

Tvrdenie 2.18. *Nech κ, λ, μ, κ_i a λ_i pre $i \in \{1, 2\}$ sú ľubovoľné kardinálne čísla. Potom platí:*

(a) *Ak $\kappa_1 \leq \lambda_1$ a $\kappa_2 \leq \lambda_2$, tak $\kappa_1 + \kappa_2 \leq \lambda_1 + \lambda_2$.*

(b) *Ak $\kappa_1 \leq \lambda_1$ a $\kappa_2 \leq \lambda_2$, tak $\kappa_1 \cdot \kappa_2 \leq \lambda_1 \cdot \lambda_2$.*

(c) $\kappa \leq \kappa + \lambda$ *pre* $\lambda \geq 0$

(d) $\kappa \leq \kappa \cdot \lambda$ *pre* $\lambda \geq 1$

(e) $\kappa + \kappa = 2 \cdot \kappa$

(f) $\kappa \cdot \kappa = \kappa^2$

(g) $\kappa + \kappa \leq \kappa \cdot \kappa$

(h) $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$

(i) $\kappa \leq \kappa^\lambda$ *pre* $\lambda \geq 1$

(j) $\lambda \leq \kappa^\lambda$ *pre* $\kappa \geq 2$

(k) *Ak* $\kappa_1 \leq \kappa_2$ *a* $\lambda_1 \leq \lambda_2$, *tak* $\kappa_1^{\lambda_1} \leq {\kappa_2}^{\lambda_2}$.

Kapitola 3

Kombinatorika

3.1 Prirodzené čísla a matematická indukcia

Kombinatorika je matematická disciplína, ktorá sa zaoberá úlohami o štruktúrach definovaných na konečných množinách. Najčastejšie ide o podmnožiny, usporiadané n-tice, relácie, zobrazenia, rozklady a množstvo iných objektov, ktoré jednotne nazývame *kombinatorickými konfiguráciami*. Aj keď korene kombinatoriky siahajú hlboko pred náš letopočet, rozvoj kombinatoriky ako modernej disciplíny je úzko spojený s nástupom informatiky. Kombinatorika tvorí jeden zo základných pilierov tohto vedného odboru. Dnešnú kombinatoriku charakterizuje niekoľko všeobecných typov úloh. Spomedzi nich sú najdôležitejšie:

(1) zostrojiť konfigurácie požadovaných vlastností;

(2) nekonštruktívnymi metódami dokázať existenciu alebo neexistenciu konfigurácie istých vlastností;

(3) určiť počet všetkých konfigurácií daného typu;

(4) charakterizovať také konfigurácie pomocou iných pojmov, vlastností a parametrov;

(5) nájsť algoritmus, ktorý umožňuje všetky požadované konfigurácie zostrojiť;

(6) spomedzi všetkých konfigurácií vybrať optimálnu (alebo extremálnu – maximálnu, či minimálnu) podľa daných kriterií.

Spomedzi nich sa v tejto kapitole budeme stretávať najmä s úlohami typu (4), (3) a (1).

Ako sme povedali, kombinatorika sa zaoberá prevažne konečnými štruktúrami. Je tu však jedna nekonečná množina, ktorá má pre kombinatoriku podstatný význam: množina $\mathbb{N} = \{0, 1, 2, \ldots\}$ všetkých prirodzených čísel. O tejto množine už vieme, že je lineárne usporiadaná bežnou reláciou $\leq$ podľa veľkosti. Toto usporiadanie má jednu veľmi dôležitú vlastnosť – vlastnosť *dobrého usporiadania*:
Každá neprázdna podmnožina množiny $\mathbb{N}$ *má najmenší prvok.*

To, že prirodzené čísla majú túto vlastnosť, sa nahliadne ľahko sporom: keby existovala v $\mathbb{N}$ neprázdna podmnožina M bez najmenšieho prvku, tak by sme ľahko skonštruovali ostro klesajúcu nekonečnú postupnosť $n_0 > n_1 > n_2 > \ldots$ prvkov množiny M. Lenže taká postupnosť v $\mathbb{N}$ očividne neexistuje.

Ďalšia dôležitá vlastnosť množiny $\mathbb{N}$ je základom metódy matematickej indukcie, ktorá je v kombinatorike prakticky všadeprítomná. Znie takto:

Nech $M \subseteq \mathbb{N}$ *je podmnožina spĺňajúca dve podmienky*:

(I1) $0 \in M$;

(I2) ak $x \in M$, tak potom aj $(x + 1) \in M$.

Potom $M = \mathbb{N}$.

Princíp matematickej indukcie môžeme teraz sformulovať takto.

Teoréma 3.1. *Nech* $(V(n))_{n\in\mathbb{N}}$ *je postupnosť výrokov. Predpokladajme, že*

(i) *platí výrok* $V(0)$*;*

(ii) *pre každé prirodzené číslo* n*, ak platí* $V(n)$ *, tak potom platí* $V(n + 1)$*,*

Potom výrok $V(n)$ *platí pre každé prirodzené číslo.*

Poznámka. Bod (i) sa nazýva *báza indukcie* a bod (ii) sa nazýva *indukčný krok*. □

Dôkaz. Definujme množinu $A = \{n \in \mathbb{N};$ platí výrok $V(n)\}$. Podmienka (i) našej teorémy znamená, že $0 \in A$. Podmienka (ii) hovorí, že platí implikácia "ak $n \in A$, tak aj $(n + 1) \in A$." To znamená, že sú splnené vyššie spomenuté podmienky (I1) a (I2), a preto $A = \mathbb{N}$. □

Bežne sa využíva niekoľko modifikácií teorémy 3.1. Stáva sa, že vlastnosť $V(n)$ platí iba pre prirodzené čísla $n \geq n_0$ pre nejaké číslo n_0. V tom prípade najprv overíme pravdivosť výroku $V(n_0)$ a potom dokážeme pravdivosť implikácie: pre každé $n \geq n_0$, ak platí $V(n)$, tak platí aj $V(n+1)$. Tým je potom dokázaná pravdivosť výroku $V(n)$ pre každé $n \geq n_0$. Niekedy je výhodné použiť ďalší variant matematickej indukcie – *úplnú matematickú indukciu.*

Teoréma 3.2. *Predpokladajme, že z platnosti výroku $V(k)$ pre každé $k < n$ vyplýva aj platnosť výroku $V(n)$. Ak platí výrok $V(0)$, tak výrok $V(n)$ platí pre každé prirodzené číslo n.*

Výhodou úplnej matematickej indukcie je, že využíva silnejší indukčný predpoklad – namiesto výroku $V(n-1)$ je to výrok $V(0) \wedge V(1) \wedge \ldots \wedge V(n-1)$ – čo môže uľahčiť vykonanie indukčného kroku. Poznamenajme, že overenie platnosti $V(0)$ nemožno vynechať.

3.2 Dirichletov princíp

V tejto časti sa budeme zaoberať jednoduchým no veľmi dôležitým princípom, ktorý má široké použitie pri riešení rozličných problémov a často vedie k prekvapujúcim záverom. Je známy v rôznych formách. Najjednoduchšia je azda táto:
Ak $n+1$ predmetov ukladáme do n priečinkov, tak aspoň jeden priečinok bude obsahovať dva alebo viac predmetov.

Exaktnejšie môžeme tento princíp sformulovať takto:
Neexistuje injektívne zobrazenie $(n+1)$-prvkovej množiny do n-prvkovej množiny.

Dokážeme všeobecnejšie tvrdenie

Teoréma 3.3. *Nech A a B sú konečné množiny, pričom $|A| = n$, $|B| = m$ a $n > m$ Potom neexistuje žiadne injektívne zobrazenie $f\colon A \to B$.*

Dôkaz. Nech S je množina všetkých prirodzených čísel s takých, že existuje s-prvková množina, ktorá sa dá injektívne zobraziť na t-prvkovú, kde $t < s$. Naším cieľom je ukázať, že $S = \emptyset$. Predpokladajme, sporom, že $S \neq \emptyset$. Potom (na základe princípu dobrého usporiadania) S má najmenší prvok. Nech n je najmenší prvok množiny S a nech $f\colon \{a_1, a_2, \ldots, a_n\} = A \to B = \{b_1, b_2, \ldots, b_m\}$ je injekcia, kde $m < n$. Zrejme $m \geq 2$, lebo inak by boli všetky zobrazenia $A \to B$ konštantné, a teda nie injektívne. Predpokladajme, že $f(a_n) = b_r$ pre nejaké $r \in \{1, 2, \ldots, m\}$. Keby každý z prvkov

$f(a_1), f(a_2), \ldots, f(a_{n-1})$ bol rôzny od b_m, tak zúženie zobrazenia f na množinu $a_1, a_2, \ldots, a_{n-1}$ by bolo injektívnym zobrazením $A - \{a_n\} \to B - \{b_m\}$. To by však bol spor s voľbou čísla n. Preto musí existovať $j \in \{1, 2, \ldots, n-1\}$, že $f(a_j) = b_m$. Kedže f je injekcia, $f(a_n) \neq b_m$, takže $r \leq m - 1$. No potom zobrazenie $g : A - \{a_n\} \to B - \{b_m\}$ definované predpisom

$$\begin{aligned} g(a_j) &= b_r, \\ g(a_i) &= f(a_i) \quad \text{pre } i \neq j, \text{ kde } i \in \{1, 2, \ldots, n-1\} \end{aligned}$$

je opäť injektívne. Znova sme dostali spor s definíciou čísla n, a teda množina S je prázdna. □

Prvýkrát upozornil na tento jednoduchý princíp nemecký matematik 19. storočia P. Dirichlet. Dnes je známy aj ako „holubníkový princíp“ podľa toho, že ak viac ako n holubov používa n holubníkových dier, tak aspoň dva holuby vychádzajú tou istou dierou. Poznamenajme, že tento princíp nedáva nijaký návod ako nájsť dieru používanú viac ako jedným holubom. Preto sa tento princíp často považuje za nekonštruktívny, a teda existenčný.

Medzi dôsledky Dirichletovho princípu patrí aj skutočnosť, že ak konečná množina má m prvkov aj n prvkov, tak $m = n$.

