Kombinatorika a grafy I.

Písemná zkouška, případně ústní dozkoušení.
Prakticky umět využít věty a důkazy.

Odhady na důležité funkce
Motivační otázka
Čeho je více, grafů na n vrcholech, nebo permutací na n prvcích?

Grafů je $2^{\binom{n}{2}}$, počet permutací $\{1, \dots, n\}$ je $n!$

Odhady na $n!$

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

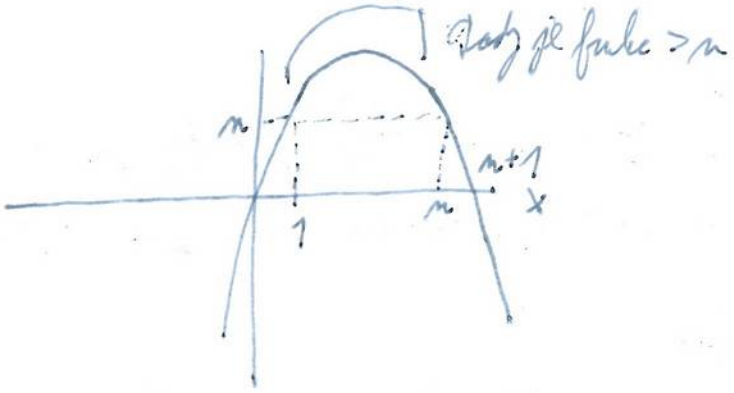
Důkaz: $n! = \prod_{i=1}^{n} i \leq \prod_{i=1}^{n} n = n^n$

Druhý odhad je malinko těžší:

$$(n!)^2 = (1 \cdot 2 \cdot 3 \cdot \dots \cdot n) \cdot (1 \cdot 2 \cdot 3 \cdot \dots \cdot n) =$$
$$= (1 \cdot n) \cdot (2 \cdot (n-1)) \cdot (3 \cdot (n-2)) \cdot \dots \cdot (n \cdot 1)$$
$$= \prod_{i=1}^{n} i \cdot (n - i + 1)$$

Tvrdím, že $\forall i \in \{1, \dots, n\} \quad i \cdot (n - i + 1) \geq n$

$i \cdot (n - i + 1) = -i^2 + (n+1) \cdot i$



$$(n!)^2 = \prod_{i=1}^{n} i\cdot(n-i+1) \geq \prod_{i=1}^{n} n = n^n$$

odmocníme

$$n! \geq n^{n/2}$$

$$2^{\binom{n}{2}} = 2^{\frac{n\cdot(n-1)}{2}} = 2^{\frac{n^2}{2}-\frac{n}{2}}$$

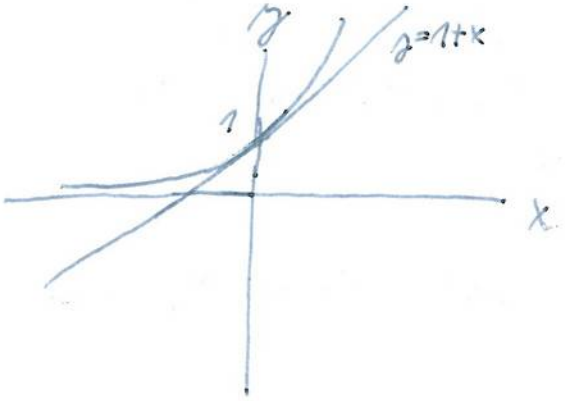
$$n^n = \left(2^{\log_2 n}\right)^n = 2^{n\cdot\log_2 n}$$
$$n^{n/2} = 2^{\frac{n}{2}\log_2 n}$$

Počet grafů je větší než počet permutací.

Věta: $\forall n \in \mathbb{N}: \quad \left(\frac{n}{e}\right)^n \leq n! \leq en\cdot\left(\frac{n}{e}\right)^n$

Důkaz: využijeme následující fakty

1) $e^x = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \ldots = \sum_{j=0}^{\infty} \frac{x^j}{j!}$
2) $e^x \geq 1 + x$



Dolní odhad

$e^x = 1 + x + \frac{x^2}{2} + \ldots \geq \frac{x^n}{n!}$, tedy $n! \geq \frac{x^n}{e^x}$

Zvolíme za $x := n$, potom $n! \geq \frac{n^n}{e^n} = \left(\frac{n}{e}\right)^n$.

Horní odhad

Dokážeme $n! \leq en\cdot\left(\frac{n}{e}\right)^n$ indukcí dle n:

$n=1 \quad n! = 1, \quad e \cdot 1 \cdot \left(\frac{1}{e}\right) = 1$ ✓

Předpokládejme $n! \le e \cdot n \left(\frac{n}{e}\right)^n$

Chceme $(n+1)! \le e \cdot (n+1) \cdot \left(\frac{n+1}{e}\right)^{n+1}$

$$(n+1)! = (n+1) \cdot n! \le (n+1) \cdot e n \cdot \left(\frac{n}{e}\right)^n = \underbrace{e \cdot (n+1) \cdot \frac{\left(\frac{n+1}{e}\right)^{n+1}}{\left(\frac{n+1}{e}\right)^{n+1}} \cdot n \left(\frac{n}{e}\right)^n}$$

$$= e(n+1) \cdot \left(\frac{n+1}{e}\right)^{n+1} \cdot \frac{n \cdot \left(\frac{n}{e}\right)^n}{\left(\frac{n+1}{e}\right)^{n+1}} = e \cdot (n+1) \cdot \left(\frac{n+1}{e}\right)^{n+1} \cdot \frac{n^{n+1} \cdot e}{(n+1)^{n+1}}$$

$$= e \cdot (n+1) \cdot \left(\frac{n+1}{e}\right)^{n+1} \cdot \left(\frac{n}{n+1}\right)^{n+1} \cdot e = e \cdot (n+1) \cdot \left(\frac{n+1}{e}\right)^{n+1} \cdot \underbrace{\left(1 - \frac{1}{n+1}\right)^{n+1}} \cdot e$$

$$\le e \cdot (n+1) \cdot \left(\frac{n+1}{e}\right)^{n+1} \qquad e^{-\frac{1}{n}} < 1$$

Stirlingova formule

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

Odhady na binomický koeficient pro $k, n \in \mathbb{N}_0 \quad 0 \le k \le n$

Připomenutí:

1) $\binom{n}{k}$ je počet k-prvkových podmnožin $\{1, \dots, n\}$
2) $\binom{n}{k} = \frac{n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-k+1)}{k!} = \frac{n!}{(n-k)! \cdot k!}$
3) $\binom{n}{k} = \binom{n}{n-k}$
4) $\binom{n}{0} = 1 \le \binom{n}{1} \le \binom{n}{2} \le \dots \le \binom{n}{\lfloor \frac{n}{2} \rfloor} = \binom{n}{\lceil \frac{n}{2} \rceil} \ge \binom{n}{n-1} \ge \binom{n}{n} = 1$
5) $\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} = 2^n$

Tvrzení: Pro $1 \le k \le n$: $\left(\frac{n}{k}\right)^k \le \binom{n}{k} \le \left(\frac{en}{k}\right)^k$

Důkaz: $\binom{n}{k} = \frac{n \cdot (n-1) \cdot \dots \cdot (n-k+1)}{k!} = \frac{n}{k} \cdot \frac{n-1}{k-1} \cdot \dots \cdot \frac{n-k+1}{1}$

stačí: $\frac{n}{k} \le \frac{n-1}{k-1} \le \frac{n-2}{k-2} \le \dots \le \frac{n-k+1}{1}$

Tedy $\binom{n}{k} \ge \left(\frac{n}{k}\right)^k$

$$\binom{n}{k} = \frac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{k!} \le \frac{n^k}{\left(\frac{k}{e}\right)^k} = \left(\frac{en}{k}\right)^k$$

Věta: Pro $1 \le k \le n$ platí $\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{k} \le \left(\frac{en}{k}\right)^k$

Důkaz: Předpokládejme $x \in (0,1]$.

Víme, že $e^x \ge 1+x$

Tedy $e^{nx} \ge (1+x)^n = \sum_{j=0}^{n}\binom{n}{j}\cdot x^j = \binom{n}{0}+\binom{n}{1}x+\binom{n}{2}x^2+\ldots+\binom{n}{n}\cdot x^n$

$\ge \binom{n}{0}+\binom{n}{1}x+\cdots+\binom{n}{k}x^k$

$\ge \binom{n}{0}\cdot x^k+\binom{n}{1}x^k+\ldots+\binom{n}{k}x^k$

Tedy $\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{k} \le \frac{e^{nx}}{x^k}$

dosadím $x=\frac{k}{n}$: $\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{k} \le \frac{e^{n\cdot\frac{k}{n}}}{\left(\frac{k}{n}\right)^k} = \left(\frac{en}{k}\right)^k$.

Odhady pro kombinační číslo $\binom{2n}{n}$, $n \in \mathbb{N}$

Tvrzení: $\frac{2^{2n}}{2n+1} \le \binom{2n}{n} \le 2^{2n}$

Důkaz: $\binom{2n}{0}+\binom{2n}{1}+\binom{2n}{2}+\ldots+\binom{2n}{2n} = 2^{2n}$

tj: $\binom{2n}{n} \le 2^{2n}$

$2^{2n} \le (2n+1)\cdot\binom{2n}{n}$

$\frac{2^{2n}}{(2n+1)} \le \binom{2n}{n}$

$$\binom{2n}{0}+\binom{2n}{1}+\ldots+\binom{2n}{2n} = \sum_{j=0}^{2n}\binom{2n}{j} = (2n+1)\cdot\binom{2n}{n}$$

Věta: $\forall n \in \mathbb{N}: \frac{2^{2n}}{2\sqrt{n}} \le \binom{2n}{n} \le \frac{2^{2n}}{\sqrt{2n}}$

Důkaz: Definujeme výraz $P(n) := \frac{\binom{2n}{n}}{2^{2n}} = \frac{(2n)!}{n!\,n!\,2^{2n}}$

$$= \frac{\prod_{j=1}^{2n} j}{\left(\prod_{j=1}^{n} j\right)\cdot\left(\prod_{j=1}^{n} j\right)\left(\prod_{j=1}^{2n} 2\right)} = \frac{\prod_{j=1}^{2n} j}{\left(\prod_{j=1}^{n} 2j\right)\cdot\left(\prod_{j=1}^{n} 2j\right)} = \frac{1\cdot3\cdot5\cdots(2n-1)}{2\cdot4\cdot6\cdot8\cdots\cdot2n}$$

$$P^2(n) = \frac{1\cdot3\cdot3\cdot5\cdot5\cdot7\cdot7\cdot\ldots\cdot(2n-1)\cdot(2n-1)}{2\cdot2\cdot4\cdot4\cdot\ldots\cdot(2n)\cdot(2n)}$$

Všimněme si: pro $j \geq 2$ $\quad \frac{j \cdot j}{(j-1)\cdot(j+1)} = \frac{j^2}{j^2-1} > 1$ a

$$\frac{(j-1)\cdot(j+1)}{j \cdot j} < 1$$

$$P^2(n) = \frac{1\cdot 1}{2} \cdot \underbrace{\frac{3\cdot 3}{2\cdot 4}}_{>1} \cdot \underbrace{\frac{5\cdot 5}{4\cdot 6}}_{>1} \cdot \underbrace{\frac{7\cdot 7}{6\cdot 8}}_{>1} \cdot \ldots \cdot \underbrace{\frac{(2n-1)\cdot(2n-1)}{(2n-2)\cdot(2n)}}_{>1} \cdot \frac{1}{(2n)} > \frac{1}{4n}$$

tj. $P(n) \geq \frac{1}{2\sqrt{n}}$

$$P^2(n) = 1 \cdot \underbrace{\frac{1\cdot 3}{2\cdot 2}}_{<1} \cdot \underbrace{\frac{3\cdot 5}{4\cdot 4}}_{<1} \cdot \underbrace{\frac{5\cdot 7}{6\cdot 6}}_{<1} \cdot \ldots \cdot \underbrace{\frac{(2n-3)\cdot(2n-1)}{(2n-2)\cdot(2n-2)}}_{<1} \cdot \underbrace{\frac{2n-1}{(2n)\cdot(2n)}}_{<1} <$$

$$< \frac{2n-1}{(2n)(2n)} < \frac{1}{2n}$$

nejlepší z členů

tj. $P(n) \leq \frac{1}{\sqrt{2n}}$

2. přednáška

Vytvořující funkce

Motivační příklad: P pětikorun, D dvoukorun a K korun.
$a_n :=$ počet způsobů jak zaplatit n Kč.

$a_5 = 4$ (5), (2)(2)(1), (2)(1)(1)(1), (1)(1)(1)(1)(1)
(pokud $P \geq 1, D \geq 2, K \geq 5$)

$M := 5P + 2D + K$ (kolik nejvíce můžeme zaplatit)

Definujme polynom $P(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = \sum_{n=0}^{M} a_n x^n$

Pozorování: $P(x) = \underbrace{(1 + x^5 + x^{10} + \ldots + x^{5P})}_{x^0} \cdot \underbrace{(1 + x^2 + x^4 + \ldots + x^{2D})}_{x^0} \cdot \underbrace{(1 + x + x^2 + \ldots + x^K)}_{x^0}$

$$= \underbrace{x^0 \cdot x^0 \cdot x^0}_{x^0} + \underbrace{x^0 \cdot x^0 \cdot x^1}_{x^1} + \underbrace{x^0 \cdot x^2 \cdot x^0}_{x^2} + \underbrace{x^0 \cdot x^0 \cdot x^2}_{x^2} + \dots$$

$$+ \underbrace{x^5 \cdot x^0 \cdot x^0 + x^0 x^4 \cdot x^1 + x^0 \cdot x^2 \cdot x^3 + x^0 \cdot x^0 \cdot x^5}_{\boxed{4} \cdot x^5}$$

4 způsoby jak zaplatit 5 kč

$$= a_0 x^0 + a_1 \cdot x^1 + \dots + a_n x^n + \dots + a_M x^M$$

$$P(x) = \frac{1 - x^{5 \cdot (P+1)}}{1 - x^5} \cdot \frac{1 - x^{2 \cdot (D+1)}}{1 - x^2} \cdot \frac{1 - x^{K+1}}{1 - x}$$ (součty geometrické řady)

<u>Def</u>: (Vytvořující funkce pro posloupnost $a_0, a_1, \dots$) je funkce $f(x) := \sum_{n=0}^{\infty} a_n \cdot x^n$

Značení: $[x^n] f(x)$ … „koeficient u x^n v mocninné řadě pro $f(x)$" tj. $[x^n] f(x) = a_n$.

