

1 Úvod

Poznámka (Co je diskrétní matematika)

Protipól matematiky spojité. Souhrnný název pro matematické disciplíny, zabývající se diskrétními objekty.

Poznámka (Co je potřeba)

Cvičení + zkouška z věcí z přednášky.

Poznámka (literatura)

Kapitoly z diskrétní matematiky od Matouška.

Definice 1.1 (Důkaz (neformální))

Rozebírání tvrzení na tvrzení, která už jsou zřejmá.

Definice 1.2 (Definice (neformální))

Definujeme objekty pomocí jednodušších a jednodušších, až axiomů.

Definice 1.3 (Důkaz sporem)

Dokážeme φ tím, že vyvrátíme φ

Definice 1.4 (Důkaz matematickou indukcí)

Dokážeme $\varphi(n), \forall n \in \mathbb{N}$ tak, že dokážeme $\varphi(0) \wedge (\forall n \in \mathbb{N})(\varphi(n) \implies \varphi(n+1))$

Definice 1.5 (Dolní a horní celá část)

$\lceil x \rceil$ je nejbližší nižší celé číslo k x

$\lfloor x \rfloor$ je nejbližší vyšší celé číslo k x

Definice 1.6 (Sčítání mnoha čísel)

$\sum_{i=13}^n x_i = x_{13} + x_{14} + \dots + x_n =$ Sčítání x od indexu 13 do indexu n

$$\sum_{\emptyset} = 0$$

Definice 1.7 (Sčítání mnoha čísel)

$\prod_{i=13}^n x_i = x_{13} \cdot x_{14} \cdot \dots \cdot x_n =$ Násobení x od indexu 13 do indexu n

$$\prod_{\emptyset} = 1$$

Poznámka (Klasické množiny)

$\mathbb{N} \ \mathbb{Z} \ \mathbb{Q} \ \mathbb{R} \ \mathbb{C}$

Poznámka (Klasické množinové operace)

$$x \in \mathbb{A}$$

$$\mathbb{A} \subseteq \mathbb{B}$$

$$\mathbb{A} \cap \mathbb{B}$$

$$\mathbb{A} \cup \mathbb{B}$$

$$\mathbb{A} \setminus \mathbb{B}$$

$$\mathbb{A} \triangle \mathbb{B} = (\mathbb{A} \setminus \mathbb{B}) \cup (\mathbb{B} \setminus \mathbb{A}) = \text{disperze}$$

$$2^{\mathbb{A}} = \mathcal{P}(\mathbb{A})$$

Definice 1.8 (Uspořádaná dvojice)

Uspořádaná dvojice je (x, y) nebo $\{\{x\}, \{x, y\}\}$.

Vytváří se např. kartézským součinem $\mathbb{A} \times \mathbb{B} := \{(a, b) | a \in \mathbb{A}, b \in \mathbb{B}\}$.

Uspořádaná trojice je $(x, y, z) = ((x, y), z) = (x, (y, z))$. Atd. pro n -tice.

Definice 1.9 (Relace)

\mathbb{A} je relace (binární) mezi množinami \mathbb{X} a $\mathbb{Y} \equiv \mathbb{A} \subseteq \mathbb{X} \times \mathbb{Y}$.

\mathbb{A} je relace (binární) na množině $\mathbb{X} \equiv$ mezi \mathbb{X} a \mathbb{X} .

Inverze je relace mezi \mathbb{Y} a \mathbb{X} : $R^{-1} := \{(y, x) | (x, y) \in R\}$.

Skládání $T = R \circ S = \{(x, z) | \exists y : x R y \wedge y S z\}$

Diagonála = diagonální relace: $\triangle x := \{(x, x) \in \mathbb{X}\}$

Definice 1.10 (Funkce = zobrazení)

Funkce z množiny \mathbb{X} do množiny \mathbb{Y} je relace A mezi \mathbb{X} a \mathbb{Y} taková, že $\forall x \in \mathbb{X} \exists! y \in \mathbb{Y} : x A y$

Definice 1.11 (Vlastnosti funkcí)

Funkce $f : \mathbb{X} \rightarrow \mathbb{Y}$ je:

- prostá (injektivní) $\equiv \nexists x, x' \in \mathbb{X} : x \neq x' \wedge f(x) = f(x')$
- na \mathbb{Y} (surjektivní) $\equiv \forall y \in \mathbb{Y} \exists x \in \mathbb{X} : f(x) = y$
- vzájemně jednoznačná (bijektivní, 1-1 (jedna ku jedné)) $\forall y \in \mathbb{Y} \exists! x \in \mathbb{X} : f(x) = y$

Definice 1.12 (Vlastnosti relací)

Relace R na \mathbb{X} je:

- reflexivní $\equiv \forall x \in \mathbb{X} : xRx$
- symetrická $\equiv \forall x, y \in \mathbb{X} : xRy \implies yRx (\Leftrightarrow R = R^{-1})$
- antisymetrická $\equiv \forall x, y \in \mathbb{X} : xRy \wedge yRx \implies x = y$
- tranzitivní $\equiv \forall x, y, z \in \mathbb{X} : xRy \wedge yRz \implies xRz$

Definice 1.13 (Ekvivalence)

Relace se nazývá ekvivalence, pokud je tranzitivní, reflexivní a symetrická.

