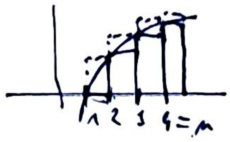
• Odhady kombinatorických funkcí



• $e\left(\frac{n}{e}\right)^n \le n! \le en\left(\frac{n}{e}\right)^n$

Dk: $\ln(n!) = \sum_{i=1}^{n} \ln(i) \Rightarrow \int_1^n \ln(x)\,dx < \ln(n!) < \int_1^{n+1} \ln(x)\,dx \ \ldots \ \blacksquare$

• $\left(\frac{n}{e}\right)^n \le n!$

n-tý člen

Dk: $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} \overset{x=n}{\Rightarrow} e^n \ge \frac{n^n}{n!} \Rightarrow n! \ge \left(\frac{n}{e}\right)^n \ \blacksquare$

• $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$

Dk: 1) $a_n := \lim_{n\to\infty} \frac{n!}{\sqrt{n}\, n^n e^{-n}}$ konverguje k $A \in \mathbb{R}^+$

$b_n := \ln(a_n)$ $\quad \nearrow \quad \frac{a_n}{a_{n+1}} = \frac{n!}{n^{n+\frac{1}{2}} e^{-n}} \cdot \frac{(n+1)^{n+\frac{1}{2}} e^{-n-1}}{(n+1)\,n!} = \frac{1}{e}\left(\frac{n+1}{n}\right)^{\frac{2n+1}{2}}$

$\Rightarrow b_n - b_{n+1} = \ln\left(\frac{a_n}{a_{n+1}}\right) = \frac{2n+1}{2} \ln\left(\frac{n+1}{n}\right) - 1$

$\rightarrow$ chci $\frac{n+1}{n} = \frac{1+k}{1-k} \Rightarrow k = \frac{1}{2n+1}, \quad 0 < k < 1$

□ $b_n - b_{n+1} = \frac{1}{2k} \ln\left(\frac{1+k}{1-k}\right) - 1$

👁: $\ln\left(\frac{1+k}{1-k}\right) = \ln(1+k) - \ln(1-k) \overset{*}{=} \left(k - \frac{k^2}{2} + \frac{k^3}{3} - \ldots\right) - \left(-k - \frac{k^2}{2} - \frac{k^3}{3} - \ldots\right)$

$\overset{*}{=} 2\left(k + \frac{k}{3} + \ldots\right) = 2\sum_{i=0}^{\infty} \frac{k^{2i+1}}{2i+1}$

□ $b_n - b_{n+1} = \frac{1}{2k} \cdot 2\sum_{i=0}^{\infty} \frac{k^{2i+1}}{2i+1} - 1 = \sum_{i=0}^{\infty} \frac{k^{2i}}{2i+1} - 1 = \sum_{i=1}^{\infty} \frac{k^{2i}}{2i+1} > 0$

$\Rightarrow b_n > b_{n+1} \Rightarrow (b_n)$ je klesající $\Rightarrow (a_n)$ je klesající

□ $b_n - b_{n+1} = \sum_{i=1}^{\infty} \frac{k^{2i}}{2i+1} < \sum_{i=1}^{\infty} k^{2i} = k^2 + k^4 + k^6 + \ldots \overset{*}{=} k^2 \cdot \frac{1}{1-k^2} =$

$= \frac{\frac{1}{(2n+1)^2}}{1 - \frac{1}{(2n+1)^2}} = \frac{1}{(2n+1)^2 - 1} = \frac{1}{4n^2 + 4n} = \frac{1}{4n(n+1)} = \frac{1}{4n} - \frac{1}{4(n+1)}$

$\Rightarrow b_n - \frac{1}{4n} < b_{n+1} - \frac{1}{4(n+1)} \Rightarrow \left(b_n - \frac{1}{4n}\right)$ je rostoucí

$\Rightarrow b_n > b_n - \frac{1}{4n} > b_1 - \frac{1}{4} = \frac{3}{4} \Rightarrow a_n > e^{\frac{3}{4}} \Rightarrow (a_n)$ je omezená $\blacksquare$

2) $\frac{\pi}{2} = \frac{2}{1} \cdot \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdot \frac{6}{5} \cdot \frac{6}{7} \cdots = \lim_{n\to\infty} \frac{(2n)!!^2}{(2n-1)!!^2\,(2n+1)} = \lim_{n\to\infty} \frac{(2n)!!^2\,(2n)!!^2}{(2n-1)!!^2\,(2n)!!^2\,(2n+1)} =$

$= \lim_{n\to\infty} \frac{2^{4n} \cdot n!^4}{(2n)!^2 (2n+1)} \Rightarrow \sqrt{\frac{\pi}{2}} = \lim_{n\to\infty} \frac{4^n\, n!^2}{(2n)!\sqrt{2n+1}} \Rightarrow \sqrt{\pi} = \lim_{n\to\infty} \frac{4^n\, n!^2}{(2n)!\sqrt{n}}$

$\Rightarrow \sqrt{\pi} = \lim_{n\to\infty} \frac{4^n A^2 \cdot (\sqrt{n}\, n^n e^{-n})^2}{A\sqrt{2n}\,(2n)^{2n} e^{-2n} \sqrt{n}} = \frac{A}{\sqrt{2}} \Rightarrow A = \sqrt{2\pi}$

$\blacksquare$

- $\left(\frac{n}{k}\right)^k \le \binom{n}{k} \le \left(\frac{en}{k}\right)^k, \quad 1 \le k \le n$

Dk: ① $\binom{n}{k} = \frac{n}{k}\cdot\frac{n-1}{k-1}\cdot\frac{n-2}{k-2}\cdot\ldots\cdot\frac{n-k+1}{1} > \left(\frac{n}{k}\right)^k$

$\quad < \quad < \quad < \cdots <$

$\frac{n}{k} < \frac{n-1}{k-1} \quad \because \quad nk - n < nk - k$ ✓

② $\binom{n}{k} = \frac{n^{\underline{k}}}{k!}$, $\; n^{\underline{k}} < n^k$, $\; k! > \left(\frac{k}{e}\right)^k$, $\;\binom{n}{k} < \frac{n^k}{\left(\frac{k}{e}\right)^k} = \left(\frac{en}{k}\right)^k$ ■

- $\frac{2^{2n}}{2n+1} \le \binom{2n}{n} \le 2^{2n}$ → $2n$-tá řada p.Δ má součet 2^{2n}, # prvků $= 2n+1$

- $\frac{2^{2n}}{2\sqrt{n}} \le \binom{2n}{n} \le \frac{2^{2n}}{\sqrt{2n}}$

Dk: Definujeme $P := \binom{2n}{n}\cdot 2^{-2n}$ a ukážeme $\frac{1}{2\sqrt{n}} \le P \le \frac{1}{\sqrt{2n}}$

$$P = \frac{\binom{2n}{n}}{2^{2n}} = \frac{(2n)!}{2^n n! \cdot 2^n n!} = \frac{(2n)!!\,(2n-1)!!}{(2n)!!\cdot(2n)!!} = \frac{(2n-1)!!}{(2n)!!} = \frac{1\cdot3\cdot5\cdot\ldots\cdot(2n-1)}{2\cdot4\cdot6\cdot\ldots\cdot(2n)}$$

① $$P^2 = \underbrace{\frac{1\cdot3}{2\cdot2}}_{<1}\cdot\underbrace{\frac{3\cdot5}{4\cdot4}}_{<1}\cdots\underbrace{\frac{(2n-3)(2n-1)}{(2n-2)(2n-2)}}_{<1}\cdot\frac{2n-1}{2n\cdot2n} < \frac{2n-1}{2n\cdot2n} < \frac{1}{2n} \Rightarrow P < \frac{1}{\sqrt{2n}}$$

② $$P^2 = \frac{1}{2}\cdot\underbrace{\frac{3\cdot3}{2\cdot4}}_{>1}\cdot\underbrace{\frac{5\cdot5}{4\cdot6}}_{>1}\cdots\underbrace{\frac{(2n-1)(2n-1)}{(2n-2)\cdot2n}}_{>1}\cdot\frac{1}{2n} > \frac{1}{2}\cdot\frac{1}{2n} \Rightarrow P > \frac{1}{2\sqrt{n}}$$ ■

- $\binom{2n}{n} \sim \frac{2^{2n}}{\sqrt{\pi n}}$

Dk: Ukážeme $P \sim \frac{1}{\sqrt{\pi n}}$ pomocí Wallisova produktu.

$$\frac{\sin x}{x} = 1 + \frac{x^2}{3!} + \frac{x^4}{5!} + \frac{x^6}{7!} + \ldots = 0 \iff \sin(x) = 0 \iff x = k\pi,\ k\in\mathbb{Z},\ k\neq0$$

$$= \left(1-\frac{x}{\pi}\right)\left(1+\frac{x}{\pi}\right)\left(1-\frac{x}{2\pi}\right)\left(1+\frac{x}{2\pi}\right)\cdots = \left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{4\pi^2}\right)\left(1-\frac{x^2}{9\pi^2}\right)\cdots$$

$$= \prod_{n=1}^{\infty}\left(1-\frac{x^2}{n^2\pi^2}\right)$$

$x = \frac{\pi}{2}$: $$\frac{2}{\pi} = \prod_{n=1}^{\infty}\left(1-\frac{1}{4n^2}\right) = \prod_{n=1}^{\infty}\left(\frac{4n^2-1}{4n^2}\right) = \prod_{n=1}^{\infty}\frac{2n-1}{2n}\cdot\frac{2n+1}{2n} = \frac{1}{2}\cdot\frac{3}{2}\cdot\frac{3}{4}\cdot\frac{5}{4}\cdots$$

$$\Rightarrow \frac{2}{\pi} = \lim_{n\to\infty}\frac{(2n-1)!!^2\,(2n+1)}{(2n)!!^2} \quad\wedge\quad P = \frac{(2n-1)!!}{(2n)!!}$$

$$\Rightarrow \frac{2}{\pi} = \lim_{n\to\infty}P^2\cdot(2n+1) \Rightarrow \frac{\sqrt{2}}{\sqrt{\pi}} = \lim_{n\to\infty}P\sqrt{2n+1} \Rightarrow P \sim \frac{\sqrt{2}}{\sqrt{\pi}\sqrt{2n+1}} \sim \frac{1}{\sqrt{\pi n}}$$ ■

- Generující funkce

Def: Generující fce. posloupnosti $(a_n) \in \mathbb{R}$ je $f(x) := \sum_{n=0}^{\infty} a_n x^n$.

Pokud $\exists k > 0$ t.ž. $\forall n: |a_n| \leq k^n$, tak

$$|f(x)| = \sum_n |a_n| |x|^n \leq \sum_n k^n |x|^n \text{ což konverguje pro } |kx| < 1,$$

takže $f(x)$ konverguje absolutně a stejnoměrně pro $|x| < \frac{1}{k}$.

Navíc má na $(-\frac{1}{k}, \frac{1}{k})$ derivace všech řádů

Def: Mějme gen. fci. $f(x) := \sum_{n=0}^{\infty} a_n x^n$, potom definujeme $[x^n] f(x) := a_n$.

Pozorování: Generující fce odpovídají Taylorovým řadám v nule.

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots$$

$$\left.\begin{aligned} f(0) &= a_0 \\ f'(0) &= a_1 \\ f''(0) &= 2 \cdot 1 \cdot a_2 \\ f^{(n)}(0) &= n!\, a_n \end{aligned}\right\} \quad a_n = \frac{f^{(n)}(0)}{n!} \implies f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} x^n$$

$\implies f(x)$ jednoznačně určuje posloupnost (a_n)

Příklady:

$[x^n] \frac{1}{1-x} = 1$, ... $1 + x + x^2 + \dots = \frac{1}{1-x}$

$[x^n] \frac{1}{(1-x)^2} = n+1$, ... $1 + 2x + 3x^2 + \dots = \frac{1}{(1-x)^2}$ derivace

$[x^n] \frac{1}{(1-x)^r} = \binom{r+n-1}{n}$, ... $\frac{1}{(1-x)^r} = \sum_{n=0}^{\infty} \binom{-r}{n} (-x)^n$ ~ bin. věta

$[x^n] a(x) b(x) = \sum_{k=0}^{n} a_k b_{n-k}$, ... $a(x) b(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \dots$ konvoluce

$$= \sum_{n=0}^{\infty} x^n \sum_{k=0}^{n} a_k b_{n-k}$$

$$\int \frac{1}{1-x} dx = \int (1 + x + x^2 + \dots) dx$$

$$\implies \ln(1-x) = -1 - \frac{x^2}{2} - \frac{x^3}{3} - \frac{x^4}{4} - \dots$$

$$\int \frac{1}{1+x} dx = \int (1 - x + x^2 - x^3 + \dots) dx$$

$$\implies \ln(1+x) = 1 - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \dots$$

$$[x^n](1+x)^r = \binom{r}{n}$$

$$[x^n] \frac{x}{1-x-x^2} = F_n = \frac{1}{\sqrt{5}} (\varphi^n - \phi^n)$$

Důležité

$$[x^n] x^k f(x) = [x^{n-k}] f(x)$$

$$[x^n] \frac{1}{x^k} f(x) = [x^{n+k}] f(x)$$

$$[x^n] f(ax) = a^n \cdot [x^n] f(x)$$

$$[x^n] (f(x) + g(x)) = [x^n] f(x) + [x^n] g(x)$$

$$[x^n] (k + f(x)) = \begin{cases} k + f(0), & n = 0 \\ [x^n] f(x), & n \geq 1 \end{cases}$$

