Aplikace lineární algebry v kombinatorice

prof. RNDr. Jan Kratochvíl, CSc.

4. března 2021

Obsah

1 Maticovy popis grafu, det, kostry

Věta 1.1 (Pocet sledu). *Pro kazdy graf G a každé přirozené číslo k obsahuje k-ta mocnina matice sousednosti A pocty sledu délky k mezi vrcholy grafu G, konkretně* $(A^k)_{a,b} = \#$ *sledu délky k mezi a - b v G.*

Důkaz. Indukci podle k.

1. k = 0, sledy délky 0, neboli $u - u$. Což odpovídá dle definice $A^0 = I$.
2. k = 1. Sled je pravě 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 pozice (w, b) je 1 pokud existuje taková hrana, jinak 0. Proto

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

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

□

Definice 1.2. $L_G^{(n)}$ se dostane tak, ze vyškrtneme n-ty řádek a sloupec z Laplaceove matice.

Lemma 1.3.

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

Důkaz. 1) Nechť $w \subseteq E$ je kostra. Pak je stromem $\Rightarrow$ má list v_1. Přemístíme řádek odpovídající v_1 do prvního řádku. Nechť e_1 je hrana $v_1 - v_t$. Dáme ji do prvního sloupce. Pak na pozice (0,0) je ± 1. Taky první řádek je $(\pm 1, 0, ...0)$ protože vrchol je list.
Odstraníme v_1, nechť v_2 je další list a e_2 jého hrana. Pak druhy řádek je $(??, \pm 1, 0, ...0)$. Tak pokračujeme dal.
Může se ale stát, ze další vrchol je u který jsme zrovna odstranili. Použijeme tvrzeni, ze strom má aspoň 2 listy. Pak můžeme vzít nějaký další vrchol. Po ukončení přemisťovaní dostaneme ± 1 na diagonále. Nad diagonálou same $0 \Rightarrow det = \pm 1$. Přemístěním jsme měnili znamenko 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 1.4 (Pocet koster). *$det(L_G^{(n)}) = \#$ koster grafu G.*

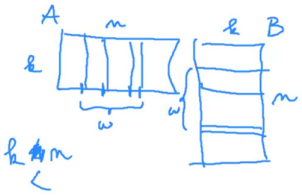
Důkaz. Vezmeme matice incidence I_G (jenom 2 jedničky ve sloupci, v řádku # 1 je $deg(v)$), v každém její sloupci nahradíme jednu jedničku hodnotou (-1). Výslednou matici označme D_G.
$I_G * I_G^T$ = skal. součin řádku i, j. Na diagonále $deg(v)$, mimo diag. 1 pro hrany, 0 - nehrany. Změníme pravě jednu 1ku ve každém sloupci na -1 (tím dostaneme orient. graf).

$$D_G * D_G^T = L_G$$

Rovnost platí protože skalární součin stejného řádku dá $deg(v)$ jelikož $-1 * -1 = 1$. Pokud násobíme různé řádky, příslušné vrcholy nejsou spojené hranou - 0. Jinak mají pravě 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-Benet vzoreček (det součiny obdelnikových matic)

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

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



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

Pro každou matici $detA = detA^T$, pak

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

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

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

Což je # koster G

□

2 Sudo-lichomesta, 2-vzdálenost množin bodu

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

$$det(S_1 + b_1, S_2 + b_2, ..., S_k + b_k) = det(S_1, S_2 + b_2, ..., S_K + b_K) + det(b_1, S_2 + b_2, ..., S_K + b_K)$$

Pak linearita v 2. složce atd.

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

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

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

Důkaz. Nechť A-matice incidence $\{A_i\}$. Radek odpovídá prvkům, sloupec - množinám. Na pozice $(r,s) = 1 \Rightarrow$ prvek r leží v množině A_s.
Vezmeme $A^T * A$ nad $\mathbb{R}$. Pak ve výsledné matice na pozice (r,s) je $|A_r \cap A_s|$. Jelikož průniky jsou 1-prvkové, máme matici 1-cek. Na diagonále jsou $|A_i|$ velikosti množin.

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

Tvrdíme, ze $det(A^T A \neq 0)$. Pak matice je regulární a $rank = k$.
BUNO

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

Máme matici, kde na diagonále jsou velikosti množin, jinak 1.
Nahledneme $a_2 \geq 2$. Jinak pokud $a_1 = a_2 \Rightarrow \exists x \in A_1 \cap A_2 \Rightarrow A_1 = A_2 = \{x\}$.
Nechť 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 zbývají det kde je jeden sloupec z S, zbytek z J.

$$det(S+J) = det(S) + \sum_{i}^{k} det(J^i S) =$$

Determinanty matic $J^i S$ kde z J je pouze i-ty 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 ≥ 0, druhy $\prod > 0$ protože od $i = 2, a_i \geq 2$. $\sum$ je zlomek kladných clenu, takže $\sum \geq 0$. Dohromady $det(J+S) > 0$

□

Věta 2.3 (sudo-lichomesta). *Nechť $A_1, ..., A_k$ jsou různé $\subseteq [n]$, $|A_i| = 1 \mod 2 \; \forall i, |A_i \cap A_j| \equiv 0 \mod 2, i \neq j \Rightarrow k \leq n$*

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

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

□

Definice 2.4. Množina bodu v $\mathbb{R}^n$ je s-vzdálenostní pokud vzájemně vzdálenostní bodu nabývají celkem nejvýše s hodnot.

Pozorování 2.5. 1-vzdálenostní množiny jsou simplexy. Zobecnění rovnostranného $\triangle$ do vyšších dimenzi. Indukci dokážeme, ze $m_1(n) = n+1$. Při přechodu do vyšší dimenze existuje pravě jeden bod který můžeme použit. Proces podobny kompaktizace topologického prostoru.

