

# Aplikace lineární algebry v kombinatorice

prof. RNDr. Jan Kratochvíl, CSc.

8. února 2021



## Obsah

1	Maticovy popis grafu, det, kostry	2
2	Sudo-lichomesta, 2-vzdalenost mnozin bodu	3
3	Sudo-sudomesta, Prostor cyklu grafu	6
4	Seiduv switching	8
5	Spektrum grafu, Moorovy grafy	12
6	Silne regularni grafy, propletani vl cisel	13
7	Odhady pomoci spektra	17
8	Shannonova kapacita	22
9	Samoopravne a perfektni kody, Lloydova veta	25

# 1 Maticovy popis grafu, det, kostry

**Definice 1.1.** Matice sousednosti grafu  $G$

**Věta 1.2 (Pocet sledu).** Pro každý graf  $G$  a každé přirozené číslo  $k$  obsahuje  $k$ -ta mocnina matice sousednosti  $A$  počty sledu delky  $k$  mezi vrcholy grafu  $G$ , konkrétně  $(A^k)_{a,b} = \#$  sledu delky  $k$  mezi  $a - b$  v  $G$ .

*Důkaz.* Indukci podle  $k$ .

1.  $k = 0$ , sledy delky 0, neboli  $u - u$ . Což odpovídá dle definice  $A^0 = I$ .
2.  $k = 1$ . Sled je právě hrana.
3. indukční krok:

$$(A^{k+1})_{a,b} = (A^k * A)_{a,b} = \sum_{w \in V} (A^k)_{a,w} * A_{w,b} =$$

na pozici  $(w, b)$  je 1 pokud existuje taková hrana, jinak 0. Proto

$$= \sum_{w, bw \in E} (A^k)_{a,w} =$$

Dle I.P. se rovná počtu sledu delky  $k$  mezi  $a - w$ . Pak mezi vrcholy  $a - w$  existuje sled delky  $k$ . Rozdělíme sledy dle konečného vrcholu, který je soused  $b$ . Každý z těchto sledu jednoznačně prodloužíme na sled delky  $(k+1)$  do vrcholu  $b$ . Z toho předchozí součet je právě # počet sledu delky  $(k+1)$  mezi  $a - b$ .

□

**Definice 1.3.**  $L_G^{(n)}$  se dostane tak, že vyskrtneme  $n$ -ty řádek a sloupec z Laplaceovy matice.

**Lemma 1.4.**

$$\forall w \subseteq E, |w| = n - 1 : \det((D_G^{(u)})_w) = \begin{cases} 0 & \text{pro } (V, w) \neq \text{tree} \\ \pm 1 & \text{pro } (V, w) = \text{tree} \end{cases}$$

*Důkaz.* 1) Necht  $w \subseteq E$  je kostra. Pak je stromem  $\Rightarrow$  má list  $v_1$ . Premístíme řádek odpovídající  $v_1$  do prvního řádku. Necht  $e_1$  je hrana  $v_1 - v_t$ . Dame ji do prvního sloupce. Pak na pozici  $(0,0)$  je  $\pm 1$ . Taký první řádek je  $(\pm 1, 0, \dots, 0)$  protože vrchol je list. Odtráhneme  $v_1$ , necht  $v_2$  je další list a  $e_2$  jeho hrana. Pak druhý řádek je  $(0, \pm 1, 0, \dots, 0)$ . Tak pokračujeme dál.

Můžeme se ale stát, že další vrchol je  $u$  který jsme zrovna odstranili. Použijeme tvrzení, že strom má aspoň 2 listy. Pak můžeme vzít nějaký další vrchol. Po ukončení přemísťování dostaneme  $\pm 1$  na diagonale. Nad diagonalou samé 0  $\Rightarrow \det = \pm 1$ . Přemístěním jsme menili znaménko  $\det$ . Ale  $\det^2 = 1$ .

2) Máme graf  $w \subseteq E, |w| = |V| - 1$  který není strom  $\Rightarrow$  není souvislý  $\Rightarrow$  má aspoň 2 komponenty souvislosti.  $V = V_1 \dot{\cup} V_2$ . BUNO  $u \in V_2$ . Pak z  $V_1$  do  $V_2$  nevede žádná hrana, část matice je 0. Pak součet řádku odpovídající  $V_1, E(V_2)$  a  $V_2, E(V_1)$  je 0  $\Rightarrow$  řádky jsou LZ a  $\det$  je 0.

□

**Věta 1.5 (Pocet koster).**  $\det(L_G^{(n)}) = \# \text{ koster grafu } G$

*Důkaz.* Vezmeme matice incidence  $I_G$  (jenom 2 jedničky ve sloupci, v radku # 1 je  $\deg(v)$ ), v každém jejím sloupci nahradíme jednu jedničku hodnotou  $(-1)$ . Vyslednou matici označme  $D_G$ .

$I_G * I_G^T = \text{skal. součin radku } i, j$ . Na diagonale  $\deg(v)$ , mimo diag. 1 pro hrany, 0 - nehrany. Zmeníme prave jednu 1ku ve každém sloupci na  $-1$  (tim dostaneme orient. graf).

$$D_G * D_G^T = L_G$$

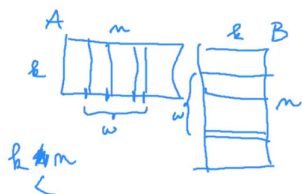
Rovnost platí protože skalární součin stejného radku da  $\deg(v)$  jelikož  $-1 * -1 = 1$ . Pokud násobíme různé řádky, příslušné vrcholy nejsou spojeny hranou - 0. Jinak mají právě 1 společnou pozici a dostaneme  $-1 * 1 = -1$ .

Pak  $\det(L_G^{(u)})$  spočítáme jako  $\det(D_G^{(u)} * (D_G^{(u)})^T)$

Použijeme Cauchy-Binetovu formulu (det součinu obdelnikových matic)

$$\det(A * B) = \sum_{\substack{w \subseteq \{1, 2, \dots, n\} \\ |w|=k}} \det A_w * \det B^w$$

Kde  $A_w$  jsou n sloupců matice A,  $B^w$  - n řádků matice B.



$$\det L_G^{(u)} = \sum_{\substack{w \subseteq E \\ |w|=n-1}} \det(D_G^{(u)}) * \det(D_G^{(u)})^T =$$

Pro každou matici  $\det A = \det A^T$ , pak

$$= \sum_{\substack{w \subseteq E \\ |w|=n-1}} \det(D_G^{(u)})^2$$

Kostra musí mít  $(n-1)$  vrcholů; v det se díváme na všechny podmnožiny hran  $|w| = n-1$ . Ptáme se jestli je strom. Proto suma nahoře je právě

$$\sum_{\substack{w \\ (V,w) \text{ je kostra}}} 1$$

Což je # koster G

□

## 2 Sudo-lichomesta, 2-vzdálenost množin bodů

**Lemma 2.1.**  $\det(S_1 + b_1, S_2 + b_2, \dots, S_k + b_k) = \det(S + B)$ ,  $S_i, b_i \in T^k$  kde  $S_i, b_i$  jsou sloupce matic  $S, B$ , jde spočítat jako:

$$\det(S_1 + b_1, S_2 + b_2, \dots, S_k + b_k) = \det(S_1, S_2 + b_2, \dots, S_k + b_k) + \det(b_1, S_2 + b_2, \dots, S_k + b_k)$$

Pak linearita v 2. sloupci atd.

$$\det(S+B) = \sum_{w \subseteq [k]} \det(S^w T)$$

kde  $S^w$  znamená, že jsme vzali sloupce odpovídající indexům v  $w$ . Ostatní sloupce jsou z  $T$ .

**Věta 2.2 (skoro disjunktní systémy množin).** Necht  $A_1, \dots, A_k$  jsou různé  $\subseteq [n]$ ,  $|A_i \cap A_j| = 1, i \neq j \Rightarrow k \leq n$

*Důkaz.* Necht  $A$ -matice incidence  $\{A_i\}$ . Řádek odpovídá prvkům, sloupec - množinám. Na pozici  $(r, s) = 1 \Rightarrow$  prvek  $r$  leží v množině  $A_s$ .

Vezmeme  $A^T * A$  nad  $\mathbb{R}$ . Pak ve výsledné matici na pozici  $(r, s)$  je  $|A_r \cap A_s|$ . Jelikož průniky jsou 1-prvkové, máme matici 1-ček. Na diagonále jsou  $|A_i|$  velikosti množin.

$$k = \text{rank}(A^T A) \leq \text{rank} A \leq n \Rightarrow k \leq n$$

Tvrdíme, že  $\det(A^T A) \neq 0$ . Pak matice je regulární a  $\text{rank} = k$ .

BUNO

$$|A_i| = a_i, a_1 \leq a_2 \leq \dots \leq a_k$$

Máme matici, kde na diagonále jsou velikosti množin, jinak 1.

Náhledněme  $a_2 \geq 2$ . Jinak pokud  $a_1 = a_2 \Rightarrow \exists x \in A_1 \cap A_2 \Rightarrow A_1 = A_2 = \{x\}$ .

Necht  $J$  je matice jedniček. Matici  $A$  můžeme napsat jako  $J + I * (a_i - 1)$  kde  $(a_i - 1)$  je na diagonále. Použijeme vlastnost  $\det$  jako multilineární formy, viz lemma 2.1. Pokud vezmeme 2 sloupce z  $J$ , tak  $\det$  bude 0. Takže zbyvají  $\det$  kde je jeden sloupec z  $S$ , zbytek z  $J$ .

$$\det(S+J) = \det(S) + \sum_i^k J^i S =$$

Determinanty matic  $J^i S$  kde z  $J$  je pouze  $i$ -tý sloupec lze spočítat rozvojem dle  $i$ -ho řádku kde je pouze 1 jednička.

$$= \prod_1^k (a_i - 1) + \prod_2^k (a_i - 1) + \sum_{j=2}^k \frac{\prod_1^k (a_i - 1)}{a_j - 2}$$

Kde 2. produkt máme protože  $a_1$  se může rovnat 1, zbytek jsou větší. První  $\prod$  je  $\geq 0$ , druhý  $\prod > 0$  protože od  $i = 2, a_i \geq 2$ .  $\sum$  je zlomek kladných členů, takže  $\sum \geq 0$ . Dohromady  $\det(J+S) > 0$

□

**Věta 2.3 (súdo-lichomesta).** Necht  $A_1, \dots, A_k$  jsou různé  $\subseteq [n]$ ,  $|A_i| \equiv 1 \pmod{2} \forall i, |A_i \cap A_j| \equiv 0 \pmod{2}, i \neq j \Rightarrow k \leq n$

*Důkaz.* Vezmeme matice incidence jako v předchozí větě. Uvažme matici  $A^T * A$  nad  $\mathbb{Z}_2$ . Pak na diagonále jsou mohutnosti množin  $\equiv 1 \pmod{2}$ , mimo diagonálu průniky  $\equiv 0 \pmod{2}$ . Neboli  $A^T * A = I \Rightarrow \text{rank} = k$ . Pak jako minule:

$$k = \text{rank}(A^T A) \leq \text{rank} A \leq n \Rightarrow k \leq n$$

□

**Definice 2.4.** Mnozina bodu v  $\mathbb{R}^n$  je s-vzdalenostni pokud vzajemne vzdalenostni bodu nabyvaji celkem nejvyse s hodnot.

