

# Kombagra

Tomáš Turek

*Přednáška 1*

---

## Odhady faktoriálu

- $n \in \mathbb{N} : n!$
- Poskládání  $n$  prvků.

### Tvrzení 1.1

- $\forall n \in \mathbb{N} : n^{n/2} \leq n! \leq n^n$

### Věta 1.2:

- $\forall n \in \mathbb{N} : e(\frac{n}{e})^n \leq n! \leq en(\frac{n}{e})^n$

### Lemma 1.3:

- $1 + x \leq e^x$

### Věta 1.4 (Stirlingův vzorec):

$$n! \approx n\sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$
$$\lim_{n \rightarrow \infty} \frac{n!}{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n} = 1$$

## Binomický koeficient

- počet  $k$ -prvkových podmnožin  $n$ -prvkových množin
- $n, k \in \mathbb{N} : \binom{n}{k} = \frac{n!}{k!(n-k)!}$

### Pozorování 1.5:

1.  $\forall n, k \in \mathbb{N} : \left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq n^k$
2. největší prvek  $\binom{n}{\lceil \frac{n}{2} \rceil} = \binom{n}{\lfloor \frac{n}{2} \rfloor}$

### Binomická věta

$$\frac{2^{2m}}{2m+1} \leq \binom{2m}{m} \leq 2^{2m}$$

### Věta 1.6:

$$\forall m \in \mathbb{N} : \frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}$$

- užití Stirlingovského vzorce:  $\binom{2m}{m} \approx \frac{2^{2m}}{\sqrt{\pi m}}$
- $\forall k, n \in \mathbb{N} : n > k, \binom{n}{k} \leq \left(\frac{en}{k}\right)^k$

### Aplikace (náhodné procházky)

- $n$  kroků a v každém bodě mám 50 % že půjdu doprava anebo doleva
- střední hodnota počtu návratů do 0
- $X$  - počet návratů do 0
- $A_{2n}$  = jev po  $2n$  krocích se dostanu do 0
- $X = \sum_{n=1}^{\infty} I_{A_{2n}}$
- $Pr[A_{2n}] = \frac{\binom{2n}{n}}{2^{2n}}$

$$\begin{aligned} \mathbb{E}[X] &= \mathbb{E}\left[\sum_{n=1}^{\infty} I_{A_{2n}}\right] = \sum_{n=1}^{\infty} \mathbb{E}[I_{A_{2n}}] = \\ &= \sum_{n=1}^{\infty} Pr[I_{A_{2n}}] = \sum_{n=1}^{\infty} \frac{\binom{2n}{n}}{2^{2n}} \geq \sum_{n=1}^{\infty} \frac{1}{2\sqrt{n}} = \infty \end{aligned}$$

Přednáška 2

---

### Vytvořující funkce

- početní metoda, kde spojitými funkcemi vyjadřujeme posloupnosti

### Definice

- Pro posloupnost  $(a_i)_{i=0}^{\infty}$  je mocninnou řadou  $a(x) = \sum_{i=0}^{\infty} a_i x^i$ .
- Posloupnost lze převést na funkci, ale při převodu nazpátek je třeba aby posloupnost nerostla moc rychle.

### Příklady:

1.  $a_i = 1$  pokud  $0 \leq i \leq n$  jinak  $a_i = 0$ . Tedy  $(a_i)_{i=0}^{\infty} = (1, \dots, 1, 0, 0, \dots)$ .  
Potom funkce je  $\frac{1-x^{n+1}}{1-x}$  z geometrické řady.
2.  $\forall i : a_i = 1$  to je potom nekonečná geometrická řada, takže je to  $\frac{1}{1-x}$ .
3.  $a_i = \binom{n}{i}$  potom funkce vychází z binomické věty, takže je  $(1+x)^n$ .

### Tvrzení 2.1:

- Pokud pro  $(a_i)_{i=0}^\infty \exists k \in (R)$  takové, že  $\forall i : |a_i| \leq k^i$ , pak pro všechna  $x \in (-\frac{1}{k}, \frac{1}{k})$  řada  $a(x) = \sum_{i=0}^\infty a_i x^i$  konverguje absolutně a na libovolném  $\epsilon$  okolí 0 určuje i *koefficienty* $_a$ , protože  $i_a = \frac{a^{(i)}(0)}{i!}$ .

### Postup

1. kombinatorický objekt s neznámým počtem
2. vytvářející funkce
3. rozklad na vytvářející funkce se známými koeficienty
4. určení hodnoty

### Tabulka

Operace	Posloupnosti	Funkce
Součet	$(a_0 + b_0, a_1 + b_1, \dots)$	$(a + b)(x) = \sum_{i=0}^\infty (a_i + b_i)x^i$
$\alpha$ -násobek	$(\alpha a_0, \alpha a_1, \dots)$	$\alpha a(x) = \sum_{i=0}^\infty (\alpha a_i)x^i$
Posun vpravo o $n$ pozic	$(0, 0, \dots, a_0, a_1, \dots)$	$x^n a(x) = \sum_{i=0}^\infty a_i x^{i+n}$
Posun vlevo o $n$ pozic	$(a_n, a_{n+1}, \dots)$	$\sum_{i=0}^\infty (a_{i+n} x^i = \frac{a(x) - \sum_{i=0}^{n-1} a_i x^i}{x^n}$
Dosazení $\alpha x$	$(a_0, \alpha a_1, \alpha^2 a_2, \dots)$	$a(\alpha x) = \sum_{i=0}^\infty a_i + \alpha^i x^i$
Dosazení $x^n$	$(a_0, 0, \dots, 0, a_1, 0, \dots, 0, a_2, \dots)$	$a(x^n) = \sum_{i=0}^\infty a_i x^{ni}$
Derivace	$(a_1, 2a_2, 3a_3, \dots)$	$a'(x) = \sum_{i=1}^\infty i a_i x^{i-1}$
Integrál	$(0, a_0, \frac{a_1}{2}, \frac{a_2}{3}, \dots)$	$\int_0^x a(x) dx = \sum_{i=0}^\infty \frac{a_i}{i+1} x^{i+1}$
Součin	$(c_0, c_1, c_2, \dots)$	$a(x)b(x) = \sum_{i=0}^\infty (c_i)x^i$

