Linearní Algebra v Kombinatorice

Ladislav Láska
Jan Musílek

29. prosince 2014

Obsah

1 Lineární nezávislost

Definice Vektory v_i jsou lineárně nezávislé, pokud neexistuje netriviální řešení rovnice $\sum_i \alpha_i v_i = 0$.

1.1 Sudo-licho města

Definice Nechť $|X| = n$ a $A_1, \ldots, A_m \subseteq X$ $A_i \neq A_j$ jsou neprázdné podmnožiny. Úloha A-B město se ptá, jak velké může být m, pokud $|A_i| \sim B$ a $|A_i \cap A_j| \sim A$ (tedy pro sudo-licho město máme omezení na liché velikosti a sudé průniky).

Věta Pro úlohu sudo-licho město platí $m \leq n$.

Důkaz Počítejme nad $GF(2)$. Matice A nechť je charakteristická matice dimenze $n \times m$. Podívejme se na součin AA^T, tedy na matici skalárních součinů:

$$AA^T = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_m \end{pmatrix} \cdot \big(A_1, A_2, \ldots, A_m\big) = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \ddots \\ & & & 1 \end{pmatrix} \tag{1}$$

Tedy víme, že $\operatorname{rank}(AA^T) = m$ a $\operatorname{rank}(A) \leq n$. Z vlastností ranku již snadno získáme nerovnost $m = \operatorname{rank}(AA^T) \leq \operatorname{rank}(A) \leq n$. **TODO:** důkaz rankové nerovnosti obrázkem pomocí zobrazení □

Věta Nechť $|X| = n$ a $A_1, \ldots, A_m \subseteq X$ že platí $|A_i \cap A_j| = 1$ a $A_i \neq A_j$. Potom $m \leq n$.
Důkaz Podobně jako v předchozím příkladě vezměme matici charakteristických vektorů A a podívejme se na součit AA^T, tentokrát již nad Q:

$$AA^T = \begin{pmatrix} |A_1| & & 1 & \\ & \ddots & & \\ 1 & & \ddots & \\ & & & |A_m| \end{pmatrix} \tag{2}$$

Dále označme $a_i := |A_i|$. Můžeme předpokládat, že $a_1 \leq a_2 \leq \cdots \leq a_m$. Zřejmě také $a_2 > 1$ (jinak $A_1 = A_2$). Nyní bychom chtěli dokázat, že je matice regulární – proto se podíváme na determinant této matice:

$$|AA^T| = \left| \begin{pmatrix} a_1 & & 1 & \\ & \ddots & & \\ 1 & & \ddots & \\ & & & a_m \end{pmatrix} \right| = \left| \mathbf{1} + \begin{pmatrix} a_1 - 1 & & 0 & \\ & \ddots & & \\ 0 & & \ddots & \\ & & & a_m - 1 \end{pmatrix} \right| \tag{3}$$

Zatímco matice jedniček je singulární **TODO:** Pochopit proč se to dá spočítat, ale determinant vyjde kladně. □

1.2 Dvouvzdálenostní množiny

Věta $P_1, P_2, \ldots, P_m$ jsou body v $\mathbb{R}^n$ a $\exists \alpha, \beta \in \mathbb{R}$ t. že $\|P_i P_j\| \in \alpha, \beta$. Pak $m(n) \leq \frac{(n+1)(n+4)}{2}$.
Důkaz

$$F(x,y) = (\|x,y\|^2 - \alpha^2)(\|x,y\|) - \beta^2) \qquad F : (\mathbb{R}^n \to \mathbb{R}) \tag{4}$$
$$f_i(x) = F(x, P_i) \qquad f_i : \mathbb{R}^n \to \mathbb{R} \tag{5}$$

Když jsou $f_1, f_2, \ldots, f_m$ lineárně nezávislé, pak $m \leq$ dim(prostor funkcí $\mathbb{R}^n \to \mathbb{R}$). Lineární kombinace $\sum_{i=1}^{m} \gamma_i f_i(x) = 0$.

$$f_i(P_j) = \alpha^2\beta^2 \qquad \text{pro } i = j \tag{6}$$
$$f_i(P_j) = 0 \qquad \text{pro } i \neq j \tag{7}$$

$$\forall j : \sum_{i=1}^{m} \gamma_i f_i(P_j) = \alpha^2\beta^2\gamma_j = 0 \qquad \Rightarrow \qquad \forall j : \gamma_j = 0 \tag{8}$$

Z toho plyne, že funkce $f_1, f_2, \ldots f_m$ jsou lineárně nezávislé.

$$f_i(x) = ((x_1 - p_1)^2 + \cdots + (x_n - p_n)^2 - \alpha^2)((x_1 - p_1)^2 + \cdots + (x_n - p_n)^2 - \beta^2) \tag{9}$$
$$= (x_1^2 + \cdots + x_n^2 - 2p_1x_1 - \ldots - 2p_nx_n - \alpha^2)(x_1^2 + \ldots - 2p_1x_1 - \ldots - \beta^2) \tag{10}$$

p_i^2 se ztratí do α a β. Následuj rozbor případů po roznásobení:

$$(x_1^2 + \cdots + x_n^2)(x_1^2 + \cdots + x_n^2) \qquad 1 \tag{11}$$
$$(x_1^2 + \cdots + x_n^2)x_i \qquad n \tag{12}$$
$$x_i^2 \qquad n \tag{13}$$
$$x_ix_j \qquad \binom{n}{2} \tag{14}$$
$$x_i \qquad n \tag{15}$$
$$1 \qquad 1 \tag{16}$$
$$\tag{17}$$

Případ $(x_1^2 + \cdots + x_n^2)$ není potřeba, vyjádříme ho jako kombinaci x_i^2. Velikost lineárního obalu:

$$\binom{n}{2} + 3n + 2 = \frac{n(n-1)}{2} + \frac{6n}{2} + \frac{4}{2} = \frac{n^2 - 5nn + 4}{2} = \frac{(n+1)(n+4)}{2}$$

□

Věta Pro dvouvzdálenostní množinu na kouli platí:

$$\frac{n(n+1)}{2} \leq m_{sf}(n) \leq \frac{n(n+3)}{2}$$

Důkaz

Horní odhad (ostatní řádky nepotřebujeme, $(x_1^2 + \cdots + x_n^2)$ se na kouli posčítá na konstantu):

$$x_i^2 \qquad n \tag{18}$$

$$x_i x_j \qquad \binom{n}{2} \tag{19}$$

$$x_i \qquad n \tag{20}$$

$$\tag{21}$$

$$\binom{n}{2} + 2n = \frac{n(n-1)}{2} + \frac{4n}{2} = \frac{n^2+3n}{2} = \frac{n(n+3)}{2}$$

Dolní odhad (konstrukce 2-vzdálenostní množiny v $\mathbb{R}^n$):

Body budou všechny vektory délky n s dvěma jedničkovými souřadnicemi. Vzdálenost dvou bodů s 1 na různých souřadnicích je 2, zatímco vzdálenost bodů které se v jedné souřadnici shodují je $\sqrt{2}$.

Uvažujme nyní body v $\mathbb{R}^{n+1}$ místo v $\mathbb{R}^n$. Takových je $\binom{n+1}{2}$.

$\sum x_i^2 = 2 \Rightarrow$ všechny body leží na sféře[1]
$\sum x_i = 2 \Rightarrow$ všechny body leží v nadrovině

$$\left\{x | \sum x_i = 2\right\} \cap \mathbb{R}^{n+1} \simeq \mathbb{R}^n$$

Tedy máme 2-vzdálenostní množinu $\binom{n+1}{2}$ bodů na kouli v $\mathbb{R}^n$.

1.3 Fišerova nerovnost

Věta Nechť máme graf K_n a jeho hranově disjunktní rozklad na m úplných bipartitních grafů. Potom $m \geq n-1$.

Důkaz Označme si úplné bipartitní grafy $B_1, \ldots, B_m$ a X_k, Y_k jejich partity, přičemž jednotlivý B_i nemusí být pokrývat všechny vrcholy K_n. Mějme matici A_k pro graf B_k velikosti $n \times n$ definovanou:

$$a_{ij} = \begin{cases} 1 & \text{pokud } i \in X_k \text{ a } j \in Y_k \\ 0 & \text{jinak} \end{cases} \tag{22}$$

[1] x_i je i-tá souřadnice bodu x

Protože v každém nenulovém řádku jsou jedničky právě pro sousedy daného vrcholu v druhé partitě, jsou všechny nenulové řádky stejné (sousedství jsou stejná), A_k má tedy hodnost 1.

Nyní uvažme matici $A = A_1 + \ldots + A_m$. Hodnost součtu je nanejvýš rovna součtu hodností, proto $\text{rank}(A) \leq m$. Nyní budeme chtít dokázat, že $\text{rank}(A) \geq n - 1$:

Protože každá hrana grafu náleží právě jednomu B_k, je jednička právě na jednom z míst a_{ij} nebo a_{ji} (pozor, matice nejsou matice sousednosti – rozlišují partitu!). Na diagonále A jsou pak samé nuly. Sečtením $A + A^T$ získáme matici incidence K_n, tedy $A + A^T = J_n - I_n$.

Dále pro spor předpokládejme, že $\text{rank}(A) \leq n - 2$. Připíšeme k matici jeden řádek samých jedniček, čímž hodnost zvýšíme nanejvýš o 1. Protože ale A nemá plnou hodnost, existuje netriviální lineární kombinace sloupců, která dává $\vec{0}$ – nechť jsou její koeficienty zaznamenány ve vektoru $\vec{x} \in \mathbb{R}^n$ a tedy $A\vec{x} = \vec{0}$. Zároveň protože poslední řádek jsou samé jedničky, platí $\sum x_i \cdot 1 = 0$ a tedy také $J_n\vec{x} = 0$. Počítejme dvěmi způsoby:

$$x^T(A + A^T)x = x^T(J_n - I_n)x = x^T(J_n x) - x^T(I_n x) = 0 - x^T x = -\sum x_i^2 < 0 \tag{23}$$

$$x^T(A + A^T)x = x^T A^T x + x^T A x = 0^T x + x^T 0 = 0 \tag{24}$$

což dává spor. □

1.4 Dolní odhad na Ramseyovo číslo

Věta (Ramsey) $\forall n\ \exists N\ \forall G$ na $\geq N$ vrcholech má $\omega(G) \geq n$ nebo $\alpha(G) \geq n$.

Víme, že $R_2(n) = \min N \leq \binom{2n-2}{n-1}$. Konstrukcí si ukážeme dolní odhad.

Věta $R_2(n) \geq \binom{n-1}{3}$

Důkaz $|X| = n - 1$. Zkonstruujeme $G = \left(V = \binom{X}{3}, E = \{ab : |a \cap b| = 1, a, b \in V\}\right)$.