<u>Fakty</u>: 1) Pokud $a_0, a_1, \dots$ je posloupnost splňující, že $|a_n| < c^n$ pro každé dostatečně velké n, tak potom $f(x) = \sum_{n=0}^{\infty} a_n x^n$ konverguje pro každé $x \in (-\frac{1}{c}, \frac{1}{c})$. Navíc funkce f má v 0 derivace všech řádů, dá se derivovat „člen po členu".

$$f'(x) = \sum_{n=0}^{\infty} n \cdot a_n x^{n-1}$$

$$f''(x) = \sum_{n=0}^{\infty} n \cdot (n-1) \cdot a_n x^{n-2}$$ (žádné záporné členy tam nejsou (díky n a $n-1$))

$$f^{(k)}(x) = \sum_{n=0}^{\infty} n \cdot (n-1) \cdots (n-k+1) \cdot a_n \cdot x^{n-k}$$

Tudíž $a_0 = f(0)$, $f'(0) = a_1$, $f''(0) = 2 \cdot a_2$, …, $f^{(k)}(0) = k!\, a_k$.

2) Nechť $f(x) = \sum_{n=0}^{\infty} a_n x^n$ je vytvořující funkce pro $a_0, a_1, a_2, \dots$
Nechť $g(x) = \sum_{n=0}^{\infty} b_n x^n$ je vytvořující funkce $b_0, b_1, \dots$

Potom $f(x) \cdot g(x)$ je vytvořující funkce pro $a_0 b_0, a_0 b_1 + a_1 + b_0,$
$a_2 b_0 + a_1 b_1 + a_0 b_2, \dots,$
$a_1 b_0 + a_{n-1} \cdot b_1 + \dots + a_0 b_n$

$$f(x) \cdot g(x) = \left(\sum_{n=0}^{\infty} a_n x^n \right) \cdot \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{\infty} a_k \cdot b_{n-k} \right) x^n$$

$[x^n] f(x) \cdot g(x)$

Příklady: $1, 1, 1, \dots$ má vytvořující funkci $1 + x + x^2 + \dots = \frac{1}{1-x}$
$3, 3, 3, \dots$ má vytvořující funkci $3 + 3x + 3x^2 + \dots = 3(1 + x + x^2 + \dots)$ $\frac{3}{1-x}$

$\frac{1}{1-3x}$ (za x jsem dosadil $3x$) $1 + (3x)^2 + (3x)^3 + \dots 3^n x^n$
posloupnost $1, 3, 3^2, 3^3, \dots, 3^n$

Def: (Zobecněný binomický koeficient)
Pro $r \in \mathbb{R}$ a $k \in \mathbb{N}$ definujeme zobecněný bin. koeficient $\binom{r}{k}$, je definován takto:

$$\binom{r}{k} = \frac{r \cdot (r-1) \cdot \dots \cdot (r-k+1)}{k!}$$

(Speciálně $\binom{r}{0} = 1$ pro $\forall x \in \mathbb{R}$) součin dělky 0 se definuje jako 1.

Tvrzení: (Zobecněná binomická věta)
Pro $\forall r \in \mathbb{R}$ je $(1+x)^r$ vytvořující funkce pro posloupnost $\binom{r}{0}, \binom{r}{1}, \binom{r}{2}, \dots$, t.j. $(1+x)^r = \sum_{n=0}^{\infty} \binom{r}{n} \cdot x^n$

Poznámka: Ta řada konverguje pro $\forall x \in (-1, 1)$

Částečný důkaz: definujme $f(x) := (1+x)^r$

k-tá derivace $f(x)$: $f^{(k)}(x) = \alpha\cdot(\alpha-1)\cdot(\alpha-2)\cdot\ldots\cdot(\alpha-k+1)\cdot(1+x)^{\alpha-k}$

$f(x)$ je vytvořující funkce pro $f(0)$, $f'(0)$, $\frac{f''(0)}{2}$, $\ldots$, $\frac{f^{(n)}(0)}{n!}$, $\ldots$

kde $\frac{f^{(n)}(0)}{n!} = \frac{\alpha\cdot(\alpha-1)\cdot(\alpha-2)\cdot\ldots\cdot(\alpha-k+1)}{n!} = \binom{\alpha}{n}$

Příklad: Mějme $m \in \mathbb{N}$, která posloupnost má vytvořující funkci: $f(x) = \frac{1}{(1-x)^m}$

$$\frac{1}{(1-x)^m} = (1-x)^{-m} = (1+(-x))^{-m} \overset{\text{ZBV}}{=} \sum_{n=0}^{\infty} (-x)^n \binom{-m}{n} = \sum_{n=0}^{\infty} \underbrace{(-1)^n \cdot \binom{-m}{n}}_{x^n}$$

Navíc $(-1)^n \cdot \binom{-m}{n} = \frac{(-1)^n\cdot(-m)\cdot(-m-1)\cdot(-m-2)\cdot\ldots\cdot(-m-n+1)}{n!}$

$= \frac{m\cdot(m+1)\cdot(m+2)\cdot\ldots\cdot(m+n-1)}{n!} = \binom{m+n-1}{n} = \binom{m+n-1}{m-1}$

$\frac{1}{(1-x)^m}$ je vytvořující posloupnost pro $\binom{m-1}{m-1}, \binom{m}{m-1}, \binom{m+1}{m-1}, \ldots, \binom{m+n-1}{m-1}, \ldots$

Příklad: Fibonaccího čísla: $F_0 = 0$

$F_1 = 1$

$F_n = F_{n-1} + F_{n-2} \quad \forall n \geq 2$

Není na první pohled vidět explicitní vzorec.

Definujme vytvořující funkci pro fibonaccího čísla.

$f(x) = \sum_{n=0}^{\infty} F_n x^n$. Cíl vzít pro $f(x)$.

$F_n = F_{n-1} + F_{n-2} \quad \underline{\forall n \geq 2}$

$F_n x^n = F_{n-1} x^n + F_{n-2} x^n \quad \underline{\forall n \geq 2}$

$$\underbrace{\sum_{n=2}^{\infty} F_n x^n}_{S_1} = \underbrace{\left(\sum_{n=2}^{\infty} F_{n-1} x^n\right)}_{S_2} + \underbrace{\left(\sum_{n=2}^{\infty} F_{n-2} x^n\right)}_{S_3}$$

$f(x) = F_0 x^0 + F_1 x^1 + F_2 x^2 + \ldots +$

$S_1 = F_2 x^2 + F_3 x^3 + F_4 x^4 + \ldots = f(x) - F_0 x^0 - F_1 x^1 = f(x) - x$

$$S_2 = F_1x^2 + F_2x^3 + F_3x^4 + \dots = x\cdot(F_1x + F_2x^2 + F_3x^3 + \dots)$$
$$= x\cdot(f(x) - \underbrace{F_0x^0}_{0}) = x\cdot f(x)$$

$$S_3 = F_0x^2 + F_1x^3 + F_2x^4 + \dots = x^2\cdot(F_0x^0 + F_1x^1 + F_2x^2 + \dots) = x^2 f(x)$$

$$f(x) - x = S_1 = x\cdot f(x) + x^2 f(x)$$
$$f(x) - xf(x) - x^2 f(x) = x$$
$$f(x)(1 - x - x^2) = x$$
$$f(x) = \frac{x}{1 - x - x^2}$$

Mějme posloupnost splňující: $a_n = \alpha\cdot a_{n-1} + \beta a_{n-2} + \gamma a_{n-3} + \delta$ pro $n \geq 3$

$a_0, a_1, a_2, \alpha, \beta, \gamma, \delta$ jsou nějaké konstanty.

Cíl: vzorec pro $f(x) = \sum_{n=0}^{\infty} a_n x^n$

$a_n = \alpha\cdot a_{n-1} + \beta\cdot a_{n-2} + \gamma\cdot a_{n-3} + \delta_\infty \quad (n \geq 3)$

$$\sum_{n=3}^{\infty} a_n x^n = \sum_{n=3}^{\infty} \alpha a_{n-1}x^n + \sum_{n=3}^{\infty} \beta a_{n-2}x^n + \sum_{n=3}^{\infty} \gamma a_{n-3}x^n + \sum_{n=3}^{\infty} \delta x^n$$

$$f(x) - (a_0 + a_1x + a_2x^2) = x\alpha\left(f(x) - (a_0 + a_1x)\right) + x^2\beta\cdot(f(x) - a_0)$$
$$+ x^3\gamma f(x) + \delta\cdot\left(\frac{1}{1-x} - (1 + x + x^2)\right)$$
$$f(x)\cdot(1 - \alpha x - \beta x^2 - \gamma x^3) = \delta\left(\frac{1}{1-x} - (1 + x + x^2)\right) + \text{nějaký polynom}(x)$$

2. přednáška

Připomenutí:

$$\frac{1}{1-x} = 1 + x + x^2 + \dots$$
$$\frac{a}{b - cx} = \frac{a}{b}\cdot\frac{1}{1 - \frac{c}{b}x} = \frac{a}{b}\cdot\left(1 + \frac{c}{b}x + \left(\frac{c}{b}\right)^2 x^2 + \dots\right)$$
$$\frac{1}{(1-x)^m} = \sum_{n=0}^{\infty}\binom{n+m-1}{m-1}x^n$$

Def: Racionální funkce je funkce tvaru $\frac{P(x)}{Q(x)}$, kde $P(x)$ a $Q(x)$ jsou polynomy.

Fakt: (Rozklad na parciální zlomky nad $\mathbb{C}$)
Nechť $f(x) = \frac{P(x)}{Q(x)}$, kde $P(x)$ a $Q(x)$ jsou polynomy (nad $\mathbb{C}$) a stupeň P je menší než stupeň Q.
Nechť $Q(x)$ má tvar $Q(x) = \beta (x-\rho_1)^{n_1} \cdot (x-\rho_2)^{n_2} \cdot \ldots \cdot (x-\rho_k)^{n_k}$, kde $\rho_1, \ldots \rho_k$ jsou navzájem různé kořeny $Q(x)$ a n_i je násobnost ρ_i ($\rho_1, \ldots \rho_k \in \mathbb{C}$, $n_1, \ldots, n_k \in \mathbb{N}$).
Potom $f(x) = \sum_{\substack{1 \le i \le k \\ 1 \le j \le n_i}} \frac{\alpha_{i,j}}{(x-\rho_i)^j}$, kde $\alpha_{i,j} \in \mathbb{C}$ jsou konstanty.

Navíc pokud $P(x)$ i $Q(x)$ mají reálné koeficienty a i všechny kořeny $\rho_1, \ldots, \rho_k$ jsou reálné, tak potom i všechny konstanty $\alpha_{i,j}$ jsou reálné.

Poznámka: Někdy je praktičtější hledat parciální zlomky ve tvaru $\frac{\alpha_{i,j}}{(1-\frac{x}{\rho_i})^j}$ a je s jednotkou, nejedná se o to samé α jako výše

Příklad: Fibonacciho čísla. $F_0 = 0$
$F_1 = 1$
$F_n = F_{n-1} + F_{n-2} \quad \forall n \ge 2$

$f(x) = \sum_{n=0}^{\infty} F_n \cdot x^n = \frac{x}{1-x-x^2}$ (vytvořující funkce pro Fibonaccihi čísla)

$1-x-x^2$ má kořeny $\rho_1 = \frac{1-\sqrt{1+4}}{-2} = \frac{\sqrt{5}-1}{2}$
$\rho_2 = \frac{-\sqrt{5}-1}{2}$

$f(x) = \frac{\alpha_1}{1-\frac{x}{\rho_1}} + \frac{\alpha_2}{1-\frac{x}{\rho_2}}$

$\frac{\alpha_1}{1-\frac{x}{\rho_1}} = \alpha_1 \cdot \left(1 + \frac{x}{\rho_1} + \left(\frac{x}{\rho_2}\right)^2 + \left(\frac{x}{\rho_3}\right)^3 + \ldots\right)$

$\frac{\alpha_2}{1-\frac{x}{\rho_2}} = \alpha_2 \cdot \left(1 + \frac{x}{\rho_2} + \left(\frac{x}{\rho_2}\right)^2 + \left(\frac{x}{\rho_2}\right)^3 + \ldots\right)$

$F_n = \alpha_1 \cdot \frac{1}{\rho_1^n} + \alpha_2 \cdot \frac{1}{\rho_2^n}$

Výpočet α_1 a α_2 (protože dosadím, tak aby to vyšlo)

$0 = F_0 = \alpha_1 \cdot \frac{1}{\rho_1^0} + \alpha_2 \cdot \frac{1}{\rho_2^0} = \alpha_1 + \alpha_2$

$1 = F_1 = \alpha_1 \cdot \frac{1}{\rho_1^1} + \alpha_2 \cdot \frac{1}{\rho_2^1} = \alpha_1 \cdot \left(\frac{1}{\rho_1} - \frac{1}{\rho_2}\right)$

$$\Longrightarrow \alpha_1 = \frac{1}{\frac{1}{\rho_1} - \frac{1}{\rho_2}} = -\alpha_2$$

Příklad: Nechť C_n je počet binárních zakořeněných stromů o n vnitřních vrcholy (stromy lišící se přiřazením podstromů u vrcholu jsou různé)

$C_0 = 1$ (•)
$C_1 = 1$ ()
$C_2 = 2$ ( , )
$C_3 = 5$ ( ,  ,  ,  , )

C_n se nazývají Catalanova čísla.

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

Cíl: vzorec pro $C(x)$ a pro C_n.

Pro $n \geq 1$ platí

$$C_n = C_0 \cdot C_{n-1} + C_1 \cdot C_{n-2} + C_2 \cdot C_{n-3} + \dots + C_{n-1} \cdot C_0 = \sum_{j=0}^{n-1} C_j \cdot C_{n-j-1}$$

$C_0 \cdot C_{n-1}$
$\| $
1

$C_1 \cdot C_{n-2}$

$C_j \cdot C_{n-j-1}$

pro $n \geq 1$:

$$C_n x^n = x^n \cdot (C_0 \cdot C_{n-1} + C_1 \cdot C_{n-2} + \dots + C_{n-1} \cdot C_0)$$

$$\sum_{n=1}^{\infty} C_n x^n = \sum_{n=1}^{\infty} x^n \cdot (C_0 \cdot C_{n-1} + \dots + C_{n-1} C_0)$$

$$C(x) - 1 = x \cdot \sum_{n=1}^{\infty} x^{n-1} (C_0 \cdot C_{n-1} + \dots + C_{n-1} C_0)$$

$$C(x) - 1 = x \cdot C^2(x) \quad \leftarrow \text{(kvadratická rovnice)} \Rightarrow x \cdot C^2(x) - C(x) + 1 = 0$$

$$C^2(x) = \left(\sum_{n=0}^{\infty} C_n \cdot x^n\right) \cdot \left(\sum_{n=0}^{\infty} C_n \cdot x^n\right) = \sum_{n=0}^{\infty} x^n \cdot (C_0 \cdot C_n + C_1 \cdot C_{n-1} + \dots + C_n \cdot C_0)$$

Pro $x \neq 0$!