### Řešení rekurentních rovnic

- ukázka na Fibonacciho čísla
- určíme  $F_n$  jako koeficient funkce  $F(x) = \sum_{i=0}^\infty F_i x^i$
- máme  $F_{n+2} = F_{n+1} + F_n, \forall n \geq 0$
- **vynásobíme rovnicí  $x^n$ :  $F_{n+2}x^n = F_{n+1}x^n + F_nx^n$**
- **sčítáme přes  $n \geq 0$ :  $\sum_{n \geq 0} F_{n+2}x^n = \sum_{n \geq 0} F_{n+1}x^n + \sum_{n \geq 0} F_nx^n$**
- to se rovná

$$\frac{F(x) - F_0 - F_1 x}{x^2} = \frac{F(x) - F_0}{x} + F(x)$$

- teď určíme

$$F(x) = \frac{x}{1 - x - x^2} = \frac{x}{(1 - \frac{1+\sqrt{5}}{2}x)(1 - \frac{1-\sqrt{5}}{2}x)} = \frac{\frac{1}{\sqrt{5}}}{1 - \frac{1+\sqrt{5}}{2}x} - \frac{\frac{1}{\sqrt{5}}}{1 - \frac{1-\sqrt{5}}{2}x}$$

- to už lze převést

$$F_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right]$$

- to je tzv. **Binetův vzorec**
- tento postup funguje pro všechny **Homogenní lineární rekurence k-tého stupně s konstantními koeficienty**, tedy typu  $a_{n+k} = \alpha_{k-1}a_{n+k-1} + \dots + \alpha_0 a_n, k \in \mathbb{N}, \alpha_{k-1}, \dots, \alpha_0 \in \mathbb{R}$

Přednáška 3

---

## Aplikace vytvářících funkcí

- nadefinujeme zobecněnou **binomickou vět** pro  $n \in \mathbb{R}, r \in \mathbb{Z}_0^+ : \binom{n}{r} := \frac{n(n-1)(n-2)\dots(n-r+1)}{r!}$ , speciálně  $\binom{n}{0} = 1$

**Věta 3.1 (Zobecněná binomická věta):**

$\forall r \in \mathbb{R}$  je  $(1+x)^r$  vytvářící funkcí posloupnosti  $\left(\binom{r}{0}, \binom{r}{1}, \binom{r}{2}, \dots\right)$  a řada  $\sum_{i=0}^{\infty} \binom{r}{i} x^i$  konverguje pro  $\forall x \in (-1, 1)$ .

**Důsledek 3.2:**

$\forall n \in \mathbb{N} \forall x \in (-1, 1)$  platí  $\frac{1}{(1-x)^n} = \sum_{i=0}^{\infty} \binom{n+i-1}{n-1} x^i$ .

## Aplikace - počítání binárních zakořeněných stromů

- **Zakořeněný binární strom** - buď je prázdný, nebo obsahuje speciální vrchol zvaný **kořen** a pár zakořeněných stromů, které tvoří **levý** a **pravý podstrom**.
- $b_n$  = počet bin. zak. stromů na  $n \in \mathbb{N}_0$  vrcholech
- potom  $b(x) = \sum_{n=0}^{\infty} b_n x^n$  je příslušná vytvářící funkce

**Věta 3.3:**

- Pro každé  $n \in \mathbb{N}_0$  platí  $b_n = \frac{1}{n+1} \binom{2n}{n}$ . Kde se  $\frac{1}{n+1} \binom{2n}{n}$  značí jako  $C_n$  a říká se mu **n-té Catalanovo číslo**.
- Catalanova čísla mají mnoho interpretací, například počet triviálních uzávorkování s  $n$  páry závorek anebo počet triangulací.

Přednáška 4

---

## Konečně projektivní roviny (KPR)

- jistá nová struktura, která je velice symetrická a vzácná
- jedná se o množinový systém (**hypergraf** - zobecnění grafu, kde hrany mohou být k-tice)
- využívá se v samoopravných kódech
- přichází z geometrie

### Eukleidovy axiomy

1. každé 2 body určují přímku
2. každou úsečku lze prodloužit na přímku
3. ze zadaného bodu lze opsat kružnici procházejícím druhým zadaným bodem
4. všechny pravé úhly jsou stejné
5. bodem lze k přímce vést právě 1 rovnoběžku

### Definice KPR:

- Konečná množina  $\mathcal{X}$  a systém  $\mathcal{P}$  podmnožin  $\mathcal{X}$  tvoří KPR  $(\mathcal{X}, \mathcal{P}) = (\text{body}, \text{přímky})$  pokud splňuje tyto tři axiomy:
  1.  $\forall x, y \in \mathcal{X}, x \neq y, \exists! P \in \mathcal{P} : \{x, y\} \subseteq P$ 
    - každé 2 body určují právě jednu přímku
  2.  $\forall P, Q \in \mathcal{P}, P \neq Q : |P \cap Q| = 1$ 
    - každé 2 přímky se protínají právě v 1 bodě
  3.  $\exists C \subseteq \mathcal{X}, |C| = 4, \forall P \in \mathcal{P} : |C \cap P| \leq 2$ 
    - existují 4 body v obecné poloze
- Jako příklad je **Fanova rovina**, která má 7 přímek a 7 bodů.

### Tvrzení 4.1:

- V KPR obsahuje každá přímka stejný počet bodů.  $\forall P, Q \in \mathcal{P} |P| = |Q|$

### Řád projektivní roviny:

- $(\mathcal{X}, \mathcal{P})$  je  $|P| - 1$  pro  $P \in \mathcal{P}$

### Tvrzení 4.2:

- Je-li  $(\mathcal{X}, \mathcal{P})$  KPR řádu  $n$ , pak platí:
  1. každým bodem prochází právě  $n + 1$  přímek
  2.  $|\mathcal{X}| = n^2 + n + 1$
  3.  $|\mathcal{P}| = n^2 + n + 1$

### Dualita KPR

- “přechod z přímek na body a z bodů na přímky”

- **duální množinový systém** k množinovému systému  $(\mathcal{X}, \mathcal{P})$  je  $(\mathcal{P}, \{\{P \in \mathcal{P} : x \in P\} : x \in \mathcal{X}\})$ , zkráceně **duál**

**Tvrzení 4.3:**

- Duálem KPR řádu  $n$  je KPR řádu  $n$ .