**Pozorování 2.5.** 1-vzdalenostni množiny jsou simplex. Zobecnění rovnostranného  $\triangle$  do vyšších dimenzí. Indukci dokážeme, že  $m_1(n) = n + 1$ . Při přechodu do vyšší dimenze existuje práce jeden bod který můžeme použít. Proces podobný kompaktizace topologického prostoru.

**Věta 2.6 (2-vzdalenostní množ).** Necht  $m_s(n)$  znací počet bodu s-vzdalenostní množ v  $\mathbb{R}^n$ , pak:

$$\binom{n+1}{2} \leq m_2(n) \leq 1/2 * (n+1)(n+4)$$

*Důkaz.* 1) Dolní odhad

Vezmeme vektory, které mají právě 2 jedničky, jinak 0. Takových máme  $\binom{n}{2}$ .

Pokud 2 vektoru mají 1 společnou pozici,  $d(x, y) = \sqrt{2}$ . Jinak pokud mají 2 společné pozice, tak  $d(x, y) = 2$ . Vzdálenost počítáme jako kanonickou Euklidovou normu.

$$m_2(n) \geq \binom{n}{2}$$

Zesílíme dolní odhad: přemístíme se do  $\mathbb{R}^{n+1}$ . Jelikož  $\sum_i^{n+1} x_i = 2$ , body jsou v nadrovine dimenzi  $\mathbb{R}^n$  kterou lze vzorit do  $\mathbb{R}^n$ . Pak:

$$m_2(n) \geq \binom{n+1}{2}$$

2) Horní odhad

Máme body  $A_1, A_2, \dots, A_t$ .  $A_i = (a_{i,1}, a_{i,2}, \dots, a_{i,n}) \in \mathbb{R}^n$ . Označme vzdálenosti  $k \neq m \in \mathbb{R}$ . Definujme funkce  $F: \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$ ,  $F(x, y) = (d(x, y)^2 - m^2) * (d(x, y)^2 - k^2)$ . Pokud je vzdálenost  $m \vee k \Rightarrow F = 0$ .

Pak  $f_i(x), f_i(x) = F(x, A_i)$ . Částečně dosazení. Tyto funkce jsou v V.P. funkci z  $\mathbb{R}^n$ . Tvrdíme že  $\{f_i(x)\}$  jsou LN. Pokud dosadíme 2 různé prvky do  $f_i$  tak dostaneme 0 dle definice zobrazení F. Pro stejný bod  $f_i = a^2 b^2 \neq 0$ .

$$\sum_1^t f_i * x_i = 0, x_i \in \mathbb{R}, 0 = \text{nulová funkce}$$

Podíváme se na tuto funkce (lin kombinace funkci) v nějakém bode  $A_j$ .

$$\forall j (\sum_1^t f_i * x_i)(A_j) = \sum_1^t f_i * x_i(A_j) = x_j a^2 b^2 = 0 \Rightarrow x_j = 0$$

Neboli funkce jsou LN. Jejich počet je omezen podprostorem funkci nad  $\mathbb{R}^n$  ve kterém žijou.

$$f_i(x) = (d(x, A_i)^2 - m^2) * (d(x, A_i)^2 - k^2) = ((\sum_j^t (x_j - a_{i,j})^2 - a^2) * ((\sum_j^t (x_j - a_{i,j})^2 - b^2))$$

$f_i$  jsou polynomu stupně 4. # polynomu dle dimenze:

1.  $k = 0$  konstantni  $= 1$ .
2.  $k = 1$  je  $n$ .
3.  $k = 2$  je  $\binom{n}{2}$  pro ruzna  $x_i, x_j$  a  $n$  pro  $x_i^2$ .
4.  $k = 3$   $\binom{n}{3}$  pro ruzna  $x_i, x_j, x_k$ . Pro  $x_i^2 x_j = n(n-1)$  a  $n$  pro  $x_i^2$ .
5.  $k = 4$  podobne

Nase funkce jsou z podprostoru polynomu  $\deg = 4$ . Zvolme vhodnou bazi.

$$U = \langle 1, x_i, x_i * x_j, x_i^2, (\sum x_j^2)x_i, (\sum x_j^2)^2 \rangle \forall i, j$$

Dostaneme  $\dim(U) = 1 + n(\text{lin}) + n(kv) + n(kv * \text{lin}) + \binom{n}{2}(\text{lin}2) + 1 = 2 + 3n + 1/2n(n-1) = 1/2(4 + 5 + n^2)$ . Generator  $\sum x_j^2$  nepotrebujeme protoze je lin kombinaci  $x_j^2$ .  $\square$

### 3 Sudo-sudomesta, Prostor cyklu grafu

**Věta 3.1 (Sudo-sudomesta).** *Necht  $A_1, \dots, A_k$  jsou různé  $\subseteq [n]$ ,  $|A_i| \equiv 0 \pmod{2} \forall i, |A_i \cap A_j| \equiv 0 \pmod{2}, i \neq j \Rightarrow k \leq 2^{\lfloor \frac{n}{2} \rfloor}$*

*Důkaz.* Udelame bijekci množina  $\rightarrow$  charakteristický vektor. Pak lin kombinace je taky sudo-sudomesto. Dal

$$\langle A_i, A_j \rangle = \sum_{x \in X} (A_i)_x (A_j)_x = \sum_{x \in A_i \cap A_j} 1 = |A_i \cap A_j| \pmod{2}$$

$$\langle A_i, A_i \rangle = |A_i|$$

Pak  $\langle A_i, A_j \rangle \equiv 0 \pmod{2}$ . Vezmeme  $m = \sum b_i A_i$ , tak

$$\langle A_i, m \rangle = \langle A_i, \sum b_i A_i \rangle = \sum b_i \langle A_i, A_j \rangle = 0$$

$$\langle m, m \rangle = \langle \sum b_i A_i, m \rangle = \sum b_i \langle A_i, m \rangle = 0$$

Z toho maximalni (vzhledem k inkluzi) system tvorici sudo-sudomesto je nutne podpostor.

$$\forall x \in M \forall y \in M \langle x, y \rangle = 0 \Rightarrow \forall x \in M : x \in M^\perp \Rightarrow M \subseteq M^\perp$$

$$\langle M \rangle \subseteq M^\perp \Rightarrow \dim M \leq \dim M^\perp = n - \dim M \Rightarrow \dim \langle M \rangle \leq \lfloor n/2 \rfloor \Rightarrow \dim M \leq \lfloor n/2 \rfloor$$

Odhad je tesny: spojime body do 2jic tvorici rozklad X. Pak množiny budou vsechny mozne podmnožiny obsahující 2ce. Je jich  $2^{\lfloor n/2 \rfloor}$   $\square$

**Definice 3.2.** Uvazme bijekci mezi napnutým podgrafem H a jeho charakteristickým vektorem. Množina vseh napnutých podgrafu  $\nu_G$  tvorí V.P. nad  $\mathbb{Z}_2$ , scitani vektoru odpovida symmetricke diferenci množiny hran.

**Definice 3.3.** Množina napnutých podgrafu je Eulerovska pokud  $\forall u \in V, \deg(u) \equiv 0 \pmod{2}$ . Znacime  $\xi_G$ . Pak  $\beta_G$  je množina elementarnich rezu, t.j.  $B_A = (V, \{xy : x \in A, y \in V \setminus A, xy \in E\}), A \subseteq V$ .



**Věta 3.4 (Eulerovské grafy).**  $\xi_G, \beta_G$  jsou V.P. podprostory  $\nu_G$ . Platí  $\xi_G^\perp = \beta_G \wedge \beta_G^\perp = \xi_G$ . Pokud navíc je graf souvislý,  $\dim(\beta_G) = |V| - 1 \wedge \dim(\xi_G) = |E| - |V| + 1$ .

*Důkaz.* 1) Nasobení skalarem je automaticky splněno, protože těleso je  $\mathbb{Z}_2$ .

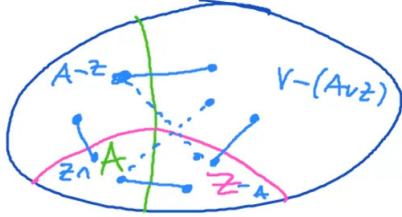
2)  $H_1 + H_2 = (V_1, E(H_1) \div E(H_2))$ . Taký patří do V.P.

3) Ukážeme  $\forall H_1, H_2 \in \xi_G : H_1 + H_2 \in \xi_G$ . Zvolme vrchol  $u$ , nechť  $\deg_{H_1} u = 2k, \deg_{H_2} u = 2l$ , taký  $h$  je počet společných hran obou podgrafů.

$$\deg_{H_1+H_2} u = 2k - h + 2l - h = 2k + 2l - 2h \equiv 0 \pmod{2}$$

Součet 2 Eulerovských grafů je Eulerovský graf.

4) Ukážeme  $\forall A, Z \subseteq V(G) : B_A + B_Z \in \beta_G$ .



Z obrázku prezijou pouze hrany vedoucí z  $A - Z$  do  $V - (Z \cup A)$ , hrany z  $A - Z$  do  $Z \cap A$ , hrany  $(Z \cap A)$  do  $Z - A$  a hrany ze  $Z - A$  do  $V - (Z \cup A)$ . Ostatní byly ve 2 rezích. Zůstane rez  $B_{A \div Z}, A \div Z = (A - Z) \cup (Z - A)$ .

$$B_A + B_Z = B_{A \div Z}$$

Tvrdíme že  $B_G = \langle B_{\{u\}}, u \in V \rangle$ . Prostor el. rezu je generovaný hvězdami. Protože

$$B_A = \sum_{u \in A} B_{\{u\}}$$

Hrany uvnitř  $A$  se smažou sym. diferencí, hrany vedoucí ven z  $A$ , které nejsou společné zůstanou.

5)  $G$  souvislý  $\Rightarrow \dim B_G = |V| - 1$ . Nahledneme ze sectení všech hvězd dává  $\emptyset$  graf. Neboli každá hrana patří ke 2 hvězdám.

Zafixujeme vrchol  $u$ , secteme hvězdy kromě  $u$ .  $\sum_{a \neq u} B_{\{a\}} = \emptyset - B_{\{u\}} = B_{\{u\}} \neq \emptyset$  Pokud vezmeme všechny kromě 1 hvězdy, tak jsou LN a generují všechny rezy. Z toho  $\Rightarrow \dim B_G = |V| - 1$ .