Věta 2.6 (2-vzdálenostni množ). *Nechť $m_s(n)$ značí počet bodu s-vzdálenostní 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 pravě 2 jedničky, jinak 0. Takových máme $\binom{n}{2}$.
Pokud 2 vektoru mají 1 společnou pozice, $d(x,y) = \sqrt{2}$. 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 nadrovině dimenzi $\mathbb{R}^n$ kterou lze vnořit do $\mathbb{R}^n$. Pak:

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

2) Horní odhad
Máme body $A_1, A_2, ..., A_t$. $A_i = (a_{i,1}, a_{i,2}, ..., a_{i,n}) \in \mathbb{R}^n$. Označme vzdálenosti $k \neq m \in \mathbb{R}$. Definujme funkce $F : \mathbb{R}^n \times \mathbb{R}^n \to R, F(x,y) = (d(x,y)^2 - m^2) * (d(x,y)^2 - k^2)$. Pokud je vzdálenost $m \vee k \Rightarrow F = 0$.
Pak $f_i(x) = F(x, A_i)$. Částečné dosazeni. Tyto funkce jsou v V.P. funkci z $\mathbb{R}^n$. Tvrdíme ze $\{f_i(x)\}$ jsou LN. Pokud dosadíme 2 různé prvky do f_i tak dostaneme 0 dle definice zobrazeni F. Pro stejný bod $f_i = a^2 b^2 \neq 0$.

$$\sum_1^t f_i * x_i = 0, x_i \in R, 0 = nulová\, funkce$$

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

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

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

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

f_i jsou polynomu stupně 4. # polynomu dle dimenze:

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

Funkce f_i jsou z podprostoru polynomu $deg = 4$. Zvolme vhodnou bázi.

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

Dostaneme $dim(U) = 1 + n(lin) + n(kv) + n(kv * lin) + \binom{n}{2}(lin2) + 1 = 2 + 3n + 1/2n(n-1) = 1/2(4+5+n^2)$. Generátor $\sum x_j^2$ nepotřebujeme protože je lin kombinaci x_j^2.

□

3 Sudo-sudomesta, Prostor cyklu grafu

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

Důkaz. Uděláme bijekci množina → charakteristicky vektor. Pak lin kombinace je taky sudo-sudomesto. Dal

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

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

Pak $\langle A_i, A_j \rangle = 0 \mod 2$. 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 maximální (vzhledem k inkluzi) systém tvořící sudo-sudomesto je nutně podprostor.

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

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

Odhad je těsný: spojíme body do 2-jic tvořící rozklad X. Pak množiny budou všechny možné podmnožiny obsahující 2ce. Je jich $2^{\lfloor n/2 \rfloor}$ □

Definice 3.2. Uvažme bijekci mezi napnutým podgrafem H a jého charakteristickým vektorem. Množina všech napnutých podgrafu ν_G tvoří V.P. nad $\mathbb{Z}_2$, sčítaní vektoru odpovídá symetrické diferenci množiny hran.

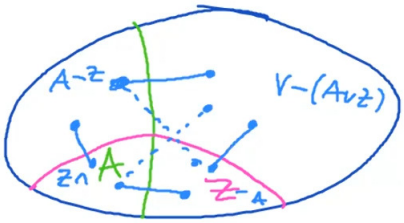
Definice 3.3. Množina napnutých podgrafu je Eulerovská pokud $\forall u \in V, deg(u) = 0 \mod 2$. Značíme ξ_G. Pak β_G je množina elementárních řezu, t.j. $B_A = (V, \{xy : x \in A, y \in V \setminus A, xy \in E\}), A \subseteq V$.

Věta 3.4 (Eulerovske grafy). *ξ_G, β_G jsou V.P. podprostory ν_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) Násobení skalárem je automaticky splněno, protože těleso je $\mathbb{Z}_2$.
2) $H_1 + H_2 = (V_1, E(H_1) \div E(H_2))$. Taky 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 $deg_{H_1} u = 2k, deg_{H_2} u = 2l$, taky h je počet společných hran obou podgrafu.

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

Součet 2 Eulerovských grafu je Eulerovsky graf.
4) Ukážeme $\forall A, Z \subseteq V(G) : B_A + B_Z \in \beta_G$.



Z obrázku přežijou pouze hrany vědoucí 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 řezích. Zůstane rez $B_{A \div Z}, A \div Z = (A - Z) \cup (Z - A)$.

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

Tvrdíme ze $B_G = \langle B_{\{u\}}, u \in V \rangle$. Prostor elementárních řezu je generovaný hvězdami. Protože

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

Hrany uvnitř A se smažou symetrickou diferenci, hrany vědoucí ven z A, které nejsou společné zůstanou.
5) G souvislý $\Rightarrow dim B_G = |V| - 1$. Náhledneme ze sečtení všech hvězd dává $\emptyset$ graf. Neboli každá hrana patří ke 2 hvězdám.
Zafixujeme vrchol u, sečteme 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 generuji všechny řezy. Z toho $\Rightarrow dim B_G = |V| - 1$.
Pozorovaní:

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

Uvažme hvězdu $B_{\{u\}}$ a $deg_H u = 0 \mod 2$. Pak symetrická diference smaže přávě sudy počet hran z hvězdy a nově počet hran je taky sudy.

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

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

□

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 Eulerovske podgrafy). $\forall G \exists V_1 \dot\cup V_2 = V(G), G[V_i]$ *je Eulerovsky.*

Důkaz. Uvažme $M = \xi_G$ v tvrzeni z lemmatu. $\bar{1} = G$, má 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 dizjunktní, takže máme 2 Eulerovské podgrafy a mezi nimi elementární rez. Pokud rez smažeme, graf je sjednoceni dvou Eulerovských podgrafu.

