Aplikace lineární algebry v kombinatorice

prof. RNDr. Jan Kratochvíl, CSc.

7. února 2021

Obsah

1 Maticovy popis grafu, det, kostry

Definice 1.1. Matice sousednosti grafu G

Věta 1.2 (Pocet sledu). *Pro kazdy graf G a kazde prirozene cislo k obsahuje k-ta mocnina matice sousednosti A pocty sledu delky k mezi vrcholy grafu G, konkretne* $(A^k)_{a,b} = \#$ *sledu delky k mezi a - b v G.*

Důkaz. Indukci podle k.

1. k = 0, sledy delky 0, neboli $u-u$. Coz odpovida dle definice $A^0 = I$.
2. k = 1. Sled je prave hrana.
3. indukcni 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 takova hrana, jinak 0. Proto

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

   Dle I.P. se rovna poctu sledu delky k mezi $a-w$. Pak mezi vrcholy $a-w$ existuje sled delky k. Rozdelime sledy dle konecneho vrcholu, ktery je soused b. Kazdy z techto sledu jednoznacne prodlouzime na sled delky $(k+1)$ do vrcholu b. Z toho predchozi soucet je prave # pocet sledu delky $(k+1)$ mezi $a-b$.

□

Definice 1.3. $L_G^{(n)}$ se dostane tak, ze vyskrtneme n-ty radek a slopec z Laplaceove matice.

Lemma 1.4.

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

Důkaz. 1) Necht $w \subseteq E$ je kostra. Pak je stromem $\Rightarrow$ ma list v_1. Premistime radek odpovidajiici v_1 do prvniho radku. Necht e_1 je hrana $v_1 - v_t$. Dame ji do prvniho sloupce. Pak na pozice (0,0) je ± 1. Taky prvni radek je $(\pm 1, 0, ...0)$ protoze vrhol je list.
Odtranime v_1, necht v_2 je dalsi list a e_2 jeho hrana. Pak druhy radek je $(??, \pm 1, 0, ...0)$. Tak pokracujeme dal.
Muze se ale stat, ze dalsi vrhol je u ktery jsme zrovna odstranili. Pouzijeme tvrzeni, ze strom ma aspon 2 listy. Pak muzeme vzit nejaky dalsi vrhol. Po ukonceni premistovani dostaneme ± 1 na diagonale. Nad diagonalou same 0 $\Rightarrow det = \pm 1$. Premistenim jsme menili znamenko det. Ale $det^2 = 1$.
2) Mame graf $w \subseteq E, |w| = |V| - 1$ ktery neni strom $\Rightarrow$ neni souvisly $\Rightarrow$ ma aspon 2 komponenty souvislosti. $V = V_1 \dot\cup V_2$. BUNO $u \in V_2$. Pak z V_1 do V_2 nevede zadna hrana, cast matice je 0. Pak soucet radku odpovidajici $V_1, E(V_2)$ a $V_2, E(V_1)$ je 0 $\Rightarrow$ rakdy jsou LZ a det je 0.

□

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

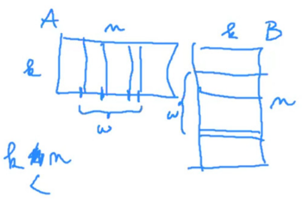
Důkaz. Vezmeme matice incidence I_G (jenom 2 jednicky ve sloupci, v radku # 1 je $deg(v)$), v kazdem jejim sloupci nahradime jednu jednicku hodnotou (-1). Vyslednou matici oznacme D_G.
$I_G * I_G^T =$ skal. soucin radku i, j. Na diagonale $deg(v)$, mimo diag. 1 pro hrany, 0 - nehrany. Zmenime prave jednu 1ku ve kazdem sloupci na -1 (tim dostaneme orient. graf).

$$D_g * D_G^T = L_G$$

Rovnost plati protoze skalarni soucin stejneho radku da $deg(v)$ jelikoz $-1*-1 = 1$. Pokud nasobime ruzne radky, prislusne vrcholy nejsou spojene hranou - 0. Jinak maji prave 1 spolecnou pozici a dostaneme $-1*1 = -1$.
Pak $det(L_G^{(u)})$ spocitame jako $det(D_G^{(u)} * (D_G^{(u)})^T)$
Pouzijeme Cauchy-Benet formulu (det souciny obdelnikovych matic)

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

Kde A_w jsou n sloupcu matice A, B^w - n radku matice B.



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

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

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

Kostra musi mit $(n-1)$ vrcholu; v det se divame na vsechny podmoziny hran $|w| = n-1$. Ptame se jestli je strom. Proto suma nehore je prave $\sum_{(V,w) je\ kostra}^{w} 1 = \#$ koster G. ∎

2 Sudo-lichomesta, 2-vzdalenost mnozin bodu

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

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

Pak linearita v 2. slozce atd.

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

kde S^w znamena, ze jsme vzali sloupce odpovidajici indexum v w. Ostatni sloupce jsou z T.

Věta 2.2 (skoro dizjunktni systemy mnozin). *Necht* $A_1, ..., A_k$ *jsou ruzne* $\subseteq [n]$, $|A_i \cap A_j| = 1, i \neq j \Rightarrow k \leq n$

Důkaz. Necht A-matice incidence $\{A_i\}$. Radek odpovida prvcim, sloupec - mnozinam. Na pozice $(r,s) = 1 \Rightarrow$ prvek r lezi v mnozine A_s.
Vezmeme $A^T * A$ nad $\mathbb{R}$. Pak ve vysledne matice na pozice (r,s) je $|A_r \cap A_s|$. Jelikoz pruniky jsou 1-prvkove, mame matici 1-cek. Na diagonale jsou $|A_i|$ velikosti mnozin.

