Kombinatorika a Grafy I

poznámky z přednášky

Tomáš Sláma
2. 1. 2021

Toto PDF bylo automaticky vygenerováno z webové stránky https://slama.dev/kombinatorika-a-grafy-i, která je preferovaný způsob jak dokument číst. Za případné chyby způsobené převodem se omlouvám.

Obsah

Úvodní informace

Tato stránka obsahuje moje poznámky z přednášky Martina Kouteckého z akademického roku 2020/2021. Pokud by byla někde chyba/nejasnost, nebo byste rádi někam přidali obrázek/text, tak stránku můžete upravit pull requestem (případně mi dejte vědět na mail.

1. přednáška

Odhady faktoriálu

Věta (meh odhad)

$$n^{n/2} \leq n! \leq \left(\frac{n+1}{2}\right)^n$$

Důkaz ($\geq$)

$$\begin{aligned}(n!)^2 &= 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n \cdot n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 \\ &= \prod_{i=1}^{n} (i \cdot (n-i+1))\end{aligned}$$

Využijeme A-G nerovnost:

$$\sqrt{ab} \leq \frac{a+b}{2}$$

$$\sqrt{i(n+1-i)} \leq \frac{i+n+1-i}{2} = \frac{n+1}{2}$$

Dostáváme:

$$n! = \prod_{i=1}^{n} \sqrt{i \cdot (n-i+1)} \leq \left(\frac{n+1}{2}\right)^n$$

Důkaz ($\leq$) $n \leq i(n-i+1), \forall i \in [n]$:

- $i = 1$ platí
- $i = 2 \rightarrow$ jeden člen je vždy ≥ 2, druhý $\geq n/2$

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

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

Věta (nice odhad)

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

Důkaz (indukcí)

- $n = 1$:

$$1 \leq e \cdot 1 \cdot \frac{1}{e}$$

- $n - 1 \rightarrow n$:

$$\begin{aligned}n! = n\,(n-1)! &\leq^{\text{IP}} en\,(n-1)\left(\frac{n-1}{e}\right)^{n-1} \\ &= en\left(\frac{n}{e}\right)^n \left(\frac{e}{n}\right)^n (n-1)\left(\frac{n-1}{e}\right)^{n-1} \\ &= en\left(\frac{n}{e}\right)^n \underbrace{\left(\frac{n-1}{n}\right)^n}_{\leq 1} e\end{aligned}$$

Důkaz, toho proč ten výraz ≤ 1:

$$\left(1-\frac{1}{n}\right)^n e \leq \left(e^{-\frac{1}{n}}\right)^n e = e^{-1}e = 1 \qquad 1+x \leq e^x$$

- pozn.: $a \leq b \implies a = bc$ pro $c \leq 1$, proto to vlastně děláme
- pro dolní mez postupujeme podobně, ale je potřeba indukční krok dokazovat pro $n \to n+1$, místo $n-1 \to n$.

Věta (Stirlingova formule)

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

Odhady binomických koeficientů

(👀): pro malé $k << n \ldots \binom{n}{k} = \frac{n!}{(n-k)!k!} = \frac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{k!} \leq n^k$

Věta (hodně meh odhad)

$$\frac{2^n}{n+1} \leq \binom{n}{\lfloor n/2 \rfloor} \leq 2^n$$

Důkaz:

- součet všech čísel v řádku je 2^n, tak jistě to největší nebude větší
- největší sčítanec je rovněž alespoň tak velký jako průměrný

Věta (nice odhad)

$$\frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}$$

Důkaz: Nejprve jedno kouzlo:

$$P = \frac{1\cdot 3\cdot 5\cdot \ldots \cdot (2m-1)}{2\cdot 4\cdot 6\cdot \ldots \cdot 2m} = \frac{1\cdot 3\cdot 5\cdot \ldots \cdot (2m-1)}{2\cdot 4\cdot 6\cdot \ldots \cdot 2m}\frac{2\cdot 4\cdot 6\cdot \ldots \cdot 2m}{2\cdot 4\cdot 6\cdot \ldots \cdot 2m} = \frac{(2m)!}{2^{2m}\left(m!\right)^2} = \frac{\binom{2m}{m}}{2^{2m}}$$

Chceme tedy:

$$\frac{1}{2\sqrt{m}} \leq P \leq \frac{1}{\sqrt{2m}}$$

Pak ještě druhé kouzlo:

$$\begin{aligned}\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{4^2}\right)\ldots\left(1-\frac{1}{(2m)^2}\right) &= \left(\frac{1\cdot 3}{2\cdot 2}\right)\left(\frac{3\cdot 5}{4\cdot 4}\right)\ldots\left(\frac{(2m-1)(2m+1)}{(2m)^2}\right)\\ &= P^2(2m+1) < 1 \qquad \text{// součin věcí} < 1\end{aligned}$$

Máme tedy:

$$\begin{aligned}P^2 &< \frac{1}{2m+1} < \frac{1}{2m}\\ P &< \frac{1}{\sqrt{2m}}\end{aligned}$$

Druhá strana analogicky (uvažujeme $\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{5^2}\right)\ldots = \left(\frac{2\cdot 4}{3^2}\right)\left(\frac{4\cdot 6}{5^2}\right)\ldots = \frac{1}{2(2m)P^2}$).

2. přednáška

Náhodné procházky

Definice (náhodná procházka) Náhodný proces, v každém kroku se panáček začínající v bodu 0 posune ze své aktuální pozice doprava nebo doleva.

- kde bude po n krocích?
- $\lim_{n\to\infty} \ldots$ že se po n krocích vrátil (někdy v průběhu) do počátku?
- $\lim_{n\to\infty} \ldots$ $\mathbb{E}$[#návratů do počátku]?
  - dokážeme, že jde k nekonečnu

Zadefinujeme si náhodnou veličinu $X = I_{S_2} + I_{S_4} + \ldots + I_{S_{2n}}$:

- $I_{S_{2n}} \ldots$ indikátor, že nastal jev „po $2n$ krocích jsem v počátku“
- $\mathbb{E}[X] = \mathbb{E}$[#návratů do počátku].
- Pr[po $2n$ krocích jsem v počátku] $= \binom{2n}{n}/2^{2n}$.
  - nahoře jsou možnosti vyrovnaných počtů kroků doprava/doleva
  - dole jsou všechny scénáře pro $2n$ kroků

$$\frac{\binom{2n}{n}}{2^{2n}} \geq \frac{\frac{2^{2n}}{2\sqrt{n}}}{2^{2n}} = \frac{1}{2\sqrt{n}}$$

$$\begin{aligned}
\mathbb{E}[X] &= \mathbb{E}\left[\sum_{i=1}^{\infty} I_{S_{2i}}\right] \\
&= \sum_{i=1}^{\infty} \mathbb{E}\left[I_{S_{2i}}\right] && \text{// linearita střední hodnoty} \\
&= \sum_{i=1}^{\infty} \Pr\left[I_{S_{2i}}\right] && \text{// střední hodnota indikátoru je pravděpodobnost} \\
&\geq \sum_{i=1}^{\infty} \frac{1}{2\sqrt{i}} && \text{// použití odhadu výše; diverguje}
\end{aligned}$$

- zajímavost: ve $2D$ to také platí, ale ve $3D$ už ne (konverguje k nějakému konstantnímu číslu)!

Generující funkce

Definice (mocninná řada) je nekonečná řada tvaru $a(x) = a_0 + a_1x^1 + a_2x^2 + \ldots$, kde $a_0, a_1 \ldots \in \mathbb{R}$.

Příklad: $a_0 = a_1 = \ldots = 1 \mapsto 1 + x + x^2 + \ldots$

- pro $|x| < 1$ řada konverguje k $\frac{1}{1-x}$, můžeme tedy říct, že $(1, 1, \ldots) \approx \frac{1}{1-x}$

Tvrzení: $(a_0, a_1, a_2, \ldots)$ reálná čísla. Předpoklad: pro nějaké K t. ž. $|a_n| \leq K^n$. Poté řada $a(x)$ pro každé $x \in \left(-\frac{1}{K}, \frac{1}{K}\right)$ konverguje (dává smysl). Funkce $a(x)$ je navíc jednoznačně určena hodnotami na okolí 0.

Definice (vytvořující/generující funkce) nechť $(a_0, a_1, \ldots)$ je posloupnost reálných čísel. Vytvořující funkce této posloupnosti je mocninná řada $a(x) = \sum_{i=0}^{\infty} a_i x^i$.

operace	řada	úprava
součet	$a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots$	$a(x) + b(x)$
násobek	$\alpha a_0, \alpha a_1, \alpha a_2, \ldots$	$\alpha a(x)$
posun doprava	$0, a_0, a_1, \ldots$	$xa(x)$
posun doleva	$a_1, a_2, a_3, \ldots$	$\frac{a(x)-a_0}{x}$
substituce αx	$a_0, \alpha a_1, \alpha^2 a_2, \ldots$	$a(\alpha x)$

operace	řada	úprava
substituce x^n	$a_0, 0, \overset{n-1}{\ldots}, 0, a_1, 0, \overset{n-1}{\ldots}, 0, a_2, \ldots$	$a(x^n)$
derivace	$a_1, 2a_2, 3a_3, \ldots$	$a'(x)$
integrování	$0, a_1, a_2/2, a_3/3, \ldots$	$\int_0^x a(t)dt$
konvoluce	$\sum_{k=0}^{n} a_k \cdot b_{n-k}$	$a(x) \cdot b(x)$

Všechny důkazy jsou jednoduché rozepsání z definice.

Zobecněná binomická věta

Tvrzení: $r \in \mathbb{R}, k \in \mathbb{N}$, def. $\binom{r}{k} = \frac{r \cdot (r-1) \cdot (r-2) \cdot \ldots \cdot (r-k+1)}{k!}$

- pro $r \in \mathbb{N}$ se shoduje s tím, co už známe
- vyplývá z toho, že funkce $(1+x)^r$ je vytvořující funkcí posloupnosti $\left(\binom{r}{0}, \binom{r}{1}, \binom{r}{2}, \ldots\right)$
- (👀)**:** pokud r je záporné celé, pak $\binom{r}{k} = (-1)^k \binom{-r+k-1}{k} = (-1)^k \binom{-r+k-1}{-r-1}$, tedy $\frac{1}{(1-x)^n} = (1-x)^{-n} = \binom{n-1}{n-1} + \binom{n}{n-1}x + \binom{n+1}{n-1}x^2 + \ldots$

Příklad: V krabici je 30 červených, 40 žlutých a 50 zelených míčků. Kolika způsoby lze vybrat 70?

$$
\begin{aligned}
&(1 + x + \ldots + x^{30})(1 + x + \ldots + x^{40})(1 + x + \ldots + x^{50}) = \\
&= \frac{1 - x^{31}}{1 - x} \frac{1 - x^{41}}{1 - x} \frac{1 - x^{51}}{1 - x} \qquad \text{// posuneme o 31 míst a odečteme} \\
&= \frac{1}{(1-x)^3} \left(1 - x^{31}\right) \left(1 - x^{41}\right) \left(1 - x^{51}\right) \\
&= \left(\binom{2}{2} + \binom{3}{2} x + \binom{4}{2} x^2 + \ldots \right) \left(1 - x^{31}\right) \left(1 - x^{41}\right) \left(1 - x^{51}\right) \\
&= 1 + \ldots + \left[\binom{72}{2} - \binom{72-31}{2} - \binom{72-41}{2} - \binom{72-51}{2} \right] x^{70} + \ldots \\
&= 1061
\end{aligned}
$$

Kde poslední rovnost platí, protože:

- z posledních 3 závorek si vybereme 1 a z první závorky koeficient u 70
- ze druhé x^{31} a z první koeficient u $72 - 31$
  - analogicky pro 41 a 51 ze třetí a čtvrté

3. přednáška

Fibonacciho čísla

Definice: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}, \forall n \geq 2$

- $F(x) = F_0 + F_1 x + F_2 x^2 + F_3 x^3$

F_0	F_1	F_2	F_3	F_4	Vytvořující funkce
0	1	$F_0 + F_1$	$F_1 + F_2$	$F_2 + F_3$	$F(x)$
0	0	F_1	F_2	F_3	$xF(x)$
0	0	F_0	F_1	F_2	$x^2F(x)$
0	1	0	0	0	x

Algebraickou úpravou dostáváme:

$$\begin{aligned}
F(x) &= \frac{x}{1-x-x^2} \\
&= \frac{x}{\left(1-\frac{1+\sqrt{5}}{2}x\right)\left(1-\frac{1-\sqrt{5}}{2}x\right)} && \text{// algebra} \\
&= \frac{\frac{1}{\sqrt{5}}}{1-\frac{1+\sqrt{5}}{2}x} - \frac{\frac{1}{\sqrt{5}}}{1-\frac{1-\sqrt{5}}{2}x} && \text{// parciální zlomky} \\
&= \frac{1}{\sqrt{5}}\left(\frac{1}{1-\frac{1+\sqrt{5}}{2}x} - \frac{1}{1-\frac{1-\sqrt{5}}{2}x}\right) && \text{// tvary } \frac{\pm 1}{1-\lambda_{1,2}x}
\end{aligned}$$

Pro daný koeficient vytvořující funkce tedy máme:

$$\begin{aligned}
F_n &= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \underbrace{\left(\frac{1-\sqrt{5}}{2}\right)^n}_{\text{jde k 0}}\right] \\
&= \left\lfloor \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n \right\rfloor
\end{aligned}$$