• Využití gen. funkcí

1) kombinatorické počítání

$a_n :=$ # způsobů jak zaplatit n kč pomocí 1kč, 2kč a 5kč

$$\Rightarrow \sum_{n=0}^{\infty} a_n x^n = (1+x+x^2+\dots)(1+x^2+x^4+\dots)(1+x^5+x^{10}+\dots)$$
$$= \frac{1}{1-x}\cdot\frac{1}{1-x^2}\cdot\frac{1}{1-x^5}$$

2) asymptotické odhady

$$e^x = 1+\frac{x}{1}+\frac{x^2}{2!}+\dots > \frac{x^n}{n!} \Rightarrow e^n > \frac{n^n}{n!} \Rightarrow n! > \left(\frac{n}{e}\right)^n$$

3) dokazování rovnosti posloupností

→ myšlenka: ukážeme že (a_n) a (b_n) mají stejné gen. fce $\Rightarrow a_n = b_n$

$a_n :=$ # způsobů jak zapsat n jako součet lichých čísel, $a_0 = 1$

$b_n :=$ # způsobů jak zapsat n jako součet jedniček a dvojek, $b_0 = 1$

$$a(x) = 1 + \underbrace{(x+x^3+\dots)}_{\text{1 číslo}} + \underbrace{(x+x^3+\dots)^2}_{\text{2 čísla}} + \underbrace{(x+x^3+\dots)^3}_{\text{3 čísla}} + \dots =$$
$$= 1+\frac{x}{1-x^2} + \left(\frac{x}{1-x^2}\right)^2 + \dots = \frac{1}{1-\frac{x}{1-x^2}} = \frac{1-x^2}{1-x-x^2}$$

$$b(x) = 1+(x+x^2)+(x+x^2)^2+(x+x^2)^3+\dots =$$
$$= \frac{1}{1-x-x^2}$$

→ dokaž $a_{n+1} = b_n$

$$\left.\begin{aligned} a(x) &= a_0 + a_1 x + a_2 x^2 + \dots \\ a'(x) &= a_1 + a_2 x + a_3 x^2 + \dots \end{aligned}\right\} \; a'(x) = \frac{a(x)-a_0}{x}$$

$$a'(x) = \left(\frac{1-x^2}{1-x-x^2} - \frac{1-x-x^2}{1-x-x^2}\right)\frac{1}{x} = \frac{1}{1-x-x^2} = b(x) \Rightarrow a'(x) = b(x)$$

$$\Rightarrow [x^n]\,a'(x) = a_{n+1} = [x^n]\,b(x) = b_n \qquad \blacksquare$$

4) řešení rekurencí

$$a_0 = 4,\ a_1 = 3,\ a_{n+2} = a_{n+1} + 2a_n + 3\cdot 2^n,\ n \geq 0. \to a_n = ?$$

$$\begin{aligned} f(x) &= 4 + 3x + (3 + 2\cdot 4 + 3\cdot 2^0)x^2 + \dots \\ x f(x) &= 4x + 3 x^2 + \dots \\ 2x^2 f(x) &= 2\cdot 4 x^2 + \dots \\ \frac{3x^2}{1-2x} &= 3\cdot 2^0 \, x^2 + 3\cdot 2^1 x^3 + \dots \end{aligned}$$

$$f(x) - x f(x) - 2x^2 f(x) - \frac{3x^2}{1-2x} = 4 - x$$

$$\Rightarrow f(x)(1-x-2x^2) = \frac{3x^2+4-x-8x+2x^2}{1-2x}$$

$$f(x) = \frac{5x^2-9x+4}{(1-2x)(1+x)(1-2x)} = \frac{2}{1+x} + \frac{\frac{3}{2}}{1-2x} + \frac{\frac{1}{2}}{(1-2x)^2}$$

$$a_n = [x^n]\,f(x) = 2\cdot(-1)^n + \frac{3}{2}\cdot 2^n + \frac{1}{2}\cdot(n+1)\cdot 2^n = \underline{\underline{2^{n-1}(n+4) + (-1)^n\cdot 2}}$$

- **Řešení rekurencí obecně**

→ máme nějaké zadání $a_n =$ „něco s a_0 až a_{n_0}" pro $n > n_0$, $a_0, \dots a_{n_0}$ dané

1. vynásob rovnici x^n
2. sečti to pro všechna n, pro která to platí – tedy $n \geq n_0 + 1$
3. vyjádři všechny sumy pomocí $f(x) = \sum_{n=0}^{\infty} a_n x^n$
4. dopočítej $f(x)$

$$a_n = a_{n-1} + a_{n-2}, \quad n \geq 2$$

1. $a_n x^n = a_{n-1} x^n + a_{n-2} x^n$
2. $\sum_{n=2}^{\infty} a_n x^n = \sum_{n=2}^{\infty} a_{n-1} x^n + \sum_{n=2}^{\infty} a_{n-2} x^n, \quad f(x) = \sum_{n=0}^{\infty} a_n x^n$
3. $f(x) - a_0 - a_1 x = (f(x) - a_0) x + f(x) \cdot x^2$
4. $f(x) - x f(x) - x^2 f(x) = a_0 + a_1 x + a_0 x \Rightarrow f(x) = \dfrac{a_0 + x(a_0 + a_1)}{1 - x - x^2}$

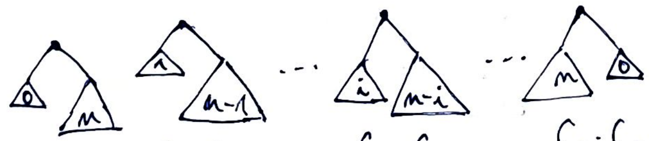
- **Catalanova čísla**

Def: Binární strom je zakořeněný strom, jehož každý vnitřní vrchol má 2 potomky; na pořadí potomků záleží.

Def: Definujeme Catalanova čísla jako $C_n :=$ # bin. stromů s n vnitřními vrcholy.
$= $ # bin. stromů s $n+1$ listy

Tvrzení: $C_n = \frac{1}{n+1}\binom{2n}{n}$

Př: $C_0 = 1$, $C_1 = 1$, $C_2 = 2$, $C_3 = 5$ 

C_{n+1}: 

$C_0 \cdot C_n \quad C_1 \cdot C_{n-1} \quad \cdots \quad C_i \cdot C_{n-i} \quad \cdots \quad C_n \cdot C_0$

$$C(x) := \sum_{n=0}^{\infty} C_n x^n$$

$$\Rightarrow C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k} = [x^n] C^2(x) \quad \leftarrow \text{konvoluce } C(x) \text{ s } C(x)$$

$$\begin{aligned} C(x) &= C_0 + C_1 x + C_2 x^2 + \dots \\ x C^2(x) &= C_0 C_0 x + (C_0 C_1 + C_1 C_0) x^2 \dots \end{aligned} \Bigg\} \; C(x) - x C^2(x) = C_0 \Rightarrow \underline{\underline{C(x) = 1 + x C^2(x)}}$$

$$x C^2(x) - C(x) + 1 = 0 \Rightarrow \frac{1 \pm \sqrt{1-4x}}{2x} \left< \begin{matrix} C^+(x) \\ C^-(x) \end{matrix} \right. \; ? \quad C(0) = C_0 = 1 \qquad \lim_{x \to 0} C^-(x) = 1$$

$$\lim_{x \to 0} C^+(x) \text{ neex}, \quad \Rightarrow C(x) = C^-(x)$$

$$\Rightarrow C_n = [x^n] \frac{1 - \sqrt{1-4x}}{2x} = \frac{1}{2} [x^{n+1}] (1 - \sqrt{1-4x}) = -\frac{1}{2} [x^{n+1}] \sqrt{1-4x} = -\frac{1}{2} (-4)^{n+1} [x^{n+1}] \sqrt{1+x} =$$

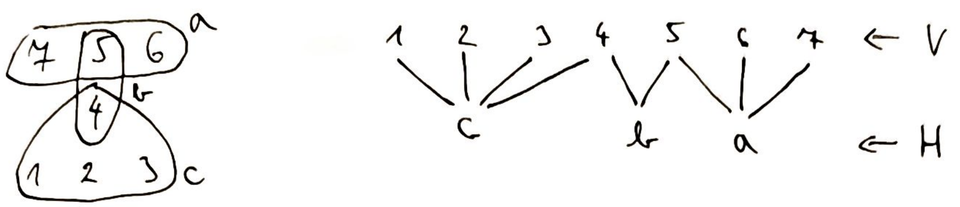
$$= (-1)^n \cdot 2^{2n+1} \binom{\frac{1}{2}}{n+1} = (-1)^n \cdot 2^{2n+1} \cdot \frac{\frac{1}{2} \cdot (-\frac{1}{2})(-\frac{3}{2}) \cdots (\frac{1}{2} - n)}{(n+1)!} =$$

$$= 2^n \cdot \frac{1 \cdot 1 \cdot 3 \cdot \ldots \cdot (2n-1)}{(n+1)!} = \frac{2^n \cdot (2n-1)!! \, n!}{n! \, (n+1)!} = \frac{(2n-1)!! \, (2n)!!}{n! \, (n+1)!} = \frac{(2n)!}{n! \, (n+1)!} = \underline{\underline{\frac{1}{n+1} \binom{2n}{n}}}$$

• Projektivní roviny

Def: Hypergraf je dvojice (V,H), kde H je množina hyperhran $H \subseteq P(V) = 2^V$. Hyperhrana je množina vrcholů.

Def: Graf incidence hypergrafu (V,H) je bipartitní graf s partitami V a H, kde mezi $x \in V$ a $h \in H$ vede hrana $\equiv x \in h$.



Def: Projektivní rovina je hypergraf $(X,\mathcal{P})$ t.ž.

A1) $\forall x,y \in X : \exists! p \in \mathcal{P} : x \in p \wedge y \in p$ … ∀ dvěma body prochází právě 1 přímka

A2) $\forall p,q \in \mathcal{P} : \exists! x \in X : x \in p \wedge x \in q$ … ∀ dvě přímky mají právě 1 průsečík

A3) $\exists Č \subseteq X, |Č| = 4 : \forall p \in \mathcal{P} : |p \cap Č| \leq 2$ … ∃ čtverec = 4 body v obecné poloze

Def: Konečná projektivní rovina KPR je projektivní r. $(X,\mathcal{P})$, kde X a $\mathcal{P}$ jsou konečné.

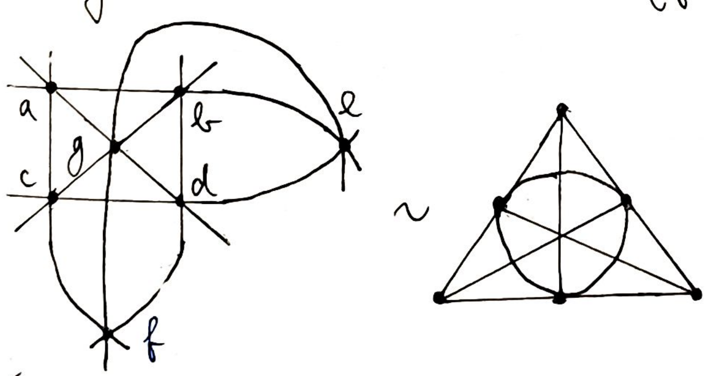
• Fannova rovina

→ myšlenka: pojďme zkonstruovat tu nejmenší možnou KPR

• body: a, b, c, d, e, f, g
• přímky: ab, ac, ad, bc, bd, cd, egf

} ∀ p.r. má alespoň 7 bodů a 7 přímek

↳ ∀ p.r. obsahuje Fannovu rovinu



• Značení: Pro KPR $(X,\mathcal{P})$, $x,y \in X$, $x \neq y$ značí $\overline{xy}$ přímku obsahující x a y.

→ ukáže se, že bodů je vždy stejně jako přímek
→ a že všechny přímky mají stejnou velikost

Tvrzení: V každé KPR $(X,\mathcal{P})$ mají všechny přímky stejný počet bodů (velikost).

Dk: Sporem... nechť v naší KPR $\exists$ přímky $p, q \dots |p| < |q|$.

Označme $x := p \cap q$ a body $p=\{y_1,\dots y_k\}$, $q=\{z_1,\dots z_l\}$, $k<l$.

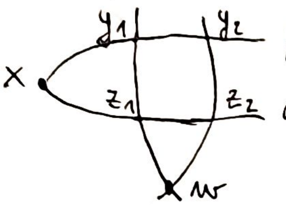
Lemma: $\exists$ bod $w \in X$ t.ž. $w \notin p \cup q$.

Dk: Podívejme se na čtverec Č.

→ Pokud $Č \setminus (p \cup q) \neq \emptyset$, volme $w \in Č \setminus (p\cup q)$.

→ jinak $Č \subseteq p \cup q$, takže $|Č \cap p| = |Č \cap q| = 2$. BÚNO $Č = \{y_1, y_2, z_1, z_2\}$

↳ potom $w := \overline{y_1 z_1} \cap \overline{y_2 z_2}$.



→ kdyby $w \in p$, tak $\{w, y_1\} \subseteq p \cap \overline{y_1 z_1}$ ↯

→ nemůže se stát $y_1 = w$?

↳ potom $y_1 \in \overline{y_2 z_2} \Rightarrow |Č \cap \overline{y_2 z_2}| = |\{y_1, y_2, z_2\}| = 3$ ↯ ■

⇒ Uvažme přímky $\overline{wz_1}, \overline{wz_2}, \dots \overline{wz_l}$. $\forall$ z nich protíná p a jsou různé.

⇒ $|p| < |q|$ ⇒ z principu holubníku $\exists v \in p$ co je obsažen v alespoň dvou z těchto přímek.

⇒ w a v mají alespoň 2 společné přímky ↯ ■

Def: KPR $(X,\mathcal{P})$ má řád $n \in \mathbb{N} \equiv \forall p \in \mathcal{P}: |p| = n+1$. → F.R. má řád 2

Lemma: V proj. rovině $(X,\mathcal{P})$ platí $\forall x \in X \ \exists p \in \mathcal{P}: x \notin p$.