□

4 Seiduv switching

Definice 4.1. Nechť V je V.P nad T. Lineární forma je lineární zobrazeni $f : V \to T$. Pak lineární formy tvoří V.P. nad T. Značíme V^* a je tzv. duální prostor k V.

Definice 4.2. Nechť $B = \{b_1, b_2, ..., b_n\}$ je báze V, pak $B^* = \{f_1, f_2, ..., f_n\}$ je duální báze, pokud formy jsou dáne předpisem:

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

Definice 4.3. Nechť A,B jsou V.P nad T, $dimA = n, dimB = k$. Nechť $\varphi : A \to B$ homomorf. Pak duální homomorf k φ je zobrazeni $\varphi^* : B^* \to A^*$ dáne předpisem:

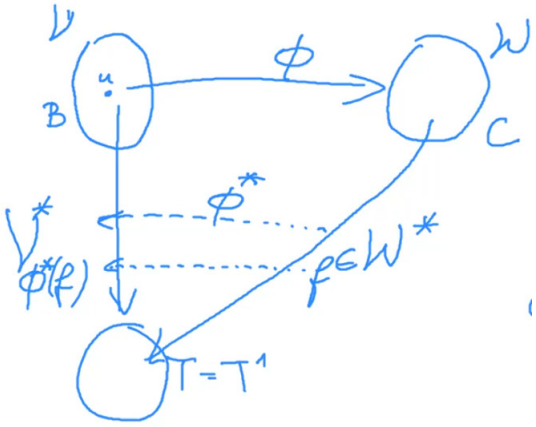
$$\forall f \in B^* \ \forall u \in A : (\varphi^*(f))(u) = f(\varphi(u))$$

Věta 4.4 (Matice duálního homomorf(BD)). *Matice duálního homomorf vzhledem k duálním bázím je transponovanou matici k matici primárního homomorf.*

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

Důkaz. Matice zobrazeni lineární formy z prostoru $f : V \to T$ je

$$_B[f]_k = (f(b_1), f(b_2), ..., f(b_n))$$



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

Duální homomorf $\phi^* : W^* \to V^*$ je definován:

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

Jelikož lineární formy jsou n-tice, tak $dim(V) = dim(V^*)$.
Matice ϕ je ${}_B[\phi]_C \in T^{k\times n}$. Matice ϕ^* je ${}_{C^*}[\phi^*]_{B^*} \in T^{n\times k}$.
Veta říká, ze

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

□

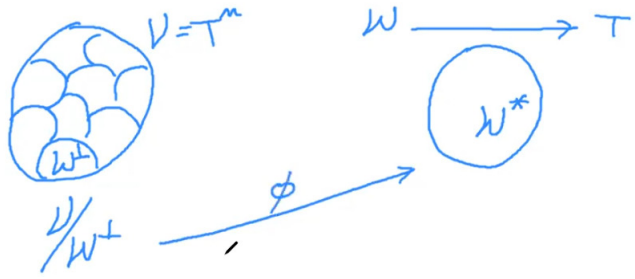
Definice 4.5. Faktorprostor: faktorizace dle podprostoru W prostoru V (podgrupa). V/W jsou množiny $\forall u \in V u + W$. Pak i faktorprostor je V.P vůči operacím:

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

Platí: $dim(V/W) = dimV - dimW$.

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

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



Důkaz.
Pak izomorfizm ϕ je definován:

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

Udělali jsme lineární formu z bilineární??
Pokud dosadíme proměnnou:

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

Chceme aby ϕ bylo korektně definované a splňovalo vlastnosti izomorfuzmu:
1) korektnost definice
2) lineární zobrazeni
3) proste
4) na
Důkaz:
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) Skalární součin je bilineární forma, z toho ϕ je lineární zobrazeni.
3) Nechť $\phi(v+W^\perp) = 0 \Rightarrow \forall x \in W : \langle v, x\rangle = 0 \Rightarrow v \in W^\perp \Rightarrow v+W^\perp = \bar{0}+W^\perp$. Takže v kernelu je pouze $W^\perp$.

4) Nahledneme z dimenzi.

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

Rovnost dimenzi platí protože zobrazeni je prosté.

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

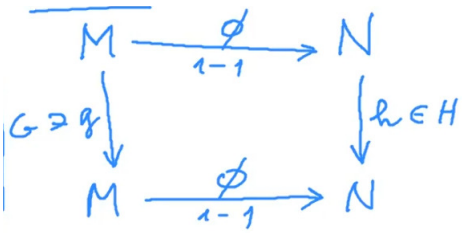
Z LA $Im(\phi)$ je vnořený podprostor stejné dimenzi jako nadprostor $\Rightarrow$ jsou stejné.

□

Věta 4.7 (Burnsidovo lemma(BD)).

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

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



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

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

Pak

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

Diagram komutuje

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

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

Definice 4.9. Seiduv switching vymění všechny hrany a nehrany vycházející z $u \in V$. Ostatní vrcholy a hrany beze změn. Grafy $G \sim G' \iff G'$ lze získat z G postupným přepinaním vrcholu.

Poznámka 4.10.

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

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

Poznámka 4.11. Dva grafy na stejné množině vrcholu jsou Seidelovsky ekvivalentní $\iff$ jsou ve stejné třídě faktorizace V_{K_V}/β_{K_V}. Proto je tříd ekvivalence tolik, kolik je Eulerovských grafu na dáne množině vrcholu.