Príklad 3.1. V Bratislave sa v každom okamihu vyskytujú aspoň dvaja ľudia, ktorí majú rovnaký počet vlasov na hlave. Nech A je množina obyvateľov Bratislavy a $B = \{0, 1, \ldots, 200000\}$. Zobrazenie $f : A \to B$ priraďuje bratislavčanovi x jeho počet vlasov $f(x) \in B$ (počet vlasov človeka neprevyšuje 200 000). Keďže $|A| > 200001$, zobrazenie nemôže byť injektívne. Poznamenajme, že toto zobrazenie sa každú chvíľu mení – stačí sa učesať. □

Príklad 3.2. V postupnosti $(a_1, a_2, \ldots, a_n)$ ľubovoľných n prirodzených čísel existuje súvislá podpostupnosť $(a_{k+1}, a_{k+2}, \ldots, a_l)$ taká, že súčet $a_{k+1} + a_{k+2} + \cdots + a_l$ je deliteľný číslom n.

Aby sme sa o tom presvedčili, uvažujme n súčtov $a_1,\ a_1 + a_2, \ldots, a_1 + a_2 + \cdots + a_n$. Ak je medzi nimi niektorý deliteľný číslom n, sme hotoví. Nech preto každý z nich dáva po delení číslom n nenulový zvyšok. Keďže súčtov je n, no možných hodnôt pre zvyšky je len $n - 1$, dva z týchto súčtov povedzme $a_1 + a_2 + \cdots + a_r$ a $a_1 + a_2 + \cdots + a_s$ (pričom $r < s$) dávajú po delení číslom n ten istý zvyšok z. Máme teda

$$\begin{aligned} a_1 + a_2 + \cdots + a_r &= bn + z \\ a_1 + a_2 + \cdots + a_s &= cn + z \end{aligned}$$

pre vhodné $b, c \in \mathbb{Z}$. Odčítaním prvého súčtu od druhého dostávame

$$a_{r+1} + a_{r+2} + \cdots + a_s = (c - b)n,$$

čo znamená, že posledný súčet je deliteľný číslom n. □

Uvedieme ešte silnejšiu formu Dirichletovho princípu:

Teoréma 3.4. *Ak $f\colon A \to B$ je zobrazenie konečných množín také, že $|A| = n$, $|B| = m$ a $n/m > r$ pre nejaké prirodzené číslo r, tak existuje prvok množiny B, na ktorý sa zobrazí aspoň r prvkov množiny A.*

Dôkaz. Nech $B = \{1, 2, \ldots, m\}$ a nech n_i je počet prvkov množiny A, ktoré sa zobrazia na prvok $i \in B$. Keby pre každé z čísel n_i platilo $n_i \leq r$, tak by sme dostali

$$r < \frac{n}{m} = \frac{n_1 + n_2 + \ldots + n_m}{m} \leq \frac{mr}{m} = r.$$

Tento spor dokazuje teorému. □

Poznamenajme, že teoréma 3.3 vyplýva z teorémy 3.4, keď položíme $r = 1$.

3.3 Základné enumeračné pravidlá

Úloha určiť počet kombinatorických konfigurácií daného typu je jednou z najtypickejších kombinatorických úloh. Existuje obrovské množstvo rôznych druhov kombinatorických konfigurácií, keďže existuje nepreberné množstvo praktických úloh kombinatorického charakteru. Veľká väčšina úloh sa však dá zaradiť do jednej z nasledujúcich tried s dvoma podtriedami:

1. Určiť počet *neusporiadaných konfigurácií*, pričom opakovanie objektov v konfiguráciách je alebo nie je povolené.

2. Určiť počet *usporiadaných konfigurácií*, pričom opakovanie objektov v konfiguráciách je alebo nie je povolené.

Čitateľ iste pozná pojem kombinácií, ktorý spadá pod bod A, a pojem variácií, spadajúci pod bod B. Tieto dva pojmy však na riešenie kombinatorických úloh nestačia, pretože konfigurácie môžu kombinovať usporiadané aj neusporiadané črty. Oveľa dôležitejšie je preto ovládať základné enumeračné

pravidlá a ovládnuť umenie „matematizácie“ kombinatorických úloh – čo znamená vedieť vyabstrahovať konfigurácie v podobe podmnožín, usporiadaných k-tic, zobrazení, relácií rozkladov a podobne, a potom na ich zrátanie enumeračné pravidlá použiť.

Prvé z nich je veľmi jednoduché:

Teoréma 3.5 (Pravidlo súčtu)**.** *Nech $X_1,\ X_2, \ldots, X_n,\ n \geq 2$ sú navzájom disjunktné podmnožiny konečnej množiny X, pričom $X = X_1 \cup X_2 \cup \ldots \cup X_n$. Potom*

$$|X| = |X_1| + |X_2| + \cdots + |X_n|.$$

Dôkaz. Nech najprv $n = 2$. Nech $X_1 = \{a_1, a_2, \ldots, a_r\}$ a $X_2 = \{b_1, b_2, \ldots, b_s\}$. Keďže $X_1 \cap X_2 = \emptyset$, platí $X_1 \cup X_2 = \{c_1, c_2, \ldots, c_r, c_{r+1}, \ldots, c_{r+s}\}$, kde $c_i = a_i$ pre $i \in \{1, 2, \ldots, r\}$ a $c_j = b_{j-r}$ pre $j \in \{r+1, \ldots, r+s\}$. Z tohto už ľahko vidno, že $|X| = |X_1 \cup X_2| = |X_1| + |X_2|$. Pre $n \geq 3$ sa dôkaz ľahko dokončí matematickou indukciou. □

Opakovaným použitím tohto pravidla získavame ďalšie pravidlo. Je zložitejšie, no má častejšie použitie.

Teoréma 3.6 (Pravidlo súčinu)**.** *Nech $X_1,\ X_2, \ldots, X_n,\ n \geq 2$, sú ľubovoľné konečné množiny. Potom $|X_1 \times X_2 \times \cdots \times X_n| = |X_1| \cdot |X_2| \cdot \cdots \cdot |X_n|$.*

Dôkaz. Budeme postupovať indukciou vzhľadom na n, pričom v indukčnom kroku použijeme pravidlo súčtu. Tvrdenie teorémy platí aj pre $n = 1$ (ale nič nehovorí) a to využijeme ako bázu indukcie. Nech teraz tvrdenie teorémy platí aj pre nejaké $n \geq 1$. Ukážeme, že platí aj pre $n+1$. Chcem určiť počet prvkov množiny $X_1 \times X_2 \times \cdots \times X_n \times X_{n+1}$. Ak $X_{n+1} = \emptyset$, tak $|X_1 \times X_2 \times \cdots \times X_n \times \times X_{n+1}| = 0 = |X_1| \cdot |X_2| \cdot \cdots \cdot |X_{n+1}|$. V tomto prípade teda tvrdenie platí. Nech preto $|X_{n+1}| = s \geq 1$, pričom $X_{n+1} = \{a_1, a_2, \ldots, a_s\}$. Položme pre každé $i \in \{1, 2, \ldots, s\}$

$$Y_i = X_1 \times X_2 \times \cdots \times X_n \times \{a_i\}.$$

Je zrejmé, že $|Y_i| = |X_1 \times X_2 \times \cdots \times X_n|$ a podľa indukčného predpokladu teda platí

$$|Y_i| = |X_1| \cdot |X_2| \cdot \cdots \cdot |X_n|.$$

Pretože

$$X_1 \times X_2 \times \ldots \times X_n \times X_{n+1} = \bigcup_{k=1}^{s} Y_i$$

a množiny $Y_1, Y_2, \ldots, Y_s$ sú navzájom disjunktné, z pravidla súčtu dostávame

$$|X_1 \times X_2 \times \cdots \times X_{n+1}| = \sum_{k=1}^{s} |Y_k| = |X_1| \cdot |X_2| \cdot \cdots \cdot |X_n| \cdot |X_{n+1}|.$$

□

Príklad 3.3. Koľko štvorciferných čísel deliteľných piatimi môžeme vytvoriť z cifier 0, 1, 3, 5, 7? Nech $M = \{0, 1, 3, 5, 7\}$. Potom každé hľadané číslo je charakterizované usporiadanou štvoricou, ktorá patrí do množiny

$$U = (M - \{0\}) \times M \times M \times \{0, 5\}.$$

Podľa pravidla súčinu dostávame

$$|U| = 4 \cdot 5 \cdot 5 \cdot 2 = 200.$$

Príklad 3.4. Koľkokrát za deň cifry na digitálnych hodinách ukazujú rastúcu postupnosť? Čas na ukazateli digitálnych množín môžeme zakódovať usporiadanou šesticou prirodzených čísel $x = (x_1, x_2; x_3, x_4; x_5, x_6)$. Predpokladajme, že $x_1 < x_2 < \cdots < x_6$. Hoci vo všeobecnosti čas musí spĺňať $x_1 \leq 2$, vidíme, že $x_1 = 2$ by nevyhnutne viedlo k $x_5 \geq 6$, čo nie je možné. Preto $x_1 \in \{0, 1\}$ a $x_5 \leq 5$. Ak $x_1 = 1$, tak $x_5 = 5$ a ak $x_1 = 0$, tak $x_5 = 4$ alebo 5. Množinu X hľadaných postupností rozdelíme takto

$$\begin{aligned} X_1 &= \{x \in X;\ x_1 = 1\}, \\ X_{04} &= \{x \in X;\ x_1 = 0, x_5 = 4\}, \\ X_{05} &= \{x \in X;\ x_1 = 0, x_5 = 5\}. \end{aligned}$$

V prvej množine sú postupnosti tvaru $(1, 2; 3, 4; 5, x_6)$, z čoho vyplýva $|X_1| = 4$. V druhej sú postupnosti tvaru $(0, 1; 2, 3; 4, x_6)$, takže $|X_{04}| = 5$. Počet prvkov množiny $|X_{05}|$ spočítame takto: pre (x_2, x_3, x_4) sú len tieto možnosti: $(1, 2, 3), (1, 2, 4), (1, 3, 4), (2, 3, 4)$. Pre x_6 sú možnosti $6, 7, 8, 9$. Každá postupnosť v X_{05} je charakterizovaná usporiadanou dvojicou $((x_2, x_3, x_4), x_6)$, ktorých je podľa pravidla súčinu $4 \cdot 4 = 16$. Napokon podľa pravidla súčtu dostávame $|X| = |X_1| + |X_{04}| + |X_{05}| = 4 + 5 + 16 = 25$. □

3.4 Variácie

Variácie spolu s kombináciami patria medzi najjednoduchšie a najbežnejšie kombinatorické konfigurácie.Zatiaľ čo variácie sú usporiadané štruktúry, kombinácie sú neusporiadané. Ukazuje sa, že jednoduchšie je začat študium usporiadaných konfigurácií a na neusporiadané sa dívať ako na triedy ekvivalencie usporiadaných štruktúr.