Pozorování:

$$\forall H \subseteq V : H \in \xi_G \iff \langle H, B_A \rangle = 0 \quad \forall B_A \in B_G \iff \langle H, B_{\{u\}} \rangle = 0 \quad \forall u \in V$$

Uvažme hvězdu  $B_{\{u\}}$  a  $\deg_H u = 0 \pmod{2}$ . Pak symmetrická diference smaže prave sudý počet hran z hvězdy a nové počet hran je také sudý.

$$\forall u \in V : \langle H, B_{\{u\}} \rangle = 0 \iff \deg_H u \equiv 0 \pmod{2}$$

$$\text{Pak } \forall H \subseteq V : H \in \xi_G \iff H \in \beta_G \Rightarrow \xi_G^\perp = (\beta_G)^\perp = \beta_G \Rightarrow \dim(\xi_G) = |E| - |V| + 1$$

□

**Lemma 3.5.**  $M \subseteq \mathbb{Z}_2^n : \bar{1} \in \langle M \rangle + M^\perp$ .

*Důkaz.*  $\forall x \in M \cup M^\perp : \langle x, x \rangle = 0$ . Nad  $\mathbb{Z}_2$  ale  $\langle x, x \rangle = \langle x, \bar{1} \rangle$ . Pak

$$x \perp \bar{1} \Rightarrow \bar{1} \in (M \cap M^\perp)^\perp = M^\perp + (M^\perp)^\perp = M^\perp + M$$

□

**Věta 3.6 (Rozklad na 2 Eulerovské podgrafy).**  $\forall G \exists V_1 \cup V_2 = V(G), G[V_i]$  je Eulerovský.

*Důkaz.* 1) Uvažme  $M = \xi_G$  v tvrzení z lemmatu.  $\bar{1} = G$ , ma všechny hrany  $\Rightarrow \bar{1} \in \xi_G + \xi_G^\perp = \xi_G + \beta_G$ .

$$\forall G : \exists A \subseteq V(G), \exists H \in \xi_G : G = H + B_A$$

Tento rozklad je disjunkt, takže máme 2 Eulerovské podgrafy a mezi nimi elementární rez. Pokud rez smažeme, graf je sjednocení dvou Eulerovských podgrafů.  $\square$

## 4 Seiduv switching

**Definice 4.1.** Necht  $V$  je V.P nad  $T$ . Lineární forma je lin. zobrazení  $f : V \rightarrow T$ . Pak lineární formy tvoří V.P. nad  $T$ . Znamy  $V^*$  a je tzv. dualní prostor k  $V$ .

**Definice 4.2.** Necht  $B = \{b_1, b_2, \dots, b_n\}$  je báze  $V$ , pak  $B^* = \{f_1, f_2, \dots, f_n\}$  je dualní báze, pokud formy jsou dány předpisem:

$$f_i(b_j) = \begin{cases} 1 & \text{pro } i = j \\ 0 & \text{pro jinak} \end{cases}$$

**Definice 4.3.** Necht  $A, B$  jsou V.P nad  $T$ ,  $\dim A = n, \dim B = k$ . Necht  $\varphi : A \rightarrow B$  homomorf. Pak dualní homomorf k  $\varphi$  je zobrazení  $\varphi^* : B^* \rightarrow A^*$  dány předpisem:

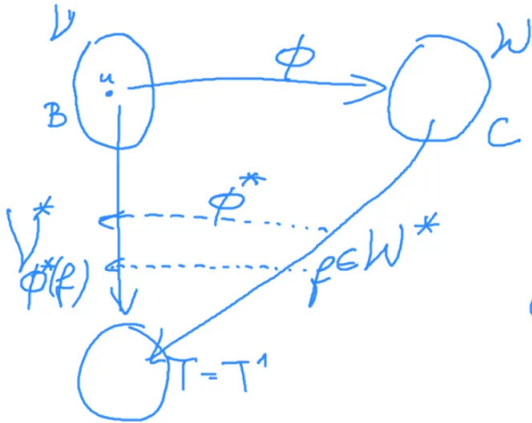
$$\forall f \in B^* \forall u \in A : (\varphi^*(f))(u) = f(\varphi(u))$$

**Věta 4.4 (Matice dualního homomorf(BD)).** Matice dualního homomorf vzhledem k dualním bazím je transponovaná matice k matici primárního homomorf.

$${}_C[\varphi^*]_{B^*} = ({}_B[\varphi]_C)^T$$

*Důkaz.* Matice zobrazení lineární formy z prostoru  $f : V \rightarrow T$  je

$${}_B[f]_k = (f(b_1), f(b_2), \dots, f(b_n))$$



Máme homomorf  $\phi : V \rightarrow W$ , pak lineární formy  $h : W \rightarrow T$ .

Dualni homomorf  $\phi^* : W^* \rightarrow V^*$  je definovan:

$$\phi^*(f)(u) = f(\phi(u))$$

Jelikož lin formy jsou n-tice, tak  $\dim(V) = \dim(V^*)$ .

Matice  $\phi$  je  ${}_B[\phi]_C \in T^{k \times n}$ . Matice  $\phi^*$  je  ${}_{C^*}[\phi^*]_{B^*} \in T^{n \times k}$ .

Veta rika, ze

$${}_{C^*}[\phi^*]_{B^*} = ({}_B[\phi]_C)^T$$

□

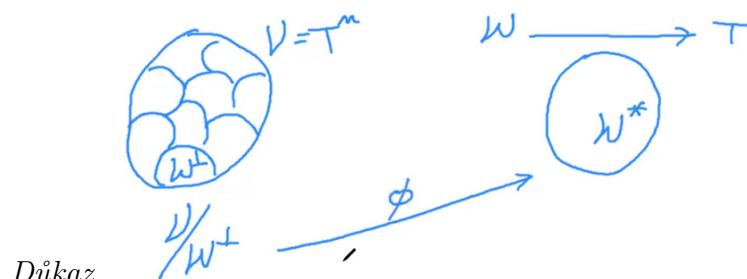
**Definice 4.5.** Faktorprostor: faktorizace dle podprostoru  $W$  prostoru  $V$  (podgrupa).  $V/W$  jsou množiny  $\forall u \in V u + W$ . Pak i faktorprostor je V.P vuci operacim:

$$(u + W) + (a + W) = (u + a)W, \lambda \cdot (u + W) = (\lambda \cdot u) + W$$

Plati:  $\dim(V/W) = \dim V - \dim W$ .

**Věta 4.6 (Izomorfismus faktorprostoru).** Necht  $V = T^n$  a necht  $W$  je podprostor. Pak

$$V/W^\perp \sim W^*$$



Důkaz.

Pak izomorf  $\phi$  je definovan:

$$\phi(v + W^\perp) = \langle v, \cdot \rangle$$

Udelali jsme linearni formu z bilinearni??

Pokud dosadime promennou:

$$\forall x \in W : \phi(v + W^\perp)(x) = \langle v, x \rangle$$

Chceme aby  $\phi$  bylo korektně definované a splnovalo vlastnosti izomorf:

- 1) korektnost definice
- 2) lin zobrazení
- 3) proste
- 4) na

Dukaz:

- 1)  $a \in v + W^\perp \iff a = v + b, b \in W^\perp$ . Pak

$$\langle a, x \rangle = \langle v + b, x \rangle = \langle v, x \rangle + \langle b, x \rangle$$

Protože  $x \in W \Rightarrow \langle b, x \rangle = 0 \Rightarrow \langle v, x \rangle = \langle a, x \rangle$ .

- 2) Skalarni soucin je bilinearni forma, z toho  $\phi$  je linearni zobrazení.

- 3) Necht  $\phi(v + W^\perp) = 0 \Rightarrow \forall x \in W : \langle v, x \rangle = 0 \Rightarrow v \in W^\perp \Rightarrow v + W^\perp = \bar{0} + W^\perp$ . Takze v kernelu je pouze  $W^\perp$ .

4) Nahledneme z dimenzi.

$$\dim(\text{Im}(\phi)) \leq \dim(W^*) \wedge \dim(\text{Im}(\phi)) = \dim(V/W^\perp)$$

Rovnost dimenzi platí protože zobrazení je prosté.

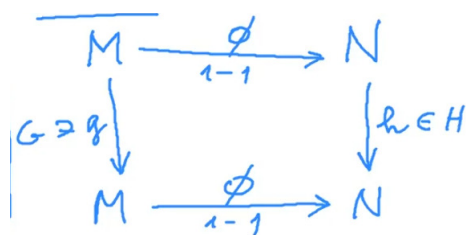
$$\dim(\text{Im}(\phi)) = \dim(V) - \dim(W^\perp) = \dim(V) - (\dim(V) - \dim(W)) = \dim(W) = \dim(W^*)$$

Z LA  $\text{Im}(\phi)$  je vnorený podprostor stejné dimenze jako nadprostor  $\Rightarrow$  jsou stejné.  $\square$

**Věta 4.7 (Burnsidovo lemma(BD)).**

**Lemma 4.8.** *Nechť grupa  $G$  provádí akci na množině  $M$ , grupa  $H$  na  $N$ . Nechť  $\varphi : M \rightarrow N$  bijekce.*

$$\text{if } g \in G, h \in H, \forall m \in M : h\varphi(m) = \varphi(gm) \Rightarrow |G_g| = |H_h|$$



*Důkaz.* Prvky v  $M_g$  jsou  $gm = m$ . Prvky v  $N_h$  jsou  $hn = n$ . Kvůli bijekci  $\varphi$  lze jednoznačně vyjádřit jako:

$$n = \varphi(m) = \varphi(\varphi^{-1}(n))$$

Pak

$$h\varphi(m) = \varphi(m)$$

Diagram komutuje

$$\varphi(gm) = \varphi(m)$$

$\varphi$  je bijekce, takže prosté  $\Rightarrow gm = m$ . Dohromady  $\# hn = n$  je totéž jako  $\# gm = m$ .  $\square$

**Definice 4.9.** Seidelův switching vymění všechny hrany a nehrany vycházející z  $u \in V$ . Ostatní vrcholy a hrany beze změny. Grafy  $G \sim G' \iff G'$  lze získat z  $G$  postupným prepínáním vrholů.

**Poznámka 4.10.**

$$G \sim G' \iff \exists A \subseteq V(G) : G' = S(G, A)$$

kde  $S(G, A)$  je switch celé podmnožiny. Hrany mezi  $A$  a zbytkem se prohodi.

**Poznámka 4.11.** Dva grafy na stejné množině vrcholů jsou Seidelovsky ekv  $\iff$  jsou ve stejné třídě faktorizace  $V_{K_V}/\beta_{K_V}$ . Proto je tříd ekvivalence tolik, kolik je Eulerovských grafů na dané množině vrcholů.

**Věta 4.12 (Počet neizomorfních tříd Seidel switching).** *Počet neizomorfních tříd ekvivalence při Seidelově switchingu na  $n$  vrcholech je roven počtu Eulerovských grafů na  $n$  vrcholech.*

Důkaz. Pro liché  $n$ , označme

$$\{A = \{u | \deg_G(u) \equiv 1 \pmod{2}\}, |A| \equiv 0 \pmod{2}\}$$

Uděláme switch množiny  $A$ :  $(G, A)$ . Vezmeme vrchol  $u \in V \setminus A$  Pak  $\deg_G(u) = a + b$ , kde  $a$  je počet hran mimo  $A$ ,  $b$  je počet hran vedoucích do  $A$ .

Po switchu:

$$\deg_{S(G,A)}(u) = a + |A| - b = \deg_G(u) - 2b - |A| \equiv 0 \pmod{2}$$

Vezmeme vrchol  $u \in A$ ,  $\deg_G(u) = c + d$ , kde  $c$  jsou hrany v  $A$ ,  $d$  hrany mimo  $A$ .

