Lineární algebra v kombinatorice[1]

Jan Bok
Pavel Dvořák
Jan Horáček
Radek Hušek
Karel Král
Ladislav Láska
Honza Musílek
Stanislava Tlustá
Martina Vaváčková

Tomáš Gavenčiak (ed.)

25. září 2015

[1]Tyto poznámky k predmětu „Lineární algebra v kombinatorice“ na MFF UK jsou rozpracované a mohou být nekompletní. Budete-li se chtít do jejich tvorby zapojit, ozvěte se na `gavento@ucw.cz`.

Obsah

1 Lineární nezávislost **2**
- 1.1 Sudo-licho města a skorodisjunktní systémy podmnožin . . . 2
- 1.2 Dvouvzdálenostní množiny . . . 3
- 1.3 Fisherova nerovnost . . . 4

2 Skalární součin **5**
- 2.1 Ortogonální doplněk . . . 5
- 2.2 Sudo-sudo města . . . 6
- 2.3 Eulerovské a úplné bipartitní podgrafy . . . 6

3 Shannonova kapacita a Lovászova ϑ funkce **8**
- 3.1 Shannonova kapacita . . . 8
- 3.2 Funkční reprezentace grafu . . . 12

4 Vlastní čísla grafu **14**
- 4.1 Vlastní čísla matic . . . 14
- 4.2 Mooreovy grafy . . . 16
- 4.3 Silně regulární grafy . . . 18
- 4.4 Rayleighův princip a proplétání . . . 22

5 Náhodné procházky **24**
- 5.1 Markovovské řetězce . . . 24
- 5.2 Stabilní distribuce a konvergence . . . 26

6 Expandéry **26**
- 6.1 Expanze . . . 26
- 6.2 Mixing lemma . . . 27
- 6.3 Vzdálenostní mocniny a zig-zag součin . . . 28

7 Perfektní kódy **28**
- 7.1 Samoopravné kódy . . . 28
- 7.2 Lloydova věta . . . 29
- 7.3 Vzdálenostně regulární grafy . . . 30
- 7.4 Charakteristické polynomy . . . 31
- 7.5 Lloydova věta . . . 32
- 7.6 Vzdálenostně regulární grafy . . . 32
- 7.7 Reprezentace vzdálenostně regulárních grafů polynomy . . . 32
- 7.8 Charakteristické polynomy . . . 34
- 7.9 Důkaz Lloydovy věty . . . 36
- 7.10 Charakterizace perfektních kódů . . . 38

1 Lineární nezávislost

Definice Vektory $v_1, \ldots, v_n$ jsou *lineárně nezávislé*, jestliže neexistuje netriviální řešení rovnice $\sum_{i=1}^{n} \alpha_i v_i = 0$.

1.1 Sudo-licho města a skorodisjunktní systémy podmnožin

Definice Buď X n-prvková množina a $A_1, \ldots, A_m$ systém jejích podmnožin takový, že $A_i \neq A_j$ pro $i \neq j$. Úloha *A-B město* se ptá, jak velké může být m, je-li $|A_i| \sim B$ a $|A_i \cap A_j| \sim A$ pro všechna $i, j = 1, \ldots, m$, $i \neq j$.

V případě sudo-licho města tedy máme omezení na liché velikosti a sudé průniky.

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

Důkaz Podmnožinu množiny X ztotožněme s jejím charakteristickým vektorem délky n a označme A matici o rozměrech $m \times n$, která má v i-tém řádku vektor A_i^T. Platí

$$A_i^T A_j \bmod 2 = \begin{cases} 1, & \text{je-li } i = j, \\ 0, & \text{je-li } i \neq j, \end{cases} \tag{1}$$

tedy nad GF(2) máme

$$AA^T = \begin{pmatrix} A_1^T \\ A_2^T \\ \vdots \\ A_m^T \end{pmatrix} \cdot \big(A_1, A_2, \ldots, A_m\big) = I, \tag{2}$$

speciálně $\operatorname{rank}(AA^T) = m$. Jelikož každý sloupec matice AA^T je lineární kombinací sloupců matice A, je $\operatorname{rank}(AA^T) \leq \operatorname{rank}(A) \leq n$. Tedy $m \leq n$. □

Věta Nechť pro $A_1, \ldots, A_m \subseteq X$ platí $|A_i \cap A_j| = 1$ a $A_i \neq A_j$, $i \neq j$. Potom $m \leq n$.

Důkaz Stejně jako v předchozím důkazu označme A matici charakteristických vektorů a podívejme se na součin AA^T, tentokrát však nad $\mathbb{Q}$:

$$AA^T = \begin{pmatrix} a_1 & & 1 \\ & \ddots & \\ 1 & & a_m \end{pmatrix}, \quad \text{kde } a_i = |A_i|. \tag{3}$$

Dokážeme-li, že tato matice je regulární, získáme kýženou nerovnost $m \leq n$.