Dk: Vezmu čtverec Č ⇒ $a, b, c \in Č \setminus \{x\}$.

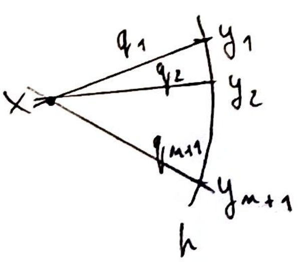
Alespoň 1 z přímek $\overline{ab}, \overline{ac}$ neobsahuje x. Jinak $\{a, x\} \subseteq \overline{ab} \cap \overline{ac}$ ↯. ■

Tvrzení: V každé KPR $(X,\mathcal{P})$ řádu n platí:

1) $\forall$ přímka má $n+1$ bodů
2) $\forall$ bod patří do $n+1$ přímek
3) $|X| = n^2+n+1$
4) $|\mathcal{P}| = n^2+n+1$

Dk:

2) Volme $x \in X$. Podle lemmatu $\exists p \in \mathcal{P}: x \notin p$ → $p = \{y_1, \dots y_{n+1}\}$



→ definujeme přímky $q_1, \dots q_{n+1}$: $q_i = \overline{xy_i}$

→ tvrdíme $i \neq j \Rightarrow q_i \neq q_j$; kdyby $q_i = q_j$, tak $\{y_i, y_j\} \subseteq q \cap p$ ↯

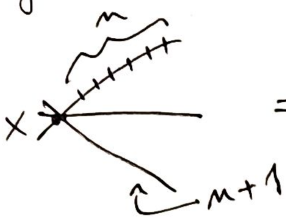
→ tvrdíme, že $\forall r \in \mathcal{P}: x \in r \Rightarrow r \in \{q_1, \dots q_{n+1}\}$

↳ $|r \cap p| = 1$, nechť y_i je jejich průnik, potom $r = \overline{xy_i} = q_i$

⇒ bodem x prochází právě $n+1$ přímek

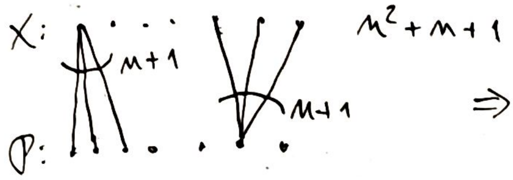
3) $x \in X$, nechť jím prochází $p_1, \dots p_{n+1}$.

$\forall y \in X \setminus \{x\}\ \exists!\, q \in \mathcal{P}: x, y \in q \Rightarrow q \in \{p_1, \dots p_{n+1}\}$ } $\forall$ bod z $X \setminus \{x\}$ patří do právě 1 z těchto přímek



$\Rightarrow |X| = 1 + (n+1) \cdot n = n^2 + n + 1$

4) Podívejme se na graf incidence $(X, \mathcal{P})$. $\to$ 2 partity < body, přímky

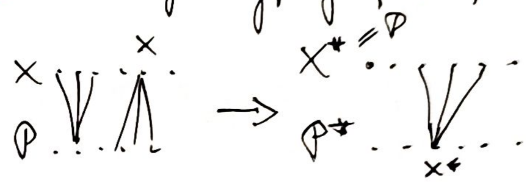


$\Rightarrow \#\text{hran} = (n^2+n+1)(n+1) = |\mathcal{P}|(n+1)$

$n^2+n+1 = |\mathcal{P}|$ ∎

Def: Mějme proj. rovinu $(X, \mathcal{P})$. Potom duální p.r. k $(X, \mathcal{P})$ je hypergraf $(X^*, \mathcal{P}^*)$, kde

1) $X^* := \mathcal{P}$
2) pro $x \in X$ definujeme $x^* := \{p \in \mathcal{P} \mid x \in p\}$
3) $\mathcal{P}^* := \{x^* \mid x \in X\}$



Tvrzení: $(X^*, \mathcal{P}^*)$ je projektivní rovina.

Dk: $(X^*, \mathcal{P}^*)$ splní A1 $\iff \forall p, q \in X^*\ \exists!\, x^* \in \mathcal{P}^*: \{p, q\} \subseteq x^*$

$\forall p, q \in \mathcal{P}\ \exists!\, x \in X: x \in p \ \&\ x \in q \iff (X, \mathcal{P})$ splní A2

$(X^*, \mathcal{P}^*)$ splní A2 $\iff \dots \iff (X, \mathcal{P})$ splní A1

$(X^*, \mathcal{P}^*)$ splní A3 $\iff \exists\, \check{C}^* \subseteq X^*, |\check{C}^*| = 4\ \&\ \forall x^* \in \mathcal{P}^*: |x^* \cap \check{C}^*| \le 2$

$\exists\, \check{C}^* \subseteq \mathcal{P}, |\check{C}^*| = 4\ \&\ \forall x \in X$: nejvýše 2 přímky z $\check{C}^*$ prochází x

↳ žádné 3 přímky z $\check{C}^*$ neprochází stejným bodem

Dk: Dle A3 $\exists\, \check{C} = \{a, b, c, d\} \subseteq X$ t.ž. žádné 3 body $\check{C}$ neleží na 1 přímce.

$\check{C}^* := \{\overline{ab}, \overline{bc}, \overline{cd}, \overline{ad}\}$ → volme BÚNO $\overline{ab}, \overline{bc}, \overline{cd}$

↳ $\overline{ab} \cap \overline{bc} = \{b\}$, $\overline{bc} \cap \overline{cd} = \{c\}$ $\Rightarrow \overline{ab} \cap \overline{bc} \cap \overline{cd} = \emptyset$ ∎

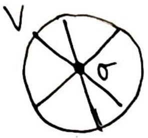
Duální p.r. nám dávají zadarmo duální vlastnosti a tvrzení.

- $(X, \mathcal{P})$: pro $\forall$ bod $\exists$ přímka, co ho neobsahuje
  $(X^*, \mathcal{P}^*)$: pro $\forall$ přímku $\exists$ bod, který na ní neleží

• **Konstrukce KPR řádu $n \in \mathbb{N}$**

1, Nechť T je konečné těleso s n prvky $\Rightarrow$ n je mocnina prvočísla
Uvažme vektorový prostor $V = T^3$ nad T, $\dim(V) = 3$, $|V| = n^3$.

2, Nechť X je množina podprostorů dimenze 1 ve V.
co vždy vezmu nějaký vektor a všechny jeho násobky $\Rightarrow$ $\forall$ ten podprostor má n prvků



$\#$ nenulových vektorů $= n^3 - 1 = |X|(n-1)$

$$\Rightarrow |X| = \frac{n^3-1}{n-1} = n^2+n+1$$

3, Pro $\forall$ podprostor $p \subseteq V$, $\dim(p) = 2$ definujeme $\tilde{p} := \{x \in X \mid x \subseteq p\}$

4, $\mathcal{P} := \{\tilde{p} \mid p \subseteq V, \dim(p) = 2\}$, $|\mathcal{P}| = n^2+n+1$ $\because$ $\forall$ podprostor dimenze 1 má ort. doplněk dimenze 2

5, Tvrdím $(X, \mathcal{P})$ je proj rovina.

Dk: A1: 2 pp. dim. 1 generují právě 1 p.p. dim. 2
A2: 2 pp. dim. 2 mají průnik pp. dim. 1.

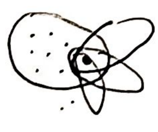
P, Q podprostory V: $\dim(P) + \dim(Q) - \dim(P \cap Q) = \dim(\mathrm{span}(P \cup Q))$
$$2 + 2 - \underset{?}{\geq 1} = 3$$

A3: $\exists$ 4 různé vektory, co generují pp. dim. 1 a každé 3 jsou lin. nezávislé.
↳ $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(1,1,1)$

• **Příklad:** Ve hře Dobble je 55 karet, přičemž na každé kartě je 8 symbolů a každé dvě karty mají právě jeden symbol společný.
→ kolik alespoň musí být ve hře symbolů? (v návodu se píše přes 50)

Řešení: Kdyby to byla proj. r., tak má řád 7,
takže symbolů by mělo být $49 + 7 + 1 = 57$.

$\exists$ symbol co je na 8 kartičkách, kdyby ne, tak



↩ 8 symbolů, každý z nich na ≤ 6 dalších kartičkách
$$\Rightarrow \#\text{kartiček} \leq 1 + 8 \cdot 6 = 49 < 55 \ \lightning$$

$$\Rightarrow \exists \text{ symbol na 8 kartičkách} \Rightarrow 1 + \underbrace{7}_{\text{další symboly}} \cdot \underbrace{8}_{\text{kartičky}} = 57 \text{ symbolů.}$$

• Toky v sítích

Def: Toková síť je (V, E, z, s, c), kde
- V je množina vrcholů
- E je množina orientovaných hran $E \subseteq V \times V$, povolujeme smyčky
- $z \in V$ je zdroj
- $s \in V$ je stok
- $c: E \to \mathbb{R}_0^+$ je kapacita

Def: Tok v síti (V, E, z, s, c) je funkce $f: E \to \mathbb{R}_0^+$ t.ž.
1) $\forall e \in E: \ 0 \leq f(e) \leq c(e)$
2) $\forall v \in V \setminus \{z, s\}: \ \sum_{uv \in E} f(uv) = \sum_{vu \in E} f(vu)$ neboli $f[In(v)] = f[Out(v)]$

Značení: pro $v \in V$: $In(v) := \{uv \in E\}$ $\quad$ pro $A \subseteq V$: $In(A) := \{uv \in E \mid u \notin A, v \in A\}$

$Out(v) := \{vu \in E\}$ $\quad$ $Out(A) := \{vu \in E \mid v \in A, u \notin A\}$

pro $F \subseteq E$: $f[F] = \sum_{e \in F} f(e)$

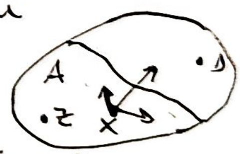
Def: Velikost toku f je $w(f) := f[Out(z)] - f[In(z)]$.
Maximální tok je tok, který má největší velikost.

Věta: V každé tokové síti existuje maximální tok.

Dk: Očíslujme hrany $E = \{e_1, \dots e_m\}$. Pak tok reprezentujme jako $(f(e_1), \dots f(e_m)) \in \mathbb{R}^m$. Množina všech toků je uzavřená a omezená (všechny složky jsou omezené kapacitami) podmnožina $\mathbb{R}^m$, takže je kompaktní. Ta funkce $w(f_1, \dots f_m)$ je nějaký polynom, takže je spojitá. Každá spojitá fce na kompaktní množině nabývá maxima.

Lemma: Pro tok f v síti (V, E, z, s, c) a pro $A \subseteq V$, $z \in V$ & $s \notin A$ platí

$$w(f) = f[Out(A)] - f[In(A)].$$



Dk: Víme $w(f) = f[Out(z)] - f[In(z)]$
$\forall x \in A \setminus \{z\}: \ 0 = f[Out(x)] - f[In(x)]$
$\oplus$ $\quad w(f) = \sum_{x \in A} f[Out(x)] - \sum_{x \in A} f[In(x)]$

$E_A := \{uv \in E \mid u \in A \ \& \ v \in A\} = E \cap A \times A$

$$= f[Out(A)] + f[E_A] - f[In(A)] - f[E_A]$$
$$= f[Out(A)] - f[In(A)]$$ $\blacksquare$

Def: <u>Řez</u> v síti (V, E, z, s, c) je množina hran $R \subseteq E$ t.ž.
$\forall$ orientovaná cesta $z \to s$ obsahuje alespoň jednu hranu z R.

Def: <u>Kapacita řezu</u> R je $c(R) := \sum_{e \in R} c(e)$. → ten zjevně vždy existuje

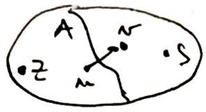
<u>Minimální řez</u> je řez, který má ze všech řezů nejmenší kapacitu.

Def: Nechť $A \subseteq V$: $z \in A$ & $s \notin A$, pak $Out(A)$ je řez. Každý takový řez je <u>elementární řez</u>.

$\forall$ řez R obsahuje nějaký elementární řez jako podmnožinu.

Dk: $A := \{x \in V \mid \exists$ cesta $z \to x$ co nevyužívá hrany $R\}$

Zjevně $z \in A$ & $s \notin A$, tedy $Out(A)$ je e. řez. Tvrdíme $Out(A) \subseteq R$.



kdyby $uv \in Out(A)$, $uv \notin R$, tak z definice A : $v \in A$ ↯

Lemma: Nechť f je tok a R řez v síti (V, E, z, s, c). Potom $w(f) \leq c(R)$.

Dk: Definujeme $A := \{x \in V \mid \exists$ cesta $z \to x$ co nevyužívá hrany $R\}$, $z \in A$, $s \notin A$, $Out(A) \subseteq R$

$w(f) = f[Out(A)] - f[In(A)] \leq f[Out(A)] \leq c(Out(A)) \leq c(R)$. ■

Def: <u>Nenasycená cesta</u> pro tok f je <u>neorientovaná</u> cesta $x_1 e_1 x_2 e_2 \dots x_{k-1} e_{k-1} x_k$, t.ž.

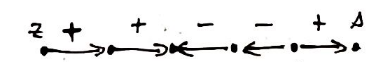
$\forall i$: $e_i = (x_i, x_{i+1})$ … dopředná hrana … platí $f(e_i) < c(e_i)$
nebo $e_i = (x_{i+1}, x_i)$ … zpětná hrana … platí $f(e_i) > 0$

Def: <u>Zlepšující cesta</u> pro f je nenasycená cesta $z \to s$.

: Pokud má tok f zlepšující cestu, tak není maximální.