Catalanova čísla

- b_n = počet binárních zakořeněných stromů na n vrcholech
  - $b_n = \sum_{k=0}^{n-1} b_k \cdot b_{n-k+1}$, rekurzíme se na obě části
  - jde si rozmyslet[1], že $b(x) = x \cdot b(x) \cdot b(x) + 1$
    - x je tam kvůli posunu, aby vycházelo správně indexování (suma nejde do n)
    - 1 je tam kvůli tomu, aby nultý člen správně vycházel

[1] Rekurence pro b_n vypadá skoro jako konvoluce sama sebe, takže by se nám líbilo něco jako $b(x) = b(x)^2$. Jenže narozdíl od konvoluce pronásobujeme jen prvních $n-1$ prvků. Uvažme tedy posloupnost $0, b_0, b_1, b_2, \ldots$ generovanou funkcí $xb(x)$. Ta je již skoro konvolucí sama sebe – n-tý prvek se v sumě požere s nulou. Jediná nepřesnost je u b_0, protože podle definice konvoluce $b_0 = 0 \cdot b_0 + b_0 \cdot 0 = 0$, ale my víme $b_0 = 1$. Stačí tedy přičíst jedničku posunutou o jedna doprava, čímž dostaneme $xb(x) = (xb(x))^2 + x$. Jinými slovy $b(x) = xb(x)^2 + 1$.

$$
\begin{aligned}
b(x) &= x \cdot b(x)^2 + 1 \\
b(x)_{1,2} &= \frac{1 \pm \sqrt{1-4x}}{2x} \qquad \text{// ten s + nedává smysl, diverguje}
\end{aligned}
$$

$$
\begin{aligned}
b(x) &= \frac{1 - 1 - \sum_{k=1}^{\infty} (-4)^k \binom{1/2}{k} x^k}{2x} \qquad \text{// } \sqrt{1-4k} \overset{\text{ZBV}}{=} \sum_{k=0}^{\infty} (-4)^k \binom{1/2}{k} x^k \\
&= -\frac{1}{2} \sum_{k=1}^{\infty} (-4)^k \binom{1/2}{k} x^{k-1}
\end{aligned}
$$

$$
\begin{aligned}
b_n &= -\frac{1}{2}(-4)^{n+1} \binom{1/2}{n+1} \qquad \text{// konkrétní koeficient} \\
&= \frac{1}{2}(-1)^n 2^{2n+2} \frac{\frac{1}{2} \cdot \left(\frac{1}{2} - 1\right) \cdot \overset{n+1}{\cdots} \cdot \left(\frac{1}{2} - n\right)}{(n+1)!} \\
&= \frac{1}{2}(-1)^n 2^{2n+2} \frac{\frac{1}{2} \cdot \left(-\frac{1}{2}\right) \cdot \overset{n+1}{\cdots} \cdot \left(-\frac{2n-1}{2}\right)}{(n+1)!} \\
&= \frac{1}{2} 2^{2n+2} \frac{\frac{1}{2} \cdot \frac{1}{2} \cdot \ldots \cdot \frac{2n-1}{2}}{(n+1)!} \qquad \text{// krácení záporných čísel} \\
&= 2^n \frac{1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1)}{(n+1)!} \cdot \frac{n!}{n!} \qquad \text{// krácení 2} \\
&= \frac{1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1)}{(n+1)n!} \cdot \frac{2 \cdot 4 \cdot 6 \cdot \ldots \cdot 2n}{n!} \qquad \text{// rozdistribuování 2} \\
&= \frac{1}{n+1} \frac{(2n)!}{(n!)^2} \\
&= \frac{1}{n+1} \binom{2n}{n}
\end{aligned}
$$

Konečné projektivní roviny

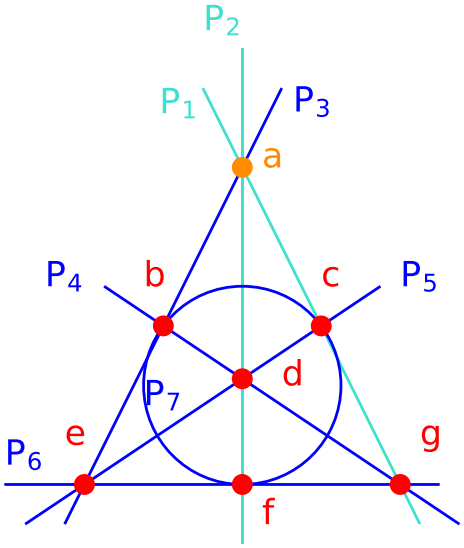
Definice (KPR) Nechť X je konečná množina, $\mathcal{P}$ systém podmnožin množiny X. $(X, \mathcal{P})$ je KPR pokud: [2]

1. Existuje $\mathcal{C} \subseteq X, |\mathcal{C}| = 4$ t. ž. $\forall P \in \mathcal{P} : |P \cap \mathcal{C}| \leq 2$
   - „každá přímka obsahuje ≤ 2 body z $\mathcal{C}$“
2. $\forall P, Q \in \mathcal{P}, P \neq Q : \exists! x \in X$ t. ž. $P \cap Q = \{x\}$
   - „každé dvě přímky se protínají právě v 1 bodě“
3. $\forall x, y \in X, x \neq y \exists! P \in \mathcal{P}$ t. ž. $x, y \in \mathcal{P}$
   - „každé dva body určují právě 1 přímku“

- $x \in X$ je bod
- $P \in \mathcal{P}$ je přímka

Příklad (Fanova rovina)

[2] První axiom zajišťuje netrivialitu. Není těžké si rozmyslet, že lze nahradit axiomem *“Existují alespoň 2 různé přímky, z nichž každá má alespoň 3 body”*. Bez některé z těchto podmínek by definici vyhovovala např. libovolně velká množina bodů s právě jednou přímkou, která by všechny body spojovala. Případně by k tomuto schématu šel přidat ještě jeden bod, který by s každým dalším byl spojen dvoubodovou přímkou.



$$X = \{a, b, c, d, e, f, g\}$$

$$P = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\} = \{\{a, c, g\}, \{a, d, f\}, \{a, b, e\}, \{b, d, g\}, \{c, d, e\}, \{e, f, g\}, \{b, c, f\}\}$$

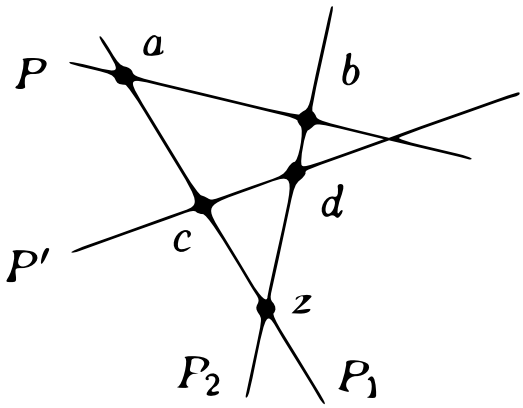
Počet bodů a přímek

Tvrzení: „v KPR mají všechny přímky stejný počet bodů“

Pomocné tvrzení: $\forall P, P' \in \mathcal{P} \exists z \in X$, které neleží ani na jedné z nich.

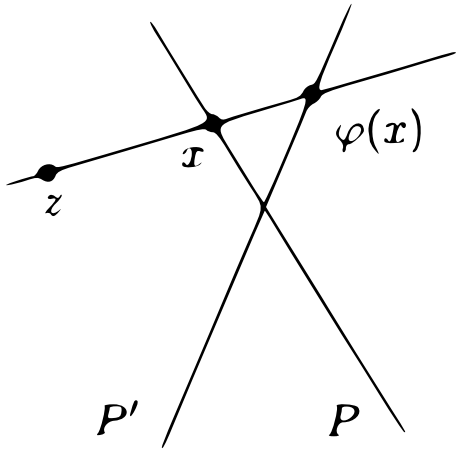
Dokáže se přes to přes rozbor příkladů toho, jak vedou přímky přes $\mathcal{C}$:

- pokud nevedou přes všechny body z $\mathcal{C}$, pak máme vyhráno
- pokud vedou, tak existují dvě další přímky P_1 a P_2 vedoucí kolmo na naše přímky, jejich průnik je hledaný bod; původní přímky jím vést nemohou, protože pak by dvě přímky sdílely 2 body, což nelze
- $P_1 \neq P$, protože pak by P obsahovala alespoň 3 body z $\mathcal{C}$. Podobně ostatní nerovnosti.



4. přednáška

Důkaz původního tvrzení: pro přímky P, P' a bod z (který nesdílí) budeme dělat bijekci tak, že budu tvořit přímky z bodu z na body z P, které budou rovněž protínat body z P'.



Definice (řád KPR) řádem $(X, \mathcal{P})$ je $n = |P| - 1$ pro jakoukoliv $P \in \mathcal{P}$.

Tvrzení: nechť $(X, \mathcal{P})$ je KPR řádu n. Pak:

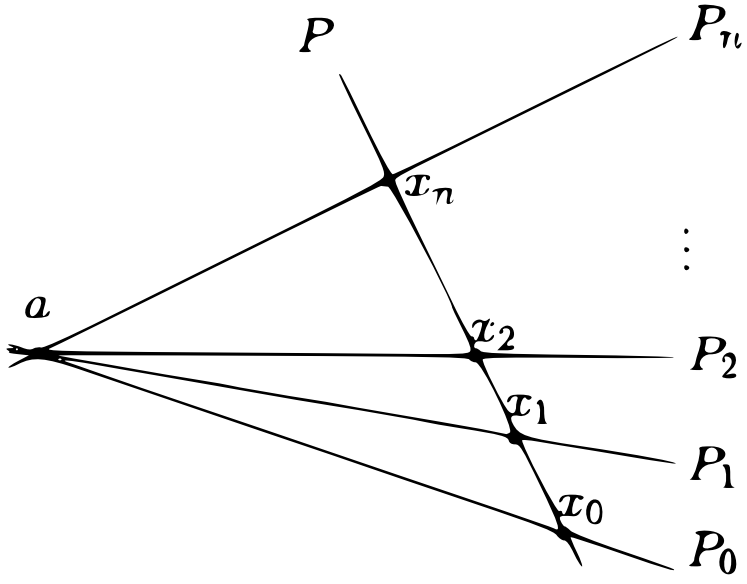
1. každým bodem prochází $n + 1$ přímek
2. $|X| = n^2 + n + 1$
3. $|\mathcal{P}| = n^2 + n + 1$

Důkaz:

1. triviálně z definice. 2. viz. níže. 3. vychází z duality (viz. další kapitola).

Vezměme libovolné $x \in X$. Pak $\exists P \in \mathcal{P} : x \notin P$, protože vezmeme-li body $a, b, c \in \mathcal{C}$, pak přímky ab a ac nemohou mít další společný bod než a (došlo by ke sporu s některým z axiomů). [3]

Poté stačí uvážit následující obrázek a spočítat body/přímky. Další bod už neexistuje, protože kdyby existoval, tak by jím musela procházet přímka z x a ta by rovněž někde protínala P (a nesplňovala tak axiomy).



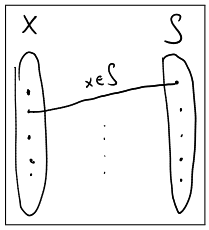
Bodů na obrázku je $\overbrace{1}^{x} + \underbrace{(n+1)}_{P_0 \ldots P_n} \overbrace{n}^{\text{body } P_i, \text{ bez } x} = n^2 + n + 1.$

[3] Explicitní důkaz (3): Pro každý bod započítejme všechny přímky jím procházející. Dostaneme tak $(n^2 + n + 1)(n + 1)$ přímek. Ale každou jsme započítali $(n + 1)$-krát – jednou pro každý z jejích bodů.

Dualita KPR

Definice (incidenční graf) nechť $(X, \mathcal{S})$ je množinový systém ($\mathcal{S} \subseteq 2^X$). Jeho incidenční graf je bipartitní graf

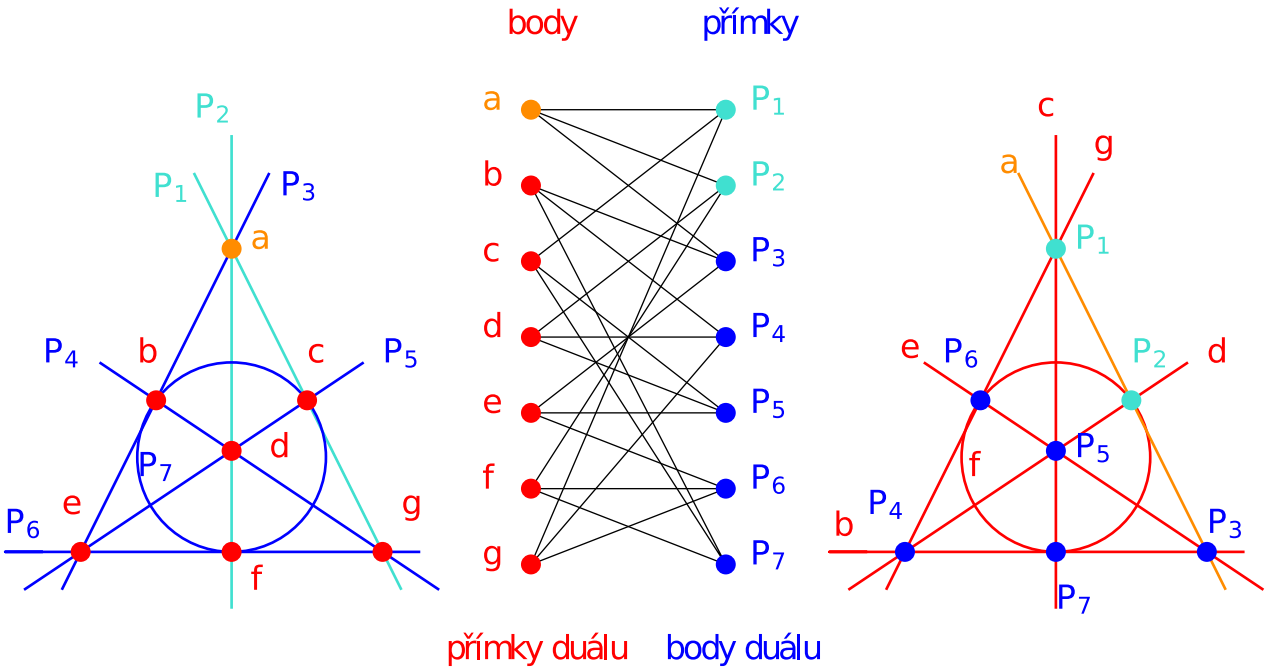
$$(V = X \cup \mathcal{S}, E = \{(x, s) \in X \times \mathcal{S} \mid x \in s\})$$



Definice (duál grafu) $(Y, \mathcal{T})$ je duál $(X, \mathcal{S})$ pokud $Y = \mathcal{S}$ a $\mathcal{T} = \{\{s \in \mathcal{S} \mid x \in s\} \mid x \in X\}$

- **(👀):** incidenční graf $(Y, \mathcal{T})$ je incidenční graf $(X, \mathcal{S})$ s prohozením stran

Příklad (duál Fanovy roviny)



Věta: duál KPR je KPR.

