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 $\varphi(0) \land (\forall n \in \mathbb{N})(\varphi(n) \implies \varphi(n+1))$

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)

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

$\sum_{\emptyset} = 0$

Definice 1.7 (Sčítání mnoha čísel)

$\prod_{i=13}^{n} x_i = x_{13} \cdot x_{14} \cdot \ldots \cdot x_n =$ 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 $T = R \circ S = \{(x, z) | \exists y : xRy \wedge ySz\}$

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 $\forall x \in \mathbb{X} \exists ! y \in \mathbb{Y} : xAy$

Definice 1.11 (Vlastnosti funkcí)

Funkce $f : \mathbb{X} \to \mathbb{Y}$ 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 (Vlastnoti 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

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

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) $\forall \mathbb{A} \in \mathcal{S} : \mathbb{A} \neq \emptyset$,
(R2) $\forall \mathbb{A}, \mathbb{B} \in \mathcal{S} : \mathbb{A} \neq \mathbb{B} \implies \mathbb{A} \cap \mathbb{B} = \emptyset$,
(R3) $\bigcup_{\mathbb{A} \in \mathcal{S}} = \mathbb{X}$.

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. Nezakreslujeme tranzitivitu

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

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 $\exists x_2 < x_1 ... \exists k \in \mathbb{N} x_k$ 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)

$$\omega(X, \leq) := \text{maximum z délek řetězců („výška uspořádání“)}$$
$$\alpha(X, \leq) := \text{maximum z „délek“ (velikostí) antiřetězců („šířka uspořádání“)}$$

Věta 1.3 (O dlouhém a Širokém)

$$\forall (X, \leq) \check{C}UM : \alpha(X, \leq) \cdot \omega(X, \leq) \geq |X|$$

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

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

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 $X_{i+1} := \{x \in Z_i | x \text{je minimální v} Z_i\}$.

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, $r_j \notin X_{j-1} \implies \exists r_{j-1} \in X_{j-1} : r_{j-1} < r_j$.)

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

$\square$

Věta 1.4

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

Důkaz (Indukcí)

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

$\square$

Věta 1.5

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

Důkaz

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

$\square$

Věta 1.6

Nechť $X \neq \emptyset$ je konečná množina, $\mathcal{S} := \{S \subseteq X || S| \text{je sudá}\}$, $\mathcal{L} := \{L \subseteq X || L| \text{je lichá}\}$. 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 $f(S) := S \triangle \{a\}$ je bijekce z $\mathcal{S}$ do $\mathcal{L}$. $\square$

Věta 1.7

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

Poznámka (Možná značení)

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

Poznámka (Kódování funkcemi)

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

Definice 1.25 (Kombinační číslo)

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

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 $k \geq 0$: $\left|\binom{X}{k}\right| = \binom{|X|}{k}$.

Poznámka (Vlastnosti kombinačních čísel)

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

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

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

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0 \text{ BV } A = 1,\ B = -11$$

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... □

Věta 1.10 (Princip inkluze a exkluze)

Pro konečné množiny $A_1 - A_n$:

$$\left| \bigcup_{i=1}^{n} \right| = \sum_{k}^{n} (-1)^{k+1} \sum_{I \in \binom{\{1,2,\ldots,n\}}{k}} \left| \bigcap_{i \in I} A_i \right|$$

Nebo alternativně:

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

Důkaz
Pro každý prvek $x \in \bigcup_i A_i$ spočítáme příspěvky k levé (vždy 1) a k pravé straně. Nechť x patří právě j množin z $A_1, \ldots, A_n$. Průniky k-tic: (1) $k > j$ přispěje 0. (2) $k \leq j$ přispěje $(-1)^{k+1}\binom{j}{k}$. Součet toho je alternující řada kombinačních čísel „bez 1“, tedy součet je 1. □

Důkaz (Druhý)
Vyjdeme z

$$\prod_{i=1}^{n}(1+x_i) = \sum_{I\subseteq\{1,\ldots,n\}} \prod_{i\in I} x_i.$$

Definujeme si charakteristickou funkci a zjistíme, že ch. f. průniku je součin, doplňku je 1-ch. f. původního, sjednocení je doplněk průniku doplňků a velikost je součet ch. funkce. Tedy dosadíme za x_i mínus charakteristické funkce (1 nám vypadla z prázdné podmnožiny):

$$1 - c_{\bigcup_i A_i} = \left(\sum_{\emptyset\neq I\subseteq\{1,\ldots,n\}} (-1)^{|I|} \cdot c_{\bigcap_{i\in I} A_i} \right) + 1$$

Následně ještě přeformulujeme do velikostí a získáme princip inkluze a exkluze. $\square$

Příklad (Šatnářka)
Šatnářka náhodně vydala klobouky gentlemanům. Jaká je pravděpodobnost, že se ani jeden klobouk nedostal k majiteli?