Dk: Mohu ho zlepšit o $\varepsilon := \min(\{c(e_d) - f(e_d) \mid e_d \text{ dopředná}\} \cup \{f(e_z) \mid e_z \text{ zpětná}\})$

udělám $f(e_d) \mathrel{+}= \varepsilon$
$f(e_z) \mathrel{-}= \varepsilon$



ΔIn: + 0 − 0
ΔOut: + 0 − 0
$\Big\}$ $\Delta In = \Delta Out \Rightarrow In' = Out'$ ✓ ■

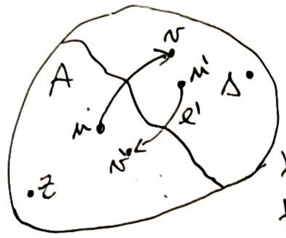
<u>Věta</u>: Pro tok f v síti (V, E, z, s, c) jsou následující tvrzení ekvivalentní:

1) f je maximální
2) f nemá zlepšující cestu
3) $\exists$ řez R t.ž. $c(R) = w(f)$, R je minimální $\because \overset{\forall f}{w(f)} \leq \overset{\forall R}{c(R)}$

Dk: $1 \Rightarrow 2$: $\neg 2 \Rightarrow \neg 1$ f má zlepšující cestu $\Rightarrow f$ není maximální ✓

$3 \Rightarrow 1$: pro $\forall$ tok f' a řez R' platí $w(f') \leq c(R')$
tedy $\forall$ tok f': $w(f') \leq c(R) = w(f)$ $\Rightarrow f$ je maximální ✓

2 ⇒ 3: Definujeme $A := \{x \mid \exists$ nenasycená cesta $z \to x\}$



Zjevně $z \in A$ & $s \notin A$ ⇒ $Out(A)$ je elementární řez

$R := Out(A)$, ukážeme $w(f) = c(R)$

$\forall\, e = uv \in Out(A)$: $f(e) = c(e)$ … kdyby $f(e) < c(e)$, tak $v \in A$ ↯

$\forall\, e' = u'v' \in In(A)$: $f(e) = 0$ … kdyby $f(e) > 0$, tak $u' \in A$ ↯

$\Rightarrow w(f) = f[Out(A)] - f[In(A)] = c(Out(A)) - 0 = c(R)$ ■

Důsledek (Minimaxová věta o toku a řezu): $w(f_{max}) = c(R_{min})$.

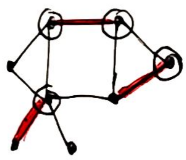
Dk: Dle věty $\exists$ řez R t.ž. $w(f_{max}) = c(R) \geq c(R_{min})$ & $w(f_{max}) \leq c(R_{min})$ ■

Důsledek 2: V síti, kde $\forall$ kapacity $\in \mathbb{Z}$ najde F.F. alg. max. tok $f: E \to \mathbb{Z}$.

• Aplikace toků v sítích

Def: Párování (matching) v grafu $G=(V,E)$ je $M \subseteq E$ t.ž. $\forall$ vrchol je v nejvýše jedné hraně v M.

Def: Vrcholové pokrytí (vertex cover) v G je $C \subseteq V$ t.ž. $\forall$ hrana obsahuje aspoň jeden vrchol z C.



Def: Perfektní párování je takové párování M, kde $\forall$ vrchol patří do právě jedné hrany M

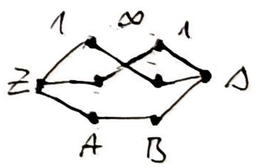
👁 Pokud je M párování a C vrcholové pokrytí v $G=(V,E)$, tak $|M| \leq |C|$.

Dk: $\forall e \in M$ musí být pokryta vrcholem z C, zároveň $\forall v \in C$ pokryje nejvýše jednu hranu z M  není párování ■

Věta (König-Egerváry): V každém bipartitním grafu platí $|M_{max}| = |C_{min}|$.

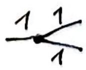
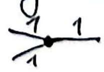
Dk: Nechť $G=(V,E)$ je bipartitní graf s partitami A, B.

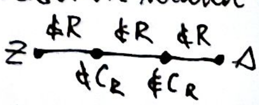
Vytvoříme tokovou síť $(V \cup \{z,s\}, E^+, z, s, c)$, kde



- $E^+ := \{zx \mid x \in A\} \cup (E \cap A \times B) \cup \{ys \mid y \in B\}$
- $c(zx) := 1$, $c(y,s) := 1$, pro $x \in A$, $y \in B$
- $c(xy) := |A| + |B| + 1$ … efektivně ∞

Určitě $|M_{max}| \leq |C_{min}|$. Nechť f je max tok a R min. řez v té síti. $w(f) = c(R)$.

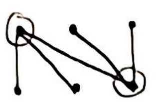
- $M_f := \{e \in E \mid f(e) > 0\}$, tečou tam jedničky $\Rightarrow |M_f| = w(f)$ … když f podle F.F.
  ↳ toto je párování, jinak  nebo  .
- $C_R := \{x \in A \mid zx \in R\} \cup \{y \in B \mid ys \in R\}$ 👁 R určitě neobsahuje žádnou hranu z A do B
  ↳ toto je vrcholové pokrytí, kdyby ne, tak R není řez



[illegible] jedničky

$|C_{min}| \leq |C_R| = |R| = c(R) = w(f) = |M_f| \leq |M_{max}| \leq |C_{min}| \Rightarrow$ všechno to jsou rovnosti ■

V bipartitním grafu s partitami A, B má $\forall$ párování velikost $\leq \min(|A|,|B|)$.

 pokrytí 2 $\Rightarrow$ párování ≤ 2 $\Rightarrow$ tohle není těsný odhad

<u>Značení</u>: pro $X \subseteq V$ označíme $N(X) := \{y \in V \setminus X \mid \exists x \in X : xy \in E\}$ ... sousedi X

<u>Věta (Hallova)</u>: Nechť G je bp. graf s partitami A, B.

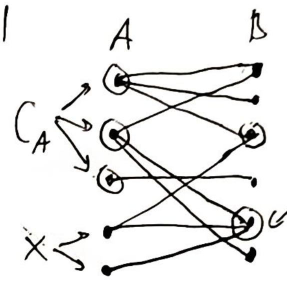
Potom G má párování velikosti $|A| \iff \underline{\forall X \subseteq A : |N(X)| \geq |X|}$. Hallova podmínka

$\Rightarrow$: z $\forall v \in A$ potřebuju vést párovací hranu $\Rightarrow$ pro $\forall X \subseteq A$ potřebuju alespoň $|X|$ sousedů.

$\Leftarrow$: Nechť M je maximální párování v G & pro spor předpokládejme $|M| < |A|$.

Podle K-E věty $\exists$ pokrytí C, kde $|C| = |M| < |A|$

$$\left.\begin{aligned} C_A &:= C \cap A \\ C_B &:= C \cap B \\ X &:= A \setminus C_A \end{aligned}\right\} \begin{aligned} &N(X) \subseteq C_B \Rightarrow |C_B| \geq |N(X)| \\ &|C_A| + |C_B| = |C| < |A| \end{aligned}$$



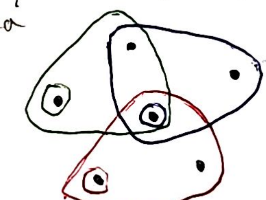
$\Rightarrow X \subseteq A$ $\quad |X| = |A| - |C_A| > |C_B| \geq |N(X)|$

$\Rightarrow |X| > |N(X)|$ což je spor s Hallovou podmínkou ↯ ■

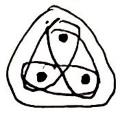
<u>Def</u>: Systém různých reprezentantů (SRR) v hypergrafu $H = (V, E)$ je funkce $r : E \to V$ t.ž.

1, $\forall e \in E : r(e) \in e$

2, $\forall e, f \in E : e \neq f \Rightarrow r(e) \neq r(f)$ $\quad$ r je prostá



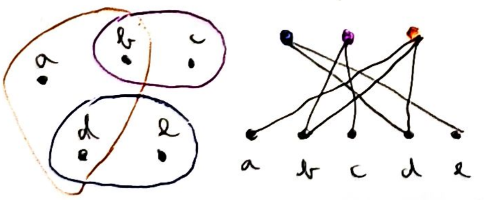
→ hrany + z $\forall$ hrany nějaký reprezentant

: Když nastane něco jako  tj. 4 hrany, ale jen 3 vrcholy, tak to nejde.

<u>Věta (Hallova pro hypergrafy)</u>: Hypergraf $H = (V, E)$ má SRR

$$\iff \underline{\forall F \subseteq E : \left|\bigcup_{e \in F} e\right| \geq |F|} \quad \text{Hallova podmínka}$$

<u>Dk</u>: Nechť I_H je graf incidence H.



H má SRR $\iff$ I_H má párování velikosti $|E|$

Hallova podmínka pro $H \iff$ bip. Hallova p. pro I_H ■

To, že nejsou cykly zabrání ↻ ... potom bych mohl jednou použít → a podruhé ↙

$\Rightarrow$ 2 cesty v síti

ale jen 1 cesta v G

Opakuj k-krát:

1. začni v x
2. jdi po hranách $S(f)$ dokud nebudeš v y (cesta)
3. použité hrany odstraň z $S(f)$

→ proč to funguje? Je to tok $\Rightarrow$ z $\forall$ vrcholu kam dojdu vede hrana (kirch. zákon)

→ tohle sníží velikost toku o 1, ale $f \geq k$

• Hranová a vrcholová souvislost grafu

⇒ od teď $G=(V,E)$ je neorientovaný, konečný graf & $|V|\geq 2$.

Def: Pro $F\subseteq E$: $G-F := (V, E\setminus F)$

Def: $F\subseteq E$ je hranový řez ≡ $G-F$ je nesouvislý.

G je hranově k-souvislý ≡ neobsahuje žádný hranový řez velikosti $< k$.

↳ smazání méně než k hran ho souvislost nerozbije.

👁 G je hranově 1 souvislý ⟺ G je souvislý.

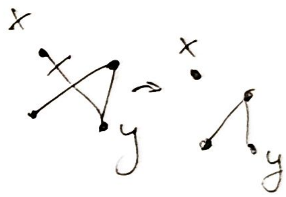
👁 G je hranově k-souvislý, $k\geq 2$ ⇒ G je hranově $(k-1)$-souvislý.

Def: Stupeň hranové souvislosti (hranová souvislost) grafu G je

$K_e(G) := \max\{k \mid G \text{ je hranově } k\text{-souvislý}\}$ = velikost nejmenšího hran. řezu

1-souvislý ✓ 2-souvislý ✓ 3-souvislý ✗ ⇒ $K_e(G)=2$

Def: Pokud $x,y\in V$, $x\neq y$, tak hranový xy-řez je $F\subseteq E$ t.ž. x a y jsou v různých komponentách $G-F$.

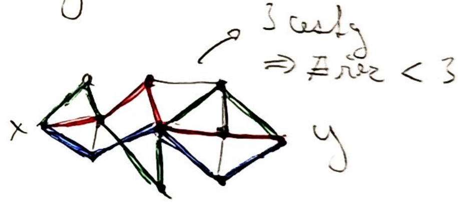


Věta: (Menger, hranová xy-verze): $\forall k\in\mathbb{N}$, $\forall x,y\in V$, $x\neq y$:

G obsahuje k hranově disjunktních $x\to y$ cest.

⟺

G neobsahuje hranový xy-řez velikosti $< k$.



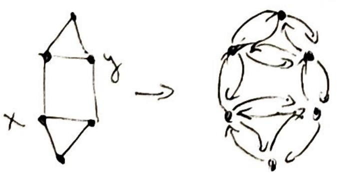
Dk: ⇒: Pokud mám k hranově disj. $x\to y$ cest,

tak ∀ xy-řez musí obsahovat alespoň 1 hranu z ∀ té cesty

⇐: Nechť G neobsahuje hranový xy-řez velikosti $< k$

↳ vyrobíme tokovou síť $(V, \vec{E}, x, y, c)$, $c=1$

• $\vec{E} := \{uv, vu \mid \{u,v\}\in E\}$ .. u — v →



👁 v té síti ∄ řez $< k$ … vznikl by xy-řez v G

⇒ |min. řez| = |max. tok| $\geq k$

→ intuitivně: když teče $\geq k$, tak tam musí být hodně cest / tak tok vyžírá co nejméně hran

Nechť f je celočíselný max. tok t.ž. $S(f) := \{e\in\vec{E} \mid f(e)=1\}$ je co nejmenší.

👁 f neobsahuje žádný orientovaný cyklus, jinak spor s minimalitou $S(f)$

⇒ teď už z $S(f)$ můžeme hladově vyrobit k hranově disj. cest v té síti, resp. v G.

Věta (Menger, globální hranová verze): Graf je hranově k-souvislý $\iff$ mezi $\forall$ dvěma různými vrcholy $\exists$ k hranově disjunktních cest.

Dk: G je hranově k-souv. $\iff \nexists$ hranový řez vel. $< k$

$\iff \forall x,y$ různé $\nexists$ hr. xy-řez vel. $< k$

(někdy toky F-F věta) $\iff \forall xy$ různé $\exists$ k hranově disjunktních cest.

- **Vrcholová souvislost**

Def: Pro $A \subseteq V$ je $G - A := (V \setminus A, E \cap \binom{V \setminus A}{2})$

Def: $A \subseteq V$ je vrcholový řez $\equiv$ $G - A$ je nesouvislý.

👁 K_n nemá žádný vrcholový řez ⟶

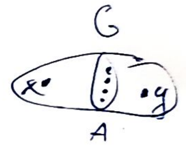
Def: Graf G je vrcholově k-souvislý $\equiv |V| \geq k+1$ a neobsahuje vrcholový řez vel. $< k$.

