Diskrétní matematika

Petr Kovář
petr.kovar@vsb.cz

Vysoká škola báňská – Technická univerzita Ostrava

zimní semestr 2022/2023
DiM 470-2301/01, 470-2301/03*, 470-2301/05

O tomto souboru

Tento soubor je zamýšlen především jako pomůcka pro přednášejícího. Řadu důležitých informací v souboru nenajdete, protože přednášející je říká, ukazuje, případně maluje na tabuli. Přednášky jsou na webu k dispozici, aby studenti mohli snadno dohledat probíraná témata z přednášek, které zameškali.

Pro samostatné studium doporučuji skripta:

- M. Kubesa: Základy diskrétní matematiky, výukový text
- P. Kovář: Úvod do teorie grafů, výukový text

Pro přípravu ke zkoušce a písemkám doporučuji cvičebnici:

- P. Kovář: Cvičení z diskrétní matematiky, sbírka příkladů

Vše na http://homel.vsb.cz/~kov16/predmety_dm.php

Kapitola 0. Opakování

- množiny, podmnožiny a operace s nimi
- princip inkluze a exkluze
- relace
- důkazové techniky

Množiny a množinové operace

Množina

je soubor různých (rozlišitelných) objektů. Obvykle značíme velkými písmeny $A, B, X, M, \ldots$
Prvky množin značíme malými písmeny $a, b, x, \ldots$
Prázdná množina $\emptyset$ nikoli $\{\emptyset\}$!

Množiny zadáváme

- výčtem prvků (taxativně): $M = \{a, b, c, d\}$,
  platí $a \in M$, $d \in M$, ale $e \notin M$
- charakteristickou vlastností: $N = \{x : x \in \mathbb{N}, x > 5\}$.

Mohutnost množiny M

udává počet prvků v množině M, značíme $|M|$.

Podmnožina

A je podmnožinou B, jestliže pro každé $a \in A$ je také $a \in B$.
Píšeme $A \subseteq B$.

Množinové operace

Sjednocení množin $A \cup B = \{x : x \in A \text{ nebo } x \in B\}$
Průnik množin $A \cap B = \{x : x \in A \text{ a současně } x \in B\}$
Rozdíl množin $A \setminus B = \{x : x \in A \text{ a současně } x \notin B\}$
Symetrický rozdíl množin $A \Delta B = (A \setminus B) \cup (B \setminus A)$

Příklady

$$A = \{a, b, c\}, \; B = \{c, d\}$$

$$A \cup B = \{a, b, c, d\}, \quad A \cap B = \{c\}, \quad A \setminus B = \{a, b\}, \quad A \Delta B = \{a, b, d\}$$

Otázky

Najdete takové dvě množiny A, B, že $A \setminus B = B \setminus A$?
Najdete takové dvě *různé* množiny A, B, že $A \setminus B = B \setminus A$?

Rozšířené sjednocení a průnik množin

Rozšířené sjednocení $\bigcup_{i=1}^{n} X_i$ a průnik $\bigcap_{i=1}^{n} X_i$ množin.

Mějme množinu J, lze použít i $\bigcup_{j \in J} X_j$ a $\bigcap_{j \in J} X_j$.

Příklady

$$A_i = \{1, 2, \ldots, i\}$$

$$\bigcup_{i=1}^{5} A_i = \{1, 2, 3, 4, 5\}, \quad \bigcap_{i=1}^{5} A_i = \{1\}, \quad \bigcap_{i=1}^{\infty} A_i = \{1\}$$

Otázky

Jak vypadá $\bigcap_{j \in J} A_j$ pro $J = \{2, 5\}$?

Jak vypadá $\bigcup_{j \in J} A_j$ pro $J = \mathbb{N}$?

Kartézský součin a kartézská mocnina

Kartézský součin množin $A \times B = \{(a, b) : a \in A,\ b \in B\}$
je množina všech uspořádaných dvojic prvků vybraných po složkách
z množin A a B v daném pořadí.
$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i,\ i = 1, 2, \ldots, n\}$
Pro $A_1 = A_2 = \ldots = A_n$ dostaneme kartézskou mocninu A^n.
Definujeme $A^0 = \{\emptyset\}$, $A^1 = A$.

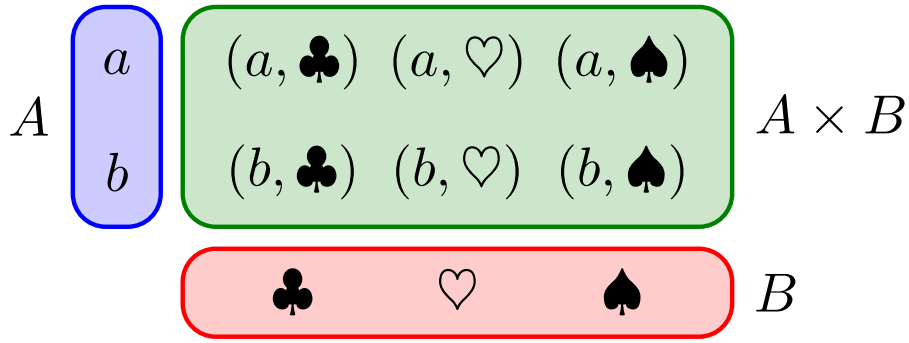
Příklad

$$A = \{a, b\},\ B = \{\clubsuit, \heartsuit, \spadesuit\}$$

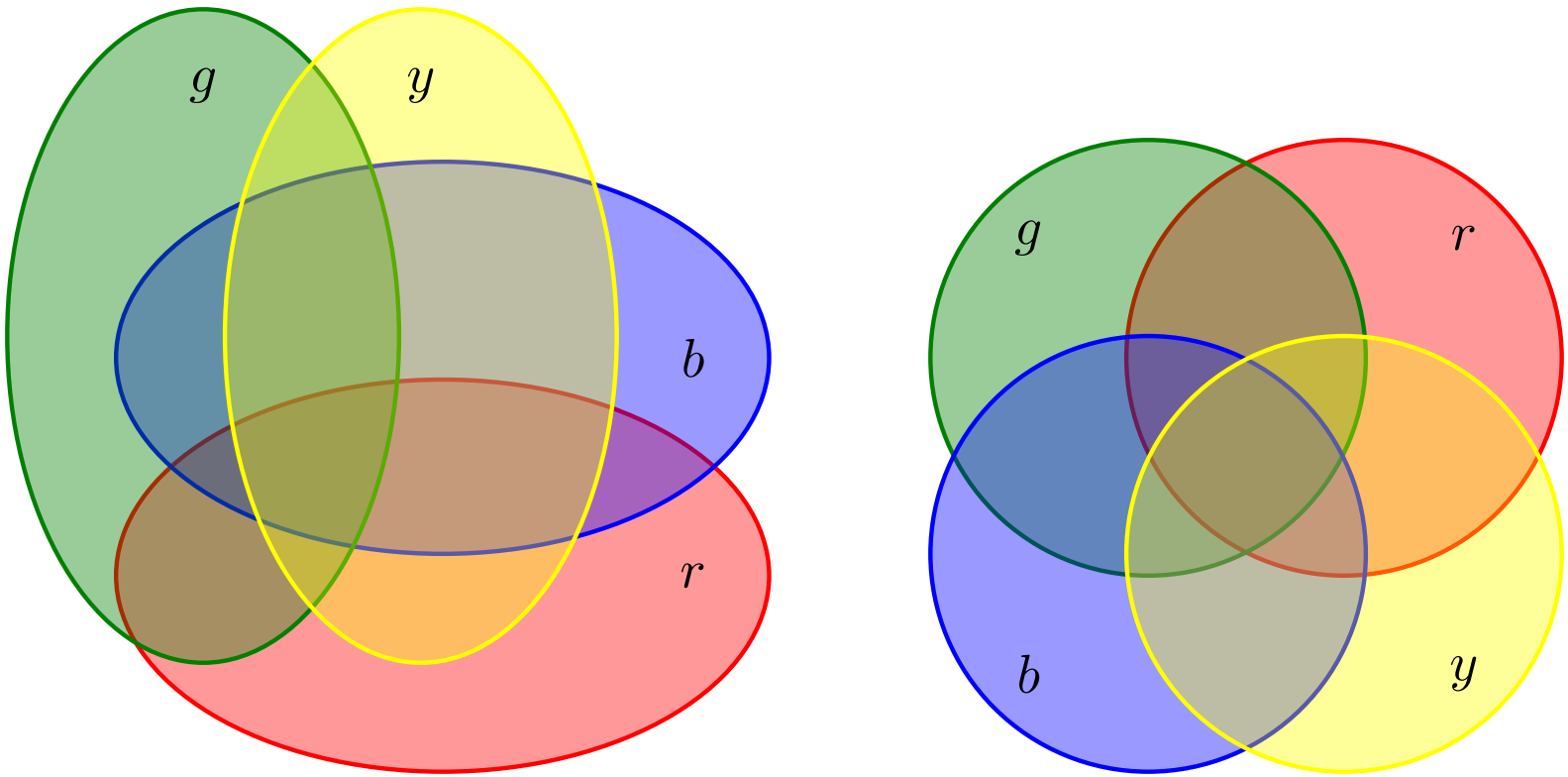
$$A \times B = \{(a, \clubsuit), (a, \heartsuit), (a, \spadesuit), (b, \clubsuit), (b, \heartsuit), (b, \spadesuit)\}$$

Typický příklad

Kartézské souřadnice (x, y) v $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ a (x, y, z) v $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$.



Kartézský součinu množin $A \times B = \{a, b\} \times \{\clubsuit, \heartsuit, \spadesuit\}$.



Všechny možné podmnožniny množiny barev $C = \{r, g, b, y\}$.

Potenční množina

je množina obsahující všechny podmnožiny množiny A

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

Množinový systém nad A

nebo také systém množin nad A je nějaká množina $\mathcal{T} \subseteq 2^A$.
Dáváme přednost termínu „systém množin“ před „množina množin“.

Příklady

$$A = \{a, b\} \qquad 2^A = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

$$\left|2^A\right| = 2^{|A|}$$

Doplněk množiny na univerzu

Univerzum obsahuje všechny možné prvky.
Pro dané A obsahuje doplněk $\overline{A}$ právě ty prvky, které nepatří do A.

Otázky

$$B \times A \times B = ?, \quad A \times \emptyset = ?, \quad \emptyset \times \emptyset = ?, \quad \emptyset^0 = ?, \quad \emptyset^\emptyset = ?$$

Které množinové operace jsou

- komutativní?
- asociativní?