Věta 4.12 (Pocet neiz trid Seide switching). *Počet neizomorfních tříd ekvivalence při Seidelově switchingu na n vrcholech je roven počtu Eulerovských grafů na n vrcholech.*

Důkaz. Pro lichá n, označme

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

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:

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

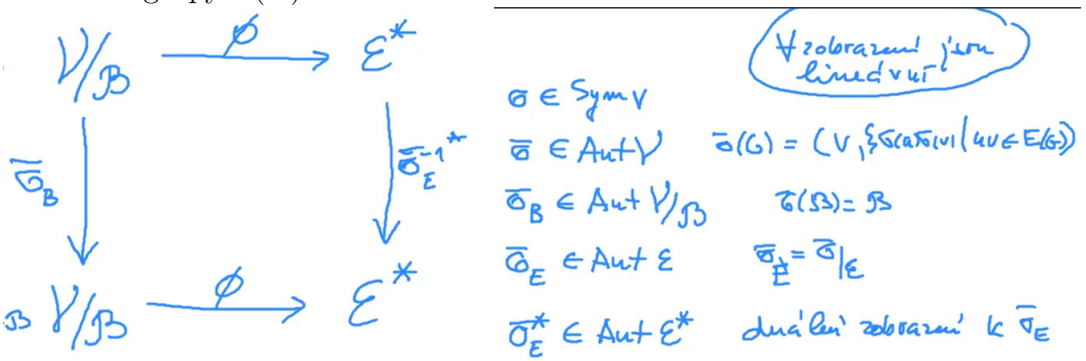
Vezmeme vrchol $u \in A, deg_G(u) = c + d$, kde c jsou hrany v A, d hrany mimo A.
Po switchu:

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

Kde $(c + d)$ je liché, $|V|$ je liché, $|A|$ je sude. Dohromady sude.
Takže kazdy graf lze přeswitchovat na Eulerovský graf. Přeswitcheni Eulerovského grafu se změní na neeulerovský. V každém switching třídě je 1 Eulerovský graf.
Pro n sude. Nechť ν. je V.P. všech grafu na dáne množině vrcholu, B je prostor elementárních řezu na uplném grafu, ξ prostor Eulerovských grafu.

$$\beta = \xi^{\perp} \Rightarrow \xi^* \simeq \nu / B$$

Prvky ν/B jsou právě třídy ekvivalence dle Seidelovem switchingu. Chceme zjistit počet orbit akci grupy $S(V)$.



Tvrdíme ze diagram komutuje. Nechť $G \in \nu$

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

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

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

□

5 Spekrum grafu, Moorovy grafy

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

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

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

Důkaz. 1) r = 1, cesta délky 2
2) r = 2, kružnice délky 5
3) r = 3 Petersenuv graf
4) r = 7 Hofman, Singleton graf
Ostatní r, nechť G je Mooruv graf, na $n = r^2+1$ vrcholech. Vezmeme matice sousednosti. A^2 má počet sledu délky 2 mezi vrcholu $a-b$. 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 $\lambda \in Sp(A) \Rightarrow \lambda^2 + \lambda - (r-1) \in Sp(A^2) = Sp(J)$.
J má $(n-1)$ násobné vlastní číslo $\lambda = 0$. Poslední vlastní číslo je n. Pak

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

r-regulární graf má největší vlastní 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 $m_1 + m_2 = n - 1 = r^2$. Taky

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

Vyřešíme systém 2 rovnic o 2 neznámých. Nechť

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

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

1) Nechť $s \notin Q \Rightarrow s/2 \notin Q \wedge r \in N \Rightarrow m_1 = m_2 \Rightarrow r^2 - 2r = 0 \Rightarrow r = 2$. 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: $24 - 9 - s^4 + (...)s = 0$.

$$s^4 + s(...) - 15 = 0 \Rightarrow s|15 \Rightarrow s = \{1,3,5,15\} \Rightarrow r = \{1,3,7,57\}$$

□

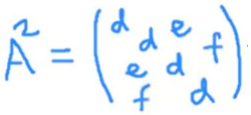
6 Silne regulární grafy, propletani vl cisel

Definice 6.1. Silně regulární je graf pokud není uplný (triviální případ) a $\exists d, e, f \in \mathbb{N}$: $\forall v \in V\ deg(v) = d$. Každé 2 sousední vrcholy mají e společných sousedu (2 vrcholy leží v $e\triangle$), každé 2 nesousední vrcholy mají f společných sousedu ($\exists f$ cest délky 2).

Věta 6.2 (Silne regulární grafy (nebude u zkousky)). *Je-li G silné regulární s parametry d, e, f, pak nastává jedna z 2 možností:*

- $f = e+1, d = 2f, |V(G)| = 2d+1$ *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. Nechť A je matice sousednosti G, $n = |V(G)|$, uvažme A^2. Na diagonále jsou stupně d, mimo diagonálu pokud v A byla 1 - změní se na e, 0 se změní na f.



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

Dosadíme vlastní číslo $\lambda \in Sp(A)$.

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

d odpovídá vlastnímu vektoru $\bar{1}$ u A, u J vlastnímu vektoru $\bar{1}$ odpovídá n. Dosadíme d:

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

Zafixujme nějaký vrchol $x \in V$. Kolik $\exists$ indukovaných cest délky 2:

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

Máme d způsobu zvolit souseda x, pak vrchol a má d sousedu, e jsou společné s x, x taky patří mezi sousedy. Dostaneme $d(d-e-1)$. Na druhou stranu z pohledu vrcholu b. X má $(n-d-1)$ nesousedu, pak vrchol a je mezi f sousedu (x,b). Dostaneme $f(n-d-1)$.
Pro $\lambda \in Sp(A) \setminus \{d\}$ zbývá 0:

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

Označme $D = \sqrt{(e-f)^2 - 4(f-d)}$. Pak $\lambda_1 = 1/2(e-f+s), p$ krát a $\lambda_2 = 1/2(e-f-s), q$ krát.
Z násobnosti vlastních čísel

$$1 + p + q = n$$
$$a + p\lambda_1 + q\lambda_2 = tr(A) = 0$$
$$tr(A^2) = \sum \lambda_i^2 = nd \Rightarrow d^2 + p\lambda_1^2 + q\lambda_2^2 = nd$$

Vyřešíme soustavu 3 rovnic o 3 neznámých. Dosadíme hodnoty λ_1, λ_2 do 2. rovnice:

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

Nastávaji 2 případy:
1) $s \notin \mathbb{Q} \Rightarrow$ poslední sčítanec je iracionální a nutně $p = q = 1/2(n-1)$.