Buď $C(x) = \frac{1+\sqrt{1-4x}}{2x}$

nebo $C(x) = \frac{1-\sqrt{1-4x}}{2x}$

$\frac{1+\sqrt{1-4x}}{2x}$ nelze spojitě dodefinovat pro $x=0 \Longrightarrow$ není to vytvořující funkce

$C(x) = \frac{1-\sqrt{1-4x}}{2x}$ je vytvořující funkce pro Catalanova čísla.

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

(Toby nám nepomůže rozklad na parciální zlomky, nejedná se o racionální funkci)

$= \frac{1}{2}[x^{n+1}] \cdot (1 - \sqrt{1-4x}) = \frac{1}{2}[x^{n+1}] \cdot \left(-\sqrt{1-4x}\right) = -\frac{1}{2}[x^{n+1}] \cdot (1-4x)^{1/2} =$

(1 ovlivní koeficient u x^0, to mě nezajímá)

$= -\frac{1}{2}[x^{n+1}] \sum_{n=0}^{\infty} \binom{1/2}{n} \cdot (-4x)^n = -\frac{1}{2} \cdot \binom{1/2}{n+1} \cdot (-4)^{n+1} =$

$= -\frac{1}{2} \cdot (-4)^{n+1} \cdot \frac{(\frac{1}{2}) \cdot (\frac{1}{2}-1) \cdot (\frac{1}{2}-2) \cdot \dots \cdot (\frac{1}{2}-n)}{(n+1)!} = -\frac{1}{2} \cdot (-4)^{n+1} \cdot \frac{\frac{1}{2} \cdot (-\frac{1}{2}) \cdot (-\frac{3}{2}) \cdot \dots \cdot (-\frac{2n-1}{2})}{(n+1)!}$

$= \frac{1}{2} \cdot 4^{n+1} \cdot \frac{\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{3}{2} \cdot \dots \cdot \frac{2n-1}{2}}{(n+1)!} = \frac{1}{2^{n+2}} \cdot 4^{n+1} \cdot \frac{1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-1)}{(n+1)!} =$

$= \frac{4^{n+1}}{2^{n+2}} \cdot \frac{1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-1) \cdot 2 \cdot 4 \cdot \dots \cdot (2n)}{(n+1)! \cdot 2 \cdot 4 \cdot \dots \cdot (2n)} = \frac{4^{n+1}}{2^{n+2}} \cdot \frac{(2n)!}{(n+1)! \cdot 2^n \cdot (n!)} = \frac{(2n)!}{(n+1)! \cdot n!} =$

$= \frac{1}{n+1} \cdot \binom{2n}{n}$ (příkladek ☺)

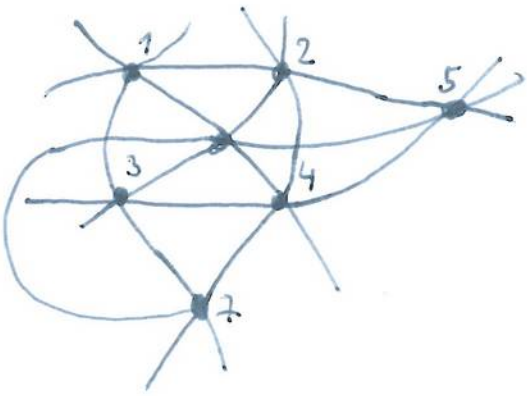
Tento vzorec je možné odvodit i kombinatoricky, ale je to celkem abstrakt.

Projektivní roviny a latinské čtverce

Def: (Hypergraf) je dvojice $H=(V,E)$, kde E je množina podmnožin V
V ... vrcholy
E ... množina hyperhran

Def: (Projektivní rovina)
je hypergraf (B,P) splňující:
"body" "přímky"

1) $\forall x,y \in B: x \neq y \Rightarrow \exists! p \in P: x \in p \wedge y \in p$
2) $\forall p,q \in P: p \neq q \Rightarrow |p \cap q| = 1$
3) $\exists Q \subseteq B: |Q| = 4 \wedge \forall p \in P: |p \cap q| \leq 2$



$P = \{ \{1,2,5\}, \{1,3,7\}, \{1,4,6\}, \{2,3,6\}, \{2,4,7\}, \{3,6,7\}, \{3,4,5\} \}$

Toto je ta samá projektivní rovina jaker je na deskách.
Kapitol z diskrétní matematiky.

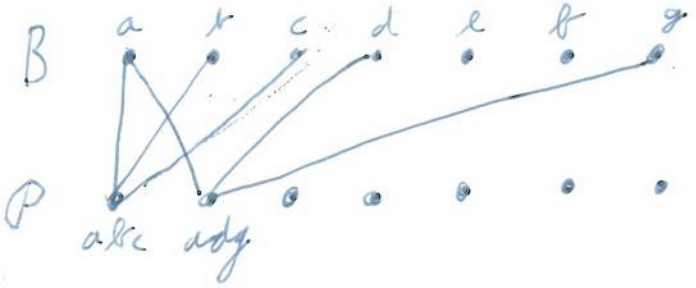
4. přednáška

Konečná projektivní rovina (KPR) je projektivní rovina (B,P), kde B i P jsou konečné.

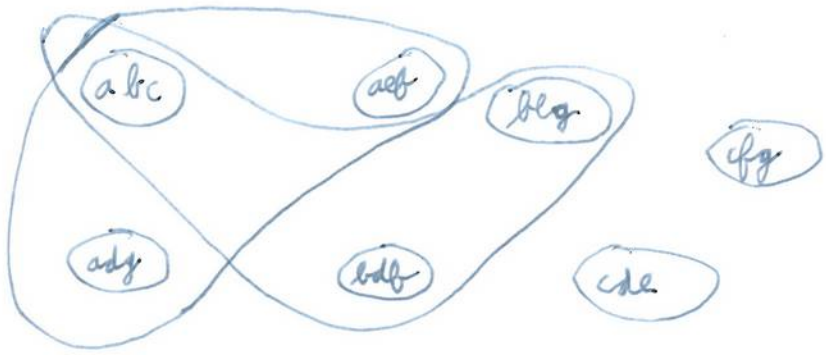
Fanova rovina: $B = \{a,b,c,d,e,f,g\}$
$P = \{\{a,b,c\},\{a,d,g\},\{a,e,f\},\{b,d,f\},\{b,e,g\},\{c,d,e\},\{c,f,g\}\}$

Značení: $\overline{ab}$ .... přímka obsahující body a a b.

Graf incidence: KPR (B,P) bipartitní graf G s partitami B a P, kde mezi $b \in B$ a $p \in P$ vede hrana v $G \Leftrightarrow b \in p$



Def: Duální projektivní rovina ke KPR (B,P) je hypergraf (P,B^*), kde $B^* = \{\{p \in P : b \in p\}, b \in B\}$



Lemma: Duální projektivní rovina ke KPR (B,P) je opět KPR

Důkaz: nechť (P,B^*) je duální ke (B,P).

(P,B^*) splní 1) axiom projektivní roviny $\Leftrightarrow \forall p,q \in P : p \neq q \; \exists! b^* \in B^* : \{p,q\} \in b^*$

$\Leftrightarrow \forall p,q \in P \; \exists! b \in B : b \in p \cap q \Leftrightarrow (B,P)$ splní 2) axiom projektivní roviny

(P,B^*) splní 2) axiom projektivní roviny $\Leftrightarrow$ splní 1) axiom projektivní roviny

(P, B^*) splní 3) axiom projektivní roviny $\iff \exists Q^* \subseteq P : |Q^*| = 4 \wedge$
$\forall b^* \in B^* : |b^* \cap Q^*| \subseteq 2$.
$\Longleftarrow \exists Q^* \subseteq P : |Q^*| = 4 \wedge$
$\forall b \in B$: b je obsažena v nejvýše 2 přímkách z Q^*.

Více: (B, P) splní 3) axiom projektivní roviny. Volme $Q \subseteq B$ dle 3) podmínky axiomu projektivní roviny, $Q = \{a, b, c, d\}$.
Definujme $Q^* = \{\overline{ab}, \overline{bc}, \overline{cd}, \overline{ad}\}$. Vidíme, že $|Q^*| = 4$:
kdyby např. $\overline{ab} = \overline{bc}$, tak $|\overline{ab} \cap Q| \geq 3$, spor s volbou Q.

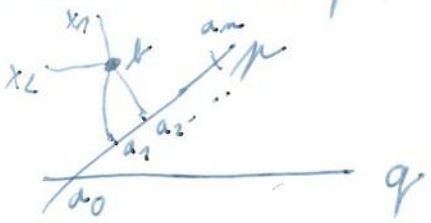
Vidíme, že žádné 3 přímky z Q^* nemají společný bod: kdyby např. $\overline{ab}, \overline{bc}, \overline{cd}$ měly společný bod, tak $b = c$, spor s $|Q| = 4$.
Tedy (P, B^*) splní 3) axiom projektivní roviny.

Lemma: Nechť (B, P) je KPR, nechť $p, q \in P$, potom $\exists b \in B : b \notin p \cup q$.
Důkaz: Nechť $Q = \{a, b, c, d\}$ je volena dle 3) axiomu projektivní roviny. Nechť p a q jsou libovolné přímky.
Kdyby Q obsahovala bod nepatřící do $p \cup q$, jsme hotovi.
Předpokládejme $Q \subseteq p \cup q$. Potom $|Q \cap p| \geq 2 = |Q \cap q|$ a $p \cap Q$ a $q \cap Q$ jsou disjunktní. BÚNO $p = \overline{ab}$ a $q = \overline{cd}$.
Nechť e je průsečík $\overline{ad}$ a $\overline{bc}$. Tvrdím $e \notin Q$: kdyby např. $e = a$, tak $a, b, c \in \overline{bc}$, tj. $|\overline{bc} \cap Q| \geq 3$, spor s 3) axiomem projektivní roviny. Tvrdím $e \notin p$: kdyby $e \in p$, tak $p = \overline{ab}$ a $\overline{bc}$ mají 2 spol. body b, e, spor.
Podobně se ukáže $e \notin q$. ∎

Lemma*: Nechť (B, P) je KPR. Nechť $a, b \in B$, potom $\exists p \in P : a \neq p \wedge b \notin p$.
Důkaz: Nechť (P, B^*) je duální k (B, P).
Dle lemmatu: pro $a^* = \{p \in P, a \in p\}$ a $b^* = \{p \in P, b \in p\}$
$\exists p \in P : p \neq a^* \cup b^*$
Tj.: přímka p neobsahuje a ani b.

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

Důkaz: Pro spor $\exists p, q \in \mathcal{P} : |p| > |q|$. Nechť a_0 je v průniku p a q. Nechť $p = \{a_0, a_1, a_2, \dots, a_n\}$. Dle lemma $\exists b \in B : b \notin p \cup q$. Nechť $\gamma_i = \overline{b a_i}$ pro $i = 1, \dots, n$.



Tvrdím, že pro $i = 1, \dots, n$. γ_i se liší od p i od q, protože $b \in \gamma_i$, ale $b \notin p \cup q$.

Tvrdím, že pro $i = 1, \dots, n$: $a_0 \notin \gamma_i$, protože kdyby $a_0 \in \gamma_i$ tak $\gamma_i \cap p$ obsahuje a_0 i a_1, spor.
Pro $i \neq j$, $r_i \neq r_j$, jinak by $r_i \cap p$ obsahovalo a_i i a_j.
Definujme c_i jako bod v $l_i \cap q$. Tvrdím pro $i \neq j$ jsou c_i a c_j různé body. Kdyby $c_i = c_j$, tak r_i a r_j mají v průniku b i c_i, SPOR.
Tj. l_q obsahuje aspoň $n+1$ bodů $a_0, c_1, c_2, \dots, c_n$ spor s $|q| < |p|$.

Def (Řád)
KPR $(B, \mathcal{P})$ je číslo n takové, že každá přímka má $n+1$ bodů.

Věta: Nechť $(B, \mathcal{P})$ je KPR řádu n. Potom
1) Každý bod $b \in B$ je obsažen v právě $n+1$ přímkách
2) $|B| \leq n^2 + n + 1$
3) $|B| = n^2 + n + 1$

Důkaz: 1) Nechť b je libovolný bod. Nechť p je přímka neprocházející b.
Nechť $|p| = n+1$, $p = \{a_0, a_1, \dots, a_n\}$. Potom body b procházejí právě přímky $\overline{a_0 b}$, $\overline{a_1 b}$, $\dots$, $\overline{a_n b}$,

nové pro $i \neq j$ ... $\overline{a_i b} \neq \overline{a_j b}$, jinak by $\overline{a_i b}$ a p měla 2 společné body.

2) Nechť $b \in B$ je lib. bod, nechť $p_0, p_1, \dots, p_n$ jsou přímky obsahující b. Každý bod $c \in B \setminus \{b\}$ leží na právě jedné přímce p_i která b. Navíc každá p_i obsahuje n bodů různých od b. Tj, $|B| = 1 + (n+1) \cdot n = n^2 + n + 1$

3) 

Počet hran v grafu incidence
$|B| \cdot (n+1)$ (plyne z 1)
$|P| \cdot (n+1)$ (definice řádu)
$\Rightarrow |B| = |P| = n^2 + n + 1$

Def: (Latinský čtverec)
Latinský čtverec řádu n je matice tvaru $n \times n$ vyplněná čísly $1, \dots, n$, tak, že žádný řádek ani sloupec neobsahuje stejné číslo vícekrát.

Dva latinské čtverce M, M' řádu n jsou ortogonální, pokud $\forall i \in \{1, \dots, n\}$ $\forall j \in \{1, \dots, n\}$ existuje právě jeden řádek r a sloupec s tak, že $M_{r,s} = i$ a $M'_{r,s} = j$

M

1	2	3
2	3	1
3	1	2

M'

1	2	3
3	1	2
2	3	1

1 1	2 2	3 3
2 3	3 1	1 2
3 2	1 3	2 1

3. přednáška

Věta: Nechť $M^{(1)}, M^{(2)}, \dots, M^{(t)}$ jsou latinské čtverce řádu n, které jsou navzájem ortogonální. Potom $t \le n-1$.

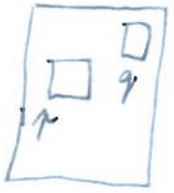
Důkaz: Definujme $x :=$ počet způsobů, jak zvolit čtverec $M \in \{M^{(1)}, \dots, M^{(t)}\}$ a dvě různá políčka p a q, která mají v M stejnou hodnotu.