Klika v G je *skorodisjunktní systém podmnožin* $X \Rightarrow \omega(G) \leq |X| = n - 1$.

Vrcholy jsou nezávislé, pokud $|a \cap b| \in \{0, 2\}$ a velikost nezávislé množiny v G je tedy *sudo-licho město* $\Rightarrow \alpha(G) \leq |X| = n - 1$. □

2 Skalární součin

Mějme vektorový prostor $V = T^n$.

Definice (Skalární součin) $\langle x, y\rangle = \sum x_i y_i \quad (= \sum x_i \overline{y_i}$ nad $\mathbb{C})$

2.1 Ortogonální doplněk

Definice $M \subseteq T^n \quad M^\perp = \{x \mid \forall a \in M : \langle x, a\rangle = 0\}$ je ortogonální doplněk M.

Pozorování $\dim M^\perp = n - \dim \langle M\rangle$

Pozorování $(M^\perp)^\perp = \mathcal{L}M$

Důkaz „$\supseteq$“ jednuduché „$\subseteq$“ přes dimenze $\quad n - (n - k) = k = \dim M$ □

Definice (Součet podprostorů) $\mathcal{L}M + \mathcal{L}N = \mathcal{L}(M \cup N)$

Pozorování

$$\dim(\mathcal{L}M + \mathcal{L}N) + \dim(\mathcal{L}M \cap \mathcal{L}N) = \dim \mathcal{L}M + \dim \mathcal{L}N$$

Důsledek Podprostory $M, N << T^n : \dim M + \dim N > n \Rightarrow \dim M \cap N \geq 1 \Rightarrow \exists u \neq 0, u \in M \cap N$.

Důsledek Pro tělesa, ve kterých platí $\langle x, x \rangle \neq 0$ pro $x \neq 0$ platí:

$$M << T^n \Rightarrow M \cap M^\perp = \{0\} \Rightarrow \dim(M + M^\perp) = n \Rightarrow M + M^\perp = T^n$$

2.2 Sudo-sudo města

Definice $|X| = n$, $A_1, A_2, \ldots A_k \subseteq X$, $|A_i| \equiv 0 \mod 2$, $|A_i \cap A_j| \equiv 0 \mod 2$. Jaké největší může být $k = k(n)$?

Věta $k(n) \geq 2^{\frac{n}{2}}$

Důkaz Utvoříme páry – $2^{\frac{n}{2}}$ je počet podmnožin $\frac{n}{2}$ prvkové množiny. □

Věta $k(n) \leq 2^{\frac{n}{2}}$

Důkaz [2] $A_i \in GF(2^n)$. Nechť $M = \{A_1, A_2, \ldots A_k\}$ je maximální (co do inkluze) sudo-sudo město. Ukážeme že M je vektorový prostor. Vektory mají sudé průniky *(sudo-sudo město)* nad $GF(2)$ tedy platí $\forall x, y \in M : \langle x, y \rangle = 0$. Dále:

$$\emptyset \in M \tag{25}$$
$$\forall u \in M, \forall c \in GF(2) : c \cdot u \in M \tag{26}$$
$$\forall x, u, v \in M : \langle x, u + v \rangle = \langle x, u \rangle + \langle x, v \rangle = 0 + 0 = 0 \tag{27}$$
$$\forall u, v \in M : \langle u + v, u + v \rangle = \langle u, u \rangle + 2\langle u, v \rangle + \langle v, v \rangle = 0 + 0 + 0 = 0 \tag{28}$$

Když $M << GF(2)^n$ a $\dim M = k$, pak $|M| = 2^k$.

$$\forall x \in M : x \in M^\perp \quad \Rightarrow \quad M \subseteq M^\perp \quad \Rightarrow \quad \dim M \leq \dim M^\perp$$

$$k = \dim M \leq \dim M^\perp = n - k \quad \Rightarrow \quad 2k \leq n \quad \Rightarrow \quad k \leq \frac{n}{2}$$

□

2.3 Eulerovské a úplné bipartitní podgrafy

$G = (V, E)$ je souvislý graf. $V_G = \{$ spanning[3] podgrafy $G \}$

Tvrzení V_G je vektorový prostor nad $GF(2)$, místo stčítání vektorů je symetrická diference. $V_H \in GF(2)^E$.

TODO: Obrázek se symetrickou diferencí podgrafů.

Definice $\varepsilon_G = \{$ eulerovské podgrafy $\equiv \forall$ stupně sudé $\}$. Součtem dvou eulerovských podgrafů je eulerovský podgraf, tvoří tedy podprostor V_G.

[2] A_i budeme považovat za charakteristický vektor podmnožiny A_i v množině X.

[3] Česky též „napnuté“ – podgrafy obsahující všechny vrcholy grafu G (i kdyby některé z nich byly izolované).

Lemma $\dim \varepsilon_G = |E| - n + 1$

Důkaz Vybereme si libovolnou kostru T grafu G. Pro každou hranu, která není v kostře existuje právě jedna elementární kružnice K_e určená touto hranou. $\{K_e \mid e \in E(G) - E(T)\}$ tvoří lineárně nezávislé vektory. Lze dokázat, že tvoří bázi ε_G.

Z toho $\dim \varepsilon_G = |E| - n + 1$, což je počet hran mimo kostru. □

Definice $\beta_G = \{$ úplné bipartitní spanning podgrafy G $\}$. β_G je prostor všech řezů v G.

Lemma $\beta_G << V_G$, $\beta_G = \langle \{$ hvězdy $\} \rangle$

Důkaz Každý úplný bipartitní podgraf lze zapsat jako symetrickou diferenci hvězd. Vezmeme hvězdy ze všech vrcholů v jedné z partit. Mezi těmito vrcholy se hrany vyruší, mezi vrcholy z druhé partity žádné nevedou a všude jinde ano.

Mám-li dva různé úplné bipartitní podgrafy, rozepíšu si je na součet hvězd a výsledkem musí být dle výše uvedeného opět úplný bipartitní podgraf.

Věta $\varepsilon_G^\perp = \beta_G$. Tedy eulerovské podgrafy jsou ortogonálním doplňkem úplných bipartitních podgrafů.

Důkaz Vezmeme si $H \in \varepsilon_G$ eulerovský podgraf a $u \in V(G)$. H_u označíme hvězdu z vrcholu u. Platí $\langle H, H_u \rangle = \deg_H u$, neboť hvězda obsahuje všechny hrany jdoucí z u a žádné jiné. Protože v H vychází z každého vrcholu sudý počet hran a počítáme nad $GF(2)$:

$$\forall u : \langle H, H_u \rangle = 0 \quad \Rightarrow \quad \forall B \in \beta_G : \langle H, B \rangle = 0 \quad \Rightarrow \quad H \in \beta_G^\perp \quad \Rightarrow \quad \varepsilon_G \subseteq \beta_G^\perp$$

Naopak, každý podgraf H, který je kolmý na všechny hvězdy je nutně eulerovský:

$$\forall u : \langle H, H_u \rangle = 0 \quad \Rightarrow \quad \forall u : \deg_H u \equiv 0 \mod 2 \quad \Rightarrow \quad H \in \varepsilon_G \quad \Rightarrow \quad \beta_G^\perp \subseteq \varepsilon_G$$

Tedy $\varepsilon_G = \beta_G^\perp$, protože $\varepsilon_B^\perp = \left(\beta_G^\perp\right)^\perp = \beta_G$. □

Důsledek $\dim \varepsilon_G = \dim \beta_G^\perp = |E| - n + 1$.

Věta $M \subseteq GF(2)^n \quad \Rightarrow \quad (1, 1, \ldots, 1) \in \langle M \rangle + M^\perp = \langle M \cup M^\perp \rangle$

Důkaz $\langle M \rangle \cap M^\perp$

(a) $\dim(\langle M \rangle \cap M^\perp) = 0 \quad \Rightarrow \quad \dim(\langle M \rangle + M^\perp) = k + n - k = n \Rightarrow \langle M \rangle + M^\perp = GF(2)^n \Rightarrow (1, 1, \ldots, 1) \in \langle M \rangle + M^\perp$

(b) $\dim(\langle M \rangle \cap M^\perp) > 0 \quad \Rightarrow \quad \exists u \in \langle M \rangle \cap M^\perp$
$\forall u \in \langle M \rangle \cap M^\perp : \langle u, u \rangle = 0 \Rightarrow \sum u_i^2 \equiv 0 \mod 2 \Rightarrow \sum u_i = \langle u, (1, 1, \ldots, 1) \rangle$
nad $GF(2)$ platí $u_i^2 = u_i$
$\Rightarrow (1, 1, \ldots, 1) \in (\langle M \rangle \cap M^\perp)^\perp = \langle M \rangle^\perp + (M^\perp)^\perp = M^\perp + \langle M \rangle$

□

Věta $\forall G \; \exists V_1, V_2, \; V_1 \dot\cup V_2 = V(G)$ t. že $G[V_1]$ i $G[V_2]$ mají všechny stupně sudé.

Důkaz $M = \varepsilon_G << V_G$

$G = (1, 1, \ldots, 1) \in \varepsilon_G + \varepsilon_G^\perp = \varepsilon_G + \beta_G$ □

Důsledek $\exists H \in \varepsilon_G \; \exists B \in \beta_G : G = H + B$ (tedy každý graf lze zapsat jako symetrickou diferenci eulerovského podgrafu a hranového řezu).

3 Shannonova kapacita a Lovászova ϑ funkce

3.1 Shannonova kapacita

Definice Domečkový součin grafů G a H je graf $G \boxtimes H$ takový, že:

$$V(G \boxtimes H) = \{(u, v) \mid u \in V(G), v \in V(H)\}$$

$$E(G \boxtimes H) = \{((u_1, v_1), (u_2, v_2))\} \begin{cases} u_1 = u_2, v_1 \sim v_2 & \text{(sousedí)} \\ v_1 = v_2, u_1 \sim u_2 \\ v_1 \sim v_2, u_1 \sim u_2 \end{cases}$$

Motivací ke zkoumání Shannonovy kapacity grafu může být posílání zpráv. Potřebujeme-li kód, který opraví jednu chybu, můžeme na C_5 najít pouze dvě kódová slova ($\alpha(C_5) = 2$). Naproti tomu, $\alpha(C_5 \boxtimes C_5) = 5 > 2^2$. Posílání zpráv ve větších blocích tedy může být efektivnější.