Def: Vrcholová souvislost grafu G je $k_v(G) := \max\{k \mid G \text{ je vrcholově } k\text{-souvislý}\}$

👁 $k_v(K_n) = n - 1$

👁 k_v(neúplný graf) = velikost nejmenšího vrcholového řezu

Def: Pro $x, y \in V$ různé je vrcholový xy-řez množina $A \subseteq V \setminus \{x, y\}$ t.ž. x, y jsou v různých komponentách $G - A$.



Def: Dvě cesty v G z x do y jsou vnitřně vrcholově disjunktní (VVD) $\equiv$ nemají žádný společný vrchol, kromě x a y.

👁 dvě VVD cesty jsou hranově disjunktní.

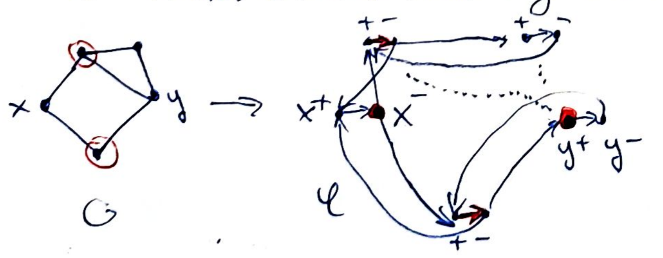
Věta (Menger, xy-vrcholová verze) $\forall k \in \mathbb{N}$, $\forall x, y \in V$ různé a nesousední vrcholy

G obsahuje k VVD cest z x do y $\iff$ G neobsahuje vrcholový xy-řez vel. $< k$

👁 důvod proč xy jsou nesousední: kdyby $x - y$, tak $\nexists$ žádný vrch. xy-řez.

Dk: $\Rightarrow$: $\forall$ xy řez musí obsahovat alespoň 1 vrchol z $\forall$ té cesty $\Rightarrow$ velikost aspoň k.

$\Leftarrow$: Nechť G nemá vrch. xy-řez vel $< k$. Vyrobíme síť $\mathcal{G}$ takto.



pro $\forall$ vrchol $v \Rightarrow v^+$ a v^-, $v^+ \to v^-$

hrany $u \to v \Rightarrow u^- \to v^+$ a $v^- \to u^+$

$\Rightarrow c(v^+ \to v^-) = 1$, $c(u^- \to v^+) = c(v^- \to u^+) = \infty$

Zdroj $= x^-$, stok $= y^+$

👁 $\forall$ min. řez v $\mathcal{G}$ obsahuje pouze hrany kapacity 1

👁 vrcholový xy-řez v G určuje min. řez v $\mathcal{G}$ a naopak & mají stejnou velikost

$\Rightarrow \mathcal{G}$ nemá řez kapacity $< k$

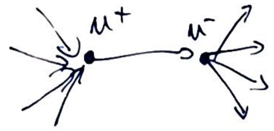
⇒ teď už stejná argumentace jako u hran

- $|\text{Min řez}| = |\text{Max tok}| \geq k$

⇒ stejnou argumentací jako předtím $\mathcal{G}$ obsahuje k hranově disj. $x^- \to y^+$ cest, označme je $\vec{P}_1, \dots \vec{P}_k$.

Ty cesty jsou i VVD

∵ $\forall\ x^- \to y^+$ cesta v $\mathcal{G}$, co obsahuje u^+ nebo u^- pro nějaké $u \neq x, y$, tak musí obsahovat i hrana u^+u^-



pokud nějaká cesta obsahuje u^+u^-, tak žádná jiná cesta už nemůže obsahovat u^+ nebo u^-

⇒ $\vec{P}_1, \dots \vec{P}_k$ jsou VVD a určují tedy k VVD $x \to y$ cest v G. ∎

<u>Lemma</u>: Nechť G je graf, $v \in V(G)$ a $G^- := G - v$. Potom $K_v(G^-) \geq K_v(G) - 1$

<u>Dk</u>: Nechť $K_v(G) = k$.

1, Pokud je G úplný, potom G^- je také úplný a $K_v(G^-) = K_v(G) - 1$.

2, Pokud není G úplný, tak k = velikost nejmenšího vrch. řezu v G.

a, pokud $G - v$ je úplný  , tak $K_v(G^-) = |V(G)| - 2 = (|V(G)| - 1) - 1 \geq K_v(G) - 1$.

b, pokud nějaký nejmenší vrch. řez G obsahuje v, tak velikost nejmenšího vrch. řezu $G^- = K_v(G^-) = k - 1 = K_v(G) - 1$.

c, jinak se odebráním v nic nezmění, čili $K_v(G^-) = K_v(G)$

Spor: Kdyby $K_v(G^-) \leq K_v(G) - 1$, tak by v G byl nějaký vrch. řez s méně než k vrcholy, takže tento řez spolu s v by měl nejvýše k vrcholů, takže by to byl min. řez v G ↯ ∎

Není potřeba

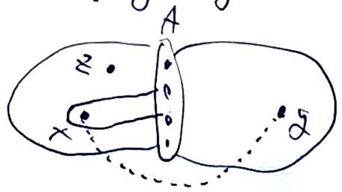
<u>Lemma</u>: Nechť G je graf, $e = xy \in E(G)$ a $G^- := G - e$. Potom $K_v(G^-) \geq K_v(G) - 1$.

<u>Dk #2</u>: Nechť A je nejmenší vrch. řez v G^-. Potom $K_v(G^-) = A$. Chceme $K_v(G) \leq |A| + 1$.

1, Pokud $\exists$ komponenta $G^- - A$, která neobsahuje x ani y, tak A je i vrch. řez v G.

2, Jinak má $G^- - A$ 2 komponenty – 1. obsahuje x (G^-_x) a 2. obsahuje y (G^-_y)

a, G^-_x obsahuje i jiný vrchol než x, tak $A \cup \{x\}$ je řez v G ⇒ $K_v(G) \leq |A| + 1$. →

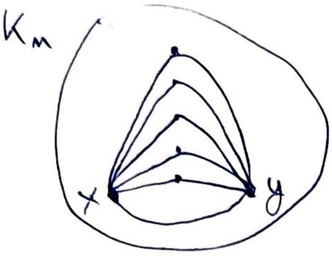


b, obdobně když G^-_y obsahuje jiný vrchol než y

c, Pokud G^-_x i G^-_y mají jen 1 vrchol, tak $|V| = |A| + 2$, tedy $K_v(G) \leq |V| - 1 = |A| + 1$.

Věta (Menger, globální vrcholová verze): G je vrcholově k-souvislý $\iff$ mezi $\forall x,y \in V$ různými $\exists$ k navzájem VVD cest.

Dk: Pokud $G = K_n$, tak $K_v(G) = n-1$, tedy G je vrch. k-souv. $\iff k \leq n-1$.



... $n-1$ VVD cest z x do y

Nechť G není úplný.

$\Leftarrow$: G musí mít aspoň $k+1$ vrcholů & žádný v. řez vel. $< k \Rightarrow G$ je k-souv.

$\Rightarrow$: Nechť x,y jsou různé vrcholy.

1, $\{x,y\} \notin E$: podle xy-verze M. věty $\exists k$ $x \to y$ VVD cest. ✓

2, $\{x,y\} \in E$: Nechť $G^- := G - e$, podle Lemmatu $K_v(G^-) \geq k-1$.

podle xy-verze M. věty $\exists$ $k-1$ $x \to y$ VVD cest
a navíc ta hrana xy co jsem smazal je cesta } k cest

Důsledek: Pro každý graf G platí $K_v(G) \leq K_e(G)$.

Dk: Nechť $K_v(G) = k$, potom mezi $\forall x,y \in V$, $x \neq y$ $\exists k$ různých VVD cest
$\Rightarrow \exists k$ různých hranově disj. cest $\Rightarrow G$ je hranově k-souvislý.

$\Rightarrow$ vrcholová k-souvislost je silnější

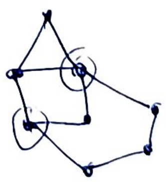
Konvence: "k-souvislý graf" znamená "vrcholově k-souvislý".

Def: Přidání ucha ke grafu $G=(V,E)$ je tato operace

1, zvolím dva různé vrcholy $x,y \in V$

2, pro $d \geq 0$ přidám vrcholy $z_1, z_2, \dots, z_d$

3, přidám hrany cesty $x z_1 z_2 \dots z_d y$

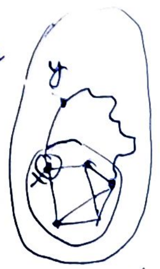


přidání hrany je také přidání ucha

Ušaté lemma: G je 2-souvislý $\iff$ G lze vyrobit z kružnice přidáváním uší.

Dk: $\Leftarrow$: Kružnice je 2 souvislá a přidávání uší nevyrobí řez velikosti 1.

$\Rightarrow$: Nechť C je libovolná kružnice v G. Nechť $G_{max} = (V_{max}, E_{max})$ je největší podgraf G, co je možné vyrobit přidáváním uší z C.



Pro spor $G_{max} \neq G$.

1, $V_{max} = V$, ale $E_{max} \neq E$ ↯ protože přidání hrany = přidání ucha

2, $V_{max} \neq V$. G je souvislý $\Rightarrow \exists xy \in E : x \in V_{max}, y \notin V_{max}$

G je 2-s. $\Rightarrow G - x$ je souv $\Rightarrow \exists$ cesta z y do něčeho ve V_{max} $\to$ tahle cesta spolu s xy je ucho ↯

Platí: $K_e(G)-1 \le K_e(G-e) \le K_e(G)$ & $K_v(G)-1 \le K_v(G-e) \le K_v(G)$

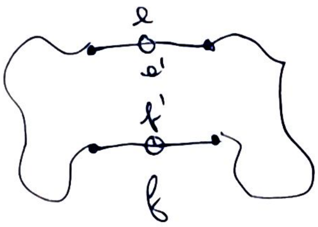
Tvrzení pro 2-souvislé grafy:

Graf G je 2-souvislý, právě když ... G alespoň 3 vrcholy

1, pro každé jeho dvě hrany e, f $\exists$ cyklus obsahující e a f

2, pro každé tři různé vrcholy x, y, z $\exists$ $x \to z$ cesta přes y.

Dk: 1) $\Rightarrow$: podrozdělíme hrany e, f

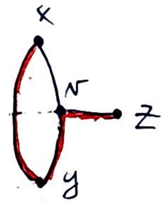


$\forall$ dva vrcholy x, y G obsahuje cyklus s x a y ... $\because$ $\exists$ 2 VVD cesty

$\Rightarrow$ uděláme cyklus s e' a f' $\Rightarrow$ leží na něm e i f

$\Leftarrow$: $\forall$ dvě hrany leží na cyklu $\Rightarrow$ mezi $\forall$ dvěma vrcholy jsou alespoň 2 VVD c.

2) $\Rightarrow$:



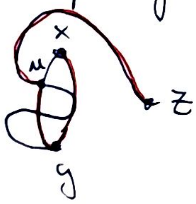
2 souvislý $\Rightarrow$ $\exists$ cyklus s x a y

↳ vezmu si nejkratší cestu ze z do toho cyklu $\Rightarrow v$

$\Rightarrow$ udělám cestu $x \to y \to v \to z$

Pokud $v = x$, tak to nefunguje

$\Rightarrow$ použijeme $y \to z$ cesta



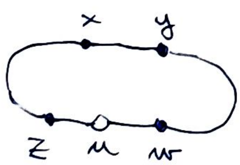
u = poslední průsečík toho xy-cyklu s tou $y \to z$ cestou

$\Rightarrow$ udělám cestu $x \to y \to u \to z$

co když ta $y \to z$ cesta vede přes x?

$\to$ tak vezmu tu druhou – jsou VVD, takže ta x neobsahuje

$\Leftarrow$: ukážeme, že pro $\forall$ dvě hrany $\exists$ cyklus s nimi ... 1



$\to$ hranu zw podrozdělím ... to tu podmínku neporuší

$\Rightarrow$ udělám cestu z x do y přes u $\Rightarrow$ to je cyklus ∎

$\forall$ k-regulární bip. graf má perfektní párování

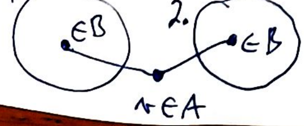
Dk: obě partity stejně velké $\Rightarrow$ použiju $|\text{max. pár.}| = |\text{min. vrch. pokrytí}| = |\text{partity}|$

Tvrzení: Každý souvislý k-regulární ($k \ge 2$) bip. graf je 2-souvislý.

Dk: Pro spor. nechť není 2-souvislý. Potom $\exists$ vrcholový řez velikosti $1 \to v$. part.

Ten řez rozdělí graf na alespoň 2 komponenty – BÚNO všichni sousedi v jsou v B

$\to$ počítejme hrany v nějaké komponentě



pomocí A: $\#\text{hran} = k \cdot \#\text{vrcholů}$

pomocí B: $\#\text{hran} = k \cdot \#\text{vrcholů} - \overbrace{\#\text{hran do } v}^{1 \le \# < k}$

$\Big\}$ # hran modulo k nesedí ∎

• **Cayleyho vzorec**

$S_n :=$ # stromů na množině vrcholů $\overbrace{\{1, \dots n\}}^{[n]}$ = # koster úplného g. na n vrch.

$S_1 = 1$

$S_2 = 2$

$S_3 = 3$ 

$S_4 = 16$ 

4x 12x

<u>Věta</u>: $S_n = n^{n-2}$

<u>Dk</u>: <u>Def</u>: <u>Kořenový strom</u> je strom, kde se 1 vrchol určil jako kořen a všechny hrany zorientovaly směrem ke kořeni.