Důkaz: ověření axiomů v duálním světě: [4]

1. $\exists \mathcal{C}$ čtveřice přímek t. ž. $\forall x \in X$ leží na nanejvýš 2 přímkách z $\mathcal{C}$
   - stejné jako „žádné 3 přímky z $\mathcal{C}$ nemají společný bod“
   - zvolím $\mathcal{C} = \{ab, cd, ad, bc\}$, což funguje (zkusit si rozkreslit)
2. $\forall x, y \in X, x \neq y : \exists! P \in \mathcal{P}$ t. ž. jimi prochází právě 1 přímka
   - stejné jako původní axiom o přímkách
3. analogicky viz. $\widehat{}$

Důsledek: $(X, \mathcal{P})$ je řádu $n \implies |\mathcal{P}| = n^2 + n + 1$

- duál $(Y, \mathcal{T})$ je duál $(X, \mathcal{P})$, ten je stejného řádu a proto je i velikost $|\mathcal{P}| = n^2 + n + 1$

Konstrukce KPR

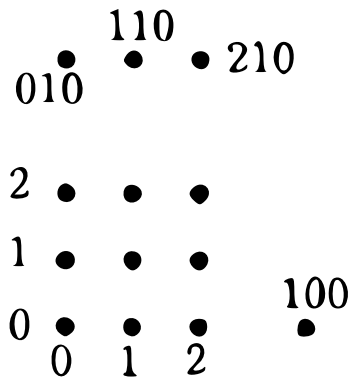
Pro KPR řádu p^k, p prvočíslo vezmu algebraické těleso $\mathbb{K}$ řádu n (příklad $\mathbb{K} = \mathbb{Z}_3$).

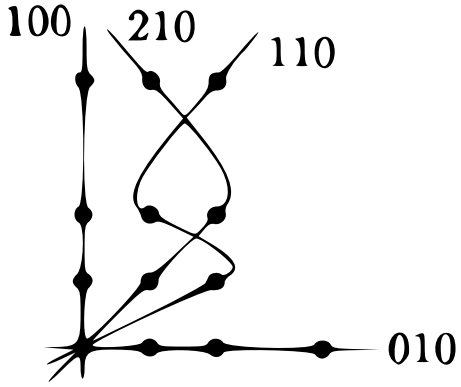
---

[4]

1. „každá přímka obsahuje ≤ 2 body z $\mathcal{C}$“
2. „každé dvě přímky se protínají právě v 1 bodě“
3. „každé dva body určují právě 1 přímku“

- $T = \mathbb{K}^3 \setminus (0,0,0)$
- na T zavedu ekvivalenci $(x,y,t) \in T$ je ekvivalentní s $(\lambda x, \lambda y, \lambda t), \forall \lambda \in \mathbb{K} \setminus 0$
- body X jsou ekvivalenční třídy nad T
- reprezentanti: poslední nenulová složka je 1
  - trojice tvaru $(x,y,1), (x,1,0), (1,0,0)$
  - můžu si to dovolit, na reprezentanta převedu prostým pronásobením
  - počet je $n^2 + n + 1$, což sedí
- přímky $\mathcal{P}$: pro každou $(a,b,c) \in T$ definujeme přímku $P_{a,b,c}$ jako množinu bodů (x,y,t) splňující $ax + by + ct = 0$
  - $\forall (x,y,t) \in T, \forall \lambda \neq 0 : (x,y,t)$ splňuje $\iff (\lambda x, \lambda y, \lambda t)$ splňuje
  - $\forall (a,b,c) \in T, \forall \lambda$ fixuji $(x,y,t) \in T : ax + by + ct = 0 \iff \lambda ax + \lambda by + \lambda ct = 0 \implies$ přímky $P_{a,b,c} = P_{\lambda a, \lambda b, \lambda c} \implies |\mathcal{P}| = |X|$ a mohu si opět zvolit reprezentanty





Ověření axiomů:

1. $\mathcal{C} = \{(1,0,0), (0,1,0), (0,0,1), (1,1,1)\}$ [5]
   - jsou po třech lineárně nezávislé, proto (1) platí
2. dvojice přímek (a_1, b_1, c_1) a (a_2, b_2, c_2) určují jeden bod:
   - jsou lineárně nezávislé a dimenze jádra následující matice je tedy 1 a určují jeden bod (až na α-násobek, což je definice bodů)

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix} \begin{pmatrix} x \\ y \\ t \end{pmatrix} = 0$$

3. analogické, protože role (x,y,t) a (a,b,c) je identická

5. přednáška

Latinské čtverce

Definice (latinský čtverec) řádu n je tabulka $n \times n$ vyplněná čísly $[n]$, kde v žádném řádku či sloupci se symboly neopakují.

- **(👀):** A je LČ $\implies$ po následujících operacích je stále:
  - permutace symbolů
  - permutace sloupců/řádků

Definice (ortogonalita) LČ A, B jsou ortogonální, pokud pro každou dvojici symbolů $a, b \in [n]$ existují indexy $i, j \in [n]$ t. ž. $(A)_{i,j} = a, (B)_{i,j} = b$.

---

[5]

1. „každá přímka obsahuje ≤ 2 body z $\mathcal{C}$“
2. „každé dvě přímky se protínají právě v 1 bodě“
3. „každé dva body určují právě 1 přímku“

- když přeložím čtverce přes sebe, najdu políčko (i, j) obsahující dvojici (a, b)
- **(👀):** počet dvojic symbolů n^2 = počtu políček
  - zobrazení je bijekce
  - $\forall(a, b)$ se objeví v OLČ právě jednou
- **(👀):** A, B jsou NOLČ $\implies$ pokud dělám operace z předchozího pozorování v obou čtvercích, tak ortogonalitu zachovávám, jinak nutně ne

Příklad: dvou navzájem ortogonálních latinských čtverců stupně n:

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{array} \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{array}$$

Lemma: pro daný řád n může existovat nejvýše $n-1$ NOLČ.

Důkaz: mějme maximální rodinu NOLČ $L_1, \ldots, L_m$ a permutujme symboly tak, aby každý první řádek byl $1, 2, 3, \ldots, n$; uvažme symbol na pozici $(2, 1)$:

- není 1, ta je na pozici $(1, 1)$
- není nějaké $k \in \{2, \ldots, n\}$ ve dvou čtvercích zároveň

Čtverců je dohromady tedy nejvýše $n-1$.

Tvrzení: pokud $L_1, \ldots, L_{n-1}$ jsou NOLČ, potom $\forall k, k', k \neq k', \forall l, l', l \neq l' \exists i : (L_i)_{k,l} = (L_i)_{k',l'}$

Důkaz: zpermutujeme symboly tak, aby $\forall i\, (L_i)_{k,l} = 1$: [6]

$$\underbrace{\begin{bmatrix} (1) & \\ & ? \end{bmatrix} \quad \begin{bmatrix} (1) & \\ & ? \end{bmatrix} \quad \cdots \quad \begin{bmatrix} (1) & \\ & ? \end{bmatrix}}_{n-1}$$

Ve sloupci s otazníkem nemůže symbol 1 být:

- v řádku s (1)
- ve dvou čtvercích na stejném místě

Mám tedy $n-1$ možností a musím přijít na $n-1$ různých řešení. Jedno z nich tedy vyjde na ?.

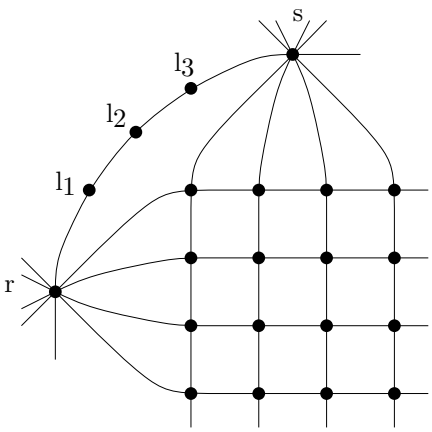
NOLČ $\iff$ KPR

Věta: $\exists L_1, \ldots, L_{n-1}$ NOLČ $\iff \exists KPR$ řádu n.

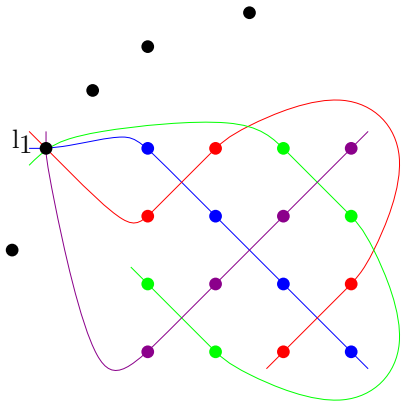
Důkaz (konstrukce $\Rightarrow$)

- dány čtverce $L_1, \ldots, L_{n-1}$
- body: $r, s, l_1, l_{n-1}, m_{1,1}, m_{1,2}, \ldots, m_{1,n}, \ldots, m_{n,n}$
- přímky:
  - I : $\{r, s, l_1, \ldots, l_n - 1\}$
  - II : řádky – $\forall i \in [n] : \{r, m_{i,1}, m_{i,2}, \ldots, m_{i,n}\}$
  - III : sloupce – $\forall i \in [n] : \{s, m_{1,i}, m_{2,i}, \ldots, m_{n,i}\}$
  - IV : $\underbrace{\forall i \in [n]}_{\text{latinské čtverce}}, \underbrace{\forall j \in [n]}_{\text{symboly}} : \{l_i\} \cup \left\{ m_{k,l} \mid (L_i)_{k,l} = j \right\}$

[6] Pro libovolné dvě pozice (které se liší v řádku a sloupci) existuje čtverec, který na nich má stejné hodnoty.



I, II, III



IIII

L_1

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Ověření axiomů:

1. $\mathcal{C} = \{r, s, m_{1,1}, m_{2,2}\}$ [7]
2. mezi:
   - $I, II \to r$
   - $I, III \to s$
   - $I, IV \to l_i$
   - $II, II \to r$
   - $III, III \to s$
   - $II, III \to m_{k,l}$
   - $II, IV \to$ čtverec je latinský, na řádku se symbol někde vyskytuje
   - $III, IV \to$ obdobně $\widehat{\ }$
   - $IV, IV \to$
     - různé čtverce: přesně definice ortogonality (existuje dvojice souřadnic pro dvojici symbolů)
     - stejné čtverce: l_i
3. mezi:
   - $r, s, l_i \to$ I
   - $r, m_{k,l} \to$ II
   - $s, m_{k,l} \to$ III
   - $l_i, m_{k,l} \to$ IV, symbol $(L_i)_{k,l}$ určuje, o kterou přímku z l_i jde
   - $m_{k,l}, m_{k',l'} \to$
     - stejný řádek: II
     - stejný sloupec: III
     - jinak: IV a existuje, vycházíme z minulého pozorování

Důkaz (konstrukce $\Leftarrow$)

- dána KPR $(X, \mathcal{P})$, hledáme $L_1, \ldots, L_{n-1}$
  1. zvolíme libovolně přímku $I = \{r, s, l_1, \ldots, l_{n-1}\}$
  2. $\exists n$ přímek protínající r – typ II a opět oindexuji body
  3. analogicky $\widehat{\ }$, typ III, průsečíky jsou $m_{k,l}$
  4. pro bod l_i oindexuj přímky $Q_1, \ldots, Q_n$; čtverec L_i má 1 na indexech Q_1, 2 na Q_2, ...