Otázky

$$|A \times B| = ?, \quad |2^A| \stackrel{?}{=} |A^2|, \quad |2^A| \stackrel{?}{<} |A^2|, \quad |2^A| \stackrel{?}{\leq} |A^2|$$

Otázky

Množina S obsahuje všechna sudá čísla.
Jak vypadá $\overline{S}$ pro univerzum $\mathbb{Z}$? Jak vypadá $\overline{S}$ pro univerzum $\mathbb{R}$?

Číselné obory a celočíselný interval

Přirozená a celá čísla

přirozená čísla značíme $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$ neobsahují číslo 0
přirozená čísla včetně nuly značíme $\mathbb{N}_0 = \{0, 1, 2, 3, 4, 5, \ldots\}$
celá čísla značíme $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$

Interval celých čísel od a do b

je množina $\{a, a+1, \ldots, b-1, b\}$
značíme: $[a, b] = \{a, a+1, \ldots, b-1, b\}$

srovnejte s intervalem reálných čísel (a, b)

Příklady

$[3, 7] = \{3, 4, 5, 6, 7\}$ $[-2, -2] = \{-2\}$
$[5, 0] = \emptyset$ (prázdná množina)

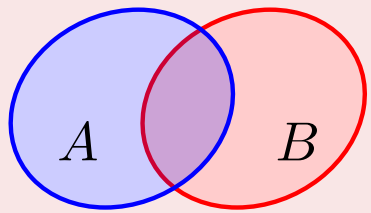
Princip inkluze a exkluze

Nazýván také „princip zapojení a vypojení“, nebo „zahrnutí a vyloučení“.
Pro malá n jej často intuitivně používáme:

Věta

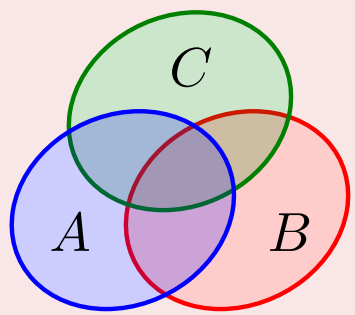
Počet prvků ve sjednocení dvou množin je:

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



Počet prvků ve sjednocení tří je:

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



Obecný tvar principu inkluze a exkluze

Počet prvků ve sjednocení n množin je:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\substack{J\subseteq\{1,\ldots,n\}\\ J\neq\emptyset}} (-1)^{|J|-1} \cdot \left|\bigcap_{i\in J} A_i\right|.$$

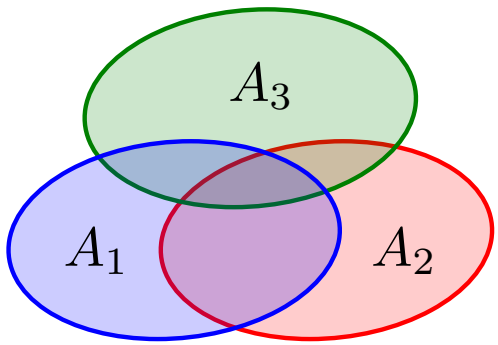
Abychom zjistili, kolik prvků má sjednocení

- sečteme velikosti jednotlivých množin,
- odečteme velikosti průniků všech dvojic,
- přičteme velikosti průniků všech trojic,
- odečteme velikosti průniků všech čtveřic,
- ...

Velikost sjednocení tří množin

Například pro $n = 3$ dostáváme

$$\begin{aligned}\left|\bigcup_{i=1}^{3} A_i\right| &= \sum_{\substack{J\subseteq\{1,2,3\}\\ J\neq\emptyset}} (-1)^{|J|-1} \cdot \left|\bigcap_{i\in J} A_i\right| = \\ &= |A_1| + |A_2| + |A_3| - \\ &\quad - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + \\ &\quad + |A_1 \cap A_2 \cap A_3|.\end{aligned}$$

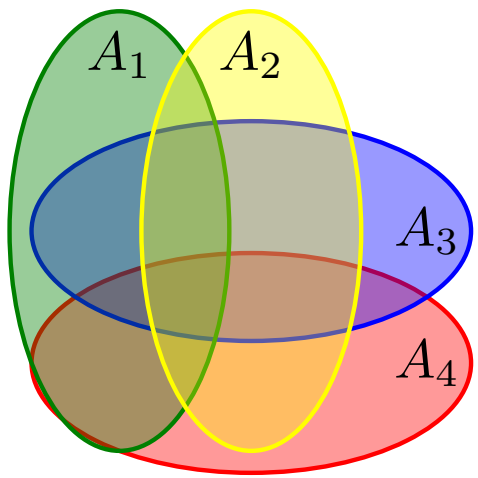


Velikost sjednocení čtyř množin

pro $n = 4$ dostáváme

$$\left|\bigcup_{i=1}^{4} A_i\right| = \sum_{\substack{J\subseteq\{1,2,3,4\}\\ J\neq\emptyset}} (-1)^{|J|-1} \cdot \left|\bigcap_{i\in J} A_i\right| =$$

$$\begin{aligned}
= \quad & |A_1| + |A_2| + |A_3| + |A_4| - \\
- \quad & |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| - |A_1 \cap A_4| - |A_2 \cap A_4| - |A_3 \cap A_4| \\
+ \quad & |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| - \\
- \quad & |A_1 \cap A_2 \cap A_3 \cap A_4|.
\end{aligned}$$



Speciální tvar principu inkluze a exkluze

Jednodušší tvar (s méně sčítanci), mají-li množiny a průniky i množin stejné velikosti:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^{k-1} \cdot \binom{n}{k} \cdot \left|\bigcap_{j=1}^{k} A_j\right|.$$

Abychom zjistili, kolik prvků má sjednocení

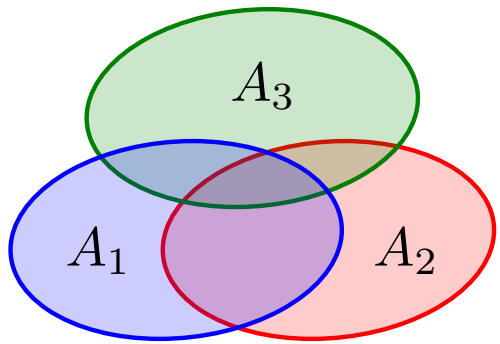
- počet jednoprvkových množin množin,
- odečteme počet dvouprvkových průniků $\times$ velikost průniků dvojic,
- přičteme počet tříprvkových průniků $\times$ velikost průniků trojic,
- odečteme počet čtyřprvkových průniků $\times$ velikost průniků čtveřic,
- ...

Velikost sjednocení tří množin mají-li množiny i průniky množin stejné velikosti

Pro $n = 3$ dostáváme

$$\left|\bigcup_{i=1}^{3} A_i\right| = \sum_{k=1}^{3}(-1)^{k-1} \cdot \binom{3}{k} \cdot \left|\bigcap_{j=1}^{k} A_j\right| =$$

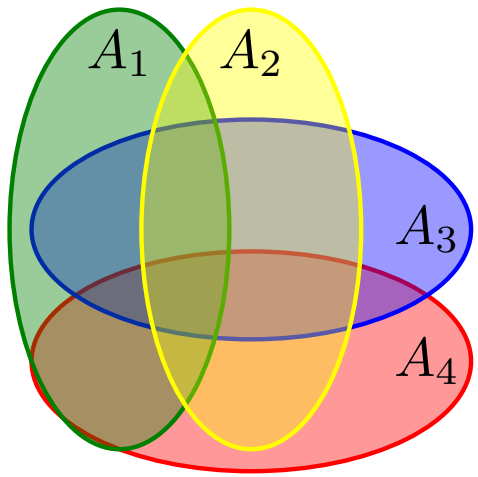
$$= \binom{3}{1} \cdot |A_1| - \binom{3}{2} \cdot |A_1 \cap A_2| + \binom{3}{3} \cdot |A_1 \cap A_2 \cap A_3|.$$



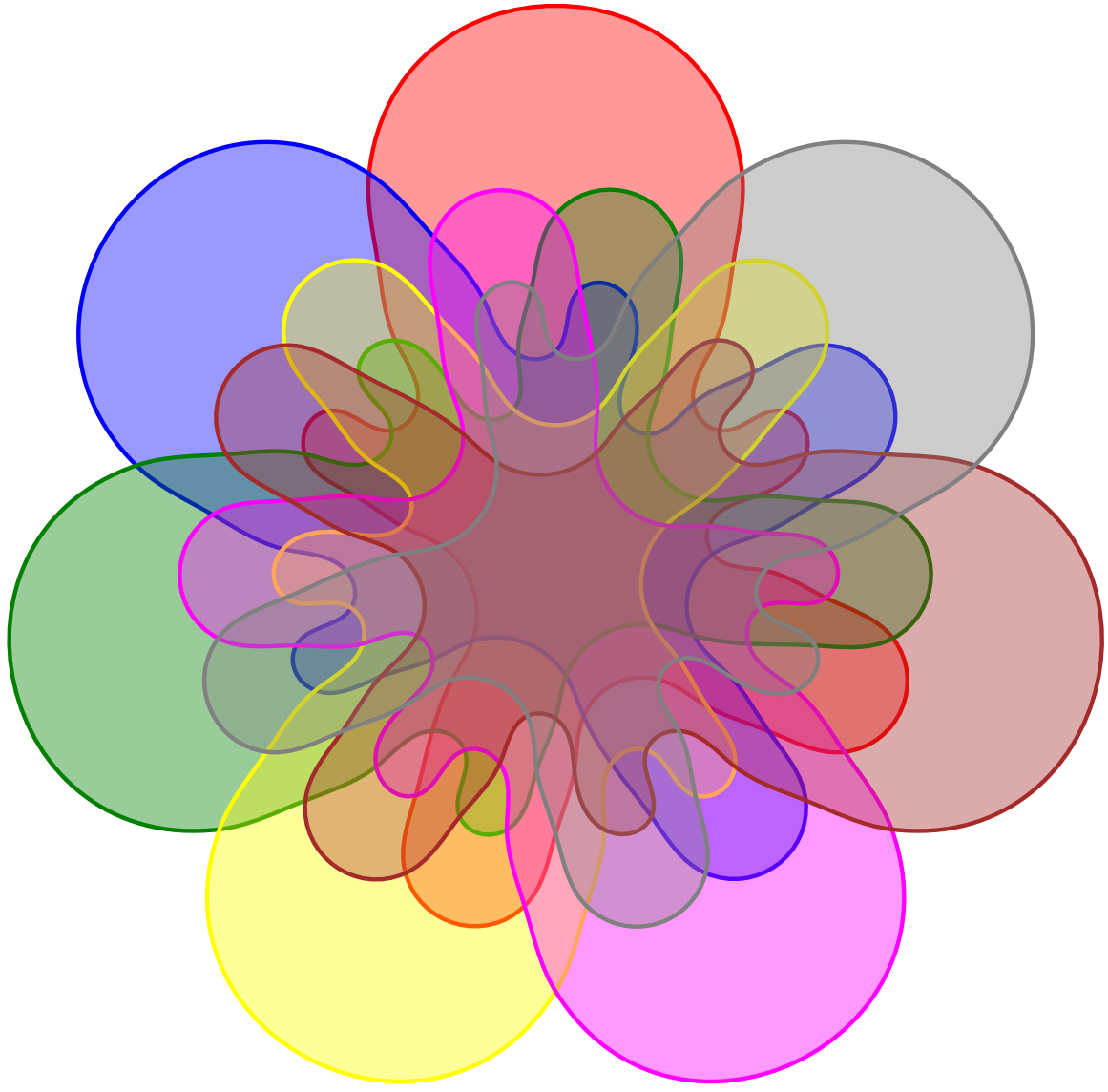
Velikost sjednocení čtyř množin mají-li množiny i průniky množin stejné velikosti