Ako prvý odvodíme výsledok o počte zobrazení medzi konečnými množinami. Pripomeňme označenie z predchádzajúcej kapitoly: pre lubovolné množiny A a B označujeme symbolom B^A množinu všetkých zobrazení $A \to B$.

Teoréma 3.7. *Ak A a B sú konečné množiny, pričom $|A| = n$ a $|B| = m$, tak*

$$\left|B^A\right| = |B|^{|A|} = m^n.$$

Dôkaz. Teorému dokážeme indukciou vzhľadom na n. Pre $n = 0$ (a každé prirodzené číslo $m = |B|$) teoréma platí, lebo $B^\emptyset = \{\emptyset\}$. Predpokladajme teraz, že teoréma platí pre nejaké $n \geq 0$ a všetky prirodzené čísla m. Nech $|A| = n+1$, pričom $A = \{a_1, \ldots, a_n, a_{n+1}\}$. Ak $B = \emptyset$, tak $\emptyset^A = \emptyset$ a tvrdenie platí. Ak $m \geq 1$ a $B = \{b_1, b_2, \ldots, b_m\}$, pre $k \in \{1, 2, \ldots, m\}$ položíme

$$Y_k = \{f \in B^A; f(a_{n+1}) = b_k\}.$$

Množiny Y_k sú navzájom disjunktné a $B^A = \cup_{k=1}^m Y_k$. Okrem toho zúženia zobrazení $f \in Y_k$ na množinu $A - \{a_{n+1}\}$ sú po dvoch rôzne a dávajú všetky zobrazenia $\{a_1, a_2, \ldots, a_n\} \to B$, z indukčného predpokladu dostávame $|Y_k| = m^n$. Napokon

$$\left|B^A\right| = \sum_{k=1}^{m} |Y_k| = m \cdot m^n = m^{n+1} = |B|^{|A|}.$$

□

Pre $A = \{1, 2, \ldots, n\}$ a $|B| = m$ sa prvky množiny B^A nazývajú *variácie s opakovaním* n-tej triedy z m prvkov (množiny B). V súhlase s označením zavedením v článku 2.4 namiesto šípkového označenia pre tieto zobrazenia používame označenie sekvenciálne $f\colon \{1, 2, \ldots, n\} \to B$ označujeme $(f(1), f(2), \ldots, f(n)) = (f_1, f_2, \ldots, f_n)$. Z tohto vyjadrenia je zrejmé, že existuje bijekcia $B^{\{1,2,\ldots,n\}} \to B \times B \times \cdots \times B$ (n-krát) a teda Teoréma 3.7 vyplýva aj priamo z pravidla súčinu.

Napríklad ak $B = \{a, b\}$, tak všetky variácie tretej triedy z množiny B, usporiadané lexikograficky, sú :

$$(a,a,a),\ (a,a,b),\ (a,b,a),\ (a,b,b),\ (b,a,a),\ (b,a,b),\ (b,b,a),\ (b,b,b).$$

Poznámka. Teorémy 3.5-3.7 sú základom definície súčtu, súčinu a mocnenia ľubovolných kardinálnych čísel, ako sme ich zaviedli v článku 2.6. Tieto definície teda zovšeobecňujú našu praktickú skúsenosť z konečných množín na nekonečné množiny ľubovolnej kardinality. □

Teoréma 3.8. *Nech A je konečná množina, $|A| = n$. Potom počet všetkých podmnožín množiny A je $|\mathcal{P}(A)| = 2^n$.*

Dôkaz. Počet podmnožín množiny A je totožný s počtom charakteristických funkcií definovaných na množine A, čiže je rovnaký ako počet zobrazení $A \to \{0, 1\}$. Podľa teorémy 3.7 takých zobrazení je ich 2^n. □

Teraz určíme počet všetkých injektívnych zobrazení medzi dvoma množinami.

Teoréma 3.9. *Nech A a B sú konečné množiny, pričom $|A| = n$ a $|B| = m$. Potom počet všetkých injektívnych zobrazení z A do B je*

$$m \cdot (m-1) \dots (m-n+1) = \prod_{i=0}^{n-1} (m-i)\,.$$

Dôkaz. Nech I_B^A označuje počet injekcií $A \to B$. Budeme postupovať indukciou vzhľadom na n. Ak $A = \emptyset$, tak existuje jediná injekcia $A \to B$. V súčine $\prod_{i=0}^{-1}(m-i)$ máme nulový počet činiteľov, a taký súčin sa definitoricky kladie za 1. Teda v tomto prípade výsledok platí. Predpokladajme, že tvrdenie našej teorémy je správne pre nejaké $n \geq 0$ a pre všetky prirodzené čísla m. Nech $|A| = n + 1$ a nech $A = \{a_1, a_2, \dots, a_n, a_{n+1}\}$. Ak $B = \emptyset$, tak $B^A = \emptyset$ a tvrdenie platí. Nech teda $m \geq 1$ a $B = \{b_1, b_2, \dots, b_m\}$. Definujme teraz pre každé $k \in \{1, 2, \dots, m\}$ množinu

$$Y_k = \{f \in B^A; \quad f \text{ je injektívne a } f(a_{n+1}) = b_k\}.$$

Množiny $Y_1, Y_2, \dots, Y_m$ sú navzájom disjunktné a každá injekcia $A \to B$ patrí do nejakej z nich. Preto $|Y_1| + |Y_2| + \dots + |Y_m| = I_B^A$.

Určíme $|Y_k|$ pre ľubovolné k. Kedže zúžením injekcie je opäť injekcia, zúženia zobrazení $f \in Y_k$ na množinu $A - \{a_{n+1}\}$ sú injekcie $A - \{a_{n+1}\} \to B - \{b_k\}$. Naviac medzi zúženiami sa každá taká injekcia vyskytuje práve raz. Preto

$$|Y_k| = I_{B-\{b_k\}}^{A-\{a_{n+1}\}}.$$

Podľa indukčného predpokladu

$$|Y_k| = \prod_{i=0}^{n-1}(m-1-i) = \prod_{i=1}^{n}(m-i).$$

Odtiaľ vyplýva, že

$$I_B^A = m\prod_{i=1}^{n}(m-i) = \prod_{i=0}^{n}(m-i)$$

□

Všimnime si, že ak $|A| > |B|$, tak Teoréma 3.9 hovorí, že neexistuje žiadna injekcia $A \to B$, čo je obsah teorémy 3.3. Dirichletov princíp je teda dôsledkom teorémy 3.9.

Injekcie z množiny $A = \{1, 2, \ldots, n\}$ do množiny B, kde $|B| = m$, sa nazývajú *variácie (bez opakovania) n-tej triedy* z m prvkov (množiny B).

Na označenie počtu variácií bez opakovania n-tej triedy z m prvkov používame symbol $m^{\underline{n}} = m(m-1)\ldots(m-n+1)$, pričom v súhlase s teorémou 3.9 platia vzťahy $m^{\underline{0}} = 1$ a $m^{\underline{1}} = m$ číslo $m^{\underline{n}}$ sa nazýva *n-tý klesajúci faktoriál z m*. Číslo $m^{\underline{m}} = m(m-1)\cdot\cdots\cdot 2\cdot 1$ sa označuje $m!$ a nazýva sa *m-faktoriál*.

Príklad 3.5. Máme zostaviť vlajku z troch rovnakých vodorovných farebných prvkov, alebo troch rovnakých zvislých prvkov, pričom máme k dispozícii látky n rôznych farieb (v neobmedzenom množstve). Nech H je množina vlajok prvého a V množina vlajok druhého druhu. Zrejme $H \cap V = \emptyset$ a $|H| = |V|$. Každú vlajku z množiny H charakterizuje usporiadaná trojica rôznych farieb, čiže injekcia $\{1, 2, 3\} \to F$, kde F je množina farieb. Z teorémy 3.9 vyplýva, že $|H| = n(n-1)(n-2) = n^{\underline{3}}$, a teda počet rôznych vlajok je $2n^{\underline{3}}$. □

Napríklad variácie bez opakovania druhej triedy z prvkov množiny $B = \{1, 2, 3\}$ sú (v lexikografickom usporiadaní) $(1,2), (1,3), (2,1), (2,3), (3,1), (3,2)$.

Ak $A = \{1, 2, \ldots, n\}$ a $|B| = n$, tak variácie n-tej triedy z n prvkov množiny B nie sú nič iné ako bijekcie $A \to B$ a ich počet je podľa teorémy 3.9 $n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1 = n!$. Tieto variácie sa nazývajú *permutáciami množiny* B. (Niekedy je o permutáciach výhodné predpokladať, že $A = B$.)

Zo zápisu permutácie ako postupnosti, v ktorej sa vyskytujú bez opakovania všetky prvky množiny B je zrejmé, že každá permutácia množiny B určuje nejaké lineárne usporiadanie množiny B. Obrátene, každé lineárne usporiadanie množiny B definuje permutáciu f množiny B – ak $b \in B$ je i-ty najmenší prvok množiny B (t.j. i-ty z ľava), stačí položiť $f(i) = b$.

Teoréma 3.10. *Existuje vzájomne jednoznačná korešpondencia medzi permutáciami ľubovolnej množiny B a lineárnymi usporiadaniami množiny B. Preto počet lineárnych usporiadaní n-prvkovej množiny je $n!$*

Na záver vyslovíme ešte *zovšeobecnené pravidlo súčinu*, ktoré je zosilnením teorémy 3.9. Dôkaz indukciou prenechávame čitateľovi.