Jsou NOLČ, protože:

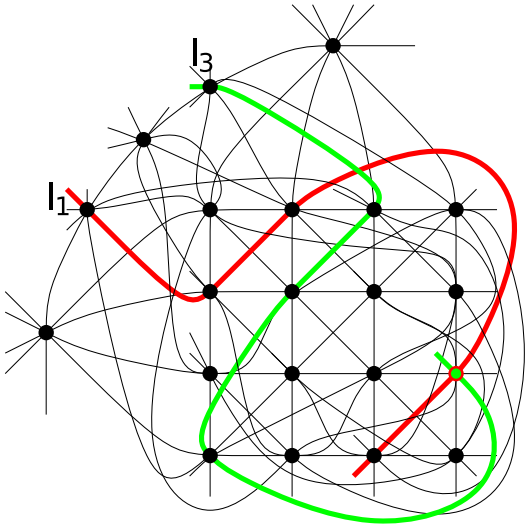
- průsečíky IV s II, III jsou jednoznačné $\implies$ čtverce jsou latinské

---

[7]

1. „každá přímka obsahuje ≤ 2 body z $\mathcal{C}$“
2. „každé dvě přímky se protínají právě v 1 bodě“
3. „každé dva body určují právě 1 přímku“

- jednoznačnost průniku dvou přímek typu IV – dvě různé přímky typu IV odpovídající dvěma různým čtvercům dávají souřadnici, kde se má dvojice symbolů nachází $\implies$ ortogonalita



$(L_1)_{k,l} = 2$

$(L_3)_{k,l} = 3$

pro k = 3, l = 4

L_1

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

L_3

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

6. přednáška

Počítání dvěma způsoby

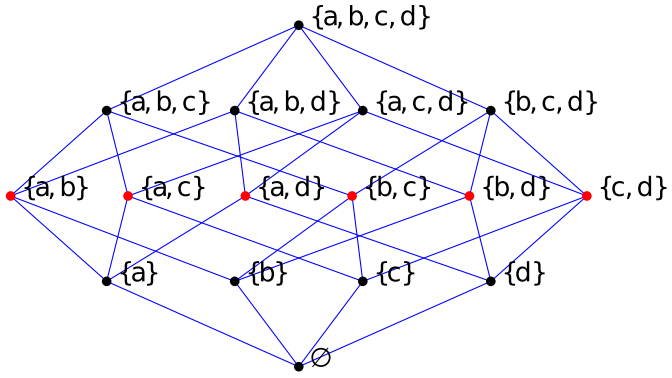
Tvrzení: počet podmnožin $X = \left|\binom{X}{k}\right| = \binom{|X|}{k}$

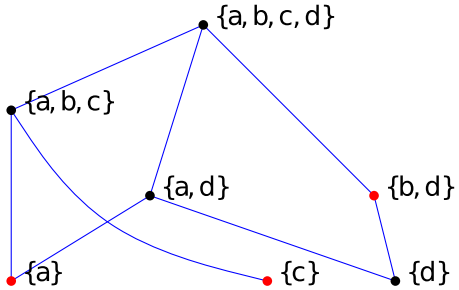
Důkaz: nechť máme bublinu s tečkami, každá reprezentuje uspořádanou k-tici prvků z X.

- počet teček $= n(n-1)(n-2)\dots(n-k+1) = \frac{n!}{(n-k)!}$ (vyberu 1. prvek, 2. prvek,...)
- v každé buňce k-tic (ekvivalenční třídě přes příslušnou relaci) se stejnými prvky je $k!$ prvků, počet buněk je to, co chceme (neuspořádaná k-tice)

$$\frac{n!}{(n-k)!} = \left|\binom{X}{k}\right| \cdot k!$$
$$\left|\binom{X}{k}\right| = \frac{n!}{(n-k)!k!} = \binom{n}{k}$$

Věta (Spernerova) nechť $(\mathcal{P}, \subseteq)$ je částečné uspořádání, kde $\mathcal{P}$ je množinový systém. Nechť $\mathcal{M}$ je největší antiřetězec $(\forall M_1, M_2 \in \mathcal{M}, M_1 \neq M_2 : M_1 \not\subseteq M_2 \wedge M_2 \not\subseteq M_1)$. Pak $|\mathcal{M}| \leq \binom{n}{\lceil \frac{n}{2} \rceil}$, kde $n = |X|$.

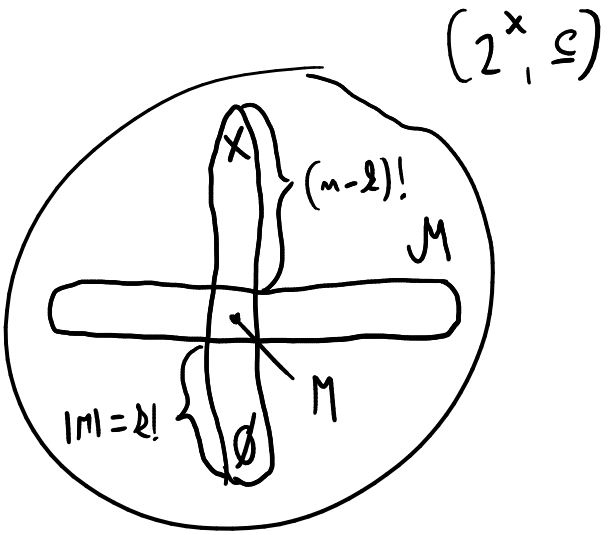




Tvrzení (pomocné) $\sum_{M \in \mathcal{M}} |M|!(n - |M|)! \leq n!$. Přes dvojí počítání počtu permutací na X:

- počet permutací $= n!$ (očividné)

- počet permutací $\geq \sum_{M \in \mathcal{M}} |M|!(n - |M|)!$, protože:
  - pro každé M dostanu jinou množinu permutaci
  - M určuje množinu permutací takovou, že nejprve permutuji M, potom $X \setminus M$:



- $\emptyset \subseteq \{x_1\} \subseteq \{x_1, x_2\} \subseteq \ldots \subseteq M \subseteq \ldots \subseteq X$
  - zajímá nás, kolik různých řetězců obsahuje M
- **(👀):** každý maximální řetězec obsahuje ≤ 1 $M \in \mathcal{M}$

Důkaz (přes pomocné tvrzení)

$$\sum_{M \in \mathcal{M}} |M!|(n - |M|)! \leq n!$$

$$\sum \binom{n}{\lceil \frac{n}{2} \rceil}^{-1} \leq \sum_{M \in \mathcal{M}} \frac{|M!|(n - |M|)!}{n!} \leq 1 \qquad \text{// používáme větší kombinační číslo}$$

$$|\mathcal{M}| \leq \binom{n}{\lceil \frac{n}{2} \rceil}$$

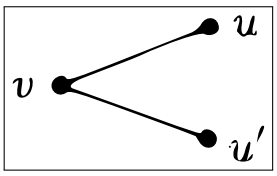
Grafy bez C_k

Motivace:

- kolik nejvíce hran má G, když nemá $C_k, \forall k$?
  - je to strom, tedy $n - 1$
- kolik nejvíce hran má G, když nemá C_3?
  - $\mathcal{O}(n^2)$, uvažme bipartitní graf

Věta: graf G s n vrcholy bez C_4 má nejvýše $\frac{1}{2}\left(n^{3/2} + n\right)$ hran.

Důkaz: dvojí počítání „vidliček“ (cest delky 2):



1. pro pevnou dvojici $\{u, u'\}$ mám nanejvýš 1 vidličku (dvě by tvořily čtyřcyklus), tedy # vidliček $\leq \binom{n}{2}$
2. pro pevný vrchol v máme # vidliček $= \binom{d_i}{2}$

$$\#\text{ vidliček } = \sum_{i=1}^{n} \binom{d_i}{2} \leq \binom{n}{2}$$

Také víme (z principu sudosti), že:

$$|E| = \frac{1}{2} \sum_{i=1}^{n} d_i$$

Předpoklad: nemáme izolované vrcholy ($d_i \geq 1$), jsou zbytečné. Pak $\binom{d_i}{2} \geq \frac{(d_i-1)^2}{2}$.

$$\frac{n^2}{2} \geq \binom{n}{2} \geq \sum_{i=1}^{n} \binom{d_i}{2} \geq \sum \frac{(d_i-1)^2}{2} = \sum \frac{k_i^2}{2} \qquad // \text{ substituce } \sum k_i^2 \leq n^2$$

Využijeme Cauchy-Schwartzovu nerovnost na $x = (k_1, \ldots, k_n), y = (1, \ldots, 1)$:

$$xy = \sum k_i = \sum (d_i - 1) = 2|E| - n || x ||_2 = \sqrt{\sum k_i^2} \leq \sqrt{n^2} = n \qquad ||y||_2 = \sqrt{\sum 1} = \sqrt{n}$$

$$2|E| - n = xy \leq ||x||_2 ||y||_2 = n^{3/2}$$
$$|E| \leq \frac{1}{2}\left(n^{3/2} + n\right)$$

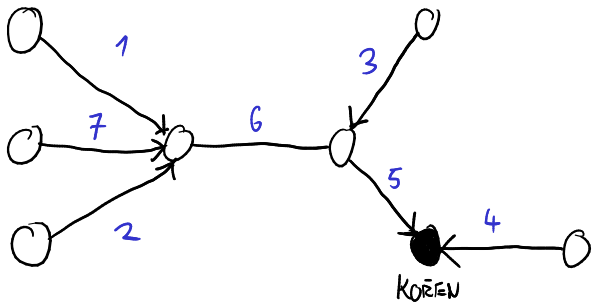
Počítání koster

Věta (Cayleyho formule) počet koster úplného grafu $\kappa(n) = n^{n-2}$.

- udělal jsem o tomhle důkazu krátké video, pokud máte rádi grafičtější důkazy
- pozor, počítám i izomorfní kostry!

Důkaz: počítání $(T, r,)$, kde:

- T je strom na n vrcholech
- r kořen (hrany vedou do kořene, ne z něho)
- očíslování hran (nějaké), $: E \mapsto [n-1]$



1. $\#(T, r,) = \kappa(n) \cdot n \cdot (n-1)!$
   - T je to, co hledáme
   - r volíme libovolně z n vrcholů
   - je prostě random očíslovaní na $n-1$ hranách
2. představa: přidávám hrany, až nakonec dojdu k $(T, r,)$ a jsem v k-tém kroce:
   - (👀): nesmím vést hranu uvnitř komponenty (cykly)
   - (👀): musím vést hranu pouze z kořene dané komponenty (jeden vrchol by měl 2 rodiče)
   1. zvolím, kam šipka povede… n způsobů
   2. zvolím komponentu, ze které povede… $n-k-1$
      - máme $n-k$ komponent a 1 je blokovaná

$$\#(T, r,) = \prod_{k=0}^{\overbrace{n-2}^{\text{počet šipek je } n-1}} n(n-k-1) = n^{n-1}(n-1)!$$
$$\kappa(n) \cdot n \cdot (n-1)! = n^{n-1}(n-1)!$$
$$\kappa(n) = n^{n-2}$$

7. přednáška

Toky

Definice (síť) je čtveřice (G, z, s, c), kde:

- G je orientovaný graf, $z, s \in V(G)$
- $c : E \mapsto \mathbb{R}_{\geq 0}$

Definice (tok) v síti je $f : E \mapsto \mathbb{R}_{\geq 0}$, t. ž.: [8]

1. $\forall e \in E(G)$ platí $0 \leq f(e) \leq c(e)$
2. $\forall v \in V(G), v \notin \{z, s\}$ platí $\sum f(x, v) = \sum f(v, y)$

Definice (velikost toku) $w(f) = \sum f(z, x) - \sum f(x, z)$

Věta: existuje maximální tok.

Definice (pseudo) Nástin je takový, že množina toků je kompaktní a obsahuje tedy i maximum (nevznikne nám tam nějaká divnost). [9]

Definice (řez) v síti je množina hran $R \subseteq E(G)$ taková, že v grafu $(V, E \setminus R)$ neexistuje cesta ze zdroje do stoku.

- **kapacita** řezu je $c(R) = \sum_{e \in R} c(e)$, analogicky tok
- $S(A, B) = \{(x, y) \in E \mid x \in A, y \in B\}$
  - neobsahuje hrany z B do A!
  - je to **elementární** řez (vezmu dvě množiny vrcholů a všechny hrany mezi nimi)
    - každý v inkluzi minimální ($R \setminus e$ není řez) řez je elementární

max flow, min cut

Věta (max flow, min cut) pro každou síť je maximální tok roven minimálnímu řezu.

Lemma: pro každou $A \subseteq V$ t. ž. $z \in A, s \notin A$ a pro libovolný tok f platí:

$$w(f) = f(A, V \setminus A) - f(V \setminus A, A)$$

Důkaz:

$$\begin{aligned} w(f) &= \sum_{u \in A} \left(\sum_{(u,x) \in E} f(u, x) - \sum_{(x,u) \in E} f(x, u) \right) && \text{// pouze definice} \\ &= \sum_{u \in A, v \notin A} f(u, v) - \sum_{u \notin A, v \in A} f(v, u) && \text{// hrany uvnitř A přispějí jednou + a jednou −} \\ &= f(A, V \setminus A) - f(V \setminus A, A) \end{aligned}$$

Důsledek: $w(f) \leq c(R)$, protože

$$w(f) = f(A, V \setminus A) - f(V \setminus A, A) \leq f(A, V \setminus A) \leq c(A, V \setminus A) \leq c(R)$$

Definice (nasycená cesta) je (neorientovaná) cesta, pokud $\exists e$ na cestě t. ž. buďto:

- vede po směru a $f(e) = c(e)$
- vede proti směru a $f(e) = 0$

---

[8]

1. omezení shora kapacitami
2. Kirchhoff

[9] To, co teče ven ze zdroje.

Definice (nasycený tok) je tok takový, že každá (neorientovaná) cesta ze z do s je nasycená.

Tvrzení: f je maximální $\iff$ f je nasycený.