Definice 1.14 (Ekvivalenční třídy)

$$R[x] = \{y \in \mathbb{X} | xRy\}$$

Věta 1.1

- 1) $\forall x \in \mathbb{X} R[x] \neq \emptyset$
- 2) $\forall x, y \in \mathbb{X} : R[x] = R[y] \text{ XOR } R[x] \cap R[y] = \emptyset$
- 3) $\{R[x] | x \in \mathbb{X}\}$ určuje ekvivalenci R jednoznačně

┌

Důkaz

1) triviální

2) Dokážeme: pokud $R[x] \cap R[y] \neq \emptyset$, pak $R[x] = R[y]$. (Tranzitivita).

3)

└

□

Definice 1.15 (Rozklad množiny)

Množinový systém $\mathcal{S} \subseteq 2^{\mathbb{X}}$ je rozklad množiny \mathbb{X} tehdy, když

(R1) $\forall A \in \mathcal{S} : A \neq \emptyset$,

(R2) $\forall A, B \in \mathcal{S} : A \neq B \implies A \cap B = \emptyset$,

(R3) $\bigcup_{A \in \mathcal{S}} A = \mathbb{X}$.

Definice 1.16 (Uspořádání)

Relace R na množině \mathbb{X} je uspořádání $\equiv R$ je reflexivní, antisymetrická a tranzitivní.

┌

Poznámka

Někdy se říká částečné uspořádání a částečně uspořádaná množina (čum), aby se zdůraznilo, že nemusí být lineární.

└

Definice 1.17 (Uspořádaná množina)

Dvojice (X, R) , kde X je množina a R je uspořádání na ní.

Definice 1.18 (Porovnatelné prvky a lineární uspořádání)

$xy \in X$ jsou porovnatelné $\equiv xRy \vee yRx$

Uspořádání R je lineární $\equiv \forall x, y \in X$ porovnatelné.

Definice 1.19 (Ostrá nerovnost)

(X, \leq) ČUM $\rightarrow (X, <) : x < y \equiv x \leq y \wedge x \neq y$

Definice 1.20 (Hasseův diagram)

┌

Poznámka

Splňuje následující: 1. To, co je nahoře je větší než to, co je dole

2. Nezakresluje tranzitivitu

└

Definice 1.21 (Bezprostřední předchůdce $(x \triangleleft y)$)

x je bezprostřední předchůdce y v uspořádání $\leq \equiv x < y \wedge (\nexists z : x < z \wedge z < y)$

V hasseově diagramu jsou mezi vrcholy (prvky množiny) hrany pouze, pokud dolní vrchol je bezprostředním předchůdcem toho nahoře.

Definice 1.22 (Nejmenší, minimální, největší a maximální prvek)

- $x \in \mathbb{X}$ je nemenší $\equiv \forall y \in \mathbb{X} : x \leq y$
- $x \in \mathbb{X}$ je minimální $\equiv \nexists y \in \mathbb{X} : y < x$
- největší a maximální obdobně

Lemma 1.2

Každá konečná neprázdná ČUM má minimální prvek.

┌

Důkaz (Důkazík)

└ $x_1 \in \mathbb{X}$ zvolíme libovolně, pokud x_1 není minimální $\exists x_2 < x_1 \dots \exists k \in \mathbb{N} x_k$ je minimální. \square

Definice 1.23 (Řetězec)

Pro (X, \leq) ČUM $A \subseteq X$ je řetězec $\equiv \forall a, b \in A : a, b$ jsou porovnatelné.

Naopak $A \subseteq X$ je antiřetězec (nezávislá množina) $\equiv \nexists a, b \in A$ různé a porovnatelné.

Definice 1.24 (Délka nejdelšího řetězce)

$\omega(X, \leq) :=$ maximum z délek řetězců („výška uspořádání“)

$\alpha(X, \leq) :=$ maximum z „délek“ (velikostí) antiřetězců („šířka uspořádání“)

Věta 1.3 (O dlouhém a Širokém)

$$\forall (X, \leq) \text{ ČUM} : \alpha(X, \leq) \cdot \omega(X, \leq) \geq |X|$$

(Neboli buď $\alpha \geq \sqrt{|X|}$ nebo $\omega \geq \sqrt{|X|}$.)

┌ *Důkaz*

Sestrojíme $X_1 := \{x \in X \mid x \text{ je minimální}\}$.