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

Tvrdime, ze $det(A^T A \neq 0)$. Pak matice je regularni a $rank = k$. BUNO $|A_i| = a_i, a_1 \leq a_2 \leq ... \leq a_k$. Mame matici, kde na diagonale jsou velikosti mnozin, jinak 1.
Nahledneme $a_2 \geq 2$. Jinak pokud $a_1 = a_2 \Rightarrow \exists x \in A_1 \cap A_2 \Rightarrow A_1 = A_2 = \{x\}$.
Necht J je matice jednicek. Matici A muzeme napsat jako $J + I * (a_i - 1)$ kde $(a_i - 1)$ je na diagonale. Pouzijeme vlastnost det jako multilinearni formy, viz lemma. Pokud vezmeme 2 sloupce z J, tak det bude 0. Takze zbyvaji 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-ty sloupec lze spocitat rozvojem dle i-ho radku kde je pouze 1 jednicka.

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

Kde 2. produkt mame protoze a_1 se muze rovnat 1, zbytek jsou vetsi. Prvni $\prod$ je ≥ 0, druhy $\prod > 0$ protoze od $i = 2, a_i \geq 2$. $\sum$ je zlomek kladnych clenu, takze $\sum \geq 0$. Dohromady $det(J + S) > 0$

□

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

Důkaz. Vezmeme matice incidence jako v predchozi vete. Uvazme matici $A^T * A$ nad $\mathbb{Z}_2$. Pak na diagonale jsou mohutnosti mnozin $= 1 \mod 2$, mimo diagonalu pruniky $= 0 \mod 2$. Neboli $A^T * A = I \Rightarrow rank = k$. Pak jako minule:

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

□

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 mnoziny jsou simplexy. Zobecneni rovnostranneho $\triangle$ do vyssich dimenzi. Indukci dokazeme, ze $m_1(n) = n + 1$. Pri prechodu do vyssi dimenze existuje prace jeden bod ktery muzeme pouzit. Proces podobny kompaktizace topologickeho prostoru.

Věta 2.6 (2-vzdalenostni mnoz). *Necht* $m_s(n)$ *znaci pocet bodu s-vzdalenostni mnoz v* $\mathbb{R}^n$*, pak:*

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

Důkaz. 1) Dolni odhad
Vezmeme vektory, ktere maji prave 2 jednicky, jinak 0. Takovych mame $\binom{n}{2}$.
Pokud 2 vektoru maji 1 spolecnou pozice, $d(x,y) = \sqrt{2}$. Jinak pokud maji 2 spolecne pozice, tak $d(x,y) = 2$. Vzdalenost pocitame jako kanonickou Euklidovou normu.

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

Zesilime dolni odhad: premistime se do $\mathbb{R}^{n+1}$. Jelikoz $\sum_i^{n+1} x_i = 2$, 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) Horni odhad
Mame body $A_1, A_2, ..., A_t$. $A_i = (a_{i,1}, a_{i,2}, ..., a_{i,n}) \in \mathbb{R}^n$. Oznacme vzdalenosti $k \neq m \in \mathbb{R}$. 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 vzdalenost $m \vee k \Rightarrow F = 0$.
Pak $f_i(x), f_i(x) = F(x, A_i)$. Castecne dosazeni. Tyto funkce jsou v V.P. funkci z $\mathbb{R}^n$. Tvrdime ze $\{f_i(x)\}$ jsou LN. Pokud dosadime 2 ruzne prvky do f_i tak dostaneme 0 dle definice zobrazeni F. Pro stejny bod $f_i = a^2 b^2 \neq 0$.

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

Podivame se na tuto funkce (lin kombinace funkci) v nejakem 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 pocet je omezen podprostorem funkci nad $\mathbb{R}^n$ ve kterem zijou.

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

f_i jsou polynomu stupne 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 $dim(U) = 1 + n(lin) + n(kv) + n(kv * lin) + \binom{n}{2}(lin2) + 1 = 2 + 3n + 1/2n(n-1) = 1/2(4 + 5 + n^2)$. Generator $\sum x_j^2$ nepotrebujeme protoze je lin komvinaci x_j^2.
□

3 Sudo-sudomesta, Prostor cyklu grafu

Věta 3.1 (Sudo-sudomesta). *Necht* $A_1, ..., A_k$ *jsou ruzne* $\subseteq [n]$, $|A_i| = 0 \mod 2 \; \forall i, |A_i \cap A_j| \equiv 0 \mod 2, i \neq j \Rightarrow k \leq n$

Důkaz. Udelame bijekci mnozina $\rightarrow$ 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 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 rozdklad X. Pak mnoziny budou vsechny mozne podmnoziny obsahujici 2ce. Je jich $2^{\lfloor n/2 \rfloor}$ □

Definice 3.2. Uvazme bijekci mezi napnutym podgrafem H a jeho charakteristickym vektorem. Mnozina vsech napnutych podgrafu ν_G tvori V.P. nad $\mathbb{Z}_2$, scitani vektoru odpovida symmetricke diferenci mnoziny hran.

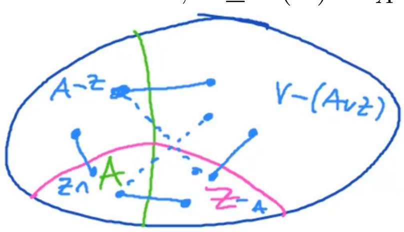
Definice 3.3. Mnozina napnutych podgrafu je Eulerovska pokud $\forall u \in V, deg(u) = 0 \mod 2$. Znacime ξ_G. Pak β_G je mnozina elementarnich rezu, t.j. $B_A = (V, \{xy : x \in A, y \in V \setminus A, xy \in E\}), A \subseteq V$.