**Existence KPR:**

- Kromě Fanovy roviny zatím neznáme žádné další příklady konečných projektivních rovin. Ale samozřejmě se ví o dalších které existují jmenovitě pro  $(2, 3, 4, 5, 7, 8, 9, 11)$  a 12 už se neví.

**Domněnka**

- KPR řádu  $n$  existuje  $\Leftrightarrow n$  je mocnina prvočísla
- pořad otevřené

**Věta 4.4:**

- Pokud existuje algebraické těleso o  $n$  prvcích, potom existuje KPR řádu  $n$ .
- konstrukce funguje nad každým tělesem a například nad  $\mathbb{R}$  dává **reálnou projektivní rovinu**

*Přednáška 5*

---

**Latinský čtverec**

- řádu  $n \in \mathbb{N}$  je tabulka  $n \times n$  čísel z  $\{1, \dots, n\}$ , ve které se žádné číslo neopakuje v žádném řádku ani sloupci.

**Ortogonalita**

- Latinský čtverce  $L, L'$  stejného řádu jsou **ortogonální**, pokud pro každé  $l, l' \in \{1, \dots, n\}$  existují  $i, j \in \{1, \dots, n\}$ , takové že  $L_{ij} = l, L'_{ij} = l'$ .
- zapisuje se jako  $L \perp L'$

**Pozorování 5.2:**

- Pro ortogonální latinské čtverce  $L, L'$  řádu  $n$  a pár  $(l, l') \in \{1, \dots, n\} \times \{1, \dots, n\}$  je pozice  $(i, j)$  s  $L_{ij} = l, L'_{ij} = l'$  určena jednoznačně.

**Pozorování 5.3:**

- Je-li  $L = (L_{ij})_{i,j=1}^n$  latinský čtverec a  $\Pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  permutace, tak potom  $\Pi(L) := (\Pi(L_{ij}))_{i,j=1}^n$  je latinský čtverec stejného řádu.

- $\Rightarrow$  BÜNO první řádek je vždy vzestupná řada
- $\Rightarrow$  Je-li  $L \perp L'$ , pak  $\Pi(L) \perp L'$

**Důsledek 5.4:**

- Počet **navzájem ortogonálních** nanejvýš čtverců řádu  $n \in \mathbb{N}$  je  $n - 1$ .

**Věta 5.5:**

- Konečná projektivní rovina řádu  $n \geq 2$  existuje  $\Leftrightarrow$  existuje  $n - 1$  navzájem ortogonálních latinských čtverců řádu  $n$ .

*Přednáška 6*

---

## Toky v sítích

- Sít je čtveřice  $(G, z, s, c)$ , kde  $G = (V, E)$  je orientovaný graf (tedy  $V \subseteq V \times V$ ),  $z \in V$  je **zdroj**,  $s \in V$  je **stok** ( $z \neq s$ ) a  $c : E \rightarrow \mathbb{R}_0^+$ . Hodnotu  $c(e)$  nazýváme **kapacitou** hrany  $e \in E$ .
- Tok v síti  $(G = (V, E), z, s, c)$  je  $f : E \rightarrow \mathbb{R}_0^+$  splňující následující podmínky:
  1.  $\forall e \in E : 0 \leq f(e) \leq c(e)$ 
    - velikost toku je omezená kapacitou
  2.  $\forall u \in V \setminus \{z, s\} : \sum_{v:(u,v) \in E} f(u, v) - \sum_{v:(v,u) \in E} f(v, u) = 0$ 
    - **Kirchhoffův zákon** co přitéká do vrcholu, musí odtéct
- **Velikost toku**  $f$  je  $w(f) = \sum_{v:(z,v) \in E} f(z, v) - \sum_{v:(v,z) \in E} f(v, z)$

**Tvzezení 6.1:**

- Pro každou síť existuje maximální tok.

**Řez v síti**  $(G, z, s, c)$

- je  $R \subseteq E$  taková, že každá orientovaná cesta ze zdroje  $z$  do stoku  $s$  používá aspoň jednu hranu z  $R$ .
- speciálně hrany vycházející ze  $z$  či hrany vycházející do  $s$  tvoří řez
- **kapacita řezu**  $R$  je  $c(R) = \sum_{e \in R} c(e)$
- řezu je jen konečně mnoho  $\Rightarrow$  jistě existuje řez minimální kapacity

**Věta 6.2 (hlavní věta o tocích):**

- Velikost maximálního toku = kapacita minimálního řezu, nebo-li, pro každou síť platí:  $\max w(f) = \min c(R)$ , kde  $f$  je tok a  $R$  řez.

### Elementární řez

- pro  $A \subseteq V$ , kde  $z \in A$  a  $s \notin A$ , nazveme množinu  $R_A = \{e = (u, v) \in E : u \in A, v \notin A\}$  **elementárním řezem**
- opravdu se jedná o řez, protože pokaždé su musí nějak opustit  $A$

### Pozorování 6.3:

- Každý řez  $R$  obsahuje elementární řez.

### Pozorování 6.4:

- Každý **v inkluzi minimální** řez  $R$  je elementární. Nebo-li  $R \setminus \{e\}$  není řezem pro  $\forall e \in R$ .