Budu počítat x 2 způsoby:

1) $x = \underbrace{n}_{\text{počet voleb } p} \cdot \underbrace{(n-1)}_{\text{počet voleb } q \neq p,\ q \text{ má stejnou hodnotu jako } p} \cdot t$ ← počet voleb latinského čtverce řádu n, tedy počet voleb M

Formalizace: $x = |\{(M, p, q),\ M \in \{M^{(1)}, \dots, M^{(t)}\},\ p \in \{1,\dots,n\} \times \{1,\dots,n\},\ q \in \{1,\dots,n\} \times \{1,\dots,n\},\ p \neq q,\ M_p = M_q\}|$

2) $x = \underbrace{n^2}_{\#p} \cdot \underbrace{(n-1)^2}_{\#q \text{ v jiném sloupci a řádku než } p} \cdot 1$ ← počet $M \in \{M^{(1)}, \dots, M^{(t)}\}$, kde $M_p = M_q$ (ortogonalita)



$\Rightarrow n^2 \cdot (n-1) \cdot t = x \le n^2 \cdot (n-1)^2$

$\Rightarrow t \le n-1$

Věta: Existuje konečná projektivní rovina řádu $n \iff \exists\, n-1$ navzájem ortogonálních latinských čtverců řádu n.

Idea důkazu: ($\Leftarrow$)

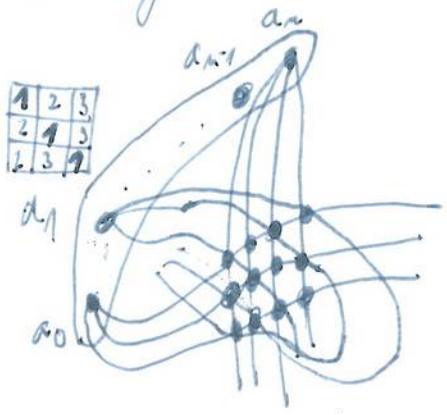
1	2	3
3	1	2
2	3	1

$M^{(1)}$

,

1	2	3
2	3	1
3	1	2

$M^{(2)}$



Ví se:

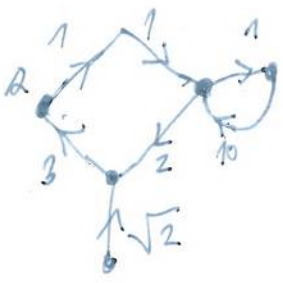
1) Pokud n je mocnina prvočísla, tak $\exists$ konečná projektivní rovina řádu n
2) Pro $n=6$ i pro $n=10$ neexistuje konečná projektivní rovina řádu n
3) pro obecné n se neví, jestli $\exists$ konečná projektivní rovina řádu n

Toky v sítích

Def: Tková síť je čtveřice (G, z, s, c), kde
$G=(V,E)$ je orientovaný graf, nesmí obsahovat ani stejně orientované násobné hrany, může vést $u \rightleftarrows v$
$z \in V$ ... "zdroj"
$s \in V \setminus \{z\}$ "stok" ("spotřebič")
c ... funkce $E \to [0, +\infty)$ ($c(e)$ ... kapacita hrany)

Značení: pro orientovaný graf $G=(V,E)$:
pro $v \in V$. $\mathrm{Out}(v)$: množina hran vycházejících z v.
$\mathrm{In}(v)$: množina hran vstupujících do v
pro $A \subseteq V$. $\mathrm{Out}(A)$ ... množina hran se začátkem v A a koncem v $V \setminus A$.
$\mathrm{In}(A)$.. hrany z $V \setminus A$ do A.

Tok v síti (G, z, s, c) je funkce $f: E \to [0, +\infty)$ splňující
1) $\forall e \in E: 0 \le f(e) \le c(e)$
2) $\forall v \in V \setminus \{z, s\}: \sum_{e \in \mathrm{Out}(v)} f(e) = \sum_{e \in \mathrm{In}(v)} f(e)$



Velikost toku: $\|f\| := \sum_{e \in Out(z)} f(e) - \sum_{e \in In(z)} f(e)$

Maximální tok: Tok s největší velikostí ze všech toků v dané síti.

Fakt: Každá síť má maximální tok, pokud jsou kapacity celočíselné, existuje max tok, který je celočíselný.

Řez v tokové síti (G, z, s, c) je množina hran $R \subseteq E$ taková, že každá orientovaná cesta ze z do s obsahuje alespoň 1 hranu z R.

Kapacita řezu $c(R) := \sum_{e \in R} c(e)$

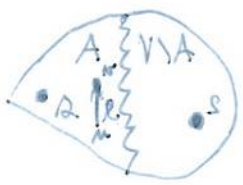
Minimální řez je řez s nejmenší kapacitou.

Lemma: Nechť f je tok v síti (G, z, s, c), nechť $A \subseteq V$ je množina taková, že $z \in A$, $s \notin A$.
Potom $\|f\| = \sum_{e \in Out(A)} f(e) - \sum_{e \in In(A)} f(e)$

Důkaz: Víme: $\sum_{e \in Out(z)} f(e) - \sum_{e \in In(z)} f(e) = \|f\|$
Pro $\forall v \in A \setminus \{z\}$: $\sum_{e \in Out(v)} f(e) - \sum_{e \in In(v)} f(e) = 0$
} soustava rovnic

Sečteme tyto rovnice:

$$\underbrace{\sum_{x \in A} \sum_{e \in Out(v)} f(e) - \sum_{v \in A} \sum_{e \in In(A)} f(e)}_{(*)} = \|f\|$$



Pro hranu $e=(u,v)$, která má oba konce v A dodejme (*) hodnotu $f(e)$; $-f(e) \Rightarrow$ příspěvky e se vyruší.

$$Tj.: (*) = \sum_{e \in Out(A)} f(e) - \sum_{e \in In(A)} f(e). \quad \blacksquare$$

Důsledek: Nechť f je tok v R síti (G, z, s, c). Potom $\|f\| \leq c(R)$.

Důkaz: Definujme $A := \{v \in V$: existuje orientovaná cesta se z do v nenasycující hrany $R\}$

jistě $z \in A$, $s \notin A$.

Dle lemmatu platí: $\|f\| - \sum_{e \in Out(A)} f(e) - \underbrace{\sum_{e \in In(A)} f(e)}_{\geq 0} \leq \sum_{e \in Out(A)} f(e) \leq \sum_{e \in Out(A)} c(e)$

$\leq \sum_{e \in R} c(e) = c(R)$

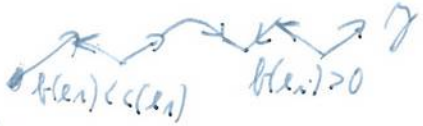
Každá hrana z $Out(A)$ je v R.

Def: Nechť f je tok v (G, z, s, c). Nechť x a y jsou vrcholy G. **Nenasycená cesta** z x do y je posloupnost různých vrcholů $x = x_1, x_2, x_3, \ldots, x_k = y$ taková, že $\forall i \in \{1, \ldots, k-1\}$ platí:

aspoň jedna z těchto možností:

1) $\exists$ hrana $e_i = (x_i, x_{i+1})$ a $f(e_i) < c(e_i)$

2) $\exists$ hrana $e_i = (x_{i+1}, x_i)$ a $f(e_i) > 0$



x_1
||
x

Zlepšující cesta: nenasycená cesta z z do s.

Věta: Pro tok f v (G, z, s, c) jsou následující tvrzení ekvivalentní:

1) f je maximální
2) f nemá zlepšující cestu
3) existuje řez R takový, že $\|f\| = c(R)$.

Důsledek: Pokud f_{max} je maximální tok v R_{min} je minimální řez v síti (G, z, s, c), tak $\|f_{max}\| = c(R_{min})$

Důkaz: Ukážeme postupně implikace $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$

$1 \Rightarrow 2$: Kdyby f měl zlepšující cestu $z = x_1, x_2, \dots, x_k = s$
tak na každé dopředné hraně zvýšíme tok o $\varepsilon > 0$ a na zpětné hraně snížíme tok o $\varepsilon > 0$, dostaneme nový tok velikosti $\|f\| + \varepsilon$ (ε dost malé).
Čj: f není maximální.

$2 \Rightarrow 3$: Nechť neexistuje zlepšující cesta
$A := \{v \in V : \exists \text{ nenasycená cesta z } z \text{ do } v\}$,
vidíme: $z \in A$, $s \notin A$, pro $\forall e \in Cut(A): f(e) = c(e)$
$\forall e \in In(A): f(e) = 0$

Definujeme $R := Cut(A)$

$$\|f\| = \sum_{e \in Cut(A)} f(e) - \sum_{e \in In(A)} f(e) = \sum_{e \in Cut(A)} c(e) = c(R)$$

3 ⇒ 1 plyne z předchozího kroku

6. přednáška

Königova-Egerváryho věta, Hallova věta

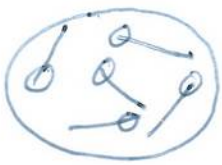
Párování: v grafu $G=(V,E)$ je množina hran $M \subseteq E$ taková, že každé dvě hrany M jsou disjunktní.

Vrcholové pokrytí: grafu $G=(V,E)$ je množina vrcholů $C \subseteq V$ taková, že každá hrana G dopadá nejméně jeden vrchol C.

$m(G)$ .... velikost největšího párování ("matching" = párování)
$vc(G)$ .... velikost nejmenšího vrch. pokrytí v G ("vertex cover" = vrch. pokrytí)

$m(G) \leq vc(G)$

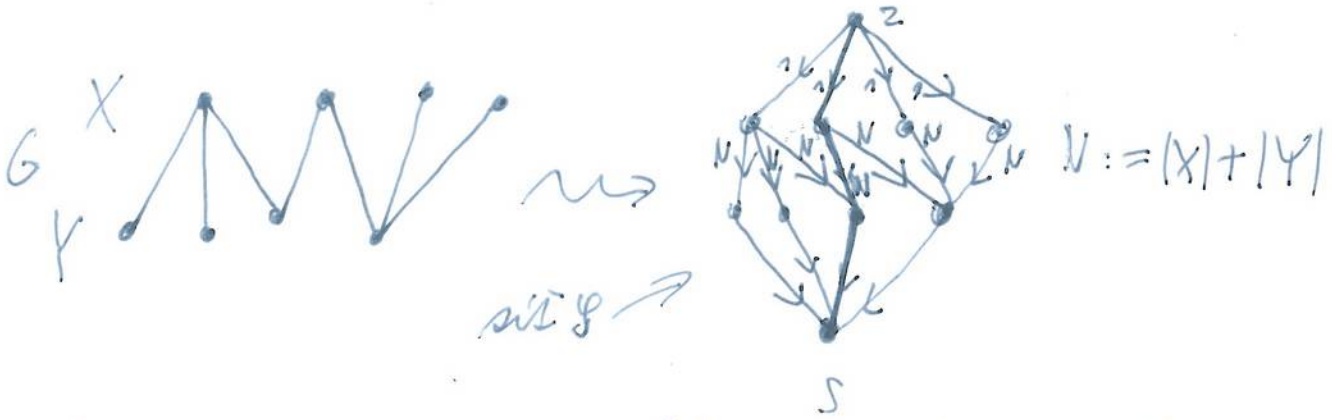
Každá hrana pokrytí pokryje nejvýše dvě hrany v největším párování jedním vrcholem.



$vc(C_5) = 3$

Věta: (König a Egerváry, 1931)
Pro každý bipartitní graf G platí $m(G) = vc(G)$.

Důkaz: Nechť $G=(V,E)$ je bipartitní graf s partitami X a Y



$N := |X| + |Y|$

Víme, že $m(G) \leq vc(G)$. Dokážeme $m(G) \geq vc(G)$.

Dokážeme: $m(G) \geq$ || max. tok v S || $= c \cdot$ (min. řez v S) $\geq vc(G)$, kde S je toková síť vzniklá tak, že ke G přidáme vrcholy z, s, přidáme hrany se z do X a z Y do s, hrany mezi X a Y orientujeme z X do Y, kapacity $c(e)$

$$c(e) = \begin{cases} 1 & \text{pokud } e \text{ vede ze } z \text{ do } X \text{ nebo z } Y \text{ do } s \\ N := |X| + |Y| & \text{pokud } e \text{ vede mezi } X \text{ a } Y \end{cases}$$

Důkaz I: Nechť f je max. tok v S

BÚNO f je celočíselný. 👁: $\forall e \in f(e) \in \{0, 1\}$.

Definujme $M := \{e \in E(G) \mid f(e) = 1\}$. Potom N je párování.

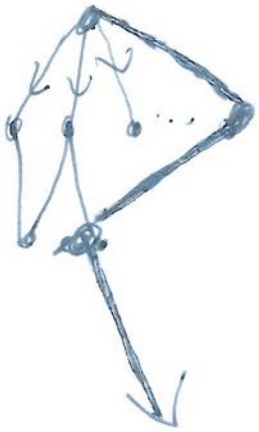
Nemůže nastat, protože kapacita je 1.

Navíc $|M| = \|f\|$, tj. $m(G) \geq |M| = \|f\|$.

Důkaz II: Nechť R je min. řez v S.

Potom R obsahuje jen hrany se z do X a z Y do s.

$C := \{v \in X \cup Y, v \text{ obsažen v hraně z } R\}$



Potom C je vrch. pokrytí G.
$|C| = c(R)$ (= # hran v R)
Tj: $\nu_c(G) \leq |C| = c(R)$ ∎

Postačující podmínky pro hladkou větu

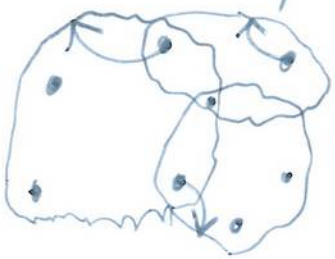
$G = (V, E)$ je bipartitní graf s partitami X a Y.
Značení: pro $v \in X$ $N(v)$ .... množina sousedů vrcholu v,
tj. $N(v) = \{w \in Y : \{v, w\} \in E\}$

$$\text{pro } A \subseteq X : N(A) := \bigcup_{v \in A} N(v)$$

Def: Nechť $H = (V, E)$ je hypergraf. Systém různých reprezentantů pro H je funkce $r : E \to V$ taková, že:

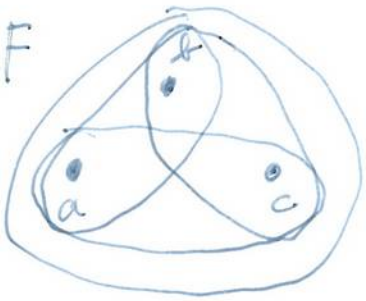
1) $\forall e \in E : r(e) \in e$
2) r je prostá (tj. $e \neq e' \Rightarrow r(e) \neq r(e')$)

$r(e)$ .... reprezentant hyperhrany e



Úlohy ve větě a jejich reprezentanti.