Po switchu:

$$\deg_{S(G,A)}(u) = c + |V \setminus A| - d = c + d - 2d + |V| - |A|$$

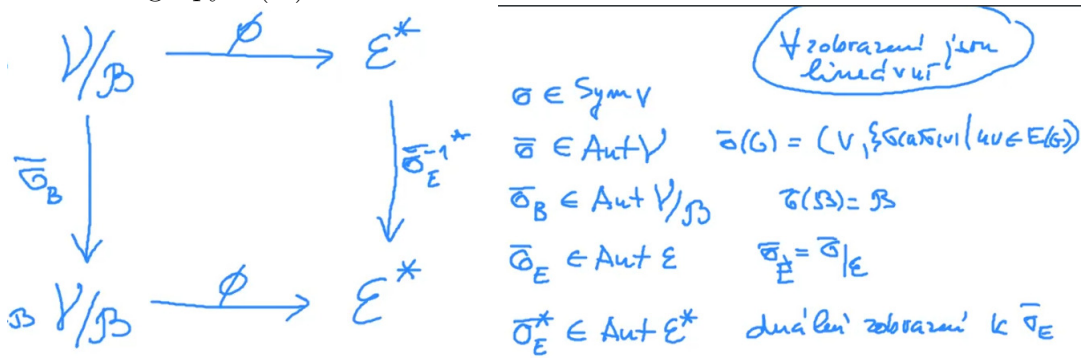
Kde  $(c + d)$  je liché,  $|V|$  je liché,  $|A|$  je sudé. Dohromady sudé.

Takže každý graf lze preswitchovat na Eulerovský graf. Preswitchení Eulerovského grafu se změní na neeulerovský. V každém switchingu tride je 1 Eulerovský graf.

Pro  $n$  sudé. Necht  $K$  je V.P. všech grafů na dané množině vrcholů,  $B$  je prostor el. rezu na úplném grafu,  $\xi$  prostor Eulerovských grafů.

$$\beta = \xi^\perp \Rightarrow \xi^* \simeq K/B$$

Prvky  $\nu/B$  jsou právě třídy ekvivalence dle Seidelova switchingu. Chceme zjistit počet orbit akce grupy  $S(V)$ .



Tvrdíme že diagram komutuje. Necht  $G \in \nu$

$$\bar{\sigma}_B(G + B) \rightarrow \sigma(G) + B, \phi(\sigma(G) + B) \rightarrow \langle \bar{\sigma}(G), \cdot \rangle \in \xi^*$$

$$\phi(G + B) \rightarrow \langle G, \cdot \rangle \in \xi^*, (\bar{\sigma}^{-1})^*(\langle G, \cdot \rangle)$$

Tvrdíme že poslední prvky ve dvou řádcích jsou stejné.

$$\forall X \in \xi : \langle \bar{\sigma}(G)(X) \rangle = (\bar{\sigma}^{-1})^*(\langle G, \cdot \rangle) = \langle G, (\bar{\sigma}^{-1})(G) \rangle$$

Levá část

$$\langle \bar{\sigma}(G)(X) \rangle = |\{e | e \in E(\bar{\sigma} \cap E(X))\}|$$

Pravá část

$$\langle G, (\bar{\sigma}^{-1})(G) \rangle = |\{e | e \in E(G) \cap (\bar{\sigma}^{-1})(X)\}|$$

Z toho diagram komutuje.

Pak dle Burnsideova lemmatu:  $\# \text{ orbit } \nu/B \text{ při akci } S(\nu) = \frac{1}{n!} \sum |(\nu/B)_\sigma|$ .

Taky  $\# \text{ orbit } \xi^* \text{ při akci } S(V) = \frac{1}{n!} \sum |(\xi^*)_\sigma| = \frac{1}{n!} \sum |(\nu/B)_{\sigma^{-1}}|$ . Zbývá dokázat, že  $\# \text{ orbit}$  je stejný i pro  $\xi$  místo  $\xi^*$ .

□

## 5 Spektrum grafu, Moorovy grafy

**Definice 5.1.** Necht  $G$  je  $r$ -regulární graf obvodu většího než 4 (nema ani  $\triangle$  ani kružnice délky 4). Pak  $|V(G)| \geq r^2 + 1$ .

**Definice 5.2.** Moorovy grafy splňují definice nahore, ale navíc  $|V(G)| = r^2 + 1$ .

**Věta 5.3 (Moorovy grafy).** Moorovy grafy existují pro  $r = 1, 2, 3, 7$ , pravděpodobně  $r = 57$ . Pro žádné jiné  $r$  neexistují.

*Důkaz.* 1)  $r = 1$ , cesta délky 2

2)  $r = 2$ , kružnice délky 5

3)  $r = 3$  Petersenův graf

4)  $r = 7$  Homan, Singleton graf

Ostatní  $r$ , necht  $G$  je Moorův graf, na  $n = r^2 + 1$  vrcholech. Vezmeme matice sousednosti.  $A^2$  má počet sledů délky 2 mezi vrcholem  $a - b$ . Na diagonále máme  $r$ , mimo diagonálu je 0 pokud mezi  $a - b$  v původním grafu vedla hrana. Naopak  $A^2$  bude mít 1, pokud mezi  $a - b$  nevedla hrana v  $G$ .

$$A^2 = rI + (J - I - A) \Rightarrow A^2 = (r - 1)I + J - A \Rightarrow A^2 + A - (r - 1)I = J$$

Vezmeme polynom  $P(x) = x^2 + x - (r - 1)$ . Pokud by  $\lambda \in Sp(A) \Rightarrow \lambda^2 + \lambda - (r - 1) \in Sp(A) = Sp(J)$ .

$J$  má  $(n - 1)$  násobné vlastní číslo  $\lambda = 0$ . Poslední vl. číslo je  $n$ . Pak

$$\lambda^2 + \lambda - (r - 1) = 0 \vee n$$

$r$ -regulární graf má největší vl. číslo  $r$ . Dosadíme  $r$  do rovnice.  $r^2 + r - (r - 1) = r^2 + 1 = n$ . Ostatní jsou nulové.

$$\lambda_{1,2} = 1/2 * (-1 \pm \sqrt{1 + 4(r - 1)}) = 1/2 * (-1 \pm \sqrt{4r - 3})$$

Pak  $Sp(A) = \{r, \lambda_1^{m_1}, \lambda_2^{m_2}\}$ . Ze spektra  $J$  víme  $m_1 + m_2 = n - 1 = r^2$ . Taký

$$\sum \lambda_i = tr(A) = 0 \Rightarrow r + m_1 \lambda_1 + m_2 \lambda_2 = 0$$

Vyřešíme systém 2 rovnic o 2 neznámých. Necht

$$s = \sqrt{4r - 3}, s^2 = 4r - 3, r = 1/4 * (s^2 + 3)$$

$$r + -1/2(m_1 + m_2) + s/2(m_1 - m_2) = 0 \wedge m_1 + m_2 = r^2 \Rightarrow r - 1/2r^2 + s/2(m_1 - m_2) = 0$$

1) Necht  $s \notin Q \Rightarrow s/2 \notin Q \wedge r \in N \Rightarrow m_1 = m_2 \Rightarrow r^2 - 2r = 0 \Rightarrow r = 2$ . Pro 2 máme takový graf.

2) Jinak  $s \in N \Rightarrow 1/4(s^2 + 3) - (1/4(s^2 + 3))^2 * 1/2 + s/2(m_1 - m_2) = 0$ . Vynásobíme 32.

$$8(s^2 + 3) - (s^2 + 3)^2 + 16s(m_1 - m_2) = 0$$

Podíváme se jako na polynom  $s$ :  $24 - 9 - s^4 + (\dots)s = 0$ .

$$s^4 + s(\dots) - 15 = 0 \Rightarrow s | 15 \Rightarrow s = \{1, 3, 5, 15\} \Rightarrow r = \{1, 3, 7, 58\}$$

□

## 6 Silne regularni grafy, propletani vl cisel

**Definice 6.1.** Silne regularni je graf pokud neni uplny (trivialni pripad) a  $\exists d, e, f \in \mathbb{N} : \forall v \in V \deg(v) = d$ . Kazde 2 sousedni vrcholy maji  $e$  spolecnych sousedu (2 vrcholy lezi v  $e \triangle$ ), kazde 2 nesousedni vrcholy maji  $f$  spolecnych sousedu ( $\exists f$  cest delky 2).

**Věta 6.2 (Silne regularni grafy (nebude u zkousky)).** Je-li  $G$  silne regularni s parametry  $d, e, f$ , pak nastava jedna z 2 moznosti:

- $f = e + 1, d = 2f, |V(G)| = 2d + 1$  nebo
- $\exists s \in \mathbb{N} : s^2 = (e - f)^2 - 4(f - d) \wedge \frac{d}{2fs}((d - 1 + f - e)(s + f - e) - 2f) \in \mathbb{N}$ .

*Důkaz.* Necht  $A$  je matice sousednosti  $G$ ,  $n = |V(G)|$ , uvazme  $A^2$ . Na diagonale jsou stupne  $d$ , mimo diagonalu pokud v  $A$  byla 1 - zmeni se na  $e$ , 0 se zmeni na  $f$ .

$$A^2 = \begin{pmatrix} d & e & f \\ e & d & f \\ f & f & d \end{pmatrix}$$

$$A^2 = dI + eA + (J - I - A)f \Rightarrow A^2 + (f - e)A + (f - d)I = fJ$$

Dosadime vl. cislo  $\lambda \in Sp(A)$ .

$$\lambda^2 + (f - e)\lambda + (f - d) \in Sp(fJ) = \{f * n, 0^{(n-1)}\}$$

$d$  odpovida vl. vektoru  $\bar{1}$  u  $A$ , u  $J$  vl. vektoru  $\bar{1}$  odpovida  $n$ . Dosadime  $d$ :

$$d^2 + (f - e)d + f - d = fn \Rightarrow d(d - e - 1) = f(n - d - 1)$$

Zafixujme nejaky vrchol  $x \in V$ . Kolik  $\exists$  indukovanych cest delky 2:

$$|\{(x, a) | xa, ab \in E(G) \wedge xb \notin E(G)\}|$$

Mame  $d$  zpusobu zvolit souseda  $x$ , pak vrchol  $a$  ma  $d$  sousedu,  $e$  jsou spolecne s  $x$ ,  $x$  taky patri mezi sousedy. Dostaneme  $d(d - e - 1)$ . Na druhou stranu z pohledu vrcholu  $b$ .  $x$  ma  $(n - d - 1)$  nesousedu, pak vrchol  $a$  je mezi  $f$  sousedu  $(x, b)$ . Dostaneme  $f(n - d - 1)$ .

Pro  $\lambda \in Sp(A) \setminus \{d\}$  zbyva 0:

$$\lambda^2 + (f - e)\lambda + f - d = 0 \Rightarrow \lambda_{1,2} = \frac{e - f \pm \sqrt{(e - f)^2 - 4(f - d)}}{2}$$

Oznacme  $D = \sqrt{(e - f)^2 - 4(f - d)}$ . Pak  $\lambda_1 = 1/2(e - f + s)$ ,  $p$  krat a  $\lambda_2 = 1/2(e - f - s)$ ,  $q$  krat.