Věta 3.4 (Eulerovske grafy). ξ_G, β_G *jsou V.P. podprostory* ν_G. *Plati* $\xi_G^{\perp} = \beta_G \wedge \beta_G^{\perp} = \xi_G$. *Pokud navic je graf souvisly,* $dim(\beta_G) = |V| - 1 \wedge dim(\xi_G) = |E| - |V| + 1$.

Důkaz. 1) Nasobeni skalarem je automaticky splneno, protoze teleso je $\mathbb{Z}_2$.
2) $H_1 + H_2 = (V_1, E(H_1) \div E(H_2))$. Taky patri do V.P.
3) Ukazeme $\forall H_1, H_2 \in \xi_G : H_1 + H_2 \in \xi_G$. Zvolme vrchol u, necht $deg_{H_1} u = 2k, deg_{H_2} u = 2l$, taky h je pocet spolecnych hran obou podgrafu.

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

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



Z obrazku prezijou pouze hrany vedouci z $A-Z$ do $V-(Z\cup A)$, hrany z $A-Z$ do $Z\cup A$, hrany $(Z\cap A)$ do $Z-A$ a hrany ze $Z-A$ do $V-(Z\cup A)$. Ostatni byly ve 2 rezich. Zustane rez $B_{A\div Z}, A\div Z=(A-Z)\cup(Z-A)$.

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

Tvrdime ze $B_G=\langle B_{\{u\}}, u\in V\rangle$. Prostor el. rezu je generovany hvezdami. Protoze

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

Hrany uvnitr A se smazou sym. diferenci, hrany vedouci ven z A, ktere nejsou spolecne zustanou.
5) G souvisly $\Rightarrow dimB_G=|V|-1$. Nahledneme ze secteni vsech hvezd dava $\emptyset$ graf. Neboli kazda hrana patri ke 2 hvezdam.
Zafixujeme vrchol u, secteme hvezdy krome u. $\sum_{a\neq u} B_{\{a\}}=\emptyset-B_{\{u\}}=B_{\{u\}}\neq\emptyset$ Pokud vezmeme vsechny krome 1 hvezdy, tak jsou LN a generuji vsechny rezy. Z toho $\Rightarrow dimB_G=|V|-1$.
Pozorovani:

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

Uvazme hvezdu $B_{\{u\}}$ a $deg_H u=0 \mod 2$. Pak symmetricka diference smaze prave sudy pocet hran z hvezdy a nove pocet hran je taky sudy.

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

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

□

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

Důkaz. 1) Uvazme $M=\xi_G$ v tvrzeni z lemmatu. $\bar{1}=G$, ma vsechny 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 rozdklad je dizjunktni, takze mame 2 Eulerovske podgrafy a mezi nimi elementarni rez. Pokud rez smazeme, graf je sjednoceni dvou Eulerovskych podgrafu.

□

4 Seiduv switching

Definice 4.1. Necht V je V.P nad T. Linearni forma je lin zobrazeni $f : V \to T$. Pak linearni formy tvori V.P. nad T. Znacime V^* a je tzv. dualni prostor k V.

Definice 4.2. Necht $B = \{b_1, b_2, ..., b_n\}$ je baze V, pak $B^* = \{f_1, f_2, ..., f_n\}$ je dualni baze, pokud formy jsou dane predpisem:

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

Definice 4.3. Necht A,B jsou V.P nad T, $dimA = n, dimB = k$. Necht $\varphi : A \to B$ homomorf. Pak dualni homomorf k φ je zobrazeni $\varphi^* : B^* \to A^*$ dane predpisem:

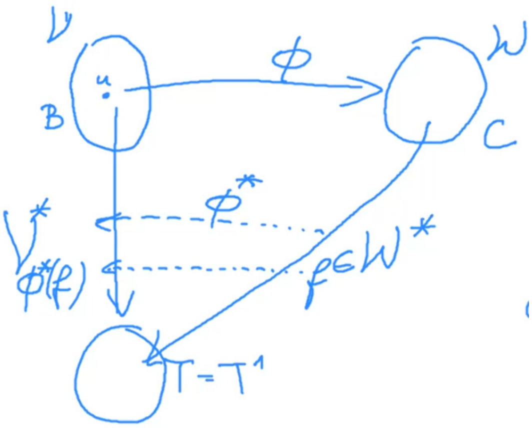
$$\forall f \in B^* \ \forall u \in A : (\varphi^*(f))(u) = f(\varphi(u))$$

Věta 4.4 (Matice dualniho homomorf(BD)). *Matice dualniho homomorf vzhledem k dualnim bazim je transponovanout matici k matici primarniho homomorf.*

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

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

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



Mame homomorf $\phi : V \to W$, pak linearni formy $h : W \to T$.
Dualni homomorf $\phi^* : W^* \to V^*$ je definovan:

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

Jelikoz lin 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 rika, ze

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

□

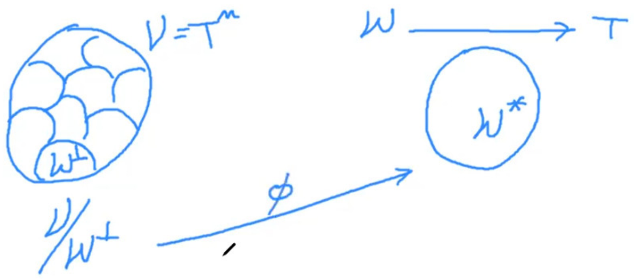
Definice 4.5. Faktorprostor: faktorizace dle podprostoru W prostoru V (podgrupa). V/W jsou mnoziny $\forall u \in V u + W$. Pak i faktorprostor je V.P vuci operacim:

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

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

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

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



Důkaz.
Pak izomorf ϕ 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 ϕ bylo korektne definovane a splnovalo vlastnosti izomorf:
1) korektnost definice
2) lin zobrazeni
3) proste
4) na
Dukaz:
1) $a \in v+W^{\perp} \iff a = v+b, b \in W^{\perp}$. Pak

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

Protoze $x \in W \Rightarrow \langle b, x \rangle = 0 \Rightarrow \langle v, x \rangle = \langle a, x \rangle$.
2) Skalarni soucin je bilinearni forma, z toho ϕ je linearni zobrazeni.
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.