Pokud $|E| > |V|$, tak $H = (V, E)$ nemá systém různých reprezentantů



$|F| = 4$

$\left|\bigcup_{e \in F} e\right| = |\{a, b, c\}| = 3$

Věta: (Hall, 1935)

1) (hypergrafová verze) Hypergraf $H = (V, E)$ má systém různých reprezentantů $\iff$ $\boxed{\forall F \subseteq E : |F| \le \left|\bigcup_{e \in F} e\right|}$ Hallova podmínka

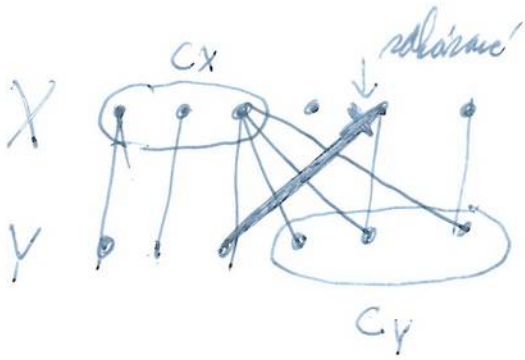
2) (bipartitní verze) Bipartitní graf G s partitami X a Y má párování $|X| \iff \forall A \subseteq X : |A| \le |N(A)|$

Důkaz: bipartitní verze „$\Rightarrow$" Nechť G má párování M velikosti $|X|$

Volme $A \subseteq X$. Potom $|N(A)| \ge$ počet vrcholů spárovaných s vrcholy A $= |A|$

„$\Leftarrow$" Předpokládejme, že $m(G) < |X|$. Cíl najít $A \subseteq X$ takovou, že $|N(A)| < |A|$.
König-Egerváry: $vc(G) = m(G) < |X|$. Nechť C je nějaká vrcholové pokrytí G

$C_X := C \cap X$, $C_Y := C \cap Y$. Platí $|C_X| + |C_Y| = |C| = vc(G) < |X|$

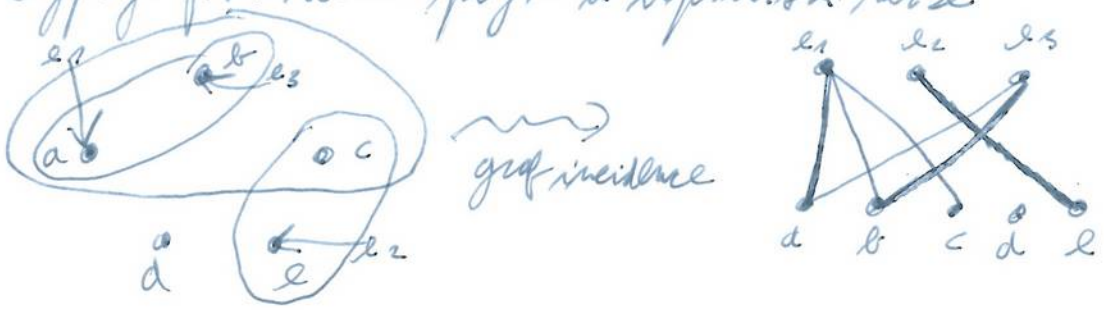


$A := X \setminus C_X$

👁: $N(A) \subseteq C_Y$, tj. $|N(A)| \subseteq C_Y$

👁: $|A| = |X| - |C_X| > (|C_X| + |C_Y|) - |C_X| = |C_Y|$

Hypergrafová verze plyne z bipartitní verze



👁 Nechť G je graf incidence hypergrafu $H = (V, E)$.
Partity G: $X := E$
$Y := V$

Systém různých reprezentantů v hypergrafu $\overset{1:1}{\Longleftrightarrow}$ párování velikosti $|X|$ v G

H splní Hallovu podmínku $\Longleftrightarrow \forall A \subseteq X : |A| \leq |N(A)|$,
protože $N(A) = \bigcup_{e \in A} e$. ■

7. přednáška

Vrcholová a hranová souvislost

(Odvahost při pokrytí grafu)

Značení: $G=(V,E)$ je graf

pro $e \in E$: $G-e = (V, E \setminus \{e\})$

pro $v \in V$: $G-v = (V \setminus \{v\}, E \cap \binom{V \setminus \{v\}}{2})$

Def: Množina hran $F \subseteq E$ je *hranový řez* v grafu $G=(V,E)$, pokud smazání všech hran z F vznikne nesouvislý graf.
Množina $W \subseteq V$ je *vrcholový řez* v G, pokud po smazání vrcholů z W vznikne nesouvislý graf.

Každý graf s alespoň 2 vrcholy hranový řez

Každý graf, který nějakou hranu má, alespoň 1-vrcholový řez

Def: *Hranová souvislost* grafu G, značená $K_e(G)$, je velikost nejmenšího hranového řezu v G.

Vrcholová souvislost grafu G, značená $K_v(G)$ je definována takto:

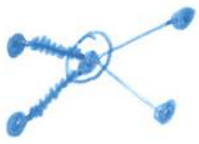
$$K_v(G) = \begin{cases} \text{velikost nejmenšího vrcholového řezu, pokud } G \text{ není úplný graf} \\ n-1, \text{ pokud } G \text{ je izomorfní } K_n \end{cases}$$

Def: Graf G je hranově k-souvislý, pokud jeho $K_e(G) \geq k$

⚠ alespoň

Graf G je (vrcholově) k-souvislý, pokud $K_v(G) \geq k$

Pro G s alespoň 2 vrcholy: G je hranově 1-souvislý $\iff$ G je vrcholově 1-souvislý $\iff$ G je souvislý



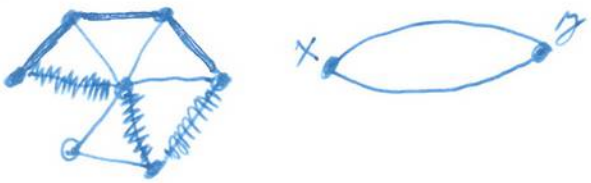
$K_e(G)=2$: G je hranově 1-souvislý i hranově 2-souvislý

$K_v(G)=1$: G je vrcholově 1-souvislý, ale ne vrcholově 2-souvislý

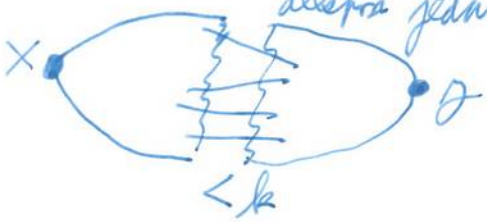
Def: Hranový řez F v grafu G odděluje vrcholy x a y, pokud x a y jsou v různých komponentách souvislosti $(V, E\setminus F)$.

Věta: Nechť $G=(V,E)$ je graf, nechť $k\in\mathbb{N}$, nechť x a y jsou 2 různé vrcholy G. Potom: 1) G obsahuje hranový řez F, kde $|F|<k$, F odděluje x a y. ⟺ 2) G neobsahuje k hranově disjunktních cest z x do y.

Důkaz:

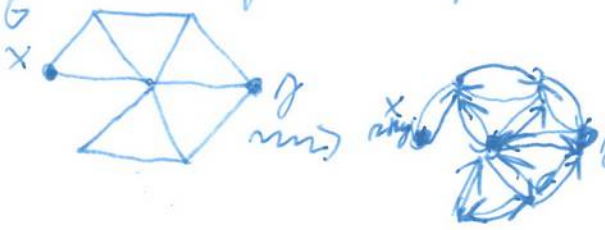


$1 \Rightarrow 2$ jasné, protože každá cesta z x do y musí obsahovat alespoň jednu hranu z řezu F



$2 \Rightarrow 1$ (důkaz obrazem)

Předpokládejme, že neplatí 1)



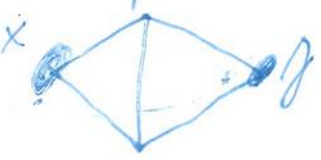
kapacity 1

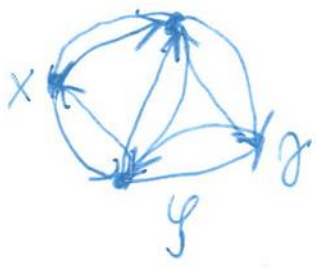
Vyrobíme tokovou síť $S(\vec{G}, x, y, c)$ kde $\vec{G}$ vznikne z G tak, že se každá hrana $\{u,v\}$ v G nahradí dvojicí hran (u,v) a (v,u). Kapacity jsou rovny jedné. Nechť f_{max} je maximální tok v S a R_{min} minimální řez v S. Pokud kapacita R_{min} je $< k$, potom definujeme $F = \{\{u,v\}, (u,v) \in R_{min} \text{ nebo } (v,u) \in R_{min}\}$.
Potom F je hranový řez v G oddělující x a y, $|F| \leq |R_{min}| = c(R_{min}) < k$

SPOR s tím, že neplatí 1)

Takže $c(R_{min}) = |R_{min}| \geq k$. Tedy $\|f_{max}\| \geq k$.
Cíl najít k hranově disjunktních cest z x do y. BÚNO f_{max} je celočíselný, tj. $\forall \vec{e} \in S : f_{max}(\vec{e}) \in \{0,1\}$. Definujme $T \subseteq E(\vec{G})$ takto: $T = \{\vec{e} : f_{max}(\vec{e}) = 1\}$

Zvolme maximální tok tak, aby f_{max} byl celočíselný a zároveň $|T|$ byla co nejmenší. Potom T neobsahuje žádný orientovaný cyklus. Kdyby T obsahovala orientovanou kružnici $\vec{C}$, tak na hranách $\vec{C}$ snížíme f_{max} z 1 na 0. Najdeme k hranově disjunktních cest $x \to y$ takto: hladově vyrazíme z x po orientované cestě, jejíž hrany patří do T, dál dorazíme do y. Tak získáme cestu P_1 z x do y. Potom z T odebereme hrany P_1, čímž hrany v T odpovídají toku velikosti $\|f_{max}\| - 1$. Opakováním nejdeme alespoň k hranově disjunktních cest z x do y v S, čemu odpovídá k hranově disjunktních cest z x do y v G. ■





Věta : (Menger, hranová verze, 1927)
Graf $G=(V,E)$ s alespoň 2 vrcholy je hranově k-souvislý $\iff$ mezi každou dvojicí různých vrcholů vede alespoň k hranově disjunktních cest.

Důkaz : „$\Longrightarrow$" G je hranově k-souvislý $\iff$ neexistuje hranový řez velikosti $< k$ $\iff$ žádnou dvojici různých vrcholů nelze oddělit hranovým řezem velikosti $< k$ $\iff$ mezi každou dvojicí různých vrcholů vede k hranově disjunktních cest.

Def: Dvě cesty z x do y jsou vnitřně vrcholově disjunktní, pokud nemají žádný společný vrchol kromě x a y.

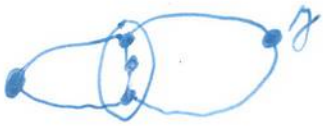
Věta : Nechť $G=(V,E)$ je graf, $k \in \mathbb{N}$ číslo, x, y dva nesousední různé vrcholy, potom:

1) Existuje vrcholový řez W : $|W|<k$, W odděluje x a y

$\Downarrow$

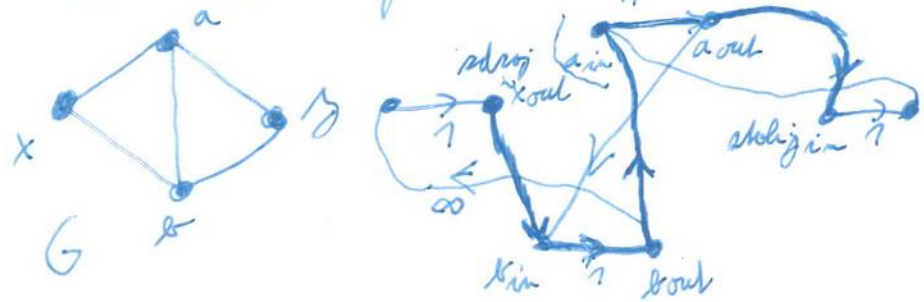
2) Neexistuje k VVD cest z x do y.

Idea důkazu : 1) $\Longrightarrow$ 2) ✓



G

2) $\Longrightarrow$ 1) Nějaké síť



Lemma: Nechť $G=(V,E)$ má alespoň 2 vrcholy, nechť $e \in E$.
Potom $\kappa_v(G-e) \geq \kappa_v(G)-1$

Důkaz: cvičení (odebráním hrany se žádná množina může o 1)

Věta: (Menger, vrcholová verze, 1927)
Graf G je vrcholově k-souvislý $\Leftrightarrow$ mezi každými 2 různými vrcholy existuje alespoň k VVD cest.

Důkaz: „$\Leftarrow$" jasné, G má alespoň $k+1$ vrcholů a žádný vrcholový řez velikosti $< k$.

„$\Rightarrow$" Nechť G je k-souvislý, nechť x a y jsou různé vrcholy. Cíl najít k VVD cest z x do y. Pokud $\{x,y\} \notin E$, prosím věta, hotovo ✓
Pokud $\{x,y\} \in E$, říkejme jí e. Definuji $H=G-e$,
Lemma: $\kappa_v(H) \geq k-1$, věta: $\exists (k-1)$ VVD cest $x \to y$ v H → přidám e jako k-tou cestu.

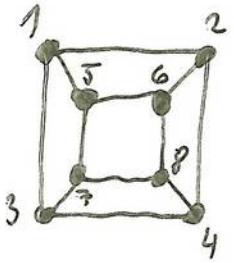
8. přednáška

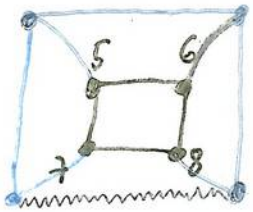
Připomenutí:
G je vrcholově 2-souvislý $\Leftrightarrow \kappa_v(G) \geq 2$
$\Leftrightarrow$ G je úplný a má alespoň 3 vrcholy nebo není úplný a neobsahuje vrcholový řez velikosti 1 nebo 0
$\Leftrightarrow$ G má alespoň 3 vrcholy a žádný
Menger vrcholový řez velikosti 1 nebo 0.
$\Leftrightarrow$ G má alespoň 2 vrcholy a každé dva vrcholy lze propojit dvěma VVD cestami
HK
$\Leftrightarrow$ G má alespoň 2 vrcholy a každé 2 vrcholy na společné kružnici.

Def: **Přidat ucho** ke grafu G znamená zvolit dva různé vrcholy x, y v G a přidat do G nové hrany a vrcholy tvořící cestu z x do y.

Pozn: Přidání jedné hrany do grafu je speciální případ přidání ucha.

Věta: ("lemma o uších")
Graf $G=(V,E)$ je vrcholově[2] souvislý $\iff$ G lze vyrobit z kružnice posloupností přidání uší.

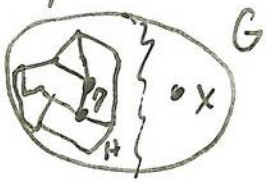




Důkaz: „$\Leftarrow$" jednodušše se přesvědčíme, že přidáním ucha do vrcholu 2-souvislého grafu nevznikne vrcholový řez velikosti 1 nebo 0.