Z nasobnosti vl. cisel

$$\begin{aligned} 1 + p + q &= n \\ a + p\lambda_1 + q\lambda_2 &= tr(A) = 0 \\ tr(A^2) &= \sum \lambda_i^2 = nd \Rightarrow d^2 + p\lambda_1^2 + q\lambda_2^2 = nd \end{aligned}$$

Vyresime soustavu 3 rovnic o 3 neznamych. Dosadime hodnoty  $\lambda_1, \lambda_2$  do 2. rovnici:

$$d + 1/2p(e - d + s) + 1/2q(e - f - s) = 0 \Rightarrow d + 1/2(p + q)(e - f) + 1/2(p - q)s = 0$$

Nastavaji 2 případy:

1)  $s \notin \mathbb{Q} \Rightarrow$  poslední scítanec je iracionalni a nutne  $p = q = 1/2(n-1)$ .

$$d + 1/2(n-1)(e-f) = 0 \Rightarrow \frac{2d}{n-1} = (f-e)$$

Pak stupeň vrcholu  $d \leq (n-1)$

$$\frac{2d}{n-1} = (f-e) \leq \frac{2(n-1)}{2} = 2$$

Pokud  $(f-e) = 2 \Rightarrow d = n-1 \Rightarrow G = K_n$  což jsme vyloučili definicí. Jinak

$$(f-e) = 1 \wedge n = 2d+1$$

Pracujme s 3. rovnicí:

$$d^2 + 1/2(n-1) * 1/4(e-f+s)^2 + 1/2(n-1) * 1/4(e-f-s)^2 = nd$$

dosadíme  $(e-f) = -1$ .

$$d^2 + 1/2(n-1) * 1/4(s-1)^2 + 1/2(n-1) * 1/4(-1-s)^2 = nd$$

$$8d^2 + (n-1)(s^2 - 2s + 1) + (n-1)(s^2 + 2s + 1) = 8nd$$

$$8d^2 + (n-1)(s^2 - 2s + 1 + s^2 + 2s + 1) = 8nd$$

$$8d^2 + (n-1)(2s^2 + 2) = 8nd$$

$$4d^2 + (n-1)(s^2 + 1) = 4nd$$

Dosadíme  $n = 2d-1$

$$4d^2 + 2d(s^2 + 1) = 4(2d+1)d$$

$$2d + (s^2 + 1) = 2(2d+1)$$

Pak  $s^2 = 1 + 4(d-f)$

$$2d + 2 + 4d - 4f = 4d + 2$$

$$2d = 4f \Rightarrow d = 2f$$

2) Jinak  $s \in \mathbb{Z}$  Dosadíme do 2. a 3. rovnice  $n$ , vyřešíme pro  $p, q$ .

$$d + 1/2p(e-d+s) + 1/2q(e-f-s) = 0$$

$$d^2 + 1/2(n-1) * 1/4(e-f+s)^2 + 1/2(n-1) * 1/4(e-f-s)^2 = (1+q+p)d$$

Zbavíme se jmenovatele a roznásobíme kvadraty v 3.

$$p(e-d+s) + 1/2q(e-f-s) = 2d$$

$$p((e-f+s)^2 - 4d) + q((e-f-s)^2 - 4d) = 4d(1-d)$$

Spocítáme  $p, q$  pomocí determinantu.

$$p = \frac{\begin{vmatrix} -2d & e-f-s \\ 4d(1-d) & (e-f-s)^2 - 4d \end{vmatrix}}{\begin{vmatrix} e-f+s & e-f-s \\ (e-f+s)^2 - 4d & (e-f-s)^2 - 4d \end{vmatrix}}$$



Dolní determinant

$$\begin{aligned} & (e-f+s)((e-f-s)^2-4d) - (e-f-s)((e-f+s)^2-4d) = \\ & (e-f+s)(e-f-s)(e-f-s-e+f-s) + 4d(e+f-s+e-f-s) = \\ & ((e-f)^2-s^2)(-2s) + 4d(-2s) = (-2s)((e-f)^2+4d-s^2) \end{aligned}$$

Dosadíme  $s^2 = (e-f)^2 + 4(d-f)$ .

$$(-2s)((e-f)^2+4d-(e-f)^2-4(d-f)) = -8fs$$

Horní determinant:

$$\begin{vmatrix} -2d & e-f-s \\ 4d(1-d) & (e-f-s)^2-4d \end{vmatrix}$$

2 hours later...

$$p = \frac{d((d-1+f-e)(s+f-e)-2f)}{2fs} \in \mathbb{Z}$$

□

**Věta 6.3 (Friendship theorem).** *Necht v grafu  $G$  mají každé 2 různé vrcholy právě 1 spol. souseda. Pak  $G$  obsahuje vrchol, který sousedí se všemi ostatními vrcholy grafu.*

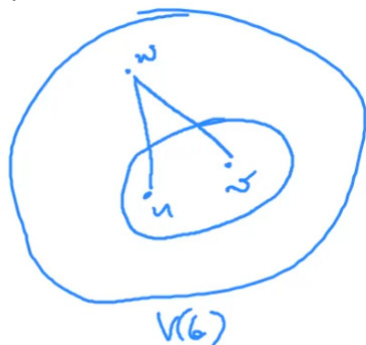
*Důkaz.* Pokud platí  $e = f = 1 \Rightarrow \exists v \in V$  který sousedí se všemi ostatními vrcholy.

Necht  $N_G(u)$  je množina sousedů  $u \in V$ . Vezmeme množinový systém  $\{N_G(u) | u \in V\}$ .

Pak průnik dvou množin je jednoprvkový.

$$\forall a \neq b : |N_G(a) \cap N_G(b)| = 1$$

Taky z obrázku



$$\forall a \neq b : \exists! N_G(w) : a, b \in N_G(w)$$

Což je skoro konečná projektivní rovina KPR. Chybí 3. axiom. Rozebereme 2 případy:

1) 3. axiom platí  $\Rightarrow \{N_G\}$  je KPR. Pak

$$\forall a |N_G(a)| = m+1 = \deg(a)$$

$$n = |V(G)| = m^2 + m + 1$$

Z čehož  $G$  je silně regulární s parametry  $d = m+1 \wedge e = f = 1$ . První případ nastat nemůže kvůli podmince na  $e = f = 1$ . Neboli 2 případ:

$$p = \frac{d((d-1+f-e)(s+f-e)-2f)}{2fs} \in \mathbb{Z}$$

$$(e-f)^2 - 4(f-d) = s^2 \wedge e = f = 1 \Rightarrow s = 2\sqrt{m} = 2t$$

Dosadíme

$$p = \frac{t^2+1}{4t}((t^2*2t)-2) = \frac{(t^2+1)(t^3-1)}{2t} \notin N : t > 1$$

Pripad  $t = 1 \Rightarrow m = 1$  není zajímavý protože KPR řádu 1 je  $\Delta$ .

2) 3. axiom neplatí  $\Rightarrow \{N_G\}$  z teorie KPR buď všechno leží na 1 primce nebo jeden vrchol samostatně a zbytek na primce. Pak ten samostatný vrchol je hledán soused všech:

$$\exists a : N_G(a) = V(G) \setminus \{a\}$$

□

**Věta 6.4 (vl. čísla Hermitovské matice(BD)).** Necht  $A \in \mathbb{C}^{n \times n}$  je Hermitovská,  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$  její vl. čísla. Necht  $b_1, b_2, \dots, b_n \in \mathbb{C}^n$  je ortonormalní báze vl. vektorů. Pak pro  $k = 1, 2, \dots, n$  platí

$$x^*Ax \geq \lambda_k x^*x \forall x \in \langle \{b_1, b_2, \dots, b_k\} \rangle$$

$$x^*Ax \leq \lambda_k x^*x \forall x \in \langle \{b_k, b_{k+1}, \dots, b_n\} \rangle$$

**Věta 6.5 (Propletání vl. čísel).** Necht  $A \in \mathbb{C}^{n \times n}$  je Hermitovská,  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$  její vl. čísla. Necht  $B$  je hlavní podmatice řádu  $k \times k$  (vznikne vynecháním  $(n-k)$  řádků), Necht  $b_1, b_2, \dots, b_n \in \mathbb{C}^n$  jsou vl. čísla matice  $B$ . Pak platí

$$\lambda_i \geq b_i \geq \lambda_{i+n-k}$$

*Důkaz.* Nejprve se podíváme na případ vynechání  $i$ -ho řádku. Necht  $B$  má ortonormalní báze  $y_1, y_2, \dots, y_{n-1} \in \mathbb{C}^{n-1}$ . Vnoríme tyto vektory do  $\mathbb{C}^n$  tak, že na pozici  $i-1$  vložíme 0. Označíme je  $z(y)$ . Pak

$$z^*(y)Az(y) = y^*By$$

Uvažme 3 množiny,  $j$  je libovolné

$$S_1 = \langle \{x_j, x_{j+1}, \dots, x_n\} \rangle$$

$$S_2 = \langle \{y_1, y_2, \dots, y_j\} \rangle$$

$$S_3 = \{z(y) : y \in S_2\}$$

$$\dim S_1 = n - j + 1$$

$$\dim S_3 = \dim S_2 = j$$

$$\dim S_1 + \dim S_3 = n + 1 > \dim(S_1 + S_2)$$

Z toho  $\dim(S_1 \cap S_2) > 0 \Rightarrow \exists l \neq 0 : l \in S_1 \cap S_2$ . Podíváme se na

$$l \in S_1 \Rightarrow l^*Al \geq \lambda_j l^*l$$

$$l \in S_3, y \in S_2, l = z(y) : l^*Al = y^*By \geq b_j y y^* = b_j l^*l \geq \lambda_j l^*l$$

$$\lambda_j l^*l \geq b_j l^*l \Rightarrow \lambda_j \geq b_j$$

Ted dokazeme  $b_j \geq \lambda_{j+1}$

$$\begin{aligned} S_1 &= \langle \{x_1, x_2, \dots, x_{j+1}\} \rangle \\ S_2 &= \langle \{y_j, y_{j+1}, \dots, y_{n-1}\} \rangle \\ S_3 &= \{z(y) : y \in S_2\} \\ \dim S_1 &= j+1 \\ \dim S_3 &= \dim S_2 = n-j \\ \dim S_1 + \dim S_3 &= n+1 > \dim(S_1 + S_2) \end{aligned}$$

$$\begin{aligned} l \in S_1 &\Rightarrow l^* A l \geq \lambda_{j+1} l^* l \\ l \in S_3, y \in S_2, l = z(y) : l^* A l &= y^* B y \leq b_j y y^* = b_j l^* l \geq \lambda_j l^* l \\ \lambda_j l^* l &\geq b_j l^* l \Rightarrow \lambda_{j+1} \leq b_j \end{aligned}$$

Ted pro obecne k.