Pro $n = 4$ dostáváme

$$\begin{aligned}\left|\bigcup_{i=1}^{4} A_i\right| &= \sum_{k=1}^{n}(-1)^{k-1} \cdot \binom{n}{k} \cdot \left|\bigcap_{j=1}^{k} A_j\right| = \\ &= \binom{4}{1} \cdot |A_1| - \binom{4}{2} \cdot |A_1 \cap A_2| + \\ &+ \binom{4}{3} \cdot |A_1 \cap A_2 \cap A_3| - \binom{4}{4} |A_1 \cap A_2 \cap A_3 \cap A_4|.\end{aligned}$$



Vennův diagram pro sedm množin – Adelaide



Příklad

Ve třídě je 25 žáků. 17 z nich se učí anglicky a 10 německy. 4 se učí anglicky a německy, 4 anglicky a francouzsky, 2 německy a francouzsky a jeden studuje všechny tři jazyky. Kolik studentů se učí jen francouzsky?

Množiny označíme A, N a F. Zapíšeme si

$$|A| = 17,\ |N| = 10,\ |A \cap N| = |A \cap F| = 4,\ |N \cap F| = 2,\ |A \cap N \cap F| = 1$$

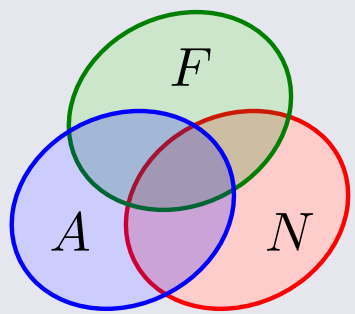
Z rovnice

$$|A \cup N \cup F| = |A| + |N| + |F| - |A \cap N| - |N \cap F| - |A \cap F| + |A \cap N \cap F|$$

dostaneme

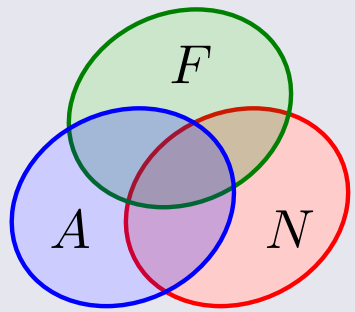
$$|F| = |A \cup N \cup F| - |A| - |N| + |A \cap N| + |N \cap F| + |A \cap F| - |A \cap N \cap F|$$

$$|F| = 25 - 17 - 10 + 4 + 4 + 2 - 1 = 7.$$



Příklad (pokračování)

Ale někteří z těchto 7 studentů se učí i jiné jazyky!



Jen francouzsky

$$x = |F| - |A \cap F| - |N \cap F| + |A \cap N \cap F|$$
$$x = 7 - 4 - 2 + 1 = 2 \text{ žáci.}$$

Jen francouzsky se učí 2 žáci.

0.3. Relace a zobrazení

Při studiu diskrétní matematiky nevystačíme s naivním přístupem k pojmům funkce, uspořádání nebo být ekvivalentní, je potřeba tyto pojmy korektně definovat. Všechny vycházejí ze společného základu – relace.

Význam pojmů ekvivalence a funkce překračuje rámec předmětu Diskrétní matematiky.

Přehled

- pojem relace
- uspořádání a ekvivalence
- funkce a zobrazení
- skládání zobrazení
- princip inkluze a exkluze

0.3.1. Binární a n-ární relace (na množině a mezi množinami)

Připomeňme: Kartézský součin množin $A \times B = \{(a, b) : a \in A, b \in B\}$ je množina všech uspořádaných dvojic prvků vybraných po složkách z množin A a B (v daném pořadí).

Definice

(Heterogenní) binární relace R mezi množinami A, B je libovolné podmnožina kartézského součinu $A \times B$, tj.

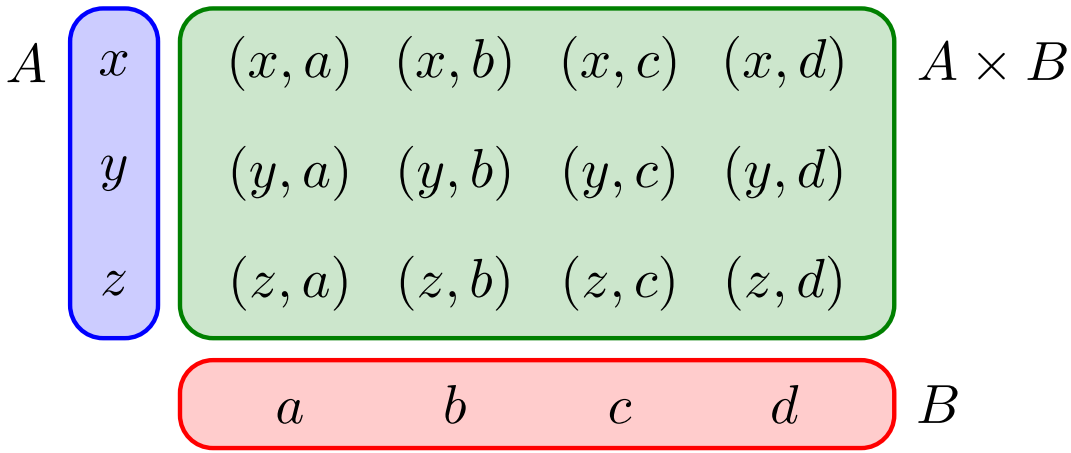
$$R \subseteq A \times B.$$

Říkáme, že „prvek $x \in A$ je v relaci s $y \in B$“ (v tomto pořadí).
Píšeme $(x, y) \in R$ nebo $(x, y) \notin R$, často jen xRy.
(např. $x = y$, $x < y$ místo $(x, y) \in =$, $(x, y) \in <$)

Definice – obecnější

(Heterogenní) n-ární relace S mezi množinami $A_1, A_2, \ldots, A_n$ je libovolné podmnožina kartézského součinu $A_1 \times A_2 \times \cdots \times A_n$, tj.

$$S \subseteq A_1 \times A_2 \times \cdots \times A_n.$$



Kartézský součinu množin $A \times B = \{x, y, z\} \times \{a, b, c, d\}$.

Příklad

Záznam v databázi odpovídá jednomu prvku relace. Například výsledek zkoušky v Edisonu:

(jméno, osobní číslo, datum, bodové hodnocení)

Prvek součinu $Jmeno \times OsCis \times Datum \times Body$

V databázi můžeme vyhledat všechny záznamy s předepsanými vlastnostmi:

- studenti, kteří vykonali zkoušku ve zvolený den,
- studenti, kteří přišli na zkoušku společně,
- bodové výsledky v daném termínu,
- ...

Výsledek může určovat vztah (relaci) mezi prvky *stejné* množiny součinu:

- vztah (relaci) mezi studenty,
- relaci mezi body za písemku.

Definice

(Homogenní) binární relace R na množině A je libovolné podmnožina kartézského součinu $A \times A = A^2$, tj.

$$R \subseteq A^2.$$

Definice

(Homogenní) n-ární relace S na množině A je libovolné podmnožina kartézské mocniny $A \times A \times \cdots \times A = A^n$, tj.

$$S \subseteq A^n.$$

Příklad

- Relace mezi studenty, kteří získali stejnou známku z DiM.
- Relace mezi dvojicemi studentů, kdo má vyšší skóre z písemky.
- Relace mezi dokumenty s podobnými pojmy (plagiáty)...

Binární relace je speciální případ n-ární relace. (unární, ternární, ...). (Homogenní) relace na dané množině je speciální případ (heterogenní) relace mezi množinami. Více v předměty UTI.

Definice

(Binární) relace R na množině A je

- reflexivní pokud $(x, x) \in R$ pro všechna $x \in A$,
- symetrická pokud $(x, y) \in R \Leftrightarrow (y, x) \in R$ pro všechna $x, y \in A$,
- antisymetrická pokud $(x, y), (y, x) \in R \Rightarrow x = y$ pro všechna $x, y \in A$,
- tranzitivní pokud $(x, y), (y, z) \in R \Rightarrow (x, z) \in R$ pro všechna $x, y, z \in A$.
- lineární (úplná) pokud $(x, y) \in R$ nebo $(y, x) \in R$ pro každé $x, y \in A$

Příklady

- relace rovnosti „$=$“ je reflexivní, tranzitivní, symetrická i antisymetrická
- relace menší „$<$“ je tranzitivní a antisymetrická, „$\leq$“ je i reflexivní
- relace dělitelnosti „$|$“ na $\mathbb{N}$ (i $\mathbb{N}_0$) je reflexivní, tranzitivní a antisymetrická
- relace „být příbuzný“ je jistě symetrická, tranzitivní a reflexivní
- relace „podřízený/nadřízený“ je antisymetrická a tranzitivní
- relace „dorozumění se“ je obvykle symetrická, nemusí být tranzitivní

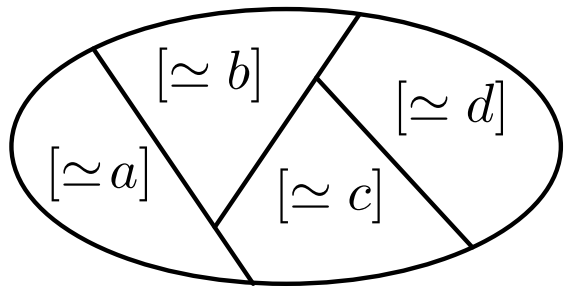
0.3.2. Relace ekvivalence

Definice

Ekvivalence na množině A je *reflexivní, symetrická a tranzitivní* binární relace na množině A. Značíme $\simeq$.