Všimněme si, že pro všechna i je $a_i \geq 1$, přičemž rovnost nastává nejvýše pro jedno z nich. Můžeme tedy předpokládat, že pro $i \geq 2$ platí $a_i \geq a_1 \geq 1$ (tedy $a_i \geq 2$). Odečtením prvního řádku od všech ostatních získáme matici

$$B = \begin{pmatrix} a_1 & 1 & 1 & \ldots & 1 \\ 1 - a_1 & a_2 - a_1 & & & \\ 1 - a_1 & & a_3 - a_1 & & 0 \\ \vdots & & & \ddots & \\ 1 - a_1 & & 0 & & a_m - a_1 \end{pmatrix}, \tag{4}$$

jejíž determinant spočteme z definice jako

$$\det(B) = a_1 \cdot \prod_{i=2}^{m}(a_i - a_1) - (1 - a_1) \cdot \sum_{i=2}^{m} \prod_{\substack{j=2 \\ j \neq i}}^{m}(a_j - a_1). \tag{5}$$

Protože $1 - a_1 \leq 0$ a pro $i \geq 2$ je $a_i - a_1 > 0$, dostáváme $\det(B) > 0$. Tedy B je regulární. Přičtení prvního řádku k ostatním na regularitě zřejmě nic nezmění, a proto je i AA^T regulární, což jsme chtěli dokázat. □

Soubor podmnožin z předchozí věty se nazývá *skorodisjunktní systém podmnožin*. Sudolicho města a skorodisjunktní systémy podmnožin nyní využijeme ke konstrukci dolního odhadu Ramseyova čísla.

Věta (Ramsey) Pro každé $n \in \mathbb{N}$ existuje $N \in \mathbb{N}$ takové, že každý graf G na aspoň N vrcholech splňuje $\omega(G) \geq n$ nebo $\alpha(G) \geq n$.

Víme, že $R_2(n) = N_{\min} \leq \binom{2n-2}{n-1}$. Ukážeme nerovnost $R_2(n) \geq \binom{n-1}{3}$.

Věta (Dolní odhad Ramseyova čísla) Existuje graf na $\binom{n-1}{3}$ vrcholech, který má kliku i nezávislou množinu velikosti nejvýše $n - 1$.

Důkaz Buď X množina, $|X| = n - 1$. Sestrojíme graf

$$G = \left(V = \binom{X}{3}, E = \{uv; |u \cap v| = 1, u, v \in V\} \right). \tag{6}$$

Klika v G je skorodisjunktní systém podmnožin X, tedy $\omega(G) \leq |X| = n - 1$. Vrcholy jsou nezávislé, pokud $|a \cap b| \in \{0, 2\}$, tedy nezávislá množina v G je sudo-licho město a $\alpha(G) \leq |X| = n - 1$. □

1.2 Dvouvzdálenostní množiny

Věta Nechť $a, b \in \mathbb{R}^+$ a $P_1, P_2, \ldots, P_m$ jsou body v $\mathbb{R}^n$ takové, že platí $|P_iP_j| \in \{a, b\}$, $i \neq j$. Pak $m \leq \frac{(n+1)(n+4)}{2}$.

Důkaz Pro každé P_i definujme polynom $f_i \colon \mathbb{R}^n \to \mathbb{R}$ předpisem

$$f_i(x) = (\|P_i - x\|^2 - a^2)(\|P_i - x\|^2 - b^2). \tag{7}$$

Platí

$$f_i(P_j) = \begin{cases} a^2b^2, & \text{pokud } i = j, \\ 0 & \text{jinak,} \end{cases} \tag{8}$$

a pro každé $j = 1, \ldots, m$ je

$$\sum_{i=1}^{m} \alpha_i f_i(P_j) = \alpha_j a^2 b^2 = 0, \quad \text{právě když} \quad \alpha_j = 0. \tag{9}$$

Polynomy $f_1, \ldots, f_m$ jsou tedy lineárně nezávislé a $\dim\langle f_1, \ldots, f_m\rangle = m$.