„$\Rightarrow$" Nechť G je 2-souvislý. Nechť $H=(V_H, E_H)$ je co nejlepší podgraf G, který lze vyrobit z kružnice posloupností přidání uší. Chceme dokázat, že $H=G$. Pro spor předpokládejme, že $H \neq G$. Rozlišíme 2 případy.

1) $V_H \neq V$: Nechť x je libovolný vrchol z $V \setminus V_H$, nechť y je libovolný vrchol z V_H (jistě $H \neq \emptyset$, protože G obsahuje alespoň 4 hrany). G je souvislý $\Rightarrow$ G má cestu z x do y $\Rightarrow$



$\Rightarrow$ G má hranu $e = \{x', y'\}$ takovou, že $x' \in V \setminus V_H$ a $y' \in V_H$. Protože G je vrcholově 2-souvislý, tak $G - y'$ je souvislý, tj. $G - y'$ obsahuje cestu z x' do $V_H \setminus \{y'\}$. Nechť P je nejkratší takováto cesta. Jistě žádný vnitřní vrchol P není v H (z minimality). Nechť y'' je koncový vrchol P patřící do H. Potom $P \cup e$ tvoří ucho, které lze přidat k H, spor s maximalitou H.

2) $V_H = V$, $E_H \neq E$: potom ale jakoukoliv hranu $e \in E \setminus E_H$ lze přidat k H jako ucho, spor s maximalitou H.

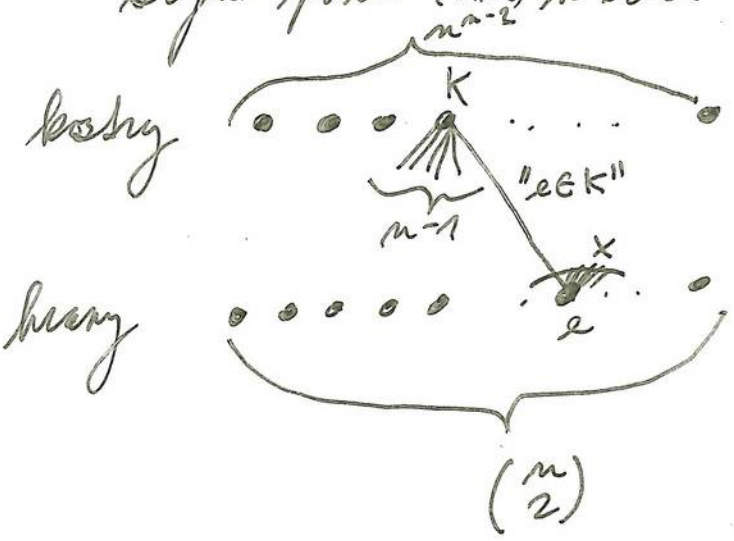
Počítání dvěma způsoby

Věta (Cayleho formule)
Pro $n \geq 1$ graf K_n má n^{n-2} koster.
$n = 2$  1 koster
$n = 3$  : 
$n = 4$  : 4 kostry izomorfní, 12 kostr izomorfních  } 16 koster

Důsledek: Pro $n \geq 2$: graf K_n^-, vzniklý z K_n smazáním jedné hrany, hrany má $(n-2) \cdot n^{n-3}$ koster.

Důkaz důsledku: Nechť e je hrana K_n. Nechť X_n je počet kostěr K_n, které obsahují e.

Víme, že: K_n má n^{n-2} kostěr. Každá kostra K_n má $n-1$ hran. K_n má $\binom{n}{2}$ hran. Každá hrana K_n je ve stejném počtu (X_n) kostěr.



Spočítejme dvěma způsoby počet uspořádaných dvojic (K, n), kde K je kostra K_n a n je hrana v K.

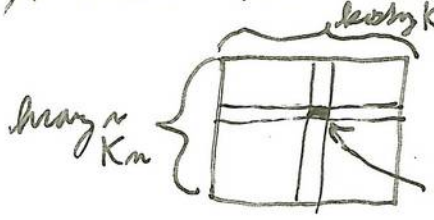
1. způsob: počet těchto dvojic je $n^{n-2} \cdot (n-1)$
2. způsob počet těchto dvojic je $\binom{n}{2} \cdot X_n$

$n^{n-2} \cdot (n-1) = \binom{n}{2} \cdot X_n \Rightarrow$

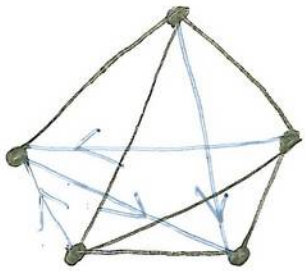
$X_n = 2 n^{n-3}$

K_n má $n^{n-2} - X_n = (n-2) \cdot n^{n-3}$

Ekvivalentně si bipartitní graf můžeme představit jako nějakou tabulku (matici)



Důkaz: Označme k_n počet kostěr K_n. Jakoženáhodná kostra - kostra, kde jeden vrchol je kořen a všechny hrany jsou orientovány do kořene.

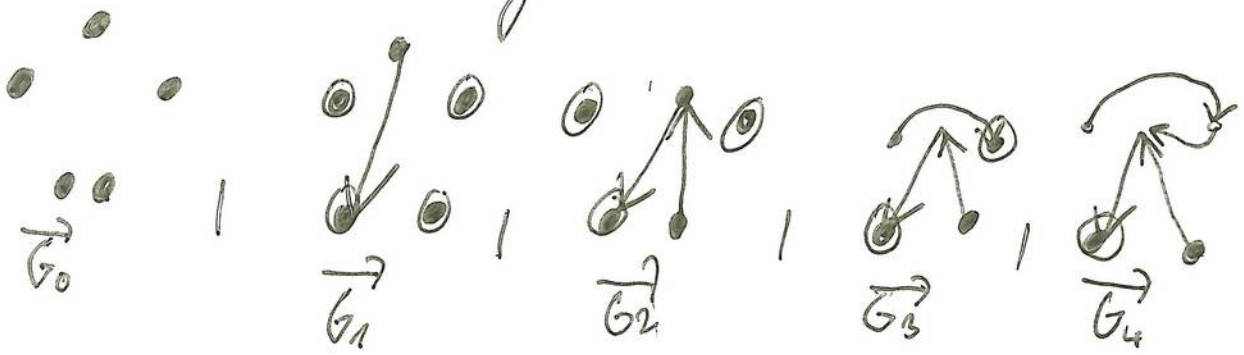


Označme Z_n počet zakořeněných kostek.

$Z_n = n \cdot k_n$, protože každou kostku lze zakořenit v některém z n vrcholů.

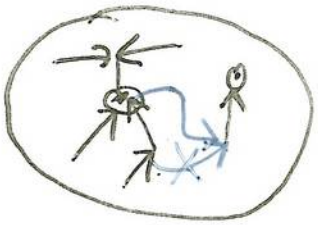
Def: (Pavlos)
Rozklad vytrvalé kostky je posloupnost orientovaných grafů $\vec{G_0}, \vec{G_1}, \dots, \vec{G_{n-1}}$ kde

1) $\forall i = 0, \dots, n-1$: $\vec{G_i}$ má i orientovaných hran, každá komponenta G_i je zakořeněný strom. (Důsledek: $\vec{G_i}$ má $n-i$ komponent, $\vec{G_{n-1}}$ je zakořeněná kostka)
2) $\forall i = 0, \dots, n-2$: $\vec{G_{i+1}}$ vznikne z $\vec{G_i}$ přidáním jedné orientované hrany



Označme si p_n počet pavlosů
Nechť $\vec{G_0}, \dots, \vec{G_{n-1}}$ je pavlos, nechť $\vec{G_{i+1}}$ vznikl přidáním hrany $\vec{e_{i+1}}$

1) Konce e_{i+1} patří do různých komponent G_i.
2) Zdálek e_{i+1} je kostra příslušné komponenty G_i.



Počet způsobů, jak přidat hranu do $\overrightarrow{G_i}$ aby vznikl graf, jehož každá komponenta je zakořeněný strom je $n\cdot(n-i-1)$, protože mám n možností jak zvolit konec přidané hrany a pouze $n-i-1$ možností, jak zvolit začátek přidané hrany v kterém nějaké komponenty neobsahující zvolený konec.

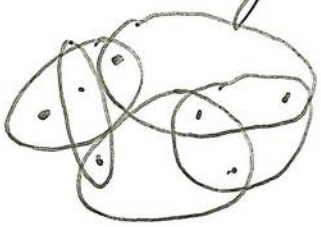
$$P=\prod_{i=0}^{n-2} n\cdot(n-i-1)=n^{n-1}\cdot(n-1)!$$

$$\Longrightarrow Z_n=n^{n-1}\Longrightarrow k_n=n^{n-2} \qquad \blacksquare$$

9. přednáška

$[n]=\{1,2,3,\dots,n\}$
$2^{[n]}=\{M : M\subseteq[n]\}$ } značení pro Spernerovu větu

Systém množin je <u>nezávislý</u>, pokud neobsahuje dvě různé množiny A,B takové, že $A\subset B$.

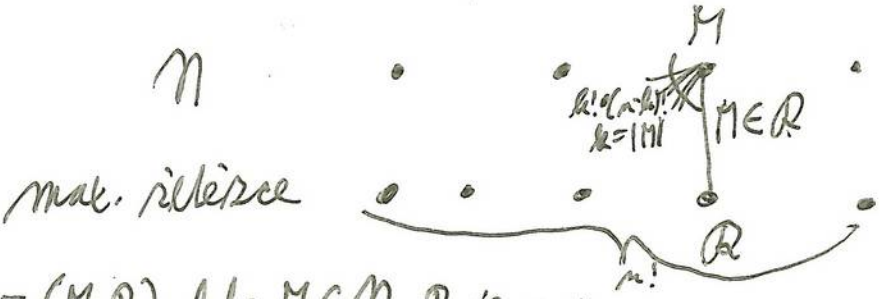


$\exists$ nezávislý systém $\subseteq 2^{[n]}$ velikosti $\binom{n}{\lfloor \frac{n}{2}\rfloor}=\binom{n}{\lceil \frac{n}{2}\rceil}$
(např. systém všech $\lfloor\frac{n}{2}\rfloor$-prvkových podmnožin $[n]$)

<u>Věta</u>: (Sperner, 1927)
Každý nezávislý systém $\mathcal{H}\subseteq 2^{[n]}$ má nejvýše $\binom{n}{\lfloor\frac{n}{2}\rfloor}$ množin

<u>Důkaz</u>: Nechť $\mathcal{H}\subseteq 2^{[n]}$ je nezávislý systém. Chceme dokázat $|\mathcal{H}|\leq\binom{n}{\lfloor\frac{n}{2}\rfloor}$. Def. maximální řetězec v $2^{[n]}$

je posloupnost $M_0 \subset M_1 \subset M_2 \subset \dots \subset M_n \subseteq [n]$, kde
$\forall i = 0, \dots, n : |M_i| = i$.
Příklad pro $n=4$: $\emptyset \subset \{3\} \subset \{1,3\} \subset \{1,3,4\} \subset \{1,2,3,4\}$
maximálních řetězců v $2^{[n]}$ je $n!$



$x := (M, \mathcal{R})$, kde $M \in \mathcal{N}$, $\mathcal{R}$ je max. řetězec a $M \in \mathcal{R}$.

Kolik je jich celkem?
⇕
počet dvojic $(M, \mathcal{R})$ kde $M \in \mathcal{N}$, $\mathcal{R}$ je max. řetězec a $M \in \mathcal{R}$

Počítejme x dvěma způsoby
1. způsob: mám $n!$ maximálních řetězců, každý z nich obsahuje nejvýše 1 množinu z $\mathcal{N}$, jinak by šlo výpočet nebyl nezávislý. Odtud: $x \le n!$

2. způsob: volme $M \in \mathcal{N}$, $k := |M|$.

$$\underbrace{\emptyset \subset \dots \subset \dots \subset \dots \subset M_k}_{k! \text{ možností}} \underbrace{\subset \dots \subset \dots \subset \dots \subset}_{(n-k)! \text{ možností na výsledek}}$$

M je obsažena v $k!(n-k)!$ řetězcích.
Odtud $x = \sum_{M \in \mathcal{N}} |M| \cdot (n-|M|)!$

$$n! \ge \sum_{M \in \mathcal{N}} |M|! \cdot (n-|M|)!$$

$$\iff 1 \ge \sum_{M \in \mathcal{N}} \frac{|M|! \cdot (n-|M|)!}{n!} = \sum_{M \in \mathcal{N}} \frac{1}{\binom{n}{|M|}} \ge \sum_{M \in \mathcal{N}} \frac{1}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} = \frac{|\mathcal{N}|}{\binom{n}{\lfloor \frac{n}{2} \rfloor}}$$

tj. $\left(\binom{n}{\lfloor \frac{n}{2} \rfloor}\right) \geq |n|$

Ramseyovy věty

Motivační úvození:

1) V každé skupině 6 lidí lze najít buď 3 lidi z nichž každá dvojice se navzájem zná nebo 3 lidi z nichž žádná dvojice se navzájem nezná.

1) $\Leftrightarrow$ 2) $\Leftrightarrow$ 3)

2) V každém grafu na 6 vrcholech je buď klika velikosti 3 nebo nezávislá množina velikosti 3.

3) V každém obarvení hran grafu K_6 dvěma barvami existuje jednobarevný trojúhelník.

Důkaz (2) Nechť G je graf na 6 vrcholech, nechť x je libovolný vrchol, rozlišíme 2 případy

a) x má stupeň alespoň 3

Buď jsou 2 sousedé spojeni hranou $\Rightarrow$ tvoří spolu s x klika velikosti 3 nebo sousedé tvoří nezávislou množinu velikosti 3

b) x má stupeň $\leq 2 \Longrightarrow x$ má ≥ 3 nesousedy ...
spočítáme s případem a)

Značení: pro graf $G=(V,E)$
$w(G)$ velikost největší kliky v G
$\alpha(G)$ velikost největší nezávislé množiny v G

Věta: (Ramsey, 1930)
$\forall k,l \in \mathbb{N}\ \exists N(k,l) \in \mathbb{N}$: každý graf G o alespoň $N(k,l)$ vrcholy splňuje buď $w(G) \geq k$ nebo $\alpha(G) \geq l$.

Důkaz: indukcí podle $k+l$
Pro $k=1, l=1$ lze vzít $N(1,1)=1$
Pro $k=1$, l obecné, stačí $N(1,l)=1$, podobně $N(k,1)=1$
Pro $k=2$, l obecné: funguje $N(2,l)=l$
víme $N(3,3)=6$

Mějme $k,l \geq 3$. Dle IP $\exists N(k-1,l)$ a $N(k,l-1)$ splňující vlastnosti z věty. Volme $N := N(k-1,l)+N(k,l-1)$.
Tvrdím, že pro $N(k,l)=N$ věta platí.