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

Rovnost dimenzi plati protoze zobrazeni je proste.

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

Z LA $Im(\phi)$ je vnoreny podpostor stejne dimenzi jako nadprostor $\Rightarrow$ jsou stejne.

□

Věta 4.7 (Burnsidovo lemma(BD)).

Lemma 4.8. *Necht grupa G provadi akci na mnozine M, grupa H na N. Necht $\varphi : M \to N$ bijekce.*

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

$$
\begin{tikzcd}
M \arrow[r, "\phi"', "1-1"] \arrow[d, "G \ni g"'] & N \arrow[d, "h \in H"] \\
M \arrow[r, "\phi", "1-1"'] & N
\end{tikzcd}
$$

Důkaz. Prvky v M_g jsou $gm = m$. Prvky v N_h jsou $hn = n$. Kvuli bijekci n lze jednoznacne vyjadrit jako:

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

Pak

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

Diagram komutuje

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

φ je bijekce, takze proste $\Rightarrow gm = m$. Dohromady $\#\ hn = n$ je totez jako $\#\ gm = m$. $\square$

Definice 4.9. Seiduv switching vymeni vsechny hrany a nehrany vychazejici z $u \in V$. Ostatni vrcholy a hrany beze zmen. Grafy $G \sim G' \iff G'$ lze ziskat z G postupnym prepinanim vrholu.

Poznámka 4.10.

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

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

Věta 4.11 (Pocet neiz trid Seide switching). *Počet neizomorfních tříd ekvivalence při Seidelově switchingu na n vrcholech je roven počtu Eulerovských grafů na n vrcholech.*

$$
\begin{tikzcd}
\mathcal{V}/\mathcal{B} \arrow[r, "\phi"] \arrow[d, "\bar\sigma_B"'] & \mathcal{E}^* \arrow[d, "\bar\sigma_E^{-1*}"] \\
\mathcal{V}/\mathcal{B} \arrow[r, "\phi"] & \mathcal{E}^*
\end{tikzcd}
$$

∀ zobrazení jsou lineární

$\sigma \in \mathrm{Sym}\, V$

$\bar\sigma \in \mathrm{Aut}\, \mathcal{V}$ $\quad \bar\sigma(G) = (V, \{\sigma(u)\sigma(v) \mid uv \in E(G)\})$

$\bar\sigma_B \in \mathrm{Aut}\, \mathcal{V}/\mathcal{B}$ $\quad \sigma(\mathcal{B}) = \mathcal{B}$

$\bar\sigma_E \in \mathrm{Aut}\, \mathcal{E}$ $\quad \bar\sigma_E = \bar\sigma|_{\mathcal{E}}$

$\bar\sigma_E^* \in \mathrm{Aut}\, \mathcal{E}^*$ $\quad$ duální zobrazení k $\bar\sigma_E$

Důkaz.
Pak dle Burnsidova lemmatu: $\#$ orbit V/B pri akci $S(V) = \frac{1}{n!}\sum |(V/B)_\sigma|$.
Taky $\#$ orbit ξ^* pri akci $S(V) = \frac{1}{n!}\sum |(\xi^*)_\sigma| = \frac{1}{n!}\sum |(V/B)_{\sigma^{-1}}|$. Zbyva dokazat, ze $\#$ orbit je stejny i pro ξ misto ξ^*.

$\square$

5 Spekrum grafu, Moorovy grafy

Definice 5.1. Necht G je r-regularni graf obvodu vetsiho nez 4 (nema ani $\triangle$ ani kruznice delky 4). Pak $|V(G)| \geq r^2 + 1$.

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

Věta 5.3 (Moorovy grafy). *Moorovy grafy existuji pro* $r = 1, 2, 3, 7$*, pravdepodobne* $r = 57$*. Pro zadne jine r neexistuji.*

Důkaz. 1) r = 1, cesta delky 2
2) r = 2, kruznice delky 5
3) r = 3 Petersenuv graf 4) r = 7 Homan, Singleton graf
Ostatni r, necht G je Mooruv graf, na $n = r^2 + 1$ vrcholech. Vezmeme matice sousednosti. A^2 ma pocet sledu delky 2 mezi vrcholu $a - b$. Na diagonale mame r, mimo diagonalu je 0 pokud mezi $a - b$ v puvodnim grafu vedla hrana. Naopak A^2 bude mit 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 ma ($n - 1$ nasobne vlasne cislo $\lambda = 0$. Posledni vl. cislo je n. Pak

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

r-regularni graf ma nejvetsi vl. cislo r. Dosadime r do rovnice. $r^2 + r - (r-1) = r^2 + 1 = n$. Ostatni jsou nulove.

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

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

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

Vyresime system 2 rovnic o 2 neznamych. 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 mame takovy graf.
2) Jinak $s \in N \Rightarrow 1/4(s^2+3) - (1/4(s^2+3))^2 * 1/2 + s/2(m_1 - m_2) = 0$. Vynasobime 32.

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

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

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

□

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.

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

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

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

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

Vyresime soustavu 3 rovnic o 3 neznamych. Dosadime hodnoty λ_1, λ_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 pripady:
1) $s \notin \mathbb{Q} \Rightarrow$ posledni scitanec 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 stupen vrcholu $d \leq (n-1)$

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

Pokud $(f-e) = 2 \Rightarrow d = n-1 \Rightarrow G = K_n$ coz jsme vyloucili definici. Jinak

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

Pracujme s 3. rovnici:

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

dosadime $(e-f) = -1$.