$K_n :=$ # kořenových stromů $= n \cdot S_n$ ... n různých kořenů

Pokud v nějakém stromě zorientujeme hrany tak, aby z ∀ vrcholu odcházela nejvýš 1 hrana, tak $\exists! \, k \in V$ z něhož žádná hrana neodchází; a navíc jsou všechny hrany orientované do k.

<u>Dk</u>: strom má $n-1$ hran $\Rightarrow$ z $n-1$ vrcholů musí odcházet hrana
$\Rightarrow$ z právě 1 neodchází

<u>Def</u>: <u>Povykos</u> (Postup vytvoření koř. stromu) je posloupnost $n-1$ orientovaných hran $(e_1, e_2, \dots e_{n-1})$ na vrcholech $[n]$ t.ž. $([n], \{e_1, \dots e_{n-1}\})$ je koř. strom.

$P_n :=$ # povykosů $= (n-1)! \, K_n$

Posloupnost or. hran $(e_1, e_2, \dots e_{n-1})$ je povykos $\Leftrightarrow$ pro $\forall k \in [n-1]$

1) hrana e_k spojuje vrcholy z různých komponent grafu tvořeného hranami $e_1, \dots e_{k-1}$
$\Rightarrow$ zabráníme cyklům

2) hrana e_k vychází z vrcholu z něhož nevychází žádná z hran $e_1, \dots e_{k-1}$
... protože v k. stromě může z ∀ vrcholu odcházet nejvýš 1 hrana.
→ v ∀ komponentě je právě 1 takový vrchol a sice její kořen

$\Rightarrow$ Jak vyrobit nějaký povykos?

$e_1 \dots n \cdot (n-1)$ možností, n komponent → do jiné k.
$e_2 \dots n \cdot (n-2)$, $n-1$ komponent → $n-2$ jiných k.
$e_k \dots n \cdot (n-k)$, $n-k+1$ komponent → $n-k$ jiných k

} začíná jinde než končí & začíná v kořeni dané komponenty

konec ↑ ↑ začátek

$\Rightarrow P_n = n^{n-1} \cdot (n-1)! \Rightarrow K_n = n^{n-1} \Rightarrow \underline{\underline{S_n = \frac{K_n}{n} = n^{n-2}}}$

- **Spernerova věta**
  - počítání dvěma způsoby

👁 bipartitní graf: $A, B \Rightarrow |E| = \sum_{x \in A} \deg(x) = \sum_{x \in B} \deg(x)$

Značení: $\mathcal{P}$ ... potenční množina

$\binom{[n]}{k} :=$ množina všech k-prvkových podmnožin $[n] = \{X \in \mathcal{P}([n]) \mid |X| = k\}$

Def: Antiřetězec v $\mathcal{P}([n])$ je množina $A \subseteq \mathcal{P}([n])$ t.ž. $\forall M_1, M_2 \in A,\ M_1 \neq M_2$ neplatí $M_1 \subseteq M_2$ ani $M_2 \subseteq M_1$. } antiřetězec uspořádání je obecně nějaká množina, kde jsou všechny prvky neporovnatelné

Příklad: antiřetězce v $\mathcal{P}([4])$

např: $\{\{1\},\{2\},\{3\},\{4\}\},\ \{\emptyset\},\ \emptyset,\ \{\{1,2,3\},\{3,4\}\},\ \overbrace{\{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}}^{\binom{[4]}{2}}$

Věta (Spernerova): Největší antiřetězec v $\mathcal{P}([n])$ má velikost $\binom{n}{\lceil \frac{n}{2} \rceil} = \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

↳ je to množina $\binom{[n]}{\lceil \frac{n}{2} \rceil}$, respektive $\binom{[n]}{\lfloor \frac{n}{2} \rfloor}$

Dk: 1, ⟶ tohle jsou antiřetězce

2, neexistuje žádný větší

Nechť $a = \{A_1, A_2, \dots A_k\}$ je antiřetězec, chceme $k \leq \binom{n}{\lceil \frac{n}{2} \rceil}$

Def: Nasycený řetězec v $\mathcal{P}([n])$ je posloupnost $M_0, M_1, \dots M_n \subseteq [n]$, kde $M_0 \subseteq M_1 \subseteq M_2 \subseteq \dots \subseteq M_n \subseteq [n]$ a $|M_i| = i$.

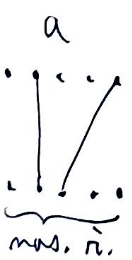
Příklad: $n=4$: $\emptyset \subseteq \{2\} \subseteq \{2,4\} \subseteq \{2,4,3\} \subseteq \{2,4,3,1\} = [4]$

👁 $\exists$ jich $n!$ a navíc $\forall$ nas. řetězec obsahuje nejvýš 1 množinu z a

$\Rightarrow$ počítejme dvěma způsoby dvojice (A, R), kde $A \in a$, $A \in R$, R je nas. řetězec

1, přes nas. řetězce #dvojic $\leq n!$ → celkem jich je $n!$, ale $\forall$ obsahuje max. 1 A

2, pro $A \in a$ mám $|A|!\,(n-|A|)!$ nas. řetězců obsahujících A



$$\underbrace{\emptyset \subseteq \{2\} \subseteq}_{|A|!} \underset{A}{\{1,2\}} \subseteq \underbrace{\dots \subseteq [n]}_{(n-|A|)!}$$ ... celkem tedy je $n+1$ věcí ... $A+1+n-A = n+1$

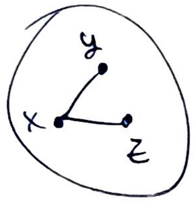
$$n! \geq \sum_{A \in a} |A|!\,(n-|A|)!$$

$$\Rightarrow 1 \geq \sum_{A \in a} \frac{1}{\binom{n}{|A|}} \geq \sum_{A \in a} \frac{1}{\binom{n}{\lceil \frac{n}{2} \rceil}} = |a| \cdot \frac{1}{\binom{n}{\lceil n/2 \rceil}} \Rightarrow |a| \leq \binom{n}{\lceil n/2 \rceil}$$ ∎

• <u>Odhad na počet hran v grafu, co neobsahuje C_4 jako podgraf</u>

<u>Věta</u>: Nechť $G=(V,E)$ je graf na n vrcholech, co neobsahuje C_4 jako podgraf.
kružnice
Potom $|E| \in O(n\sqrt{n})$.

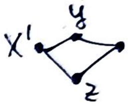
<u>Dk</u>: Označme $H := \#$ dvojic $(x, \{y,z\})$ t.ž. $x,y,z \in V$, $y \neq z$, x je soused y i z.



Počítejme H dvěma způsoby

1) pro dané x máme přesně $\binom{\deg(x)}{2}$ možností

$$\Rightarrow H = \sum_{x\in V} \binom{\deg x}{2} = \sum_{x \in V} \frac{\deg(x)\cdot(\deg x - 1)}{2} \geq \frac{1}{2}\sum_{x\in V} (\deg x - 1)^2$$

2) pro dané $\{y,z\} \in \binom{V}{2}$ $\exists!$ společný soused, jinak  $\to C_4$ ↯

$$H \leq \binom{|V|}{2} = \frac{n(n-1)}{2} \leq \frac{n^2}{2}$$

$$\Rightarrow n^2 \geq \sum_{x\in V} (\deg x - 1)^2, \quad |E| = \frac{1}{2}\sum_{x\in V} \deg x$$

→ víme horní odhad součtu druhých mocnin, chceme 1. mocniny.

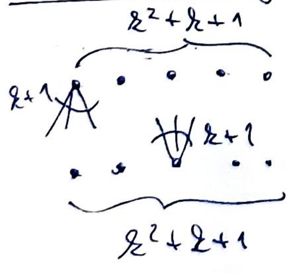
⇒ použijeme nerovnost mezi kvadr. a arit. průměrem ... $k \geq a$

$$n \geq \frac{1}{n}\sum_{x\in V} (\deg x - 1)^2 \Rightarrow \sqrt{n} \geq \sqrt{\frac{1}{n}\sum_{x\in V}(\deg x - 1)^2} \quad \text{... kvadr. průměr}$$

$$\Rightarrow \sqrt{n} \geq \sqrt{\frac{1}{n}\sum_{x\in V}(\deg x - 1)^2} \geq \frac{1}{n}\sum_{x\in V}(\deg(x) - 1) = \frac{1}{n}(2|E| - n)$$

$$\Rightarrow n\sqrt{n} \geq 2|E| - n \Rightarrow |E| \leq \frac{1}{2}(n\sqrt{n} + n) \in O(n\sqrt{n}). \quad \blacksquare$$

<u>Odhad je těsný</u>: Mějme incidenční graf konečné proj. roviny řádu k.



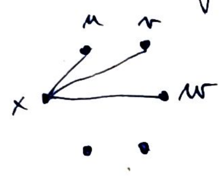
$$\left.\begin{aligned} &\Rightarrow |V| = 2(k^2+k+1) \in \Theta(k^2) \\ &|E| = (k^2+k+1)(k+1) \in \Theta(k^3) \end{aligned}\right\} |E| \in \Theta(|V|^{3/2})$$

• Ramseyovy věty

Def: Klika v grafu $G=(V,E)$ je $K \subseteq V$ t.ž. $\forall u,v \in K: uv \in E$. → úplný podgraf

Nezávislá množina je $N \subseteq V$ t.ž. $\forall u,v \in N: uv \notin E$. → prázdný podgraf

V každém grafu na 6 vrcholech $\exists$ klika velikosti 3 nebo NzMna vel. 3



1, x má aspoň 3 sousedy u, v, w

↳ jsou aspoň 2 spojeni hranou? — ano ⇒ klika; ne ⇒ u, v, w jsou NzMna

2, x nemá aspoň 3 sousedy – podobně

Ekvivalentně: Když v K_6 obarvím hrany červeně a modře, tak vždy tam bude 1-barevný trojúhelník.

Věta: (Ramseyova, grafová verze): $\forall k, l \in \mathbb{N}: \exists n \in \mathbb{N}$ t.ž.

$\forall$ graf na n vrcholech obsahuje kliku vel. k nebo NzMnu vel. l.

Def: Označíme $R(k,l)$ nejmenší n pro které to platí. Ramseyova čísla

$R(3,3)=6$ ∵ C_5  … věděli jsme $R(3,3) \leq 6$.

$R(k,l) = R(l,k)$.

Dk: Indukcí podle $k+l$.

1. $R(k,1) = 1 = R(1,l)$

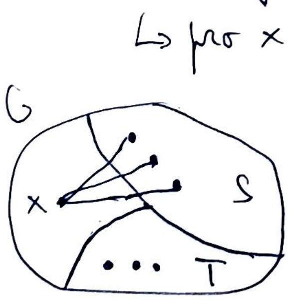
$R(k,2) = k = R(2,k)$ — úplný ⇒ klika; neúplný ⇒ nějaké 2 vrcholy nespojené ⇒ NzMna

2. Mějme $k, l \geq 3$.

Definujme $n := R(k,l-1) + R(k-1,l)$ … $\exists$ dle indukčního p.

Nechť G je libovolný graf na n vrcholech.

↳ pro $x \in V(G)$ označíme S sousedy x a $T := V \setminus (S \cup \{x\})$



$|S| + |T| = n-1 = R(k,l-1) + R(k-1,l) - 1$

⇒ platí buď

1. $|S| \geq R(k-1,l)$
2. $|T| \geq R(k,l-1)$

} kdyby ani jedno nenastalo, tak $|S|+|T| < n-1$ ↯

1, $G_S :=$ podgraf G indukovaný S

$|V(G_S)| = |S| \geq R(k-1,l)$

⇒ G_S obsahuje buď

a, kliku vel. $k-1$, ale x je se všemi spojený ⇒ klika vel. k

b, nz. mnu. vel. l … hotovo

2, analogicky

■

Důsledek: $\forall m \in \mathbb{N}\ \exists n \in \mathbb{N}$: $\forall$ graf na n vrcholech má kliku nebo NzMnu vel. m.

Ekvivalentně: $\forall m\ \exists n$: $\forall$ obarvení hran úplného grafu K_n červeně a modře obsahuje jednobarevnou kliku velikosti m.

Věta (vícebarevná verze R.v.): $\forall b \in \mathbb{N}, \forall m \in \mathbb{N}\ \exists n \in \mathbb{N}$ t.ž.

$\forall$ b-obarvení hran K_n obsahuje jednobarevnou kliku velikosti m.

$\sim \exists$ množina m vrcholů t.ž. všechny hrany mezi nimi mají stejnou barvu.

Dk: Označme $R^*_b(m)$ nejmenší n, pro které to platí.

... připomeňme $R(k,l)$ = nejmenší n, kde K_n má při obarvení červeně a modře

Indukcí podle počtu barev.

1, pro $b=1$: $R^*_1(m) = m$

pro $b=2$: $R^*_2(m) = R(m,m)$, což už víme, že existuje

2, Mějme $b>2$. Nechť $N := R(m, R^*_{b-1}(m))$. podle i.p. existuje

$\Rightarrow$ Mějme nějaké obarvení K_N pomocí b barev. Nechť ty barvy jsou modrá a $b-1$ odstínů červené.

Když zapomenu, že ty červené jsou různé, tak podle klasické R.v. v tom obarvení existuje

a, modrá klika velikosti m ... hotovo ✓

b, klika X velikosti $R^*_{b-1}(m)$ t.ž. všechno to jsou odstíny červené.

↳ podle i.p. pro $b-1$ a m $\exists$ nějaké $N \in \mathbb{N}$ t.ž. $\forall K_N$ obsahuje jednobarevnou kliku velikosti m

↳ X má z definice $R^*_{b-1}(m)$ dost vrcholů $\Leftarrow X$ indukuje úplný graf

$\Rightarrow$ v X $\exists$ nějaká jedno-odstínová klika velikosti m.

