Kombinatorika a grafy

Karel Velička

20. ledna 2024

Doc. RNDr. Vít Jelínek Ph.D.

Obsah

1 Definice **2**
1.1 Vytvořující funkce . . . 2
1.2 Projektivní roviny . . . 2
1.3 Toky v sítích . . . 2
1.4 Ramseyovy věty . . . 3
1.5 Samoopravné kódy . . . 3

2 Věty a tvrzení **4**
2.1 Odhady kombinatorických funkcí . . . 4
2.2 Vytvořující funkce . . . 6
2.3 Projektivní roviny . . . 8
2.4 Toky v sítích . . . 10
2.5 Cayleyho vzorec . . . 14
2.6 Počítání dvěma způsoby . . . 15
2.7 Ramseyovy věty . . . 17
2.8 Samoopravné kódy . . . 18

1 Definice

1.1 Vytvořující funkce

Definice 1. *(Vytvořující funkce):* Vytvořující funkce posloupnosti $a_0, a_1, \ldots = (a_n)_{n=0}^{\infty} \in \mathbb{R}$ je funkce proměnné x definována jako součet $f(x) = \sum_{n=0}^{\infty} a_n x^n$.

Definice 2. *(Catalanova čísla):* $(C_n)_{n=0}^{\infty}$ udávájí počet binárních stromů s n vnitřními vrcholy.

1.2 Projektivní roviny

Definice 3. *(Hypergraf):* je dvojice (V, H), kde H je množina podmnožin V, tedy $H \subseteq \mathcal{P}(V)$. Prvky V jsou *vrcholy* a prvky H jsou *hyperhrany.*

Definice 4. *(Graf incidence):* hypergrafu (V, H) je bipartitní graf s partitami V a H, kde mezi $x \in V$ a $h \in H$ vede hrana $\iff x \in h$.

Definice 5. *(Projektivní rovina):* je hypergraf $(X, \mathcal{P})$, kde prvky X jsou *body* a prvky $\mathcal{P}$ jsou *přímky*, t.ž.:

(i) *Každé dva různé body určují právě jednu přímku.*
$\forall x, y \in X, x \neq y,\ \exists! p \in \mathcal{P} : \{x, y\} \subseteq p$

(ii) *Každé dvě různé přímky se protínají v právě jednom bodě.*
$\forall p, q \in \mathcal{P}, p \neq q : |p \cap q| = 1$

(iii) *Existuje čtveřice bodů taková, že žádné tři body neleží na stejné přímce.*
$\exists C \in X, |C| = 4,\ \forall p \in \mathcal{P} : |p \cap C| \leq 2$

Definice 6. *(Řád projektivní roviny):* KPR $(X, \mathcal{P})$ má *řád* $n \in \mathbb{N}$, pokud každá její přímka má $n + 1$ bodů.

Definice 7. *(Duální projektivní rovina):* k projektivní rovině $(X, \mathcal{P})$ je hypergraf $(X^*, \mathcal{P}^*)$, kde:

(i) $X^* = \mathcal{P}$,

(ii) pro $x \in X$ definujeme $x^* := \{x \in p \mid p \in \mathcal{P}\}$,

(iii) $\mathcal{P}^* = \{x^* \mid x \in X\}$.

1.3 Toky v sítích

Definice 8. *(Toková síť):* Je pětice (V, E, z, s, c):

- $V \equiv$ množina vrcholů
- $E \equiv$ množina orientovaných hran $E \subseteq V \times V$
- $z \in V \equiv$ zdroj
- $s \in V \setminus \{z\} \equiv$ stok/ spotřebič
- $c : E \to [0, +\infty) \equiv c(e)$ je kapacita hrany e

Definice 9. *(Tok):* V síti (V, E, z, s, c) je funkce $f : E \to [0, +\infty)$ splňující:

(i) $\forall e \in E : 0 \leq f(e) \leq c(e)$

(ii) $\forall x \in V \setminus \{z, s\} : \sum_{\substack{y \in V \\ (x,y) \in E}} f(x, y) = \sum_{\substack{y \in V \\ (x,y) \in E}} f(x, y)$, respektive $\forall x \in V \setminus \{z, s\} : f[In(x)] = f[Out(x)]$.

Definice 10. *(Velikost toku):* Velikost toku f v síti (V, E, z, s, c) je $w(f) := f[Out(z)] - f[In(z)]$.

Definice 11. *(Maximální tok):* je takový tok, který má největší velikost.

Definice 12. *(Řez):* v síti (V, E, z, s, c) je množiana hran $R \subseteq E$, t.ž.: každá orientovaná cesta ze z do s má neprázdný průnik s R.

- *Kapacita* řezu $R \equiv c(R) = \sum_{e \in R} c(e)$
- *Minimální* řez je řez, který má ze všech řezů nejmenší kapacitu.

Definice 13. *(Elementární řez):* Nechť $A \subseteq V$ je množina vrcholů, t.ž. $z \in A$ a $s \notin A$. Potom zjevně $Out(A)$ tvoří řez. Každý takový řez je *elementární řez.*

Definice 14. *(Nenasycená cesta):* Nechť f je tok v síti (V, E, z, s, c). *Nenasycená cesta* pro f je neoreintovaná cesta $x_1e_1x_2e_2 \dots x_{k-1}e_{k-1}x_ke_kx_{k+1}$, kde $\forall i = 1, \dots, k$:

- e_i je buď *dopředná hrana*, tedy $e_i = (x_i, x_{i+1})$, nebo
- e_i je *zpětná hrana*, tedy $e_i(x_{i+1}, x_i)$.

Zároveň platí $f(e_i) < c(e_i)$ pro každou dopřednou hranu a $f(e_i) > 0$ pro každou zpětnou hranu.

Definice 15. *(Zlepšující cesta):* Zlepšující cesta pro f je nenasycená cesta ze z do s.

Definice 16. *(Párování):* v grafu $G = (V, E)$ je množina hran $M \subseteq E$, t.ž. každý vrchol patří do nejvýše jedné hrany z M.

Definice 17. *(Vrcholové pokrytí):* v grafu $G = (V, E)$ je množina vrcholů $C \subseteq V$, t.ž. každá hrana obsahuje alespoň jeden vrchol z C.

Definice 18. *(Systím různých reprezentantů - SRR):* v hypergrafu $H = (V, E)$ je funkce $r : E \to V$, t.ž.:

1. $\forall e \in E : r(e) \in e$, kde $r(e)$ je *reprezentant* hyperhrany e
2. $\forall e, f \in E : e \neq f \implies r(e) \neq r(f)$, tedy funkce r je prostá

Definice 19. *(Hranový řez):* $F \subseteq E$ je hranový řez v G pokud $G \setminus F$ je nesouvislý.

Definice 20. *(Hranová $k-$souvislost):* G je hranově $k-$souvislý, pokud neobsahuje žádný hranový řez velikosti menší než k.

Definice 21. *(Vrcholová k-souvislost):* Graf G je *vrcholově k-souvislý*, pokud má alespoň $k+1$ vrcholů a neobsahuje žádný vrcholový řez velikosti $< k$.

Definice 22. *(Vrcholová souvislost):* grafu G, značeno $K_v(G)$, je největší k, t.ž.: G je vrcholově k-souvislý.

1.4 Ramseyovy věty

Definice 23. *(Klika):* v grafu $G = (V, E)$ je množina vrcholů, t.ž. každé dva jsou spojené hranou.

Definice 24. *(Nezávislá množina):* v grafu $G = (V, E)$ je množina vrcholů, t.ž. žádné dva nejsou spojené hranou.

1.5 Samoopravné kódy

Definice 25. *(Hammingova vzdálenost):* Pro $x, y \in \mathbb{Z}_2^n$ je *Hammingova vzdálenost* $d(x, y) :=$ počet i, t.ž. $x_i \neq y_i$.

Definice 26. *(Hammingova váha):* $||x|| :=$ počet i, t.ž. $x_i \neq 0$.

Definice 27. *(Minimální vzdálenost):* pro kód $C \in \mathbb{Z}_2^n$ je $\Delta(C) := \min\limits_{\substack{x,y \in C \\ x \neq y}} d(x, y)$.