Definice Shannonova kapacida grafu:

$$\Theta(G) = \sup_{i \geq 1} (\alpha(G^i))^{1/i}$$

Lemma $\Theta(G \boxtimes H) \geq \Theta(G) \cdot \Theta(H)$

Důkaz Vezměme si maximální nezávislou množinu v G a maximální nezávislou množinu v H. Z vlastností domečkového součinu plyne, že mezi vrcholy $G \boxtimes H$ zkombinovanými z těchto množin nepovede žádná hrana a tudíž budou tvořit nezávislou množinu velikosti alespoň $\alpha(G) \cdot \alpha(H)$.

Pozorování $\Theta(G^i) \geq \Theta(G)^i$

Důkaz Postupnou iterací lemmatu.

Definice Ortonormální reprezentace grafu G je funkce $\rho : V(G) \to \mathbb{R}^d$, $\|\rho(v)\| = 1$. Pro každé $(u, v) \notin E(G)$ platí $\rho(u) \perp \rho(v)$, neboli $\langle \rho(u), \rho(v) \rangle = 0$.

Definice Lovászova theta funkce:

$$\vartheta(G, \rho) = \max_{v \in V(G)} \frac{1}{\langle \rho(v), e_1 \rangle^2}$$

Vezmeme si reprezentaci grafu C_5 ta se skládá z pěti vektorů $v_1, \ldots, v_5$ a jednoho speciálního vektoru e_1, vůči kterému budeme ostatní vztahovat. Protože se jedná o ortonormální reprezentaci, musí každé dva nesousední vrcholy z C_5 svírat pravý úhel. Představíme si „paraplíčko“, kde vektor e_1 tvoří držadlo a vektory $v_1, \ldots, v_5$ jsou okolo něj a tvoří dráty deštníku. Představme si dále, že deštník roztahujeme, dokud nebudou každé dva nesousední dráty svírat pravý úhel. Pak můžeme spočíst úhel mezi dráty a držadlem, který vyjde $\langle \rho(v), e_1 \rangle = 5^{-\frac{1}{4}}$. Z toho:

$$\vartheta(C_5, \rho) = \sqrt{5}$$

Definice $\vartheta(G) = \min_{\rho \text{ ONR}} \vartheta(G, \rho)$

Z toho plyne $\vartheta(C_5) \leq \sqrt{5}$. Kdybychom ještě znali vztah mezi $\Theta(G)$ a $\vartheta(G)$, měli bychom vyhráno. Tuto charakterizaci přináší následující věta.

Věta $\Theta(G) \leq \vartheta(G)$

Důkaz K důkazu věty budeme potřebovat dvě pomocná lemmata.

Lemma (O vztahu ϑ a α) Nechť H je graf a ρ nějaká jeho ortonormální reprezentace. Pak $\alpha(H) \leq \vartheta(H, \rho)$.

Důkaz Nechť A je nějaká nezávislá množina H. Zřejmě vektory $\rho(v)$ pro $v \in A$ tvoří ortonormální systém vektorů. Přáli bychom si odhadnout, jak velký bude skalární součin $\langle \rho(v), e_1 \rangle^2$, z čehož nám vztah vyplyne.

Nechť u je libovolný vektor a b_i jsou vektory ortonormální báze. Chceme-li vyjádřit vektor u proti bázi b_i, získáme i-tou souřadnici skalárním součinem $\langle b_i, u \rangle$ (můžeme si to představovat tak, že z vektorů b_i složíme matici předhocu). Použijeme-li Pythagorovu větu, získáme:

$$||u||^2 = \sum_{i=1}^{n} \langle b_i, u \rangle^2 \tag{29}$$

Pokud aplikujeme tento poznatek na vektory ρv rozšířené na bázi (což jistě lze), a vektor e_1, rovnost se změní na nerovnost (nezajímají nás přidané vektory) a s vědomím, že všechny vektory máme ortonormální, získáme:

$$1 = ||u||^2 \geq \sum_{v \in A} \langle \rho(v), e_1 \rangle^2 \tag{30}$$

Tedy existuje alespoň jeden vrchol w, že $\langle \rho(w), e_1 \rangle^2 \leq 1/|A|$ a dosadíme-li do zlomku z definice ϑ, získáme odhad $\alpha(G) = |A| \leq \vartheta(H, \rho)$, což jsme chtěli dokázat. □

Lemma (O součinu ϑ) Nechť H_1 a H_2 jsou grafy, a ρ_i jejich ortonormální reprezentace. Potom existuje ortonormální reprezentace ρ silného součinu $H_1 \boxtimes H_2$, pro niž platí $\vartheta(H_1 \boxtimes H_2, \rho) = \vartheta(H_1, \rho_1) \cdot \vartheta(H_2, \rho_2)$.

Důkaz Zadefinujme si funkci ρ pro vrcholy v_i následovně:

$$\rho(v) = \rho_1(v_1) \otimes \rho_2(v_2) \tag{31}$$

Kde operace $\otimes$ je tenzorový součin vektorů, tedy pro $x \in \mathbb{R}^n$ a $y \in \mathbb{R}^m$ je výsledek vektor $z \in \mathbb{R}^{mn}$, který obsahuje všechny součiny $x_i y_i$.

Zbývá pouze ověřit, že dělá správnou věc. Podívejme se tedy nejdříve na skalární součin:

$$\langle x \otimes y, x' \otimes y' \rangle = \langle x | x' \rangle \cdot \langle y | y' \rangle \tag{32}$$

Pokud levou a pravou stranu zvlášť rozepíšeme, je vidět, že roznásobením sum napravo získáme sumu nalevo a rovnost tedy platí:

$$\sum_{ij} (x_i y_j) \cdot (x'_i y'_j) = \left(\sum_i x_i x'_i \right) \left(\sum_j y_j y'_j \right) \tag{33}$$

Zde již jednoduchou úvahou zjistíme, že ρ je stále ortonormální reprezentace: zjevně pro kolmé vektory jsou opět kolmé, a všechny vektory si zachovají délku 1. Nyní se stačí podívat, co se stane s ϑ funkcí, rozepišme si ji ted z definice:

$$\begin{aligned}
\vartheta(H_1 \boxtimes H_2, \rho) &= \max_{v \in V(H_1 \boxtimes H_2)} \frac{1}{\langle \rho(v), e_1 \rangle^2} \\
&= \max_{v \in V(H_1 \boxtimes H_2)} \frac{1}{\langle \rho_1(v_1) \otimes \rho_2(v_2), e_{11} \otimes e_{12} \rangle^2} \\
&= \max_{v \in V(H_1 \boxtimes H_2)} \frac{1}{\langle \rho_1(v_1), e_{11} \rangle^2 \cdot \langle \rho_2(v_2), e_{12} \rangle^2} \\
&= \max_{v_1 \in V(H_1)} \frac{1}{\langle \rho_1(v_1), e_{11} \rangle^2} \cdot \max_{v_2 \in V(H_2)} \frac{1}{\langle \rho_2(v_2), e_{12} \rangle^2} \quad = \vartheta(H_1, \rho_1) \cdot \vartheta(H_2, \rho_2)
\end{aligned}$$

A lemma je dokázáno. □

Důkaz (Věty o vztahu Θ a ϑ)

$$\alpha(G^i) \leq \vartheta(G^i) \leq \vartheta(G)^i$$

První nerovnost plyne z lemma o vztahu ϑ a α. Druhá plyne z opakovaného použití lemma o součinu ϑ. □

Lemma (O dvojité kapacitě) $\Theta(G + \overline{G}) \geq \sqrt{2|G|}$

Důkaz Ukážeme, že $\alpha((G + \overline{G})^2) \geq 2|G|$.

$$V_{G+\overline{G}} = \{v_1, ..., v_n, v'_1, ..., v'_n\}$$

Vezeme graf $(G + \overline{G})^2$ a najdeme v něm nezávislou množinu A:

$$A = \begin{Bmatrix} (v_1, v'_1), (v_2, v'_2), \dots \\ (v'_1, v_1), (v'_2, v_2), \dots \end{Bmatrix}$$

Velikost A je zřejmě $2|G|$ a z definice Shannonovy kapacity dostaneme:

$$\Theta(G + \overline{G}) \geq \sqrt{2|G|}$$

□

3.2 Funkční reprezentace grafu

Definice Nechť G je graf, $\mathcal{F}$ je systém funkcí, X množina reprezentantů a $\mathbb{F}$ těleso. Pak pro vrchol v mějme $c_v \in X$ a $f_v \in \mathcal{F}$, že $f_v : X \to \mathbb{F}$ a platí:

1. $f_v(c_v) \neq 0$
2. $uv \notin E_G \Rightarrow f_u(c_v) = 0$

Definice Dimenzi $\mathcal{F}$ definujeme jako $\dim \mathcal{L}(\{f_v\})$, tedy chápeme funkce jako vektorový prostor.

Lemma (O vztahu α a $\dim \mathcal{F}$) G má reprezentaci $\mathcal{F}$, pak $\alpha(G) \leq \dim \mathcal{F}$.

Důkaz Nechť A je nezávislá v G. Pak $\{f_a\}_{a\in A}$ je lineárně nezávislá, stejně jako $\{c_a\}_{a\in A}$. Vyhodnotím reprezentující funkci v bodech A.

$$M = \begin{pmatrix} f_1(c_1) & f_2(c_2) & \dots \\ f_2(c_1) & f_2(c_2) & \dots \\ \vdots & & \end{pmatrix} \tag{34}$$

Matice M bude mít na diagonále nenuly a všude jinde nuly. Tím pádem jsou její řádky lineárně nezávislé a její dimenze je $|A|$. Navíc zjevně $\dim M \leq \dim \mathcal{F}$. □

Lemma (O dimenzi součinu reprezentací) Pokud G_1 má reprezentaci $\mathcal{F}_1$, G_2 reprezentaci $\mathcal{F}_2$ nad stejným tělesem, pak $G = G_1 \boxtimes G_2$ má reprezentaci $\mathcal{F}$ a $\dim \mathcal{F} \leq \dim \mathcal{F}_1 \cdot \dim \mathcal{F}_2$.

Důkaz Definujeme:

$$\begin{aligned} X &= X_1 \times X_1 \\ c_{(v_1,v_2)} &= (c_{v_1}, c_{v_2}) \\ f_{(v_1,v_2)}((x_1,x_2)) &= f_{v_1}(x_1) \cdot f_{v_2}(x_2) \end{aligned}$$

Ověříme, že výše uvedené je funkční reprezentace a vezmeme si B_1 bázi $\mathcal{F}_1$ a B_2 bázi $\mathcal{F}_2$. Pak $\{b_1 \otimes b_2\}_{b_1\in B_1, b_2\in B_2}$ generuje celý prostor $\mathcal{F}$ a tudíž:

$$\dim \mathcal{F} \leq |B_1| \cdot |B_2| = \dim \mathcal{F}_1 \cdot \dim \mathcal{F}_2$$

□

Lemma (O vztahu Θ a $\dim \mathcal{F}$) G má reprezentaci $\mathcal{F}$, pak $\Theta(G) \leq \dim \mathcal{F}$.