Je-li $x = (x_1, \ldots, x_n)$ a $P_i = (p_{i1}, \ldots, p_{in})$, můžeme f_i rozepsat jako

$$f_i(x) = \Big(\underbrace{(x_1 - p_{i1})^2 + \cdots + (x_n - p_{in})^2}_{\sum_{j=1}^n x_j^2 - 2\sum_{j=1}^n p_{ij}x_j + \sum_{j=1}^n p_{ij}^2} - a^2\Big)\left((x_1 - p_{i1})^2 + \cdots + (x_n - p_{in})^2 - b^2\right). \quad (10)$$

Generátory prostoru $\langle f_1, \ldots, f_m\rangle$ jsou tedy také polynomy $(x_1^2+\cdots+x_n^2)^2$, $(x_1^2+\cdots+x_n^2)x_i$, x_i^2, x_ix_j, x_i a 1. Těchto polynomů je celkem

$$1 + n + n + \binom{n}{2} + n + 1 = \frac{(n+1)(n+4)}{2}, \quad (11)$$

tedy $m = \dim\langle f_1, \ldots, f_m\rangle \leq \frac{(n+1)(n+4)}{2}$. □

Množina $\{P_1, \ldots, P_m\}$ z předchozí věty se nazývá *dvouvzdálenostní množina.*

Věta Nechť $\{P_1, \ldots, P_m\}$ je dvouvzdálenostní množina v $\mathbb{R}^n$ taková, že všechna P_i leží na jedné sféře. Pak platí

$$\frac{n(n+1)}{2} \leq m_{\max} \leq \frac{n(n+3)}{2}. \quad (12)$$

Důkaz Nejprve ukážeme horní odhad. Definujme f_i stejně jako v důkazu předchozí věty. Opět platí $\dim\langle f_1, \ldots, f_m\rangle = m$, ale za generující polynomy stačí vzít x_i^2, x_ix_j a x_i, neboť na sféře je $x_1^2 + \cdots + x_n^2$ konstantní. Generujících polynomů je $n + \binom{n}{2} + n = \frac{n(n+3)}{2}$, tedy $m \leq \frac{n(n+3)}{2}$.

Nyní ukážeme vhodnou konstrukcí dolní odhad. Vezmeme ty body v $\mathbb{R}^{n+1}$, které mají dvě souřadnice jedničkové a všechny ostatní nulové. Vzdálenost dvou bodů s jedničkami na různých pozicích je 2 a vzdálenost dvou bodů s jednou jedničkou společnou je $\sqrt{2}$. Skutečně se tedy jedná o dvouvzdálenostní množinu.

Pro všechna P_i platí

$$\sum_{j=1}^{n+1} p_{ij}^2 = 2 \quad \text{a} \quad \sum_{j=1}^{n+1} p_{ij} = 2, \quad (13)$$

tedy body $P_1, \ldots, P_m$ ($m = \binom{n+1}{2} = \frac{n(n+1)}{2}$) leží na jedné sféře v $\mathbb{R}^{n+1}$ a zároveň v jedné nadrovině dimenze n. Průnikem této sféry a této nadroviny je hledaná sféra v $\mathbb{R}^n$. □

1.3 Fisherova nerovnost

Věta (Fisherova nerovnost) Mějme hranově disjunktní rozklad úplného grafu K_n na m úplných bipartitních grafů. Pak $m \geq n - 1$.

Důkaz Označme $B_1, \ldots, B_m$ úplné bipartitní grafy v rozkladu K_n. Dále označme X_i, Y_i partity grafu B_i a $A_i = ((A_i)_{jk})$ matici o rozměrech $n \times n$ indexovanou vrcholy grafu K_n a definovanou následovně:

$$(A_i)_{jk} = \begin{cases} 1, & \text{pokud } j \in X_i \text{ a } k \in Y_i, \\ 0 & \text{jinak.} \end{cases} \quad (14)$$

Nulové řádky matice A_i odpovídají vrcholům grafu K_n mimo partitu X_i, zatímco jedničky v nenulových řádcích odpovídají sousedům vrcholů z X_i. Protože B_i je úplný bipartitní graf, mají všechny vrcholy z X_i stejné sousedy. Všechny nenulové řádky jsou tedy stejné a matice A_i má hodnost 1.

Položme $A = A_1 + \ldots + A_m$. Protože každá hrana grafu K_n náleží právě jednomu B_i, má matice $A = (a_{jk})$ jedničku právě na jednom z míst a_{jk} nebo a_{kj}. Na diagonále A jsou samé nuly. Z předchozích pozorování vyplývá, že $A + A^T$ je matice incidence K_n, tedy $A + A^T = J - I$, kde J je matice samých jedniček.

Ukážeme, že $\text{rank}(A) \geq n-1$. Pro spor předpokládejme, že $\text{rank}(A) \leq n-2$. Přidáním řádku samých jedniček k matici A vytvoříme matici A', pro kterou platí $\text{rank}(A') \leq n-1$. Protože A' nemá plnou hodnost, existuje netriviální lineární kombinace jejích sloupců, která dává nulový vektor. Nechť jsou její koeficienty zaznamenány ve vektoru $x = (x_1, \ldots, x_n)^T$. Tedy $A'x = 0$ a rovněž $Ax = 0$. Protože v posledním řádku matice A' jsou samé jedničky, platí $\sum_{i=1}^{n} 1 \cdot x_i = 0$, a tedy i $Jx = 0$. Počítejme dvěma způsoby:

$$x^T(A + A^T)x = x^T Ax + x^T A^T x = x^T 0 + 0^T x = 0, \tag{15}$$

$$x^T(A + A^T)x = x^T(J - I)x = x^T Jx - x^T Ix = x^T 0 - x^T x = -\sum_{i=1}^{n} x_i^2 < 0, \tag{16}$$

což je spor. Tedy $\text{rank}(A) \geq n-1$.