Definice

Mějme relaci ekvivalence $\simeq$ na množině A. Třídou ekvivalence prvku x (značíme $[\simeq x]$) rozumíme podmnožinu $[\simeq x] = \{z \in A : z \simeq x\}$.



Relace ekvivalence vyjadřuje vztah „mít stejnou vlastnost“.

Příklady

- relace kongruence (mít stejný zbytek po dělení číslem n); značí se $\equiv$
- relace vyjadřující vztah mezi studenty „mít stejnou známku z DIM“
- relace „synonyma v jazyce“ je (většinou) ekvivalence

Definice rozkladu množiny Y

Říkáme, že podmnožiny $X_1, X_2, \ldots, X_m$ množiny Y tvoří rozklad Y, jestliže

- $X_1, X_2, \ldots, X_m$ jsou po dvou disjunktní: $X_i \cap X_j = \emptyset$ pro $\forall i \neq j$
- jejich sjednocení je úplné: $X_1 \cup X_2 \cup \cdots \cup X_m = Y$

Otázky

- příklad rozkladu, který má konečně mnoho nekonečných tříd rozkladu
- příklad rozkladu, který má nekonečně mnoho tříd rozkladu
- příklad rozkladu, který má nekonečně mnoho nekonečných tříd rozkladu

Mezi relací ekvivalence na množině A a rozkladem množiny A je úzký vztah:

Věta

Různé třídy ekvivalence $\simeq$ na množině A tvoří rozklad A.

Platí i opačné tvrzení: rozklad množiny A určuje relaci ekvivalence na A.

Věta

Různé třídy ekvivalence $\simeq$ na množině A tvoří rozklad A.

Důkaz Všimneme si, že pro každou dvojici $a \simeq b$ se třídy ekvivalence rovnají $[\simeq a] = [\simeq b]$ i když mají jiné označení, neboť pro každé $x \in [\simeq a]$ je $x \simeq a$, z tranzitivity $x \simeq b$ a tedy $x \in [\simeq b]$. Dále ověříme:

- $\bigcup_{x \in A} [\simeq x] = A$
  Je zřejmé z reflexivity relace $\simeq$, neboť $x \in [\simeq x]$.
- $[\simeq x] \cap [\simeq y] = \emptyset$ pro každé $x \not\simeq y$
  Ukážeme nepřímo, tj. $[\simeq x] \cap [\simeq y] \neq \emptyset$, potom $[\simeq x] = [\simeq y]$.
  Mějme $u \in [\simeq x] \cap [\simeq y]$. Pak podle definice třídy rozkladu je $u \simeq x$ a $u \simeq y$, což z tranzitivity a symetrie dává $x \simeq y$. To ale znamená, že každý prvek $u \in [\simeq x]$ je také v $[\simeq y]$ a naopak, tj. $[\simeq x] = [\simeq y]$. $\square$

Příklady

- rozklad množiny přirozených čísel podle relace kongruence při dělení n
- rozklad množiny studentů podle relace „mít stejnou známku z DIM“
- rozklad záznamů v databázi v závislosti na hodnotě vybraného parametru.

0.3.3. Relace částečného uspořádání

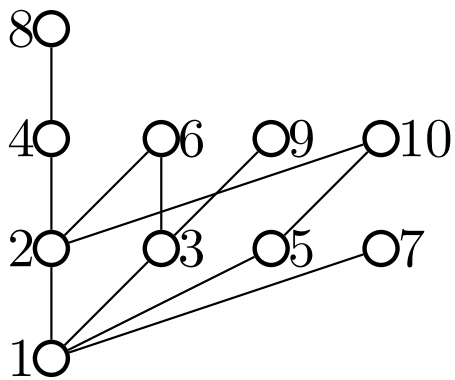
Uspořádání a ekvivalence jsou nejběžnější typy relací.

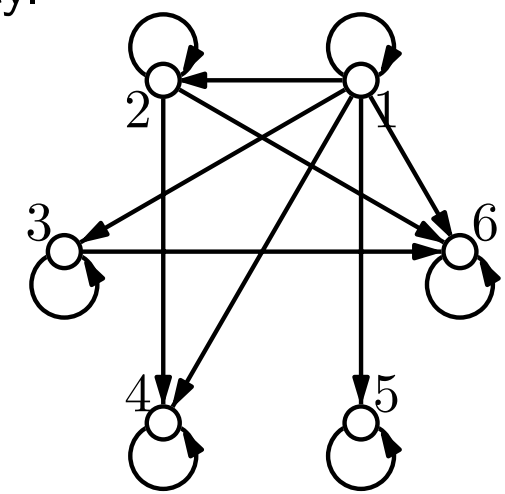
Definice

Částečné uspořádání $\preceq$ je *reflexivní, antisymetrická a tranzitivní* binární relace na množině A. Množina s relací $\preceq$ se nazývá poset.

Slovo *částečné* zdůrazňuje, že se nemusí jednat o *úplnou* relaci na A, tj. ne každá dvojice prvků musí být v relaci xRy nebo yRx.
Částečné uspořádání můžeme znázornit pomocí hasseovského diagramu

- je-li $x \preceq y$, bude prvek y zakreslen výš než prvek x,
- prvky x a y spojíme čárkou, jestliže $x \preceq y$; vynecháme všechny spojnice, které vyplynou z tranzitivity.





Příklady

- relace inkluze $\subseteq$ (být podmnožinou). Dvě množiny mohou snadno být neporovnatelné inkluzí, třeba $\{1, 2\}$ a $\{1, 3, 4\}$.
- relace dělitelnosti $|$ na $\mathbb{N}$ (předchozí obrázek)
- rozehraný turnaj po prvním kole — některé týmy spolu ještě nehrály, nevíme kdo je „lepší“

Definice

Je-li $a \preceq b$, říkáme, že a je menší než prvek b v částečném uspořádání $\preceq$. Dále prvky a, b jsou neporovnatelné, jestliže není ani $a \preceq b$, ani $b \preceq a$. Říkáme, že posloupnost $a_1, a_2, \ldots, a_n$ tvoří řetězec v částečném uspořádání $\preceq$, jestliže $a_1 \preceq a_2 \preceq \cdots \preceq a_n$.

Prvek m nazveme maximální v částečném uspořádání $\preceq$ množiny A, jestliže neexistuje prvek $x \in A$ větší než m, tj. $\forall x \in A : m \preceq x \Rightarrow x = m$. Prvek m je největší v částečném uspořádání $\preceq$ množiny A, pokud je každý jiný prvek $x \in A$ je menší než m, tj. $\forall x \in A : x \preceq m$.

Minimální a nejmenší prvek v částečném uspořádání definovány analogicky.

Příklady

- 1 je nejmenší přirozené číslo (bez nuly) v uspořádání podle velikosti
- množina $\{2, 3, 4, 5, 6\}$ uspořádaná dělitelností nemá nejmenší prvek, minimální prvky jsou 2, 3, a 5; prvky 4 ani 6 nejsou minimální prvky, protože $2|4$ a $2|6$, (tj. „2 je menší než 4 a 6“)
- přirozená čísla nemají největší ani maximální prvek v klasickém uspořádání podle velikosti
- kladná racionální čísla nemají nejmenší ani minimální prvek
- nezáporná racionální čísla mají nejmenší prvek 0 (je i minimální)

Částečné uspořádání $\preceq$ se nazývá lineární uspořádání na množině A (zkráceně uspořádání na A), pokud nemá neporovnatelné prvky.
Máme-li uspořádání na A, tak můžeme prvky A uspořádat do jednoho řetězce.

Příklady

- klasické uspořádání celých, racionálních či reálných čísel podle velikosti
- abecední (lexikografické) uspořádání slov – vždy umíme rozhodnout

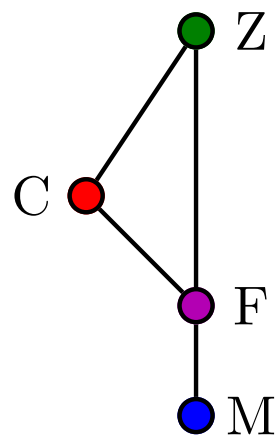
Příklad

Závodu se účastnila čtyři auta: červené, modré, zelené a fialové. Červené auto přijelo do cíle dříve než fialové. Zelené auto přijelo dříve než červené. Fialové auto přijelo dříve než modré. Zelené auto přijelo dříve než fialové. Které auto přijelo poslední?

Zavedeme relaci na množině aut. Auto x je v relaci s autem y (v tomto pořadí), pokud auto x přijelo později než auto y.

Jedná se o relaci částečného uspořádání: je tranzitivní a antisymetrická, ale není reflexivní. Bez újmy na platnosti řešení můžeme doplnit relaci o triviální dvojice „auto x dorazilo dříve nebo současně jako auto y“.

Můžeme nakreslit hasseovský diagram, ve kterém jsou auta, které přijela dříve, zakreslena výše.



0.3.4. Zobrazení (funkce)

Definice

Mějme binární relaci $f \subseteq A \times B$, pro kterou platí, že ke každému $x \in A$ existuje *právě jedna* uspořádaná dvojice $(x, y) \in f$, kde $y \in B$. Potom relaci f nazýváme zobrazení množiny A do množiny B; zapisujeme $f : A \to B$.

Zobrazení množiny A do množiny B v DiM říkáme funkce.

Druhý (jediný) prvek dvojice zapisujeme jednoduše jako $y = f(x)$ místo $(x, y) \in f$.

Poznámka

Obvykle je pojem funkce chápán jako speciální případ zobrazení, kdy $A, B \subseteq \mathbb{R}$ (případně $\mathbb{C}$). V tomto kurzu budeme pojmy *funkce* a *zobrazení* považovat za synonyma.