### Lemma 6.5:

- Je-li  $f$  tok a  $R_A$  elementární řez, pak platí

$$w(f) = \sum_{u \in A, v \notin A, (u,v) \in E} f(u, v) - \sum_{u \in A, v \notin A, (v,u) \in E} f(v, u)$$

### Fordův-Fulkersonův algoritmus

1. Nastav  $f(e) = 0$  pro  $\forall e \in E$
2. Dokud  $\exists$  zlepšující cesta  $P$ , vylepšuj po ní tok o  $\epsilon_P$
3. Stávající tok  $f$  vrať jako maximální

### Věta 6.6 (věta o celočíselnosti):

- Jsou-li kapacity celočíselné, pak F.F. najde max. tok po konečně mnoha krocích a navíc má takový tok celočíselnou velikost.
- existují sítě s iracionálními kapacitami, kde F.F. nenajde max. tok a ani nekonverguje k výsledku
- v síti s celočíselnými kapacitami má F.F. alg. časovou složitost  $O(w(f)(|V| + |E|))$ , kde  $f$  je tok
  - takže je to v čase  $O(|V| + |E|)$
- pokud bychom specifikovali výběr zlepšující cesty na nejkratší dostaneme **Edmondsův-Karpův algoritmus**, který má časovou složitost  $O(|V| + |E|^2)$

Přednáška 7

---

### Königova-Egerváryho věta

- V grafu  $G = (V, E)$  nazveme množinu  $C \subseteq V$  **vrcholovým pokrytím**, pokud  $C \cap e \neq \emptyset$  pro  $\forall e \in E$ .



- Zjistit minimální velikost vrcholové pokrytí je NP-těžká úloha.
- **Párováním** v  $G$  je podgraf tvořený disjunktními hranami.

**Věta 7.1 (Königova-Egerváryho věta):**

- V bipartitním grafu je velikost min. vrcholového pokrytí rovna velikosti maximálního párování (do počtu hran).

**Hallova věta**

- Mějme konečné množiny  $X$  a  $I$ .
- **Množinový systém**  $\mathcal{M}$  je  $(M_i : i \in I)$ , kde  $M_i \subseteq X$ .
- **Systém různých reprezentantů (SRR)** pro  $\mathcal{M}$  je prosté zobrazení  $f : I \rightarrow X$  takové, že  $\forall i \in I : f(i) \in M_i$ .
  - tedy  $f$  je výběr jednoho prvku z každé  $M_i$  takový, že žádný prvek nevybereme víckrát
- **Incidenční graf** systému  $\mathcal{M}$  je bipartitní graf  $G_{\mathcal{M}} = (I \cup X, E)$ , kde  $E = \{\{i, x\} : i \in I, x \in X, x \in M_i\}$
- Pokud  $\mathcal{M}$  má SSR  $\Leftrightarrow S_{\mathcal{M}}$  obsahuje párování velikosti  $|I|$ .

**Věta 7.2 (Hallova věta):**

- $\mathcal{M}$  má SSR  $\Leftrightarrow \forall J \subseteq I : |\cup_{j \in J} M_j| \geq |J|$
- pravé části se říká **Hallova podmínka**
- také se věta označuje jako **Hall's marriage theorem**
- s axiomem výběru by šlo dokázat variantu s konečnými  $M_i$  a nekonečnými  $I, X$ 
  - s nekonečnými  $I, X$  to platit nemusí

**Rozšiřování latinských obdélníků**

**Důsledek 7.3:**

- V každém bipartitním grafu  $G = (A \cup B, E)$  s  $E \neq \emptyset$  a  $\deg_G(x) \geq \deg_G(y)$  pro každé  $x \in A, y \in B$  existuje párování velikosti  $|A|$ .

**Latinský obdélník**

- typu  $k \times n$  pro  $k \leq n$  je tabulka s řádky s  $n$  sloupci vyplněnými symboly  $1, \dots, n$  tak, že se v žádném řádku ani sloupci žádný symbol neopakuje.

**Věta 7.4:**

- Každý latinský obdélník typu  $k \times n$  lze doplnit na latinský čtverec řádu  $n$ .

*Přednáška 8*

## Míra souvislosti grafu

- graf je **souvislý** pokud jsou každé dva vrcholy spojené cestou, jinak je graf **nesouvislý** a je rozložen na aspoň dvě **komponenty souvislosti**
- budeme zkoumat jak moc je graf odolný proti rozpadnutí po odebrání hrany nebo vrcholu
- **Hranovým řezem** v grafu  $G = (V, E)$  je množina hran  $F \subseteq E$  taková, že graf  $G - F = (V, E \setminus F)$  je nesouvislý. (Také se někdy nazývá jako **separátor**.)
- **Vrcholovým řezem** v grafu  $G = (V, E)$  je množina vrcholů  $A \subseteq V$  taková, že graf  $G - A = (V \setminus A, E \cap \binom{V \setminus A}{2})$  je nesouvislý.
- **Hranová souvislost** grafu  $G = (V, E)$  je

$$k_e(G) = \begin{cases} \min\{|F| : F \text{ je hranový řez v } G\} \\ k_e(G) = 1 \text{ pokud } G \equiv K_1 \end{cases}$$

- **Vrcholová souvislost** grafu  $G = (V, E)$  je

$$k_v(G) = \begin{cases} \min\{|A| : A \text{ je vrcholový řez v } G\} \\ k_v(G) = 1 \text{ pokud } G \equiv K_1 \\ k_v(G) = n - 1 \text{ pokud } G \equiv K_n, n \geq 2 \end{cases}$$

- *nesouvislé grafy mají vrch. i hran. souvislost 0*
- pro  $r \in \mathbb{N}_0$  je graf **hranově  $r$ -souvislý**, pokud  $k_e(G) \geq r$
- pro  $r \in \mathbb{N}_0$  je graf **vrcholově  $r$ -souvislý**, pokud  $k_v(G) \geq r$
- $\forall G = (V, E), G \neq K_1 : k_e(G), k_v(G) \leq \min\{\deg_G(v), v \in V\}$

### Lemma 8.1:

- $\forall G = (V, E) \forall e \in E : k_e(G) - 1 \leq k_e(G - e) \leq k_e(G)$
- Po odebrání hrany klesne hranová souvislost maximálně o 1.

### Lemma 8.2:

- $\forall G = (V, E) \forall e \in E : k_v(G) - 1 \leq k_v(G - e) \leq k_v(G)$
- Po odebrání hrany klesne vrcholová souvislost maximálně o 1.