Zároveň platí, že $\text{rank}(A) \leq \text{rank}(A_1) + \cdots + \text{rank}(A_m)$, protože prostor řádkových vektorů matice A je generován řádkovými vektory matic $A_1, \ldots, A_m$. To nám dává nerovnost $n - 1 \leq \text{rank}(A) \leq m$. □

2 Skalární součin

Definice *Skalárním součinem* vektorů $x = (x_1, \ldots, x_n)^T$ a $y = (y_1, \ldots, y_n)^T$ z vektorového prostoru $\mathbb{F}^n$ rozumíme číslo $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i \in \mathbb{F}$ (případně $\langle x, y \rangle = \sum_{i=1}^{n} x_i \overline{y_i}$ pro $\mathbb{F} = \mathbb{C}$).

2.1 Ortogonální doplněk

Definice Nechť $M \subseteq \mathbb{F}^n$. Množinu $M^\perp = \{x \mid \forall a \in M \colon \langle x, a \rangle = 0\}$ nazveme *ortogonálním doplňkem* M.

Definice *Součet podprostorů* $\langle M \rangle$ a $\langle N \rangle$ (symbol $\langle X \rangle$ značí lineární obal X) definujeme jako

$$\langle M \rangle + \langle N \rangle = \{u + v \mid u \in \langle M \rangle, v \in \langle N \rangle\} = \langle M \cup N \rangle. \tag{17}$$

Pozorování Pro $M, N \subseteq \mathbb{F}^n$ platí:

(i) $\dim M^\perp = n - \dim\langle M \rangle$,
(ii) $(M^\perp)^\perp = \langle M \rangle$,
(iii) $(\langle M \rangle \cap \langle N \rangle)^\perp = M^\perp + N^\perp$,
(iv) $(\langle M \rangle + \langle N \rangle)^\perp = M^\perp \cap N^\perp$,
(v) $\langle M \rangle + M^\perp = \mathbb{F}^n$.

Věta (Dimenze spojení a průniku) Pro podprostory $U, V \subseteq \mathbb{F}^n$ platí

$$\dim(U+V) + \dim(U \cap V) = \dim U + \dim V. \tag{18}$$

Všimněme si, že pro tři podprostory už předchozí pozorování neplatí. Máme-li například v rovině tři přímky p, q, r procházející počátkem, pak $\dim(p+q+r) = 2$, zatímco $\dim p + \dim q + \dim r - \dim(p \cap q) - \dim(p \cap r) - \dim(q \cap r) + \dim(p \cap q \cap r) = 3$.

Důsledek Nechť $U, V \subseteq \mathbb{F}^n$ jsou podprostory, pro které platí $\dim U + \dim V > n$. Pak $\dim U \cap V \geq 1$, tedy existuje $u \neq 0$, $u \in U \cap V$.

Důsledek V prostorech, ve kterých je skalární součin opravdu skalárním součinem, tedy $\langle x, x\rangle \neq 0$ pro $x \neq 0$, platí navíc $U \cap U^\perp = \{0\}$.

Například v $\mathrm{GF}(2)^2$ je $\langle (1,1), (1,1)\rangle = 0$, tedy $(1,1) \in \langle (1,1)\rangle \cap \langle (1,1)\rangle^\perp$.

2.2 Sudo-sudo města

V následující větě zachováme značení z kapitoly o lineární nezávislosti.

Věta Pro sudo-sudo město platí $m_{\max} = 2^{\lfloor n/2 \rfloor}$.

Důkaz Nejprve sestrojíme sudo-sudo město o velikosti $m = \lfloor \frac{n}{2} \rfloor$. Rozdělíme prvky množiny X do dvojic (pokud jeden přebývá, odložíme ho stranou a dále se jím nebudeme zabývat) a za $A_1, \ldots, A_m$ vezmeme všechny neprázdné podmnožiny množiny X, které obsahují z každé dvojice buď oba prvky, nebo žádný. Takových podmnožin je $2^{\lfloor n/2 \rfloor}$ a evidentně se jedná o sudo-sudo město.