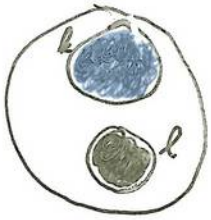
Důkaz tvrzení:
Nechť $G=(V,E)$ je graf na N vrcholech. Nechť x je libovolný vrchol, rozlišme 2 případy.
a) x má alespoň $N(k-1,l)$ sousedů. Nechť H je podgraf indukovaný sousedy x. IP. H má kliku velikosti $k-1$ nebo nezávislou množinu velikosti l.
Pokud $w(H) \geq k-1$, ke největší klice v H přidáme x a máme kliku v G velikosti $\geq k$.

Pokud $\alpha(H) \geq \ell$, tak $\alpha(G) \geq \ell$, protože.

b) x má méně než $N(k-1, \ell)$ sousedů, tak x má alespoň $(|V|-1) - (N(k-1,\ell)-1) = N(k, \ell-1)$

1) nesousedů" (tj. vrcholů různých od x nesousedících s x)
Nechť H je podgraf G indukovaný nesousedy x.
Pokud $\omega(H) \geq k$, tak $\omega(G) \geq k$
Pokud $\alpha(H) \geq \ell - 1$, tak přidám x, získáme $\alpha(G) \geq \ell$ ■

Ekvivalentní verze: $\forall k, \ell \in \mathbb{N}\ \exists N(k,\ell) \in \mathbb{N}$: pro každé obarvení hran $K_{N(k,\ell)}$ červeně a modře existuje modrá kopie K_k nebo červená kopie K_ℓ.



Důsledek R.V. ("Ramseyova verze")
$\forall k \in \mathbb{N}\ \exists N(k) \in \mathbb{N}\ \forall G$ graf s alespoň $N(G)$ vrcholy splní $\omega(G) \geq k$ nebo $\alpha(G) > k$.

Věta: (Vícebarevná verze R.V.)
$\forall b \in \mathbb{N}\ \forall k_1, k_2, \dots k_n \in \mathbb{N}\ \exists N_0(k_1, k_2, \dots, k_n) \in \mathbb{N}$ takové, že pro $\forall$ obarvení φ hran $K_{N_0(k_1,\dots,k_n)}$ pomocí barev $1, 2, 3, \dots, n$ $\exists$ barva $i \in \{1, \dots b\}$ takové, že v obarvení φ existuje úplný podgraf na k_i vrcholech, jehož všechny hrany mají barvu i.

Důkaz: Indukce podle b

$b=1$: $N_1(k_1) = k_1$

$b=2$: $N_2(k_1, k_2) = N(k_1, k_2)$ z předchozí věty

b barev $1, 2, \ldots, b$

$b \geq 3$ Volme $N := N_2(k_1, N_{k-1}(k_2, \ldots, k_b))$ Mějme obarvení K_N o b barvami: najdeme buď klikou velikosti k_1 v barvě 1, nebo klikou velikosti $N_{k-1}(k_2, \ldots, k_b)$ na níž jsou jen barvy $2, 3, \ldots b$ (pomocí indukce najdeme klikou velikosti k_i barvy i uvnitř kliky velikosti $N_{k-1}(k_2, \ldots k_b)$ obarvená $b-1$ barvami.

10. přednáška

Připomenutí: $\forall b \in \mathbb{N}\ \forall k_1, \ldots, k_b \in \mathbb{N}\ \exists N \in \mathbb{N}$ $\forall$ obarvení $\varphi(K_n) \to \{1, 2, \ldots, b\}$ $\exists$ barva $i \in \{1, \ldots, b\}$ $\exists$ úplný podgraf na k_i vrcholech jehož všechny hrany mají ve φ barvu i.

Důsledek: $\forall b \in \mathbb{N}\ \forall k \in \mathbb{N}\ \exists N\ \forall$ obarvení $\varphi: E(K_n) \to \{1, \ldots, b\}$ obsahuje úplný podgraf na k vrcholech, jehož hrany mají stejnou barvu.

Značení: $\binom{X}{p} :=$ množina p-prvkových podmnožin X

X množina
$p \in \mathbb{N}$

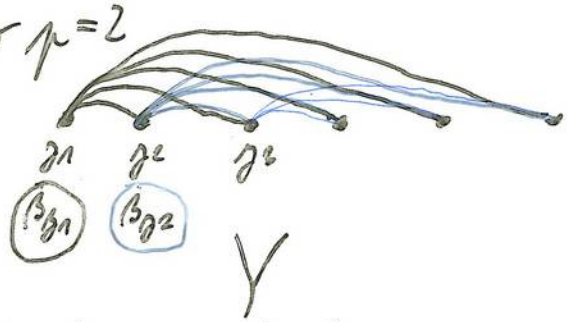
Pro obarvení $\varphi : \binom{X}{p} \to \{1, \dots, b\}$ řekneme, že $Y \subseteq X$ je homogenní ve φ, pokud všechny p-tice z $\binom{Y}{p}$ mají stejnou barvu, tj. $\exists i \in \{1, \dots, b\} \; \forall e \in \binom{Y}{p} : \varphi(e) = i$.

Věta : (Ramsey, konečná verze)
$\forall p \in \mathbb{N} \; \forall b \in \mathbb{N} \; \forall k \in \mathbb{N} \; \exists N \in \mathbb{N}$ a obarvení $\varphi : \binom{V}{p} \to \{1, \dots, b\}$, kde V je libovolná N-prvková množina vrcholů, $\exists$ homogenní $Y \subseteq V$. $|Y| = k$.

Věta : (Ramsey, nekonečná verze)
Nechť V je nekonečná spočetná množina vrcholů. Potom $\forall p \in \mathbb{N} \; \forall b \in \mathbb{N}$ a obarvení $\varphi : \binom{V}{p} \to \{1, \dots, b\}$ $\exists$ nekonečná homogenní množina $Y \subseteq V$.

Def : Nechť $V = \mathbb{N}$, mějme $\varphi : \binom{V}{p} \to \{1, \dots, b\}$. Řekneme, že množina $Y \subseteq V$ je skorohomogenní, pokud platí: $\forall y \in Y$ všechny p-tice z $\binom{Y}{p}$ jejichž nejmenší prvek je y mají stejnou barvu. Formálně: $\forall y \in Y \; \exists \beta_y \in \{1, \dots, b\} \; \forall e \in \binom{Y}{p}$: $\min(e) = y \Longrightarrow \varphi(e) = \beta_y$.

obrázek pro $p = 2$



Lemma : Každá nekonečná skorohomogenní množina Y obsahuje nekonečnou homogenní podmnožinu.

Důkaz : Mějme $b \in \mathbb{N}$, $V = \mathbb{N}$ a φ jako v definici skorohomogenní množiny. $\forall y \in Y$ máme β_y jako v definici. $\exists$ barva $i \in \{1, \dots, b\}$ taková, že $\beta_y = i$ pro nekonečně mnoho vrcholů $y \in Y$.

Definujeme $X := \{y \in Y, \beta_y = i\}$, potom X je nekonečná homogenní podmnožina Y.

V nekonečná spočetná množina $\Rightarrow \forall p \in \mathbb{N}\ \forall b \in \mathbb{N}\ \forall \varphi : \binom{V}{p} \to \{1, \dots, b\}$
$\exists$ nekonečná homogenní množina $Y \subseteq V$.

Důkaz: BÚNO $V = \mathbb{N}$. Indukcí podle p.

$p=1$: pro obarvení $\varphi : \binom{V}{1} \to \{1, \dots, b\}$ existuje barva $i \in \{1, \dots, b\}$ použitá nekonečně často.
Potom $Y := \{v \in V : \varphi(\{v\}) = i\}$ je nekonečná homogenní množina.

$p > 1$: předpokládáme, že věta platí pro barvení $\binom{V}{p-1} \to \{1, \dots, b\}$

$p=2$

Zvídám vrably, kteří nejsou obarveni barvou, která se vyskytuje nekonečně-krát. Z holubníkového principu určitě barva musí existovat.

$y_1 < y_2 < y_3 < y_4 < \dots$
β_1 β_2 β_3

$p=3$ Nějaká úleva oproti $p=2$

$p > 1$ Teď formálně: předpokládejme, že věta platí pro barvení $\binom{V}{p-1} \to \{1, \dots, b\}$
Nějak dáno $\varphi : \binom{V}{p} \to \{1, \dots, b\}$. Cíl: najít homogenní množinu $Y = \{y_1 < y_2 < y_3 < \dots\}$. Dokážeme, že lze najít posloupnost vrcholů $y_1 < y_2 < y_3 < \dots$, posloupnost barev $\beta_1, \beta_2, \beta_3, \dots \in \{1, \dots, b\}$ a posloupnost nekonečných množin $K_1 \supseteq K_2 \supseteq K_3 \supseteq \dots$ tak, že platí pro každé $n \geq 1$

1) y_n je menší než všechny prvky K_n
2) každá p^{-1}-tice vrcholů tak, že k y_n přidáme $p-1$ prvků K_n má barvu β_n
3) $\{y_{n+1}, y_{n+2}, \dots\} \subseteq K_n$

Indukcí: $K_0 = V$

Předpokládejme, že pro nějaké $n \geq 1$ už máme K_{n-1}, a že pro $n' \in \{1, \dots, n-1\}$ existují $y_{n'}, \beta_{n'}, K_{n'}$ dle podmínek 1) – 3). Ukážeme, jak najít y_n, β_n, K_n.

$y_n = \min K_{n-1}$

Definujeme pomocné obarvení $\tilde{\varphi}_n : \binom{K_{n-1} \setminus \{y_n\}}{p-1} \to \{1, \dots, b\}$

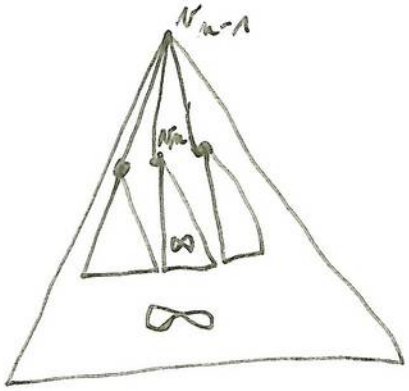
předpisem $\tilde{\varphi}_n(e) := \varphi(\{y_n\} \cup e)$

Dle indukce: $\tilde{\varphi}_n$ má nekonečnou homogenní podmnožinu $K_n \subseteq K_{n-1} \setminus \{y_n\}$ a každá $(p-1)$-tice $\binom{K_n}{p-1}$ má stejnou barvu $:= \beta_n$.

Každá $Y = \{y_1 < y_2 < \dots\}$ je skorohomogenní. $\overset{\text{lemma}}{\Longrightarrow}$
$\exists$ nekonečná homogenní $X \subseteq Y$ pro φ.

Věta: (Königovo lemma, 1927)
Nechť T je zakořeněný strom s nekonečně mnoha vrcholy, jehož každý vrchol má konečný stupeň. Potom T obsahuje nekonečnou cestu začínající v kořeni.

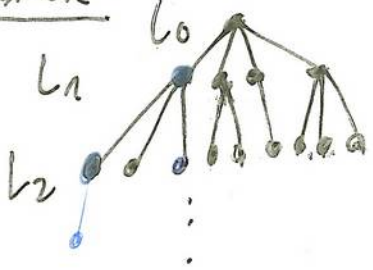
Důkaz: Definujme posloupnost vrcholů $v_0, v_1, v_2, \dots$ tak, že v_0 je kořen stromu T, $\forall n \geq 1$: v_{n-1} je rodič v_n, $\forall n \geq 0$: podstrom zakořeněný ve v_n má nekonečně mnoho vrcholů.
Postupujme indukcí podle $n \geq 0$. $v_0 = \text{kořen}(T)$.
Nechť máme vrcholy $v_0, v_1, \dots, v_{n-1}$: jako v_n zvolme takového potomka v_{n-1}, že jeho podstrom



má nekonečně mnoho vrcholů. Potom posloupnost $v_0, v_1, v_2, \dots$ tvoří hledanou cestu.

Tvrzení: Nechť G je graf na množině vrcholů $\{1,2,\dots\} = \mathbb{N}$. Pokud se dá každý konečný podgraf G obarvit b barvami, tak i G lze obarvit b barvami.

Důkaz:



L_k: všechna možná obarvení podgrafu G na vrcholech $1,2,\dots k$ tak, že $v_{k-1} \in L_{k-1}$ a $v_k \in L_k$ vede hrana, pokud obarvení v_k je rozšířením obarvení v_{k-1}.

11. přednáška

Opravné kódy

info: 10-10-11

kódování ↓

11011011 ⇝ 11111011

Příklad: Strojové opakování $0 \rightsquigarrow 000$, $1 \rightsquigarrow 111$

$\dots 000$

$\dots 001 \xrightarrow{\text{oprava}} 000$

je jasné, že došlo ke chybě

$C = \{000, 111\}$

$(3,1,3)$-kód

kontrola parity

$x_1, x_2, \dots, x_7 \in \{0,1\}$ $\quad C = \{x \in \mathbb{Z}_2^n : \|x\| \text{ je sudá}\}$

$(8,7,2)$-kód

$\downarrow$

$x_1, x_2, \dots, x_7, x_8$, kde $x_8 = x_1 + x_2 + \dots + x_7$ nad $\mathbb{Z}_2$

Omezíme se na:

1) binární kódy (nad $\mathbb{Z}_2$)
2) blokové kódy (mám "bloky" pevné délky $k \in \mathbb{N}$, kódují do "kódových slov" pevné délky $n \in \mathbb{N}$
3) chyby neměnící délku slov, příjemce nezná pozici chyb

Definice: slovo .... řádkový vektor nad $\mathbb{Z}_2$

Hammingova váha slova x, značená $\|x\|$ je počet nenulových symbolů v x (jedniček)

Hammingova vzdálenost slov x, y stejné délky, značená $d(x,y)$ je rovna $\|x-y\|$

Poznámka: $d(x,y)$ je metrika na $\mathbb{Z}_2^n$, tj.: $\forall x \in \mathbb{Z}_2^n : d(x,x) = 0$

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

$\forall x,y,z \in \mathbb{Z}_2^n : d(x,y) + d(y,z) \geq d(x,z)$

Definice: kód je podmnožina $\mathbb{Z}_2^n$ pro nějaké $n \in \mathbb{N}$. Prvky kódu jsou kódová slova.