Definice 28. *((n, k, d)-kód):* je množina $C \in \mathbb{Z}_2^n$ taková, že $|C| = 2^k$ a $\Delta(C) = d$.

Definice 29. *(Lineární kód):* je kód $C \in \mathbb{Z}_2^n$, který je vektorový podprostor $\mathbb{Z}_2^n$.

Definice 30. *(Generující matice kódu C):* pro lineární (n, k, d)-kód je matice $G \in \mathbb{Z}_2^{k \times n}$, jejíž řádky tvoří bázi C.

Definice 31. *(Kódování):* Nechť C je (n, k, d)-kód pro $k \in \mathbb{N}$, tak *kódování* pro C je bijekce $\mathbb{Z}_2^k \to C$.

Definice 32. *(Dekódování):* (n, k, d)-kódu C je funkce $g : \mathbb{Z}_2^n \to C$ taková, že $\forall x \in \mathbb{Z}_2^n : d(x, g(x)) = \min\limits_{y \in C} d(x, y)$.
(Přiřazujeme nejbližší slovo; slovo s nejmenší vzdáleností.)

Definice 33. *(Duální kód k C "orotgonální doplněk"):* $C^\perp := \{\langle x, y \rangle = 0 \mid y \in \mathbb{Z}_2^n, \forall x \in C\}$

Definice 34. *(Kontrolní matice):* Nechť C je lineární (n, k, d)-kód. *Kontrolní matice* kódu C je matice, jejíž řádky tvoří bázi $C^\perp$.

Definice 35. *(Hammingovy kódy):* Nechť $r \in \mathbb{N}, r \geq 2$, nechť K_r je matice s r řádky a $2^r - 1$ sloupci, jejíž sloupce jsou nenulové a různé. Potom Hammingovy kódy H_r jsou kódy s kontrolní maticí K_r.

2 Věty a tvrzení

2.1 Odhady kombinatorických funkcí

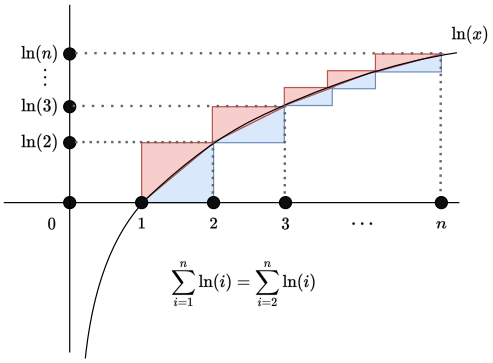
Věta 1. *(Odhad faktoriálu 2):*

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

Důkaz: Dokazovat budeme za pomoci integrálu a součtu, $n!$ je ale násobek, musíme proto užít vlastnosti logaritmů:

$$\ln(n!) = \sum_{i=1}^{n} \ln(i) = \sum_{i=2}^{n} \ln(i).$$

Obr. 1: *Součet "schodů" podél křivky*



- *Dolní odhad:* Budeme sčítat "schody" nad křivkou:

$$\begin{aligned} \ln(n!) &\geq \int_1^n \ln(x)dx = \\ &= [x\ln(x) - x]_1^n = n\ln(n) - n + 1 \implies \\ n! &= e^{n\ln n - n + 1} = e\left(\frac{n}{e}\right)^n \end{aligned}$$

- *Horní odhad:* Podobně jako dolní odhad, jen budeme sčítat "schody" pod křivkou:

$$\sum_{i=1}^{n-1} \ln(i) = \ln((n-1)!) \leq n\ln(n) - n + 1$$

Vy výsledku dostaneme:

$$\begin{aligned} n\ln n - n + 1 \geq ln((n-1)!) &\implies e^{n\ln n - n + 1} \geq (n-1)! \implies \\ &\implies n \cdot e^{n\ln n - n + 1} \geq n! \implies \\ &\implies n \cdot e\left(\frac{e}{n}\right)^n \geq n! \end{aligned}$$

□

Věta 2. *(Odhad kombinačního čísla):* Pro $1 \leq k \leq n$ platí $\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{en}{k}\right)^k$.

Důkaz: Budeme využívat vztahu $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

- *Dolní odhad:*

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

Dostáváme, že $\frac{n}{k}$ je nejmenší a zbytek je rostoucí posloupnost.

- *Horní odhad:*

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdot\ldots\cdot(n-k+1)}{k!} \leq \frac{n^k}{\left(\frac{k}{e}\right)^k} = \left(\frac{e\cdot n}{k}\right)^k$$

  Tento vztah platí, protože $\left(\frac{k}{e}\right)^k$ je dolní odhad $k!$.

□

Věta 3. *(Odhad binomického čísla $\binom{2m}{m}$):*

$$\forall m \in \mathbb{N}_0 : \frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}$$

Důkaz: Definujme $P := \frac{\binom{2m}{m}}{2^{2m}}$ a dokažme, že $\frac{1}{2\sqrt{m}} \leq P \leq \frac{1}{\sqrt{2m}}$.

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

- *Horní odhad:*

$$\begin{aligned} P^2 &= \frac{1\cdot 1\cdot 3\cdot 3\cdot 5\cdot 5\cdot\ldots\cdot(2m-1)\cdot(2m-1)}{2\cdot 2\cdot 4\cdot 4\cdot 6\cdot 6\cdot\ldots\cdot(2m)\cdot(2m)} \overset{\text{Pozorování 2.}}{=} \\ &= 1\cdot\frac{1\cdot 3}{2\cdot 2}\cdot\frac{3\cdot 5}{4\cdot 4}\cdot\frac{5\cdot 7}{6\cdot 6}\cdot\ldots\cdot\frac{(2m-3)\cdot(2m-1)}{(2m-2)\cdot(2m-2)}\cdot\frac{2m-1}{(2m)\cdot(2m)} \leq \\ &\leq \frac{2m-1}{(2m)\cdot(2m)} < \frac{1}{2m}, \text{ a proto tedy } P \leq \frac{1}{\sqrt{2m}}. \end{aligned}$$

- *Dolní odhad:*

$$\begin{aligned} P^2 &= \frac{1\cdot 1\cdot 3\cdot 3\cdot 5\cdot 5\cdot\ldots\cdot(2m-1)\cdot(2m-1)}{2\cdot 2\cdot 4\cdot 4\cdot 6\cdot 6\cdot\ldots\cdot(2m)\cdot(2m)} \overset{\text{Pozorování 3.}}{=} \\ &= \frac{1}{2}\cdot\frac{3\cdot 3}{2\cdot 4}\cdot\frac{5\cdot 5}{4\cdot 6}\cdot\ldots\cdot\frac{(2m-1)\cdot(2m-1)}{(2m-2)\cdot(2m)}\cdot\frac{1}{2m} \geq \\ &\geq \frac{1}{4m}, \text{ a proto tedy } P^2 \geq \frac{1}{4m} \text{ a } P \geq \frac{1}{2\sqrt{m}}. \end{aligned}$$

□

2.2 Vytvořující funkce

Věta 4. *(Zobecněná binomická věta):* Pro $d \in \mathbb{R}$ platí $(1+x)^d = \sum_{n=0}^{\infty} \binom{d}{n} x^n$, pro $|x| < 1$.