Nyní ukážeme nerovnost $m \leq \lfloor \frac{n}{2} \rfloor$. Nechť $M = \{A_1, A_2, \ldots, A_m\}$ je co do inkluze maximální sudo-sudo město. Ztotožníme-li množiny A_i s jejich charakteristickými vektory, pak pro všechna $i, j \in \{1, \ldots, n\}$ je $\langle A_i, A_j\rangle \bmod 2 = 0$. Tedy M je vektorový prostor nad $\mathrm{GF}(2)$, neboť platí:

$$\begin{aligned}
&\emptyset \in M,\\
&\forall u \ \in M, \forall c \in \mathrm{GF}(2)\colon c \cdot u \ \in M,\\
&\forall x, \forall u, v \in M\colon \langle x, u+v\rangle = \langle x, u\rangle + \langle x, v\rangle = 0 + 0 = 0,\\
&\forall u, v \in M\colon \langle u+v, u+v\rangle = \langle u, u\rangle + 2\langle u, v\rangle + \langle v, v\rangle = 0 + 0 + 0 = 0.
\end{aligned}$$

Pokud $x \in M$, pak také $x \in M^\perp$, a tedy $M \subseteq M^\perp$. To znamená, že

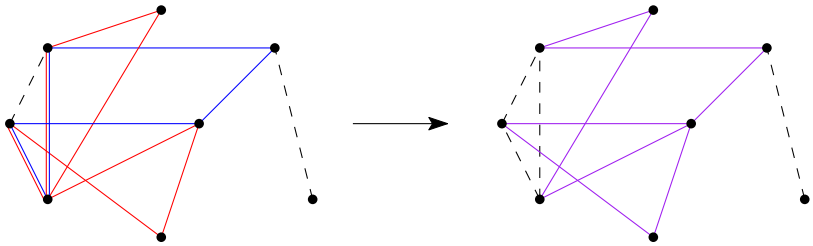
$$\dim M \leq \dim M^\perp = n - \dim M, \qquad \text{ekvivalentně } \dim M \leq \left\lfloor \frac{n}{2} \right\rfloor. \tag{19}$$

Jelikož $M \subseteq \mathrm{GF}(2)^n$ a $\dim M \leq \lfloor \frac{n}{2} \rfloor$, je $|M| = m \leq 2^{\lfloor n/2 \rfloor}$. □

2.3 Eulerovské a úplné bipartitní podgrafy

Definice Nechť $G = (V, E)$ je souvislý graf. *Spanning podgraf* (česky též „napnutý“ podgraf) grafu G je graf obsahující všechny vrcholy a některé hrany G.

Spanning podgraf ztotožníme s jeho charakteristickým vektorem délky $|E|$. Sčítání spanning podgrafů nad $\mathrm{GF}(2)$ je realizováno symetrickou diferencí.



Tvrzení Množina V_G všech spanning podgrafů G je vektorový prostor nad GF(2).

Definice *Eulerovský spanning podgraf* grafu G je takový spanning podgraf, který má všechny stupně sudé.

Množinu všech eulerovských spanning podgrafů G označme ε_G. Součtem dvou eulerovských podgrafů je zřejmě opět eulerovský podgraf, tedy ε_G je podprostorem V_G.

Lemma Platí $\dim \varepsilon_G = |E| - n + 1$, kde $n = |V|$.

Důkaz Nechť T je libovolná kostra grafu G. Pro každou hranu $e \in E(G)\backslash E(T)$ existuje právě jedna elementární kružnice K_e určená touto hranou. Množina

$$K_T = \{K_e \mid e \in E(G)\backslash E(T)\} \tag{20}$$

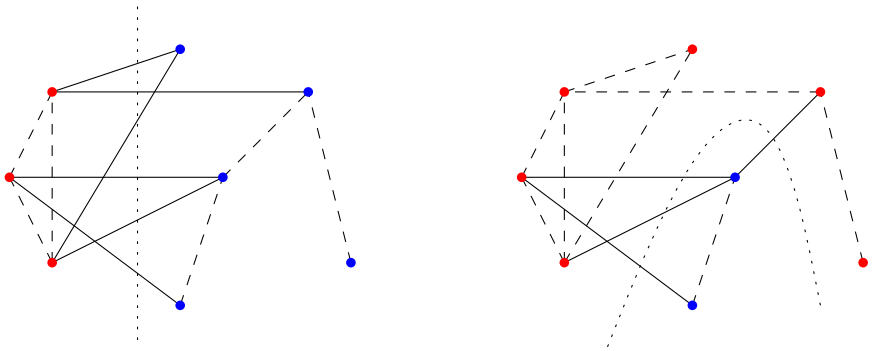
je lineárně nezávislá, neboť pro $e \in E(G)\backslash E(T)$ má kružnice K_e jako jediná nenulovou e-tou souřadnici.

Pro $L \in \varepsilon_G$ položme

$$L' = \sum_{e \in E(L)\backslash E(T)} K_e. \tag{21}$$

Graf $L+L'$ neobsahuje žádné hrany mimo kostru a současně je součtem eulerovských grafů, tedy je nutně eulerovský. Jediným eulerovským podgrafem kostry je 0, což znamená, že $L + L' = 0$ a $L = L'$. Tedy K_T tvoří bázi ε_G a platí $\dim \varepsilon_G = |K_t| = |E| - n + 1$. □

Definice *Úplný bipartitní spanning podgraf* grafu G je řez v G.