### Důsledek 8.3:

- $\forall G = (V, E) : k_v(G) \leq k_e(G)$
- vrcholová souvislost je maximálně stejná jako hranová souvislost
- nerovnost může být ostrá (“motýlek”)

### Věta 8.4 (Ford-Fulkersonova věta):

- $\forall G \forall t \in \mathbb{N} : k_e \geq t \Leftrightarrow$  mezi každými 2 vrcholy grafu  $G$   $\exists \geq t$  hranově disjunktních cest
- varianat Fordovy-Fulkersonovy věty platí i pro vrcholovou souvislost

**Věta 8.5 (Menseroova věta):**

- $\forall G \forall t \in \mathbb{N} : k_e(G) \geq t \Leftrightarrow$  mezi každými 2 vrcholy grafu  $G$   $\exists \geq t$  vrcholově disjunktních cest (mimo  $u, v$ )
- jelikož lze zjistit tok maximální velikosti v polynomiálním čase, tak máme algoritmus na zjištění  $k_e(G), k_v(G)$  také v polynomiálním čase

*Přednáška 9***2-souvislost podrobněji**

- hranový řez velikosti 1 se nazývá **most**
- vrcholový řez velikosti 1 se nazývá **artikulace**
- pro graf  $G = (V, E)$  s  $e \in E$  označme  $G \div e$  graf vzniklý z  $G$  operací **podrozdělení hrany  $e$**  na cestu délky 2

**Lemma 9.1:**

- Pro každý graf  $G = (V, E)$  a pro každou hranu  $e \in E$  platí:
- $G$  je vrcholově 2-souvislý  $\Leftrightarrow G \div e$  je vrcholově 2-souvislý

**Věta 9.2 (Ušaté lemma):**

- graf  $G$  je vrcholově 2-souvislý  $\Leftrightarrow G$  lze vytvořit z  $K_3$  operacemi přidávání a podrozdělování hran
- Proč “Ušaté lemma”?
  - Přidání hrany a její podrozdělení odpovídám přidání cesty mezi 2 vrcholy (=“přípení ucha”).

**Alternativní znění věty 9.2:**

- $G$  je vrcholově 2-souvislý  $\Leftrightarrow G$  lze vytvořit z cyklu přidáváním uší
- protože přidávání ucha lze simulovat přidáním hrany a jejím podrozdělením

**Počítání dvěma způsoby**

- Metoda důkazů v kombinatorice.
- Určíme nějaký neznámý počet  $X$  vyjádřením nějakého počtu  $Z$  dvěma výrazy, z nichž jeden  $X$  obsahuje a druhý ne  $\Rightarrow$  máme vyjádření pro  $X$

**Cayleyho vzorec**

- Kolika způsoby lze vytvořit strom na vrcholech  $\{1, \dots, n\}$ ?
- Nebo-li jaká je počet koster  $\kappa(n)$  grafu  $K_n$ ?
  - Kostra grafu  $G = (V, E)$  je strom  $T = (V, E')$  s  $E' \subseteq E$

**Věta 9.3 (Cayleyho vzorec):**

- Pro každé  $n \geq 1$  platí  $\kappa(n) = n^{n-2}$ .
- Existuje řada důkazů s velmi odlišnými myšlenkami, ukážeme si nej-jednodušší založený na počítání dvěma způsoby.

**Věta 9.4:**

- Graf  $K_n - e$  má  $(n-2)n^{n-3}$  koster pro  $n \geq 2$ .
- Počet koster  $\kappa(G)$  grafu  $G = (\{1, \dots, n\}, E)$  lze určit pomocí determinantu.
- Uvažme **Laplacián**  $L(G)$  grafu  $G$ , tedy matici  $L(G) = (L_{ij})_{i,j=1}^\infty$ , kde

$$L_{ij} = \begin{cases} \deg_G(i) & \text{pokud } i = j \\ -1 & \text{pokud } (i, j) \in E \\ 0 & \text{jinak} \end{cases}$$

**Věta 9.5 (Kirchhoffova věta):**

- $\forall G : \kappa(G) = \det(L(G)^{1,1})$ , kde  $(L(G)^{1,1})$  je Laplacián  $L(G)$  bez 1. řádků a 1. sloupce.

*Přednáška 10*

---

**Spernerova věta**

- systém  $\mathcal{M} \subseteq 2^{\{1, \dots, n\}}$  podmnožin  $n$ -prvkové množiny  $\{1, \dots, n\}$  je **nezávislý**, pokud platí:  $\forall A, B \in \mathcal{M}, A \neq B : A \not\subseteq B \wedge A \not\supseteq B$

**Věta 10.1 (Spernerova věta):**

- Každý nezávislý systém v  $2^{\{1, \dots, n\}}$  obsahuje  $\leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$  množin a tento odhad je těsný.
- Ekvivalentně: Nejdelší antiřetězec v  $(2^{\{1, \dots, n\}}, \subseteq)$  má právě  $\binom{n}{\lfloor \frac{n}{2} \rfloor}$  prvků.

**Úvod do Ramseyovy teorie**

- “Každý velký systém obsahuje homogenní podsystem” dané velikosti.
- **obarvení** množiny  $X$   $r$  barvami (zkráceně  $r$ -obarvení) je libovolné zobrazování přiřazující každému prvku  $x \in X$  jednu z  $r$  barev

**Věta 10.2 (Dirichletův princip, Pigeonhole principle):**

- $\forall r, n_1, \dots, n_r \in \mathbb{N}$ : obarvíme-li prvky množiny  $X$   $r$  barvami, pak je-li  $|X| \geq 1 + \sum_{i=1}^r (n_i - 1)$ ,  $X$  obsahuje  $n_i$  prvků  $i$ -té barvy
- Co kdybychom chtěli obarvit dvojice?

- Pro  $k, l \in \mathbb{N}$  buď  $R(k, l)$  nejmenší  $N \in \mathbb{N}$  takové, že každé 2-obarvení (*BÚNO: červené a modré obarvení*)  $E(K_N)$  obsahuje červené  $K_k$  nebo modré  $K_l$  jako podgraf.