Z obrazku

$$\lambda_i \geq k_i \geq \lambda_{i+k}, i = 1, 2, \dots, n-k$$

□

**Věta 6.6 (Nezav množina a vl čísla).** Necht  $G$  je graf o  $n$  vrcholech s vl čísly  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ . Pak

$$\alpha(G) \leq \min\{|\{i : \lambda_i \leq 0\}|, |\{i : \lambda_i \geq 0\}|\}$$

*Důkaz.* Necht  $W \subseteq V(G)$  je nezav množina velikosti  $\alpha$ . Matice sousednosti této množiny je nulová  $\alpha \times \alpha$ . Taký je to hlavně podmatice  $A_G$ . Proto její vl. čísla (nuly) propletaji vl čísla  $G$ . Z toho

$$\lambda_\alpha \geq 0 \geq \lambda_{n-\alpha+1}$$

□

## 7 Odhady pomoci spektra

**Věta 7.1 (Propletani A).** Necht  $A \in \mathbb{C}^{n \times n}$  Hermitovská.  $S \in \mathbb{C}^{m \times n}$  taková, že  $S^* S = I$ . Potom vl čísla  $S^* A S$  propletaji vl čísla matice  $A$ .

*Důkaz.* Radky matice  $S$  jako vektory v  $\mathbb{C}^n$  lze rozšířit na ortonormalní báze  $\mathbb{C}^n$  (Gram-Schmidt z LA). Sestavíme z ní matici  $T$ , necht

$$R = \begin{pmatrix} S \\ T \end{pmatrix}$$

Pak  $RR^* = I$  a

$$RAR^* = \begin{pmatrix} SAS^* & SAT^* \\ TAS^* & TAT^* \end{pmatrix}$$

Pak  $SAS^*$  je hlavní podmatice  $RAR^*$ , a vln. čísla  $SAS^*$  propleťají vln. čísla  $RAR^*$ . Pritom  $Sp(RAR^*) = Sp(A)$  z LA, protože matice jsou podobné.  $\square$

**Věta 7.2 (Propletani B).** *Necht:*

$$\begin{pmatrix} A_{11} & A_{12} & \dots & A_{1m} \\ A_{21} & A_{22} & \dots & A_{2m} \\ \dots & \dots & \dots & \dots \\ A_{m1} & A_{m2} & \dots & A_{mm} \end{pmatrix}.$$

*Je Hermitovská matice v blokovém tvaru.  $A_{ij} \in \mathbb{C}^{m_i \times n_j}$ .  $\sum_{i=1}^m n_i = n$ .*

*Pak necht  $B \in \mathbb{C}^{m \times m}$  je matice jejíž prvky  $b_{ij} = \frac{\sum_{a \in A_{ij}} a}{n_i}$  jsou průměrné radkové součty bloky  $A$ . Potom vln. čísla  $B$  propleťají vln. čísla  $A$ .*

*Důkaz.* Vezmeme matici  $P \in \{0,1\}^{m \times n}$ . Bude rozdělena do bloku velikosti  $n_i, i = 1, 2, \dots, m$ . V každém radku 1ky jsou v bloku  $i$ , jinak nuly.

Potom  $PP^T$  je diagonální matice  $D$  protože jedničky jsou na různých pozicích. Sk. součin dvou různých radků je 0. Na diagonále je norma  $i$ -ho radku  $= n_i$ .

Použijeme matici  $P$  abychom dostali radkové součty matice  $A$ :

V matici  $PA$  dostaneme sloupcový součet po blocích. Pak v matici  $PAP^T$  dostaneme součty všech prvků v blocích.

Pro rovnost s maticí  $B$  ještě potřebujeme vydělit  $n_i$ . Na což použijeme  $D^{-1}$  která má na diagonále  $\frac{1}{n_i}$ .

$$B = D^{-1}PAP^T$$

Necht  $S = D^{-1/2}P$ .  $S$  je reálná matice, pro níž platí

$$SS^T = D^{-1/2}PP^T(D^{-1/2})^T = D^{-1/2}DD^{-1/2} = E$$

Dle Věty o propletání A 7.1, vln. čísla  $SAS^T$  propleťají vln. čísla  $A$ .

$$SAS^T = D^{-1/2}PAP^T(D^{-1/2})^T = D^{-1/2}DBD^{-1/2} = D^{1/2}BD^{-1/2}$$

Pak  $SAS^T$  a  $B$  jsou podobné  $\Rightarrow$  mají stejné spektrum.

$$Sp(SAS^T) = Sp(B)$$

$\square$

**Věta 7.3 (Nezav množ v d-regularním).** Necht  $G$  je  $d$ -regularní graf o  $n$  vrcholech s vl čísly  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ . Pak

$$\alpha(G) \leq n \frac{-\lambda_n}{d - \lambda_n}$$

*Důkaz.* Necht  $A$  je matice sousednosti grafu  $G$ .

$$Sp(A) = \{\lambda_1 = d \geq \lambda_2 \geq \dots \geq \lambda_n\}$$

$$Sp(J) = \{n, 0^{n-1}\}$$

Matice  $A, J$  komutují  $\Rightarrow$  mají společnou ortonormalní báze.

$$\exists X : X^* X = E, X^* A X = \Lambda_A$$

Kde  $\Lambda_A$  je diagonální matice s vl. čísly na diagonále, rozmístěné dle uspořádání. Podobně pro  $J$ :

$$X^* A X = \Lambda_A, (\Lambda_J)_{1,1} = n$$

Z věty o ortonormalní bázi vl. vektor příslušný největšímu vl. číslu je nezáporný. Ostatní mají záporné složky. Pak vektor  $\bar{1}$  je příslušný největšímu vlastnímu číslu  $A - d$ . Také odpovídá vl. číslu  $n$  matice  $J$ .

Uvažme matici:

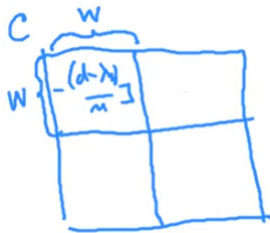
$$C = A - \frac{1}{n}(d - \lambda_n)J$$

Její vl. čísla jsou lin. kombinace vl. čísel  $A, J$ .

$$X^* C X = X^* \left( A - \frac{1}{n}(d - \lambda_n)J \right) X = X^* A X - \frac{1}{n}(d - \lambda_n)X^* J X = \Lambda_A - \Lambda_K = \Lambda_C$$

Kde  $(\Lambda_K)_{1,1} = d - \lambda_n$ , jinak 0. Z toho  $\Lambda_C$  má na diagonále  $\{\lambda_n, \lambda_2, \dots, \lambda_n\}$ . Odtud  $\lambda_n$  je největší vl. číslo matice  $C$ .

Necht  $W \subseteq V(G)$  je nezav. množ  $G$ ,  $|W| = \alpha(G)$ . Pak matice  $A$ , po seskupení řádků odpovídajících  $W$ , má nulovou hlavní podmatice odpovídající  $W$ . Z toho matice  $C$  má na těchto pozicích  $-\frac{1}{n}(d - \lambda_n)$ . Také je to hlavní podmatice.



Vl. čísla matice  $-\frac{1}{n}(d - \lambda_n)J$  propleťají vl. čísla matice  $C$ .

$$Sp\left(-\frac{1}{n}(d - \lambda_n)J\right) = \{0^{\alpha-1}, \alpha * -\frac{1}{n}(d - \lambda_n)\}$$

Z věty o propletání:

$$\alpha(G) * -\frac{1}{n}(d - \lambda_n) \geq \lambda_n \Rightarrow \alpha(G) \leq n \frac{-\lambda_n}{d - \lambda_n}$$

□

**Důsledek 7.4.** Necht  $G$  je  $d$ -regulární graf o  $n$  vrcholech s vl. čísly  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ . Pak

$$\chi(G) \geq 1 + \frac{\lambda_1}{|\lambda_n|}$$

Plyne z toho, že  $\chi(G) \geq \frac{n}{\alpha(G)}$ . Barvení grafu je rozložení na  $\chi(G)$  nezávislých množin. Každá z nich má velikost  $\chi(G)/\alpha(G)$ . Kombinací dvou nerovností dostaneme tvrzení.

**Věta 7.5 (Polomer spektra grafu).** Necht  $G$  je graf o  $n$  vrcholech s vl. čísly  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ . Pak

$$\Delta(G) \geq \lambda_1 \geq \deg_{avg}(G)$$

Kde  $\Delta(G)$  je max deg grafu.

*Důkaz.* 1) Nerovnost  $\Delta(G) \geq \lambda_1$ . Doplňme  $G$  na  $\Delta$ -regulární graf  $H$  tak, aby  $G$  byl jeho indukovaný podgraf. Pak vl. čísla  $G$  proleťají vl. čísla  $H$ .  $\lambda_{max}(H) = \Delta \Rightarrow \Delta(G) \geq \lambda_1$ .

2) Nerovnost  $\lambda_1 \geq \deg_{avg}(G)$ . Vezmeme matice sousednosti  $A$ , představíme ji jako matici s 1 blokem. Pak matice průmerných radkových součtu je  $B = \deg_{avg}(G)$  jednoprvková.

Dle Věty o proleťání B 7.2,  $Sp(B) = \{\deg_{avg}(G)\}$  proleťá spektrum  $A \Rightarrow \lambda_1 \geq \deg_{avg}(G)$ .  $\square$

**Věta 7.6 (Barevnost libovolného grafu).** Necht  $G$  je graf o  $n$  vrcholech s vl. čísly  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ . Pak

$$\chi(G) \leq 1 + \lambda_1$$

*Důkaz.* Necht  $H$  je  $\chi$ -kritický indukovaný podgraf grafu  $G$ . Minimalní stupeň vrcholu v  $\chi$ -kritickém grafu je aspoň  $\chi - 1$ . Označme jeho největší vl. číslo jako  $h_1$ . Z věty o proleťání plyne  $\lambda_1 \geq h_1$ . Z věty polomeru spektra 7.5 dostáváme

$$h_1 \geq \deg_{avg}(H) \geq \delta(H) \geq \chi - 1 \Rightarrow \lambda_1 \geq \chi - 1$$

$\square$

**Věta 7.7 (Nezav. množ. v libovolném grafu).** Necht  $G$  je graf o  $n$  vrcholech s vl. čísly  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ . Pak

$$\alpha(G) \leq n \frac{-\lambda_1 \lambda_n}{\sigma^2(G) - \lambda_1 \lambda_n}$$

*Důkaz.* Necht  $W \subseteq V(G)$  je nezav. množ.  $G$ ,  $|W| = \alpha(G)$ . Rozdělíme matici  $A$  dle  $W$  a  $V \setminus W$ .

$$A = \begin{array}{c|c} W & V \setminus W \\ \hline \begin{array}{c} \text{ } \\ \text{ } \end{array} & \begin{array}{c} A_{12} \\ \text{ } \end{array} \\ \hline \begin{array}{c} V \setminus W \\ \text{ } \end{array} & \begin{array}{c} A_{21} \\ A_{22} \end{array} \end{array} \left. \begin{array}{l} \} \alpha \\ \} n - \alpha \end{array} \right\}$$

Použijeme Větu o proleťání B 7.2.

$$B = \begin{pmatrix} 0 & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

Pak  $Sp(B) = \{h_1 \geq h_2\}$  proleťá  $Sp(A) = Sp(G)$ .