Minimální vzdálenost kódu $\triangle(C) := \min\{d(x,y) : x,y \in C, x \neq y\}$

(n,k,d)-kód ... je kód $C \in \mathbb{Z}_2^n$, $|C| = 2^k$, $\triangle(C) = d$

kódování pro (n,k,d)-kód C, kde $k \in \mathbb{N}$ je bijekce

$$\mathcal{K} : \mathbb{Z}_2^k \longrightarrow C$$

dekódování (oprava chyb) pro (n,k,d)-kód C je funkce

(dokonce není jednoznačné) $\phi : \mathbb{Z}_2^n \longrightarrow C$ taková, že $d(x, \phi(x)) = \min_{y \in C} d(x,y)$

lineární kód: je vektorový podprostor $\mathbb{Z}_2^n$

$C = \{000, 111\} \subseteq \mathbb{Z}_2^3$ je lineární kód

$C = \{x \in \mathbb{Z}_2^8 : \|x\| \text{ sudá}\}$ je lineární kód

$\{x = (x_1, x_2, \dots, x_j) \in \mathbb{Z}_2^8 : x_1 + x_2 + \dots + x_8 = 0 \text{ nad } \mathbb{Z}_2\}$

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

Definice: Generující matice lineárního (n, k, d)-kódu C je matice typu $k \times n$ nad $\mathbb{Z}_2$, jejíž řádky tvoří bázi C. (není určena jednoznačně)

Příklad: $C = \{000, 111\}$ $G = 111$

$C = \{x \in \mathbb{Z}_2^8 : \|x\| \text{ sudá}\}$

$$G = \begin{pmatrix} 1000\,0001 \\ 0100\,0001 \\ 0010\,0001 \\ \vdots \\ 0000\,0001 \end{pmatrix} \qquad G = \begin{pmatrix} 110000\dots0 \\ 011000\dots0 \\ \vdots \\ 00\dots\dots011 \end{pmatrix}$$

Tvrzení: Nechť C je lineární (n, k, d)-kód s generující maticí G. Potom zobrazení π definované $\pi(y) = yG$ je kódování pro C.

Důkaz: Chceme π je bijekce $\mathbb{Z}_2^k \to C$. Nechť $b_1, b_2, \dots, b_k$ jsou řádky G ($y_j : b_1, \dots, b_k$ je báze C). Nechť $y = (y_1, \dots, y_k) \in \mathbb{Z}_2^k$ je libovolný. Potom $\pi(y) = yG = y_1 b_1 + y_2 b_2 + \dots + y_k b_k$.

$\mathbb{Z}_2 \quad \mathbb{Z}_2^n$

Jistě yG je v C, protože yG je lineární kombinace báze C.

Navíc π je prosté: pokud $\pi(y)=\pi(y')$ tak $y_1b_1+y_2b_2+\dots+y_kb_k=y'_1b_1+\dots+y'_kb_k$

tj. $(y_1-y'_1)b_1+(y_2-y'_2)b_2+\dots+(y_k-y'_k)b_k=0$

tj. $y=y'$ ■

Příklad: $y=(y_1y_2\dots y_k)$

$G=111$ $\quad yG_1=(y_1,y_2,y_3,\dots,y_7,y_1+y_2+\dots+y_7)$

$0\to000$ $\quad yG_2=(y_1,y_1+y_2,y_2+y_3,\dots,y_6+y_7,y_7)$

$1\to111$

Def: Pro $x=(x_1,\dots,x_n)\in\mathbb{Z}_2^n$ a $y=(y_1,\dots,y_n)\in\mathbb{Z}_2^n$ definuji skalárním součinem nad $\mathbb{Z}_2$ ($\forall x,y:\langle x,y\rangle\in\{0,1\}$) $\langle x,y\rangle := x_1y_1+x_2y_2+\dots+x_ny_n=xy^T$

x a y jsou ortogonální, pokud $\langle x,y\rangle=0$

⚠ může existovat vektor $x\neq0$ pro nějž $\langle x,x\rangle=0$.

Pro množinu $C\subseteq\mathbb{Z}_2^n$ definuji ortogonální doplněk $C^\perp$ jako

$$C^\perp:=\{x\in\mathbb{Z}_2^n:\forall y\in C:\langle x,y\rangle=0\}$$

Fakt: 1) $\forall C\in\mathbb{Z}_2^n$: $C^\perp$ je vektorový podprostor $\mathbb{Z}_2^n$

2) Pokud C je podprostor $\mathbb{Z}_2^n$ dimenze k, tak $C^\perp$ má dimenzi $n-k$

3) Pokud C je podprostor, tak $(C^\perp)^\perp=C$

Def: **Kontrolní matice** lineárního kódu (n,k,d)-kódu C je matice typu $(n-k)\times n$ nad $\mathbb{Z}_2$, jejíž řádky tvoří bázi $C^\perp$.

Příklad: $C=\{000,111\}\subseteq\mathbb{Z}_2^3$

$C^\perp=\{000,101,110,011\}$

kontrolní matice C (= generující matice $C^\perp$) je třeba $\begin{pmatrix}101\\110\end{pmatrix}$

$C=\{x\in\mathbb{Z}_2^8 : \|x\| \text{ sudá}\}$

$C^\perp=\{0,11\ldots1\}$

kontrolní matice C: 11111111

Tvrzení: Nechť K je kontrolní matice lin. (n,k,d)-kódu C. Potom pro $x\in\mathbb{Z}_2^n$ platí $x\in C \iff Kx^T=0$

Důkaz: Nechť $b'_1,\ldots b'_{n-k}$ jsou řádky kontrolní matice K.

Tj. $b'_1,\ldots,b'_{n-k}$ je báze $C^\perp$. Potom $Kx^T=0 \iff \forall i=1,\ldots,n-k$ ($b'_i x^T=0$, $b'_i\in\mathbb{Z}_2^{n-k}$)

$b'_i x^T=0 \iff \forall i=1,\ldots,n-k : \langle b'_i, x\rangle=0 \iff$

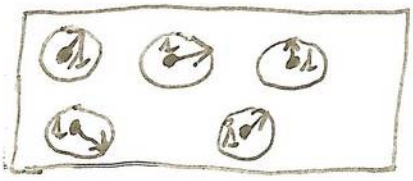
$\forall y\in C^\perp : \langle y,x\rangle=0 \iff x\in(C^\perp)^\perp \iff x\in C$

$$Kx^T=0 \iff \boxed{\begin{matrix}x_1+x_3=0\\x_1+x_2=0\end{matrix}} \quad \text{nad } \mathbb{Z}_2$$

11. přednáška

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

Def: Kód $C \in \mathbb{Z}_2^n$ *opravuje* t *násobné chyby*, pokud $\forall \hat{x} \in \mathbb{Z}_2^n$ existuje nejvýše jedno $x \in C$ takové, že $d(\hat{x}, x) \leq t$



Kód C opravuje t-násobné chyby $\iff \Delta(C) \geq 2t+1$

Lemma: Pokud C je lineární kód, pak

$$\Delta(C) = \min_{x \in C \setminus \{\phi\}} d(\phi, x) = \min_{x \in C \setminus \{\phi\}} \|x\|$$

Důkaz: Jistě $\forall x \in C \setminus \{\phi\}: \Delta(C) \leq d(\phi, x)$
Nechť $x, y \in C$ splní $d(x,y) = \Delta(C)$. Potom
$d(x,y) = d(\phi, x-y)$ a $x-y \in C$, tedy
$\Delta(C) \geq \min_{z \in C \setminus \{\phi\}} \|z\|$.

Připomeňme: kontrolní matice lineárního kódu C je matice K, jejíž řádky tvoří báze $C^\perp$.

Platí: $\forall x \in \mathbb{Z}_2^n: x \in C \iff Kx^T = 0$

Lemma: Nechť C je lineární kód s kontrolní maticí K. Potom $\Delta(C)$ je nejmenší kladné číslo d takové, že K má alespoň d sloupců, jejichž součet je 0.

Důkaz:
$$\Delta(C) := \min_{x \in C \setminus \{\phi\}} \|x\| = \min_{x \neq \phi} \{\|x\|, Kx^T = 0\} \iff$$

(pravé Kx^T je součet $\|x\|$ sloupců z K.)

$$= \min\{d;\ K \text{ obsahuje } d \text{ sloupců, jejichž součet je } 0\}$$

$K = (s_1, s_2, \dots, s_n) \in \mathbb{Z}_2^{m \times n}$

$x = (x_1, \dots, x_n) \in \mathbb{Z}_2^n$

$Kx^T = x_1 \cdot \underbrace{s_1}_{\mathbb{Z}_2^m} + x_2 \cdot s_2 + \dots + x_n s_n = \sum_{\substack{i=1 \\ x_i = 1}}^{n} s_i$

Důsledek: Pro lineární kód C s kontrolní maticí K platí:

1) $\Delta(C) \geq 2 \iff K$ neobsahuje nulový sloupec

2) $\Delta(C) \geq 3 \iff K$ neobsahuje nulový sloupec ani dva stejné sloupce

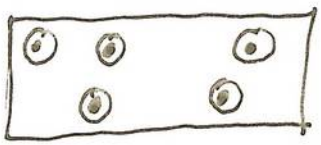
Def: Pro $m \geq 2$, *Hammingův kód* řádu m je kód, jehož kontrolní matice má jako sloupce všechny různé nenulové vektory délky m.

H_2: $K = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \Longrightarrow H_2 = \{x \in \mathbb{Z}_2^3 : Kx^T = 0\} = \{x = (x_1, x_2, x_3) \in \mathbb{Z}_2^3 : \begin{matrix} x_2 + x_3 = 0 \\ x_1 + x_3 = 0 \end{matrix}\}$

$= \{(000), (111)\}$

H_3: $K = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$: H_3 je $(7, 4, 3)$-kód

H_m je (n, k, d)-kód, kde $n = 2^m - 1$, $k = n - m = 2^m - 1 - m$, $d = 3$.



$C \subseteq \mathbb{Z}_2^n$

Tvrzení: Nechť $H_m \subseteq \mathbb{Z}_2^n$ je Hammingův kód řádu m (a tedy $n = 2^m - 1$). Potom $\forall \tilde{x} \in \mathbb{Z}_2^n \; \exists! \, x \in H_m : d(x, \tilde{x}) \leq 1$.

Důkaz: Jistě pro dané $\tilde{x}$ existuje nejvýše 1 kódové slovo splňující $d(x, \tilde{x}) \leq 1$, protože $\Delta(H_m) = 3$. Dokážeme, že pro $\tilde{x} \in \mathbb{Z}_2^n$ $\exists x \in H_m : d(x, \tilde{x}) \leq 1$.

Nechť K je kontrolní matice H_m, označme $s^T := K\tilde{x}^T$ $(s \in \mathbb{Z}_2^m)$ (syndromový vektor)

Pokud $s = \emptyset$, tak $\tilde{x} \in H_m$, beřme $x := \tilde{x}$. ✓

Předpokládejme $s \neq \phi$. Nechť s^T je rovno i-tému sloupci K.
Nechť $e_i \in \mathbb{Z}_2^n$ je slovo, jehož i-tá složka je 1, ostatní složky jsou 0.
Definujme $x := \tilde{x} + e_i$. Vidím, že $x \in H_m$: to platí, protože

$$Kx^T = K(\tilde{x}^T + e_i^T) = K\tilde{x}^T + Ke_i^T = s^T + s^T = 0$$

Př: $\tilde{x} = 1011101$

$K\tilde{x} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ (v kontrolní matici se tento vektor vyskytuje ve 4. sloupci)
$i = 4$

$x = 1010101 \in K_i$

Tvrzení: (Singletonův odhad)
Pro každý (n,k,d)-kód C platí $k + d \leq n + 1$

Důkaz: Pro slovo $x = (x_1, \dots, x_n) \in C$ definujme "zkrácení x"
jako $\rho(x) := (x_1, x_2, \dots, x_{n-d+1}) \in \mathbb{Z}_2^{n-d+1}$
Pro $x, y \in C$, $x \neq y$, platí $d(x,y) \geq d$, tedy $\rho(x) \neq \rho(y)$.
Tedy $\rho : C \to \mathbb{Z}_2^{n-d+1}$ je prosté, takže $|C| \leq |\mathbb{Z}_2^{n-d+1}|$, tj.
$k \leq n - d + 1$

Značení: $s \in \mathbb{Z}_2^n$, $\Delta \in \{0, \dots, n\}$

$B_n(s, \Delta) := \{x \in \mathbb{Z}_2^n : d(s,x) \leq \Delta\}$ (B-ball)

$V_n(\Delta) := |B_n(s, \Delta)|$ (V-volume)

Vidíme: $V_n(\Delta) = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{\Delta}$

Tvrzení: (Hammingův odhad)
Pro každý (n,k,d)-kód C platí $|C| \leq \frac{2^n}{V_n(\lfloor \frac{d-1}{2} \rfloor)}$
Tj. $k = \log_2 |C| \leq n - \log_2(V_n(\lfloor \frac{d-1}{2} \rfloor))$.

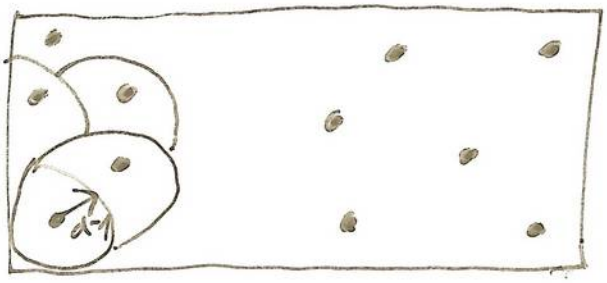
Důkaz: Pro každé $x, y \in C$, $x \neq y$ platí $B_n(x, \lfloor \frac{d-1}{2} \rfloor) \cap B_n(y, \lfloor \frac{d-1}{2} \rfloor) = \emptyset$

Tudíž $2^n = |\mathbb{Z}_2^n| \geq \left| \bigcup_{x \in C} B_n(x, \lfloor \frac{d-1}{2} \rfloor) \right| = |C| \cdot V_n(\lfloor \frac{d-1}{2} \rfloor)$

Tvrzení: (Gilbert-Varšamovův odhad)
Pro každé $n \in \mathbb{N}$ a každé $d \in \{1, \dots, n\}$ existuje (n, k, d)-kód C splňující $|C| \geq \frac{2^n}{V_n(d-1)}$

$\left(\text{Tj. } k \geq n - \log_2(V_n(d-1))\right)$

Důkaz: Nechť C je co největší (n, k, d)-kód pro nějaké k.
Tvrdím: každé $x \in \mathbb{Z}_2^n$ je ve vzdálenosti nejvýše $d-1$ od nějakého $y \in C$ (jinak by $C \cup \{x\}$ byl větší (n, k, d)-kód než C). Tudíž $\bigcup_{y \in C} B_n(y, d-1) = \mathbb{Z}_2^n$. Tedy $2^n = |\mathbb{Z}_2^n| = \left| \bigcup_{y \in C} B_n(y, d-1) \right| \leq |C| \cdot V_n(d-1)$.



(Skladově přidáváním vektorů)