**Věta 10.3 (Ramseyova věta pro 2 barvy):**

- $\forall k, l \in \mathbb{N} : R(k, l)$  je konečné. Dokonce  $R(k, l) \leq \binom{k+l-2}{k-1} = \binom{k+l-2}{l-1}$
- určit Ramseyovská čísla  $R(k, l)$  přesně je velice obtížné (už pro malé případy)
- známá čísla  $R(3, 3) = 6$ ,  $R(4, 4) = 18$

**Věta 10.4:**

- $\forall k \geq 3 : R(k, k) > 2^{k/2}$

*Přednáška 11*

- 
- rozšíření Ramseyovy věty na více barev a také na barvení  $p$ -tic vrcholů
  - pro čísla  $p, r, n_1, \dots, n_r \in \mathbb{N}$  ( $p$  - velikost barevných množin,  $r$  - počet barev,  $n_i$  - velikost 1-barevných podstruktur, které chceme najít) definujeme **Ramseyovo číslo**  $R_p(n_1, \dots, n_r)$  jako nejmenší  $N \in \mathbb{N}$  takové, že pro každou množinu  $X$  s  $|X| \geq N$  a každé  $r$ -obarvení množiny  $\binom{X}{p}$  existuje  $i \in \{1, \dots, r\}$  a  $Y \subseteq X$  takové, že  $|Y_i| = n_i$  a všechny  $p$ -tice z  $\binom{Y}{p}$  mají  $i$ -tou barvu

**Věta 11.1 (Ramseyova věta pro  $p$ -tice):**

- Pro každé  $p, r, n_1, \dots, n_r$  je  $R_p(n_1, \dots, n_r)$  konečné.

**Aplikace - Erdősova-Szekeresova věta:**

- $P$  = konečná množina bodů v rovině  $\mathbb{R}^2$ 
  - $P$  je v **obecné poloze**, pokud neobsahuje 3 body na přímce
  - $P$  je v **konvexní poloze**, pokud tvoří množinu vrcholů konvexního mnohoúhelníku

**Lemma 11.2:**

- Každá množina 5 bodů v  $\mathbb{R}^2$  v obecné poloze obsahuje 4 body v konvexní poloze.

**Věta 11.3 (Erdősova-Szekeresova věta):**

- Pro každé  $r \in \mathbb{N}$  existuje nejmenší  $ES(r) \in \mathbb{N}$  takové, že každá konečná množina s  $\geq ES(r)$  body v  $\mathbb{R}^2$  b obecné poloze obsahuje  $r$  bodů v konvexní poloze.

- Erdős-ova-Szekeresova domněnka je že  $\forall r \geq 2 : ES(r) = 2^{r-2} + 1$ .
- Zatím se zná, že to je dolní odhad a horní jako  $\leq 2^{r+o(r)}$ .

**Věta 11.4 (Nekonečná verze Ramseyovy věty):**

- Pro každé  $p, r \in \mathbb{N}$  a pro každé  $r$ -obarvení množiny  $\binom{\mathbb{N}}{p}$  existuje nekonečná  $A \subseteq \mathbb{N}$  taková, že všechny její  $p$ -tice mají v daném  $r$ -obarvení stejnou barvu.
- Nekonečná verze implikuje konečnou. Dá se dokázat sporem, my si ji ukážeme pro  $n_1 = \dots = n_n = n$ .

**Lemma 11.5 (Königovo lemma):**

- V každém zakořeněném stromě, který má nekonečně mnoho vrcholů ale jen konečné stupně existuje nekonečná cesta začínající v kořeni.

*Přednáška 12*

---

## Samoopravné kódy

- **abeceda**  $\Sigma$  = konečná množina symbolů
- **slovo** délky  $n$  = posloupnost  $n$  symbolů
- $\Sigma^n$  = množina všech slov délky  $n$
- **Hammingova vzdálenost**
  - $x, y \in \Sigma^n : d(x, y) = |\{i \in \{1, \dots, n\} : x_i \neq y_i\}|$
  - počet pozic, kde se  $x$  a  $y$  liší
  - $d$  je metrika
- $(\Sigma^n, d)$  je metrický prostor
- **(blokový) kód** je  $C \subseteq \Sigma^n$ 
  - prvky  $C$  jsou **kódová slova**
- pomocí  $C$  umíme opravit  $\leq t$  chyb, pokud  $\forall y \in \Sigma^n \exists$  nanejvýš 1 slovo  $x \in C$  t.ž.  $d(x, y) \leq t$
- parametry kódu
  1. délka =  $n$
  2. velikost abecedy  $q = |\Sigma|$
  3. dimenze  $k = \log_q |C|$
  4. vzdálenost  $d = \min_{x, x' \in C, x \neq x'} d(x, x')$
- kód s parametry  $n, k, d, q$  značíme  $(n, k, d)_q$
- v kódu s parametry  $(n, k, d)_q$  dokážeme opravit  $\leq \lfloor \frac{d-1}{2} \rfloor$  chyb
  - množiny slov ve vzdálenosti  $\leq \lfloor \frac{d-1}{2} \rfloor$  od kódových slov jsou navzájem disjunktní
  - pokud  $d \leq n$ , tak dokážeme opravit  $\leq \lfloor \frac{n-1}{2} \rfloor$

### Příklady kódů:

1. opakovací kód
  - každý symbol  $n$ -krát zopakujeme
  - parametry:  $(n, 1, n)_q$
2. charakteristický vektory KPR
  - kódová slova  $P - \{0, 1\}$  - vektor, kde na pozici  $x$  je  $1 \leftrightarrow x \in P$
  - $(X, \mathcal{P})$  - KPR řádu  $n$
  - parametry:  $(n^2 + n + 1, \log_2(n^2 + n + 1), 2n)_2$
  - $|X| = n^2 + n + 1$  a  $|C| = |\mathbb{P}| = n^2 + n + 1$
  - $d = 2n$ 
    - 2 kódové slova sdílí jednu jedničku, na zbytku se liší na  $2n$  pozicích
3. hadamardovy kódy
  - hadamardova matice řádu  $n$  je  $H \in \{-1, 1\}$ , kde  $H \cdot H^T = n \cdot I_n$
  - každý 2 různé řádky se liší na  $n/2$  pozicích
  - zvolme  $C = \{\text{řádky } H\} \cup \{-\text{řádky } H\}$
  - parametry:  $(n, 1 + \log_2(n), \frac{n}{2})_2$

$$H_1 = 1$$

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Sylvestrova konstrukce hadamardovy matice:

$$H_{n+1} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$$

*Hadamardova domněnka:* pro  $\forall k \in \mathbb{N} \exists$  hadamardova matice řádu  $4k$