Když máme X_1, \dots, X_i , $Z_i := X \setminus \left(\bigcup_{j=1}^i x_j\right)$. Pokud $Z_i = \emptyset$, tak jsme skončili, jinak $X_{i+1} := \{x \in Z_i \mid x \text{ je minimální v } Z_i\}$.

Přitom $\forall i$ X_i je antiřetězec, $\{X_1, \dots, X_k\}$ tvoří rozklad X a $\exists \{r_j \in X_j\}_{j=1}^k$, $\{r_j\}_{j=1}^k$ je řetězec. ($r_k \in X_k$ zvolíme libovolně, $r_j \notin X_{j-1} \implies \exists r_{j-1} \in X_{j-1} : r_{j-1} < r_j$.)

$$|X| = \sum_{i=1}^k |X_i| \leq k \cdot \max_{1 \leq i \leq k} |X_i| \leq \omega \cdot \alpha.$$

└

□

Věta 1.4

$\#f : N \rightarrow M = m^n, |N| = n, |M| = m, m > 0, n > 0$

┌

Důkaz (Indukcí)

$$n = 1 : \#f = m = m^1$$

$$n \rightarrow n + 1 : f \text{ jednoznačně určena } f(x) \text{ a } f' : N \setminus \{x\} \rightarrow M \implies \#f = m \cdot m^n = m^{n+1}$$

└

□

Věta 1.5

Je-li N n -prvková množina, pak $|2^N| = 2^n$.

┌

Důkaz

charakteristická funkce: $A \subseteq N \rightarrow C_A : N \rightarrow \{0, 1\} \ C_A(x) = 0, x \notin A, C_A(x) = 1, x \in A$

└

□

Věta 1.6

Nechť $X \neq \emptyset$ je konečná množina, $\mathcal{S} := \{S \subseteq X \mid |S| \text{ je sudá}\}$, $\mathcal{L} := \{L \subseteq X \mid |L| \text{ je lichá}\}$.
Potom $|\mathcal{S}| = |\mathcal{L}| = 2^{n-1}$.

┌

Důkaz

Víme, že $\mathcal{S} \cup \mathcal{L} = 2^X$. Stačí tedy $|\mathcal{S}| = |\mathcal{L}|$. Zvolíme si $a \in X$. Pak $f(S) := S \Delta \{a\}$ je bijekce z \mathcal{S} do \mathcal{L} .

└

□

Věta 1.7

Nechť N je n -prvková, M je m -prvková. Potom $\#f : N \rightarrow M$ prostých $= m \cdot (m-1) \cdot \dots \cdot (m-n+1)$.

Poznámka (Možná značení)

$$[n] := \{0, 1, \dots, \}$$
$$m^n = \frac{m!}{(m-n)!} (m \text{ na } n \text{ klesající})$$

Poznámka (Kódování funkcemi)

- $X \rightarrow \{0, 1\} \dots 2^X$
- $\{1, 2\} \rightarrow X \dots (x, y) \in X^2$
- $\{1, \dots, k\} \rightarrow X \dots$ uspořádané k -tice $\dots X^k$
- $\mathbb{N} \rightarrow X \dots$ nekonečné posloupnosti prvků X
- permutace na X , tj. počet bijekcí nebo počet lineárních uspořádání na konečném X
 $\dots |X|!$ ($0! = 1$)

Definice 1.25 (Kombinační číslo)

Kombinační číslo / binomický koeficient (n nad k) je $\binom{n}{k} := \frac{n!}{k!(n-k)!}$.

Definice 1.26

Pro množinu X a $k \geq 0$ definujeme $\binom{X}{k} := \{A \subseteq X : |A| = k\}$.

Věta 1.8

Pro každou množinu X a $k \geq 0$: $|\binom{X}{k}| = \binom{|X|}{k}$.

Poznámka (Vlastnosti kombinačních čísel)

$$\binom{n}{0} = \binom{n}{n} = 1$$
$$\binom{n}{1} = \binom{n}{n-1} = n$$
$$\binom{n}{k} = \binom{n}{n-k}$$

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \quad (\text{Lze upočítat / nebo rozdělit na případ vybereme / nevybereme konkrétní})$$

$$\sum_{k=0}^n \binom{n}{k} = 2^n \quad \text{BV } A = 1, B = 1$$

$$\sum_{k=0}^n (-1)^k \binom{n}{k} = 0 \quad \text{BV } A = 1, B = -1$$

Poznámka

Vlastnosti se dají vykoukat v tzv. Pascalově trojúhelníku.

Věta 1.9 (Binomická)

$$(A + B)^n = \sum_{k=0}^n A^k \cdot B^{n-k} \cdot \binom{n}{k}$$

Důkaz

Vybírá se k z n členů, ze kterých bude A ...

□