Teoréma 3.11. *Nech X je konečná množina. Nech $A \subseteq X^k$, $k \geq 2$, je podmnožina karteziánskeho súčinu X^k, ktorej prvky označíme $(x_1, x_2, \ldots, x_k)$ a ktorá spĺňa podmienky:*

(1) *prvok x_1 je možné z množiny X vybrať n_1 spôsobmi;*

(2) *pre každé $i \in \{1, \ldots, k-1\}$, po akomkoľvek výbere usporiadanej i-tice $(x_1, x_2, \ldots, x_i)$ je možné prvok x_{i+1} vybrať vždy n_{i+1} spôsobmi.*

Potom $|A| = n_1 \cdot n_2 \cdot \cdots \cdot n_k$.

3.5 Kombinácie bez opakovania

Kombinácie bez opakovania sú neusporiadané súbory neopakujúcich sa prvkov – inými slovami podmnožiny nejakej základnej množiny. Presnejšie povedané, *kombinácie (bez opakovania) k-tej triedy z n prvkov* množiny A sú k-prvkové podmnožiny množiny A, ktorej mohutnosť je $|A| = n$. Kombinácie k-tej triedy prvkov množiny A skátene nazývame tiež *k-kombináciami*.

Množina všetkých k-prvkových podmnožín množiny A sa označuje $\mathcal{P}_k(A)$ alebo $\binom{A}{k}$ a ich počet $\binom{n}{k}$. Symbol $\binom{n}{k}$ sa nazýva *kombinačným číslom* alebo *binomickým koeficientom* (dôvody pochopíme neskôr).

Bezprostredne z definície symbolu $\binom{n}{k}$ vyplývajú tieto jeho vlastnosti:

- Pre každé $n \geq 0$ platí $\binom{n}{0} = 1$, lebo každá množina má práve jednu prázdnu množinu.

- Pre každé $n \geq 0$ platí $\binom{n}{n} = 1$, lebo každá n-prvková množina má práve jednu n-prvkovú podmnožinu, totiž samú seba.

- Pre každé $n \geq 0$ platí $\binom{n}{1} = n$, lebo každá n-prvková množina má práve n rôznych 1-prvkových podmnožín.

- Pre každé $k \leq n$ platí $\binom{n}{k} = \binom{n}{n-k}$. Počet k-prvkových podmnožín ľubovoľnej n prvkovej množiny A je ten istý ako počet $(n-k)$-prvkových podmnožín množiny A, lebo zobrazenie $\binom{A}{k} \to \binom{A}{n-k}$, $x \mapsto A - x$ je bijekcia.

- Pre každé $k > n$ platí $\binom{n}{k} = 0$, lebo n-prvková množina nemá podmnožiny s viac ako n prvkami.

Určíme teraz hodnotu symbolu $\binom{n}{k}$.

Teoréma 3.12. *Nech A je konečná množina, pričom $|A| = n$. Potom počet k-kombinácií z množiny A je*

$$|\mathcal{P}_k(A)| = \binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots 1} = \frac{n^{\underline{k}}}{k!}.$$

Dôkaz. Nech $K = \{0, 1, \dots, k-1\}$. Budeme skúmať injekcie $K \to A$, čiže na množine I_A^K. Na I_A^K zavedieme binárnu reláciu R takto:

$$f \ R \ g \text{ práve vtedy, keď } f(\{0, 1, \dots, k-1\}) = g(\{0, 1, \dots, k-1\})$$

Potom R je relácia ekvivalencie. Každá trieda ekvivalencie C na množine I_A^K je jednoznačne určená jednou k-prvkovou podmnožinou M, na ktorú zobrazenia z množiny C zobrazia množinu $\{0, 1, \dots, k-1\}$. Ak v týchto zobrazeniach zameníme koobor A za M, dostaneme práve všetky permutácie množiny M. Preto $|C| = k!$. Každá trieda ekvivalencie na I_A^K má $k!$ prvkov. Preto $k!\binom{n}{k} = = n^{\underline{k}} = I_A^K$. Počet k-prvkových podmnožín množiny A je teda, podľa teorémy 3.9, $\binom{n}{k} = |I_A^K|/k! = n^{\underline{k}}/k!$. □

Kombinačné čísla majú veľké množstvo zaujímavých vlastností. Uvedieme aspoň niektoré z nich.

Teoréma 3.13. *Pre ľubovoľné prirodzené čísla n a k platí:*

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

Dôkaz. Tvrdenie je možné ľahko dokázať pomocou vyjadrenia $\binom{n}{k} = n^{\underline{k}}/k!$ tak, že úpravou vzťahu na ľavej strane dostaneme kombinačné číslo na pravej strane. My však dokážeme túto rovnosť pomocou množinovej interpretácie. Nech A je množina, ktorá má $|A| = n+1$ a nech $b \in A$ je pevný prvok. Množinu $\binom{A}{k+1}$ rozložíme na dve časti B_0 a B_1: B_0 bude združovať $(k+1)$-podmnožiny, ktoré neobsahujú prvok b, naproti tomu B_1 bude združovať všetky tie, ktoré prvok b obsahujú. Keďže každá množina v B_0 je podmnožinou množiny $A - \{b\}$, dostávame $|B_0| = \binom{n}{k+1}$. Každá množina v B_1 zas určuje k-prvkovú podmnožinu množiny $A - \{b\}$. Preto $|B_1| = \binom{n}{k}$. Odtiaľ

$$\binom{n+1}{k+1} = \binom{A}{k+1} = |B_0| + |B_1| = \binom{n}{k+1} + \binom{n}{k}.$$

□

Tento rekurentný vzťah je základom umiestnenia kombinačných čísel v rovine do tvaru trojuholníka, v ktorom je možné postupne vyčísľovať kombinačné čísla s použitím jediného faktu, že $\binom{n}{0} = \binom{n}{n} = 1$ pre každé n.

$$\begin{array}{ccccccc}
 & & \binom{0}{0} & & & & \\
 & \binom{1}{0} & & \binom{1}{1} & & & \\
\binom{2}{0} & & \binom{n}{1} & & \binom{2}{2} & & \\
\binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3}
\end{array}
\qquad
\begin{array}{ccccccc}
 & & 1 & & & & \\
 & 1 & & 1 & & & \\
1 & & 2 & & 1 & & \\
1 & & 3 & & 3 & & 1
\end{array}$$

Príklad 3.6. Majme domino (variant známej spoločenskej hry), ktorého každý kameň je rozdelený na dve časti a na každej polovici je vyznačená jedna z hodnôt $0, 1, \ldots, n$; žiadna z dvoch častí sa nedá odlíšiť ako prvá alebo druhá. Aká je pravdepodobnosť toho, že dva náhodne vybrané kamene sa dajú k sebe priložiť, čiže obsahujú rovnakú hodnotu aspoň na jednej strane? (Poznamenajme, že bežné domino má $n = 6$.) Kameň, na ktorom sú napísané hodnoty $i, j \in\in \{0, 1, \ldots, n\}$, môžeme jednoznačne zakódovať množinou $\{i, j\}$. Keďže sa môže stať, že $i = j$ (takým kameňom sa hovorí dublety),

máme $1 \leq |\{i,j\}| \leq 2$. Celkový počet kameňov je teda $\binom{n+1}{1} + \binom{n+1}{2} = \binom{n+2}{2}$, podľa teorémy 3.13. Špeciálne pre $n = 6$ dostávame $\binom{8}{2} = 28$. Počet všetkých možných výberov dvoch kameňov je potom

$$\binom{\binom{n+2}{2}}{2} = \frac{1}{2}\binom{n+2}{2}\left(\binom{n+2}{2} - 1\right).$$

Určíme teraz počet dvojíc kameňov, ktoré sa daju priložiť k sebe. Toto číslo je zhodné s počtom neusporiadaných dvojíc množín $\{i,j\}, \{k,l\} \in \mathcal{P}_1(\{0,1,\ldots,n\}) \cup \mathcal{P}_2(\{0,1,\ldots,n\})$ takých, že $\{i,j\} \cap \{k,l\} \neq \emptyset$. Pre každé $i \in \{0,1,\ldots,n\}$ zistíme, aký je počet dvojíc kameňov, ktoré majú spoločnú hodnotu i. Všimnime si, že okrem hodnoty i sa na týchto kameňoch objavujú ešte dve ďalšie hodnoty j a k, pričom $j \neq k$; môže sa však stať, že jedna z týchto hodnôt je totožná s i. Z tohto je jasné, že každú dvojicu kameňov so spoločnou hodnotou i môžeme jednoznačne reprezentovať dvojprvkovou množinou $\{j,k\}$. Takto dostávame $\binom{n+1}{2}$ dvojíc kameňov so spoločnou hodnotou i. Vzhľadom na počet výberov hodnoty i, dostávame $(n+1)\binom{n+1}{2}$ dvojíc kameňov domina, ktoré sa dajú priložiť k sebe. Z toho vyplýva, že pravdepodobnosť javu, že pri náhodnom výbere dvojice kameňov je možné tieto kamene priložiť k sebe, je

$$\frac{(n+1)\binom{n+1}{2}}{\binom{\binom{n+2}{2}}{2}} = \frac{2(n+1)\binom{n+1}{2}}{\binom{n+2}{2}\left(\binom{n+2}{2} - 1\right)}.$$

Pre bežné domino ($n = 6$) dostávame pravdepodobnosť $7/18 < 0{,}4$. □

Dôležitým výsledkom o kombinačných číslach je nasledujúca teoréma, ktorá vysvetľuje, prečo kombinačné čísla nazývajú aj binomické koeficienty.