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

Dosadime $n = 2d - 1$

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

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

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

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

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

Zbavime se jmenovatele a roznasobime kvadraty v 3.

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

Spocitame p,q pomoci determinantu.

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

Dolni determinant

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

Dosadime $s^2=(e-f)^2+4(d-f)$.

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

Horni determinant:

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

2 houts later...

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

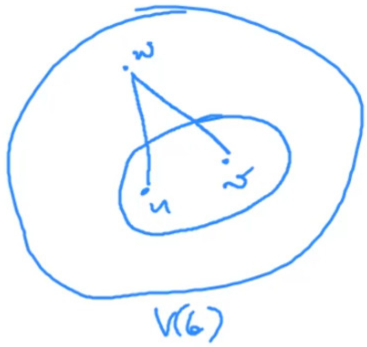
□

Věta 6.3 (Friendship theorem). *Necht v grafu G maji kazde 2 ruzne vrcholy prave 1 spol. souseda. Pak G obsahuje vrchol, ktery sousedi se vsemi ostatnimi vrcholy grafu.*

Důkaz. Pokud plati $e=f=1\Rightarrow\exists v\in V$ ktery sousedi se vsemi ostatnimi vrcholy. Necht $N_G(u)$ je mnozina sousedu $u\in V$. Vezmeme mnozinovy system $\{N_G(u)|u\in V\}$. Pak prunik dvou mnozin je jednoprvkovy.

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

Taky z obrazku



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

Coz je skoro konecna projektivna rovina KPR. Chybi 3. axiom. Rozebereme 2 pripady:
1) 3. axiom plati $\Rightarrow\{N_G\}$ je KPR. Pak

$$\forall a|N_G(a)|=m+1=deg(a)$$
$$n=|V(G)|=m^2+m+1$$

Z cehoz G je silne regularni s parametry $d=m+1\wedge e=f=1$. Prvni pripad nastat nemuze kvuli podmince na $e=f=1$. Neboli 2 pripad:

$$p = \frac{d((d-1+f-e)(s+f-e)-2f)}{2fs} \in \mathbb{Z}$$
$$(e-f)^2 - 4(f-d) = s^2 \wedge e = f = 1 \Rightarrow s = 2\sqrt{m} = 2t$$

Dosadime

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

Pripad $t = 1 \Rightarrow m = 1$ neni zajimavy protoze KPR radu 1 je $\triangle$.
2) 3. axiom neplati $\Rightarrow \{N_G\}$ z teorie KPR bud vsechno lezi na 1 primce nebo jeden vrchol samostatne a zbytek na primce. Pak ten sampstatny vrchol je hledany soused vsech:

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

□

Věta 6.4 (vl cisla Hermitovske matice(BD)). *Necht $A \in \mathbb{C}^{n\times n}$ je Hermitovska, $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n$ jeji vl. cisla. Necht $b_1, b_2, ..., b_n \in \mathbb{C}^n$ je ortonormalni baze vl 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). *Necht $A \in \mathbb{C}^{n\times n}$ je Hermitovska, $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n$ jeji vl. cisla. Necht B je hlavni podmatice radu $k \times k$ (vznikne vynechanim $(n-k)$ radky), Necht $b_1, b_2, ..., b_n \in \mathbb{C}^n$ jsou vl cisla matice B. Pak plati*

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

Důkaz. Nejprve se podivame na pripad vynechani i-ho radku. Necht B ma ortonormalni baze $y_1, y_2, ..., y_{n-1} \in \mathbb{C}^{n-1}$. Vnorime tyto vektory do $\mathbb{C}^n$ tak, ze na pozici $i-1$ vlozime 0. Oznacime je $z(y)$. Pak

$$z^*(y) A z(y) = y^* B y$$

Uvazme 3 mnoziny, j je libovolne

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

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

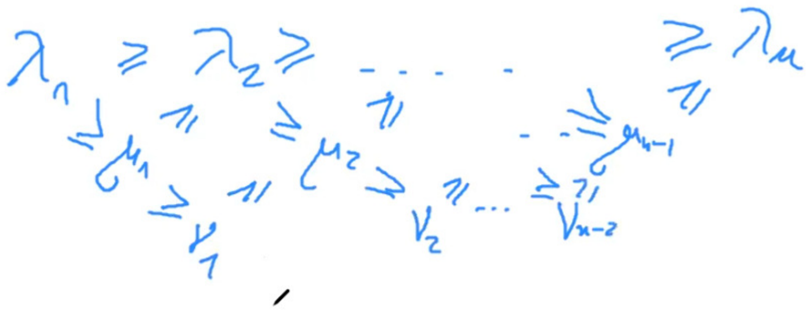
$$l \in S_1 \Rightarrow l^* A l \geq \lambda_j l^* l$$
$$l \in S_3, y \in S_2, l = z(y) : l^* A l = y^* B y \geq b_j y y^* = b_j l^* l \geq \lambda_j l^* l$$
$$\lambda_j l^* l \geq b_j l^* l \ \Rightarrow \lambda_j \geq b_j$$

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

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

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

Ted pro obecne k.



Z obrazku

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

□

Věta 6.6 (Nezav mnozina a vl cisla). *Necht G je graf o n vrcholech s vl cisly* $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n$. *Pak*

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

Důkaz. Necht $W \subseteq V(G)$ je nezav mnozina velkosti α. Matice sousednosti teto mnoziny je nulova $\alpha \times \alpha$. Taky je to hlavne podmatice A_G. Proto jeji vl. cisle (nuly) propletaji vl cisla G. Z toho

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

□

7 Odhady pomoci spektra

Věta 7.1 (Nezav mnoz v d-regularnim). *Necht G je d-regularni graf o n vrcholech s vl cisly* $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n\}$. *Pak*

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

Důkaz. Necht A je matice sousednosti grafu G.