Důkaz

$$\Theta(G) = \sup_i \alpha(G^i)^{1/i} \leq \sup_i (\dim f.r.(G^i))^{1/i} \leq \sup_i \dim f.r.(G) = \dim f.r.(G)$$

První nerovnost plyne z lemma o vztahu α a $\dim \mathcal{F}$, druhá z lemma o dimenzi součinu reprezentací. □

Věta Existuje G, H, že $\Theta(G+H) > \Theta(G) + \Theta(H)$

Důkaz Zvolím G takový, že $V_G = \binom{S}{3}$, $S = \{1, \dots, s\}$ a $E_G = \{(A,B) : |A \cap B| = 1\}$.

Reprezentaci vytvoříme nad tělesem $\mathbb{F} = \mathbb{Z}_2$, $X = \mathbb{Z}_2^s$:

$$\begin{aligned} c_A &= \text{charakteristický vektor } A \\ f_A(x) &= \sum_{a\in A} x_a \end{aligned}$$

Ověříme, že se jedná o funkční reprezentaci a všimneme si, že každá funkce f_A je kombinace tří funkcí $b_i(x) = x_i$, přičemž funkcí b_i je s.

$$\dim f.r.(G) \leq s \qquad \Rightarrow \qquad \Theta(G) \leq s$$

Dále pro $H = \overline{G}$ zvolíme reprezentaci pro $\mathbb{F} = \mathbb{R}$, $X = \mathbb{R}^s$:

$$c_A = \text{charakteristický vektor } A$$
$$f_A(x) = (\sum_{a \in A} x_a) - 1$$

Opět ověříme, že se jedná o funkční reprezentaci.

$$\dim f.r.(\overline{G}) \leq s + 1 \qquad \Rightarrow \qquad \Theta(\overline{G}) \leq s + 1$$

$$\Theta(G + \overline{G}) \geq \sqrt{2\binom{s}{3}} > 2s + 1 \geq \Theta(G) + \Theta(\overline{G})$$

První nerovnost platí z lemma o dvojité kapacitě a ostrou nerovnost musíme splnit, aby věta platila. Zvolíme si tedy $s \geq 16$. □

Definice Obecná poloha vektorů množiny $\check{N}$ v $\mathbb{R}^d$ je taková, že libovolná podmnožina velikosti $\leq d$ je lineárně nezávislá.

Definice Lokálně obecná poloha vektorů reprezentace v $\mathbb{R}^d$ na grafu G jsou takové vrcholy, že $\rho(\overline{N(v)})$ jsou lineárně nezávislé.

Věta Pro G s $|G| = n$ jsou následující tvrzení ekvivalentní:

1. G má ortogonální reprezentaci v $\mathbb{R}^d$ v obecné poloze.
2. G má ortogonální reprezentaci v $\mathbb{R}^d$ v lokálně obecné poloze.
3. G je $(n - d)$-souvislý.

4 Vlastní čísla grafu

4.1 Vlastní čísla grafu

Definice Nechť A je čtvercová matice. Potom pokud pro nějaké λ a x netriviální platí, že $Ax = \lambda x$ říkáme, že λ je vlastní číslo A a x je vlastní vektor příslušící k λ.

Definice Spektrum matice A je množina množina jejích vlastních čísel. Značíme $\mathrm{Sp}(A) = \{\lambda_1, \ldots, \lambda_n\}$.

Definice Podprostorem generovaným vlastním číslem číslem λ rozumíme $V_\lambda = \{u | Au = \lambda u\}$. Geometrická násobnost λ je poté dimenze tohoto prostoru V_λ.

Tvrzení V_λ je vektorový prostor. **Důkaz** Stačí dokázat uzavřenost. Pro $u, v \in V_\lambda$ počítejme:

$$A(u+v) = Au + Av = \lambda u + \lambda v = \lambda(u+v) \tag{35}$$

Tedy i $u+v \in V_\lambda$. □

Tvrzení Vlastní čísla matice A lze vypočítat jako kořeny rovnice $\det(A - \lambda \cdot E) = 0$.

Důkaz Z definice počítejme:

$$Au = \lambda u \tag{36}$$
$$Au - \lambda u = \vec{0} \tag{37}$$
$$(A - \lambda)u = \vec{0} \tag{38}$$
$$\det(A - \lambda E) = 0 \tag{39}$$

Přičemž v posledním kroku využíváme faktu, že pro součin netriviálního vektoru s maticí musí být matice singulární, aby mohl vyjít nulový vektor a tudíž můžeme přejít k determinantu. □

Definice Polynomu $P_A(\lambda) = \det(A - \lambda \cdot E)$ říkáme charakteristický polynom.

Definice Násobnosti kořene λ v polynomu P_A říkáme *algebraická násobnost*.

Věta Nechť $GN(\lambda)$ a $AN(\lambda)$ značí geometrickou, resp. algebraickou násobnost λ. Potom platí:

$$GN(\lambda) \geq 1 \Leftrightarrow \lambda \in \mathrm{Sp}(A) \Leftrightarrow AN(\lambda) \geq 1 \tag{40}$$
$$\text{a} \qquad GN(\lambda) \leq AN(\lambda) \tag{41}$$

Důkaz *(bez důkazu)*

Definice Hermitovská transpozice matice A je matice A^*, taková, že $A^*_{ij} = \overline{A_{ji}}$.

Definice Matice $A \in \mathbb{C}^{n\times n}$ je *normální*, pokud $AA^* = A^*A$.

Věta Matice A má ortonormální bázi složenou z vlastních vektorů právě tehdy, když je A normální.

Důkaz

„⇒“ Nechť x_i jsou vlastní vektory příslušející vlastním číslům λ_i tvořící ortonormální bázi. Z ortonormality plyne, že $XX^* = E$, kde X má ve sloupcích x_i. Podívejme se nyní jak vypadá matice X^*AX:

$$X^*AX = \underbrace{\left(\begin{array}{c} \vdots \\ \hline x_j^* \\ \hline \vdots \end{array}\right)}_{=X^*} \underbrace{\left(\begin{array}{c|c|c} \dots & \lambda_i x_i & \dots \end{array}\right)}_{=AX} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \tag{42}$$

Přičemž druhá matice vznikla ze vztahu $Ax = \lambda x$, přičemž jsme vynásobili všechny vektory naráz díky tomu, že byly v matici. Poslední rovnost plyne z pozorování, že

na pozici ij nalezneme výraz $x_j^* \lambda_i x_i = x_j^* x_i \lambda_i$ a protože vektory x_l tvoří ortonormální bázi, jsou nula pokud je $i \neq j$ a jedna jinak.

Nyní víme, že $X^*AX = D$, kde D je nějaká (konkrétní) diagonální matice. Nyní již snadno vypočteme elementárními úpravami:

$$X^*AX = D \quad \Rightarrow \quad AX = XD \quad \Rightarrow A = XDX^*$$
$$A \cdot A^* = XD\underbrace{X^* \cdot X}_{E}D^*X^* = XDD^*X^* = XD^*DX^* = XD^*\underbrace{X^* \cdot X}_{E}DX^* = A^* \cdot A$$

Přičemž jediná finta, kterou jsme použili je, že $DD^* = D^*D$, což je zřejmě pravda, protože jsou to diagonální matice.

„⇐“ **TODO:** gavento byl jen pochybny naznak

Věta Nechť $A_i \in \mathbb{C}^{n \times n}$ a $\forall i, j$ jsou A_i a A_j normální a $A_i A_j = A_j A_i$. Potom existuje společná ortonormální báze z vlastních vektorů.

Důkaz TODO: Gavento

Věta Nechť A je hermitovská matice, tedy $A = A^*$. Potom všechna její vlastní čísla jsou reálná.

Důkaz Víme, že existuje nějaké D diagonální s vlastními čísly na diagonále a X, že $X^*AX = D$. Dále počítáme:

$$D^* = (X^*(AX))^* = (AX)^*X = X^*A^*X = X^*AX = D \tag{43}$$

A komplexní sdružení tedy nesmí udělat žádnou operaci, tedy jsou vlastní čísla reálná. □

4.2 Moorovy grafy

Motivací nechť jsou r-regulární grafy bez krátkých cyklů (troj- a čtyř-úhelníků). Triviální konstrukce nám dává odhad na počet vrcholů: **TODO:** obrázek konstrukce

$$|V| \geq 1 + r + r(r-1) = r^2 + 1 \tag{44}$$

Definice Moorův graf je takový r-regulární graf bez troj- a čtyř-úhelníků, kde platí v (44) rovnost.

Věta Moorův graf existuje pro $r = 1, 2, 3, 7$, pro $r = 57$ se neví a pro žádné další r neexistuje.

Důkaz (Idea) Mějme graf G Moorův a A jeho matici sousednosti. Zapišme druhou mocninu A jako stupeň na diagonále a prohozené 0 a 1 jinde a upravme:

$$A^2 = rE + \mathbf{0} + \mathbf{1}(J - A - E) \tag{45}$$
$$A^2 = rE - J - A - E \tag{46}$$
$$A^2 + A + (1-r)E = J \tag{47}$$

Dále pro nějaké $\lambda \in \mathrm{Sp}(A)$:

$$A^2x = AAx = A\lambda x = \lambda Ax = \lambda\lambda x = \lambda^2 x \tag{48}$$

A dosadíme (47) za A:

$$Jx = (A^2 + A + (1-r)E)x = (\lambda^2 + \lambda + (1-r))x \tag{49}$$

A tedy $(\lambda^2 + \lambda + 1 - r) \in \mathrm{Sp}(J)$. Vlastní čísla matice J (matice samých jedniček) ale známe, jsou to $\{0^{(n-1)}, n^{(1)}\}$. Zjevně pro $\lambda = r$ vyjde vlastní číslo n, je tedy potřeba vyřešit kvadratickou rovnici s parametrem r:

$$\lambda^2 + \lambda + 1 - r = 0 \tag{50}$$

Jak na to půjdeme? Vyjádříme si λ známým vzorečkem pro kořeny:

$$\lambda_{1,2} = \frac{-1 \pm \sqrt{1 - 4(1-r)}}{2} = \frac{-1 \pm \sqrt{4r-3}}{2} \tag{51}$$

Násobnost označíme m_1, m_2. Protože stopa matice je suma vlastních čísel včetně násobností, platí dále rovnice (protože matice sousednosti A má na diagonále vždy nuly):

$$\mathrm{Tr}(A) = r + m_1\lambda_1 + m_2\lambda_2 = 0 \tag{52}$$

Pro další úravy označme odmocninu z diskriminantu jako $\sqrt{\cdot}$. Nejdříve upravíme do formy (násobení dvěma a přeskupení):

$$2r - r^2 + \sqrt{\cdot}(m_1 - m_2) = 0 \tag{53}$$

Všimneme si, že $r \in \mathbb{N}$, tedy máme dvě možnosti:

1. $\sqrt{\cdot} \in \mathbb{Q}$: potom $m_1 = m_2$ a tedy $r = 2$.
2. $\sqrt{\cdot} = s^2 \in \mathbb{Q}$ a $s \in \mathbb{N}$. Po menších úpravách lze zjistit, že $s \in \{1, 3, 5, 15\}$, což dává $r \in \{1, 3, 7, 57\}$.