Důkaz (maximální je nasycený)

- sporem, předpokládáme maximální f, který není nasycený, tedy existuje nenasycená cesta P
  - $\varepsilon_1 = min\{c(e) - f(e) \mid e \in P \text{ po směru }\}$
  - $\varepsilon_2 = min\{f(e) \mid e \in P \text{ proti směru }\}$
  - $\varepsilon_P = min\{\varepsilon_1, \varepsilon_2\} > 0$, protože P není nasycená
- sestrojme tok f' tak, že:
  - $f'(e) = f(e) + \varepsilon_P$ pro $e \in P$ po směru
  - $f'(e) = f(e) - \varepsilon_P$ pro $e \in P$ proti směru
  - $f'(e) = f(e)$ pro $e \notin P$

$$w(f') = \sum f'(z,x) - f'(x,z) = w(f) + \varepsilon_P$$

- f nebyl maximální, spor

Důkaz (nasycený je maximální)

- uvážíme množinu vrcholů, do kterých se lze dostat ze z po nenasycené cestě – $A = \{v \in V \mid \exists \text{ nenasycená cesta }\}$
  - $s \notin A$ (jinak f není nasycený)
  - $\forall e \in S(A, V \setminus A)$ platí $f(e) = c(e)$
  - $\forall e \in S(V \setminus A, A)$ platí $f(e) = 0$ (jinak bychom nenasycenou cestu mohli prodloužit

$$\begin{aligned} w(f) &= f(A, V \setminus A) - f(V \setminus A, A) \qquad // \text{ předešlé lemma} \\ &= c(A, V \setminus A) - 0 \\ &= c(f) \end{aligned}$$

Ford-Fulkerson

1. $f(e) = 0, \forall e \in E$
2. dokud $\exists$ zlepšující cesta P, zlepši tok přes P

Tvrzení: pokud jsou kapacity racionální, pak algoritmus doběhne. Pokud jsou přirozené, dá celočíselný tok.

- racionální: pronásobení LCM a důkaz pro přirozené
- přirozené: každé vylepšení cesty bude celočíselné a udělá to konečněkrát

(👀): Celočíselný tok lze rozdělit na celočíselný součet cest a cyklů.

Důkaz: Plyne z běhu F-F algoritmu. Tok je součtem zlepšujících cest a cyklů.

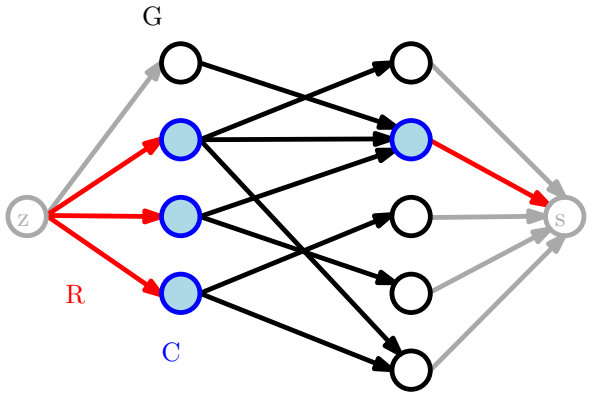
8. přednáška

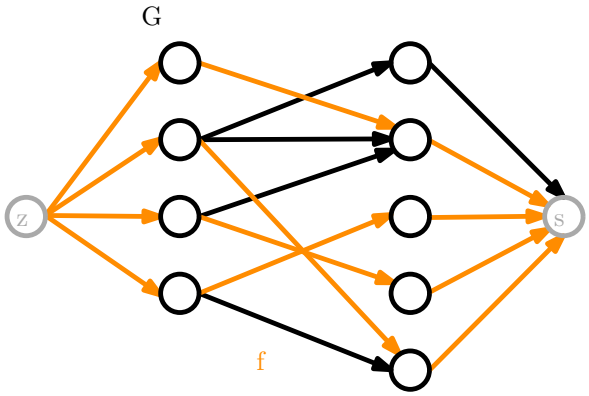
Aplikace toků v sítích

Věta (Königova) v bipartitním grafu: velikost maximálního párování = velikost minimalního vrcholového pokrytí.

- $M \subseteq E$ je **párování**, pokud $\forall e, e' \in M, e \neq e' : e \cap e' = \emptyset$
- $U \subseteq V$ je **vrcholové pokrytí**, pokud $\forall e \in E \exists u \in U : u \in e$

Důkaz: přes toky, jako na následujícím obrázku na síti kapacit 1:





- R je minimální $z-s$ řez
- C je minimální vrcholové pokrytí
- f je maximální tok
  - hrany v původním grafu jsou maximální párování
- L, P = levá a pravá část grafu (bez zdroje a stoku)

Z toku mám maximální párování M velikosti k, ze kterého sestrojím minimální řez R.

R je minimální $z-s$ řez. Ten upravíme na minimální řez R', aby neobsahoval hrany původního grafu. To jde, protože hranu původního grafu mohu vyměnit za tu ze zdroje/stoku, protože ta je jediný způsob, jak se dostat do hrany z původního vrcholu.

- $W = \{u \in L \mid (z,u) \in R'\} \cup \{v \in P \mid (v,s) \in R'\}$
  - je vrcholové pokrytí, v původním grafu by jinak existovala $z-s$ cesta a nejednalo se o řez

W je minimální vrcholové pokrytí G:

- $R = \{(z,u) \mid u \in W \cap L\} \cup \{(u,s) \mid u \in W \cap P\}$
  - je řez (pro spor by existovala cesta, kterou by W nepokryl)

Dostáváme tedy, že min. řez je roven nějakému pokrytí, a že min. pokrytí je rovno nějakému řezu, tedy že min. pokrytí je rovno min. řezu.

Definice:

- **množinový systém** na množině X je $(M_i)_{i \in I}, M_i \subseteq X$
- **systém různých reprezentantů** je funkce $f : I \mapsto X$ splňující:
  1. $\forall i \in I : f(i) \in M_i$
  2. f je prostá (jeden prvek $x \in X$ není reprezentantem dvou M)

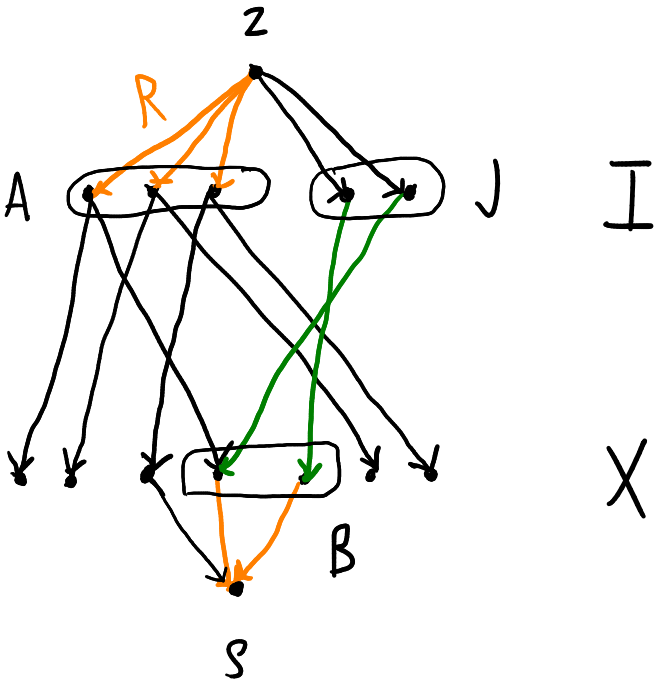
Věta (Hallova) SRR existuje $\iff \forall J \subseteq I : \left|\bigcup_{i \in J} M_i\right| \geq |J|$.

Důkaz (SSR $\Rightarrow$ Hall) zvolím libovolnou $J \subseteq I$. $\forall j \in J \exists p_j \in M_j, p_j = f(j)$, tak že prvky p_j jsou navzájem různé (f je prostá). [10]

$$|J| = |\{p_j \mid j \in J\}| \leq |\bigcup_{j \in J} M_j|$$

Důkaz (SSR $\Leftarrow$ Hall) opět najdu v grafu (celočíselný, jednotková síť) maximální tok. Najdu minimální řez z hran pouze ze zdroje/do stoku, $|R| = |R'|$. Uvážím následující obrázek:

[10] Analogicky pro grafy: bipartitní graf $G = (L \cup P, E)$ má párování pokrývající P pokud $\forall P' \subseteq P : \left|\bigcup_{v \in P'} N(v)\right| \geq |P'|$. N je sousedství (to, co vrcholy zprava na levé straně „vidí“).



- $A =$ vrcholy incidentní s R' v I
- $B =$ vrcholy incidentní s R' v X
- $J = I \setminus A$

Chceme najít systém různých reprezentantů. Dokážeme to tak, že $|R'| = |I|$, pak max. tok má velikost $|I|$ a hrany s tokem 1 mi dají SRR.

(👀): hrany z J vedou pouze do B, protože jinak by existovala $z - s$ cesta a nejednalo by se o řez, tedy $\left|\bigcup_{j\in J} M_j\right| \subseteq B$.

$$\begin{aligned}
|R'| &= c(R') && \text{// jednotkové kapacity}\\
&= |A| + |B|\\
&= \overbrace{|I| - |J|}^{|A|} + |B|\\
&\geq |I| - |J| + \left|\bigcup_{j\in J} M_j\right| && \text{// z pozorování}\\
&\geq |I| - |J| + |J| && \text{// z Hallovy podmínky}\\
&= |I| && \text{// } \implies \text{ tok má velikost alespoň } |I|
\end{aligned}$$

Definuji SRR jako $f(i) = x \in X$, pokud po hraně (i, x) něco teče.

9. přednáška

Důsledek: nechť $B = (V_1 \cup V_2, E)$ je bipartitní graf, kde $k_1 = \min\limits_{v\in V_1} \deg v, k_2 = \max\limits_{v\in V_2} \deg v$ a $k_1 \geq k_2$, pak je splněna Hallova podmínka.

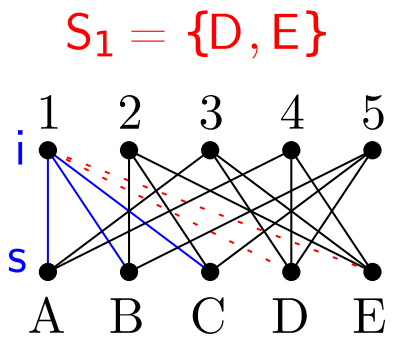
Důkaz: Ověřím Hallovu podmínku (pozor, prohozené strany). Máme-li množinu J a každá vidí alespoň k_1 hran, pak vidím $\geq |J|k_1$ hran. Abych pohltil všechny tyto hrany, tak musí napravo být alespoň $k_2|N[j]|$ vrcholů. Musí tedy platit:

$$|J|k_1 \leq \#\text{ hran} \leq k_2|N[J]|$$

Protože $k_1 \geq k_2$, pak $|N[j]| \geq |J|$.

Příklad: doplňování latinských obdélníků:

D	A	B	C	E
E	D	C	B	A



- stupně: každý sloupec má stupeň $n-k$ (počet nepoužitých symbolů)
- symboly: každý symbol se vyskytuje v řádku právě jednou, tedy ještě není v $n-k$ sloupcích

Máme tedy $(n-k)$-regulární graf, pro který $\exists$ perfektní párování (použití minulého důsledku).

Míra souvislosti neorientovaných grafu

Definice:

- **hranový řez** v grafu G je $F \subseteq E$ t. ž. $G' = (V, E \setminus F)$ je nesouvislý.
- **vrcholový řez** v grafu G je $A \subseteq V$ t. ž. $G' = (V \setminus A, E \cap \binom{V \setminus A}{2}) = G[V \setminus A]$ je nesouvislý.
- **hranová souvislost** $k_e(G) = \min\{|F| \mid F \subseteq E \text{ je hranový řez}\}$
- **vrcholová souvislost** $k_v(G) = \begin{cases} n-1 & G \cong K_n \\ \min\{|A| \mid A \subseteq V \text{ je vrcholový řez}\} & \text{jindy} \end{cases}$
- G je **hranově/vrcholově k-souvislý**, pokud $k_{e/v}(G) \geq k$
  - „potřebuješ useknout alespoň k hran/vrcholů na to, aby se graf rozpadl“
  - **(👀):** je-li 3-souvislý, pak je i 2-souvislý a 1-souvislý
  - je **kriticky** k-souvislý, pokud odstranění libovolného vrcholu sníží stupeň souvislosti
    - stromy jsou hranově 1-souvislé, vrcholově ne (co listy?)

Lemma: $\forall G, \forall e \in E$ platí $k_e(G) - 1 \leq k_e(G-e) \leq k_e(G)$

- zas tak triviální to není, u vrcholové může (odstraněním vrcholu) vzrůst (listy z kružnice)
- lemma říká, že se hranová souvislost „chová slušně“

Důkaz ($\leq$) vezmu minimální řez $F \subseteq E$ v G, $F' = F \setminus \{e\}$ jistě musí být řez v $G-e$; pak:

$$k_e(G-e) \leq |F'| \leq |F| = k_e(G)$$ [11]

Důkaz ($\geq$) vezmu minimální řez B v $G-e$ $B' = B \cup \{e\}$ je řezem v G, pak:

$$k_e(G) \leq |B'| = |B| + 1 = k_e(G-e) + 1$$
$$k_e(G) - 1 \leq k_e(G-e)$$

Tvrzení: $\forall G, \forall e \in E$ platí $k_v(G) - 1 \leq k_v(G-e) \leq k_v(G)$

Důkaz: trochu přeformulujeme… pro $H = G - e : k_v(H+e) \leq k_v(H) + 1$:

V H existuje vrcholový řez $A \subseteq V(H), k_v(H) = |A|$. Při odebrání A se H rozpadne na alespoň 2 komponenty. Sledujeme (rozebíráme případy), co se se souvislostí stane, když přidáme do grafu hranu e:

- alespoň 1 konec e leží v A:

[11] Tomovo poznámka: V důkazu $k_e(G) \leq k_v(G)$ se tohle lemma nepoužívá (alespoň tak, jak to chápu). Jsem trochu zmatený z toho, proč Martin říkal, že ano.