Příklady

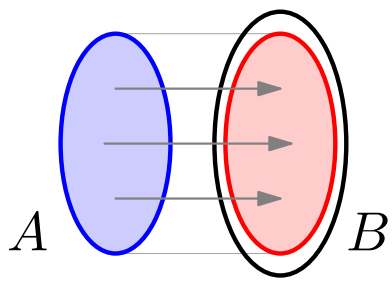
- v analýze $f : \mathbb{R} \to \mathbb{R}$, případně funkce více proměnných $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$
- zobrazení $f : A \to B$, které pointerům A přiřazuje paměťové adresy B

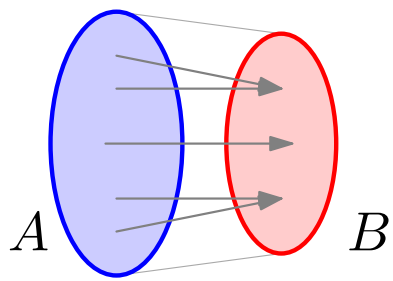
Některé vlastnosti zobrazení jsou natolik významné, že mají jména:

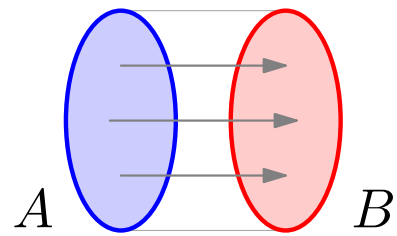
Definice

Funkce $f : A \to B$ se nazývá

- prostá (injektivní) jestliže různé prvky z A se zobrazí na různé prvky B tj. $x \neq y \Rightarrow f(x) \neq f(y)$, totéž jako $f(x) = f(y) \Rightarrow x = y$
- na (surjektivní) jestliže na každý prvek B se zobrazí nějaký prvek A tj. $\forall y \in B$ existuje $x \in A$ tak, že $f(x) = y$
- vzájemně jednoznačná (bijektivní) je-li f „prostá“ i „na“





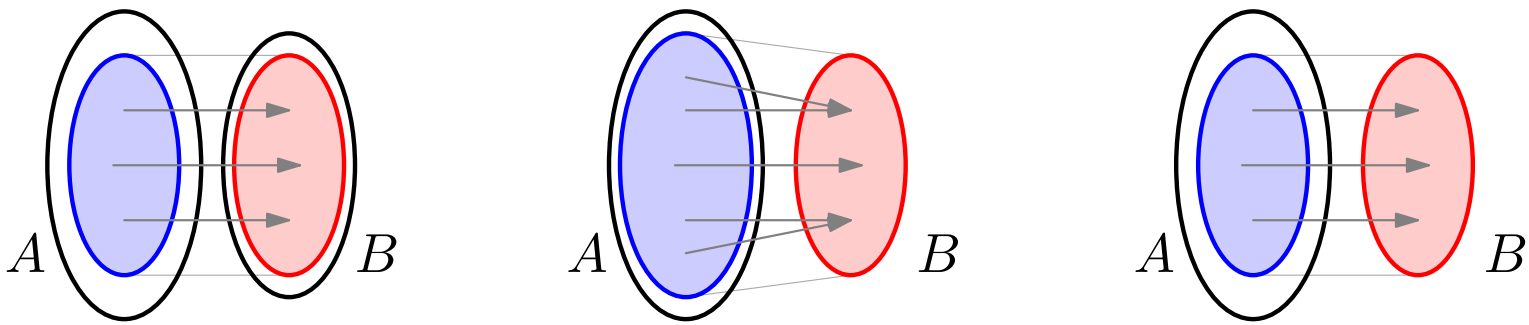


Příklady

- je-li $f : \mathbb{R} \to \mathbb{R}$, tak $f(x) = x^2$ není ani prostá ani na
- je-li $f : \mathbb{R} \to \mathbb{R}$, tak $f(x) = x^3$ je bijektivní
- je-li $f : \mathbb{R} \to \mathbb{R}$, tak $f(x) = \sqrt{x}$ není funkce ($\sqrt{-3} = ?$)

V předmětu UTI budete rozlišovat:

- totální funkci
  Binární relaci $f \subseteq A \times B$, pro kterou platí, že ke každému $x \in A$ existuje *právě* jedna uspořádaná dvojice $(x, y) \in f$, kde $y \in B$.
- parciální funkci
  Binární relaci $f \subseteq A \times B$, pro kterou platí, k žádnému $x \in A$ neexistuje *nejvýše* jedna uspořádaná dvojice $(x, y) \in f$, kde $y \in B$.



Zobrazení a funkce zavedené na předchozích slidech odpovídají totální funkci. Parciální funkce není „funkce“ ve smyslu předchozí definice.

Pozor: Bijektivní zobrazení definováno pouze pro totální zobrazení, nestačí injektivní a surjektivní zobrazení.

Skládání zobrazení

Definice skládání zobrazení

Mějme dvě zobrazení (funkce) $f : A \to B$ a $g : B \to C$.
Jejich složením rozumíme zobrazení $(g \circ f) : A \to C$ (čti „g po f“) definované vztahem

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

Ve složeném zobrazení $(g \circ f) : A \to C$ přiřadí nejdříve zobrazení f vzoru $x \in A$ jeho obraz $f(x) \in B$ a pak zobrazení g přiřadí vzoru $f(x) \in B$ jeho obraz $g(f(x)) \in C$.

Poznámka

Všimněte si: množina obrazů prvního zobrazení f musí být podmnožinou množiny vzorů druhého zobrazení g.
Pokud by tomu tak nebylo, pak složené zobrazení neexistuje!

Isomorfismus

Často se setkáváme s diskrétními strukturami, které jsou sice jinak pojmenované, jinak značené i jinak definované, ale ve své podstatě jsou analogické. Prvky jedné lze převést *bijekcí* na prvky druhé, přičemž „vlastnosti“ se zachovají. Tuto vlastnost vyjadřujeme slovem být isomorfní.

Příklady

- potenční množina množiny $\{a, b\}$ s relací „být podmnožinou“ je isomorfní množině $\{1, 2, 3, 6\}$ s relací dělitelnosti
- množina $\{1, 2, \ldots, n\}$ má stejně mnoho podmnožin jako množina $\{n+1, n+2, \ldots, 2n\}$; mezi prvky existuje snadná bijekce $b(i) = i + n$; také částečná uspořádání těchto systémů podmnožin inkluzí jsou si isomorfní přes rozšířenou bijekci $b^*(X) = \{i + n : i \in X\}$
- relace dělitelnosti na množině $\{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ je isomorfní s dělitelností na množině $\{1, 2, 4, 5, 10, 20, 25, 50, 100\}$; bijekci p v prvočíselném rozkladu nahradí prvočíslo 3 prvočíslem 5, tj. $p(1) = 1$, $p(3) = 5$, $p(6) = 10$, $p(9) = 25$, ...
- Mějme (A, ρ), (B, σ). $(A, \rho) \simeq (B, \sigma)$ jestliže existuje bijekce $f : A \to B$ kde $x \rho y \Leftrightarrow f(x) \sigma f(y)$

0.3.5. Bijekce konečné množiny, permutace

Permutaci (bez opakování) na množině A lze chápat jako bijektivní zobrazení $\pi : A \to A$.

Mějme množinu $A = [1, n]$.
Permutace na A je určena pořadím prvků $(p_1, p_2, \ldots, p_n)$. Zobrazení π definujeme předpisem $\pi(i) = p_i$.

Příklady

Permutace zapisujeme například

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 2 & 6 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 3 & 1 & 6 \end{pmatrix}.$$

Nyní můžeme permutace skládat

$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 3 & 5 & 6 \end{pmatrix}, \quad \pi \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 3 & 6 \end{pmatrix}.$$

Uvedené příklady lze chápat například jako míchání balíčku 6 karet.

Poznámky

- Všechny permutace množiny $[1, n]$ spolu s operací skládání tvoří grupu, které říkáme symetrická nebo permutační grupa. Značí se S_n.
- Každá grupa je isomorfní některé grupě (podgrupě) permutací.
- Pozor! Používají se i jiná značení pro skládání permutací.

Při zápisu permutace vynecháváme (uspořádaný) první řádek $1, 2, \ldots, n$. Zavedeme si jiný v praxi používaný zápis permutací, pomocí jejich cyklů.

Definice

Nechť π je permutace na množině A. Cyklem permutace π rozumíme takovou posloupnost $(a_1, a_2, \ldots, a_k)$ různých prvků A, že

$$\pi(a_i) = a_{i+1} \text{ pro } i = 1, 2, \ldots, k-1 \text{ a } \pi(a_k) = a_1.$$

Příklady

- $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 2 & 6 \end{pmatrix}$ zapíšeme jako $\pi = (1, 3, 5, 2)(4)(6)$
- $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 3 & 1 & 6 \end{pmatrix}$ zapíšeme jako $\sigma = (1, 2, 5)(3, 4)(6)$

Zápis permutace pomocí cyklů

Není důležité, kterým prvkem zápis permutace začínáme, avšak obvykle se snažíme začínat „od nejmenšího“ prvku.

Věta

Každou permutaci konečné množiny A lze zapsat jako složení cyklů na disjunktních podmnožinách A.

Důkaz Vezmeme libovolný (např. nejmenší) prvek $a_1 \in A$ a iterujeme zobrazení $a_2 = \pi(a_1)$, $a_3 = \pi(a_2)$ atd., až dostaneme a_1 (postup je konečný, protože A je konečná). Tak získáme první cyklus $(a_1, \ldots, a_k)$. Pokračujeme v sestavování cyklů ve zbylé množině $A \setminus \{a_1, \ldots, a_k\}$ (např. od nejmenšího prvku), dokud prvky A nevyčerpáme. □

- nevýhodou zápisu permutací pomocí cyklů je složitější skládání
- výhodou zápisu permutací pomocí cyklů je snadné určení řádu (délky) permutace, tj. počtu kolikrát složíme permutaci samu se sebou, abychom dostali zobrazení identity id, kde $\mathrm{id}(a_i) = a_i$ pro každé i.

Definice

Nechť $n \in \mathbb{N}$. Pak n-tou mocninu permutace π budeme definovat rekurentně:
$\pi^1 = \pi$ pro $n = 1$ a $\pi^n = \pi^{n-1} \circ \pi = \pi \circ \pi^{n-1}$ pro $n > 1$.

Definice

Mějme nejmenší možné $k \in \mathbb{N}$ takové, že $\pi^k = \mathrm{id}$, kde π je nějaká permutace. Potom číslo k nazýváme řád permutace π.

Příklad

Permutace $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$ má řád 6.
Snadno ověříme $\tau \circ \tau \circ \tau \circ \tau \circ \tau \circ \tau = \mathrm{id}$ a menší počet složení nedá identické zobrazení.

Věta

Řád permutace je nejmenším společným násobkem délek jednotlivých disjunktních cyklů v cyklickém zápisu permutace.