- kódy  $C, C'$  jsou ekvivalentní, pokud se liší jen pořadím pozic
  - $\exists \Pi \in S_n : X = (x_1, \dots, x_n) \in C \leftrightarrow \Pi(X) = (X_{\Pi(1)}, \dots, X_{\Pi(n)}) \in C$
- pro jaké parametry existuje kód?
  - kombinatorická koule je středem  $X \in \Sigma^n$  a poloměrem  $t$  je  $B(X, t) = \{y \in \Sigma^n : d(x, y) \leq t\}$

### Lemma 12.1:

Je-li  $C$  kód se vzdáleností  $2t + 1$ , pak  $\forall X, X' \in C : B(X, t) \cap B(X', t) = \emptyset$

### Věta 12.2 (Hammingův odhad):

$\forall$  kód  $C$  s parametry  $(n, k, d)_q$  platí, že  $|C| \leq \frac{q^n}{V(t)}$

**perfektní kód** = kód s parametry  $(n, k, 2t + 1)_q$  a s  $|C| = \frac{q^n}{V(t)}$  - opakovací kód s  $q = 2$  a lichou delkou

### Věta 12.3 (Gilbertův - Varshalův odhad):

$\forall n, q, d \in \mathbb{N} : \exists$  kód  $C$  s parametry  $(n, k, d)_q$ , kde  $|C| \geq \frac{q^n}{V(d-1)}$

**lineární kódy** - jako abecedu použít konečné těleso  $\mathbb{K} = \Sigma^n$  - podprostor vektorového prostoru  $\mathbb{K}^n$  - s parametry  $n, k, d, q$  značíme  $[n, k, d]_q$

### Příklady:

1. opakovací kódy nad  $\mathbb{Z}_p$
2. char. vektory KPR
  - nejsou lineární
3. hadamardovy kódy
  - obecně ne, ze Sylvestrový konstrukce ano

*Přednáška 13*

---

## Lineární kódy

- Víme, že každé těleso  $\mathbb{K}$  odpovídá tělesu  $\mathbb{F}_q$
- $\forall x, y, z \in \mathbb{K}^n : d(x, y) = d(x + z, y + z) = d(x - y, 0)$
- $\Rightarrow$  minimální vzdálenost  $d$  se rovná  $\min_{x, y \in C, x \neq y} \{d(x - y, 0)\} = \min_{x \in C, x \neq 0} \{d(x, 0)\}$ 
  - $\Rightarrow$  ke zjištění  $d$  není třeba zkoumat všechny dvojice, stačí počítat nenulové složky kódových slov
- Výhodou lineárních kódů je úsporný popis, namísto všech  $q^r$  prvků kódu stačí uvést  $r$  prvků nějaké jeho báze
- **Generující matice** kódu  $C$  = matice  $M \in \Sigma^{r \times n}$  jejíž řádky tvoří bázi kódu  $C$
- V prostoru  $\mathbb{F}_q^n$  definujeme **skalární součin**  $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$  pro  $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbb{F}_q^n$ .
  - Nejedná se o klasický skalární součin podle klasické definice, protože neplatí  $\langle x, x \rangle = 0 \Leftrightarrow x = 0$  (třeba  $x = (1, 1, 0, 0)$  nad  $\mathbb{F}_2^4$ ).
- **Duálním kódem** k lineárnímu kódu  $C$  je jeho ortogonální doplněk

$$C^\perp = \{x \in \mathbb{F}_q^n : \langle x, y \rangle = 0 \text{ pro každé } y \in C\}$$

- Z povahy našeho skalárního součinu nemusí platit  $C \cap C^\perp = \{0\}$ .
  - Platí  $\dim(C^\perp) + \dim(C) = n$  a  $(C^\perp)^\perp = C$
- Generující matice  $M^\perp$  kódu  $C^\perp$  se nazývá **kontrolní matice**.
  - Řádky kontrolní matice určují lineární rovnice, které musí každé slovo z  $C$  splňovat (a naopak každý vektor z  $\mathbb{F}_q^n$ , který je splňuje, je kódovým slovem v  $C$ ).
  - Nebo-li  $C = \{x \in \mathbb{F}_q^n : M^\perp x = 0\}$ .
- Mějme lineární kód  $C$  s parametry  $[n, r, d]_q$ .



### Kódování lineární kódy:

- Ze vstupního slova  $z \in \mathbb{F}_q^n$  chceme vytvořit kódové slovo  $x \in C \subseteq \mathbb{F}_q^n$ .
- Necht  $M \in \mathbb{F}_q^{r \times n}$  je generující matice kódu  $C$ .
- Pro každý lineární kód existuje ekvivalentní kód, jehož generující matice má tvar:

$$(I_r \quad B)$$

- Kde výška je  $r$  a šířka  $n$ . Říká se jí **standardní forma**.
  - Stačí generující matici upravit Gaussovou eliminací a popřípadě zpermutovat sloupce.
- $\Rightarrow$  BÚNO: Matice  $M$  je ve standardní formě.
- Jako kódové slovo zvolíme  $x = M^\top z \in C$ 
  - $\Rightarrow x$  má na prvních  $r$  souřadnicích slovo  $z$  (**informační symboly**) a na zbylých  $n - r$  souřadnicích obsahuje **kontrolní symboly**

$$\begin{pmatrix} I_r \\ B^\top \end{pmatrix} \begin{pmatrix} z \\ \cdot \end{pmatrix}$$