  - přidání e nespojí žádné 2 komponenty, A je řezem i pro $G = H + e$
- oba konce leží v 1 komponentě
  - stejný argument jako (1)
- hrana e spojuje 2 komponenty
  - pokud je počet komponent ≥ 3, tak je A stále řezem (po spojení jsou stále 2)
  - pokud není, tak:
    * BUNO $|C_1| \geq 2$; nechť $e = xy$ a x leží v C_1, pak $A \cup x$ je řezem, protože mi v obou komponentách něco zbylo
    * $|C_1| = |C_2| = 1$:
      · $|V| = |A| + 2 \implies |A| = |V| - 2 = k_v(H)$
      · $k_v(H + e) \overset{\text{def.}}{\leq} |V| - 1 = k_v(H) + 1$

Věta: $k_v(G) \leq k_e(G)$: indukcí podle počtu hran:

- pokud $|E| < |V| - 1$, pak je G nesouvislý a $k_v(G) = 0 = k_e(G)$
- nechť nadále $k_e(G) > 0$; vezmu min. hranový řez $F \subseteq E$ a $e \in F$; také $G' = G - e$
  - na G' použiju IP, tedy $k_v(G') \leq k_e(G')$
  - z lemmatu o souvislosti vrcholů (a přičtení jedničky) víme:

$$k_v(G) - 1 \leq k_v(G - e) \overset{\text{IP}}{\leq} k_e(G - e) = k_e(G) - 1$$

Kde poslední rovnost platí, protože $F' = F \setminus e$ je (z definice) řezem $G - e$.

Věta (Ford-Fulkerson) $\forall G$, pokud $k_e(G) \geq t$, pak $\forall u, v$ mezi u, v existuje alespoň t hranově disjunktních cest

Důkaz (⇐) sporem nechť existuje hranový řez F a $|F| < t$. $G \setminus F$ je rozdělený na více komponent. Vezmi $u \in C_1, v \in C_2$. Mezi u, v vedlo t hranově disjunktních cest. F nemohl přerušit všechny z nich.

Důkaz (⇒) mějme $k_e(G) \geq t$ a pro u, v hledám disjunktní cesty. Sestrojím jednotkovou síť, najdu tok z u do v. Pak vidím, že mám tok alespoň t (maximální tok je minimální řez) a začnu odčítat cesty. [12]

Věta (Mengerova) $k_v(G) \geq T \iff \forall u, v \in V \exists t$ vrcholově disjunktních cest

Důkaz (⇐) stejný jako FF, jen nahraď „hrany“ za „vrcholy“.

Důkaz (⇒) uděláme trik s dělením vrcholů na dva $(\deg_{\text{in}}, \deg_{\text{out}})$ a v libovolném řezu nahradíme hrany vedoucí do/z vrcholů za hranu spojující vrcholy.

10. přednáška

Lepení uší

Věta: graf je 2-souvislý právě tehdy, když jej lze vytvořit z K_3 posloupností:

- dělení hran
- přidávání hran

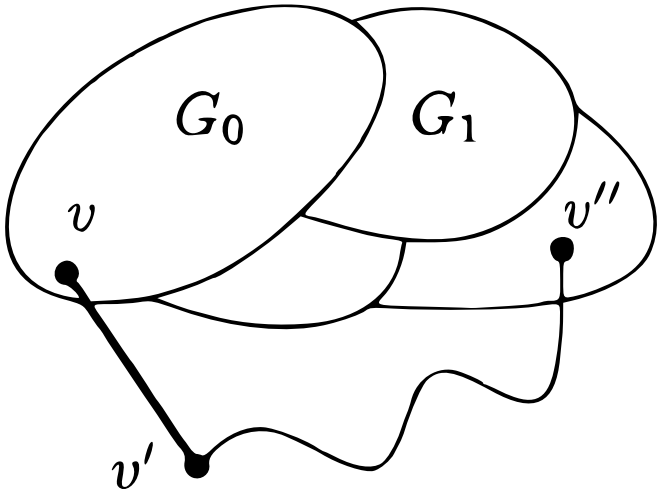
Důkaz (⇒)

- zvolme G_0 libovolně (kružnici mít musí, jinak není 2-souvislý).
- předpokládejme, že $G_j, j \leq i$ jsou definovány jako výše
- pokud $G_i = G$, tak jsme hotovi
- jinak $E_i \neq E$, G je souvislý
  - $\exists e = \{v, v'\} \in E \setminus E_i$, která se dotýká původního grafu $(e \cap V_i \neq \emptyset)$
    * pokud oba vrcholy e patří do V_i, tak ji přidám $(G_{i+1} = G_i + e)$

[12]

- oboustraně zorientuji hrany
- nastavím kapacity na 1
- vynuluji $a \xleftrightarrow[1]{1} b$
  - každou hranu využíváme 1!

∗ pokud ne: $G - v$ musí stále být souvislý (G je 2-souvislý) – prostě vezmeme nejkratší cestu zpět do nějakého G_j



Důkaz ($\Leftarrow$) stačí vidět, že nikdy nevznikne artikulace, protože uši lepím mezi 2 různé vrcholy.

Samoopravné kódy

Definice (Hammingův kód) vycházíme z fannovy roviny a o přímkách uvažujeme jako o prvcích $\mathbb{Z}_2^7$

$$H = \underbrace{\{\text{char. vektory přímek}\}}_{P_1=\{1,2,4\}=(1\ 1\ 0\ 1\ 0\ 0\ 0)} \cup \underbrace{\{\text{char. vektory doplňků přímek}\}}_{P_1+(1\ \ldots\ 1)=(0\ 0\ 1\ 0\ 1\ 1\ 1)} \cup \{(0\ \ldots\ 0), (1\ \ldots\ 1)\}$$

- $|H| = 7 + 7 + 2 = 16$
- $c \in H$ je **kódové slovo**
- H je **kód**
- **(👀):** $\forall c, c' \in H$ se liší v alespoň třech souřadnicích
  - vychází z KPR, později dokážeme obecně
- **(👀):** $\forall v \in \mathbb{Z}_2^7 \exists! c \in H$ t. ž. $d(v, c) \leq 1$
  - dostáváme z toho dekódovací pravidlo – dekóduj na nejbližší slovo!

Protokol:

1. vezmi kódovou zprávu
2. rozděl na 4-bitové bloky
3. zakóduj přes Hammingův kód
   - nějak rozumně očísluj kódová slova!
4. profit?

Výsledek:

- zpráva je o 7/4 delší
- $\Pr[\text{jeden blok se správně rozkóduje}] = \overbrace{(1-p)^7}^{\text{vše ok}} + \overbrace{7p(1-p)^6}^{\text{jeden špatně}} = (1-p)^6(1+6p)$
- $\Pr[\text{celá zpráva se správně dekóduje}] = \big((1-p)^6(1+6p)\big)^{n/4}$
  - pro $n = 100, p = 0.01$ vyjde 95%, což je nice!

Definice:

- $\Sigma \ldots$ abeceda
  - $s \in \Sigma^n \ldots$ slovo (vstup)
- $C \subseteq \Sigma^n \ldots$ kód

  - $c \in C \ldots$ kódové slovo (naše special slova)
  - $|C| \ldots$ velikost kódu (počet kódových slov)
  - $n \ldots$ délka kódu (kolikaznakové slova máme)
  - $k = \log |C| \ldots$ dimenze kódu (bude se hodit později)
- pro $x, y \in \Sigma^n : d_H(x, y) = d(x, y) \ldots$ počet souřadnic, ve kterých se liší
  - $d = \Delta(C) = \min\limits_{x,y \in C} d(x, y) \ldots$ (min.) vzdálenost C
    - $d = 1 \ldots$ nepoznám chybu
    - $d = 2 \ldots$ poznám, že došlo k chybě
    - $d = 3 \ldots$ umím opravit 1 chybu
    - $\Delta(C) \geq 2t + 1$ znamená, že „C má schopnost opravit t chyb“
- kód s vlastnostmi n, k, d se označuje $(n, k, d)-$ kód

Příklad (kódů)

1. totální kód $C = \Sigma^n$ (nic se nekóduje)
   - délka $= n$
   - velikost $= 2^n \implies k = \log |C| = n$
   - $\Delta(C) = 1$
   - $\implies (n, n, 1)-$kód
2. opakovací kód délky n (pozor, n je délka slova)
   - délka $= n$
   - velikost $= 2 \implies k = 1$
   - $\Delta(C) = n$
   - $\implies (n, 1, n)-$kód
3. paritní kód $C \subseteq \Sigma^n$ t. ž. $x \in C : \sum_{x_i} = 0$ (počet jedniček je sudý)
   - délka $= n$
   - velikost $= 2^{n-1} \implies k = n - 1$
   - $\Delta(C) = 2$, protože změna bitů mění paritu
   - $\implies (n, n - 1, 2)-$kód
4. Hammingův kód
   - $\implies (7, 4, 3)-$kód

11. přednáška

Jak nejefektivněji můžeme kódovat?

- $A(n, d) = \max\limits_{C} \log |C|$ - C jsou binární kódy délky n s min. vzdáleností $\geq d$ - $A(n, 1) = n$ (triviální kód)
- $A(n, 2) \geq n - 1$ (paritní kód má $|C| = 2^{n-1}, d = 2$) [13]

(👀): $\forall d \leq n, d \geq 2 : A(n, d) \leq A(n - 1, d - 1)$

- po odstranění bitu vzdálenost slov klesne nejvýše o 1 (pokud se slova v bytu liší); velikost nového kódu $|C'| = |C|$ (díky předpokladu funguje, žádná slova se nesloučí)

Věta (Singletonův odhad) $\forall d \leq n$ platí $A(n, d) \leq n - d + 1$

- $A(n, d) \leq A(n - 1, d - 1) \leq \ldots \leq A(n - d + 1, 1) = n - d + 1$ [14]
- rovněž dostávám $A(n, 2) \leq A(n - 1, 1) = n - 1$ a vím, že $A(n, 2) \geq n - 1$, tedy rovnost

Tvrzení: pro každé sudé $d \leq n$ je $A(n, d) = A(n - 1, d - 1)$

Důkaz: nechť C je $(n - 1, k, d - 1)$-kód. Přidáním paritního bitu ke každému slovu vytvořím $(n, k, d)-$kód, protože slova c v liché vzdálenosti (speciálně $d-1$) v C' mají vzdálenost o 1 větší (liší se jejich paritní symboly).

- $\implies$ nejzajímavější jsou kódy s lichým d (na sudé lze triviálně rozšířit)

[13] Maximální dimenze kódu (logaritmus počtu kódových slov), když určím délku a vzdálenost.

[14] Není to Simpletonův, ale Singletonův (viz. Wikipedia). Byť je ten odhad docela triviální 🙂.

Lineární kódy

Definice: kód C nad $\mathbb{Z}_2^n$ je lineární kód, pokud tvoří vektorový podprostor.

- $\forall c, c' \in C : c + c' \in C$
- $\forall \alpha \in \mathbb{Z}_2 : \alpha c \in C$

(👀): pokud C je dimenze k, pak má 2^k prvků, ale k jeho popisu stačí nějaká báze $C \equiv k$ slov t. ž. ostatní dostanu lineárními kombinacemi.

Příklad: Hammingův kód $\mathcal{H}$ je lineární a generuje ho **generující matice**

$$\begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{matrix} \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

- generující matice kódu H
- $\{v_1, \ldots, v_4\}$ je báze H
- $\forall c \in H \ \exists \alpha_1, \ldots, \alpha_4 \in \mathbb{Z}_2$ t. ž. $c = \sum_{i=1}^{4} \alpha_i v_i$

(👀): $\forall x, y, z \in C : d(x, y) = d(x + z, y + z)$

- „posunutí nějakým směrem“
- platí pro všechny kódy, ale hodí se jen u lineárních kódů, protože díky tomu, že tvoří VP je součet také kódové slovo
- $x + z, y + z \in C$ (lineární kódy)
  - $d(x, y) = d(0, y - x)$
  - $\Delta(C) = \min\limits_{x,y \in C} d(0, y - x) \implies \min\limits_{x \in C} d(0, x)$, což je počet nenulových souřadnic

---

- $\langle x, y \rangle = \sum_{i=1}^{n} x_i \cdot y_i$
  - něco jako skalární součin
  - nemusí platit, že $x \neq 0 \implies \langle x, x \rangle \neq 0$ (např. pro (1 1 0 0))

Definice (duální kód) C je ortogonální doplněk $C^\perp = \{x \mid \langle x, y \rangle = 0, \forall y \in C\}$

- může být $C \cap C^\perp \neq \{0\}$, ale platí $\dim C + \dim C^\perp = n$

(👀): $C^\perp$ je opět vektorový podprostor, je to tedy taky kód

- má také generující matici M (tzv. **paritní/kontrolní**)
- platí $C = \{x \mid Mx = 0\}$ (z definice naší „ortogonality“)
  - stačí ověřit ortogonalitu na bázové vektory

(👀): nechť G je generující matice kódu C

- G můžu zgausoeliminovat na G', která stále generuje C
- ke kódování daného slova stačí sečíst příslušné řádky G', protože se jedná o jediný způsob, jak dostat bity slova

$$c = (1\ 1\ 0\ 1) \qquad x = (\ \underbrace{1\ 1\ 0\ 1}_{\text{informační bity}}\ \overbrace{\cdots\cdots\cdots}^{\text{kontrolní/paritní bity}}\ )$$

Dekódování

Mějme C lineární kód délky n nad $\mathbb{Z}_2^4$. Bylo odesláno slovo $x \in C$ a přijato slovo $\tilde{x}$.

- mohly nastat chyby $e = \tilde{x} - x$ (chybový vektor)
  - chceme ho objevit, abychom rozluštili x

P je paritní matice kódu C, tzn. $C = \{x \mid Px = 0\}$.

Definice (syndrom) slova z je Pz, kde P je paritní matice kódu C.