Teoréma 3.14 (Binomická veta)**.** *Pre každé reálne číslo x a prirodzené číslo n platí*

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

Dôkaz. Tvrdenie zrejme platí pre $n = 0$. Ďalej budeme postupovať indukciou vzhľadom na n. Ak predpokladáme platnosť tvrdenia pre nejaké $n \geq 0$, tak použitím tvrdenia 3.13 dostávame:

$$\begin{aligned}(1+x)^{n+1} &= (1+x)^n(1+x)\\ &= \left(\sum_{k=0}^{n}\binom{n}{k}x^k\right)(1+x)\\ &= 1+\left(\binom{n}{0}+\binom{n}{1}\right)x+\left(\binom{n}{1}+\binom{n}{2}\right)x^2+\dots\\ &\quad+\left(\binom{n}{n-1}+\binom{n}{n}\right)x^n+x^{n+1}\\ &= \sum_{k=0}^{n+1}\binom{n+1}{k}x^k\end{aligned}$$

čo bolo treba dokázať. □

Poznámka. Definíciu binomického koeficientu $\binom{n}{k}$ môžeme rozšíriť z prirodzeného čísla n na ľubovoľné reálne číslo z, ak na základ jeho rozšírenia zoberieme teorému 3.12.

Položme

$$\binom{z}{k} := \frac{z^{\underline{k}}}{k!} = \frac{z(z-1)\dots(z-k+1)}{k!}.$$

Pre takéto binomické koeficienty je možné dokázať analóg binomickej teorémy, ktorý v tomto prípade vyzerá takto:

Pre ľubovoľné $z \in \mathbb{R}$ a pre každé reálne číslo z také, že $|x| < 1$ platí

$$(1+x)^z = \sum_{k=0}^{\infty}\binom{z}{k}x^k.$$

Ak $z \in \mathbb{N}$, tak všetky binomické koeficienty pre $k > z$ sú nulové a dostávame opäť tvrdenie teorémy 3.14 (pre $|x| < 1$, čo nie je až také podstatné). Takáto rozšírená binomická teoréma je užitočná pri dokazovaní rozličných vlastností kombinačných čísel. Dôkaz zovšeobecnenej binomickej teorémy presahuje rámec tohto textu. □

Dôsledok 3.15. *Platia tieto identity* ($n \geq 1$)

(a) $\sum_{k=0}^{n} \binom{n}{k} = 2^n,$

(b) $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0,$

(c) $\sum_{\substack{0\le k\le n,\\ k\ párne}} \binom{n}{k} = \sum_{\substack{0\le k\le n,\\ k\ nepárne}} \binom{n}{k} = 2^{n-1}.$

Dôkaz. Tvrdenie (a) dostaneme priamo z binomickej teorémy, ak položíme $x = 1$ a (b) dostaneme, ak položíme $x = -1$.

Jednu z rovností v (c) dostaneme, ak sčítame identity (a) a (b) a vydelíme dvoma, druhú rovnosť získame podobne odčítaním.

Identitu (a) môžeme ľahko dokázať aj kombinatorickou úvahou: na pravej strane máme 2^n, čo je $|\mathcal{P}(A)|$, kde $|A| = n$. To isté číslo môžeme vyjadriť aj v tvare súčtu

$$|\mathcal{P}(A)| = \sum_{k=0}^{n} |\mathcal{P}_k(A)|.$$

□

Teoréma 3.16 (Cauchyho sčítací vzorec)**.** *Pre všetky prirodzené čísla m a n platí*

$$\sum_{i=0}^{k} \binom{m}{i} \binom{n}{k-i} = \binom{m+n}{k}.$$

Dôkaz. Nech A_1 a A_2 sú disjunktné množiny, pričom $|A_1| = m$ a $|A_2| = n$. Položme $A = A_1 \cup A_2$. Nech $X \subseteq A$. Potom $X \cap A = X \cap (A_1 \cup A_2) = = (X \cap A_1) \cup (X \cap A_2)$. Označme $X_i = X \cap A_i, i = 1, 2, \ldots$. Potom X_1 a X_2 sú disjunktné podmnožiny A_1 resp. A_2 a $X = X_1 \cup X_2$.

Skúmajme zobrazenie

$$f\colon \mathcal{P}_k(A) \to \cup_{i=0}^{k} (\mathcal{P}_i(A_1) \times \mathcal{P}_{k-i}(A_2)),$$
$$x \mapsto (x_1, x_2).$$

Keďže každú podmnožinu X možeme vyjadriť ako zjednotenie množiny $X_1 == X \cap A_1$ s množinou $X_2 = X \cap A_2$, vidíme, že zobrazenie f je bijektívne. Z teorémy 3.12 a pravidla súčinu vieme, že $|\mathcal{P}_i(A_1) \times \mathcal{P}_{k-i}(A_2)| = \binom{m}{i}\binom{n}{k-i}$.

Požitím pravidla súčtu napokon dostávame

$$\binom{m+n}{k} = |\mathcal{P}_k(A)| = |\cup_{i=0}^{k} \mathcal{P}_i(A_1) \times \mathcal{P}_{k-1}(A_2)| = \sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i}.$$

Tým je dôkaz skončený. □

Poznámka. Tvrdenie 3.16 môžeme dokázať aj pomocou binomickej teorémy takto. Zrejme platí $(1+x)^{m+n} = (1+x)^m(1+x)^n$. Ak rozpíšeme pravú aj ľavú stranu tejto rovnosti podľa teorémy 3.14, dostáneme

$$\sum_{k=0}^{m+n} \binom{m+n}{k} x^k = \left(\sum_{i=0}^{m} \binom{m}{i} x^i\right)\left(\sum_{j=0}^{n} \binom{n}{j} x^j\right).$$

Súčty na pravej strane roznásobíme podľa distributívneho zákona a roztriedime podľa mocnín premennej x. Zistíme, že pri x^k sa vyskytuje koeficient

$$\sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i}.$$

Na ľavej strane sa pri x^k vyskytuje koeficient $\binom{m+n}{k}$. Keďže dva mnohočleny sa rovnajú práve vtedy, keď pri rovnakých mocninách premennej sa vyskytujú rovnaké koeficienty, musí platiť

$$\sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i} = \binom{m+n}{k}.$$

□

Rovnakou metódou je možné dokázať celý rad ďalších identít-vzťahov medzi kombinačnými číslami. Čitateľ si môže sám vyskúšať, aká identita vyplýva zo vzťahu $(1+x)^{n+1} = (1+x)^n(1+x)$. Na záver tohto článku sa pozrieme na číslo $\binom{n}{k}$ ako na funkciu premennej k pri pevnom n.

Teoréma 3.17. *Pre každé prirodzené číslo n platí:*

(a) ak n je párne, tak

$$\binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{n/2-1} < \binom{n}{n/2} > \binom{n}{n/2+1} > \cdots > \binom{n}{n};$$

(b) ak n je nepárne, tak

$$\binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{(n-1)/2} = \binom{n}{(n+1)/2} > \cdots > \binom{n}{n-1} > \binom{n}{n}.$$

Dôkaz. Skúmajme pomer

$$\frac{\binom{n}{k}}{\binom{n}{k-1}} = \frac{n^{\underline{k}}}{k!}\frac{(k-1)!}{n^{\underline{k-1}}} = \frac{n-k+1}{k}.$$

Ľahko zistíme, že pre $k \leq n/2$ je tento pomer väčší ako 1, a teda $\binom{n}{k} > \binom{n}{k-1}$. Ak n je nepárne, z rovnosti $\binom{n}{k} = \binom{n}{n-k}$ dostávame rovnosť $\binom{n}{(n-1)/2} = \binom{n}{(n+1)/2}$. Odtiaľ už vyplýva tvrdenie. □

Z tohto tvrdenia vyplýva, že funkcia $\binom{n}{k}$ nadobúda svoju najväčšiu hodnotu v strede celočíselneho intervalu $\langle 0, n\rangle$, pričom ak n je párne, táto hodnota sa nadobúda raz, ak n je nepárne – dvakrát. Po túto hodnotu funkcia $\binom{n}{k}$ rastie, od nej potom klesá.

3.6 Kombinácie s opakovaním, permutácie s opakovaním, polynomická veta

Najprv sa budeme venovať kombináciám s opakovaním. Z názvu týchto konfigurácií vyplýva, že ide o konfigurácie, v ktorých sa nerozlišuje poradie, no prvky sa môžu opakovať. Pri ich presnej definícii budeme vychádzať z variácií s opakovaním, teda zobrazení $\{1, 2, \ldots, k\} \to \boldsymbol{A}$. Všimnime si najprv, že na množine $\boldsymbol{A}^{\{1,2,\ldots,k\}}$ všetkých variácií s opakovaním k-tej triedy v množine B

môžeme zaviesť reláciu ekvivalencie R takto: Nech $f, g \in \boldsymbol{A}^{\{1,2,\ldots,k\}}$. Položme fRg práve vtedy, keď $|f^{-1}(\{x\})| = |g^{-1}(\{x\})|$ pre každý prvok $x \in \boldsymbol{A}$.

Inými slovami, dve variácie s opakovaním budú ekvivalentné práve vtedy, keď v oboch sa rovnaké prvky opakujú rovnaký počet krát.

Kombinácie s opakovaním k-tej triedy z m prvkov množiny $\boldsymbol{A}$ (kde $|\boldsymbol{A}| = m$) definujeme ako triedy ekvivalencie R na množine $\boldsymbol{A}^{\{1,2,\ldots,k\}}$.

Ako príklad uvedieme vyššie definovanú ekvivalenciu R na množine $\{a, b\}^{\{1,2,3,4\}}$. Triedy tejto ekvivalencie budú kombinácie s opakovaním štvrtej triedy v množine $\{a, b\}$. Variácie patriace do tej istej triedy rozkladu sú uvedené v tom istom stĺpci. Vnútri každej triedy sú variácie zobrazené lexikograficky. Variácie sú napísané ako slová-bez zátvoriek a čiarok.

aaaa	*aaab*	*aabb*	*abbb*	*bbbb*
	aaba	*abab*	*babb*	
	abaa	*abba*	*bbab*	
	baaa	*baab*	*bbba*	
		baba		
		bbaa		

Počet kombinácií s opakovaním štvrtej triedy z dvoch prvkov je teda 5.