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

Matice A, J komutuji $\Rightarrow$ maji spolecnou ortonormalni baze.

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

Kde Λ_A je diagonalni matice s vl. cisly na diagonale, rozmíštěné dle uspořadaní. Podobně pro J:

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

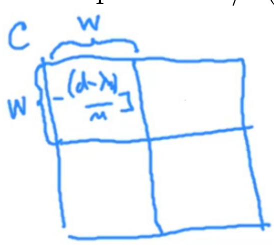
Z věty o ortonormalní bazi vl. vektor přislušný největšímu vl. číslu je nezaporný. Ostatní maji zaporné složky. Pak vektor $\bar{1}$ je prislusny nejvetsimu vlastnimu cislu A - d. Taky odpovida vl cislu n matice J.
Uvazme matici:

$$C = A - 1/n(d - \lambda_n)J$$

Jeji vl. čísla jsou lin. kombinace vl. čísel A, J.

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

Kde $(\Lambda_K)_{1,1} = d - \lambda_n$, jinak 0. Z toho Λ_C ma na diagonale $\{\lambda_n, \lambda_2, ..., \lambda_n\}$. Odtud λ_n je největší vl. číslo matice C.
Necht $W \subseteq V(G)$ je nezav. mnoz G, $|W| = \alpha(G)$. Pak matice A, po seskupeni radku odpovidajicich W, ma nulovou hlavni podmatice odpovidajici W. Z toho matice C ma na techto pozicich $1/n(d - \lambda_n)$. Taky je to hlavni podmatice.



Vl. cisla matice $-1/n(d - \lambda_n)J$ propletaji vl. cisla matice C.

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

Z vety o propletani:

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

□

Důsledek 7.2. *Necht G je d-regularni graf o n vrcholech s vl cisly* $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n\}$*. Pak*

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

Plyne z toho, ze $\chi(G) \geq \frac{n}{\alpha(G)}$*. Barveni grafu je rozlozeni ne* $\chi(G)$ *nezavislych mnozin. Kazda z nich ma velikost* $\chi(G)/\alpha(G)$*. Kombinaci dvou nerovnosti dostaneme tvrzeni.*

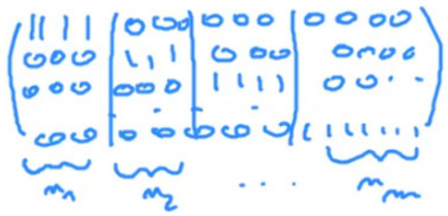
Věta 7.3 (Propletani B). *Necht:*

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

Je Hermitovska matice v blokovem 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 jejiz prvky* $b_{ij} = \frac{\sum_{a \in A_{ij}} a}{n_i}$ *jsou prumerne radkove soucty bloky A. Potom vl cisla B propletaji vl cisla A.*

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



Potom PP^T je diagonalni matice D protoze jednicky jsou na ruznych pozicich. Sk. soucin dvou ruznych radku je 0. Na diagonale je norma i-ho radku $= n_i$.
Pouzijeme matici P abychom dostali radkove soucty matici A:
V matici PA dostaneme sloupcovy soucet po blocich. Pak v matici PAP^T dostaneme soucty vsech prvku v blocich.
Pro rovnost s matici B jeste potrebujeme vydelit n_i. Na coz pouzijeme D^{-1} ktera ma na diagonale $\frac{1}{n_i}$.

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

Necht $S = D^{-1/2}P$. S je realna matice, pro niz plati

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

Dle Vety o propletani A 7.7, vl. cisla SAS^T propletaji vl cisla 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 podobne $\Rightarrow$ maji stejny spektrum.

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

□

Věta 7.4 (Polomer spektra grafu). *Necht G je graf o n vrcholech s vl cisly* $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n\}$. *Pak*

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

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

Důkaz. 1) Nerovnost $\Delta(G) \geq \lambda_1$. Doplnime G na Δ-regularni graf H tak, aby G byl jeho indukovany podgraf. Pak vl. cisla G propletaji vl cisla H. $\lambda_{max}(H) = \Delta \Rightarrow \Delta(G) \geq \lambda_1$.
2) Nerovnost $\lambda_1 \geq deg_{avg}(G)$. Vezmeme matice sousednosti A, predstavime ji jako matici s 1 blokem. Pak matice prumernych radkovych souctu je $B = deg_{avg}(G)$ jednoprvkova. Dle Vety o propletani B 7.3, $Sp(B) = \{deg_{avg}(G)\}$ propleta spektrum A $\Rightarrow \lambda_1 \geq deg_{avg}(G)$.
□

Věta 7.5 (Barevnost libovolneho grafu). *Necht G je graf o n vrcholech s vl cisly $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n\}$. Pak*

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

Důkaz. Necht H je χ-kriticky indukovany podgraf grafu G. Minimalni stupen vrcholu v χ-kritickem grafu je aspon $\chi - 1$. Oznacme jeho největší vl cislo jako h_1. Z vety o propletani plyne $\lambda_1 \geq h_1$. Z vety polomeru spektra 7.4 dostavame

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

□

Věta 7.6 (Nezav mnoz v libovolnem grafu). *Necht G je graf o n vrcholech s vl cisly $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n\}$. 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. mnoz G, $|W| = \alpha(G)$. Rozdelime matice A dle W a $V \setminus W$.

$$A = \begin{array}{c} \\ W \\ V \setminus W \end{array} \begin{array}{c} \begin{array}{cc} W & V \setminus W \end{array} \\ \left[\begin{array}{c|c} 0 & A_{12} \\ \hline A_{21} & A_{22} \end{array}\right] \end{array} \begin{array}{l} \\ \}\alpha \\ \}n-\alpha \end{array}$$

Pouzijeme Vetu o propletani B 7.3.