□

4.3 Silně regulární grafy

Definice Silně regulární graf je d-regulární, $\forall$ hranu $xy \in E$ $\exists! e$ vrcholů $u : ux, uy \in E$ a $\forall$ nehranu $xy \notin E$ $\exists! f$ vrcholů $u : ux, uy \in E$.

Abychom mohli zanedbat triviální případy, dodáváme $f > 0$ a $G \neq K_n$. Příkladem silně regulárního grafu je úplný bipartitní graf se stejně velkými partitami ($e = 0$). Nejmenším nebipartitním silně regulárním grafem je pětiúhelník ($e = 0$, $f = 1$).

Věta G je silně regulární graf s parametry d, e, f a n vrcholy. Potom:

(a) Zafixujeme f: $e = f - 1$; $d = 2f$; $n = 4f + 1$

nebo

(b) $\exists s \in \mathbb{Z}$, že platí $(e-f)^2 - 4(f-d) = s^2$
a výraz $\frac{d}{2fs}((d-1+f-e)(s+f-e)-2f)$ je přirozené číslo

Důkaz Nechť G je silně regulární, A je jeho matice sousednosti. $(A^2)_{ij} = e$, pokud $A_{ij} = 1$. Na ostatních souřadnících bude f, na diagonále d (to plyne z jednoduchého pozorování počtu sledů délky 2).

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

$$A^2 = dI + eA + f(J - I - A) = fJ + (d-f)I + (e-f)A \tag{54}$$
$$A^2 + (f-e)A + (f-d)I = fJ \tag{55}$$
$$\lambda^2 + (f-e)\lambda + (f-d) \to \mathrm{Sp}(fJ) \qquad \lambda \in \mathrm{Sp}\, A \tag{56}$$

Víme, že vlastní čísla jedničkové matice J jsou $\mathrm{Sp}(J) = \{n, 0^{n-1}\}$. Proto $\mathrm{Sp}(fJ) = \{fn, 0^{n-1}\}$. Dále víme, že d je vlastním číslem matice A, neboť graf G je d-regulární.

$$d^2 + (f-e)d + (f-d) \in \mathrm{Sp}(fJ) \tag{57}$$
$$d^2 + (f-e)d + (f-d) = fn \tag{58}$$
$$\tag{59}$$

$$\lambda \in \mathrm{Sp}(A) - \{d\} \Rightarrow \lambda^2 + (f-e)\lambda + (f-d) = 0 \tag{60}$$
$$\lambda_{1,2} = \frac{e-f \pm \sqrt{(f-e)^2 - 4(f-d)}}{2} \qquad \sqrt{(f-e)^2 - 4(f-d)} = s \tag{61}$$

$$\lambda_1 = \frac{e-f+s}{2} \qquad \lambda_2 = \frac{e-f-s}{2}$$

Matice A má vlastní čísla d (1-násobné), λ_1 (p-násobné) a λ_2 (q-násobné).

(1) $1 + p + q = n$ (celkový počet vlastních čísel)

(2) $d + p\lambda_1 + q\lambda_2 = \mathrm{Tr}\, A = 0$ (stopa[4] matice A je 0)
$d + p\left(\frac{e-f+s}{2}\right) + q\left(\frac{e-f-s}{2}\right) = 0$
$d + \left(\frac{p+q}{2}\right)(e-f) + \left(\frac{s}{2}\right)(p-q) = 0$

[4]Stopou (čtvercové) matice rozumíme součet čísel na diagonále. Je známo, že součet vlastních čísel (včetně násobností) je roven stopě matice. Značíme ji $\mathrm{Tr}\, A$.

(3) $d^2 + p\lambda_1^2 + q\lambda_2^2 = \operatorname{Tr} A^2 = nd$ (vlastní čísla matice A^2 jsou druhé mocniny vlastních čísel matice A).

(a) $s \notin Q \Rightarrow p = q \quad d + p(e-f) = 0 \Rightarrow p = \frac{d}{f-e} \Rightarrow (f-e)|d$
$f - e > 0 \quad n = 1 + 2p = 1 + \frac{2d}{f-e}$ (z rovnice (1))

Pokud $f - e = 1$, pak $e = f - 1$ (což chceme).
Pokud $f - e = 2$, pak $n = 1 + d$ a $G = K_{d+1}$, ale úplné grafy jsme si zakázali.
Pokud $f - e > 2$, pak $n < 1 + d$, což je nesmysl.

$e = f - 1 \quad \Rightarrow \quad n = 2d + 1$
$d^2 + d + (f - d) = f(2d + 1) \quad \Rightarrow \quad d = 2f \quad \Rightarrow \quad n = 4f + 1$

(b) $s \in \mathbb{Q} \Rightarrow s \in \mathbb{N}$
TODO: Prý pokračování na cvičení, nemůžu ho ale najít. Já taky ne.

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

□

Věta (Friendship theorem) Nechť $G = (V, E)$ je graf, že každé dva vrcholy u, v mají právě jednoho společného souseda. Pak existuje u, že $\deg(u) = n - 1$.

Neboli Friendship theorem tvrdí, že takový silně regulární graf musí vypadat jako mlýn (hromádka trojúhelníků, které se stýkají v jednom centrálním vrcholu). **TODO:** obrázek

Důkaz Nejprve si připomeňme, co jsou to konečné projektivní roviny.

Definice Konečná projektivní rovina je množina bodů a přímek, že:

1. Každé dvě přímky sdílejí právě jeden bod.
2. Každé dva body spojuje právě jedna přímka.
3. Existují 4 body a žádná přímka neprotíná více než dva z nich.

Nyní si označme symbolem $N(v)$ množinu sousedů vrcholu v. Všimneme si, že sousedství pro náš graf přesně odpovídají přímkám v KPR a body jsou body. Protože ale třetí podmínka by znamenala, že naše věta neplatí, budeme si přát, aby to KPR nebyla – pak snadno najdeme vrchol, který je spojený s každým dalším.

Pro spor tedy předpokládejme, že graf KPR je. Protože v KPR mají všechny přímky stejnou mohutnost, je také d-regulární. Navíc každé u, v má právě jednoho společného souseda, což znamená, že G je silně regulární s parametry $e = f = 1$.

Podle předchozí věty to ověříme: možnost (a) nastat nemůže, protože $e = f$. Počítejme tedy, že nastala možnost (b). Protože je to KPR řádu m, tak $d = m + 1$ a $n = m^2 + m + 1$.

$$(e - f)^2 - 4(f - d) = 0^2 - 4 - 4(m + 1)) = s^2 \tag{62}$$
$$4m = s^2 \tag{63}$$
$$s = 2\sqrt{m} \tag{64}$$

A ověříme celočíselnost polynomu p s tím, že $t := s/2 = \sqrt{m}$, tedy $s = 2t$ a $m = t^2$:

$$p = \frac{d}{2fs}((d-1+f-e)(s+f-e)-2f) \tag{65}$$

$$= \frac{m+1}{4t}((m+1+0)(2t+0)-2) \tag{66}$$

$$= \frac{(t^2+1)(t^3-1)}{2t} \tag{67}$$

Což má být přirozené číslo. To je pravda zřejmě jenom pro $t = 1$, tedy $n = 3$ a pokud náš graf není trojúhelník, jde to spor. Pokud to trojúhelník je, splňuje žádanou vlastnost triviálně. □

4.4 Raileighův princip a proplétání

Věta (Raileighův princip) Nechť A je matice s ortonormální bazí z vlastních vektorů x_i a vlastními čísly $\lambda_i \geq \lambda_k$. Potom:

1. $x \in \langle x_1, \ldots, x_k \rangle \Rightarrow x^*Ax \geq \lambda_k x^*x$
2. $x \in \langle x_k, \ldots, x_n \rangle \Rightarrow x^*Ax \leq \lambda_k x^*x$

Důkaz $x \in \langle x_1, \ldots, x_k \rangle \Rightarrow x = \sum_{i=1}^{k} \alpha_i x_i$

$$x^*Ax = x^*(Ax) = x^*\left(A \cdot \sum_{i=1}^{k} \alpha_i x_i\right) = x^*\left(\sum_{i=1}^{k} \alpha_i A x_i\right) = x^*\left(\sum_{i=1}^{k} \alpha_i \lambda_i x_i\right) =$$

$$= \sum_{i=1}^{k} \alpha_i \lambda_i x^* x_i = \sum_{i=1}^{k} \alpha_i \lambda_i \left(\sum_{j=1}^{k} \alpha_j x_j\right)^* x_i = \sum_{i=1}^{k} \alpha_i \lambda_i (\alpha_i x_i)^* x_i =$$

$$= \sum_{i=1}^{k} \lambda_i \underbrace{\alpha_i \overline{\alpha_i}}_{\geq 0} \geq \sum_{i=1}^{k} \lambda_k \alpha_i \overline{\alpha_i} = \lambda_k \sum_{i=1}^{k} \alpha_i \overline{\alpha_i} = \lambda_k x^*x$$

Poslední rovnost plyne z následujícího:

$$\lambda_k x^*x = \left(\sum_{i=1}^{k} \alpha_i x_i\right)^* \left(\sum_{i=1}^{k} \alpha_i x_i\right) = \sum_{i=1}^{k} \alpha_i \overline{\alpha_i}$$

Druhou nerovnost dokážeme analogicky. □

Věta (Věta o proplétání) Nechť A a B jsou matice takové, že B vznikla z A vymazáním nějakého řádku a sloupce. Potom pro vlastní čísla λ_i, μ_i matic A, B platí:

$$\lambda_1 \geq \mu_1 \geq \lambda_2 \geq \cdots \geq \mu_{n-1} \geq \lambda_n \tag{68}$$

Důkaz Dokazujeme indukcí $\lambda_k \geq \mu_k \geq \lambda_{k+1}$. Označme x_i a y_i vlastní vektory matic A a B. Zaveďme následující vektorové podprostory $\mathbb{C}^n$ (ačkoli druhý z nich nemá dostatek složek, můžeme mu jednu nulovou přidat a nic se nestane):

$$S_1 := \mathcal{L}\{x_k, \ldots, x_n\} \subseteq \mathbb{C}^n \tag{69}$$
$$S_2 := \mathcal{L}\{y_1, \ldots, y_k\} \subseteq \mathbb{C}^n \tag{70}$$

Zřejmě $\dim(S_1) + \dim(S_2) = (n-k+1) + k > n$, tedy $\exists x \in S_1 \cap S_2$. Použijeme Reileighův princip pro oba prostory a máme:

$$\mu_k \leq \frac{y^* B y}{y^* y} = \frac{x^* A x}{x^* x} \leq \lambda_k \tag{71}$$

Stačí ukázat, že $\mu_k \geq \lambda_{k+1}$ – to je ale snadné, stačí vzít $-A$ a $-B$, čímž se obrátí znaménka vlastních čísel a nerovnosti. □

Věta (Věta o proplétání při násobení maticí) Nechť A je symetrická čtvercová matice s vlastními čísly a vektory λ_i a x_i, S reálná matice, že $S^T S = I$. Definujeme $B := S^T A S$ a označíme vlastní čísla a vektory matice B jako μ_i a y_i. Potom μ_i proplétají λ_i a pokud navíc $\mu_i = \lambda_i$ pro nějaké i, tak Sy_i je vlastní vektor A příslušící vlastnímu číslu λ_i.