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

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 definici. Jinak

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

Pracujme s 3. rovnici:

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

dosadíme $(e-f) = -1$.

$$\begin{aligned} d^2 + 1/2(n-1) * 1/4(s-1)^2 + 1/2(n-1) * 1/4(-1-s)^2 &= nd \\ 8d^2 + (n-1)(s^2 - 2s + 1) + (n-1)(s^2 + 2s + 1) &= 8nd \\ 8d^2 + (n-1)(s^2 - 2s + 1 + s^2 + 2s + 1) &= 8nd \\ 8d^2 + (n-1)(2s^2 + 2) &= 8nd \\ 4d^2 + (n-1)(s^2 + 1) &= 4nd \end{aligned}$$

Dosadíme $n = 2d-1$

$$\begin{aligned} 4d^2 + 2d(s^2+1) &= 4(2d+1)d \\ 2d + (s^2+1) &= 2(2d+1) \end{aligned}$$

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

$$\begin{aligned} 2d + 2 + 4d - 4f &= 4d + 2 \\ 2d &= 4f \Rightarrow d = 2f \end{aligned}$$

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

$$\begin{aligned} d + 1/2p(e-d+s) + 1/2q(e-f-s) &= 0 \\ d^2 + 1/2(n-1) * 1/4(e-f+s)^2 + 1/2(n-1) * 1/4(e-f-s)^2 &= (1+q+p)d \end{aligned}$$

Zbavíme se jmenovatele a roznásobíme kvadráty v 3.

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

Spočítáme p, q pomoci determinantu.

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

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...

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

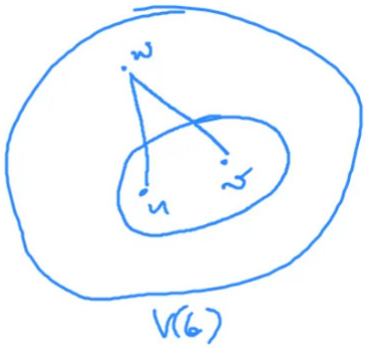
□

Věta 6.3 (Friendship theorem). *Nechť v grafu G mají každé 2 různé vrcholy právě 1 společného souseda. Pak G obsahuje vrchol, který sousedi se všemi ostatní vrcholy grafu.*

Důkaz. Pokud platí $e=f=1\Rightarrow\exists v\in V$ který sousedi se všemi ostatní vrcholy.
Nechť $N_G(u)$ je množina sousedu $u\in V$. 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

$$\begin{aligned}\forall a|N_G(a)|=m+1=deg(a)\\n=|V(G)|=m^2+m+1\end{aligned}$$

Z čehož G je silné regulární s parametry $d=m+1\wedge e=f=1$. První případ nastat nemůže kvůli podmínce 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

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

Případ $t = 1 \Rightarrow m = 1$ není zajímavý protože KPR radu 1 je $\triangle$.
2) 3. axiom neplatí $\Rightarrow \{N_G\}$ z teorie KPR bud všechno leží na 1 přímce nebo jeden vrchol samostatně a zbytek na přímce. Pak ten samostatný vrchol je hledaný soused všech:

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

□

Věta 6.4 (vl čísla Hermitovske matice(BD)). *Nechť $A \in \mathbb{C}^{n\times n}$ je Hermitovska, $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n$ její vlastní čísla. Nechť $b_1, b_2, ..., b_n \in \mathbb{C}^n$ je ortonormální báze z vlastních vektoru. Pak pro $k = 1, 2, ..., n$ platí*

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

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

Věta 6.5 (Propletani vl cisel). *Nechť $A \in \mathbb{C}^{n\times n}$ je Hermitovska, $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n$ její vlastní čísla. Nechť B je hlavni podmatice radu $k \times k$ (vznikne vynecháním $(n-k)$ řádky), Nechť $b_1, b_2, ..., b_n \in \mathbb{C}^n$ jsou vlastní čísla matice B. Pak platí*

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

Důkaz. Nejprve se podíváme na případ vynechaní i-ho řádku. Nechť B má ortonormální báze $y_1, y_2, ..., y_{n-1} \in \mathbb{C}^{n-1}$. Vnoříme tyto vektory do $\mathbb{C}^n$ tak, ze na pozici $i-1$ vložíme 0. Označíme je $z(y)$. Pak

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

Uvažme 3 množiny, j je libovolné

$$S_1 = \langle\{x_j, x_{j+1}, ..., x_n\}\rangle$$
$$S_2 = \langle\{y_1, y_2, ..., y_j\}\rangle$$
$$S_3 = \{z(y) : y \in S_2\}$$
$$dim S_1 = n - j + 1$$
$$dim S_3 = dim S_2 = j$$
$$dim S_1 + dim S_3 = n + 1 > dim(S_1 + S_2)$$