Teoréma 3.18. *Nech* $\boldsymbol{A}$ *je n-prvková množina a k prirodzené číslo. Potom počet všetkých kombinácií s opakovaním k-tej triedy v množine* $\boldsymbol{A}$ *je*

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

Dôkaz. Kombinácie s opakovaním k-tej triedy v množine $\boldsymbol{A}$ sú prvky rozkladu množiny $\boldsymbol{A}^{\{1,2,\ldots,k\}}$ indukovaného reláciou ekvivalencie R popísanej vyššie. Bez ujmy na všeobecnosti môžeme predpokladať, že $\boldsymbol{A} = \{1, 2, \ldots, n\}$. Z každej triedy ekvivalencie R, čiže kombinácie s opakovaním, vyberieme slovo, ktoré je lexikograficky najmenšie (to znamená, že v ňom sú prvky množiny $\boldsymbol{A}$ zoradené podľa veľkosti). S trochou nepresnosti budeme toto slovo stotožňovať so samotnou kombináciou s opakovaním. Nech $c_1c_2 \cdots c_k$ je teda kombinácia s opakovaním k-tej triedy v množine $\boldsymbol{A} = \{1, 2, \ldots, n\}$, pričom $c_1 \leq c_2 \leq \ldots \leq c_k$. Priraďme teraz tejto postupnosti novú postupnosť $d_1d_2 \cdots d_k$ tak, že položíme

$$f(c_i) = d_i = c_i + i - 1, \quad i = 1, 2, \ldots, k.$$

Všimnime si, že $d_i \in \{1, 2, \ldots, n+k-1\}$ a že $d_1 < d_2 < \ldots < d_k$, teda postupnosť $d_1 d_2 \ldots d_k$ reprezentuje kombináciu bez opakovania k-tej triedy z množiny $\{1, 2, \ldots, n+k-1\}$. Napríklad ak $c_1 c_2 \ldots c_k = 22233$, tak $d_1 d_2 \ldots d_k = 23467$.

Ľahko vidieť, že zobrazenie $c_1 c_2 \ldots c_k \longmapsto d_1 d_2 \ldots d_k$ je injektívne. Na druhej strane ak $\{e_1, e_2, \ldots e_k\} \subseteq \{1, 2, \ldots, n+k-1\}$ je kombinácia bez opakovania k-tej triedy, môžeme predpokladať, že $e_1 < e_2 < \ldots < e_k$. Postupnosti $e_1 e_2 \ldots e_k$ priradíme postupnosť $h_1 h_2 \ldots h_k$ takto:

$$h_i = e_i - i + 1, \quad i = 1, 2, \ldots, k.$$

Ľahko vidno, že $h_1 \leq h_2 \leq \ldots \leq h_k$ a že $h_i \in \{1, 2, \ldots, n\}$. Teda $h_1 h_2 \ldots h_k$ je kombinácia s opakovaním k-tej triedy z množiny $\boldsymbol{A}$. Okrem toho, $f(h_i) = e_i$. Z uvedeného vyplýva, že zobrazenie

$$c_1 c_2 \ldots c_k \longmapsto d_1 d_2 \ldots d_k$$

definuje bijekciu medzi kombináciami k-tej triedy s opakovaním v množine $\{1, 2, \ldots, n\}$ a kombináciami bez opakovania k-tej triedy v množine $\{1, 2, \ldots, n+k-1\}$. Hľadaný počet kombinácií s opakovaním je preto

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

□

Príklad 1. Uvažujme polynómy s viacerými premennými $x_1, x_2, \ldots, x_n$. Polynómy vytvárame z členov tvaru $x_{i_1}^{\alpha} x_{i_2}^{\beta} \ldots x_{i_l}^{\gamma}$, kde $\alpha > 0, \beta > 0, \ldots, \gamma > 0$, ktoré sa nazývajú monómy. Stupeň monómu je číslo $\alpha + \beta + \ldots + \gamma$ (v zápise automaticky predpokladáme, že $i_1, i_2, \ldots, i_l$ sú rôzne prvky množiny $\{1, 2, \ldots, n\}$). Polynóm je tvaru

$$\sum_{l=0}^{n} \sum_{i_1 < i_2 < \ldots < i_l} a_{i_1 i_2 \ldots i_l} x_{i_1}^{\varrho} x_{i_2}^{\sigma} \ldots x_{i_l}^{\tau}$$

pričom koeficienty $a_{i_1 i_2 \ldots i_l}$ sú nejaké čísla (môžu byť aj nuly) a $\varrho, \sigma, \ldots, \tau$ sú kladné exponenty (v rôznych monómoch môžu byť rôzne). Poznamenávame, že vo vnútornej sume sčítame cez všetky kombinácie l-tej triedy z množiny $\{1, 2, \ldots, n\}$.

Koľko je rozličných monómov stupňa k? Ak premenné $x_1, x_2, \ldots, x_n$ medzi sebou komutujú, tak na poradí nezáleží a exponent nad premennou vyjadruje počet opakovaní premennej v monóme – ide teda o kombinácie s opakovaním. Preto sa počet rôznych monómov stupňa k rovná číslu

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

Ak premenné medzi sebou nekomutujú, na poradí záleží, a potom máme dočinenia s variáciami s opakovaním. V tomto prípade je počet monómov n^k. □

Príklad 2. Turista chce z dovolenky poslať k priateľom pohľadnice. Má na výber n druhov pohladníc. Koľkými spôsobmi môže nakúpiť k pohladníc? Koľkými spôsobmi môže nakúpené pohľadnice poslať?

Je očividné, že nakúpené pohľadnice tvoria neusporiadaný súbor a že môžeme z jedného druhu kúpiť viacero kusov pohľadníc (ak $k > n$, zrejme ani inú možnosť nemá). Súbory pohľadníc preto tvoria kombinácie s opakovaním. To znamená, že na nákup má

$$\binom{n+k-1}{k}$$

možností.

Koľkými spôsobmi môže pohľadnice poslať? Keby boli všetky pohľadnice navzájom rôzne, tak pohľadnice sa dajú rozoslať $k!$ spôsobmi, lebo rozoslanie predstavuje bijekciu medzi rôznymi druhmi pohľadníc a ich adresátmi. Ak je však z nejakého druhu viac pohľadníc, tieto sú medzi sebou zameniteľné. Predpokladajme, že v nakúpenom súbore je k_i pohľadníc i-teho druhu, $i = 1, 2, \ldots\ldots, n$ $(k_i \geq 0)$. Dve bijekcie z množiny nakúpených pohľadníc do množiny priateľov budeme považovať za ekvivalentné, ak v obidvoch ten istý adresát dostane ten istý druh pohľadnice. Ak uvažujeme ľubovoľnú pevnú bijekciu, zámenou pohľadníc v i-tom druhu dostaneme z nej $k_i!$ ekvivaletných bijekcií. Tieto zámeny môžeme vykonať nezávisle v každom druhu. Podľa pravidla súčinu dostávame, že každá trieda ekvivalencie má $k_1!k_2! \ldots k_n!$ prvkov. Počet spôsobov rozoslania pohľadníc je teda

$$\frac{k!}{k_1!k_2! \ldots k_n!}.$$

□

V predchádzajúcom príklade sme skúmali vlastne takúto všeobecnú situáciu. Máme dve množiny A (pohľadnice) a B (priatelia), pričom $|A| = k = |B|$. Množina A je rozložená na množiny $A_1, A_2, \ldots, A_n$ s mohutnosťami $|A_i| = k_i$. V tomto mieste môžeme trocha porušiť definíciu rozkladu v tom, že pripustíme medzi množinami $A_1, A_2, \ldots, A_n$ aj prázdne množiny. Skúmame teraz bijekcie $A \to B$, pričom dve bijekcie f a g budeme považovať za ekvivalentné, ak pre každý prvok $y \in B$ existuje index $i \in \{1, 2, \ldots, n\}$ taký, že obidva prvky f^{-1} aj g^{-1} patria do tej istej množiny A_i. (V reči predchádzajúceho príkladu: každý adresát y dostal pri rozosielke f aj pri rozosielke g pohľadnicu toho istého druhu – hoci možno nie tú istú). Táto vlastnosť sa dá vyjadriť aj ináč. Nech
$p : A \to \{A_1, A_2, \ldots, A_n\}$ je projekcia množiny na svoj rozklad; to znamená, že pre ľubovoľný prvok $a \in A$ platí $p(a) = A_i$ práve vtedy, keď $a \in A_i$. Potom f aj g sú ekvivalentné vtedy a len vtedy, keď $pf^{-1} = pg^{-1}$. Triedy ekvivalencie týchto bijekcií sa nazývajú *permutáciami s opakovaním* z k_1 prvkov prvého druhu, k_2 prvkov druhého druhu, ..., k_n prvkov n-tého druhu. Úvahou v predchádzajúcom príklade sme ukázali, že počet takýchto permutácií s opakovaním je

$$\frac{k!}{k_1!k_2!\ldots k_n!}.$$

Tá istá hodnota sa objavuje aj ako počet iných konfigurácií.

Tvrdenie 3.19. *Nech A a B sú konečné množiny, kde $|A| = n$ a $|B| = k$. Nech $B = \{b_1, b_2, \ldots, b_k\}$. Potom počet zobrazení $f : A \to B$ takých, že pre každý prvok b_i platí $|f^{-1}(\{b_i\})| = n_i$, kde n_i sú zadané nezáporné celé čísla so súčtom $n_1 + n_2 + \ldots + n_k = n$, sa rovná*

$$\frac{n!}{n_1!n_2!\ldots n_k!}.$$

Dôkaz. Nech $(a_{i_1}, a_{i_2}, \ldots, a_{i_n})$ je ľubovoľná permutácia množiny A zakódovaná ako usporiadanie. Definujme zobrazenie $A \to B$ tak, že prvých n_1 prvkov množiny A pošleme na b_1, druhých n_2 prvkov na b_2 atď. Prvých n_1 prvkov môžeme však ľubovoľne spermutovať a zobrazenie sa nezmení. Nezávisle môžeme permutovať aj ďalšie skupiny. Z toho dostaneme, že $k_1!k_2!\ldots k_n!$ permutácií dáva to isté zobrazenie. Je tiež zrejmé, že každé zobrazenie také, že $|f^{-1}(\{b_i\})| == m_i$ pre každý prvok $b_i \in B$, vznikne hore uvedeným spôsobom. Preto počet týchto zobrazení je $\dfrac{n!}{n_1!n_2!\ldots n_k!}$. □

Čísla $\dfrac{n!}{n_1!n_2!\dots n_k!}$ sa zvyknú označovať $\binom{n}{n_1, n_2, \dots, n_k}$ a nazývať *polynomické koeficienty*. Ak $k = 2$, tak

$$\binom{n}{n_1, n_2} = \binom{n}{n_1} = \binom{n}{n - n_1} = \binom{n}{n_2},$$

čiže polynomické koeficienty sú prirodzeným zovšeobecnením binomických koeficientov. Vysvetlenie názvu týchto čísel poskytuje nasledujúci výsledok.