Důkaz: Označme $f(x) = (1+x)^d$. Vidíme, že:

$$\begin{aligned} f'(x) &= d(1+x)^{d-1} \\ f''(x) &= d(d-1)(1+x)^{d-2} \\ &\vdots \\ f^{(n)}(x) &= d(d-1)\cdot \ldots \cdot (d-n+1)(1+x)^{d-n} \end{aligned}$$

Určíme Taylorovým polynomem. Nechť $a_0, a_1, \ldots$ je posloupnost vytvořující funkce $f(x)$, potom $a_n = \frac{f^{(n)}(0)}{n!}\binom{d}{n}$. □

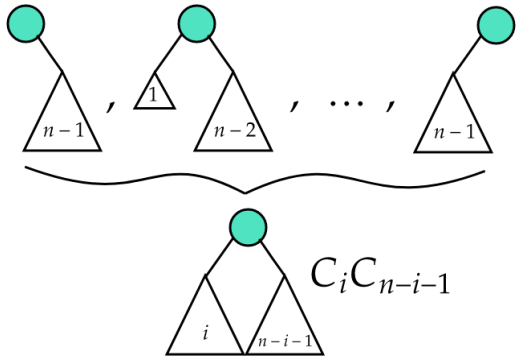
Fakt 1. Mějme funkci $f(x) = \frac{P(x)}{Q(x)}$, kde $P(x)$ a $Q(x)$ jsou polynomy se stupněm $d(P(x)) < d(Q(x))$.
Nechť $Q(x)$ má navzájem různé reálné kořeny $\rho_1, \rho_2, \ldots, \rho_k$ a nechť n_i označuje stupeň kořenu ρ_i.
Předpokládejme, že $Q(x)$ nemá nereálné kořeny, tedy $Q(x) = \gamma \cdot (x-\rho_1)^{n_1}(x-\rho_2)^{n_2} \cdot \ldots \cdot (x-\rho_k)^{n_k}$, kde $\gamma \in \mathbb{R}$.
Potom $f(x)$ se dá vyjádřit jako součet parciálních zlomků pro kořeny $\rho_1, \ldots, \rho_k$, kde parciální zlomky pro kořen ρ_i mají stupeň nejvýše n_i, neboli:

$$\exists \alpha_{i,j} \in \mathbb{R} : f(x) = \sum_{i=1}^{k} \sum_{j=1}^{n_i} \frac{\alpha_{i,j}}{(x-\rho_i)^j}.$$

Příklad 1. *(Odvození Catalanova čísla):*

Mějme funkci $C(x) := \sum_{n=0}^{\infty} C_n x^n, \quad C_0 = 1 \quad \text{a} \quad C_n = C_0 C_{n-1} + C_1 C_{n-2} + ... + C_{n-1} C_0 = \sum_{i=0}^{n-1} C_i C_{n-i-1}$:

Obr. 2: *Odvození součtu Catalanových čísel pro* $\forall n \geq 1$



$$\sum_{n=1}^{\infty} C_n x^n = \sum_{n=1}^{\infty} \left(\sum_{i=0}^{n-1} C_i C_{n-i-1} \right) x^n \implies$$
$$C(x) - 1 = x \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} C_i C_{n-i} \right) x^n = x \cdot C^2(x)$$

Dostáváme tak: $C(x) = 1 + xC^2(x)$, což si můžeme zapsat jako kvadratickou rovnici a vyjdou nám dvě řešení:

$$xC^2(x) - C(x) + 1 \implies \begin{cases} \frac{1+\sqrt{1-4x}}{2x} = C^+(x) & \text{není řešením - diverguje} \\ \frac{1-\sqrt{1-4x}}{2x} = C^-(x) & \text{konverguje k 1 při } x \to 0 \end{cases}$$

Počítáme tak dál a vyjádříme vzorec pro n-tý člen:

$$\begin{aligned} C_n &:= [x^n] \frac{1-\sqrt{1-4x}}{2x} = [x^{n+1}] \frac{1-\sqrt{1-4x}}{2} = [x^{n+1}] \left(\frac{1}{2} - \frac{\sqrt{1-4x}}{2} \right) = \\ &= -\frac{1}{2} [x^{n+1}] \sqrt{1-4x} = -\frac{1}{2} (-4)^{n+1} [x^{n+1}] \sqrt{1-x} = -\frac{1}{2} (-4)^{n+1} [x^{n+1}] (1-x)^{\frac{1}{2}} = \\ &\overset{ZBV}{=} -\frac{1}{2} (-4)^{n+1} [x^{n+1}] \binom{\frac{1}{2}}{n+1} = (-1)^n 2^{2n+1} \cdot \frac{\frac{1}{2}(\frac{1}{2}-1)(\frac{1}{2}-2) \cdot ... \cdot (\frac{1}{2}-n)}{(n+1)!} = \\ &= (-1)^n 2^{2n+1} \cdot \frac{\frac{1}{2}(-\frac{1}{2})(-\frac{3}{2}) \cdot ... \cdot (-\frac{2n-1}{2})}{(n+1)!} = 2^n \cdot \frac{1 \cdot 3 \cdot 5 \cdot ... \cdot (2n-1)}{(n+1)!} = \\ &= \frac{1 \cdot 3 \cdot 5 \cdot ... \cdot (2^n n!)}{(n+1)! n!} = \frac{(2n)!}{(n+1)! n!} = \frac{1}{n+1} \binom{2n}{n}. \end{aligned}$$

2.3 Projektivní roviny

Tvrzení 1. *Pro konečnou projektivní rovinu $(X, \mathcal{P})$ řádu n platí:*

(a) Každý bod KPR patří do právě $n+1$ přímek.

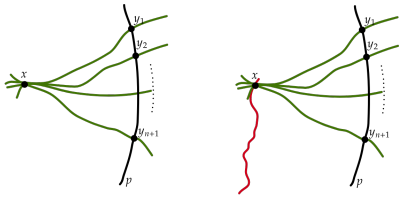
(b) Počet bodů je $|X| = n^2 + n + 1$.

(c) Počet přímek je $|\mathcal{P}| = n^2 + n + 1$.

Důkaz: Budeme postupně dokazovat jednotlivé body.

(a) Zvolme si $x \in X$ a dle Lemmatu víme, že $\exists p \in \mathcal{P} : x \neq p$.
Označme $p = \{y_1, y_2, \ldots, y_{n+1}\}$ a definujme přímky $g_1, g_2, \ldots, g_{n+1}$, kde $g_i = \overline{xy_i}$.
Tvrdíme, že pro $i \neq j$ je $g_i \neq g_j$, protože kdyby ne, tak $\{y_i, y_j\} \subseteq g_i \cap p$, což je spor. Tvrdíme $\forall r \in \mathcal{P}$, kde pokud $x \in r$, tak platí $r \in \{g_1, \ldots, g_{n+1}\}$.

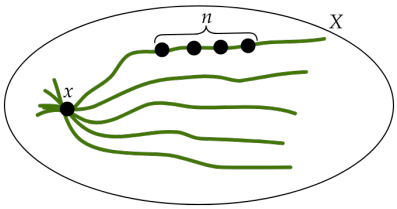
Obr. 3: *Obrázek důkazu (a)*



Zvolme si přímku $r \in \mathcal{P}$, t.ž.: $x \in r$, což má podle axiomu zřejmě $|r \cap p| = 1$. Dále nechť y je prvek $r \cap p$, potom, potom $r = \overline{xy_i} = g_i$. Tedy bodem x prochází právě $n+1$ přímek.

(b) Zvolme si $x \in X$ a nechť $p_1, p_2, \ldots, p_{n+1}$ jsou přímky procházející x. Všimněme si, že každý bod $y \in X \setminus \{x\}$ patří do právě jedné z přímek $p_1, p_2, \ldots, p_{n+1}$.
Takže $|X| = |\{x\}| + |p_1 \setminus \{x\}| + |p_2 \setminus \{x\}| + \cdots + |p_{n+1} \setminus \{x\}| = 1 + (n+1)n = n^2 + n + 1$.

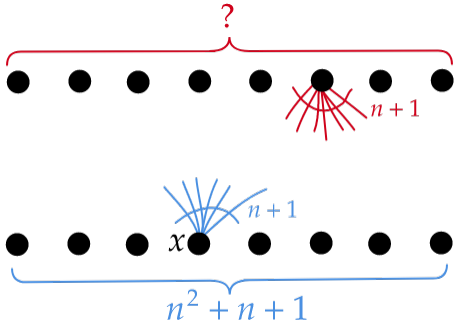
Obr. 4: *Obrázek důkazu (b)*



(c) Počítáme počet dvojic $(x, p) \in X \times \mathcal{P}$ takových, že $x \in p$. To lze udělat dvěma způsoby:
dvojic je $|X|(n+1) = (n^2 + n + 1)(n+1)$ a dvojic $|\mathcal{P}|(n+1) = (n^2 + n + 1)(n+1) \implies$

$$|\mathcal{P}|(n+1) = (n^2 + n + 1)(n+1) \implies |\mathcal{P}| = n^2 + n + 1$$

Obr. 5: *Obrázek důkazu (c)*



□

Tvrzení 2. *Duální projektivní rovina* $(X^*, \mathcal{P}^*)$ *je projektivní rovina.*

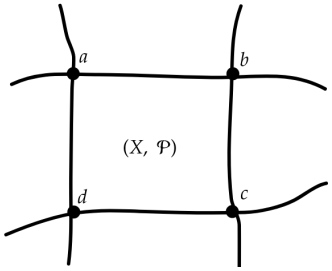
Důkaz: Musíme dokázat všechny axiomy klasické projektivní roviny. $(X^*, \mathcal{P}^*)$ splňuje:

(i) $\forall p, q \in X^*, p \neq q, \exists! x^* \in \mathcal{P}^* : \{p, q\} \subseteq x^* \iff \forall p, q \in \mathcal{P}, p \neq q, \exists! x \in X : x \in p \ \ \& \ \ x \in q$
$\iff (X, P)$ splňuje (ii).