### Dekódování lineárních kódů:

- po odeslání  $x \in C$  bylo přijato  $y \in \mathbb{F}_q^n$
- příjemce zná pouze  $y$  a chce najít kódové slovo, které je mu nejbližší
- necht  $M^\perp$  je kontrolní matice kódu  $C$ , pokud je matice  $M$  ve standardní formě pak

$$M^\perp = (-B^\top \quad I_{n-r})$$

- kde šířka je  $r$  a výška  $n - r$ , protože pak  $M^\perp M^\top = -B^\top I_r + I_{n-r} B^\top = 0$
- jako **syndrom slova**  $y \in \mathbb{F}_q^n$  nazveme součin  $M^\perp y$
- protože  $C = \{x \in \mathbb{F}_q^n : M^\perp x = 0\}$ , tak máme určené lineární zobrazení  $S : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^{n-r}$  splňující  $C = \text{Ker}(S)$
- zobrazení  $S$  nazveme **syndrom**
  - zobrazení  $S$  je na, protože platí  $\dim(\text{Ker}(S)) + \dim(\text{Im}(S)) = \dim(\mathbb{F}_q^n)$ , kde  $\text{Im}(S)$  je obraz  $S$

### Lemma 13.1:

- Zobrazení  $S$  je prosté na  $B(0, t)$  kde  $t = \lfloor \frac{d-1}{2} \rfloor$ .
- podle lemma 13.1. tedy k  $S \upharpoonright B(0, t)$  existuje inverzní zobrazení
- $S^{-1} : S(B(0, t)) \rightarrow B(0, t)$ 
  - $S^{-1}$  není lineární, ale jde popsat tabulkou s  $q^{n-k}$  prvky z  $B(0, t)$  a v této tabulce je pro každý syndrom slova uloženo nějaké slovo s minimální vahou a s daným syndromem

### Co víme:

1. Pro  $y \in B(x, t)$  máme  $S(y - x) = S(y) - S(x) = S(y)$  (díky linearitě a toho že  $x \in \text{Ker}(S)$ ).
  - neboli  $y$  a vzniklá chyba  $y - x$  mají stejný syndrom
2. Pro  $y \in B(x, t)$  máme  $y - x \in B(0, t)$  a tedy  $y - x = S^{-1}(S(y - x))$ .
  - neboli vzniklou chybu jde vyjádřit pomocí  $S$
3.  $x = y - (y - x) = y - S^{-1}(S(y - x)) = y - S^{-1}(S(y))$ 
  - nezávislý na  $x$
  - pro dané  $y$  pomocí syndromu  $S(y)$  dokážeme určit kódové slovo  $x$ , ze kterého vzniklo, nastalo-li  $\leq t$  chyb

### Jak dekódovat

- Pro přijaté slovo  $y \in \mathbb{F}_q^n$  spočítat  $x = y - S^{-1}(M^\perp y)$ , kde  $M^\perp$  je kontrolní matice a zobrazení  $S^{-1}$  máme připravené jako tabulku.
- Nastane-li  $\leq t$  chyb, je  $x$  kódové slovo, ze kterého  $y$  vzniklo.

### Tvrzení 13.2:

- Vzdálenost  $d$  kódu  $C$  = minimální počet lineárně závislých sloupců kontrolní matice  $M^\perp$ .

### Hammingovy kódy

- Příklad lineárních kódů, které jsou dokonce perfektní.
- Jejich nevýhodou je, že nedokáží opravit příliš mnoho chyb
- Například nad tělesem  $\mathbb{F}_2$ .
- Mějme parametr  $r = 3$
- Generující matice:

$$M = \begin{pmatrix} & - & l_1 & - \\ I_{2^r-r-1} & - & l_2 & - \\ & - & l_3 & - \end{pmatrix}$$

- Kde  $l_i$  jsou všechny nenulové vektory z  $\mathbb{F}_2^r$  různé od vektorů kanonické báze.
- Kontrolní matice:

$$M^\perp = \begin{pmatrix} | & | & | & \\ l_1 & l_2 & l_3 & I_r \\ | & | & | & \end{pmatrix}$$

- Parametry matic jsou  $r$  a  $2^r - r - 1$ .
- Dva vektory z  $\mathbb{F}_2^r \setminus \{0\}$  jsou lineárně závislé  $\Leftrightarrow$  jsou totožné  $\Rightarrow$  minimální počet lineárně závislých sloupců v  $M^\perp$  je 3 a podle tvrzení 13.2. je vzdálenost kódu 3.
- $\Rightarrow$  jedná se o kód s parametry  $[2^r, 2^r - r - 1, 3]_2$ , takže opraví  $\leq 1$  chybu

### Příklad

- pro  $r = 3$  dostaneme kód s parametry  $[7, 4, 3]_2$
- jedná se o kód sestavený z Fanovy roviny přidáním počátku a doplňků

### Hammingovy kódy jsou perfektní:

- stačí ukázat, že Hammingův odhad  $|C| \leq \frac{q^n}{V(t)}$  je těsný
- $t = \lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{3-1}{2} \rfloor = 1$
- $V(t) = V(1) = \sum_{i=0}^t (q-1)^i = (q-1) + 1 = 2^r - 1 + 1 = 2^r$
- $\frac{q^n}{V(1)} = \frac{2^{3r}}{2^r} = 2^{2r} = 2^{2^r - r - 1}$
- $|C| = 2^r = 2^{2^r - r - 1}$  takže Hammingův je skutečně pro Hammingovy kódy těsný

### Lepší reprezentace funkce $S^{-1}$

- tabulka reprezentující  $S^{-1}$  má pouze  $2^{n-r} = 2^{2^r - 1 - (2^r - r - 1)} = 2^r = n + 1$  prvků
- ve skutečnosti tabulku vůbec nepotřebujeme
- zpermutujeme-li sloupce a řádky  $M^\perp$  pak, aby  $i$ -tý sloupec byl binárním zápisem čísla  $i$ , pak  $S(y)$  určuje pozici na níž nastala chyba
- $\Rightarrow$  lze dékodovat tak, že pokud  $S(y) = 0$ , pak  $x = y$ , jinak je  $S(y)$  binárním zápisem čísla  $i$  a pak  $x$  = slovo vzniklé z  $y$  výměnou bitu, který je v  $y$  na pozici  $i$