Příklad

Skládání permutací zadaných pomocí cyklů

Máme dány permutace

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 2 & 6 \end{pmatrix} = (1,3,5,2)(4)(6),$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 3 & 1 & 6 \end{pmatrix} = (1,2,5)(3,4)(6).$$

Víme

$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 3 & 5 & 6 \end{pmatrix}, \quad \pi \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 3 & 6 \end{pmatrix}.$$

Složíme permutace jako cykly:

$$\sigma \circ \pi = (1,2,5)(3,4)(6) \circ (1,3,5,2)(4)(6) = (1,4,3)(2)(5)(6).$$

Podobně

$$\pi \circ \sigma = (1,3,5,2)(4)(6) \circ (1,2,5)(3,4)(6) = (1)(2)(3,4,5)(6).$$

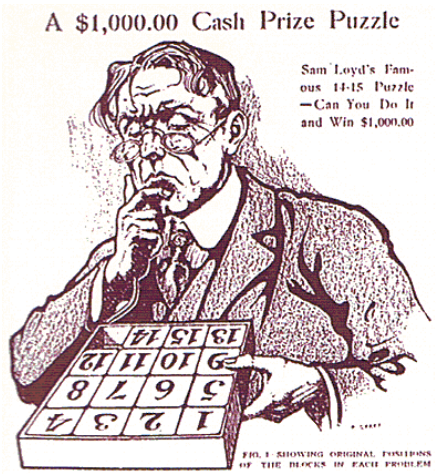
Příklad

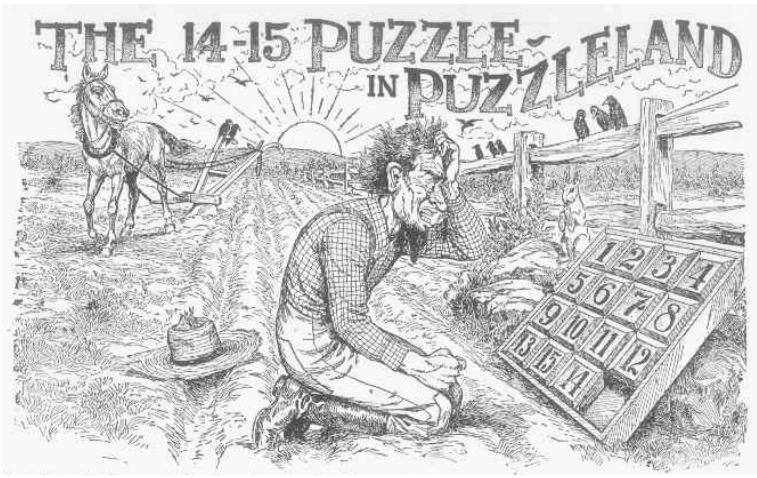
Máme automat na míchání n karet.
Pokaždé provede stejnou permutaci množiny karet $\{1, 2, \ldots, n\}$.

- použijeme-li k-krát (k je řád permutace), seřazení bude jako před mícháním
- lze ukázat, že jedním strojem nemůžeme pro $n > 2$ získat všechny permutace (všechna rozmíchání)

Příklad

Elegantní zdůvodnění, že není možno vyřešit hlavolam Loydova patnáctka s využitím permutací.





Příklad

Německý šifrovací stroj Enigma byl rozluštěn spojenci. Klíčovým krokem byla analýza, kterou v roce 1932 udělal Polský matematik Marian Rejewski rozborem grupy permutací. Byl schopen odhalit spoje jednotlivých kotoučů aniž stroj kdy viděl.

Příklad

Dešifrovací klíč pro nápovědu ve hře geocaching je popsán schématem

```
A|B|C|D|E|F|G|H|I|J|K|L|M
-------------------------
N|O|P|Q|R|S|T|U|V|W|X|Y|Z
```

Lze popsat permutací řádu 2, stejný algoritmus pro šifrování jako pro dešifrování.

Příklad

Generátor náhodných čísel v programovacích jazycích obvykle *není náhodný*, ale dává prvky permutace s velkým řádem.
Na první pohled není zřejmé, protože obvykle vypisujeme čísla zaokrouhlená z předepsané množiny čísel.

Otázky

- Jaký je rozdíl mezi bijekcí a surjekcí?
- Jak ukážete, že jsou množiny stejně velké?
- Jak ukážete, že jsou množiny s operací stejné?
- Jak porovnávat velikosti konečných množin pomocí zobrazení?
- Jak porovnávat velikosti nekonečných množin pomocí zobrazení?
- Kolik nejvíce různých rozmíchání umí automat pro 10 karet?
- Kolik nejvíce různých rozmíchání umí automat pro 32 karet?

0.4. Důkazové techniky v diskrétní matematice

Matematika se jako vědní disciplína vyznačuje svou exaktností.
Rozumíme tím schopnost dokázat tvrzení nade vší pochybnost.

Pojem matematického důkazu se vyvíjel několik století. K nejznámějším historicky doloženým důkazům patří:

- grafické důkazy Pythagorovy věty (tvrzení: Babylonská tabulka cca. 1900–1600 př.n.l., „Rhindův Papyrus“ z Egypta 1788–1580 př.n.l.,
  důkaz: Pythagorejská škola cca. 560–480 př.n.l., v Číně cca. 500–200 před n.l.)
- Euklidovy „Základy“ cca. 300 př.n.l.

V moderní matematice: pojem matematického důkazu je posloupnost elementárních ověřitelných kroků vedoucích od známých/předpokládaných faktů k novému/požadovanému tvrzení.

V diskrétní matematice jsou základní předpoklady tvořeny axiomy tzv. Peanovy aritmetiky (tj. dobře známá fakta o přirozených číslech společně s principem matematické indukce).

0.4.1. Základní logické symboly

Známé pojmy:

- Tvrzení je výrok, o kterém má smysl rozhodnout, zda je pravdivé či nepravdivé
- Logické hodnoty: 1/0, True/False, Pravda/Nepravda
- Logické spojky: „NOT“ $\neg X$, „AND“ $X \wedge Y$, „OR“ $X \vee Y$
- Implikace: „jestliže (je pravda) X, pak (musí být) Y“ $X \Rightarrow Y$
- Ekvivalence: „X (je pravda), právě když Y (je pravda)“ $X \Leftrightarrow Y$

Negace $\neg$ je unární operátor, $\wedge, \vee, \Rightarrow, \Leftrightarrow$ jsou binární operátory.

Další operátory jsou kombinací:
$A \operatorname{XOR} B$ je totéž jako $\neg(A \Leftrightarrow B)$.

Otázky

- Kolik existuje logických binárních operátorů?
- Je „ ? : “ plnohodnotný ternární operátor?

Kvantifikátory

všeobecný „Pro každé $x \in M$ platí tvrzení $P(x)$“
píšeme: $\forall x \in M : P(x)$
existenční „Existuje $x \in M$, pro které platí tvrzení $P(x)$“
píšeme: $\exists x \in M : P(x)$
Množinu M můžeme vynechat, pokud je zřejmé o jakou M se jedná.

Jak vypadá negace obecného výroku s kvantifikátorem?

Příklad

Vyslovte negaci výroku $\forall x \in M : P(x)$?
$\exists x \in M : \neg P(x)$

Příklad

Vyslovte negaci výroku $\exists x \in M : P(x)$?
$\forall x \in M : \neg P(x)$

Toto obecné schéma využijeme pro konkrétní příklady...

0.4.2. Pojem matematického důkazu

Struktura věty (tvrzení) v matematice: $P \Rightarrow D$

Přesně formulované předpoklady P, za kterých platí tvrzení věty D.

Podrobný postup, jak z předpokladů odvodit tvrzení věty nazýváme důkaz.

Matematický důkaz

nějakého tvrzení D je konečná posloupnost kroků/výroků, kde každý krok je:

- axiom – obecně platný či předpokládaný fakt (volba axiomů závisí na matematické teorii*),
- předpoklad P je podmínka, na kterou se omezíme,
- výrok odvozený z předchozích kroků užitím některého z platných odvozovacích pravidel (závisí na použité logice).

Poslední krok obsahuje jako výrok *tvrzení* D.

*Různá odvětví matematiky vychází z různých axiomů. Zatímco diskrétní matematika vychází z Peanových axiomů, například geometrie (nejstarší exaktně budovaná matematická disciplína) vychází z pěti Euklidových axiomů.

K čemu to budu jako absolvent potřebovat?

„K čemu je novorozeně?“

- správné pochopení omezení použitých metod
- argumentace pro a proti navrženému řešení
- srovnání kvality různých řešení
- 100% korektnost metody/algoritmu je někdy vyžadována (autopilot, jednotka intenzivní péče, řízení satelitů)

Příklad

Abstraktní o inverzním prvku

Dokážeme, že v libovolné (i nekomutativní!) algebraické grupě platí komutativita operace vzhledem k „násobení inverzním prvkem“. Tj. jestliže $A \cdot B = E$, potom také $B \cdot A = E$.
Vzpomeňte na násobení regulárních matic: jednotková matice může vyjít pouze pro regulární matice, neboť existuje inverzní matice.

Grupa $(G, \cdot)$ je množina prvků s jednou operací, pro kterou platí nějaké vlastnosti, tzv. *axiomy grupy*. Nás zajímají tři

1. operace je asociativní
2. v grupě existuje „jednička“ (neutrální prvek)
3. ke každému prvku existuje prvek inverzní

Poznámka

Při psaní důkazů můžeme některé elementární kroky vynechat, případně zkrátit. Nesmí však být porušena korektnost tvrzení (vynechat některý předpoklad). Míra „zkratky“ závisí i na očekávaném „průměrném čtenáři“.

Grupa $(G, \cdot)$ je množina prvků s jednou operací, pro kterou platí tzv. *axiomy grupy*. Využijeme následující tři axiomy

1. operace je asociativní:
   $\forall A, B, C \in G : (A \cdot B) \cdot C = A \cdot (B \cdot C)$
2. v grupě existuje „jednička“:
   $\exists E \in G : E \cdot A = A \cdot E = A$ pro $\forall A \in G$
3. ke každému prvku existuje prvek inverzní:
   $\forall A \in G \ \exists A^{-1} : A \cdot A^{-1} = E \ \wedge \ A^{-1} \cdot A = E.$

Důkaz tvrzení:

$$
\begin{array}{rcll}
A \cdot B & = & E & \text{předpoklad} \\
A^{-1} \cdot (A \cdot B) & = & A^{-1} \cdot E & \text{z axiomu 3. existuje } A^{-1} \\
(A^{-1} \cdot A) \cdot B & = & A^{-1} & \text{z axiomu 1. a axiomu 2.} \\
E \cdot B & = & A^{-1} & \text{z axiomu 3.} \\
B & = & A^{-1} & \text{z axiomu 2.} \\
B \cdot A & = & A^{-1} \cdot A & \\
B \cdot A & = & E & \text{z axiomu 3.}
\end{array}
$$

0.4.3. Základní důkazové techniky

- přímý důkaz: $A \Rightarrow B$
- nepřímý důkaz: $\neg B \Rightarrow \neg A$
- důkaz sporem: $A \wedge \neg B \Rightarrow spor$ (spor je současná platnost T a $\neg T$)
- důkaz matematickou indukcí (slabá a silná)

Příklad

Každé liché číslo je možno napsat jako rozdíl dvou čtverců.