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

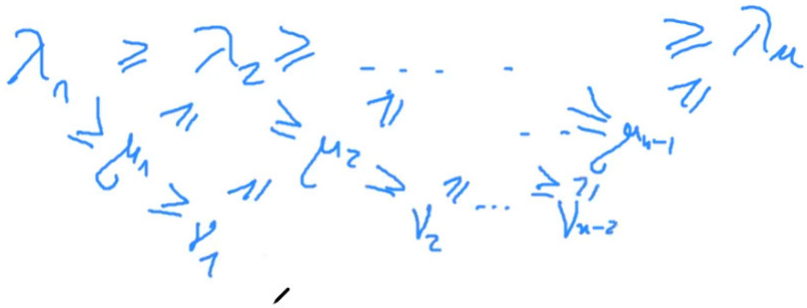
$$l \in S_1 \Rightarrow l^*Al \geq \lambda_j l^* l$$
$$l \in S_3, y \in S_2, l = z(y) : l^*Al = y^*By \geq b_j yy^* = b_j l^* l \leq \lambda_j l^* l$$
$$\lambda_j l^* l \geq b_j l^* l \ \Rightarrow \lambda_j \geq b_j$$

Teď dokážeme $b_j \geq \lambda_{j+1}$

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

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

Teď pro obecně k.



Z obrázku

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

□

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

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

Důkaz. Nechť $W \subseteq V(G)$ je nezávislá množina velkosti α. Matice sousednosti teto množiny je nulová $\alpha \times \alpha$. Taky je to hlavní podmatice A_G. Proto její vlastní čísla (nuly) propletaji vlastní čísla G. Z toho

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

□

7 Odhady pomoci spektra

Věta 7.1 (Propletani A). *Nechť $A \in \mathbb{C}^{n\times n}$ Hermitovská. $S \in \mathbb{C}^{m\times n}$ taková, ze $S^*S = I$. Potom vlastní čísla S^*AS propletáji vlastní čísla matice A.*

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

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

Pak $RR^* = I$ a

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

Pak SAS^* je hlavni podmatice RAR^*, a vlastní čísla SAS^* propletaji vlastní čísla RAR^*. Přitom $Sp(RAR^*) = Sp(A)$ z LA, protože matice jsou podobné. □

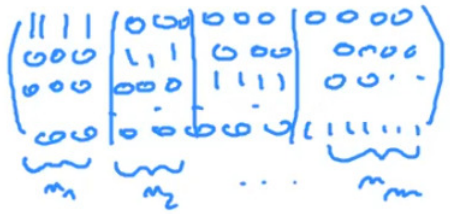
Věta 7.2 (Propletani B). *Nechť:*

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

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

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

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



Potom PP^T je diagonální matice D protože jedničky jsou na různých pozicích. Skalární součin dvou různých řádku je 0. Na diagonále je norma i-ho řádku $= n_i$.
Použijeme matici P abychom dostali řádkové součty matici A:
V matici PA dostaneme sloupcový součet po blocích. Pak v matici PAP^T dostaneme součty všech prvku v blocích.
Pro rovnost s matici B ještě potřebujeme vydělit n_i. Na což použijeme D^{-1} která má na diagonále $\frac{1}{n_i}$.

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

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

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

Dle Vety o propletani A 7.1, vlastní čísla SAS^T propletaji vlastní 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 stejný spektrum.

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

□

Věta 7.3 (Nezav množ v d-regulárním). *Nechť G je d-regulární graf o n vrcholech s vlastní čísly $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n\}$. Pak*

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

Důkaz. Nechť A je matice sousednosti grafu G.

$$Sp(A) = \{\lambda_1 = d \geq \lambda_2 \geq ... \geq \lambda_n\}$$
$$Sp(J) = \{n, 0^{n-1}\}$$

Matice A, J komutuji $\Rightarrow$ mají společnou ortonormální báze.

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

Kde Λ_A je diagonální matice s vlastní čísly na diagonále, rozmístěné dle uspořádaní. Podobně pro J:

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

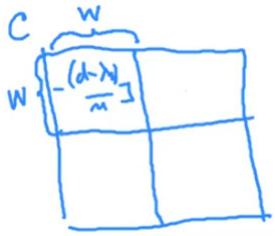
Z věty o ortonormální bázi vlastní vektor příslušný největšímu vlastnímu číslu je nezáporný. Ostatní mají záporné složky. Pak vektor $\bar{1}$ je příslušný největšímu vlastnímu číslu A - d. Taky odpovídá vlastnímu číslu n matice J.
Uvažme matici:

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

Její vlastní čísla jsou lineární kombinace vlastních čísel A, J.

$$X^*CX = X^*(A - \frac{1}{n}(d-\lambda_n)J)X = X^*AX - \frac{1}{n}(d-\lambda_n)X^*JX = \Lambda_A - \Lambda_K = \Lambda_C$$

Kde $(\Lambda_K)_{1,1} = d-\lambda_n$, jinak 0. Z toho Λ_C má na diagonále $\{\lambda_n, \lambda_2, ..., \lambda_n\}$. Odtud λ_n je největší vlastní číslo matice C.
Nechť $W \subseteq V(G)$ je nezávislá množina G, $|W| = \alpha(G)$. Pak matice A, po seskupeni řádku odpovídajících W, má nulovou hlavni podmatice odpovídající W. Z toho matice C má na těchto pozicích $-\frac{1}{n}(d-\lambda_n)$. Taky je to hlavni podmatice.



Vlastní čísla matice $-\frac{1}{n}(d-\lambda_n)J$ propletaji vlastní čísla matice C.

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

Z vety o propletaní:

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

□

Důsledek 7.4. *Nechť G je d-regulární graf o n vrcholech s vlastní čísly $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n\}$. Pak*

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

Plyne z toho, ze $\chi(G) \geq \frac{n}{\alpha(G)}$. Barveni grafu je rozložení ne $\chi(G)$ nezávislých množin. Kazda z nich má velikost $\chi(G)/\alpha(G)$. Kombinaci dvou nerovnosti dostaneme tvrzeni.