- **(👀):** kódová slova ≡ slova se syndromem 0 (viz. definice P…)

Předpoklad: chybový vektor e je slovo s nejmenší vahou ve své třídě

- **třída** $= \{e' \mid Pe' = P\tilde{x} = P(x+e) = Px + Pe = Pe\}$ (slova se stejným syndromem)
- pro syndrom $s \in Z_2^k$ je slovo $m(s) \in Z_2^n$ t. ž. $Pm(s) = s$ a $w(m(s))$ je minimální tzv. **reprezentant**

Dekódování:

- vezmu $s = P\tilde{x}$
- najdu reprezentanta $m(s)$
- výsledek dekódování $y = \tilde{x} - m(s) = \tilde{x} - m(P\tilde{x})$
  - **(👀):** y má mezi kódovými slovy nejmenší vzdálenost od $\tilde{x}$

Příklad:

- $G = \begin{matrix} v_1 \\ v_2 \end{matrix} \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$
- $k = 2$, máme 4 slova $\{v_1, v_2, (0\ \dots\ 0), v_1 + v_2\}$
- $\Delta(C) = 3$ (počet jedniček vektoru báze)
- jedná se o $(5, 2, 3)-$kód
- $P = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$

1. $\tilde{x} = v_1 = (1\ 1\ 1\ 0\ 0)$, $P\tilde{x} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ (nulový syndrom, což je správně)
2. $\tilde{x} = (0\ 0\ 1\ 0\ 1)$, $P\tilde{x} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ (nějaký syndrom)
   - podíváme se do tabulky syndromů (vybruteforcená)
   - dostaneme ze syndromu reprezentanta $m(s) = (0\ 0\ 0\ 1\ 0)$
   - spočítáme $x = \tilde{x} - e = (0\ 0\ 1\ 1\ 1)$
   - protože došlo k chybě v 1 pozici a jedná se o $(5, 2, 3)$-kód, x je správné dekódování
3. pro $\tilde{x} = (0\ 1\ 1\ 0\ 1)$ dostáváme váhu syndromu 2 a to už neopravíme

Hammingovy kódy

(👀): nechť P je kontrolní matice C. Pak $\Delta(C) =$ maximální d t. ž. $\forall d-1$ sloupců P je lineárně nezávislých.

Důkaz: kódová slova ≡ $Pc = 0$. Nechť sloupce P jsou $p_1, \dots, p_n$. Pak

$$\sum_{i=1}^{n} c_i p_i = 0$$

Pro spor nechť $\exists x$ t. ž. $\sum x_i p_i = 0$ (je tedy kódové slovo) a $w(x) < d \to$. To je spor, $\Delta(C) = d$ ale tohle slovo má $w(x) < d$. To musí nutně znamenat, že $\forall x : w(x) < d \to \sum_{i=1}^{n} x_i p_i \neq 0 \to$ každých $\leq d-1$ sloupců je tedy lineárně nezávislých.

Důsledek: pokud chci $d = 3$, potřebuji co největší matici P t. ž. $\forall 2$ sloupce jsou lineárně nezávislé. To v $\mathbb{Z}_2$ znamená, že musí být různé a žádný z nich není nulový.

$$P = \underbrace{\begin{pmatrix} 0 & 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 0 & 1 & 1 & & 1 \\ 1 & 0 & 1 & & 1 \end{pmatrix}}_{2^r - 1 \text{ nenulových } r\text{-dim. vektorů}}$$

Jedná se o binární zápisy čísel $1 \dots 2^r - 1$. Nechť C je generovaný P a $\mathcal{H}_r = C^\perp$ (P je paritní matice $\mathcal{H}_r$). Má délku $n = 2^r - 1$ a $\dim \mathcal{H}_r = n - r = 2^r - r - 1$.

- $n - r$ funguje, protože mají komplementární dimenze

Z pozorování (nezávislé sloupce) dostáváme, že $\Delta(\mathcal{H}_r) = 3$.

Věta: pro každé $r \geq 2$ je $\mathcal{H}_r$ $[2^r - 1, 2^r - r - 1, 3]$-kód.

12. přednáška

- **(👀):** $G = [I_k \mid P] \implies M = \begin{bmatrix} -P \\ I_{n-k} \end{bmatrix}^T$

Dekódování Hammingova kódu

- předpoklad: e má nejvýše 1 jedničku
  - došlo k ≤ 1 chybě
- M je ve tvaru uvedeném výše (binární zápisy čísel $1 \dots 2^r - 1$)
  - pozorování: syndrom $M\tilde{x} = Me$ je $y_i \equiv$ binární zápis $i \iff$ došlo k chybě na pozici i

Perfektnost kódu

Pokud pro C platí $\Delta(C) = 2t + 1$, pak pro každé slovo $x \in \mathbb{Z}_2^n$ je nejvýše jedno kódové slovo ve vzdálenosti $\leq t$ od x. jsou to tedy **symetrické koule** se středem x a poloměrem t, $B(x, t) = \{z \in \mathbb{Z}_2^n \mid d(x, z) \leq t\}$; jsou pro různá $x \in C$ disjunktní.

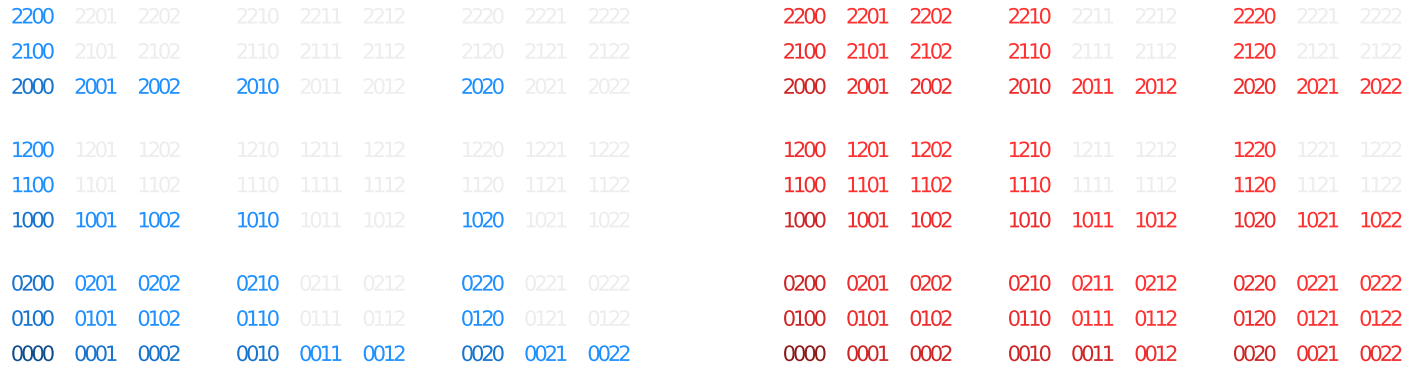
Věta (Hammingův odhad) pro binární kód s $\Delta(C) \geq 2t + 1$ platí

$$|C| \leq \frac{2^n}{V(n, t)}$$

- 2^n je počet všech slov
- $V(n, t)$ je objem kombinatorické koule dimenze n o poloměru $t = \sum_{i=0}^{t} \binom{n}{i}$ (vždy způsoby, jak si vybrat i bitů a flipnout je)

Důkaz: mám na 2^n prvcích $|C|$ disjunktních koulí objemu $V(n, t)$… koule pokrývají $|C| \cdot V(n, t)$ prvků, což je $\leq 2^n$ (méně nebo rovno všem prvkům – nevím, jestli se nepřekrývají) a vydělím.

2200	2201	2202	2210	2211	2212	2220	2221	2222
2100	2101	2102	2110	2111	2112	2120	2121	2122
2000	2001	2002	2010	2011	2012	2020	2021	2022
1200	1201	1202	1210	1211	1212	1220	1221	1222
1100	1101	1102	1110	1111	1112	1120	1121	1122
1000	1001	1002	1010	1011	1012	1020	1021	1022
0200	0201	0202	0210	0211	0212	0220	0221	0222
0100	0101	0102	0110	0111	0112	0120	0121	0122
0000	0001	0002	0010	0011	0012	0020	0021	0022



Definice: kód C je perfektní, pokud pro něj platí Hammingův odhad s rovností.

Příklad (perfektních kódů)

- totální (koule o poloměru 1)
- opakovací kód liché délky
- jednoprvkový kód (koule zaplňuje celý prostor)

Tvrzení: Hammingův kód je perfektní.

Důkaz: $\mathcal{H}_r = [2^r - 1, 2^r - r - 1, 3]$-kód.

- $3 = 2t + 1 \implies t = 1, V(n,t) = V(2^r - 1, 1) = 2^r$
  - poslední rovnost je počet vektorů lišící se v 1 souřadnici, + střed koule
- $k =$ dimenze $= 2^r - r - 1$
- $|C| = 2^k = 2^{2^r - r - 1}$

$$\frac{2^n}{V(n,t)} = \frac{2^{2^r-1}}{2^r} = 2^{2^r-r-1} = |C|$$

Hadamardův kód

- **duál Hammingova kódu** (prohození generující matice s paritní maticí pro Hammingův kód $G \longleftrightarrow K$ dává Hadamardův kód)
- $x \ldots$ zpráva délky r
- $c = (c_1, \ldots, c_{2^r-1})$
  - $c_i = \langle x, y_i \rangle$, kde y_i jsou binární zápisy čísla i

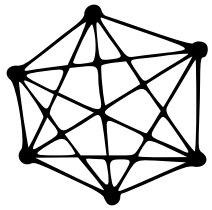
Tvrzení: Hadamardův kód je $\left[2^r, r, 2^{r-1}\right]$-kód.

(👀): $\langle x, y_i \rangle$ nenese informaci o x_1, pokud první bit y je 0 $\implies$ stačí brát $y_i, i \in \left(2^{r-1}, 2^r - 1\right)$

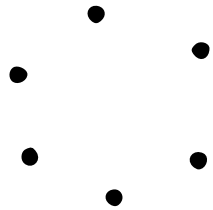
- jedná se o **rozšířený Hadamardův kód** $\left[2^r, r+1, 2^{r-1}\right]$

Ramseyova teorie

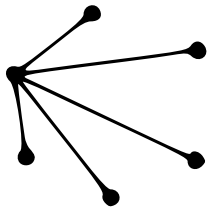
Motivace: party o 6 lidech:



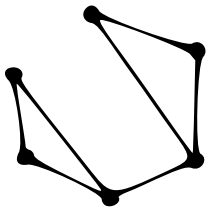
sraz maturantů po 50 letech



seznamovací večírek



večírek ctitelů

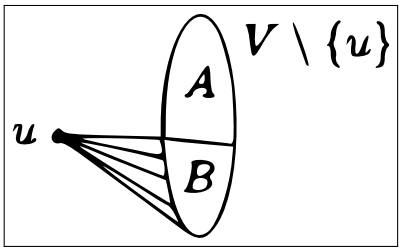


jednání dvou mafiánských bos

Věta: pro každý graf na ≥ 6 vrcholech $\exists$ podrgraf E_3 (prázdný graf) nebo K_3.

- $\omega(G) \geq 3$ – velikost maximální kliky
- $\alpha(G) \geq 3$ – velikost maximální nezávislé množiny

Důkaz: vyberu libovolný vrchol u. Podívám se na vrcholy A, se kterými nesousedí, zbytek nechť je B.



1. $|A| \geq 3, A \supseteq \{x, y, z\}$
   - všichni mezi sebou mají hranu, pak máme K_3
   - BUNO $\exists$ nehrana xy, pak $\{u, x, y\}$ tvoří E_3
2. symetricky

Věta (obecnější Ramseyova) nechť G má $\geq \binom{k+l-2}{k-1}$ vrcholů $\implies$ $\omega(G) \geq k$ nebo $\alpha(G) \geq l$.

- **(👀):** ze symetrie kombinačních čísel máme symetrii v k, l, protože $\binom{k+l-2}{k-1} = \binom{k+l-2}{l-1}$

Důkaz: indukcí podle $k + l$

- pro $k = 1, l = 1$ a $k = 2, l = 2$ jednoduché (vždy existuje hrana/nehrana)
- pro $k, l \geq 2$ a tvrzení platí pro $k, l-1$ a $k-1, l$
  - $n_1 = \binom{k+l-3}{k-1}$ a $n_2 = \binom{k+l-3}{l-1=k-2}$ (dřívější odhady)
    - **(👀):** platí, že $n = n_1 + n_2$

Zvolím $u \in G$ libovolně a opět rozdělím graf na nesousedy A a sousedy B vrcholu u. Z principu holubníku (Dirichletův princip) je $|A| \geq n_1$ nebo $|B| \geq n_2$ (jsou-li ostře menší, tak dají $n - 2$).

1. $|A| \geq n_1$, použiji indukci na A:
   - $\omega(G[A]) \geq k$ a jsem hotov
   - $\alpha(G[A]) \geq l - 1$, pak tato nezávislá množina spolu s u dává nezávislou mnozinu velikosti $\geq l$
2. analogicky: $|B| \geq n_2$, použiji indukci na B:
   - $\omega(G[B]) \geq k - 1$, pak tato klika spolu s u dává kliku velikosti $\geq k$
   - $\alpha(G[B]) \geq l$ a jsem hotov

Důsledek: $\forall k, l \exists r(k, l)$ t. ž. $\forall G : \omega(G) \geq k$ nebo $\alpha(G) \geq l$.