↳ respektive v grafu indukovaném X ▨

Značení:

$[n] := \{1, 2, \dots n\}$

pro množinu X je $\binom{X}{p}$ množina všech p-prvkových podmnožin X

Def: $K^{(p)}_n$ je p-uniformní úplný hypergraf, což je hypergraf H: $V(H) = [n]$, $E(H) = \binom{[n]}{p}$

↳ p-uniformní ... velikost všech hran je p

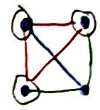
↳ úplný ... jsou tam všechny hrany co je možné $\Big\}$ $K_N = K^{(2)}_N$

Def: Pro $b \in \mathbb{N}$: b-obarvení $K_n^{(p)}$ je funkce $\binom{[n]}{p} \to [b]$. → barvíme hyperhrany

Def: Pro dané b-obarvení B hypergrafu $K_n^{(p)}$ řekneme, že množina vrcholů $X \subseteq [n]$ jednobarevná
$\equiv$ B přiřazuje všem hyperhranám v $\binom{X}{p}$ stejnou barvu.

Příklad: Pro K_n je množina vrcholů X jednobarevná v obarvení B
$\iff$ B přiřazuje všem hranám mezi těmi vrcholy stejnou barvu.

! nebarvíme vrcholy, ale hyperhrany
když řekneme, že množina vrcholů je jednobarevná, tak ty vrcholy se klidně mohou účastnit nějakých dalších jinak barevných hyperhran



Def: $K_\infty^{(p)} := (\mathbb{N}, \binom{\mathbb{N}}{p})$ ... nekonečný hypergraf

Věta (Ramsey, konečná verze): $\forall p \in \mathbb{N}, \forall b \in \mathbb{N}, \forall m \in \mathbb{N}\ \exists n \in \mathbb{N}$:
$\forall b$-obarvení $K_n^{(p)}$ obsahuje jednobarevnou m-prvkovou $\overbrace{\text{podmnožinu } [n]}^{\text{množina vrcholů}}$
~ jednobarevnou kliku velikosti m

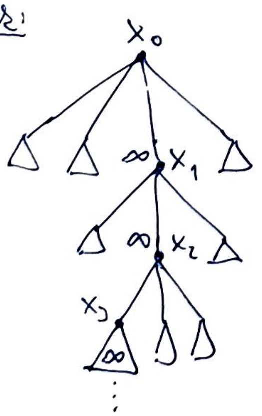
Věta (Ramsey, nekonečná verze): $\forall p \in \mathbb{N}, \forall b \in \mathbb{N}$
$\forall b$-obarvení $K_\infty^{(p)}$ obsahuje nekonečnou jednobarevnou $\overbrace{\text{podmnožinu } \mathbb{N}}^{\text{množina vrcholů}}$

$p=1$:  stačí $n = \underbrace{b\,(m-1)}_{b} + 1$ – princip holubníku pro b holubníků n holubů

$b=3$, $m=3$

Věta (Königovo lemma): Nechť T je nekonečný strom který neobsahuje vrchol ∞ stupně. Nechť x_0 je libovolný vrchol T. Potom T obsahuje nekonečnou cestu začínající v x_0.

Dk:



Zakoreníme T v x_0.
Indukcí definujeme posloupnost vrcholů $\overbrace{x_0, x_1, x_2, \dots}^{\text{nekonečná cesta}}$ tak, že tvoří cestu & pro $\forall i \in \mathbb{N}_0$: podstrom x_i má ∞ vrcholů

1, začneme s x_0.

2, Nechť už máme $x_0, x_1, \dots x_n$

$\Rightarrow$ x_n má nekonečný podstrom, ale jen konečný stupeň

holubník $\Rightarrow$ $\exists$ nějaký potomek x_n, co má nekonečný podstrom

$\Rightarrow$ libovolný z těchto potomků zvolím za x_{n+1} ■

Poznámka: Dokonce to platí v obecném souvislém lokálně konečném ∞ grafu.

Tvrzení: Z nekonečné verze R.v. plyne konečná verze.

Dk: Nechť neplatí konečná verze R.v., tedy

$\exists p\in\mathbb{N}, \exists b\in\mathbb{N}, \exists m\in\mathbb{N}, \forall n\in\mathbb{N}: \exists\, b$-obarvení $K_n^{(p)}$ neobsahující jednobar. množinu vrcholů vel. m.

Def: b-obarvení β hypergrafu $K_n^{(p)}$ je záludné
$\equiv$ v něm $\nexists$ jednobarevná množina vrcholů vel. m

$\Rightarrow$ pro spor vlastně předpokládáme, že pro $\forall n\in\mathbb{N}$ $\exists$ záludné obarvení.

$Z_n :=$ množina všech záludných b-obarvení $K_n^{(p)}$

Řekneme, že b-obarvení $\gamma\in Z_{n+1}$ rozšiřuje b-obarvení $\beta\in Z_n$, pokud pro $\forall h\in\binom{[n]}{p}$ platí $\beta(h)=\gamma(h)$.

↳ pokud mám už nějaké b-obarvení těch hyperhran na n vrcholech a přidám nový vrchol, tak barevnost starých hran zachovám. a nějak obarvím ty nové hrany – je to rozšíření.

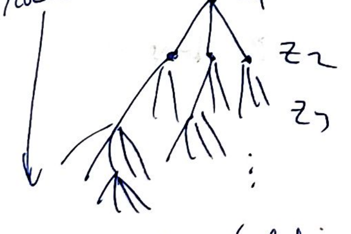
☼ $\forall\, \gamma\in Z_{n+1}$ rozšiřuje právě jedno $\beta\in Z_n$.

↳ když zapomenu, co γ vrací pro hrany obsahující vrchol $n+1$, tak dostanu přesně β

Definujme strom T na vrcholech $Z_1\cup Z_2\cup Z_3\cup\ldots = \bigcup_{n\in\mathbb{N}} Z_n$.

$\Rightarrow$ vrcholy toho stromu jsou všechna možná záludná obarvení pro b,p,m

$\{\beta,\gamma\}$ je hrana $\Leftrightarrow$ γ rozšiřuje β (nebo naopak)



V tom stromě $\exists$ nekonečná cesta $\beta_1,\beta_2,\beta_3,\ldots$, kde $\beta_i\in Z_i$

↳ ten strom je ∞ & ho lze rozšířit jen konečně mnoha způsoby

$\Rightarrow$ můžu použít Königovo lemma, co mi dá tu posloupnost

Nyní definujme obarvení $\beta:\binom{\mathbb{N}}{p}\to[b]$ takto:

- Nechť máme dánu hyperhranu $h\in\binom{\mathbb{N}}{p}$, volme $n\in\mathbb{N}$ t.ž. $h\subseteq[n]$.

  a definujme $\beta(h):=\beta_n(h)=\beta_{n+1}(h)=\beta_{n+2}(h)=\ldots$ protože ty hrany jsou rozšíření

Tvrdím, že β je záludné pro $K_\infty^{(p)}$ $\Rightarrow$ nekonečná R.v. neplatí ↯

$\rightarrow$ kdyby β nebylo záludné, tak by mělo nějakou jednobarevnou m-prvkovou mnu $X\subseteq\mathbb{N}$. Zvolíme $n\in\mathbb{N}$ aby $X\subseteq[n]$.

Potom β obarví $\binom{X}{p}$ stejně jako β_n, ale β_n je záludné obarvení $K_n^{(p)}$, takže X v něm nemůže být jednobarevná ↯

• Samoopravné kódy

- motivace: posíláme data přes nějaký nespolehlivý kanál - např. DVD - poškrábání
- omezení:
  1, všechno nad abecedou $\mathbb{Z}_2$ ... 0, 1
  2, informace rozdělena na slova pevné délky k, $\forall$ slovo kódujeme na slovo délky n
  3, chyby nemění počet symbolů
- příklady:

skreslené

• trojnásobné opakování: $0 \rightsquigarrow 000$, $1 \rightsquigarrow 111 \rightsquigarrow 011 \xrightarrow{maj.} 111 \to 1$

• kontrola parity: $x_1 x_2 x_3 \rightsquigarrow x_1 x_2 x_3 p$, $p = x_1 \oplus x_2 \oplus x_3$
↳ XOR = sčítání nad $\mathbb{Z}_2$

$$p = \begin{cases} 1 \Leftrightarrow \text{lichý } \#1 \\ 0 \Leftrightarrow \text{sudý } \#1 \end{cases} \Rightarrow x_1 x_2 x_3 p \text{ vždy sudý } \#1$$

$\Rightarrow$ 0111 ... někde je chyba, ale nevím kde
1010 ... buď to je správně, nebo se to celé hodně změnilo

Def: $\mathbb{Z}_2^n$ ... množina slov délky n nad $\mathbb{Z}_2$, slova píšeme jako řádkové vektory: $x = (x_1, \dots x_n)$

$$(x_1, \dots x_n) \oplus (y_1, \dots y_n) := (x_1 \oplus y_1, \dots x_n \oplus y_n)$$

$\Rightarrow \mathbb{Z}_2$ je těleso, $\mathbb{Z}_2^n$ je v. p.

Def: Hammingova vzdálenost pro $x, y \in \mathbb{Z}_2^n$ je $d(x,y) := \# i : x_i \neq y_i$
↳ $d(0000, 1111) = 4$, $d(0011, 0000) = 2$, $d(0101, 1110) = 3$

Hammingova váha $\|x\| := \# i : x_i \neq 0$ $\longrightarrow$ $\|00111\| = 3$ -> na $\mathbb{Z}_2$ to je #1

👁: $\|x\| = d(x, \sigma)$, $d(x,y) = \|x \oplus y\|$
↳ $1 \oplus 1 = 0 \oplus 0 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$ => #1 = # různých

↳ nulový vektor $= \sigma$

Def: Kód je nějaká $C \subseteq \mathbb{Z}_2^n$.

Pro kód $C \subseteq \mathbb{Z}_2^n$ je min. vzdálenost $\Delta(C) := \min\limits_{x,y \in C, x \neq y} d(x,y)$

(n,k,d)-kód je množina $C \subseteq \mathbb{Z}_2^n$ t.ž. $|C| = 2^k$ a $\Delta(C) = d$.

Příklady:

- 3-opakování: $C_1 = \{000, 111\}$ je $(3,1,3)$-kód
- parita: $C_2 = \{x \in \mathbb{Z}_2^4 \mid \|x\| \text{ je sudá}\}$ je $(4,3,2)$-kód

} oba jsou lineární

$= \{(x_1, x_2, x_3, x_4) \mid x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0\}$

↳ mna řešení homogenní soustavy lin. rovnic ⇒ vektorový podpr.

Def: Kód $C \subseteq \mathbb{Z}_2^n$ je lineární $\equiv$ C je v. podprostor $\mathbb{Z}_2^n$.

Protože jsme v $\mathbb{Z}_2$, tak ekvivalentně

1, $\sigma \in C$

2, $\forall x,y \in C : x \oplus y \in C$.

Pokud je (n,k,d)-kód lineární, tak k je jeho dimenze.

→ neformálně ten parametr odpovídá # bitů užitečné informace ve slově kódu

Pokud C je lineární kód, tak $\Delta(C) = \min\limits_{x \in C \setminus \sigma} d(x, \sigma) = \min\limits_{x \in C \setminus \sigma} \|x\|$.

Dk: pokud $x,y \in C$ a $d(x,y) = \Delta(C)$, tak $d(x,y) = d(x \oplus y, 0)$ | a to mi rohledinuje

Def: Nechť C je (n,k,d)-kód, potom kódování pro C je bijekce $\mathbb{Z}_2^k \to C$

↳ kódování je mechanismus převádění slov délky k na slova délky n.

Def: Pro lineární (n,k,d)-kód C je jeho generující matice $G \subseteq \mathbb{Z}_2^{k \times n}$, jejíž řádky tvoří bázi C.

Příklad:

- pro C_1 $\exists!$ gen. matice a sice $(1 \ 1 \ 1)$
- pro C_2 $\exists$ více gen. matic – libovolné 3 lin. nez. vektory sudé váhy

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \text{ nebo } G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

→ bijekce

→ zobrazení $g: x \mapsto xG$ je nějaké l.z. ... je to kódování?

$g_1 : x \mapsto xG_1 : (x_1, x_2, x_3) \mapsto (x_1, x_2, x_3, x_1 \oplus x_2 \oplus x_3)$ ... parita → tohle ✓

$g_2 : x \mapsto xG_2 : (x_1, x_2, x_3) \mapsto (x_1 \oplus x_2, x_1 \oplus x_2 \oplus x_3, x_1, x_1 \oplus x_3)$ → tohle ??

Tvrzení: Pokud G je gen. matice (n,k,d)-kódu C, tak $g: x \mapsto xG$ je kódování pro C.

Dk: Ukážeme, že $\forall x \in \mathbb{Z}_2^k : g(x) \in C$ a g je prosté (protože $|C| = |\mathbb{Z}_2^k|$, tak i bijekce)

1). Nechť $g: \mathbb{Z}_2^k \to \mathbb{Z}_2^n$, $x \mapsto xG$, a nechť $r_1, r_2, \dots r_k$ jsou řádky G.

→ ∵ tvoří bázi C, tak $r_1, \dots r_k \in C$.

→ pro $\forall x = (x_1, \dots x_k)$ máme $xG = x_1 r_1 \oplus x_2 r_2 \oplus \dots \oplus x_k r_k$, což je nějaká lineární kombinace prvků C, takže $xG \in C$.