Množinu všech úplných bipartitních spanning podgrafů G označme β_G.

Lemma Množina β_G tvoří podprostor V_G, jehož množinou generátorů jsou všechny hvězdy v G. Platí $\dim \beta_G = n - 1$.

Důkaz Každý úplný bipartitní spanning podgraf je součtem hvězd ze všech vrcholů jedné z jeho partit. K nahlédnutí, že součet dvou úplných bipartitních spanning podgrafů je opět úplný bipartitní spanning podgraf, stačí oba grafy rozepsat na součet hvězd.

Všimněme si, že součet hvězd ze všech vrcholů G je 0, ovšem libovolných $n-1$ hvězd už tvoří lineárně nezávislou množinu. Netriviální lineární kombinace $n-1$ hvězd s koeficienty v GF(2) je totiž jen součet několika (aspoň jedné a nejvýše $n-1$) z nich. Ten není nikdy nulový, neboť v G existuje hrana, pro niž se v lineární kombinaci vyskytuje hvězda z právě jednoho z jejích koncových vrcholů. Tedy $\dim \beta_G = n - 1$.

Věta Platí $\varepsilon_G^\perp = \beta_G$.

Důkaz Buď $H \in \varepsilon_G$, $u \in V(G)$ a S_u hvězda z vrcholu u. Protože

$$\langle H, S_u \rangle = \deg_H u \bmod 2 = 0,$$

platí $\langle H, B \rangle = 0$ pro všechna $B \in \beta_G$, a tedy $H \in \beta_G^\perp$, což dává inkluzi $\varepsilon_G \subseteq \beta_G^\perp$.

Naopak, každý spanning podgraf H, pro který je $\langle H, S_u \rangle = 0$, má nutně všechny stupně sudé, a je tedy eulerovský. Proto je rovněž $\beta_G^\perp \subseteq \varepsilon_G$ a věta je dokázána. □

Věta Je-li M podprostorem $\mathrm{GF}(2)^n$, pak $(1, \ldots, 1) \in M + M^\perp$.

Důkaz Je-li $\dim(M \cap M^\perp) = 0$, pak $\dim(M + M^\perp) = n$, tedy zřejmě platí $(1, \ldots, 1) \in M$. Jestliže $\dim(M \cap M^\perp) > 0$, pak existuje $x = (x_1, \ldots, x_n) \in M \cap M^\perp$, $x \neq 0$. Dále

$$\langle x, (1, \ldots, 1) \rangle = \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} x_i^2 = \langle x, x \rangle = 0, \tag{22}$$

tedy $(1, \ldots, 1) \perp x$ a nutně platí $(1, \ldots, 1) \in M + M^\perp$. □

Důsledek Každý souvislý graf lze zapsat jako symetrickou diferenci eulerovského podgrafu a hranového řezu.

Důkaz V prostoru V_G je podle předchozí věty $G = (1, \ldots, 1) \in \varepsilon_G + \beta_G$, tedy existují grafy $H \in \varepsilon_G$ a $B \in \beta_G$ takové, že $H + B = G$. □

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 kapacita 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 dvou nezávislých 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.

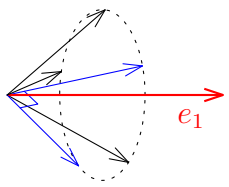
Definice Ortonormální reprezentace grafu G je funkce $\rho : V(G) \to \mathbb{R}^d$, $\|\rho(v)\| = 1$. Pro každé $(u, v) \notin E(G)$ platí $\rho(u) \perp \rho(v)$, neboli $\langle \rho(u), \rho(v) \rangle = 0$.

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 přechodu). Použijeme-li Pythagorovu větu, získáme:

$$||u||^2 = \sum_{i=1}^{d} \langle b_i, u \rangle^2 \tag{23}$$

Pokud aplikujeme tento poznatek na vektory $\rho(v)$ 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:

$$1 = ||u||^2 \geq \sum_{v \in A} \langle \rho(v), e_1 \rangle^2 \tag{24}$$

Tedy existuje alespoň jeden vrchol w, že $\langle \rho(w), e_1 \rangle^2 \leq 1/|A|$.

Stačí totiž vzít takový vrchol $w \in A$, že $\langle \rho(w), e_1 \rangle^2$ je minimální a dostáváme:

$$1 \geq \sum_{v \in A} \langle \rho(v), e_1 \rangle^2 \geq |A| \cdot \langle \rho(w), e_1 \rangle^2 \tag{25}$$

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:

$$\rho(v) = \rho_1(v_1) \otimes \rho_2(v_2) \tag{26}$$

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 $x_i y_i$.