- $r(k, l) = \min N$ t. ž. platí $\forall G$ velikosti N platí výše uvedené
- podle věty nahoře máme $r(k, l) \leq \binom{k+l-2}{k-1}$

Pár hodnot:

- $r(1,l) = 1$
- $r(k,1) = 1$
- $r(2,l) = l$
- $r(k,2) = k$
- dříve jsme dokázali, že $r(3,3) \leq 6$ a z C_5 víme, že $r(3,3) > 5$, tedy $r(3,3) = 6$

Definice ($r(k,k)$): symetrické Ramseyovo číslo, říká se mu $r(n) = r(n,n)$. „Jak velký musí být graf, abych tam našel buď E_n nebo K_n“.

Věta: $k, n \in \mathbb{N}$ t. ž. $\binom{n}{k} 2^{1-\binom{k}{2}} < 1 \implies r(k) > n$.

Co jsou čísla zač? Použijeme odhad:

- $\binom{n}{k} \leq \frac{n^k}{k!} < \frac{n^k}{2^{k/2+1}}$

$$\binom{n}{k} 2^{1-\binom{k}{2}} < \frac{n^k}{2^{k/2+1}} 2^{1-k(k-1)/2} = \left(\frac{n}{2^{k/2}}\right)^k$$

Kde poslední = platí, protože:

$$\frac{1}{2^{k/2+1}} 2^{1-k(k-1)/2} = \frac{1}{2 \cdot 2^{k/2}} \frac{2}{2^{k(k-1)/2}} = \frac{1}{2^{k/2(1+k-1)}} = \left(\frac{1}{2^{k/2}}\right)^k$$

Důsledek: $\forall k \geq 3 : r(k) > 2^{k/2}$

- dosadíme $n = 2^{k/2}$ do předchozího (předchozí je ostrý odhad, takže $1^k < 1$ funguje)

Důkaz: vezmu náhodný graf G t. ž. každá z $\binom{n}{2}$ hran má pravděpodobnost $1/2$, nezávisle na ostatních. Nechť $K \subseteq V, |K| = k$. $A_K \ldots$ jev, že $G[K]$ je klika. $\Pr[A_K] = \left(\frac{1}{2}\right)^{\binom{k}{2}} = 2^{-\binom{k}{2}}$. Obdobně B_K jev, že vznikla nezávislá množina a $C_K \ldots A_K \cup B_K \ldots \Pr[C_K] = 2 \cdot 2^{-\binom{k}{2}} = 2^{1-\binom{k}{2}}$. $p \ldots$ pravděpodobnost, že $\exists K \subseteq V$ t. ž. nastal jev C_K. Je ji těžké určit, protože jevy nejsou nezavislé (množiny se mohou překrývat), nám ale stačí odhad který předpokládá, že jsou jevy nezávislé:

$$\Pr[C] \leq \sum_{K \in V, |K|=k} \Pr[C_K] = \binom{n}{k} \cdot 2^{1-\binom{k}{2}} < 1$$

- předposlední rovnost je z definice – všechny možné K-tice
- poslední nerovnost je předpoklad věty
- máme, že pravděpodobnost, že nějaká K-prvková množina bude tvořit buďto kliku nebo nezávislou množinu velikosti k je < 1, tedy pravděpodobnost, že to nenastane je > 0, tedy $\exists$ nějaký z náhodných grafů, který tohle nesplňuje
  - pokud pravděpodobnost je nenulová, tak musí existovat nějaké množství grafů, které tenhle jev mají (protože jinak by nerovnost nebyla ostrá)

Důkaz (alternativní) Někomu může použití pravděpodobnosti připadat trochu magické. Důkaz lze ale přeformulovat explicitněji.

Uvažme všechny grafy na n vrcholech. Těch je $2^{\binom{n}{2}}$. Kolik z nich obsahuje kliku nebo nezávislou množinu velikosti alespoň k? Tedy, kolik z nich je "dobrých"? Začněme jednodušeji – označme množinu vrcholů V a mějme $K \subseteq V, |K| = k$. V kolika grafech tvoří K kliku? Hrany uvnitř K jsou fixované, ostatní můžeme nastavovat libovolně. Odpověď je tedy $2^{\binom{n}{2}-\binom{k}{2}}$. Případ nezávislé množiny je symetrický, tudíž v $2\,2^{\binom{n}{2}-\binom{k}{2}} = 2^{\binom{n}{2}-\binom{k}{2}+1}$ grafech bude K klika nebo nezávislá množina.

Nyní zásadní krok: V součtu $\binom{n}{k} 2^{\binom{n}{2}-\binom{k}{2}+1}$ přes všechny takové množiny K jsme započítali každý dobrý graf (nejspíše vícekrát, ale to nevadí). Každý dobrý graf totiž obsahuje kliku nebo nezávislou množinu velikosti **přesně** k. Tento součet je tedy horní mezí pro počet dobrých grafů.

A jsme hotovi. Předpoklad věty je totiž po přenásobení ekvivalentní nerovnosti:

$$\binom{n}{k} 2^{\binom{n}{2}-\binom{k}{2}+1} < 2^{\binom{n}{2}}$$

A z té díky našemu odhadu tranzitivně plyne, že počet dobrých grafů je menší než počet všech grafů. Tedy existuje nedobrý graf na n vrcholech a $r(k,k) > n$.

13. přednáška

Ramseyovy barevné/nekonečné věty

Věta (princip holubníku) pro každé $t, k \in \mathbb{N} \exists N$ t. ž. $\forall c : [n] \mapsto [t]$ platí, že $\forall n \geq N \exists A \subseteq [n], |A| = k$, na níž je funkce c konstantní. [15]

Důkaz: $N = t(k-1)+1$.

Věta (nekonečný princip holubníku) pro každé $t \in \mathbb{N}$ a každé $c : \mathbb{N} \mapsto [t]$ existuje nekonečná množina $A \subseteq \mathbb{N}$, pro níž je funkce c konstantní.

- z „existuje holubník s hodně holuby“ máme „existuje holubník s nekonečně holuby“

Důkaz: rozdělím $\mathbb{N}$ na $B_1, \ldots, B_t$, kde $B_i = \{m \in \mathbb{N} \mid c(m) = i\}$. Protože sjednocením je nekonečná množina pak alespoň jedna musí být nekonečná.

Věta (nekonečná Ramseyova (vícebarevná) věta) pro každé $t \in \mathbb{N}, \forall c : \binom{\mathbb{N}}{2} \mapsto [t] \exists$ nekonečná množina $A \subseteq \mathbb{N}$, pro níž je funkce c na hranách $\binom{A}{2}$ (nekonečný úplný graf) konstantní.

Důkaz: sestrojím posloupnost nekonečných množin $A_1 = \mathbb{N}$ a pro $i = 1, 2, \ldots$ opakujeme: [16]

- vybereme $v_i \in A_i$
- rozdělíme A na $B_i^1, B_i^2 \ldots, B_i^t$ podle toho, jakou barvu má hrana, která množinu spojuje s v_i
  - jelikož A_i je nekonečná, tak $\exists B_i^j$ pro nějakou barvu, která je také nekonečná
- položme $A_{i+1} = B_i^j$

(👀): posloupnost vrcholů $v_1, v_2, \ldots$ má vlastnost, že pokud $i < j$, pak $\{v_i, v_j\}$ má barvu b_i

- v každém kroku se zanořuju, ale při zanoření už platí, že všichni sousedi jsou k v_i spojeni hranou dané barvy
- $\implies$ barva hrany $\{v_i, v_j\}$ závisí pouze na i, ne na j
- mám posloupnost barev $b_1, b_2, b_3, \ldots$
  - je nekonečná, ale opakuje se tu konečně mnoho hodnot
  - aplikuji nekonečný holubník $\implies$ $\exists j \in [t]$ opakující-se nekonečněkrát a takové vrcholy vyberu, jednota barev vychází z pozorování

Věta (Ramseyova vícebarevná věta) $\forall t, k \in \mathbb{N}$ (t počet barev, k velikost kliky) $\exists N \in \mathbb{N}$ t. ž. $\forall c : \binom{[n]}{2} \mapsto [t], \forall n \geq N$ (obarvení K_n t barvami) existuje množina $A \subseteq [n], |A| = k$, pro níž je funkce c na $\binom{A}{2}$ konstantní. [17]

Důkaz: adaptujeme nekonečný na konečný případ – chtěli bychom posloupnost barev $b_1, \ldots, b_{tk}$ – když do toho praštíme holubníkem, tak máme barvu, která je tam k-krát.

- upravím konstrukci množin A_i: beru vždy největší třídu - $|A_{i+1}| \geq \frac{|A_i|-1}{t}$ (max. je větší/roven průměru)
  - potřebuji, aby konstrukce běžela alespoň tk kroků
  - potřebuji, aby $|A_{tk}| \geq 1, |A_{tk-1}| \geq t+1, \ldots, |A_1| \geq \sum_{i=0}^{tk} t^i = \frac{t^{tk+1}-1}{t-1}$
    - na zkoušce nebude – jen bychom měli vědět, že se to takhle dá umlátit

Definice (hypergraf) je zobecněný graf, kde:

- hrany jsou libovolné množiny (místo dvojic, jako v normálním grafu)

[15] „Pokud mám alespoň $\geq N$ prvků a dávám je do t holubníků, pak bude existovat holubník s alespoň k prvky.“

[16] sanity check: $A_1 \supset A_2 \supset \ldots$

[17] „Pokud $n \geq N$, tak každé obarvení K_n t barvami obsahuje jednobarevný K_k jako podgraf.“

- **uniformní** hypergraf – hrany jsou p-prvkové množiny
- p je arita hran (velikost množin), t, k jsou stejné

Věta (nekonečná Ramseyova věta pro p-tice) $\forall p, t \in \mathbb{N}$ a $\forall c : \binom{\mathbb{N}}{p} \mapsto [t] \exists A \subseteq \mathbb{N}$ nekonečná t. ž. c je na $\binom{A}{p}$ konstantní.

Důkaz: indukcí podle p, pro $p = 1$ je to nekonečný holubník (pro $p = 2$ je to Ramsey)

- IP: věta platí pro $p - 1$
- opět konstruuji nekonečnou posloupnost A_i
- v kroku i vyberu $v_i \in A_i$, nechť $A'_i = A_i \setminus \{v_i\}$

- definuji obarvení $(p-1)$-tic A'_i: $c'_i(Q) = c(Q \cup \{v_i\})$, $Q \subseteq A'_i$, $|Q| = p - 1$

- z IP pro A'_i máme, že $\exists B_i \subseteq A'_i$, na jejichž $(p-1)$-ticích je obarvení c'_i konstantní $= b_i \in [t]$ [18] a $A_{i+1} = B_i$ si vezmu do dalšího kroku

(👀): barva p-tice $\{v_{i_1}, \ldots, v_{i_p}\}$ (vzhledem k vzniklé posloupnosti $v_1, v_2, \ldots$), kde $i_1 < i_2 < i_3 < i_p$ závisí pouze na barvě prvku v_{i_1}

- vyberu z barev nějakou opakující-se nekonečněkrát a vrcholy s příslušnými indexy tvoří A

Věta (Ramseyova věta pro p-tice) $\forall p, t, k \in \mathbb{N} \exists N \in \mathbb{N}$ t. ž. $\forall n \geq N, \forall c : \binom{[n]}{p} \mapsto [t]$ $\exists A \subseteq [n], |A| = k$ t. ž. c je na $\binom{A}{p}$ konstantní.

Důkaz: mějme p, k, t z předpokladu věty. Uvážíme $c_i : \binom{[n]}{p} \mapsto [t]$. To je *dobré*, pokud $\exists$ k-prvková jednobarevná podmnožina, jinak je *špatné*. Věta tedy tvrdí, že $n \geq N$ jsou všechna c *dobrá*.

Sporem: předpokládejme, že pro nekonečně mnoho n $\exists$ *špatné* obarvení.

(👀): Pokud S_n je množina *špatných* obarvení a S_n je neprázdné, pak S_{n-1} je neprázdné, protože mám-li *špatné* obarvení p-tic nad n, tak mohu zapomenout na n-tý prvek a tak dostanu *špatné* obarvení i na $n - 1$.

- **zůžení** $z(c)(Q) = c(Q), Q \subseteq [n-1], |Q| = p$ (prostě odeberu vrchol)

Strukturu *špatných* obarvení popíšeme stromem, kde hladiny jsou obarvení S_n; platí:

- všechny hladiny jsou neprázdné (předpoklad pro spor)
- všechny hladiny jsou konečné (nad S_n může být only so much obarvení)

Lemma (Königovo) nekonečný zakořeněný strom s konečnými stupni obsahuje nekonečnou cestu z kořene.

Důkaz: pokud máme vrcholy $v_1, v_2, \ldots, v_{i-1}$ na cestě, tak v_i vezmu jako kořen podstromu, který je nekonečný a opakuju.

Díky tomuto lemmatu víme, že $\exists$ nekonečná cesta z S_0. Z nekonečné Ramseyovy věty ale víme, že kdyby tomu tak bylo, tak neplatí, protože by existovalo nekonečné obarvení přirozených čísel (podle nekonečné cesty v tomto stromu).

Forma zkoušky

Zdroje/materiály

- https://research.koutecky.name/db/teaching:kg12021_prednaska – stránka cvičení
  - odkaz na všechny obrázky, zdroje, nahrávky cvičení
- Poznámky Václava Končického z roku 2019.
- https://oeis.org/wiki/List_of_LaTeX_mathematical_symbols – matematické symboly

[18] Pomocné obarvení $(p-1)$-tic stejnými barvami, jako byla p-tice s vrcholem v_i.

Poděkování

- Matěji Kripnerovi za řadu PR opravujících chyby a přidávajících dodatečné informace.
- Filipu Peškovi za upozornění na několik překlepů/chyb v důkazech a definicích.
- Vojtěchu Kočandrlemu za PR a upozornění na překlepy.