(ii) Vychází z (i). Tedy splňuje $(ii) \iff (X, \mathcal{P})$ splňuje (i).

(iii) $\exists C^* \subseteq X^*, |C^*| = 4 \ \ \& \ \ \forall x^* \in \mathcal{P}^* : |x^* \cap C^*| \leq 2 \iff \exists C^* \subseteq \mathcal{P}^*, |C^*| = 4 \ \ \& \ \ \forall x \in X :$ *Nejvýše dvě přímky z* C *procházejí skrz* x :
Ukážeme, že $(X, \mathcal{P})$ splní výše uvedené tvrzení a to tak, že ukážeme, že $\{a, b, c, d\} \subseteq X$, t.ž.: žádné tři body C neleží na jedné přímce.

Obr. 6: *Protipříklad*



Předpokládejme $C^* := \{\overline{ab}, \overline{bc}, \overline{cd}, \overline{ad}\}$. Zvolme si například přímky $\overline{ab}, \overline{bc}, \overline{cd}$:
Jelikož $\overline{ab} \cap \overline{bc} = \{b\}$ a $\overline{bc} \cap \overline{cd} = \{c\}$, tak platí, že $\overline{ab} \cap \overline{bc} \cap \overline{cd} = \emptyset$, což nám dává spor.

□

Konstrukce konečné projektivní roviny řádu $n \in \mathbb{N}$

(1) Nechť T *je konečné těleso s* n *prvky, potom uvažujme vektorový prostor* $V = T^3 = \{(x, y, z) \mid x, y, z \in T\}$. *Platí* $|V| = n^3$.

(2) Nechť X *je množina podprostorů dimenze* 1 *ve* V. *Platí* $|X| = \frac{n^3 - 1}{n - 1} = n^2 + n + 1$.

(3) Pro každý podprostor $p \subseteq V$ *dimenze* 2 *definujme* $\tilde{p} := \{x \in X \mid x \subseteq p\}$.

(4) $\mathcal{P} = \{\tilde{p} \mid p$ *je podprostor* V *dimenze* $2\}$. *(*$|\mathcal{P}| = n^2 + n + 1 = |X|$, *v* $\dim = 1$, *protože orotgonální doplněk)*

Tvrdím, že $(X, \mathcal{P})$ *je projektivní rovina.*

(i) Z lineární nezávislosti.

(ii) P, Q *podprostory* V *:* $\overbrace{\dim P}^{2} + \overbrace{\dim Q}^{2} - \overbrace{\dim P \cap Q}^{1} = \dim(\overbrace{obalu\ P \cup Q}^{3})$.

(iii) Například $C = \{(1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 1)\}$.

2.4 Toky v sítích

Fakt 2. *V každé tokové síti existuje maximální tok.*

Věta 5. Nechť f je tok v síti (V, E, z, s, c), potom následující tvrzení jsou ekvivalentní:

(i) f je maximální

(ii) f nemá zlepšující cestu

(iii) Existuje řez R, t.ž.: $w(f) = c(R)$.

Důkaz: Dokážeme postupně implikace.

- $(i) \implies (ii)$: Kdyby měl f nějakou zlepšující cestu, tak můžeme zvětšit f a ten tak potom není maximální.
- $(iii) \implies (i)$: Víme, že pro libovolný řez R' a libovolný tok f' platí, že $w(f') \leq c(R')$. Kdyby f nebyl maximální, tak existuje tok f^+ splňující $w(f^+) > w(f)$.

  Potom pro každý řez R platí, že $c(R) \geq w(f^+) > w(f)$, tedy neexistuje žádný řez R splňující $c(R) = w(f)$.
- $(ii) \implies (iii)$: Nechť f je tok, který nemá zlepšující cestu.
  Definujeme si množinu $A = \{x \in V \mid$ ze z do x vede nenasycená cesta$\}$. Zjevně $z \in A, s \notin A$ a dále definujeme $R := Out(A) = \{u, v \in E \mid u \in A, v \notin A\}$.

  Můžeme si všimnout, že $\forall e \in Out(A) : f(e) = c(e)$ a analogicky $\forall e' \in In(A) : f(e') = 0$.

  Z *(Lemmatu 3.)* dostáváme, že:

$$w(f) = \underbrace{f[Out(A)]}_{c(Out(A))} - \underbrace{f[In(A)]}_{0} = c(Out(A)) = c(R).$$

□

Důsledek 1. *(Minimaxová věta o toku a řezu)* Nechť $f_{\max}$ je maximální tok a $R_{\min}$ je minimání řez v (V, E, z, s, c), potom $w(f_{\max}) = c(R_{\min})$.

Důkaz: Budeme dokazovat (i) $w(f_{\max}) \leq c(R_{\min})$ a (ii) $w(f_{\max}) \geq c(R_{\min})$

(i) Triviální. Víme díky předchozímu lemmatu. Pro každý tok f' a pro každý řez R' platí $w(f') \leq c(R')$.

(ii) Díky předchozí větě. Existuje řez R, t.ž.: $w(f_{\max}) = c(R) \geq c(R_{\min})$.

□

Důsledek 2. V síti, kde všechny kapacity jsou celočíselné, Ford-Fulkersonův algoritmus nalezne maximální tok, který je také celočíselný.
Algoritmus FORD-FULKERSON(G):

1. $f \leftarrow$ nulový tok
2. **while** existuje zlepšující cesta P ze $z \to s$ **do**:
3. $\quad \varepsilon \leftarrow \min_{e \in E(P)} r(e)$.
4. $\quad$ Zvětšíme tok f podél P o ε (každé hraně e po směru zvětšíme $f(e)$ a hranám proti směru zmenšíme $f(e)$)
5. **return** tok f.

Pozorování 1. *Pokud M je párování a C je vrcholové pokrytí v $G = (V, E)$, tak $|M| \leq |C|$.*

Důkaz: Každá hrana z M musí být pokrytá vrcholem z C a zároveň 1 vrchol z C, pokryje nejvýše 1 hranu z M. □

Věta 6. *(König-Egerváty):* V každém bipartitním grafu má největší párování stejnou velikost, jako nejmenší vrcholové pokrytí.

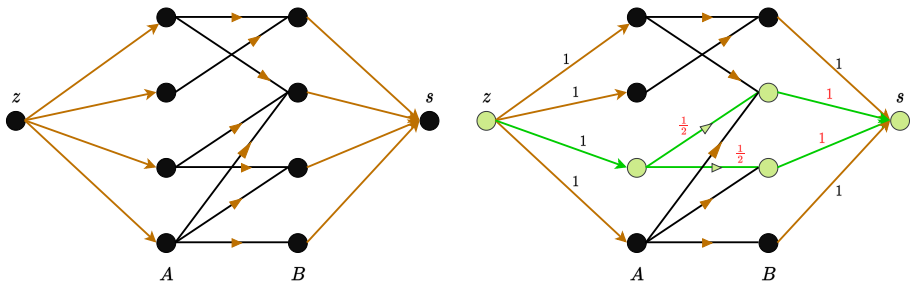
Důkaz: Nechť $G = (V, E)$ je bipartitní graf s partitami A, B. Vytvořme tokovou síť $(V \cup \{z, s\}, E^+, z, s, c)$, kde $E^+ = \{zx \mid x \in A\} \cup \{ys \mid y \in B\} \cup \{xy \mid \{xy\} \in E \ \ \& \ \ x \in A \ \ \& \ \ y \in B\}$ a $c(zx) = c(ys) = 1$ pro $x \in A, y \in B$ a $c(xy) = |A| + |B| + 1$ (záměrně hodně vysoké, aby nemohly nic omezovat - dejme tomu ∞).

