Přehled přednášky

Kapitola 3. Důkazy v diskrétní matematice

- několik důkazů „počítáním“

Kapitola 4. Relace

- motivace
- pojem relace
- uspořádání a ekvivalence
- funkce a zobrazení
- skládání zobrazení

3.6. Důkazy „metodou počítání“

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.

Metoda 3.11. 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, jestliže spočítáme, že případů, kdy možnost nemůže nastat je menší než celkový počet případů.

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.

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

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

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 rozdíl čísel dělitelný devíti.
$\square$

Otázka:
Co je špatně na uvedeném důkazu předchozího tvrzení?

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

4. Relace

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.
V rámci této kapitoly se budeme věnovat i *principu inkluze a exkluze*, který má řadu pěkných aplikací.

Přehled

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

4.1. Pojem relace

Jak víme, *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 4.1. *Relace R* na množině A
je libovolné podmnožina kartézského součinu $A \times A = A^2$, tj.

$$R \subseteq A^2.$$

Píšeme $(x, y) \in R$ nebo xRy
(např. $x = y$, $x < y$ místo $(x, y) \in =$, $(x, y) \in <$).

Definice 4.2. *n-ární relace S* na množině A
je libovolné podmnožina kartézské mocniny $A \times A \times \cdots \times A = A^n$, tj.

$$S \subseteq A^n.$$

Relace i mezi *různými* množinami.
Definice 4.1. je speciální případ tzv. *binární relace* (unární, ternární, ...).

Definice 4.3. *(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 navíc reflexivní
- relace dělitelnosti „$|$“ 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

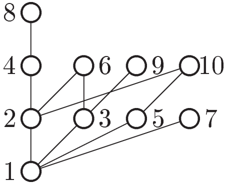
4.2. Uspořádání a ekvivalence

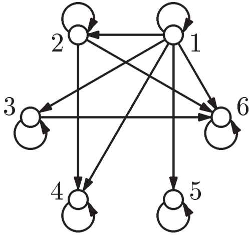
Uspořádání a ekvivalence jsou nejběžnější typy relací.

Definice 4.2. *Částečné uspořádání* $\preceq$ na množině A
je *reflexivní, antisymetrická a tranzitivní* binární relace na množině A.

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 tzv. *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.





Existují i jiná znázornění relací...

Příklady:

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

Definice

Řekneme, že prvky a, b v částečném uspořádání $\preceq$ 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:

- 0 je nejmenší přirozené číslo 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. (jsou „2 je menší než 4 a 6“)
- přirozená čísla bez nuly 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)

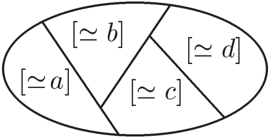
Částečné uspořádání $\preceq$ se nazývá *lineární uspořádání na množině A* (zkráceně *uspořádání na A*), pokud nemá neporovnatelné prvky.
Máme-li uspořádání na A, tak můžeme prvky A uspořádat do jednoho řetězce.

Příklady:

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

Definice 4.5. *Ekvivalence* na množině A
je *reflexivní, symetrická a tranzitivní* binární relace na množině. Značíme $\simeq$.

Definice 4.6. *Třída ekvivalence* prvku x
Máme dánu relaci ekvivalence $\simeq$ na množině A. *Třídou ekvivalence* prvku x (značíme $[\simeq x]$) rozumíme podmnožinu definovanou $[\simeq x] = \{z \in A : z \simeq x\}$.



Relace ekvivalence vyjadřuje vztah „mít stejnou vlastnost".

Příklady:

- relace rovnosti čísel (značí se $=$)
- 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 *rozklad 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 4.6.

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

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

Věta 4.6.

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. Podle definice rozkladu ověříme následující vlastnosti

- $\bigcup_{x \in A} [\simeq x] = A$
  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. $[\simeq x] \cap [\simeq y] \neq \emptyset \Rightarrow [\simeq x] = [\simeq y]$):
  Máme-li nějaké $u \in [\simeq x] \cap [\simeq y]$, tak podle definice třídy rozkladu je $u \simeq x$ a $u \simeq y$, což z tranzitivity a symetrie dává $x \simeq y$. To znamená, že $[\simeq x] = [\simeq y]$. □

Příklady:

- rozklad množiny přirozených čísel podle relace kongruence při dělení n
- rozklad množiny studentů podle relace „mít stejnou známku z DIM“

4.3. Zobrazení (funkce)

Definice 4.7. *Zobrazení (funkce)* z množiny A do B
je podmnožina kartézského součinu $f \subset A \times B$, pro kterou platí, že pro každý prvek $x \in A$ *existuje právě jeden* prvek $y \in B$ takový, aby $(x, y) \in f$.

Zobrazení zapisujeme symbolicky

$$f : A \to B$$

Druhý (jediný) prvek dvojice zapisujeme jednoduše jako

$$y = f(x)$$

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

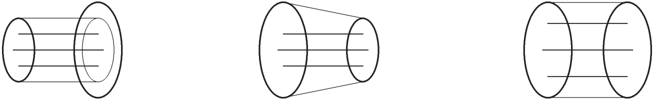
Příklady:

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

Zobrazení často chápeme jako speciální případ relace *mezi* množinami A, B (podmnožina kartézského součinu $A \times B$).
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. $\forall z \in B$ existuje $x \in A$ tak, že $f(x) = z$
- *vzájemně jednoznačná (bijektivní)* je-li f „prostá“ i „na“



Příklady:

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

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. $p(1) = 1$, $p(3) = 5$, $p(6) = 10$, $p(9) = 25$, $\ldots$
- Mějme (A, ρ), (B, σ). $(A, \rho) \simeq (B, \sigma)$ jestliže existuje bijekce
  $f : A \to B : x\rho y \Leftrightarrow f(x)\sigma f(y)$

4.4. Skládání zobrazení

Definice *skládání zobrazení*

Mějme 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

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

Permutace na množině A můžeme chápat jako bijektivní zobrazení $\pi : A \to A$. Mějme $A = [1, n]$. Permutace na A určena pořadím $(p_1, p_2, \ldots, p_n)$. Zobrazení π definujeme předpisem $\pi(i) = p_i$.

Příklady:

Permutace zapisujeme například

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

Nyní můžeme permutace skládat

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

Příště

Kapitola 4. Relace

- permutace jako cykly a skládání permutací
- princip inkluze a exkluze

Kapitola 5. Algoritmizace diskrétních struktur

- programové interpretace struktur
- implementace množin
- generování výběrů
- generátory náhodných čísel
- kombinatorická exploze