Ukážeme přímo. Mějme liché číslo $2k + 1$, kde $k \in \mathbb{Z}$, potom $2k + 1 = k^2 + 2k + 1 - k^2 = (k + 1)^2 - k^2$.

Příklad

Prvočísel je nekonečně mnoho.

Víme, že každé kladné přirozené číslo je možno napsat jako součin prvočísel. Sporem:

Předpokládáme, že prvočísel je konečně mnoho, označíme je $p_1, p_2, \ldots, p_n$ (*jsou všechna*). Ale číslo $x = p_1 \cdot p_2 \cdots p_n + 1$ není dělitelné ani jedním z prvočísel! Máme spor (= má současně platit nějaké tvrzení i jeho negace), proto předpoklad nepravdivý, tj. prvočísel je nekonečně mnoho.

0.4.4. Princip matematické indukce

Princip matematické indukce je jedna z nejčastěji používaných důkazových technik pro tvrzení (výrokové formy) závislé na přirozeném parametru n (označujeme $P(n)$).

Matematická indukce

Mějme tvrzení $P(n)$ s celočíselným parametrem n. Nechť platí:

- *Základ indukce:*
  Tvrzení $P(n_0)$ je pravdivé, kde $n_0 = 0$ nebo 1, nebo obecné celé n_0.
- *Indukční krok:*
  Vyslovíme indukční předpoklad: Pro nějaké n tvrzení $P(n)$ platí.
  Ukážeme, že pro každé $n > n_0$ z platnosti $P(n)$ plyne platnost $P(n+1)$.

Pak $P(n)$ platí pro všechna přirozená $n \geq n_0$.

Matematickou indukci lze úspěšně využívat při dokazování správnosti algoritmů.

Ukážeme několik příkladů...

Počkat!

Ale. . .

- ukážeme základ indukce,
- ukážeme platnost indukčního kroku (s využitím indukčního předpokladu),

. . . nicméně tvrzení má platit pro nekonečně mnoho hodnot!?!

Příklad

Jak vysoko lze vystoupat na žebřík?

Předpokládejme, že umíme

- vstoupit na první příčku,
- z každé příčky n vystoupit na příčku $n + 1$.

. . . tak umíme vystoupat libovolně vysoko!

Věta

Součet prvních n sudých čísel je $n(n+1)$.

$2+4+6=12=3\cdot 4$

$2+4+6+8+10+12+14+16+18+20=110=10\cdot 11$

Důkaz matematickou indukcí vzhledem k n:

Dokazujeme, že $\forall n \in \mathbb{N}$ platí $\sum_{i=1}^{n} 2i = n(n+1)$.

- *Základ indukce:* Pro $n=1$ tvrzení P(1) zní „$2=1\cdot 2$“.
- *Indukční krok:* Plyne z platnosti $P(n)$ platnost $P(n+1)$?

  Tj. pokud $\sum_{i=1}^{n} 2i = n(n+1)$, tak $\sum_{i=1}^{n+1} 2i = (n+1)(n+2)$?

  Vyslovíme *indukční předpoklad* P(n):
  Předpokládejme, že $\exists n \in \mathbb{N} : \sum_{i=1}^{n} 2i = n(n+1)$.
  Nyní
  $\sum_{i=1}^{n+1} 2i = \sum_{i=1}^{n} 2i + 2(n+1) \overset{IP}{=} n(n+1)+2(n+1) = (n+1)(n+2)$.
  Ukázali jsme že s využitím znalosti vztahu pro součet prvních n sudých čísel lze obdržet odpovídající vztah pro součet prvních $n+1$ sudých čísel.

Podle principu matematické indukce tvrzení platí $\forall n \in \mathbb{N}$. □

Struktura důkazu matematickou indukcí

Lze postupovat podle následujícího schématu:

1. Rozpoznáme, že se jedná o tvrzení dokazovatelné matematickou indukcí:
   „$\forall n \in \mathbb{N}, n \geq n_0$ platí P(n).“
2. Ukážeme *Základ indukce:* Dokážeme platnost $P(n_0)$.
3. Zformulujeme *indukční předpoklad*: $\exists n \in \mathbb{N}, n \geq n_0$ aby platilo P(n).
4. Ukážeme *Indukční krok:*
   S využitím indukčního předpokladu odvodíme platnost P(n+1).
   (Víme, jak má tvrzení nebo vztah P(n+1) vypadat!)
5. Shrneme, že platnost tvrzení P(n) pro všechna $n \geq n_0$ plyne z principu matematické indukce.

Další vzorový důkaz (dělitelnost čísel):

Věta

Pro každé přirozené číslo n je výraz $n^3 + 2n$ dělitelný 3.

Řekneme, že číslo a dělí číslo b, jestliže $\exists k \in \mathbb{Z} : b = ka$. Píšeme $a \mid b$.

Důkaz matematickou indukcí vzhledem k n:

Dokazujeme, že $\forall n \in \mathbb{N}$ platí, že 3 dělí $n^3 + 2n$.

- *Základ indukce:* Pro $n = 1$ tvrzení P(1) zní „3 dělí $1^3 + 2 \cdot 1$“.
- *Indukční krok:* Plyne z platnosti $P(n)$ platnost $P(n+1)$?

  Tj. pokud 3 dělí $n^3 + 2n$, tak 3 dělí $(n+1)^3 + 2(n+1)$.

  Vyslovíme *indukční předpoklad* P(n):
  Předpokládejme, že $\exists n \in \mathbb{N} : 3 \mid n^3 + 2n$, tj. $\exists k \in \mathbb{Z} : n^3 + 2n = 3k$.

  Nyní $(n+1)^3 + 2(n+1) = (n^3 + 3n^2 + 3n + 1) + (2n + 2) =$
  $(n^3 + 2n) + (3n^2 + 3n + 3) \overset{IP}{=} 3k + 3(n^3 + n + 1)$.
  Evidentně 3 dělí výsledný výraz, proto 3 dělí $(n+1)^3 + 2(n+1)$.

Podle principu matematické indukce tvrzení platí $\forall n \in \mathbb{N}$. □

Další vzorový důkaz (nerovnost):

Věta

Pro každé přirozené číslo $n \geq 4$ platí $n! > 2^n$.

Velikost faktoriálu $n!$ roste (super)exponenciálně vzhledem k n.

Důkaz matematickou indukcí vzhledem k n:

Dokazujeme, že $\forall n \in \mathbb{N}, n \geq 4$ platí $n! > 2^n$.

- *Základ indukce:* Pro $n = 4$ tvrzení P(4) zní „$4! > 2^4$“, tj. $24 > 16$.
- *Indukční krok:* Plyne z platnosti $P(n)$ platnost $P(n+1)$?
  Tj. ukážeme, že pokud $n! > 2^n$, tak také $(n+1)! > 2^{n+1}$.

  Vyslovíme *indukční předpoklad* P(n):
  Předpokládejme, že $\exists n \in \mathbb{N}, n \geq 4$, pro které platí $n! > 2^n$.

  Nyní $(n+1)! = (n+1) \cdot n! \overset{IP}{>} (n+1)2^n > 2 \cdot 2^n = 2^{n+1}$.

  Ukázali jsme s využitím indukčního předpokladu, že $(n+1)! > 2^{n+1}$.

Podle principu matematické indukce tvrzení platí $\forall n \in \mathbb{N}$, $n \geq 4$. □

Další příklady:

Věta

Všech zobrazení libovolné b-prvkové množiny do a-prvkové množiny je a^b.

Důkaz matematickou indukcí podle $b \in \mathbb{N}_0$:

- *Základ indukce:*
  Pro $b = 0$ máme jedinou možnost (jak nic nepřiřadit: $a^b = a^0 = 1$).
  Pro $b = 1$ máme a možných obrazů pro jediný prvek ($a^b = a^1 = a$).
- *Indukční krok:*
  IP: pro nějaké b je počet různých zobrazení $B \to A$ roven a^b.

  Mějme libovolnou množinu B o $b + 1 > 0$ prvcích. Zvolme nějaký prvek $x \in B$ (takový existuje) a označme $B' = B \setminus \{x\}$, $|B'| = b$.
  Všech zobrazení z B' do A je podle indukčního předpokladu a^b.
  Pro prvek x máme navíc nezávislý výběr z a možných obrazů. Celkem je dle principu nezávislých výběrů $a \cdot a^b = a^{b+1}$ různých zobrazení z B do A.

Podle principu matematické indukce je počet různých zobrazení z B do A roven a^b pro všechna $b \in \mathbb{N}_0$. □

Silná matematická indukce (ve srovnání s matematickou indukcí)

Matematická indukce

Mějme tvrzení $P(n)$ s celočíselným parametrem n. Nechť platí:

- *Základ indukce:*
  Tvrzení $P(n_0)$ je pravdivé, kde $n_0 = 0$ nebo 1, nebo obecné celé n_0.
- *Indukční krok:*
  Vyslovíme indukční předpoklad: Pro nějaké n tvrzení $P(n)$ platí.
  Ukážeme, že pro každé $n > n_0$ z platnosti $P(n)$ plyne platnost $P(n+1)$.

Pak $P(n)$ platí pro všechna přirozená $n \geq n_0$.

Silná matematická indukce

- *Základ indukce:* Tvrzení $P(n_0)$ je pravdivé.
- *Indukční krok:*
  Indukční předpoklad: Tvrzení $P(k)$ platí pro všechna $n_0 \leq k < n$.
  Ukážeme, že pak platí také $P(n)$.

Pak $P(n)$ platí pro všechna přirozená $n \geq n_0$.

Příklad

Pro nalámání čokolády rozměru $p \times r$ dílků je vždy potřeba $pr - 1$ zlomů.

Důkaz silnou matematickou indukcí podle $n = pr$:

- *Základ indukce:*
  Pro $n_0 = 1$ máme jeden dílek a je třeba $pr - 1 = 0$ zlomů.
- *Indukční krok:*
  Nechť nyní tvrzení platí pro všechny čokolády o méně než n dílcích. Mějme libovolnou tabulku o n dílcích. Tabulku rozlomíme a dostaneme dvě menší tabulky o s, t dílcích, kde $1 \leq s, t < n$ a $s + t = n$. Každou z nich umíme podle předpokladu nalámat pomocí $s - 1$ resp. $t - 1$ zlomů. Celkem je třeba $(s - 1) + (t - 1) + 1 = s + t - 1 = n - 1$ zlomů.