2) kdyby $\exists x_1 \neq x_2 \in \mathbb{Z}_2^k : g(x_1) = g(x_2)$, tak

$x_1 G = x_2 G \iff x_1 G - x_2 G = 0 \iff \underbrace{(x_1 - x_2)}_{\neq 0} G = 0$, což nejde, protože řádky G jsou lineárně nezávislé. ∎

Def: Dekódování (n,k,d)-kódu C je funkce $f: \mathbb{Z}_2^n \to C \subseteq \mathbb{Z}_2^n$ t.ž.

$$\forall x \in \mathbb{Z}_2^n : d(x, f(x)) = \min_{y \in C} d(x,y).$$

→ dekódování převede zkomolené slovo kódu na nějaké actual slovo kódu, aby se při tom změnilo co nejméně bitů

↳ předpokládáme totiž, že se spíš změní málo bitů, než hodně.

Příklad:

$$C_1 : f(x) = \begin{cases} 000, & \text{pokud } \|x\| \leq 1 \\ 111, & \text{jinak} \end{cases}$$

$$C_2 : f(x) = \begin{cases} x, & \text{pokud } x \in C_2 \\ x \oplus (1,0,0,0), & \text{jinak} \end{cases}$$ → tohle změní 1 bit ⇒ bude pak sudý #1

Def: Pro $x = (x_1, \dots x_n)$ a $y = (y_1, \dots y_n)$ definujeme $\langle x,y \rangle := x_1 y_1 \oplus x_2 y_2 \oplus \dots \oplus x_n y_n$.

! není to skalární součin – může se stát, že pro $x \neq 0$ je $\langle x,x \rangle = 0$. → např. $x = 1010$

Def: $C^\perp := \{ y \in \mathbb{Z}_2^n \mid \forall x \in C : \langle x,y \rangle = 0 \}$ ... duální kód k C

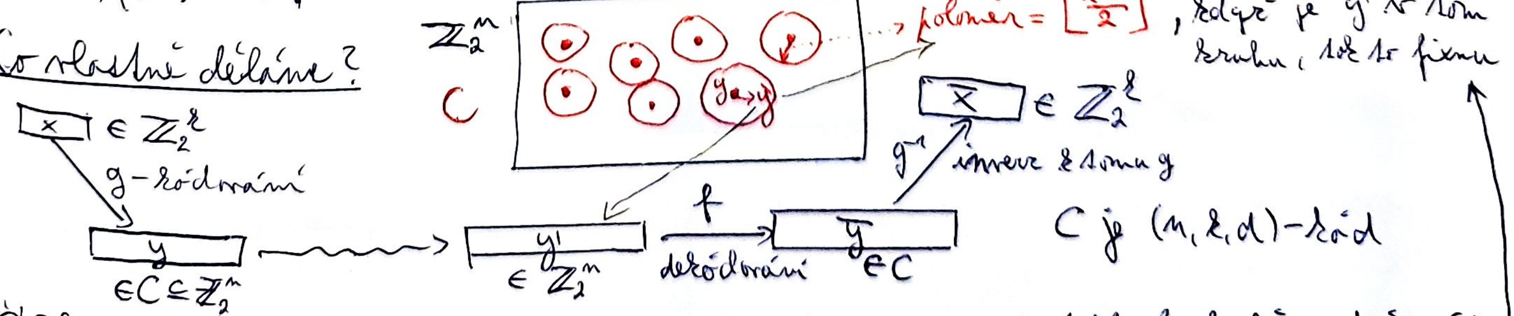
→ něco jako ortogonální doplněk

Fakt: Pokud $C \subseteq \mathbb{Z}_2^n$ je podprostor dimenze k, potom $C^\perp$ je taky v.p. a

1) $\dim(C^\perp) = n - k$,
2) $(C^\perp)^\perp = C$,

} chová se to jako ortogonální doplněk

• **Co vlastně děláme?**



👁 Pokud se při přenosu změní nejvýš $d-1$ bitů, tak poznáme, že došlo k chybě ... d je $\Delta(C)$

👁 Pokud se při přenosu změní nejvýš $\lfloor \frac{d-1}{2} \rfloor$ bitů, tak dokážu chybu jednoznačně opravit.

- Jak dělat to dekódování?

Def: Nechť C je lineární (n,k,d)-kód. Kontrolní matice kódu C je matice, jejíž řádky tvoří bázi $C^\perp$.

👁 Kontrolní matice (n,k,d)-kódu má $n-k$ řádků a n sloupců

Příklad:

$C_1 = \{000, 111\}$ … lineární $(3,1,3)$-kód.

$\Rightarrow \dim(C_1^\perp) = 2 \Rightarrow |C_1^\perp| = 4 \Rightarrow C_1^\perp = \{000, 110, 101, 011\}$

$\Rightarrow C_1$ má kontrolní matici například $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$

Tvrzení: Nechť C je lin. (n,k,d)-kód s k. maticí K.
Potom $\forall x \in \mathbb{Z}_2^n : x \in C \iff Kx^T = \sigma$ → tohle je jenom nějaká soustava $n-k$ lin. rovnic s n neznámými ⇒ řešení je k-dim podprostor

Příklad: $x = (x_1, x_2, x_3) \in \mathbb{Z}_2^3 : x \in C_1 \iff \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \sigma$

$$\iff \left.\begin{array}{l} x_1 \oplus x_2 = 0 \Rightarrow x_1 = x_2 \\ x_1 \oplus x_3 = 0 \Rightarrow x_1 = x_3 \end{array}\right\} x = 111 \vee 000 \checkmark$$

Dk: Nechť $r_1, r_2, \dots r_{n-k} \in \mathbb{Z}_2^n$ jsou řádky K.
Potom $x \in C \iff x \in (C^\perp)^\perp \iff \forall y \in C^\perp : \langle x, y \rangle = 0 \iff \forall i : \langle x, r_i \rangle = 0$ (báze $C^\perp$ jsou r_i řádky K)
$\iff Kx^T = 0.$ ∎

→ kontrolní matice umožňuje snadno kontrolovat, jestli je něco prvek kódu

👁 Nechť C je lin. (n,k,d)-kód s k. maticí K.
Víme $d = \Delta(C) = \min\limits_{x \in C \setminus \sigma} \|x\|$

👁 Navíc $\Delta(C)$ = nejmenší $s \geq 1$ t.ž. v K lze najít s sloupečků jejichž součet je 0.

Dk: $\Delta(C)$ = min. z počtů jedniček v $x \in C \setminus \sigma$
součet s sloupečků v K je $0 \iff Kx^T = 0$, kde x obsahuje s jedniček } min je stejná věc ∎

Důsledek: $\Delta(C) \geq 2 \iff K$ má všechny sloupce nenulové
$\Delta(C) \geq 3 \iff K$ ——— " ——— a navíc $\forall$ dva sloupce různé

↳ takové kódy nás budou zajímat
∵ tam můžeme opravovat chyby

Def: Nechť $r \in \mathbb{N}$, $r \geq 2$. Potom K_r je matice s r řádky a $2^r - 1$ sloupci … $K_r \in \mathbb{Z}_2^{r \times 2^r - 1}$, kde všechny sloupce jsou různé a nenulové.

→ takže sloupce K_r jsou všechny r-bitové řetězce, kromě samých nul

$K_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$ 👁 řádky K_r jsou lin. nezávislé ∵ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ je l. nez.

• Hammingovy kódy

Def: Hamingovy kódy jsou kódy H_r s kontrolní maticí K_r.

👁 H_r je lin. (n,k,d) - kód, kde

$n = 2^r - 1$, $k = n - r = 2^r - r - 1$, $d = 3$ ... víme $d \geq 3$

navíc vždy při lexikografickém usp. sloupečků se první tři z nich sečtou na nulu

$$\begin{pmatrix}1\\0\\0\\0\\\vdots\\0\end{pmatrix} + \begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix} + \begin{pmatrix}1\\0\\0\\\vdots\\0\end{pmatrix} = \begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix} \Rightarrow (11100\ldots0) \in H_r$$

je možné opravit 1 chybu

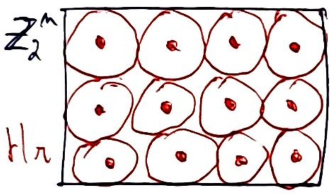
→ pro $r=8$: 255 b., 247 užitečných b.

Tvrzení: $\forall r \geq 2$, $n = 2^{r-1}$: $\forall x \in \mathbb{Z}_2^n$ existuje právě jedno $y \in H_r$ t.ž. $d(x,y) \leq 1$.

Dk: Tohle říká, že když dostanu nějaký potenciálně zkomolený vektor $x \in \mathbb{Z}_2^n$, tak umím vždy najít nějaký y z toho H_r ve vzdálenosti 0 nebo 1.

1) ∃ nejvýš 1 ∵ $\left\lfloor \frac{3-1}{2} \right\rfloor = 1$, takže ty dva kruhy jsou vždy disjunktní

2) ∃ alespoň 1



→ kruhy o poloměru 1 kolem toho H_r dělají určitý rozklad $\mathbb{Z}_2^n$ na nějaké disjunktní množiny

→ vlastně perfektně vydlaždičkují $\mathbb{Z}_2^n$

→ to že ∃ nejvýš 1 je jasné, zajímavé je, že ∃ alespoň 1

Tohle $y \in H_r$ lze najít takto:

1. spočítej $s \leftarrow K_r x^T$
2. Pokud $s = o$, tak $x \in H_r$, takže $y = x$
3. Pokud $s \neq o$, tak $i \leftarrow$ takové i, že i-tý sloupec K_r je roven s.

   Potom $y \leftarrow$ vektor, který vznikne z x změnou i-tého bitu

→ proč to funguje? $x = (1000101)$

$$K_3 x^T = \begin{pmatrix}1\\0\\0\end{pmatrix} \oplus \begin{pmatrix}1\\0\\1\end{pmatrix} \oplus \begin{pmatrix}1\\1\\1\end{pmatrix} = \begin{pmatrix}1\\1\\0\end{pmatrix} \Rightarrow \text{takže } y \leftarrow (1010101)$$

$$K_3 y^T = \begin{pmatrix}1\\0\\0\end{pmatrix} \oplus \begin{pmatrix}1\\0\\1\end{pmatrix} \oplus \begin{pmatrix}1\\1\\1\end{pmatrix} \oplus \begin{pmatrix}1\\1\\0\end{pmatrix} = \begin{pmatrix}1\\1\\0\end{pmatrix} + \begin{pmatrix}1\\1\\0\end{pmatrix} = o$$

∎

⇒ pokud se zkomolí 1 bit, tak to umíme snadno opravit

⇒ pokud se zkomolí 2 bity, tak umíme poznat, že nastala chyba, ale to opravení už nebude fungovat.

↳ tohle stejné dělal ten kód 3-kopií, ale tam na 1 užitečný bit 2 navíc, tady z celkem $2^r - 1$ bitů je pouze r kontrolních

↳ pro n bitů cca $\log(n)$ kontrolních.

Tvrzení (Singletonův odhad): Pokud existuje (n,k,d)-kód, tak $k+d \leq n+1$.

→ nemůžu mít kód, který má hodně užitečné informace a současně hodně velké d a malé n.

Dk: Definujme zobrazení $f: \mathbb{Z}_2^n \to \mathbb{Z}_2^{n-d+1}$, $(x_1, x_2, \dots x_n) \mapsto (x_1, \dots x_{n-d+1})$. ← useknu posledních $d-1$

Protože min. vzdálenost je d, tak $\forall x,y \in C: x \neq y \Rightarrow f(x) \neq f(y)$,

tedy f je prostá. Proto $|C| \leq |\mathbb{Z}_2^{n-d+1}| \Rightarrow 2^k \leq 2^{n-d+1} \Rightarrow k+d \leq n+1$ ∎

Značení:

- koule o poloměru t: $B(x,t) := \{ y \in \mathbb{Z}_2^n \mid d(x,y) \leq t \}$
- objem té koule: $V(x,t) := |B(x,t)| = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{t}$

↳ kolik bitů jim změním

Tvrzení (Hammingův odhad): Pokud $\exists$ (n,k,d)-kód C, tak

$$2^k = |C| \leq \frac{2^n}{V(\lfloor \frac{d-1}{2} \rfloor)}$$

Dk: Když $x,y \in C$, $x \neq y$, tak $B(x, \lfloor \frac{d-1}{2} \rfloor) \cap B(y, \lfloor \frac{d-1}{2} \rfloor) = \emptyset$.

→ koule o tomhle poloměru jsou disjunktní

⇒ v $\mathbb{Z}_2^n$ je 2^n prvků ⇑
v těch koulích je celkem $|C| \cdot V(\lfloor \frac{d-1}{2} \rfloor)$ prvků } v těch koulích toho určitě není víc než celkem ∎

↓ # koulí ↓ objem 1 koule

Tvrzení (Gilbert-Varshamovův odhad): $\forall n,d \in \mathbb{N}$, $d<n$ existuje kód C, takový, že $|C| \geq \dfrac{2^n}{V(d-1)}$

Dk: Hledejme C hladově. Vybereme nějaký vektor $x_0 \in \mathbb{Z}_2^n$, takže všechny vektory ve vzdálenosti $\leq d-1$ už vybrat nemůžeme. Těch je $V(d-1)$.

Tohle opakujeme, dokud v $\mathbb{Z}_2^n$ ještě je nějaký použitelný vektor, přičemž vždy vylončíme nejvýše $V(d-1)$ vektorů.

→ vektorů celkem v $\mathbb{Z}_2^n$ je 2^n

→ my jsme $|C|$-krát vylončili nejvýše $V(d-1)$ ⇒ $|C| \cdot V(d-1) \geq 2^n$ ∎

Důsledek: Pro každý (n,k,d)-kód C platí

$$\frac{2^n}{V(d-1)} \leq 2^k \leq \frac{2^n}{V(\lfloor \frac{d-1}{2} \rfloor)}.$$