Příklad Mějme vektory (a_1, a_2) a $b_1, b_2)$. Potom:

$$(a_1, a_2) \otimes b_1, b_2) = (a_1 b_1, a_1 b_2, a_2 b_1, a_2 b_2). \tag{27}$$

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

$$\langle x \otimes y, x' \otimes y' \rangle = \langle x, x' \rangle \cdot \langle y, y' \rangle \tag{28}$$

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

$$\sum_{ij}(x_i y_j)\cdot(x'_i y'_j) = \left(\sum_i x_i x'_i\right)\left(\sum_j y_j y'_j\right) \tag{29}$$

Zde již jednoduchou úvahou zjistíme, že ρ je stále ortonormální reprezentace: zjevně pro kolmé vektory jsou jejich tenzorové součiny 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)

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

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

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

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

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

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:

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

□

3.2 Funkční reprezentace grafu

Definice Nechť G je graf, X množina, $\mathbb{F}$ těleso a $\mathcal{F}\colon X \to \mathbb{F}$ systém funkcí. 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. $uv \notin E_G \Rightarrow f_u(c_v) = 0$

Jinými slovy, pro funkci f_a vrcholu a platí, že vrchol dostane vždy nenulový prvek a jeho nesousedi vždy nulový. O sousedech nehovoříme nic.

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.

$$M = \begin{pmatrix} f_1(c_1) & f_1(c_2) & \dots \\ f_2(c_1) & f_2(c_2) & \dots \\ \vdots & & \end{pmatrix} \tag{30}$$

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 $\mathcal{F}$,pro kterou platí $\dim \mathcal{F} \leq \dim \mathcal{F}_1 \cdot \dim \mathcal{F}_2$.

Důkaz Definujeme:

$$\begin{aligned} X &= X_1 \times X_2 \\ c_{(v_1,v_2)} &= (c_{v_1}, c_{v_2}) \\ f_{(v_1,v_2)}((x_1,x_2)) &= f_{v_1}(x_1) \cdot f_{v_2}(x_2) \end{aligned}$$

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 lemmatu o vztahu α a $\dim \mathcal{F}$, druhá z lemmatu o dimenzi součinu reprezentací. □

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

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

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

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

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 počet 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 lemmatu 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 matic

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 jejích vlastních čísel. Značíme $\mathrm{Sp}(A) = \{\lambda_1, \ldots, \lambda_n\}$.

Definice Podprostorem generovaným vlastním 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:

$$A(u+v) = Au + Av = \lambda u + \lambda v = \lambda(u+v) \tag{31}$$

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:

$$Au = \lambda u \tag{32}$$
$$Au - \lambda u = \vec{0} \tag{33}$$
$$(A - \lambda)u = \vec{0} \tag{34}$$
$$\det(A - \lambda E) = 0 \tag{35}$$

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:

$$GN(\lambda) \geq 1 \Leftrightarrow \lambda \in \mathrm{Sp}(A) \Leftrightarrow AN(\lambda) \geq 1 \tag{36}$$
$$\text{a} \quad GN(\lambda) \leq AN(\lambda) \tag{37}$$

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:

$$X^*AX = \underbrace{\left(\begin{array}{c} \vdots \\ \hline x_j^* \\ \hline \vdots \end{array}\right)}_{=X^*} \underbrace{\left(\begin{array}{c|c|c} \dots & \lambda_i x_i & \dots \end{array}\right)}_{=AX} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \tag{38}$$

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 $A, B \in \mathbb{C}^{n\times n}$, A a B jsou normální a komutují, tedy $AB = BA$. Potom existuje společná ortonormální báze složená z vlastních vektorů.

Důkaz Nejdříve dokážeme, že pokud je v vlastní vektor B, pak i Av je vlastní vektor B (pokud $Av \neq 0$).

Mějme $Bv = \lambda v$. Potom $A(Bv) = A(\lambda v) = \lambda Av$. Z komutativity plyne $B(Av) = \lambda(Av)$. Tedy máme, co jsme chtěli.

Nyní dokážeme, že A a B mají společný vlastní vektor, tedy že existuje nenulové v a skaláry λ, μ takové, že $Av = \lambda v$ a $Bv = \mu v$.

Nechť je λ vlastním číslem B a X přislušný prostor.

$$X = \{x : Ax = \lambda x\} \tag{39}$$

Z předchozího vidíme, že A mapuje X na X. Tedy A má vlastní vektor v X a z definice X už plyne, že A a B mají společný vlatní vektor.