Dal víme, že počet hran mezi  $W$  a  $v \setminus W$  se rovná

$$\alpha b_{12} = (n - \alpha) b_{21} \Rightarrow b_{21} = \frac{\alpha}{n - \alpha} b_{12}$$

Z LA součin vl. čísel je determinant:

$$h_1 h_2 = \det(B) = -b_{12} \cdot b_{21} = b_{12}^2 \cdot \frac{\alpha}{n - \alpha}$$

Z propletání:

$$\lambda_1 \geq h_1 \geq h_2 \geq \lambda_n \Rightarrow -h_2 \leq -\lambda_n \Rightarrow -h_1 h_2 \leq -\lambda_1 \lambda_n$$

Protože všichni sousedé vrcholu  $z \in W$  jsou z  $V(G) \setminus W \Rightarrow b_{12} \geq \delta(G)$ .

$$\begin{aligned} -\delta^2(G) \frac{\alpha}{n - \alpha} &\leq -\lambda_1 \lambda_n \\ -\delta^2(G) \alpha &\leq (n - \alpha) * (-\lambda_1 \lambda_n) \\ \alpha(\delta^2(G) - \lambda_1 \lambda_n) &\leq n(-\lambda_1 \lambda_n) \\ \alpha(G) &\leq n \frac{-\lambda_1 \lambda_n}{\delta^2(G) - \lambda_1 \lambda_n} \end{aligned}$$

□

**Věta 7.8 (Barevnost souvisleho grafu).** *Necht  $G$  je souvislý graf o  $n$  vrcholech s vl. čísly  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ . Pak*

$$\chi(G) \geq 1 + \frac{\lambda_1}{|\lambda_n|}$$

*Věta je analogická důsledku věty 1, zesiluje ji pro souvislé grafy.*

*Důkaz.* Obarvíme graf pomocí  $\chi$  barev. Necht  $x$  je reálný vl. vektor příslušný vl. číslu  $\lambda_1$  (Existuje dle Frobeniovy věty). Ze souvislosti  $x_i > 0 \forall i$ . Sestavíme matici  $P \in \mathbb{R}^{n \times n}$ .

$$P_{ij} = \begin{cases} x_j & \text{pro } j \in W \\ 0 & \text{pro } j \notin W \end{cases}$$

Pak  $PP^T = D$  je diagonální matice, na diagonále  $\sum_{u \in W_j} x_u^2 > 0$ . Necht  $S = D^{-1/2}P$ . Protože

$$SS^T = D^{-1/2}PP^T(D^{-1/2})^T = D^{-1/2}DD^{-1/2} = I$$

Dle Věty o propletání A 7.1, vl. čísla  $SAS^T$  propletaji vl. čísla  $A$ . Necht vl. čísla  $SAS^T$  jsou  $\{h_1, h_2, \dots, h_\chi\}$ . Ma na diagonále same nuly, z toho

$$\sum_{i=1}^{\chi} h_i = 0$$

Dal

$$SAS^T D^{1/2} \cdot \bar{1} = SAP^T D^{-1/2} D^{1/2} \cdot \bar{1} = SAP^T \bar{1}$$

$$P^T \cdot \bar{1} = x \Rightarrow SAP^T \bar{1} = SAx = \lambda_1 Sx = \lambda_1 D^{-1/2} PP^T \bar{1} = \lambda_1 D^{-1/2} D \bar{1} = \lambda_1 D^{1/2} \bar{1}$$

Dostáváme

$$SAS^T D^{1/2} \cdot \bar{1} = \lambda_1 D^{1/2} \bar{1} \Rightarrow \lambda_1 \in Sp(SAS^T)$$

Ale taky odpovida nenulovemu realnemu vl. vektoru, takze  $\lambda_1 = h_1$ . Pouzijeme propletani

$$h_1 = \lambda_1 \geq h_2 \geq \dots \geq h_\chi \geq \lambda_n \wedge \sum_{i=2}^{\chi} h_i = 0 \Rightarrow -\lambda_1 = h_1 = -\sum_{i=2}^{\chi} h_i$$

Pouzijeme horni odhad pro soucet pres  $\#$  scitancu krat min hodnota ( $\lambda_n$ ).

$$-\lambda_1 = h_1 = -\sum_{i=2}^{\chi} h_i \geq (\chi - 1)(-\lambda_n)$$

Po uprave

$$\chi(G) \geq 1 + \frac{\lambda_1}{|\lambda_n|}$$

□

## 8 Shannonova kapacita

**Definice 8.1.** Necht  $A$  je abcd,  $A = \{a, e, o, h, g\}$ . Pak sestavime graf  $G_A = (A, \{xy | x \sim y\})$ . Kde ekvivalence znamena, ze  $x$  je snadno zameni za  $y$ .

Pak by slo vzit nezavislou mnozinu a pouzivat jen tyto symboly. Zbylo by hodne malo symbolu.

Lepe - dohodneme se na pevne delce. Vezmeme  $C \subseteq A^n$ . Pak bezpecny kod bude pouzivat pouze slova z  $C$ . Dal sestavime  $G_{A^n}$  graf zamenitelnosti pro  $A^n$ .

**Pozorování 8.2.** 2 slova jsou zamenitelna  $\iff$  maji na  $i$ -te pozici stejne pismeno nebo zamenitelne. Presne odpovida uplnemu soucinu grafu.

**Definice 8.3.** Pro grafy  $G, H$  definujme uplny soucin grafu jako graf

$$G \boxtimes H = (V(G) \times V(H), \{(a, b)(x, y) : (a = x \vee ax \in E(G)) \wedge (b = y \vee by \in E(H))\})$$

Kde vrcholy  $a, x$  jsou z grafu  $G$ ,  $b, y$  z grafu  $H$ .

Taky definujme  $G^n = G \boxtimes G \boxtimes \dots \boxtimes G$ .

**Definice 8.4.** Shannonova kapacita grafu  $G$ :

$$\Theta(G) = \sup_k \sqrt[k]{\alpha(G^k)}, \forall k$$

**Pozorování 8.5.**

$$\forall G \Theta(G) \geq \alpha(G)$$

Pokud v grafu je nezav množina  $B \subseteq V(G)$ ,  $|B| = \alpha(G)$ . Pak  $B^k$  je taky nezav množina. Z toho

$$\sqrt[k]{\alpha(G^k)} \geq \sqrt[k]{\alpha(B^k)} = \sqrt[k]{\alpha^k(G)} = \alpha(G)$$

**Pozorování 8.6.** Necht  $\sigma(G) = \chi(-G)$ . Coz je minimalni pocet uplnych podgrafu pokrývající množinu grafu. Pak

$$\Theta(G) \leq \sigma(G)$$

Protoze  $K_n \boxtimes K_m = K_{mn}$ . Soucin uplnych je uplny graf, jina možnost není (jsou tam vsechny hrany). Takze

$$\sigma(G^k) \leq \sigma^k(G) \Rightarrow \sqrt[k]{\sigma(G^k)} \leq \sigma(G) \Rightarrow \Theta(G) \leq \sigma(G)$$



**Pozorování 8.7.**  $G$  je perfektní graf  $\Rightarrow \sigma(G) = \alpha(G)$ . Pak

$$\alpha(G) \leq \Theta(G) \leq \sigma(G) = \alpha(G)$$

**Definice 8.8.** Lovascova ortonormalní reprezentace grafu je zobrazení  $f : V \rightarrow \mathbb{R}^d$  splňující:

- $\|f(u)\| = \langle f(u), f(u) \rangle = 1 \forall u \in V$  a
- $\langle f(a), f(b) \rangle = 0 \forall a \neq b \wedge ab \notin E(G)$ .

Pak velikost reprezentace je:

$$\|f\| = \inf_{c: \|c\|=1} \max_{a \in V} \frac{1}{\langle c, f(a) \rangle^2}$$

**Příklad 8.9.** Pro graf který nemá žádný vrchol potřebujeme systém vzájemně  $\perp$  vektorů velikosti  $V(G)$ , neboli prostor dimenze  $V(G)$ .

Pro úplný graf stačí volit vektory stejného směru nebo dokonce stejné.

**Definice 8.10.** Lovascova dzeta funkce grafu  $G$ :

$$\vartheta(G) = \inf_f \|f\|$$

Chceme pro nějakou reprezentaci najít takový jeden vektor  $c$ , který minimalizuje hodnotu  $\langle c, f(u) \rangle^2$ .

**Příklad 8.11.** Pro úplný graf zvolíme reprezentaci která se skládá ze stejných vektorů,  $c$  vezmeme ve stejném směru. Pak všechny skalární součiny jsou 1. Z toho

$$\vartheta(K_n) \leq 1$$

**Definice 8.12.** *Rukojet* reprezentace  $f$  je vektor  $c$  (jeden vektor), pro který  $f$  nabývá minima. Infimum v def. velikosti ortonormalní reprezentace se nabývá, protože  $f = f(c)$  je spojitá a zdola omezena.

V definici stačí uvažovat omezenou dimenzi, např.  $d \leq |V(G)|$ .

Infimum v def. dzeta funkce se také nabývá, protože  $\|f\|$  je spojitá funkce  $f$ . Pak

$$\vartheta(G) = \min_f \min_{c: \|c\|=1} \max_{u \in V} \frac{1}{\langle c, f(u) \rangle^2}$$

**Úmluva 8.13.** Muze se stát, že rukojet je vektor kolmý na nějaký z vektorů  $f$ . Pak  $\vartheta(G) = \infty$ . Budeme se ale takovým rukojetím vyhýbat. Všechny vektory reprezentace leží v nadrovine, je jich konečně mnoho.