Nechť $C_{\min}$ je nejmenší vrcholové pokrytí v G a $M_{\max}$ je největší párování v G.

- Víme, že $|M_{\max}| \leq |C_{\min}|$, a to z *(Pozorování 7.)*.
- Nechť f je maximální tok v té síti a R je minimání řez. Díky *minimaxové větě* víme, že $w(f) = c(R)$ a nakonec BÚNO f má celočíselné hodnoty.

  Definujeme si množinu $M_f = \{\{x, y\} \in E \mid f(x, y) > 0\}$, neboli že v maximálním toku po hranách něco těče. Zjevně je M_f párování v G a navíc $|M_f| = w(f)$. *(Protože kdyby se stalo, že máme 2 hrany z A do B se společným vrcholem, tak by přiteklo do A ze zdroje 1 a odteklo z B ze dvou vrholů do stoku v součtu 2 - tok ale musí být celočíselný, takže dostaneme spor).*

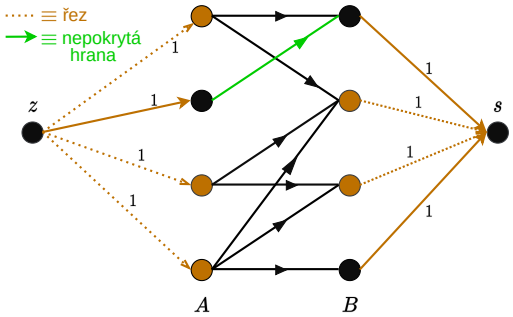
Obr. 7: *Příklad bipartitního grafu.*



(a) *Vytvoříme síť a zorientujeme hrany* (b) *Spor s celočíselným ohodnocením*

Definujeme si $C_R := \{x \in A \mid zx \in R\} \cup \{y \in B \mid ys \in R\}$. Všimněme si, že R neobsahuje žádnou hranu z A do B a jistě je tak C_R vrcholové pokrytí G.

Obr. 8: *Obrázek vzniklé sporné nepokryté hrany v biparitním grafu.*



Máme C_R, t.ž. za každou řez. hranu ze z vložím vrchol z A a za každou řez. hranu do s vložím vrchol z B.

Kdyby C_R nebylo pokrytí, tak existuje nepokrytá hrana $\{x, y\} \in E$ a potom cesta $z \to x \to y \to s$ by byla ve sporu s tím, že R je řez. *(protože by skrz tuto hranu vedla orientovaná cesta ze z do s).*

Navíc platí, že $|C_R| = |R| = c(R)$. Dostali jsme tak:

$$|C_{\min}| \leq |C_R| = c(R) \overset{\text{minimax}}{=} w(f) = |M_f| \leq |M_{\max}|.$$

□

Věta 7. *(Hallova):* Nechť G je bipartitní graf s partitami A, B. Potom G má párování velikosti

$$|A| \iff \forall X \subseteq A : |N(X)| \geq |X|.$$

Důkaz: Musím dokázat obě implikace.

$\Longrightarrow$ Pokud existuje párování velikosti $|A|$, tak pro každou $X \subseteq A$ existuje $|X|$ vrcholů spárovaných s X a ty patří do $N(X)$. Tedy $|N(X)| \geq |X|$.

$\Longleftarrow$ Pro spor. Nechť M je největší párování G, t.ž.: $|M| < |A|$. Existuje pokrytí C, kde $|C| = |M| < |A|$. Definujeme si $C_A := C \cap A$, $C_B := C \cap B$ a $X := A \setminus C_A$.

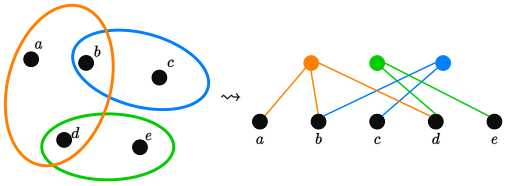
Zjistíme, že $N(X) \subseteq C_B$ a navíc, že $|X| = |A| - |C_A| > |C_B| \geq |N(X)|$, což nám dává spor.

□

Věta 8. *(Hallova - hypergrafová verze):* Hypergraf $H = (V, E)$ má SRR $\iff \forall F \subseteq E : \left|\bigcup_{e \in F} e\right| \geq |F|$.

Důkaz: Nechť $H = (V, E)$ je hypergraf, nechť I_H je jeho graf incidence.
Všimneme si, že H má SRR $\iff$ I_H má párování velikosti $|E|$.

Obr. 9: *Incidence a párování*



Dále si všimneme, že Hallova podmínka pro H, $\iff \forall F \subseteq E : \left|\bigcup_{e \in F} e\right| \iff$ bipartitní Hallova podmínka pro I_H a partitu E. Mezi těmito pozorováními platí ekvivalentní vztah díky bipartitní Hallově podmínce. □

Věta 9. *(Menger - hranová xy-verze):* Pro dva různé vecholy x, y grafu G platí, že G obsahuje $\forall k \in \mathbb{N}$ hranově disjunktních cest z x do y $\iff$ G neobsahuje hranový $xy-$řez velikosti menší než k.

Důkaz: Dokazujeme dvě implikace:

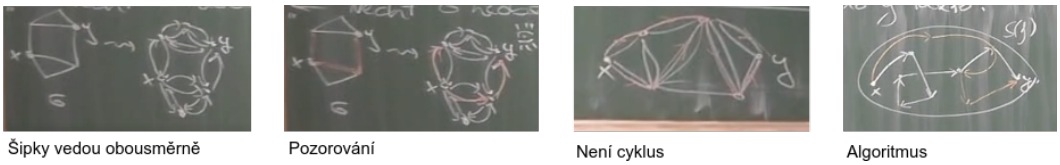
$\Longrightarrow$ Pokud mám k hranově disjunktních cest z x do y, tak každý hranový $xy-$řez musí dosahovat ≥ 1 hranu z každé té cesty.

$\Longleftarrow$ Nechť G neobsahuje hranový $xy-$řez velikosti $< k$. Vyrobíme tokovou síť $(V, \vec{E}, x, y, c)$, kde $\forall e \in \vec{E} : c(e) = 1$ a $\vec{E} = \{uv, ve \mid \{u, v\} \in E\}$.

Všimneme si, že v té síti není žádný řez velikosti $< k$. Tedy v té siti existuje tok velikosti $\geq k$.

Nechť f je celočíselný maximální tok a navíc předpokládejme, že mezi všemi celočíselnými maximálními toky zvolíme f tak, aby množina $s(f) = \{e \in \vec{E} \mid f(e) = 1\}$ byla co nejmenší.

Obr. 10: *Důkaz - pár obrázků pro pochopení*



Dále si všimneme, že $s(f)$ neobsahuje žádný orientovaný cyklus. *Jinak spor s minimalitou s(f).*

Pomocí $s(f)$ vyrobím k hranově disjunktních cest z x do y:

`opakuj` k`-krát:`

1. `zacni v` x
2. `jdi po hranach z` $s(f)$`, dokud nedojdes do` y
3. `pouzite hrany odstran z` $s(f)$

□

Věta 10. *(Menger - globální hranová verze):* Graf G je hranově $k-$souvislý $\iff$ mezi každými dvěma různými vrcholy existuje k hranově disjunktních cest.

Důkaz: G je hranově k-souvislý $\iff$ neexistuje hranový řez $< k$ $\iff$ $\forall x, y$ různé vrcholy neexistuje hranový $xy-$řez velikosti $< k$ $\iff$ $\forall xy$ různé: $\exists k$ hranově disjunktních cest z x do y. □

Věta 11. *(Menger - xy-verze pro vrcholovou souvislost):* Nechť $G = (V, E)$ je graf, nechť x, y jsou různé nesousední vrcholy a nechť $k \in \mathbb{N}$. Potom G obsahuje k navzájem VVD cest z x do y $\iff$ G neobsahuje vrcholový xy-řez velikosti $< k$.