Tj. $S_n := \{\pi | \pi \text{ permutace na } \{1,\ldots,n\}\}$, $\pi(i) = i \implies i$ je pevný bod:

$$\check{S}_n := \{\pi \in S_n | \nexists i : \pi(i) = i\}.$$

Příklad se tedy ptá na $\frac{\check{S}_n}{n!}$.

Řešení
Lepší je počítat doplněk: $A := \{\pi \in S_n | \pi \text{ má pevný bod}\}$. Definujeme si $A_i := \{\pi \in S_n | \pi(i) = i\}$. Následně vypozorujeme $A = \bigcap_i A_i$. Očividně $|A_i| = (n-1)!$, $|A_i \cup A_j| = (n-2)!$ $(i \neq j)$, ...

$$|A| = \left|\bigcup_{i=1}^{n}\right| = \sum_{k=1}^{n}(-1)^{k+1} \sum_{I\in\binom{\{1,\ldots,n\}}{k}} \left|\bigcap_{i\in I} A_i\right| = \sum_{k=1}^{n}(-1)^{k+1} \sum_{I\in\binom{\{1,\ldots,n\}}{k}} (n-k)! = \sum_{k=1}^{n}(-1)^{k+1}\binom{n}{k}(n-k)! = \sum_{k}$$

$$|A| = n!\sum_{k=1}^{n}\frac{(-1)^{k+1}}{k!} = n!(\frac{1}{1!} - \frac{1}{2!} + \frac{1}{3!} - \ldots + \frac{(-1)^{n+1}}{n!})$$

$$\check{S}_n = |A| \doteq n!\frac{1}{e}$$

2 Odhady

Například

$$2^{n-1} \leq n! \leq n^n$$
$$n^{n/2} \leq n! \leq \left(\frac{n+1}{2}\right)^n$$
$$*\left(\frac{n}{e}\right)^n \leq n! \leq en \cdot \left(\frac{n}{e}\right)^n$$
$$**\, n! \sim \left(\frac{n}{e}\right)^n \cdot \sqrt{2\pi n}$$
$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq n^k$$
$$*\binom{n}{k} \leq \left(\frac{en}{k}\right)^k$$
$$\frac{4^n}{2n+1} \leq \binom{2n}{n} \leq 4^n$$
$$*\frac{4^n}{2\sqrt{n}} \leq \binom{2n}{n} \leq \frac{4^n}{\sqrt{2n}}$$

3 Grafy

Definice 3.1 (Graf, vrcholy, hrany)

Graf je uspořádaná dvojice (V, E), kde: V je konečná neprázdná množina vrcholů (vertices) a $E \subseteq \binom{V}{2}$ je množina hran (edges).

Poznámka (Rozšíření)
Orientované, se smyčkami, multigrafy, nekonečné.

Například
Úplný graf (K_n): $V(K_n) := \{1, \ldots, n\}$ a $E(K_n) := \binom{V(K_n)}{2}$.

Prázdný graf (E_n): $V(E_n) := \{1, \ldots, n\}$ a $E(E_n) := \emptyset$.

Cesta (P_n): $V(P_n) := \{0, 1, \ldots, n\}$ a $E(P_n) := \{\{i, i+1\} \,|0 \leq i < n\}$.

Kružnice (C_n): $V(C_n) := \{0, 1, \ldots, n-1\}$ a $E(C_n) := \{\{i, i+1 \mod n\} \,|0 \leq i \leq n\}$.