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

Pak $Sp(B) = \{h_1 \geq h_2\}$ propleta $Sp(A) = Sp(G)$.
Dal vime, ze pocet 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 soucet vl cisel je determinant:

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

Z propletani:

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

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

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

□

Věta 7.7 (Propletani A). *Necht* $A \in \mathbb{C}^{n\times n}$ *Hermitovska.* $S \in \mathbb{C}^{m\times n}$ *takova, ze* $S^*S = I$. *Potom vl cisla* S^*AS *propletaji vl cisla matice* A.

Důkaz. Radky matice S jako vektory v $\mathbb{C}^n$ lze rozsirit na ortonormalní baze $\mathbb{C}^n$ (Gram-Schmidt z LA). Sestavime z ni 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 hlavni podmatice RAR^*, a vl cisla SAS^* propletaji vl cisla RAR^*. Pritom $Sp(RAR^*) = Sp(A)$ z LA, protoze matice jsou podobne. □

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

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

Veta je analogicka dusledku vety 1, zesiluje ji pro souvisle grafy.

Důkaz. Obarvime graf pomoci χ barev. Necht x je realny vl. vektor prislusny vl. cislu λ_1 (Existuje dle Frobeniove vety). Ze souvislosti $x_i > 0 \forall i$.
Sestavime 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 diagonalni matice, na diagonale $\sum_{u \in W_j} x_u^2 > 0$. Necht $S = D^{-1/2}P$. Protoze

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

Dle Vety o propletani A 7.7, vl. cisla SAS^T propletaji vl cisla A. Necht vl cisla SAS^T jsou $\{h_1, h_2, ..., h_\chi\}$. Ma na diagonale same nuly, z toho

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

Dal

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

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

Dostavame

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

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

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

Pouzijeme horni odhad pro soucet pres # scitancu krat min hodnota (λ_n).

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

Po uprave

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

$\square$

8 Shannonova kapacita

Definice 8.1. Necht A je abcda, $A = \{a, e, o, h, g\}$. 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 pozice stejne pismeno nebo zamenitelne. Presne odpovida uplneho soucinu grafu.

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

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

Kde vrcholy a,x jsou z grafu G, b,y z grafu H.
Taky definujme $G^n = G \square G \square ... \square G$.

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 mnozina $B \subseteq V(G), |B| = \alpha(G)$. Pak B^k je taky nezav mnozina. 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 pokryvajici mnoz grafu. Pak

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

Protoze $K_n \square K_m = K_m n$. Soucin uplnych je uplny graf, jina moznost neni (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 perfektni graf $\Rightarrow \sigma(G) = \alpha(G)$. Pak

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

Definice 8.8. Lovascova definice ortonormalni reprezentace grafu je zobrazeni $f : V \to \mathbb{R}^d$ splnujici:

- $||f(u)|| = \langle f(u), f(u)\rangle = 1 \forall u \in V$ 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 ktery nema zadny vrchol potrebujeme system vzajemne $\perp$ vektoru velikosti $V(G)$, neboli prostor dimenze $V(G)$.
Pro uplny graf staci volit vektory stejneho smeru nebo dokonce stejne.

Definice 8.10. Lovascova dzeta funkce grafu G:

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

Chceme pro nejakou reprezentace najit takovy jedn vektor c, ktery minimalizuje hodnotu $\langle c, f(u\langle\rangle^2$.

Příklad 8.11. Pro uplny graf zvolime reprezentaci ktera se sklada ze stejnych vektoru, c vezmeme ve stejnem smeru. Pak vsechny skalarni souciny jsou 1. Z toho

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

Definice 8.12. *Rukojet* reprezentace f je vektor c (jedn vektor), pro ktery f nabyva minima. Infimum v def velikosti ortonormalni reprezentace se nabyva, protoze $f = f(c)$ je spojita a zdola omezena.
V definici staci uvazovat omezenou dimenzi, napr $d \leq |V(G)|$.
Infimum v dev dzeta funce se taky nabyva, protoze $||f||$ je spojita funkce f. Pak

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

Úmluva 8.13. Muze se stat, ze rukojet je vektor kolmy na nejaky z vektoru f. Pak $\vartheta(G) = \infty$. Budeme se ale takovym rukojetim vyhybat. Vsechny vektory reprezentace lezi v nadrovine, je jich konecne mnoho.

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

Důkaz. Necht G je graf, a mame optimalni repr. f s rukojeti c. $||f|| = \vartheta(G)$. Taky $W \subseteq V(G)$ je nezav mnozina:

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

Vektory reprezentujici W jsou na sebe kolme. Muzeme je doplnit na ortonormalni baze B prostoru $\mathbb{R}^d$. Pak rukojet muzeme napsat jako lin. konbinace pomoci vektoru z B:

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

Dal c je jedn. 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 ortonormalni baze, takze pro $u \neq v$ je soucet nula, jinak misto posledniho sk souciny tam bude 1. Pak dostaneme soucet vlevo, ktery je vesti nez suma pro vektory reprezentace nezav mnoziny.

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

Nahledneme ze velikost sk. soucinu je omezena maximumem pro vsechny vrcholy, coz je prave $\vartheta(G)$.