Důkaz: Dokazujeme dvě implikace:

$\Longrightarrow$ Hodně disjunktních cest znamená, že tam nemůže být malý řez. Zřejmé.

$\Longleftarrow$ Nechť G nemá vrcholový xy-řez velikosti $< k$. Vyrobíme síť S:

1. za každý vrchol $u \in V$ dáme do S dva vrcholy u^+, u^- a hranu u^+u^- s kapacitou 1.
2. za každou hranu $\{u, v\} \in E$ dáme do S dvě orientované hrany u^-v^+ a v^+u^- s kapacitami "∞".
3. zdroj: x^-, stok y^+

Tvrdíme, že S nemá řez kapacity $c < k$. *Sporem, nechť takový řez existuje, potom všechny jeho hrany jsou tvatu u^+u^- pro nějaké $u \in V$ a odpovídající vrcholy v G tvoří vrcholový xy-řez velikosti $c < k$, což je spor.*

Minimaxová věta o toku a žezu. V S existuje tok velikosti $\geq k$, BÚNO tok je celočíselný, říkejme mu f.

Z existence takového toku f plyne, že obsahuje k hranově disjunktních cest z x^- do y^+ (viz. hranová verze). Označme je $\vec{P}_1, \ldots, \vec{P}_k$.

Tedy cesty $\vec{P}_1, \ldots, \vec{P}_k$ jsou i vnitřně vrcholově disjunktní, protože každá cesta (orientovaná) z x^- do y^+ v S, která obsajuje vrchol u^+ nebo u^- pro nějaké $u \in V \setminus \{x, y\}$, musí obsahovat hranu u^+u^-.

Když v cestách $\vec{P}_1, \ldots, \vec{P}_k$ nahradíme každou hranu tvaru u^+u^- jedním vrcholem u, tak dostaneme k VVD cest z x do y v G.

□

Věta 12. *(Menger - vrcholová globální verze):* G je vrcholově k-souvislý $\iff$ mezi každými dvěma vrcholy x, y existuje k navzájem VVD cest.

Důkaz: Nechť $G = K_n$, $H_v(K_n) = n - 1$, t.j. K_n je vrcholově k-souvislý $\iff$ $k \leq n - 1$. Nechť G není úplný:

$\Longrightarrow$ Mezi každými dvšma vrcholy je k VVD cest $\Longrightarrow$ G má $\geq k + 1$ vrcholů, žádný řez velikosti $< k$ $\Longrightarrow$ G je k-souvislý.

$\Longleftarrow$ Nechť x, y jsou různé vrcholy, máme případy:

(a) $\{x, y\} \neq E$. xy-verze M.v věty: $\exists k$ VVD cest z x do y.

(b) $\{x, y\} \in E$. Nechť $G^- := (V, E \setminus \{e\})$. Lemma $K_v(G^-) \geq k - 1$, xy-verze M. věty pro G^-: v $G^-\exists k - 1$ VVD cest z x do y. Přidám k nim hranu e a mám k VVD cest z x do y v G.

□

Věta 13. *(O uších):* Graf G je 2-souvislý $\iff$ G se dá vyrobit z kružnice pomocí přidáváním uší.

Důkaz: Dokazujeme dvě implikace:

$\Longleftarrow$ Každá kružnice je 2-vrcholově souvislá a přidáním hran se to nepokazí.

$\Longrightarrow$ Máme 2-souvislý graf $G = (V, E)$, C je libovolná kružnice (ta tam musí být, jinak by nebyla 2-souvislá) Zvolme graf $G_{\max} = (V_{\max}, E_{\max})$, t.ž. je největším podgrafem grafu G, který se dá vyrobit pomocí přidávání uší. Tvrdíme $G_{\max} = G$. Kdyby tomu tak nebylo, tak:

1. $V_{\max} = V, E_{\max} \subsetneq E$: přidání hrany znamená přidání ucha, což je spor s maximalitou
2. $V_{\max} \subseteq V$: G je souvislý. Dále $\exists e = \{x, y\}$, t.ž. $x \in V_{\max}$, $y \notin V_{\max}$, $G - x$ je souvislý Dostáváme z toho, že y se dá napojit i jinou cestou než přes x, takže jde připojit ucho.

□

2.5 Cayleyho vzorec

$S_n \equiv$ počet stromů na množině vrcholů $[n] = \{1, 2, \ldots, n\} \implies n^{n-2}$

Definice 36. *(Kořenový strom):* je strom, ve kterém se jeden vrchol určil jako kořen a všechny hrany se zorientovaly směrem ke kořeni. *V grafu bude každá hrana ukazovat směrem ke kořeni*

Definice 37. *(Povykos - "Postup vytváření kořenového stromu"):* je posloupnost $n-1$ orientovaných hran $(e_1, e_2, \ldots, e_{n-1})$ na vrcholech $[n]$, t.ž.: $([n], \{e_1, \ldots, e_{n-1}\})$ je kořenový strom.

Pozorování 2. *Posloupnost orientovaných hran $(e_1, e_2, \ldots, e_{n-1})$ je povykos $\iff$ pro každé $k = \{1, \ldots, n-1\}$:*

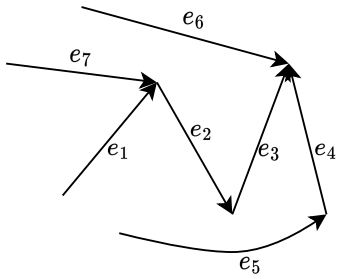
(1) hrana e_k spojuje vrcholy z různých komponent grafu tvořeného předchozími hranami $e_1, \ldots, e_{k-1}$

(2) hrana e_k vyhází z vrcholu, z něhož nevychází žádná z hran $e_1, \ldots, e_{k-1}$.

Věta 14. *(Ceyleyho vzorec, Borchardt 1860): $S_n = n^{n-2}$.*

Důkaz: Nechť K_n je počet kořenových stromů na n vrcholech a P_n je počet povykosů. Všimneme si, že $K_n = n \cdot S_n$ a že $P_n = (n-1)! \cdot K_n$ (je započítán počet všech permutací hran, které strom vytvoří).
Využijeme *Pozorování 2.* Začneme s množinou vrcholů a budeme postupně přidávat hrany až skončíme s kořenovým stromem.

Obr. 11: *Přidávání hran, tvorba kořenového stromu*



Chceme vyrobit povykos $(e_1, \ldots, e_{n-1})$ a máme $n \cdot (n-1)$ možností, jak zvolit e_1 *(druhá podmínka bude splněna automaticky, první podmínka říká, že by měla hrana spojovat dva vrcholy, takže n možností pro výběr, kde bude hrana začínat a $n-1$, kde bude končit)*
Pokračujeme, máme $n \cdot (n-2)$, kde $(n-2)$ je počet možností, jak vyrobit komponentu kde e_2 začíná (dle *(2)* musí e_2 začínat v kořeni komponenty).
Pokud už jsme vybrali $e_1, \ldots, e_{k-1}$ v souladu s *(1)* a *(2)*, tak máme $n \cdot (n-k)$ možnosí, jak vybrat hranu e_k.
Máme tedy celkem:

$$P_n = n(n-1) \cdot n(n-2) \cdot n(n-3) \cdot \ldots \cdot n \cdot 1 = \prod_{k=1}^{n-1} n(n-k) = n^{n-1}(n-1)!$$

$$K_n = \frac{P_n}{(n-1)! = n^{n-1}}$$

$$S_n = \frac{K_n}{n} = n^{n-2}.$$

□

2.6 Počítání dvěma způsoby

Definice 38. *(Antiřetězec):* v $\mathcal{P}([n])$ je množina $a \subseteq \mathcal{P}([n])$, t.ž.: $\forall M, M' \in a$, kde $M \neq M'$ neplatí $M \subseteq M'$, ani $M' \subseteq M$.