Úplný bipartitní graf $(K_{m,n})$: $V(K_n) := \{a_1, \ldots, a_n\} \cup \{b_1, \ldots, b_n\}$ a $E(K_n) := \{\{a_i, b_j\} \,|1 \leq i \leq m, 1 \leq$

Definice 3.2 (Bipartitní graf)

Graf G je bipartitní $\equiv$ $\exists$ rozklad množiny $V(G)$ na X, Y (= partity) tak, že $E(G) \subseteq \{\{x, y\} \,|x \in X, y \in Y\}$. (Lze zapsat i jako $\forall e \in e(G) : |e \cap X| = 1$.)

Definice 3.3 (Isomorfismus grafů)

Grafy G a H jsou isomorfní (značme $G \cong H$) $\equiv$ $\exists f : V(G) \to V(H)$ bijekce tak, že $\forall u, v \in V(G) : (\{u, v\} \in E(g) \Leftrightarrow \{f(u), f(v)\} \in E(H))$.

Poznámka (K nahlédnutí)
Na libovolné množině grafů je $\cong$ ekvivalence.

Definice 3.4 (Stupeň vrcholu)

Stupeň vrcholu v v grafu G je $\deg_G(v) := |\{u \in V(G)| \, \{u, v\} \in E(G)\}|$.

Definice 3.5 (Regulární graf)

Graf je k-regulární (pro $k \in \mathbb{N}$) $\equiv \forall u \in V(G) : \deg_G(u) = k$.

Graf G je regulární $\equiv \exists k : G$ je k-regulární.

Definice 3.6 (Skóre grafu)

Skóre grafu G je posloupnost stupňů všech vrcholů (až na uspořádání).

Věta 3.1

Pro každý graf (V, E) platí:

$$\sum_{v \in V} \deg(v) = 2 \cdot |E|$$

Důsledek (Princip sudosti)
$\sum_v \deg(v)$ je sudé číslo $\implies$ ($\#v \in V$ lichého stupně) je sudý.

Věta 3.2 (O skóre)

Posloupnost $D = d_1 \leq \ldots \leq d_n$ pro $n \geq 2$ je skóre grafu $\Leftrightarrow D' = d'_1, \ldots, d'_{n-1}$ je skóre grafui a $0 \leq d_n \leq n - 1$. ($d'_i = d_i$ pro $i < n - d_n$ a $d'_i = d_i - 1$ pro $i \geq n - d_n$.)

Důkaz
($\Leftarrow$) nechť G' je graf se skóre D' a vrcholy $v_1, \ldots, v_{n-1}$ tak, že $\forall i \deg_{G'}(v_i) = d_i'$. Vytvořím G doplněním vrcholu v_n a hran $\{v_i, v_n\}$ pro $i \in \{n - d_n, \ldots, n-1\}$. G má skóre D.

($\implies$) Lemma: Nechť $\mathcal{G}$ je množina všech grafů se skóre D, $\mathcal{G} \neq \emptyset$. Potom $\exists G \in \mathcal{G}$: $\{v_n, v_i\} \in E(G)$ pro všechna $i \in \{n - d_n, \ldots, n-1\}$.

Důkaz lemmatu: (Kdyby $d_n = n - 1$, pak zřejmě každý $G \in \mathcal{G}$ splňuje lemma.) Pro $G \in \mathcal{G}$ definujeme $j(G) := \max\{j | \{v_j, v_n\} \notin E(G)\}$ (kdyby $j(g) = n - d_n i - 1$, pak jsme vyhráli, jinak G nesplňuje lemma). Najdeme $G \in \mathcal{G}$, jehož $j(G)$ je minimální. Pokračujeme sporem: Kdyby $j(G) > n - d_n - 1$, musí $\exists i < j : \{v_i, v_n\} \in E(G)$. Následně chceme ukázat, že $\exists k : \{v_i, v_k\} \notin E(G) \wedge \{v_j, v_k\} \in E(G)$, to ukážeme na základě toho, že posloupnost je seřazena, tedy $d_i \leq d_j$ a vrchol v_i je spojen minimálně s jedním vrcholem, se kterým není spojené v_j (v_n). Upravíme graf G na G : $V(G\ ) := V(G), E(G\ ) := E(G) \cup \{\{v_i, v_k\}, \{v_j, v_n\}\} \setminus \{\{v_i, v_n\}, \{v_j, v_k\}\}$. Ale jelikož jsme vrcholům odstranili stejný počet hran, jako přidali, $G \in \mathcal{G}$. Navíc zřejmě $j(G\ ) < j(G)$, . $\square$