Teoréma 3.20 (Polynomická veta)**.** *Nech n a k sú kladné prirodzené čísla. Potom*

$$(x_1 + x_2 + \ldots + x_k)^n = \sum_{n_1, n_2, \dots, n_k} \binom{n}{n_1, n_2, \dots, n_k} x_1^{n_1} x_2^{n_2} \dots x_k^{n_k}, \quad n_i \geq 0$$

pričom sčítame cez všetky usporiadané n-tice prirodzených čísel $(n_1, n_2, \dots, n_k)$, pre ktoré $n_1 + n_2 + \ldots + n_k = n$.

Dôkaz. Vynásobme n činiteľov $(x_1 + x_2 + \ldots + x_k)$ a združme rovnaké monómy. Koeficient pri $x_1^{n_1} x_2^{n_2} \dots x_k^{n_k}$ je pritom počet spôsobov, ktorými sa tento monóm pri vynásobení získa. Zrejme $\boldsymbol{M} = x_1^{n_1} x_2^{n_2} \dots x_k^{n_k}$ vznikne vždy, keď x_1 vyberieme z n_1činiteľov, x_2 z n_2 činiteľov atď. Inými slovami, výraz $\boldsymbol{M}$ zodpovedá zobrazeniu z množiny n činiteľov do množiny $x_1, x_2, \dots, x_k$ pričom n_1 činiteľov je zobrazených na x_1, n_2 činiteľov na x_2 atď. Počet takýchto zobrazení je podľa tvrdenia 2.18

$$\frac{n!}{n_1!n_2!\dots n_k!} = \binom{n}{n_1, n_2, \dots, n_k}.$$

□

Poznámka. Ľahko sa nahliadne,že

$$\binom{n}{n_1, n_2, \dots, n_k} = \binom{n}{n_1}\binom{n - n_1}{n_2} \dots \binom{n - n_1 - n_2 - \ldots - n_{k-1}}{n_k}.$$

Táto rovnosť zodpovedá skutočnosti, že počet spôsobov, ktorými vznikne monóm $x_1^{n_1} x_2^{n_2} \dots x_k^{n_k}$, sa dá popísať aj takto: najprv vyberieme x_1 z n_1 členov $(x_1 + x_2 + \ldots + x_n)$, čo môžeme urobiť $\binom{n}{n_1}$ spôsobmi. Potom vyberieme x_2 z n_2 spomedzi zvyšných $n - n_1$ členov, čo môžeme urobiť $\binom{n-n_1}{n_2}$ spôsobmi,

atď. kým nevyberieme aj x_k z n_k spomedzi ostávajúcich $n-n_1-n_2\ldots-n_{k-1}$ členov, čo môžeme urobiť $\binom{n-n_1-n_2-\ldots-n_{k-1}}{n_k}$ spôsobmi. Toto vyjadrenie nie je jednoznačné, keďže poradie čísel $n_1, n_2 \ldots n_k$ môžeme ľubovoľne meniť. □

3.7 Princíp zapojenia a vypojenia

Začneme jednoduchou otázkou. Ak sú dané dve konečné množiny A a B, ako vypočítame počet prvkov ich zjednotenia? Odpoveď je očividná: od súčtu mohutností množín A a B musíme odrátať mohutnosť ich prieniku. Inými slovami,

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

Pre tri množiny je odpoveď podobná:

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

To znamená, že najprv „zapojíme“ prvky jednotlivých množín, potom „vypojíme“ prvky prienikov dvojíc množín a napokon opäť „zapojíme“ prvky prieniku všetkých troch množín. (Čitateľovi odporúčame presvedčiť sa o platnosti tohto vzťahu s pomocou Vennovho diagramu pre tri prenikajúce sa množiny.)

Princíp *zapojenia a vypojenia* (alebo *inklúzie a exklúzie*) je ďalekosiahlym zavšeobecnením vyššie uvedených vzťahov pre dve a tri množiny.

Nech $M_1, M_2, \ldots, M_n$ sú konečné množiny. Pre ľubovoľné prirodzené číslo k také, že $0 \leq k \leq n$ položme

$$S_k = \sum_{i_1<i_2<\ldots<i_k} |M_{i_1} \cap M_{i_2} \cap \ldots \cap M_{i_k}|,$$

pričom súčet prebieha cez všetky kombinácie $\{i_1, i_2, \ldots, i_k\}$ z indexov $\{1, 2, \ldots, n\}$. Pre $k = 0$ dostávame prienik množín M_i z prázdnej množiny indexov, čo podľa dohody z prvej kapitoly je univerzum – základná množina X, v ktorej vedieme všetky úvahy o množinách $M_1, M_2, \ldots, M_n$. Preto

$$S_0 = |X|.$$

Teoréma 3.21 (Princíp zapojenia a vypojenia)**.** *Nech $M_1, M_2, \ldots, M_n$ sú konečné množiny. Potom*

$$\begin{aligned} |M_1 \cup M_2 \cup \ldots \cup M_n| &= \sum_{k=1}^{n} (-1)^{k+1} \sum_{i_1<i_2<\ldots<i_k} |M_{i_1} \cap M_{i_2} \cap \ldots \cap M_{i_k}| = \\ &= \sum_{k=1}^{n} (-1)^{k+1} S_k \end{aligned}$$

Dôkaz. Nech x je ľubovoľný prvok z množiny $M_1 \cup M_2 \cup \ldots \cup M_n$. Zaveďme označenie

$$J_x = \{i;\ x \in M_i\}.$$

Aby sme ukázali, že pravá a ľavá strana rovnosti predstavujú to isté číslo, všimnime si, že prvok x je na ľavej strane zarátaný iba raz. Ak totiž preberáme prvky množiny $M_1 \cup M_2 \cup \ldots \cup M_n$, na x naďabíme len raz. Koľkokrát je započítaný na pravej strane?

Predpokladajme, že prvok x patrí do p množín M_i; to znamená, že $J_x = \{j_1, j_2, \ldots, j_p\} \subseteq \{1, 2, \ldots, n\}$. Z toho vyplýva, že v S_1 je prvok x zarátaný $p = \binom{p}{1}$-krát, totiž raz v každom sčítanci $|M_{j_1}|, |M_{j_2}|, \ldots, |M_{j_p}|$. V S_2 je x zarátaný $\binom{p}{2}$-krát, raz za každý sčítanec tvaru $|M_{j_i} \cap M_{j_2}|$. Všeobecne – prvok x je zarátaný v S_i $\binom{p}{i}$-krát. Celkove je teda prvok x na pravej strane započítaný toľkokrát:

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

Podľa dôsledku 2.14(b) dostávame

$$\binom{p}{0} - \sum_{k=0}^{p} (-1)^k \binom{p}{k} = 1 - 0 = 1,$$

čiže prvok x je aj na pravej strane zarátaný práve raz. To dokazuje našu teorému. □

Poznámka. Teorému 2.20 môžeme ľahko dokázať aj matematickou indukciou. Najprv sa presvedčíme o platnosti vzťahu pre dve množiny M_1 a M_2.

Nech je vzťah platný pre $n \geq 2$ množín. Zoberme teraz $n+1$ množín $M_1, M_2, \ldots, M_n, M_{n+1}$. Na hľadaný počet $|M_1 \cup M_2 \cup \ldots \cup M_n \cup M_{n+1}|$ použime vzťah pre dve množiny:

$$|M_1 \cup M_2 \cup \ldots \cup M_n \cup M_{n+1}| = |(M_1 \cup M_2 \cup \ldots \cup M_n) \cup M_{n+1}| = \\ = \left|\bigcup_{k=1}^{n} M_k\right| + |M_{n+1}| - \left|\left(\bigcup_{k=1}^{n} M_k\right) \cap M_{n+1}\right|.$$

Na tretí sčítanec aplikujeme distributívny zákon, čím dostaneme

$$\left|\left(\bigcup_{k=1}^{n} M_k\right) \cap M_{n+1}\right| = \left|\bigcup_{k=1}^{n} (M_k \cap M_{n+1})\right|.$$

Potom použijeme indukčný predpoklad na prvý a tretí sčítanec, keďže v obidvoch výrazoch vystupuje už zjednotenie n množín. Po úprave dostaneme požadovaný vzťah pre $n+1$. Podrobnosti prenechávame na čitateľa. □

Predpokladajme teraz, že množiny $\boldsymbol{M}_1, \boldsymbol{M}_2, \ldots, \boldsymbol{M}_n$ sú podmnožinami nejakej konečnej množiny $\boldsymbol{X}$. Aký počet má komplement množiny $\boldsymbol{M}_1 \cup \boldsymbol{M}_2 \cup \ldots \cup \boldsymbol{M}_n$ v univerze $\boldsymbol{X}$?