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

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

Scitame pres velikost nezavisle mnoziny, dostaneme $\frac{\alpha(G)}{\vartheta(G)}$ Dohromady

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

□

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

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

Důkaz. Necht f je optimalni ortonormalni repr. G s rukojeti c. Podobne g pro H s rukojeti d. Uvazme tenzorovy soucin $f \circ g$ jako ortonormalni reprezentace soucinu grafu.

$$(u,v) \in V(G \Box H), (f \circ g)(u,v) = (f(u) \circ g(v)) = (f(u)_i g(v)_j)_{i,j}, i = 1,2,...,n1; j = 1,2,...,n2$$

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 sk soucin je 0 nebo druhy z volby vrcholu. Takze

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

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

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

Max je dvou funci je mensi nez soucin 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. Vime $\alpha(C_5^2) = 5 \Rightarrow \vartheta(C_5) \geq \sqrt{5}$. Ukazeme $\vartheta(C_5) \leq \sqrt{(5)}$. Z toho

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

Odkud plati i rovnost.
Pro dukaz staci uvazit ortonormalni reprezentaci C_5 ktera se jmenuje Lovascovuv destnik.

□

9 Samoopravne a perfektni kody, Lloydova veta

Definice 9.1. Necht A je konecna mnozina (abcda), $q = |A|$. Na mnozine slov $w \in A^n, |w| = n$ definujme Hammingovu metriku jako pocet pismen ve kterych se lisi

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

Libovolnou $C \subseteq A^n$ nezyvame kodem delky n nad abcdeou o q symbolech. C opravuje t chyb, pokud

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

Pozorování 9.2. Pokud vezmeme graf vsech slov delky n, hrany povedou mezi 2 slova ktere se lisi presne v 1 souradnice. Pak grafova vzdalenost je prave Hammingova metrika. Na druhou stranu tento graf je n-ta kartezska mocnina grafu o q vrcholech.
Kod C opravuje t chyb $\iff$ okoli kodovych slov o polomeru t jsou po 2 dizjunktni.

Pozorování 9.3. Kartezsky hrana $\times$ hrana je $\square$.

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 okoli bodu x polomeru t:

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

Kde 1 je vrchol sam, pak mame n pozic na kazde muze dojit k $(q-1)$ chybam.

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

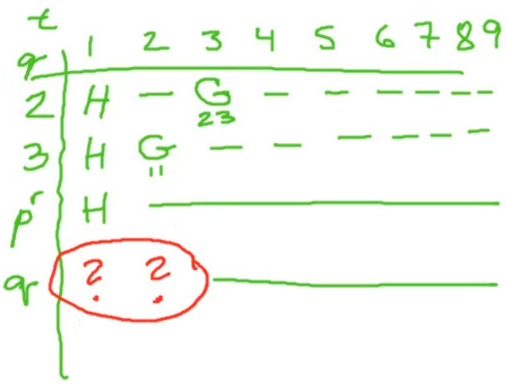
binom odpovida zpusobum zvolit pismeno. $(q-1)^i$ je pocet chyb.
Pak nerovnice pro velikost C je # vsech slov deleno velikosti okoli.

Definice 9.6. Kod je t-perfekti, prave kdyz $|C|>1$, C opravuje t chyb a nastava rovnost.

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

Cely graf je pokryty okoli o polomeru t. Vyuzivaji beze zbytku cely graf (kodova slova).

Poznámka 9.7. Perfektni kody skoro neexistuji.



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

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

Pak suma v jmenovateli deli $q^n = p^{rm}$. Takze i suma je mocnina p. Dokazeme ze suma se rovna $q^l, l \in \mathbb{N}$.

Důkaz.

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

Upravime 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 soucet geom rady. Druhy zlomek ale $\in (0,1)$. Coz dava dohromady cele cislo pouze $b=0$. $\square$

Věta 9.9 (Hammingovy kody). *Necht $q = p^r$. Pak 1-perfektni kod delky n nad abcdou o 1 symbolech existuje $\iff n = \frac{q^k-1}{q-1}, k \in \mathbb{N}$.*
Coz dostaneme dosazenim $t = 1$ do rovnice minuleho pozorovaji:

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

Necht $C \subseteq \mathbb{Z}_q^n$. Sestavime matici $H \in \mathbb{Z}_q^{k \times n}$ tak, aby sloupce byly po 2 lin. nezavisle.
V kazde slozce muzeme vzit q^k symbolu. Nulovy vektor pouzivat nemuzeme. Dohromady $q^k - 1$ vektoru. Vezmeme nejaky vektor, linearne zavisle s nim jsou jeho nasobky skalarem krome 0 - $(q-1$. Proto

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

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

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

Tvrdime, ze v jadru jsou vektory ktere maji vzdalenost aspon 3. Pokud by existovali vektory vzdalenosti 2. Jejich rozdil by taky $\in Ker(H)$. Dostali bychom vektor y ktery ma nejvyse 2 nenulove souradnice. Po vynasobeni Hy dostali bychom lin. kombinace 2 vektoru ktere jsou dle volby lin. nezavisle.

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

Důkaz. □

Věta 9.10 (Prvociselne perf. kody(BD)). *pro $q = p^r$ neexistuji perfektni kody jinych parametru nez Hammingovy, Golayovy (a opakovaci kod s parametry $q = 2, n = 2t + 1$, ktery je povazovan za trivialni).*

Věta 9.11 (Prvociselne perf. kody $t \geq 3$ (BD)). *pro $q = p^r$ neexistuji zadne t-perfektni kody opravujici $t \geq 3$ chyb.*

Věta 9.12 (Lloyd). *Pokud existuje t-perfektni kod delky n nad abcedou 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 ruznych kladnych celociselnych korenu mensich nez n. Je to polynom stupne t.
Myslenka dukazu: najdeme 2 koreny od sebe vzdalene min nez 1. Pak nemuzou byt celociselne.
Pro $t = 1, 2$ umime koreny najit, takze Lloydova veta je prilis slaba.

Důkaz. TODO predn 9 od 34:00 □

Lemma 9.13.

Důkaz. □