Podle principu silné matematické indukce tvrzení platí $\forall p, r \in \mathbb{N}$. □

Příklad

Máme sloupeček n krabic. Budeme hrát následující hru (pro jednoho/libovolný počet hráčů):
Z jednom kroku vždy rozdělíme nějaký sloupec z krabic ($z \geq 2$) na dva menší sloupce s x a y krabicemi. Za tento krok získáme počet bodů, který je dán součinem $x \cdot y$.
Hra končí, jakmile máme n sloupců každý s jedinou krabicí. Začínáme s nulovým počtem bodů a chtěli bychom dosáhnout co největšího počtu bodů. Hráč s největším počtem bodů vyhrál.

- Jakou strategii zvolit, abychom získali co největší skóre?
- Dokažte, že žádná jiná strategie nevede k vyššímu skóre.

0.4.5. Důkazy vztahů s kombinačními čísly

Pro kombinační čísla můžeme dokázat celou řadu zajímavých vztahů. Zabývá se jimi dokonce celá samostatná část diskrétní matematiky.

Fakt (na první pohled zřejmé tvrzení)

Pro všechna $n \geq 0$ platí

$$\binom{n}{0} = \binom{n}{n} = 1.$$

Lemma (pomocné tvrzení)

Pro všechna $n \geq k \geq 0$ platí

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

Tvrzení, jejichž důkaz spočívá v dosazení do definice (jedna/dvě jednoduché úpravy) považujeme za „zřejmá“ tvrzení a důkaz se neuvádí. Pokud ale důkaz vyžaduje nějaký „trik“, nebo neobvyklé úpravy (byť jen jednu jedinou úpravu), je zvykem stručně vysvětlit.

Lemma

Pro všechna $n \geq k \geq 0$ platí

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

Přímý (dosazením a úpravou)

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

$$= \frac{n! \cdot (k+1) + n! \cdot (n-k)}{(k+1)! \cdot (n-k)!} = \frac{n! \cdot (n+1)}{(k+1)! \cdot (n-k)!} =$$

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

□

Vztahy mohou sloužit jako *alternativní definice kombinačních čísel*.

$$\binom{n}{0} = \binom{n}{n} = 1 \qquad \binom{n}{k} = \binom{n}{n-k} \qquad \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}.$$

Pascalův trojúhelník

$$\binom{0}{0} = 1$$

$$\binom{1}{0} = 1 \quad \binom{1}{1} = 1$$

$$\binom{2}{0} = 1 \quad \binom{2}{1} = 2 \quad \binom{2}{2} = 1$$

$$\binom{3}{0} = 1 \quad \binom{3}{1} = 3 \quad \binom{3}{2} = 3 \quad \binom{3}{3} = 1$$

$$\binom{4}{0} = 1 \quad \binom{4}{1} = 4 \quad \binom{4}{2} = 6 \quad \binom{4}{3} = 4 \quad \binom{4}{4} = 1$$

$$\binom{5}{0} = 1 \quad \binom{5}{1} = 5 \quad \binom{5}{2} = 10 \quad \binom{5}{3} = 10 \quad \binom{5}{4} = 5 \quad \binom{5}{5} = 1$$

. . . . . .

Krajní členy mají hodnoty 1, každý vnitřní člen je součtem dvou členů bezprostředně nad ním.

Binomická věta

Pro všechna $n > 0$ platí

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n-1}x^{n-1} + \binom{n}{n}x^n.$$

Důkaz Tvrzení je možno dokázat indukcí (skripta). Avšak možný je i důkaz jednoduchou úvahou (s využitím lemmatu):
Algebraickém rozvoji součinu používáme pravidlo „vynásobit každý člen s každým“. Proto se v rozvoji vztahu $\underbrace{(1+x)(1+x)\ldots(1+x)}_{n}$ člen x^k objeví tolikrát, kolik je možností (neuspořádaně) vybrat k z n činitelů – závorek. To je právě $\binom{n}{k}$ krát = počet k prvkových podmnožin z n prvků. □

Z binomické věty ihned plyne (pro přirozená $n \geq 0$ a druhé pro $n > 0$)

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n\,,$$

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \ldots - (-1)^n\binom{n}{n-1} + (-1)^n\binom{n}{n} = 0\,.$$

0.4.6. Důkazy vztahů pro kombinatorické výběry

Při důkazech využijeme matematickou indukci a metodu dvojího počítání.

Věta

Počet všech permutací n-prvkové množiny je $n!$, pro každé $n \geq 0$.

Indukcí podle n:

Základ indukce: Tvrzení platí pro $n = 0$, protože žádné prvky lze uspořádat jen jedním způsobem. (Stejně jednoprvkové množiny.)

Indukční krok: Mějme nyní $n \geq 0$ a množinu P o $n+1$ prvcích, předpokládejme pro jednoduchost $P = \{1, 2, \ldots, n+1\}$. Zvolme první prvek $p \in P$ (existuje!) permutace z $n+1$ možností. Nezávisle na volbě prvního prvku pak sestavujeme permutace množiny $P \setminus \{p\}$.
(Jedná se sice o permutaci *jiné množiny*, ale vždy můžeme prvky $P \setminus \{p\}$ oindexovat/„přečíslovat“ na $\{1, 2, \ldots, n\}$, což neovlivní počet možností.)

Potom n-prvková množina $\{1, 2, \ldots, n\}$ má podle indukčního předpokladu $n!$ permutací, proto P má celkem $(n+1) \cdot n! = (n+1)!$ permutací. Podle principu matematické indukce plyne tvrzení $\forall n \in \mathbb{N}_0$. □

Věta

Počet všech k-prvkových variací z n-prvkové množiny je $\frac{n!}{(n-k)!}$, pro každé $n \geq k \geq 0$.

Metodou dvojího počítání:

Dvěma způsoby spočítáme počet permutací n-prvkové množiny:
Už víme, že tyto permutace lze vybrat $n!$ různými způsoby.
Současně lze vzít některou k-prvkovou variaci, její prvky zapsat na začátek permutace (dodržíme pořadí) a *zbývajících $n-k$ prvků seřadíme za nimi jedním z $(n-k)!$ různých způsobů*. Z různých variací tímto postupem získáme různé permutace, a přitom každou permutaci lze získat z variace vybírající jejích prvních k prvků.

Označíme x neznámý počet všech k-prvkových variací z n-prvkové množiny. Výše popsaným postupem vytvořit právě $x \cdot (n-k)!$ všech různých permutací n-prvkové množiny. Proto platí

$$\begin{aligned} x \cdot (n-k)! &= n! \\ x &= \frac{n!}{(n-k)!}. \end{aligned}$$

Věta

Počet všech k-prvkových kombinací z n-prvkové množiny je $\binom{n}{k}$, pro každé $n \geq k \geq 0$.

Metodou dvojího počítání:

Nyní budeme dvojím způsobem počítat všechny k-prvkové variace z n-prvkové množiny:

Na jednu stranu už víme, že jich je $\frac{n!}{(n-k)!}$, na druhou stranu můžeme z jedné k-prvkové kombinace získat celkem $k!$ různých variací uspořádáním prvků této kombinace. Označíme x neznámý počet všech k-prvkových kombinací z n-prvkové množiny a dostaneme, obdobně jako v předchozím důkazu,

$$\begin{aligned} x \cdot k! &= \frac{n!}{(n-k)!} \\ x &= \frac{n!}{k! \cdot (n-k)!} \\ x &= \binom{n}{k}. \end{aligned}$$

0.4.7. Důkazy „metodou počítání možností“

Někdy máme ukázat existenci nějakého objektu nebo vlastnosti, aniž jsme schopni objekt zkonstruovat nebo jinak specifikovat. Takovým důkazům říkáme nekonstruktivní, někdy také existenční.

Místo abychom řešení „zkonstruovali“, tak se nám podaří „spočítat“, že řešení musí existovat.

Dirichletův princip (the pigeon-hole principle)

Rozmístíme-li $\ell + 1$ (nebo více) objektů do ℓ přihrádek, v některé přihrádce musí být alespoň dva objekty.

Důkazy počítáním možností

Existenci konkrétní možnosti (ze známé množiny) ukážeme, pokud počet možností, které nemohou nastat je menší než celkový počet možností.

Příklad

Vidíme, jak do tunelu vjedou tři auta a jen dvě vidíme vyjet ven. To znamená, že jedno auto v tunelu zůstalo (přestože ho nyní nevidíme).

Příklad

8 kamarádů jelo na 9 dní dovolené. Každý den některá (jedna) trojice z nich šla na výlet. Dokažte, že někteří dva z nich ani jednou nebyli spolu na výletě.

Důkaz rozebírání možností by asi k ničemu nevedlo...
Důkaz počítáním je však snadný: Jedna trojice má celkem 3 dvojice, proto po 9 dnech se mohlo vystřídat *nejvýše různých* $9 \cdot 3$ *dvojic*, ale $9 \cdot 3 = 27 < \binom{8}{2} = 28$, jedna dvojice nám zde schází.

Otázka

Žijí na Zemi dva lidé, kteří mají stejný počet vlasů?

Příklad

V šuplíku je (poházeno) 30 párů černých ponožek, 10 párů hnědých ponožek a 3 páry bílých ponožek. Kolik musíme potmě vytáhnout ponožek, abychom měli jistotu, že máme alespoň jeden pár stejné barvy?

„Přihrádky“ Dirichletova principu budou odpovídat třem různým barvám. Vytáhneme-li čtyři ponožky (nerozlišujeme pravou a levou ponožku), musí být alespoň dvě ponožky stejné barvy.

Otázka

Máme 4 přirozená čísla. Ukažte, že mezi nimi vždy najdete dvě čísla tak, aby jejich rozdíl dělitelný číslem 3.

Otázka

Máme 3 přirozená čísla. Ukažte, že mezi nimi vždy najdete dvě čísla tak, aby jejich součet byl dělitelný nějakým prvočíslem.

Handshaking problem

V místnosti je n lidí, někteří si podali ruce. Ukažte, že alespoň dva lidé podali ruku stejnému počtu lidí.

Příklad

Máme 5 přirozených čísel. Ukažte, že mezi nimi vždy najdeme dvě čísla tak, že jejich součet je dělitelný 9.

Důkaz (chybný!) Celkem máme 9 různých zbytkových tříd po dělení číslem 9. Z pěti čísel můžeme získat 10 různých součtů. Jistě bude v každé zbytkové třídě alespoň jeden součet, v některé budou dokonce dva součty. Proto dvojice čísel, jejichž součet odpovídá zbytkové třídě 0, má součet čísel dělitelný devíti. □

Otázka

Co je špatně v uvedeném důkazu předchozího tvrzení?

Nápověda: zkuste úlohu rozebrat pro množinu pěti čísel $\{0, 2, 4, 6, 8\}$.

Kapitola 1. Posloupnosti

- posloupnosti
- sumy a produkty
- aritmetická posloupnost
- geometrická posloupnost
- horní a dolní celá část