Příklad: $n = 4$ *je antiřetězec v* $\mathcal{P}([4])$*:* $\{\{1\},\{2\},\{3\},\{4\}\}, \{\emptyset\}, \emptyset, \{\{1,2,3\},\{3,4\}\}, \{X \subseteq [4], |X| = 2\}$

Definice 39. *(Nasycený řetězec):* v $\mathcal{P}([n])$ je posloupnost $M_0, M_1, \ldots, M_n \subseteq [n]$, kde $M_0 \subseteq M_1 \subseteq \ldots, \subseteq M_n \subseteq [n]$ a $|M_i| = i$.

Příklad: $n = 4$*:* $\emptyset \subseteq \{2\} \subseteq \{1,2,4\} \subseteq \{1,2,3,4\} = [4]$ *a* $|M_i| = i$

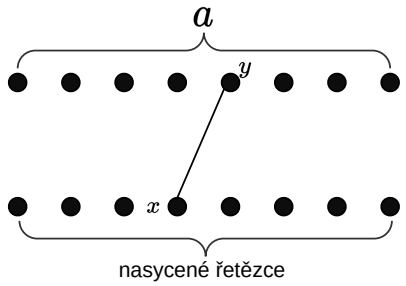
Věta 15. *(Spernerova - 1928):* Největší antiřetězec v $\mathcal{P}([n])$ má velikost $\binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil}$.

Důkaz: Musím dokázat, (i) že existuje a (ii) že neexistuje větší.

(i) Antiřetězec velikosti $\binom{n}{\lfloor n/2 \rfloor}$ je např. $\binom{[n]}{\lfloor n/2 \rfloor}$. Víme tak, že existuje.

(ii) Nechť a je antiřetězec, označme množiny, které do něj patří $a = \{A_1, A_2, \ldots, A_k\}$, kde $k = |a|$. Chceme ukázat, že $k \leq \binom{n}{\lfloor n/2 \rfloor}$.

Obr. 12: *(ii) vytvoříme bipartitní graf*



Máme $n!$ nasycených řetězců v $\mathcal{P}([n])$. Každý nasycený řetězec obsahuje nejvýš jednu množinu a.

Počítáme dvěma způsoby dvojice (A, R), kde $A \in a$ a R je nasycený řetězec. Zároveň $A \in R$.

(1) dvojic je $\leq n!$

(2) pro $A \in a$ máme $A! \cdot (n - |A|)!$ nasycených řetězců obsahující A. To lze odvodit například z $n = 4$:

$$\underbrace{\emptyset \subseteq \{2\} \subseteq}_{|A|! \text{ možností}} \underbrace{\{2,4\}}_{=A} \underbrace{\subseteq \cdots \subseteq [n]}_{(n-|A|)!}$$

Zjistili jsme tak vše potřebné, tedy:

$$n! \geq \sum_{A \in a} |A|!(n-|A|)! \implies 1 \geq \sum_{A \in a} \frac{|A|!(n-|A|)!}{n!} = \sum_{A \in a} \frac{1}{\binom{n}{|A|}} \geq \sum_{A \in a} \frac{1}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} = |a| \cdot \frac{1}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} \implies \binom{n}{\lfloor n/2 \rfloor} \geq |a|$$

□

Věta 16. Nechť $G = (V, E)$ je graf na n vrcholech, který neobsahuje C_4 jako podgraf. Potom $|E| \leq O(n^{3/2})$.

Důkaz: Nechť $G = (V, E)$ je graf bez C_4, $|V| = n$. Označme H počet dvojic $(x, \{y, z\})$ takových, že $x, y, z \in V$, $y \neq z, x$ je soused y i z.
Počítáme H dvěma způsoby:

- Pro dané $x \in V$ máme přesně $\binom{\deg(x)}{2}$ možností, jak zvolit y a z. Tedy

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

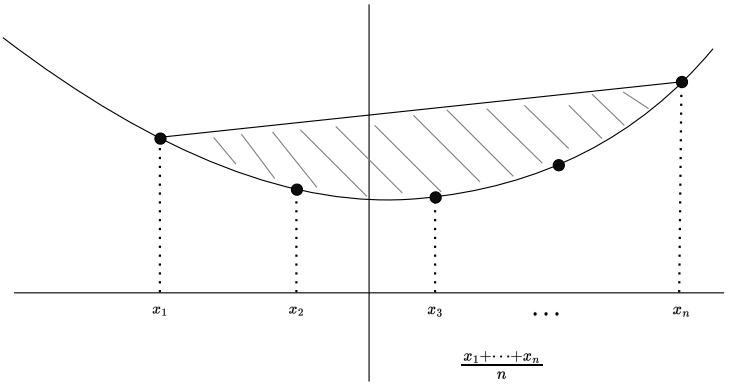
- Pro dané $\{y, z\} \in \binom{V}{2}$ existuje nejvýše jeden společný soused $x \in V$, protože jinak by G obsahoval C_4. Tedy $H \leq \binom{n}{2} \leq \frac{n^2}{2}$

Máme odhadnuto H z obou stran, proto platí:

$$\frac{n^2}{2} \geq \sum_{x \in V} \frac{(\deg(x) - 1)^2}{2}, \text{ tedy } n^2 \geq \sum_{x \in V} (\deg(x) - 1)^2.$$

My chceme $|E| = \frac{1}{2} \sum_{x \in V} \deg(x) \leq O(n^{3/2})$. Uvážme proto konvexní funkci $f(x) = (x - 1)^2$.

Obr. 13: *Konvexní funkce*



Tedy pro každé:

$$x_1, x_2, \ldots, x_n \in \mathbb{R} : f\left(\frac{x_1 + \cdots + x_n}{n}\right) \leq \frac{f(x_1) + \cdots + f(x_n)}{n}$$

$$\left(\frac{2E}{n} - 1\right)^2 \leq \left(\frac{\sum_{x \in V} \deg(x)}{n} - 1\right)^2 \leq \frac{\sum_{x \in V} (\deg(x) - 1)^2}{n} \leq n$$

$$\sqrt{n} \geq \frac{2|E|}{n} - 1 \qquad \text{//počet hran je polovina součtu stupňů}$$

$$n^{3/2} \geq 2|E| - n$$

$$\frac{1}{2}(n^{3/2} + n) \geq |E|$$

□

2.7 Ramseyovy věty

Věta 17. *(Ramseyova, grafová verze, 1930):* $\forall k \in \mathbb{N}, \forall l \in \mathbb{N}, \exists N \in \mathbb{N}$, t.ž.: Pro každý graf $G = (V, E)$ na N vrcholech obsahuje kliku velikosti k nebo nezávislou množinu velikosti l.

Důkaz: Indukcí podle $k + l$.
Můžeme si všimnout, že pro $R(k, 1) = 1 = R(1, l)$, pro $R(k, 2) = k = R(2, l)$
Mějme $k \geq 3, l \geq 3$ a definujme si $N := \overbrace{R(k, l-1) + R(k-1, l)}^{\text{existuje dle IP}}$. Nechť máme dán graf G na N vrcholech. Nechť x je libovolný vrchol G a označme S množinu sousedů vrcholu x a $T = V \setminus (S \cup \{x\})$.
Protože $|S| + |T| = N - 1 = R(k, l-1) + R(k-1, l) - 1$, tak platí $|S| \geq R(k-1, l)$, nebo $|T| \geq R(k, l-1)$.

Předpokládejme, že $|S| \geq R(k-1, l)$ a označme G_s podgraf G indukovaný S. Tedy G_s obsahuje kliku velikosti $k-1$ nebo nezávislou množinu velikosti l.
Pokud G_s obsajuje nezávislou množinu velikosti l, tak i G ji obsahuje, v takovém případě máme hotovo.
Pokud G_s obsajuje kliku velikosti $k-1$, tak klika spolu s x tvoří kliku velikosti k v G a máme tak také hotovo.
Případ $|T| \geq R(k, l-1)$ analogicky. □

Věta 18. *(Ramseyova, Vícebarevná verze):* $\forall b \in \mathbb{N}, \forall m \in \mathbb{N}, \exists N \in \mathbb{N}$, pro každé obarvení hran K_N pomocí b barev existuje množina m vrcholů, t.ž. všechny hrany mezi nimi mají stejnou barvu (resp. klika velikosti m).