Důkaz Použijeme Raileighův princip podobně, jako v předchozím tvrzení. Všimneme si, že:

$$x \in \mathcal{L}\{S^T x_k, \ldots, S^T x_{k-1}\}^\perp \Leftrightarrow Sx \in \mathcal{L}\{x_k, \ldots, x_{k-1}\}^\perp \tag{72}$$

Stačí si opět vzít vhodný prvek x z průniku:

$$x \in \mathcal{L}\{S^T x_k, \ldots, S^T x_{k-1}\}^\perp \cap \mathcal{L}\{y_1, \ldots, y_k\} \tag{73}$$

A můžeme použít Reileighův princip:

$$\lambda_i \geq \frac{S x^T A S x}{S x^T S x} = \frac{x^T B x}{x^T x} \geq \mu_i \tag{74}$$
$$\tag{75}$$

Na navíc platí pokud $\lambda_i = \mu_i$, potom:

$$\frac{x^T B x}{x^T x} = \lambda_i \quad \Rightarrow \quad x^T B x = x^T x \lambda_i \quad \Rightarrow \quad Bx = \lambda_i x \tag{76}$$

A x je vlastní vektor příslušící λ_i, jak jsme chtěli dokázat. □

Definice A je bloková matice s bloky velikosti $x_1, \ldots, x_m$. Kvocient A je matice $B^{m \times m}$, kde $b_{i,j}$ = průměr hodnot $A_{i,j}$.

$$A = \begin{pmatrix} A_{1,1} & A_{1,2} & \ldots \\ A_{2,1} & A_{2,2} & \ldots \\ \vdots & \vdots & \ddots \end{pmatrix} \qquad B = \begin{pmatrix} b_{1,1} & b_{1,2} & \ldots \\ b_{2,1} & b_{2,2} & \ldots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

Věta (Věta o proplétání kvocientu) Pokud B je kvocient A, pak vlastní čísla B proplétají vlastní čísla A.

Důkaz Mějme $\widetilde{S}$ je matici incidence blokové A:

$$\widetilde{S} = \begin{pmatrix} \boxed{1} & & 0 \\ & \boxed{1} & \\ 0 & & \boxed{1} \\ & & \boxed{1} \end{pmatrix}$$

$$\widetilde{S} \cdot \widetilde{S}^T = \text{diagonální matice } (x_1, x_2, \ldots, x_m) = D$$
$$S := \widetilde{S} \cdot D^{-\frac{1}{2}}$$
$$\widetilde{B} = S^T A S$$

Kromě toho platí:

$$S^T S = I \qquad\qquad B = D^{-\frac{1}{2}} \widetilde{B} D^{-\frac{1}{2}}$$

Tedy B je matice podobná $\widetilde{B}$ a má stejná vlastní čísla. Matice $\widetilde{B}$ proplétá matici A, což plyne z věty o proplétání při násobení maticí. □

5 Náhodné procházky

5.1 Markovovské řetězce

Definice Markovovský řetězec je orientovaný graf s váženými hranami takový, že výstupní stupeň každého vrcholu je 1. Markovoský řetězec často reprezentujeme maticí přechodu P, kde P_{ij} udává pravděpodobnost, že ze stavu i přejdeme do stavu j.

Definice Distribuce π je vektor, jehož součet je 1 a kde p_i určuje pravděpodobnost, že se nacházíme ve stavu i.

Poznámka Máme-li distribuci π a provedeme jeden krok na Markovovském řetězci s maticí přechodu P, dostaneme novou distribuci $\pi \cdot P$.

Definice Markovovský řetězec je reversibilní, existuje-li distribuce π t. že $\pi_i \cdot P_{ij} = \pi_j \cdot P_{ji}$.

Lemma Markovovský řetězec je reversibilní $\Leftrightarrow$ je odvozen z váženého neorientovaného grafu.

Důkaz

„$\Leftarrow$“ Zvolíme si π následovně a ukážeme, že splňuje reversibilní podmínku:

$$\pi_v = \frac{\deg v}{\sum_{u \in V(G)} \deg u} \qquad\qquad P_{ij} = \frac{w_G(i,j)}{\deg i}$$

$$\pi_i P_{ij} = \pi_i \frac{w_G(i,j)}{\deg i} = \frac{w_G(i,j)}{\sum_{u \in V(G)} \deg u}$$
$$\pi_j P_{ji} = \pi_j \frac{w_G(j,i)}{\deg j} = \frac{w_G(j,i)}{\sum_{u \in V(G)} \deg u}$$

„⇒“ Zvolíme váhu $w(i,j) = P_{i,j}\pi_i = P_{j,i}\pi_j = w(j,i)$ a dostaneme vážený neorientovaný graf. □

Definice π je stabilní distribuce[5], je-li $\pi \cdot P = \pi$. Jinak řečeno, stabilní distribuce se po provedení kroku nezmění.

Věta Pro G neorientovaný souvislý platí: $\forall \rho$ počáteční distribuci $\{P_G^k \cdot \rho\}_k$ konverguje $\Leftrightarrow$ G není bipartitní.

Důkaz

„⇒“ Pokud je G bipartitní, stačí jako protipříklad vzít distribuci, která začíná jenom v jedné partitě. Pak každým pronásobením matice se celá distribuce přesune do druhé partity, protože nemá kam jinam. Zjevně tedy nekonverguje k jedinému rozložení.

„⇐“ Prvně si vyjádříme distribuci jako lineární kombinaci vlastních vektorů matice P_G (to lze, protože tvoří ortonormální bázi). Tedy $\rho = \sum_i a_i p_i$. Dále si vyjadřme distribuci po k iteracích:

$$P_G^k \rho = P_G^k \sum_i a_i p_i = \sum_i P_G^k a_i p_i \tag{77}$$

Protože p_i je vlastní vektor P_G, tak $P_G p_i = \lambda_i p_i$:

$$\sum_i \lambda_i^k a_i p_i \tag{78}$$

Nyní si všimneme, že protože graf není bipartitní, tak $\lambda_1 \neq -\lambda_n$ a největší vlastní číslo distribuce je 1, protože matice P_G má řádkové i sloupcové součty konstantní 1 a zároveň je 1 má vlastní vektor samých jedniček. Tedy pro $i > 1$ platí $|\lambda_i| < 1$. Dejme nyní výraz do limity a všimneme si, že suma jde k nule díky tomu, že jediný člen závislý na k je λ_i:

$$\lim_{k \to \infty} \left(\lambda_1^k a_1 p_1 + \sum_{i>1} \lambda_i^k a_i p_i \right) = a_1 p_1 = \pi \tag{79}$$

Tedy máme stabilní distribuci, protože $a_1 p_1$ jsou po celou dobu konstantní.

[5] Někdy též zvaná „stacionární“.

Věta Nechť ρ je distribuce na vrcholech grafu a $\mu = \max\{\lambda_i, -\lambda_n\}$. Pak po t krocích platí, že $\|P_G^t\rho - \pi\|_1 \leq \mu^t\sqrt{n}$, tedy distribuce konverguje relativně rychle.

Důkaz Z předchozího důkazu víme, že $\rho = p_i a_i + \sum_{i>1} \lambda_i^t a_i p_i$ a **TODO:** vec.

Pusťme se do odhadu naší odchylky, prozatím však v L_2 normě.

$$\|P_G^t\rho - \pi\|_2^2 = \left\|\sum_{i>1} \lambda_i a_i p_i\right\|_2^2 = \sum_{i>1} \lambda_i^{2t}\|a_i p_i\|_2^2 \tag{80}$$

Nyní si zjednodušíme práci a do sumy zahrneme i první člen. Navíc odhadneme λ_i největšším vlastním číslem μ (mocnina u λ_i je sudá!).

$$\leq \mu^{2t}\sum_i \|a_i p_i\|_2^2 = \mu^{2t}\|\rho\|_2^2 \leq \mu^{2t} \tag{81}$$

Nyní stačí výraz odmocnit a vzpomenout si na analýzu, čímž víme, že $\|x\|_1 \leq \|x\|_2 \cdot \sqrt{n}$ a máme nerovnost:

$$\|P_G^t\rho - \pi\|_2 \leq \mu^t \tag{82}$$
$$\|P_G^t\rho - \pi\|_1 \leq \mu^t\sqrt{n} \tag{83}$$

Což jsme chtěli dokázat. □

5.2 Stabilní distribuce a konvergence

6 Expandéry

6.1 Expanze

Definice

- $E(S,T) = \{$ hrany mezi S a T $\}$
- $e(S,T) = |E(S,T)|$
- $e(S) =$ počet hran uvnitř S
- vrcholová expanze $h_v(G) = \min\limits_{S\subseteq V, |S|\leq \frac{n}{2}} \frac{|N(S)}{|S|}$
- hranová expanze $h(G) = \min\limits_{S\subseteq V, |S|\leq \frac{n}{2}} \frac{e(S,\bar{S})}{|S|}$

Pozorování $h_v(G) \leq h(G) \leq d.h_v(G)$

Definice

- Rodina expanderů $\{G_i\}_\infty \quad 2^i \geq |G_i| \geq i : h(G_i) \geq \varepsilon$, G_i je d-regulární.