**Lemma 8.14.**  $\forall G : \alpha(G) \leq \vartheta(G)$ .

*Důkaz.* Necht  $G$  je graf, a máme optimální repr.  $f$  s rukojetí  $c$ .  $\|f\| = \vartheta(G)$ . Taký  $W \subseteq V(G)$  je nezav. množina:

$$\alpha(G) = |W|$$

Vektory reprezentující  $W$  jsou na sebe kolmé. Můžeme je doplnit na ortonormalní bázi  $B$  prostoru  $\mathbb{R}^d$ . Pak rukojet můžeme napsat jako lin. kombinaci pomocí vektorů z  $B$ :

$$c = \sum_{b \in B} \langle c, b \rangle \cdot b$$

Dal c je jedn. vektor:

$$1 = \langle c, c \rangle = \left\langle \sum_v \langle c, v \rangle, \sum_v \langle c, v \rangle \right\rangle = \sum_u \sum_v \langle c, u \rangle \langle c, v \rangle \langle u, v \rangle$$

vektory u, v jsou z ortonormalni baze, takže pro  $u \neq v$  je součet nula, jinak místo posledního sk součinu tam bude 1. Pak dostaneme součet vlevo, který je větší než suma pro vektory reprezentace nezáv množiny.

$$\sum_{b \in B} \langle c, b \rangle^2 \geq \sum_{u \in W} \langle c, f(u) \rangle^2$$

Náhledneme ze velikost sk. součinu je omezena maximumem pro všechny vrcholy, což je právě  $\vartheta(G)$ .

$$\forall a \in V(G) : \frac{1}{\langle c, f(a) \rangle^2} \leq \vartheta(G) \Rightarrow \langle c, f(a) \rangle^2 \geq \frac{1}{\vartheta(G)}$$

$$\sum_{u \in W} \langle c, f(u) \rangle^2 \geq \sum_{a \in W} \frac{1}{\vartheta(G)}$$

Scítáme přes velikost nezávislé množiny, dostaneme  $\frac{\alpha(G)}{\vartheta(G)}$  Dohromady

$$1 = \|c\| \geq \frac{\alpha(G)}{\vartheta(G)} \Rightarrow \vartheta(G) \geq \alpha(G)$$

□

**Lemma 8.15.**  $\forall G, \forall H : \vartheta(G \boxtimes H) \leq \vartheta(G) \cdot \vartheta(H)$ . Taky

$$\forall G \forall k \in \mathbb{N} : \vartheta(G^k) \leq \vartheta^k(G)$$

*Důkaz.* Necht f je optimální ortonormalní repr. G s rukojetí c. Podobně g pro H s rukojetí d. Uvažme tenzorový součin  $f \circ g$  jako ortonormalní reprezentace součinu grafu.

$$(u, v) \in V(G \boxtimes H), (f \circ g)(u, v) = (f(u) \circ g(v)) = (f(u)_i g(v)_j)_{i,j}, i = 1, 2, \dots, n_1; j = 1, 2, \dots, n_2$$

Vezmeme  $(u, v), (u', v') : (uu' \notin E(G) \wedge u \neq u') \vee (vv' \notin E(H) \wedge v \neq v')$ . Pak

$$\langle f(u) \circ g(v), f(u') \circ g(v') \rangle = \langle f(u), f(u') \rangle \cdot \langle g(v), g(v') \rangle$$

Pak buď jeden sk součin je 0 nebo druhý z volby vrcholu. Takže

$$\langle f(u), f(u') \rangle \cdot \langle g(v), g(v') \rangle = 0$$

Pak rukojet pro  $G \boxtimes H$  bude  $c \circ d$ . Pak

$$\|f \circ g\| \leq \max_{u,v} \frac{1}{\langle c \circ d, f(u) \circ g(v) \rangle^2} = \max \frac{1}{\langle c, f(u) \rangle^2 \cdot \langle d, g(v) \rangle^2}$$

Max je dvou funcí je menší než součin max dvou funkcí:

$$\max \frac{1}{\langle c, f(u) \rangle^2 \cdot \langle d, g(v) \rangle^2} \leq \max_u \frac{1}{\langle c, f(u) \rangle^2} \max_v \frac{1}{\langle d, g(v) \rangle^2} = \vartheta(G) \cdot \vartheta(H)$$

□

**Lemma 8.16.**  $\forall G : \Theta(G) \leq \vartheta(G)$ .

*Důkaz.*

$$\Theta(G) = \sup_k \sqrt[k]{\alpha(G^k)} \leq \sup_k \sqrt[k]{\vartheta(G^k)} \leq \sup_k \sqrt[k]{\vartheta^k(G)} = \vartheta(G)$$

□

**Věta 8.17 (Shannonova kapacita  $C_5$ ).**  $\Theta(C_5) = \sqrt{5}$ .

*Důkaz.* Víme  $\alpha(C_5^2) = 5 \Rightarrow \vartheta(C_5) \geq \sqrt{5}$ . Ukážeme  $\vartheta(C_5) \leq \sqrt{5}$ . Z toho

$$\sqrt{5} \leq \Theta(C_5) \leq \vartheta(C_5) \leq \sqrt{5}$$

Odkud platí i rovnost.

Pro důkaz staci uvážit ortonormalní reprezentaci  $C_5$  která se jmenuje Lovascovův destník.

□

## 9 Samoopravné a perfektní kódy, Lloydova věta

**Definice 9.1.** Necht  $A$  je konečná množina  $(abcda)$ ,  $q = |A|$ . Na množině slov  $w \in A^n$ ,  $|w| = n$  definujeme Hammingovu metriku jako počet písmen ve kterých se liší

$$d_H(x, y) = |\{i : x_i \neq y_i\}|$$

Libovolnou  $C \subseteq A^n$  nezyvame kódem délky  $n$  nad  $abcde$  o  $q$  symbolech.  $C$  opravuje  $t$  chyb, pokud

$$d_H(x, y) > 2t + 1$$



**Pozorování 9.2.** Pokud vezmeme graf všech slov délky  $n$ , hrany povedou mezi 2 slova které se liší přesně v 1 souřadnici. Pak grafová vzdálenost je právě Hammingova metrika. Na druhou stranu tento graf je  $n$ -ta kartézská mocnina grafu o  $q$  vrcholech.

Kód  $C$  opravuje  $t$  chyb  $\iff$  okolí kódových slov o poloměru  $t$  jsou po 2 disjunktní.

**Pozorování 9.3.** Kartézsky hrana  $\times$  hrana je □.

**Definice 9.4.**

$$\Gamma(n, q) = (A^n, \{xy : d_H(x, y) = 1\}) = K_q^n$$

**Poznámka 9.5.** Pokud kód  $C$  opravuje  $t$  chyb, pak

$$|C| \leq \frac{q^n}{\sum_{i=0}^t \binom{n}{i} (q-1)^i}$$

Vezmeme okolí bodu  $x$  poloměru  $t$ :

$$|N_\Gamma(x)| = 1 + n(q-1) + \dots =$$

Kde 1 je vrchol sam, pak máme  $n$  pozic na každé muze dojít k  $(q-1)$  chybám.

$$= \frac{q^n}{\sum_0^t \binom{n}{i} (q-1)^i}$$

binom odpovídá způsobem zvolit písmeno.  $(q-1)^i$  je počet chyb. Pak nerovnice pro velikost  $C$  je # všech slov deleno velikostí okolí.

**Definice 9.6.** Kod je  $t$ -perfektní, právě když  $|C| > 1$ ,  $C$  opravuje  $t$  chyb a nastává rovnost.

$$|C| = \frac{q^n}{\sum_0^t \binom{n}{i} (q-1)^i}$$

Celý graf je pokrytý okoli o poloměru  $t$ . Využívají beze zbytku celý graf (kodová slova).

**Poznámka 9.7.** Perfektní kódy skoro neexistují.

$t$	1	2	3	4	5	6	7	8	9
$q$									
2	H	—	G	—	—	—	—	—	—
3	H	G	—	—	—	—	—	—	—
$p^r$	H	—	—	—	—	—	—	—	—
$q$	?	?							

**Pozorování 9.8.** pro  $q = p^r$ ,  $C$  je  $t$ -perfektní kod delky  $n$ .

$$|C| = \frac{q^n}{\sum_0^t \binom{n}{i} (q-1)^i} \in \mathbb{Z}$$

Pak suma v jmenovateli dělí  $q^n = p^{rm}$ . Takže i suma je mocnina  $p$ . Dokážeme že suma se rovná  $q^l, l \in \mathbb{N}$ .

*Důkaz.*

$$\sum_0^t \binom{n}{i} (q-1)^i = q^a p^b = p^{ra+b}, 0 \leq b < r$$

Upravíme sumu

$$\begin{aligned} 1 + \sum_1^t \binom{n}{i} (q-1)^i &= p^{ra+b} \\ (q-1) \sum_1^t \binom{n}{i} (q-1)^{i-1} &= p^{ra+b} - 1 \\ \sum_1^t \binom{n}{i} (q-1)^{i-1} &= \frac{q^a p^b - 1}{q-1} = \frac{q^a p^b - p^b + p^b - 1}{q-1} = p^b \frac{q^a - 1}{q-1} + \frac{p^b - 1}{p^r - 1} \end{aligned}$$

Pak  $\frac{q^a - 1}{q-1} \in \mathbb{Z}$  jako součet geom rady. Druhý zlomek ale  $\in (0, 1)$ . Což dává dohromady celé číslo pouze  $b = 0$ .  $\square$

**Věta 9.9 (Hammingovy kody).** *Necht  $q = p^r$ . Pak 1-perfektní kod délky  $n$  nad abecedou o 1 symbolech existuje  $\iff n = \frac{q^k - 1}{q - 1}, k \in \mathbb{N}$ .  
Což dostaneme dosazením  $t = 1$  do rovnice minuleho pozorovají:*

$$1 + n(q - 1) = q^k \Rightarrow n = \frac{q^k - 1}{q - 1}$$

Necht  $C \subseteq \mathbb{Z}_q^n$ . Sestavíme matici  $H \in \mathbb{Z}_q^{k \times n}$  tak, aby sloupce byly po 2 lin. nezávislé. V každé sloupci můžeme vzít  $q^k$  symbolů. Nulový vektor používat nemůžeme. Dohromady  $(q^k - 1)$  vektorů. Vezmeme nějaký vektor, lineárně závislé s ním jsou jeho násobky skalarem kromě 0 -  $(q - 1)$ . Proto

$$n = \frac{q^k - 1}{q - 1}$$

Podíváme se na  $\text{Ker}(H) \subseteq \mathbb{Z}_q^n$ . Víme

$$\dim(\text{Ker}(H)) = n - \text{rank}(H) = n - k$$

Tvrdíme, že v jádru jsou vektory, které mají vzdálenost aspoň 3. Pokud by existovali vektory vzdálenosti 2. Jejich rozdíl  $\in \text{Ker}(H)$ . Dostali bychom vektor  $y$  který má nejvýše 2 nenulové souřadnice. Po vynásobení  $H y$  dostali bychom lin. kombinace 2 vektorů, které jsou dle volby lin. nezávislé.

$$|C| = q^{n-k} = \frac{q^n}{q^k} = \frac{q^n}{1 + n(q - 1)}$$

*Důkaz.* □

**Věta 9.10 (Prvocíselné perf. kody (BD)).** *pro  $q = p^r$  neexistují perfektní kódy jiných parametrů než Hammingovy, Golayovy (a opakovací kód s parametry  $q = 2, n = 2t + 1$ , který je považován za trivialní).*

**Věta 9.11 (Prvocíselné perf. kody  $t \geq 3$  (BD)).** *pro  $q = p^r$  neexistují žádné  $t$ -perfektní kódy opravující  $t \geq 3$  chyb.*

**Věta 9.12 (Lloyd).** *Pokud existuje  $t$ -perfektní kód délky  $n$  nad abecedou o  $q$  symbolech, pak polynom:*

$$L_t(x) = \sum_{j=0}^t (-1)^j (q - 1)^{t-j} \binom{x-1}{j} \binom{n-x}{t-j}$$

*ma  $t$  různých kladných celocíselných kořenů menších než  $n$ . Je to polynom stupně  $t$ .  
Myslenka důkazu: najdeme 2 kořeny od sebe vzdálené min. 1. Pak nemůžou být celocíselné.*

*Pro  $t = 1, 2$  umíme kořeny najít, takže Lloydova věta je příliš slabá.*

*Důkaz.* TODO předn 9 od 34:00 □

**Lemma 9.13.**

*Důkaz.* □