Počítajme

$$|\boldsymbol{X} - (\boldsymbol{M}_1 \cup \boldsymbol{M}_2 \cup \ldots \cup \boldsymbol{M}_n)| = |\boldsymbol{X}| - |\boldsymbol{M}_1 \cup \boldsymbol{M}_2 \cup \ldots \cup \boldsymbol{M}_n| \\ = |\boldsymbol{X}| - \sum_{k=1}^{n} (-1)^{k+1}\ S_k = |\boldsymbol{X}| + \sum_{k=1}^{n} (-1)^k\ S_k \\ = \sum_{k=0}^{n} (-1)^k\ S_k.$$

Tým sa dostali k nasledujúcemu výsledku:

Dôsledok 3.22. *Nech $\boldsymbol{M}_1, \boldsymbol{M}_2, \ldots, \boldsymbol{M}_n$ sú podmnožiny konečnej množiny $\boldsymbol{X}$ a nech $\boldsymbol{M}_i'$ je komplement množiny $\boldsymbol{M}_i$ v univerze $\boldsymbol{X}$, $i = 1, 2, \ldots, n$. Potom*

$$|\boldsymbol{M}_1' \cap \boldsymbol{M}_2' \cap \ldots \cap \boldsymbol{M}_n'| = \sum_{k=0}^{n} (-1)^k\ S_k$$

Dôkaz. Výsledok vyplýva z predchádzajúceho výpočtu a z jedného z de Morganových zákonov. □

Predchádzajúci výsledok je základom najpoužívanejšej formy princípu zapojenia a vypojenia, ktorú teraz opíšeme.

Majme nejakú základnú množinu $\boldsymbol{X}$, pričom $|\boldsymbol{X}| = N$ a nech $\alpha_1, \alpha_2, \ldots, \alpha_n$ sú nejaké vlastnosti, ktoré prvky množiny môžu, no nemusia mať. Nech $N\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k}$ je počet prvkov množiny $\boldsymbol{X}$, ktoré majú každú z vlastností $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k}$ (a prípadne aj iné vlastnosti, no tie nás nezaujímajú). Nech $N(0) = N\alpha'_1\alpha'_2\ldots\alpha'_n$ označuje počet prvkov množiny $\boldsymbol{X}$, ktoré nemajú žiadnu z vlastností $\alpha_1, \alpha_2, \ldots, \alpha_n$. Naším cieľom je vypočítať $N(0)$.

Položme

$$\boldsymbol{M}_i = \{x \in \boldsymbol{X};\ x \text{ má vlastnosť } \alpha_i\}.$$

Potom

$$|\boldsymbol{M}_{i_1} \cap \boldsymbol{M}_{i_2} \cap \ldots \cap \boldsymbol{M}_{i_k}| = N\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k},$$

pričom prienik množín $\boldsymbol{M}_i$ z prázdnej množiny indexov dáva

$$\left|\bigcup_{i\in\emptyset} \boldsymbol{M}_i\right| = |\boldsymbol{X}| = N$$

a

$$|\boldsymbol{M}'_1 \cap \boldsymbol{M}'_2 \cap \ldots \cap \boldsymbol{M}'_n| = N\alpha'_1\alpha'_2\ldots\alpha'_n = N(0).$$

Z predchádzajúceho dôsledku dostávame

Dôsledok 3.23. *V N-prvkovej množine nech každý prvok má alebo nemá niektoré z vlastností $\alpha_1, \alpha_2, \ldots, \alpha_n$. Nech $N\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k}$ označuje počet prvkov, ktoré majú každú z vlastností $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k}$ prípadne aj nejaké iné. Nech $N(0) = N\alpha'_1\alpha'_2\ldots\alpha'_n$ označuje počet prvkov uvažovanej množiny, ktoré nemajú žiadnu z vlastností $\alpha_1, \alpha_2, \ldots, \alpha_n$. Potom*

$$N(0) = \sum_{k=0}^{n}(-1)^k S_k = \sum_{k=0}^{n}(-1)^k \sum_{i_1<i_2<\ldots<i_k} N\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k}. \qquad \square$$

Poznámka. Existuje praktický spôsob ako si môžeme ľahko zapamätať predchádzajúci vzorec ako aj množstvo podobných vzťahov. Predpokladajme, že chceme určiť počet prvkov, ktoré majú vlastnosti $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_r}$ a nemajú vlastnosti $\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_s}$. Prirodzene predpokladáme, že $\{i_1, i_2, \ldots, i_r, j_1, j_2, \ldots, j_s\} \subseteq \{1, 2, \ldots, n\}$ a že všetky uvažované vlastnosti sú navzájom rôzne. Potom hľadaný počet získame formálnym rozvojom výrazu

$$N\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_r}(1-\alpha_{j_1})(1-\alpha_{j_2})\ldots(1-\alpha_{j_s})$$

podľa distributívneho zákona, pričom kladieme $N.1 = N$, $N.\alpha_i = N\alpha_i$ a podobne. Napríklad počet prvkov, ktoré majú vlastnosť α_1 a nemajú ani vlastnosť α_2 ani α_3 je

$$\begin{aligned} N\alpha_1(1-\alpha_2)(1-\alpha_3) &= N\alpha_1(1-\alpha_2-\alpha_3+\alpha_2\alpha_3) = \\ &= N\alpha_1 - N\alpha_1\alpha_2 - N\alpha_1\alpha_3 + N\alpha_1\alpha_2\alpha_3. \end{aligned}$$

špeciálne

$$N(0) = N\alpha_1'\alpha_2'\ldots\alpha_n' = N(1-\alpha_1)(1-\alpha_2)\ldots(1-\alpha_n)$$

Rozvinutím posledného výrazu dostávame napokon vzťah z dôsledku 3.23,

$$N(1-\alpha_1)(1-\alpha_2)\ldots(1-\alpha_n) = \sum_{k=0}^{n}(-1)^k \sum_{i_1<i_2<\ldots<i_k} N\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k},$$

o čom sa ľahko presvedčíme matematickou indukciou. □

V predchádzajúcom dôsledku sme určili počet $N(0)$ všetkých spomedzi N prvkov, ktoré nemajú žiadnu z uvažovaných vlastností. Tento výsledok je možné zovšeobecniť – dá sa totiž určiť aj počet $N(r)$ všetkých prvkov, ktoré majú práve r vlastnosti, ako aj počet $N(\geq r)$ všetkých prvkov, ktoré majú aspoň r vlastností:

$$N(r) = \sum_{k=r}^{n}(-1)^{k-r}\binom{k}{r}S_k$$

$$N(\geq r) = \sum_{k=r}^{n}\binom{k-1}{r-1}S_k.$$

Dôkaz týchto vzťahov presahuje rámec tohto úvodného textu.

Niekedy je tieto súčty namáhavé presne vypočítať (čo býva pravidlom pri súčtoch so striedavými znamienkami), preto sa vtedy musíme uspokojiť s približnými hodnotami. Namiesto úplného súčtu

$$N(r) = \sum_{k=r}^{n}(-1)^{k-r}\binom{k}{r}S_k$$

s hornou hranicou sčítania n uvažujeme len súčet

$$N(r)_s = \sum_{k=r}^{r+s}(-1)^{k-r}\binom{k}{r}S_k$$

prvých s členov úplného súčtu. Tieto oscilujú okolo hľadanej hodnoty $N(r)$, pričom ak s je nepárne, čiastočný súčet je pod hľadanou hodnotou:

$$N(r)_s \leq N(r).$$

Ak s je párne, čiastočný súčet je nad hľadanou hodnotou:

$$N(r)_s \geq N(r).$$

Tieto vzťahy a odhady, známe ako Bonferroniho nerovnosti, nachádzajú svoje praktické uplatnenie pri vyčíslení pravdepodobností rozličných javov. Ich dôkazy však presahujú rámec tohto textu, a preto ich vynechávame.

Príklad 3. Skupina N pánov sa má zúčastniť večierka. Hostiteľ vyžaduje od účastníkov formálny odev – frak a tvrdý čierny klobúk. Pred vstupom do sály páni odovzdajú svoje klobúky v šatni. Večierok prebehne veľmi úspešne a páni pri svojom odchode nie sú schopní rozoznať svoje klobúky. Aká je pravdepobodnosť toho, že žiaden pán si nezoberie vlastný klobúk?

Ak pánov aj ich klobúky očíslujeme $1, 2, \ldots, N$, tak rozmiestnenie klobúkov na hlave predstavuje permutáciu množiny $\{1, 2, \ldots, N\}$. Naším cieľom je najprv určiť počet D_N permutácií, ktoré nenechávajú žiaden prvok na mieste. Počet permutácií, ktoré nechávajú na mieste k-prvkovú podmnožinu $\{i_1, i_2, \ldots, i_k\}$ je $(N-k)!$. S použitím vyššie zavedených označení dostaneme

$$S_k = \binom{N}{k}(N-k)!,$$

odkiaľ zisťujme, že hľadaný počet permutácií je

$$D_N = N(0) = \sum_{k=0}^{N}(-1)^k S_k = \sum_{k=0}^{N}(-1)^k \binom{N}{k}(N-k)! =$$
$$= \sum_{k=0}^{N}(-1)^k \frac{N!}{k!(N-k)!}(N-k)! = N! \sum_{k=0}^{N} \frac{(-1)^k}{k!}$$

Keďže všetkých permutácií N prvkov je $N!$, pravdepodobnosť toho, že žiaden pán nemá na hlave svoj klobúk je

$$\frac{N! \sum\limits_{k=0}^{N} \dfrac{(-1)^k}{k!}}{N!} = \sum_{k=0}^{N} \frac{(-1)^k}{k!}.$$

Z matematickej analýzy poznáme Taylorov rozvoj funkcie e^x, ktorý dáva vzťah

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!},$$

Pre $x = -1$ dostávame rovnosť

$$e^{-1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!},$$

z čoho vidno, že nami určená pravdepodobnosť je N-ty čiastočný súčet tohto rozvoja čísla e^{-1}. Ak je číslo N dostatočne veľké, tak hľadaná pravdepodobnosť je približne $1/e$ – o čosi viac ako $1/3$.

Na záver uvedieme ešte dve aplikácie princípu zapojenia a vypojenia. Ich dôkaz ponecháme na čitateľovi. □

Dôsledok 3.24. *Počet surjektívnych zobrazení $f\colon A \to B$, kde $|A| = n$ a $|B| == m$, je*

$$S_B^A = \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n. \qquad \square$$

Dôsledok 3.25. *Nech $\varphi(n)$ označuje počet kladných prirodzených čísel menších ako prirodzené číslo $n > 1$ a nesúdeliteľných s n. Nech $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ je kánonický rozklad čísla n na súčin mocnín rôznych prvočísiel $p_1, p_2, \dots, p_r$. Potom*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right). \qquad \square$$

Index