- Spectral gap $= d - \max\{\lambda_2, -\lambda_n\}$
- Spektrální expanze $= d - \lambda_2$
- $\lambda = \max\{\lambda_2, -\lambda_n\}$

Věta $\frac{1}{2}(d-\lambda_2) \leq h(G) \leq \sqrt{d(d-\lambda_2)}$ (G je d-regulární graf).
Důkaz (Jen první nerovnost, druhá je bez důkazu). Sporem: nechť S je množina vrcholů s malou hranovou expanzí.

Pro $x \perp (1,1,\ldots,1)$ platí $\lambda_2 \geq \frac{x^T A x}{x^T x}$ (Raileighův princip). Zvolíme $x = (n-s)1_S - s1_{\bar{S}}$, kde $s = |S|$ a 1_S je charakteristický vektor množiny S.

$$x^T x = (n-s)^2 s + s^2(n-s) = s(n-s)n$$
$$x^T A x = \sum_{(a,b)\in E} 2x_a x_b = 2(n-s)^2 e(S) - 2s(n-s)e(S,\bar{S}) + 2s^2 e(\bar{S})$$

Platí $ds = 2e(S) + e(S,\bar{S})$, neboť ds odpovídá počtu konců hran v S. Analogicky $d(n-s) = 2e(\bar{S}) + e(S,\bar{S})$ pro $\bar{S}$. Z toho si vyjádříme $e(S)$ a $e(\bar{S})$ a dosadíme do rovnice výše:

$$x^T A x = -e(S,\bar{S})n^2 + (n-s)ds(n-s+s) = (n-s)dsn - e(S,\bar{S})n^2$$
$$\lambda_2 \geq \frac{(n-s)dsn - e(S,\bar{S})n^2}{s(n-s)n} = d - \frac{n}{n-s}\cdot\frac{e(S,\bar{S})}{s}$$
$$d - \lambda_2 \leq \frac{n}{n-s}\cdot\frac{e(S,\bar{S})}{s} \leq 2\cdot\frac{e(S,\bar{S})}{s} = 2h(G)$$

□

Lemma Pro náhodný d-regulární graf skoro jistě platí $\lambda \leq 2\sqrt{d-1} + O(1)$. Bez důkazu.

6.2 Mixing lemma

Věta (Mixing lemma) $\forall G, \forall S, T \subseteq V, S \cap T = \emptyset : |e(S,T) - \frac{d\cdot|S|\cdot|T|}{n}| \leq \lambda \cdot \sqrt{|S|\cdot|T|}$
Důkaz Buďte χ_S, χ_T charakteristické vektory S a T. $u = (1,1,\ldots)$ je první vlastní vektor. $\chi_S^\perp$ značí vektor kolmý na χ_S.

$$\frac{\langle \chi_S \cdot u\rangle}{\|u\|^2} = \frac{|S|}{n} \quad \Rightarrow \quad \chi_S = u\cdot\frac{|S|}{n} + \chi_S^\perp \qquad \chi_T = u\cdot\frac{|T|}{n} + \chi_T^\perp$$

$$e(S,T) = \sum_{i\in S, j\in T} A_{ij} = \chi_T^T A \chi_S = \underbrace{\frac{|S|\cdot|T|}{n^2}\underbrace{u^T A u}_{dn}}_{\frac{d\cdot|S|\cdot|T|}{n}} + {\chi_T^\perp}^T A \chi_s^\perp$$

Zbývá dokázat, že $|{\chi_T^\perp}^T A \chi_S^\perp| \leq \lambda\cdot\sqrt{|S|\cdot|T|}$.

$$|{\chi_T^\perp}^T A \chi_S^\perp| \leq \|{\chi_T^\perp}^T\| \cdot \|A\chi_S^\perp\| \leq \|{\chi_T^\perp}^T\| \cdot \lambda \cdot \|\chi_S^\perp\|$$

První nerovnost plyne z toho, že skalární součin dvou vektorů (tedy součin jejich délek a sinu úhlu, který svírají) je vždy nejvýš roven součinu jejich délek. Druhá nerovnost plyne z toho, že si $\chi_S^\perp$ můžu vyjádřit jako lineární kombinaci vlastních vektorů A:

$$\chi_S^\perp = \sum_{i=2}^{n} y_i \alpha_i$$

Pro každý vlastní vektor y_i můžu nahradit matici A vlastním číslem λ_i (pak bude zachována rovnost) a tím spíš můžu nahradit matici A největším vlastním číslem, což je v našem případě $\lambda = \max\{\lambda_2, -\lambda_n\}$, abych zachoval nerovnost.

$$\|\chi_S\|^2 = |S| \qquad \Rightarrow \qquad \|{\chi_T^\perp}^T\| \leq \sqrt{S}$$
$$\|\chi_T\|^2 = |T| \qquad \Rightarrow \qquad \|\chi_S^\perp\| \leq \sqrt{T}$$

$$|{\chi_T^\perp}^T A \chi_S^\perp| \leq \lambda \cdot \sqrt{|S| \cdot |T|}$$

□

6.3 Vzdálenostní mocniny a zig-zag součin

7 Perfektní kódy

Perfektní kódy jsou v jistém smyslu ty nejlepší samoopravné kódy, konkrétně mají vlastnost, že žádná slova z abecedy nezůstávají nevyužita. Cílem našeho snažení bude ukázat větu, která tyto kódy charakterizuje ve smyslu při jakých parametrech může být kód perfektní. Začneme připomenutím základních pojmů, vyslovíme a dokážeme Lloydovu větu o nutné podmínce a z ní následně dokážeme (v současné podobně spíše nastíníme), kýženou charakterizaci.

7.1 Připomenutí pojmů

Definice Samoopravný kód C s parametry (n, q) je pro nás systém množin $C \subseteq M = \{0, \ldots, q-1\}^n$ (prvkům této množiny říkáme kódová slova).

Definice Grafem kódu rozumíme graf $G = (V, E)$, že $V(G) = \{0, \ldots, q-1\}^n$ a hrana mezi vrcholy u, v vede právě tehdy, když $d(u, v) = 1$, tedy liší se právě v jedné souřadnici (d je hammingovská vzdálenost). Kód v takovém grafu je pak podmnožina vrcholů, které odpovídají kódovým slovům.

Definice Kód opravuje t chyb, pokud jsou $N_t(u)$ (okolí vrcholu u do vzdálenosti t) disjunktní pro všechny dvojce kódových slov.

Definice Kód C je t-perfektní, pokud opravuje t chyb a navíc úplně pokrývá svou nosnou množinu M.

Tvrzení Pokud C opravuje t chyb, platí:

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

Důkaz Okolíčka musí být disjunktní, stačí tedy spočítat, kolik může být kódových slov, což je daný výraz: V čitateli je počet všech slov. Jmenovatel počítá velikost každého t-okolí, tedy vybírá možné souřadnice ke změně a jejich potenciální nové hodnoty.

7.2 Lloydova věta

Věta Pokud existuje t-perfektní kód s parametry (n, q), pak $L_t(x)$ (definice níže) má t různých celočíselných kořenů mezi 0 a n.

$$L_t(x) = \sum_{j=0}^{t} (-1)^j (q-1)^{t-j} \binom{x-1}{j} \binom{n-x}{t-j} \tag{84}$$

Důkaz Důkaz bude plynout touto sekcí a obsahuje spoustu pomocných lemmat a konceptů. Pro pochopení a reprodukci důkazu bude potřeba pochopit všechno mezi tímto místem a a sekcí označující samotný důkaz. Nechť práce započne.

7.3 Vzdálenostně regulární grafy

Definice Vzdálenostně regulární graf: $\exists s_{hij}$ t. že $\forall u, v \in V(G), d_G(u, v) = j : |\{w : d_G(u, w) = h, d_G(w, v) = i\}| = s_{hij}$.

Pozorování $|h - j| > j \Rightarrow s_{hij} = 0$ (plyne z Δ nerovnosti), $k = s_{110}$ (počet sousedů vrcholu $u = v$ v k-regulárním grafu)

Lemma $Z_{mi} = Z_{m-1,i-1} \cdot s_{1,i-1,i} + Z_{m-1,i} \cdot s_{1,i,i} + Z_{m-1,i+1} \cdot s_{1,i+1,i}$. Z_{mi} značí počet sledů délky m mezi vrcholy ve vzdálenosti i.

Důkaz $Z_{00} = 1$, jinak $Z_{0i} = 0$. Dále dokážeme indukcí pro $m \geq 1$ a $i \geq 1$. $s_{1,i,j}$ je nenulové pouze pro $i \in \{j-1, j, j+1\}$ (z Δ nerovnosti). V rovnici sčítáme vrcholy sousedící s u, které jsou ve vzdálenosti $i-1$, i a $i+1$ od v.

Definice Matice sousednosti $A = A_G$. $\mathcal{A}(G) = \{p(A) : p(x) \in \mathbb{C}[x]\}$. $\mathcal{A}(G)$ je vektorový prostor.

Definice Vzdálenostní matice $A_1, A_2, \ldots, A_d$ grafu G:

$$(A_i)_{uv} = \begin{cases} 1 & d_G(u, v) = i \\ 0 & \text{jinak} \end{cases} \qquad \begin{aligned} A_0 &= I \\ A_1 &= A \end{aligned}$$

7.4 Reprezentace vzdálenostně regulárních grafů polynomy

Věta $\dim \mathcal{A}(G) = d + 1$, kde d je průměr G.[6]

Důkaz $A^m = \sum_{i=0}^{d} Z_{mi} A_i$

$i > m \Rightarrow Z_{mi} = 0$

[6] Průměr grafu je maximální nejkratší vzdálenost přes všechny dvojice vrcholů.

$A^0 = Z_{0,0} \cdot A_0 = A_0$
$A^1 = Z_{1,0} \cdot A_0 + Z_{1,1} \cdot A_1 = A_1$
$A^2 = Z_{2,0} \cdot A_0 + Z_{2,1} \cdot A_1 + Z_{2,2} \cdot A_2$
$\vdots$
$A^d = Z_{d,0} \cdot A_0 + Z_{d,1} + \cdots + Z_{d,d} \cdot A_d$

Generujeme celý vektorový prostor polynomů A deg $\leq d$, tedy $\dim \mathcal{A}(G) \leq d+1$. Zároveň ale $A_0, A_1, \ldots, A_d$ jsou lineárně nezávislé a proto $\dim \mathcal{A}(G) = d+1$. □

Pozorování $\widetilde{\mathcal{A}} = \{A_0, A_1, \ldots, A_d\}$ tvoří bázi $\mathcal{A}(G)$.

Definice Matice B_h pro graf je velikosti $d \times d$, uchovávající parametry s_{hij}:

$$(B_h)_{ij} := s_{hij} \tag{85}$$

Maticí B navíc rozumíme matici B_1.