Důkaz: Indukcí podle b.

- $b = 1 : R_1^*(m) = m$
- $b = 2 : R_2^*(m) = R(m, m)$
- $b > 2$: Nechť $N = R(m, R_{b-1}^*(m))$. Mějme obarvení K_N pomocí b barev, nechť ty barvy jsou (1) modráa (2)$b-1$ odstínů červené.

  R.V. pro 2 barvy: v tom obarvení buď existuje modrá klika velikosti m, v takovém případš máme hotovo. Nebo existuje klika X velikosti R_{b-1}^*, t.ž. všechny barvy hran mezi vrcholy X jsou odstíny červené.

  X indukuje úplný graf na R_{b-1}^*, jehož hrany jsou obarveny pomocí $b-1$ barev, tedy v něm je jednobarevná klika velikosti m.

□

Notace:

- pro množinu X: $\binom{X}{p}$ je množina p-prvkových podmnožin X
- $K_N^{(p)}$ je p-uniformní úplný hypergraf, což je hypergraf $([N], \binom{[N]}{p})$, $K_\infty^{(p)}$ je nekonečný hypergraf $(\mathbb{N}, \binom{\mathbb{N}}{p})$
- pro $b \in \mathbb{N}$: b-obarvení $K_N^{(p)}$ je funkce $\binom{[N]}{p} \to [b]$
- pro dané obarvení β hypergrafu $K_N^{(p)}$ řekneme, že množina $X \subseteq [N]$ je *jednobarevná* (v obarvení β), pokud β přiřazuje všem množinám $\binom{X}{p}$ tu samou barvu.

Věta 19. *(Ramsey, konečná verze):* $\forall p \in \mathbb{N}, \forall b \in \mathbb{N}, \forall m \in \mathbb{N}, \exists N \in \mathbb{N}, \forall b$-obarvení $K_N^{(p)}, \exists$ jednobarevná m-prvková podmnožina $[N]$.

Věta 20. *(Ramsey, nekonečná verze):* $\forall p \in \mathbb{N}, \forall b \in \mathbb{N}, \forall b$-obarvení $K_\infty^{(p)}, \exists$ nekonečná jednobarevná m-prvková podmnožina $\mathbb{N}$.

Lemma 1. *(Königovo):* Nechť T je strom s nekonečně mnoha vrcholy, který neobsahuje žádný vrchol nekonečného stupně, nechť X_0 je libovolný vrchol T. Potom T obsahuje cestu začínající v X_0.

Důkaz: Zakořeňme T ve vrcholu X_0. Indukcí definujme posloupnost vrcholů $X_0, X_1, \ldots$ tak, že tvoří cestu pro $\forall i \in \mathbb{N}_0$. Podstrom zakořeněný v X_i má nekonečně mnoho vrcholů.
Už máme X_0. Nechť už máme $X_0, X_1, \ldots, X_n$, nechť $y_1, y_2, \ldots, y_k$ jsou děti X_n.
Alespoň jeden vrchol $y \in \{y_1, \ldots, y_k\}$ je kořenem nekonečného podstromu, tedy definujeme $X_{n+1} := y$.
Posloupnost $X_0, X_1, X_2, \ldots$ tvoří nekonečnou cestu v T. □

2.8 Samoopravné kódy

Tvrzení 3. Pokud G je generující matice $(n,k,d)-$kódu C, tak zobrazení, které vektoru $x = (x_1, \ldots, x_k) \in \mathbb{Z}_2^k$ přiřadí vektor xG, je kódování pro C.

Důkaz: Uvažujme zobrazení $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ definované $f(x) = xG$. Stačí ověřit

(1) $\forall x \in \mathbb{Z}_2^k : f(x) \in C$

(2) f je prosté.

Nejprve ověříme (1). Nechť $r_1, \ldots, r_k$ jsou řádky G, tedy $r_1, \ldots, r_k \in C$. Potom pro každé $x \in (x_1, \ldots, x_k)$ platí $xG = x_1 r_1 \oplus x_2 r_2 \oplus \cdots \oplus x_k r_k$, což je lineární kombinace prvků C, tedy prvek C.
Nyní ověříme (2). Kdyby nebylo prosté $\exists x \neq x' \in \mathbb{Z}_2^k : f(x) = f(x')$, tak $xG = x'G \iff (\underbrace{x - x'}_{\neq 0})G = \mathbf{0}$, což nemůže nastat, protože řádky G jsou lineárně nezávislé. □

Tvrzení 4. Nechť C je lineární (n,k,d)-kód s kontrolní maticí K. Potom $\forall x \in \mathbb{Z}_2^n : x \in C \iff Kx^T = \mathbf{0}$.

Důkaz: Nechť $r_1, \ldots, r_{n-k} \in \mathbb{Z}_2^n$ jsou řádky K. Potom:

$$\begin{aligned} x \in C &\iff x \in (C^\perp)^\perp \iff y \in C^\perp \iff \langle x, y \rangle = 0 \iff \\ &\iff \forall i = 1, \ldots, n-k : \langle x, r \rangle = 0 \iff \\ &\iff Kx^T = \mathbf{0}. \end{aligned}$$

□

Pozorování 3. *$\Delta(C)$ je nejmenší $t \geq 1$ takové, že v K lze najít t sloupců, jejichž součet je $\mathbf{0} \in \mathbb{Z}_2^{n-k}$.*

Důsledek 3. $\Delta(C) \geq 2 \iff K$ má všechny sloupce $\neq 0$. $\Delta(C) \geq 3 \iff K$ má navíc každé dva sloupce různé.

Tvrzení 5. $\forall r \geq 2$, pro $n = 2^r - 1$, $\forall x \in \mathbb{Z}_2^n$; $\exists! y \in H_r$ takové, že $d(x,y) \leq 1$. Navíc lze y nalézt algoritmem:

1. Spočítej $s := K_r x^T$
2. `if` $s = \mathbf{0}$: $x \in H_r \implies y := x$.
3. `if` $s \neq \mathbf{0}$: Nechť $i = \{1, \ldots, n\}$ je takové, že i-tý sloupec K_r je roven s. Potom nechť y je vektor, který vznikne z x změnou i-tého bitu.

Notace:

- *"Koule"* $B(x,t) := \{d(x,y) \leq t \mid y \in \mathbb{Z}_2^n\}$*, neboli okolí poloměru t kolem x v $\mathbb{Z}_2^n$.*
- *"Objem"* $V(t) := |B(x,t)| = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{t}$.

Tvrzení 6. *(Singletonův odhad):* Pokud existuje (n,k,d)-kód C, tak $k + d \leq n + 1$.

Důkaz: Nechť C je (n,k,d)-kód. Definujeme zobrazení $\Psi : \mathbb{Z}_2^n \to \mathbb{Z}_2^{n-d+1}$ tak, že $\Psi(x_1, \ldots, x_n) = (x_1, \ldots, x_{n-d+1})$.
Pro $x, y \in C$, kde $x \neq y \implies \Psi(x) \neq \Psi(y)$. Tedy $|C| \leq 2^{n-d+1}$ a proto $k \leq n - d + 1$. □

Tvrzení 7. *(Hammingův odhad):* Pokud existuje (n,k,d)-kód C, tak $|C| \leq \dfrac{2^n}{V(\lfloor \frac{d-1}{2} \rfloor)}$

Důkaz: Plyne z toho, že $x, y \in C$, kde $x \neq y$: $B(x, \lfloor \frac{d-1}{2} \rfloor) \cap B(y, \lfloor \frac{d-1}{2} \rfloor) \neq \emptyset$. □

Tvrzení 8. *(Gilbert-Varshamovův odhad):* $\forall n, d$, kde $n < d$, existuje kód C, t.ž. $|C| \geq \dfrac{2^n}{V(d-1)}$

Důkaz: Vždy vezmeme vektor, dáme ho do C a hladově hledáme vektory, dokud tam nějaké zbydou.
V každém kroku nejvýše $\frac{2^n}{V(d-1)}$ vektorů eliminujeme: 1 vybereme, ostatní jsou zakázané. Z toho plyne vzorec. □