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

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

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

Důkaz. 1) Nerovnost $\Delta(G) \geq \lambda_1$. Doplníme G na Δ-regulární graf H tak, aby G byl jeho indukovaný podgraf. Pak vlastní čísla G propletaji vlastní 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 průměrných řádkových součtu je $B = deg_{avg}(G)$ jednoprvková. Dle Vety o propletaní B 7.2, $Sp(B) = \{deg_{avg}(G)\}$ propleta spektrum A $\Rightarrow \lambda_1 \geq deg_{avg}(G)$. □

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

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

Důkaz. Nechť H je χ-kriticky indukovaný podgraf grafu G. Minimální stupeň vrcholu v χ-kritickém grafu je aspoň $\chi - 1$. Označme jeho největší vlastní číslo jako h_1. Z vety o propletaní plyne $\lambda_1 \geq h_1$. Z vety poloměru spektra 7.5 dostáváme

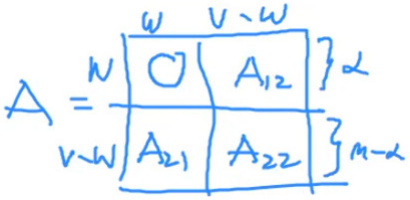
$$h_1 \geq deg_{avg}(H) \geq \delta(H) \geq \chi - 1 \Rightarrow \lambda_1 \geq \chi - 1$$

□

Věta 7.7 (Nezav množ v libovolnem grafu). *Nechť G je graf o n vrcholech s vlastní čísly $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n\}$. Pak*

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

Důkaz. Nechť $W \subseteq V(G)$ je nezávislá množina G, $|W| = \alpha(G)$. Rozdělíme matice A dle W a $V \setminus W$.



Použijeme Vetu o propletaní B 7.2.

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

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

Dal víme, ze počet hran mezi W a $v \setminus W$ se rovna

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

Z LA součin vlastních čísel je determinant:

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

Z propletaní:

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

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

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

□

Věta 7.8 (Barevnost souvislého grafu). *Nechť G je souvislý graf o n vrcholech s vlastnímu čísly $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n\}$. Pak*

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

Veta je analogická důsledku vety 1, zesiluje ji pro souvisle grafy.

Důkaz. Obarvíme graf pomoci χ barev. Nechť x je reálný vlastní vektor příslušný vlastnímu číslu λ_1 (Existuje dle Frobeniove vety). Ze souvislosti $x_i > 0 \forall i$.
Sestavíme matici $P \in \mathbb{R}^{\chi \times n}$.

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

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

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

Dle Vety o propletaní A 7.1, vlastní čísla SAS^T propletaji vlastní čísla A. Nechť vlastní čísla SAS^T jsou $\{h_1, h_2, ..., h_\chi\}$. Má na diagonále samé nuly, z toho

$$\sum_0^\chi h_i = 0$$

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 odpovídá nenulovému reálnému vlastnímu vektoru, takže $\lambda_1 = h_1$. Použijeme propletani

$$h_1 = \lambda_1 \geq h_2 \geq ... \geq h_\chi \geq \lambda_n \wedge \sum h_i = 0 \Rightarrow -\lambda_1 = h_1 = -\sum_2^\chi h_i$$

Použijeme horní odhad pro součet přes # sčítanců krát min hodnota (λ_n).

$$-\lambda_1 = h_1 = -\sum_2^\chi h_i \geq (\chi - 1)(-\lambda_n)$$

Po upravě

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

□

8 Shannonova kapacita

Definice 8.1. Nechť A je abeceda, $A = \{a, e, o, h, g\}$. Pak sestavíme graf $G_A = (A, \{xy | x \sim y\})$. Kde ekvivalence znamená, že x je snadno zamění za y.

Pak by šlo vzít nezávislou množinu a používat jen tyto symboly. Zbylo by hodně málo symbolu.
Lepe - dohodneme se na pevné délce. Vezmeme $C \subseteq A^n$. Pak bezpečný kod bude používat pouze slova z C. Dal sestavíme G_{A^n} graf zaměnitelnosti pro A^n.

Pozorování 8.2. 2 slova jsou zaměnitelná $\iff$ mají na i-te pozice stejné písmeno nebo zaměnitelné. Přesné odpovídá uplnému součinu grafu.

Definice 8.3. Pro grafy G, H definujme uplný součin 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 $G^n = G \boxtimes G \boxtimes ... \boxtimes G$.

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

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

Pozorování 8.6. Nechť $\sigma(G) = \chi(-G)$. Což je minimální počet uplných podgrafu pokrývajících množ grafu. Pak

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

Protože $K_n \boxtimes K_m = K_{mn}$. Součin uplných je uplný graf, jiná možnost není (jsou tam všechny hrany).Takže

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

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 ortonormální reprezentace grafu je zobrazeni $f : V \to \mathbb{R}^d$ 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 vzájemné $\perp$ vektoru velikosti $V(G)$, neboli prostor dimenze $V(G)$.
Pro uplný 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 reprezentace najít takový jednotkový vektor c, který minimalizuje hodnotu $\langle c, f(u)\rangle^2$.

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

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

Definice 8.12. *Rukojeť* reprezentace f je vektor c (jednotkový vektor), pro který f nabývá minima. Infimum v def velikosti ortonormální reprezentace se nabývá, protože $f = f(c)$ je spojitá a zdola omezena.
V definici stačí uvazovat omezenou dimenzi, např $d \leq |V(G)|$.
Infimum v def dzeta funkce se taky nabývá, protože $||f||$ je spojitá funkce f. Pak

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

Úmluva 8.13. Může se stát, ze rukojeť je vektor kolmý na nějaký z vektoru f. Pak $\vartheta(G) = \infty$. Budeme se ale takovým rukojetím vyhýbat. Všechny vektory reprezentace leží v nadrovině, je jich konečně mnoho.