Lemma Existuje funkce $f : \mathcal{A} \to \mathcal{A}$, že $f(A_h) = B_h$ a tuto operaci značíme $\widehat{A} = B$.

Důkaz Z předchozího lemmatu již máme bázi $\widetilde{\mathcal{A}}$ prostoru $\mathcal{A}$. Ukážeme si tedy, že můžeme přejít k bázi z menších matic B. Nejdříve si všiměme, co se děje v následujícím součinu matic:

$$(A_h A_i)_{uv} = \sum_w (A_h)_{uw} \cdot (A_i)_{wv} = s_{hid(u,v)} \tag{86}$$

Kde zmíněná suma je rozpis maticového násobení pro jednu buňku součinu. Zřejmě přičtu 1 pokaždé, když pro vrchol w platí, že $d(u,w) = h$ a $d(w,v) = i$, což je přesně definice s_{hij} pro $j = d(u,v)$. Jak takový prvek ještě můžeme vyjádřit (rozepsáním maticového násobení s použitím předchozího vzorce pro buňku)?

$$A_h A_i = \sum_{j=0}^{d} s_{hij} A_j \tag{87}$$

Což je vlastně lineární kombinace prvků z báze s koeficienty s_{hij}. Vytvořme tedy novou bázi, například takovou, která bude obsahovat právě tyto koeficienty. Do řádku i matice B'_h zapíšeme souřadnice součinu $A_h A_i$ vůdči bázi $\widetilde{A}$, tedy s_{hij}. Tím získáme matice B'_h, které jsou bazí (vytvořili jsme je zapsáním souřadnic lineárně nezávislých prvků a tak jsou lineárně nezávislé), která navíc splňuje žádané vlastnosti a tedy $B'_h = B_h$. □

Lemma (O sousedech) $B1 = \begin{pmatrix} \ddots & & \ddots & \ddots & \ddots & 0 \\ & \ddots & \ddots & \ddots & \ddots & \ddots \\ & & \ddots & \ddots & \ddots & \ddots \\ & & & \ddots & \ddots & \ddots \\ 0 & & & & \ddots & \ddots \end{pmatrix}$ je tridiagonální matice. Všechny sloupcové součty jsou stejné a jsou rovny k.

Důkaz Matice je tridiagonální, protože $s_{1,i,j}$ dává smysl jen pro $i \in \{j-1, j, j+1\}$ (z Δ nerovnosti). Navíc v j-tém sloupci je $s_{1,j-1,j} + s_{1,j,j} + s_{1,j+1,j}$, což zahrnuje všechny sousedy u, kterých je k. □

Lemma $B1 = \begin{pmatrix} \ddots & & 0 \\ & \ddots & \\ 0 & & \ddots \end{pmatrix}$ je tridiagonální matice $\Rightarrow \forall$ vlastní čísla jsou různá.

7.5 Charakteristické polynomy

Definice Definujme polynomy $v_i \in \mathbb{Q}[\lambda]$ takové, že $\deg v_i(\lambda) = i$ a:

1. $v_0(\lambda) = 1$
2. $v_1(\lambda) = \lambda$
3. pro $i \in \{2, \ldots, d-1\}$ induktivně, aby splňovaly rovnici

$$(s_{1,i,i-1}v_{i-1}(\lambda)) + (s_{1,i,i-\lambda}v_i(\lambda)) + (s_{1,i,i+1}v_{i+1}(\lambda)) = 0 \tag{88}$$

Lemma (O charakteristickém polynomu) Nechť $\lambda_1, \ldots, \lambda_d \in \mathrm{Sp}(B_1)$. Potom pokud $\lambda_i \neq k$ platí:

$$v_o(\lambda) + \ldots + v_d(\lambda) = c \cdot (\lambda - \lambda_1) \cdot \ldots \cdot (\lambda - \lambda_d) \tag{89}$$

Důkaz Vytvořme vektor $\vec{v} = (v_1(\lambda), \ldots, v_d(\lambda))$ a uvažme systém rovnic $B\vec{v} = \lambda\vec{v}$. Ten umíme řešit po řádcích (známe první dva členy vektoru a celou matici obsahující potřebné koeficienty), známe tedy vlastní čísla (kořeny této rovnice) a jejich vlastní vektory (obsahují složky $v_i(\lambda)$.

Nejprve si ukážeme, že jedno z vlastních čísel je k (všimněte si, že v předpokladech používáme d vlastních čísel, ale dimenze matice B je $d+1$). Vezměme si výše používaný systém rovnic a sečtěme levé a pravé strany. Podle Lemma o sousedech jsou sloupcové součty matice B rovny k, získáme tedy rovnici $k(v_0(\lambda)+\ldots+v_d(\lambda)) = \lambda(v_0(\lambda)+\ldots+v_d(\lambda))$, z čehož po úpravě plyne, že $\lambda = k$.

TODO: Rovnost s char. polynomem

Lemma Pro polynomy v_i platí, že $v_i(A) = A_i$ a $v_i(B) = B_i$.

Důkaz *(bez důkazu)*

Definice $z \in V(G)$, $T \in \{0,1\}^{d+1 \times n}$

$$T_{i,u} = \begin{cases} 1 & d(u,z) = i \\ 0 & \text{jinak} \end{cases}$$

Lemma (O zastřešování) $X \in \mathcal{A}(G), z \in V(G) \Rightarrow TX = \widehat{X}T$

Důkaz

$$(TA)_{iu} = \sum_w T_{iw}A_{wu} = s_{1,i,d(u,z)}$$

$$(BT)_{iu} = \sum_j B_{ij}T_{ju} = s_{1,i,d(u,z)}$$

$$TA = BT \quad \Rightarrow \quad TA^2 = BTA = B^2T \quad \Rightarrow \quad TA^m = B^mT$$

$$Tp(A) = p(B)T \quad \Rightarrow \quad TX = \widehat{X}T$$

□

Definice Definujme si pomocné polynomy: $x_i(\lambda) = v_0(\lambda) + \cdots + v_i(\lambda) \qquad S_t = x_t(A) = A_0 + A_1 + \cdots + A_t$ Kde S_t je matice, která označuje dvojce vrcholů jedničkou, pokud jsou vzdálené nanejvýš t (je to součet vzdálenostních matic do t).

Lemma C je perfektní kód (množina vrcholů) v G a c je jeho charakteristický vektor. Pak $S_t \cdot c = \vec{1}$.

Důkaz $(S_t \cdot c)_u = |\{w : w \in C, d(w,u) \leq t\}| = 1$, což plyne z definice perfektního kódu. □

Lemma $\exists$ t-perfektní kód $\Rightarrow \dim \operatorname{Ker} \widehat{S}_t \geq t$

Důkaz $z_0 = z \in C$

$z_1, z_2, \ldots, z_t \quad d(z, z_i) = i$ pro $i = 1, 2, \ldots, t$

$(T_{z_i} \cdot c)_j = \delta_{ij}$ (Kroneckerovo delta $= 1$ pro $i = j$, 0 jinak)

Tedy vektory $T_{z_i} \cdot c$ pro $i = 0, 1, \ldots, t$ jsou lineárně nezávislé.

$$\widehat{S}_t(T_{z_i} \cdot c) = (\widehat{S}_t \cdot T_{z_i}) \cdot c \overset{1}{=} T_{z_i} \cdot S_t \cdot c \overset{2}{=} T_{z_i} \cdot \vec{1} = \begin{pmatrix} k_0 \\ \vdots \\ k_d \end{pmatrix}$$

$\overset{1}{=}$ plyne z lemma o zastřešování, $\overset{2}{=}$ plyne z předchozího lemmatu. Výsledný vektor je pro všechnyvolby z_i stejný, protože jeho položky je počet sousedů s pevnými vzdálenostmi, a protože je to vzdálenostně regulární graf, jsou to nějaké hodnoty s_{hij} se stejným hij pro řádek.

$$u_i = T_{z_i} \cdot c - T_{z_0} \cdot c \qquad i = 1, 2, \ldots, t$$

$$\widehat{S}_t u_i = \widehat{S}_t T_{z_i} \cdot c - \widehat{S}_t T_{z_i} \cdot c = \begin{pmatrix} k_0 \\ \vdots \\ k_d \end{pmatrix} - \begin{pmatrix} k_0 \\ \vdots \\ k_d \end{pmatrix} = \vec{0} \quad \Rightarrow \quad u_i \in \operatorname{Ker} \widehat{S}_t$$

Vektory $u_1, \ldots, u_t$ tvoří $\operatorname{Ker} \widehat{S}_t$ a jsou lineárně nezávislé. Tedy $\dim \operatorname{Ker} \widehat{S}_t \geq t$. □

7.6 Důkaz Lloydovy věty

Zde začnou věci dávat větší smysl. Nejdříve dokážeme pomocí výše zmíněných lemat pomocné tvrzení, který dá podobný polynom, následně si s ním pohrajeme a získáme polynom Lloydův, tak jak byl zadefinován na začátku.

Věta (Lloydův prototyp) Pokud existuje t-perfektní kód v G, potom $x_t(\lambda) \backslash x_d(\lambda)$.

Důkaz Nejprve si všimněme, že $\widehat{S}_t = \widehat{X_t(A)} = \widehat{\sum_i^t A_i} = \sum_i^t B_i = X_t(B)$. Dále se podívejme na spektra B a $\widehat{S}_t$:

$$\mathrm{Sp}(B) = \{k, \lambda_1, \ldots, \lambda_d\} \tag{90}$$

$$\mathrm{Sp}(\widehat{S}_t) = \{x_t(k), x_t(\lambda_1), \ldots, x_t(\lambda_d)\} \tag{91}$$

TODO: proc a zbytek...

7.7 Charakterizace perfektních kódů

Věta Nechť $q = p^r$, a p je prvočíslo. Pak existují právě následující netriviální perfektní kódy (tedy s $|C| \geq 2$ a pokud $|C| = 2$, tak to není kód $q = 2$ a $n = 2t + 1$):

1-perfektní kód $n = \frac{q^k - 1}{q - 1}$ pro libovolné k (Hammingův)

2-perfektní kód $q = 3$ a $n = 11$ (Golayův)

3-perfektní kód $q = 2$ a $n = 23$ (Golayův)

Dál q složené neexistují perfektní kódy pro $t \geq 3$ a pro $t = 1, 2$ se to neví.

Důkaz Důkaz je technicky náročný. Základ je v Lloydově větě, která dává relativně silný nástroj jak perfektní kód poznat. Společně se hrubým odhadem na velikost kódu ukázaným na začátku sekce, lze pomocí hrubé síly a netriviální teorie čísel získat výsledek. Ten však není v naší moci.