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

Důkaz. Nechť G je graf, a máme optimální reprezentace f s rukojeti c. $||f|| = \vartheta(G)$. Taky $W \subseteq V(G)$ je nezávislá množina:

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

Vektory reprezentující W jsou na sebe kolmé. Můžeme je doplnit na ortonormální báze B prostoru $\mathbb{R}^d$. Pak rukojeť můžeme napsat jako lineární kombinace pomoci vektoru z B:

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

Dal c je jednotkový vektor:

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

vektory u, v jsou z ortonormální báze, takže pro $u \neq v$ je součet nula, jinak místo posledního skalárního součinu tam bude 1. Pak dostaneme součet vlevo, který je větší než suma pro vektory reprezentace nezávislé množiny.

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

Nahledneme že velikost skalárního součinu je omezena maximumem pro všechny vrcholy, což je právě $\vartheta(G)$.

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

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

Sčítáme 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. Nechť f je optimální ortonormální reprezentace G s rukojeti c. Podobně g pro H s rukojeti d. Uvažme tenzorový součin $f \circ g$ jako ortonormální reprezentace součinu grafu.

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

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 bud jeden skalární součin je 0 nebo druhy z volby vrcholu. Takže

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

Pak rukojeť 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 funkci je menší než součin max dvou funkci:

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

□

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 stačí uvážit ortonormální reprezentaci C_5 která se jmenuje Lovascovuv deštník.
□

9 Samoopravné a perfektní kody, Lloydova veta

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

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

Libovolnou $C \subseteq A^n$ nazýváme kodem délky n nad abecedou 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 souřadnice. Pak grafová vzdálenost je právě Hammingova metrika. Na druhou stranu tento graf je n-ta kartezská mocnina grafu o q vrcholech.
Kod C opravuje t chyb $\iff$ okolí kodových slov o poloměru t jsou po 2 dizjunktní.

Pozorování 9.3. Kartezský 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 kod C opravuje t chyb, pak

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

Vezmeme okolí bodu x poloměru t:

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

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

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

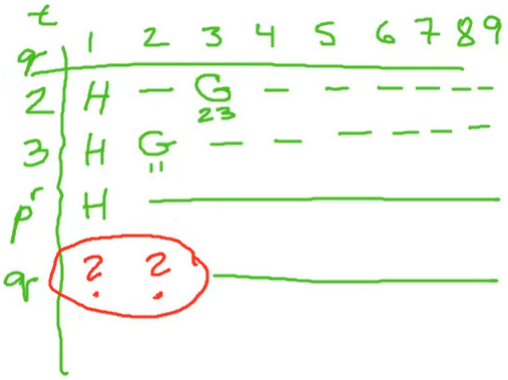
binom odpovídá způsobům zvolit písmeno. $(q-1)^i$ je počet chyb.
Pak nerovnice pro velikost C je # všech slov děleno velikosti okolí.

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

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

Cely graf je pokryty okolí o poloměru t. Využívají beze zbytku cely graf (kodova slova).

Poznámka 9.7. Perfektní kody skoro neexistuji.



Pozorování 9.8. pro $q = p^r$, C je t-perfektní kod délky 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 ze suma se rovna $q^l, l \in \mathbb{N}$.

Důkaz.

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

Upravíme sumu

$$1+\sum_1^t \binom{n}{i}(q-1)^i = p^{ra+b}$$

$$(q-1)\sum_1^t \binom{n}{i}(q-1)^{i-1} = p^{ra+b}-1$$

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

Pak $\frac{q^a-1}{q-1} \in \mathbb{Z}$ jako součet geometrické rady. Druhy zlomek ale $\in (0,1)$. Což dává dohromady cele číslo pouze $b=0$. □

Věta 9.9 (Hammingovy kody). *Nechť $q=p^r$. 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 minulého pozorovaní:

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

Důkaz. Nechť $C \subseteq \mathbb{Z}_q^n$. Sestavíme matici $H \in \mathbb{Z}_q^{k\times n}$ tak, aby sloupce byly po 2 lineárně nezávislé.
V každé složce můžeme vzít q^k symbolu. Nulový vektor používat nemůžeme. Dohromady (q^k-1) vektoru. Vezmeme nějaký vektor, lineárně závislé s nim jsou jeho násobky skalárem kromě 0 - $(q-1)$. Proto

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

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

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

Tvrdíme, ze v jádru jsou vektory které mají vzdálenost aspoň 3. Pokud by existovali vektory vzdálenosti 2. Jejich rozdíl $\in Ker(H)$. Dostali bychom vektor y který má nejvýše 2 nenulové souřadnice. Po vynásobení Hy dostali bychom lineární kombinace 2 vektoru které jsou dle volby lineárně nezávislé.

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

□

Věta 9.10 (Prvociselne perf. kody(BD)). *Pro $q=p^r$ neexistuji perfektní kody jiných parametru než Hammingovy, Golayovy (a opakovací kod s parametry $q=2, n=2t+1$, který je považován za triviální).*

Věta 9.11 (Prvociselne perf. kody $t \geq 3$ (BD)). *Pro $q=p^r$ neexistuji žádné t-perfektní kody opravující $t \geq 3$ chyb.*

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

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

má t různých kladných celočíselných kořenu menších než n. Je to polynom stupně t.
Myšlenka důkazu: najdeme 2 kořeny od sebe vzdálené min než 1. Pak nemůžou byt celočíselné.
Pro $t = 1, 2$ umíme kořeny najít, takže Lloydova veta je příliš slabá.

Důkaz. TODO předn 9 od 34:00 □