Nyní už je vše připraveno. Najdeme jeden společný vlastní vektor v_1, BÚNO je jednotkové normy. Nyní jako W označme všechny vektory kolmé na v_1. Jak už víme, A i B mapují W na W. Ve W opět najdeme společný vlastní vektor (znormovaný) a označíme ho v_2. Mějme W' vektory kolmé na v_1 i v_2. Opět můžeme celý postup opakovat. Takto dostaneme hledanou ortonormální bázi.

□

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:

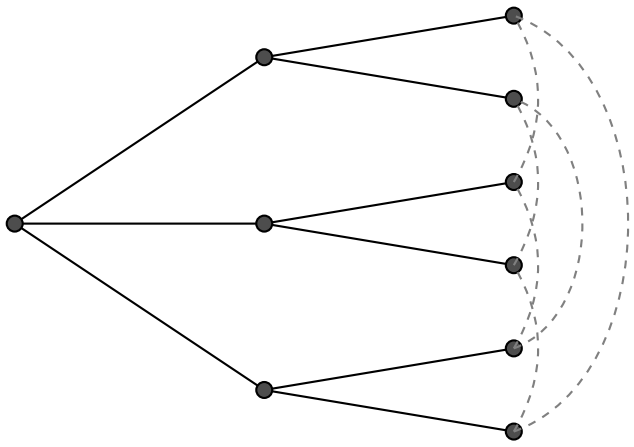
$$D^* = (X^*(AX))^* = (AX)^*X = X^*A^*X = X^*AX = D \tag{40}$$

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

4.2 Mooreovy grafy

V této části využijeme znalostí o vlastních číslech k přiblížení toho, jak mohou vypadat regulární grafy bez krátkých cyklů.

Nejprve si ukažme kolik může mít takový r-regulární graf bez krátkých cyklů (troj- a čtyřúhelníků) vrcholů. Vezměme jeden vrchol. Ten má r sousedů, z nichž žádné dva spolu nesousedí (vznikl by trojúhelník). Každý z nich má $r - 1$ nových sousedů. Ti musí být různí (vznikl by čtyřúhelník).



(41)

Dostáváme tedy odhad:

$$|V| \geq 1 + r + r(r-1) = r^2 + 1 \tag{42}$$

Definice Mooreův graf je takový r-regulární graf na $r^2 + 1$ vrcholech, který neobsahuje troj- a čtyřúhelníky.

Mooreovy grafy jsou tedy nejmenší možné regulární grafy bez krátkých cyklů. Podle následující věty není však až na výjimky možno tohoto ideálu dosáhnout.

Věta Nechť G je r-regulární Mooreův graf. Pak $r \in \{1, 2, 3, 7, 57\}$.

Poznámka
Pro $r = 1$ je hledaným grafem jedna hrana.
Pro $r = 2$ je to pětiúhelník.
Pro $r = 3$ je to Petersenův graf (viz obrázek 41).
Pro $r = 7$ je to takzvaný Hoffman-Singletonův graf.
Pro $r = 57$ není zatím známo, zda lze takový graf skutečně sestrojit.

Důkaz Pomocí poznatků o vlastních číslech získaných v předchozí části sestavíme rovnici, která nám přesně vymezí, co musí r splňovat.

Matici souslednosti grafu G označme A. Její druhá mocnina zachycuje počet sledů délky 2. Má tedy na diagonále stupeň (r). Ukážeme, že mimo diagonálu má oproti matici A prohozené nuly a jedničky. Je-li $uv \in E(G)$, pak mezi u a v nemůže existovat cesta délky 2 (vznikl by trojúhelník). Pokud $uv \notin E(G)$, tak se podíváme na konstrukci na obrázku 41. Bez újmy na obecnosti můžeme předpokládat, že u je 1. vrchol. Vidíme, že existuje cesta délky 2. Ta může být jen jedna, jinak by vznikl čtyřúhelník.

Dostáváme tedy:

$$A + A^2 = rE + (J - E), \tag{43}$$

kde E je jednotková matice a J je matice samých jedniček. Úpravou dostaneme polynomiální vztah

$$p(A) = A^2 + A + (1 - r)E = J. \tag{44}$$

Dále platí, že pro $\lambda \in \mathrm{Sp}(A)$ je $p(\lambda) \in \mathrm{Sp}(J)$. Spektrum J známe: obsahuje $n = r^2 + 1$ s násobností 1 a 0 s násobností $n - 1$.

Protože G je r-regulární, tak je r také jeho vlastním číslem. Dosazením do p dostaneme:

$$p(r) = r^2 + r + (1 - r) = r^2 + 1 = n. \tag{45}$$

Nyní zbývá vyřešit případ, kdy $p(\lambda) = 0$. Řešení této kvadratické rovnice je

$$\lambda_{1,2} = \frac{-1 \pm \sqrt{4r - 3}}{2}. \tag{46}$$

Násobnosti těchto kořenů označíme m_1, m_2. Jejich součet je zřejmě roven $n - 1 = r^2$. Využitím faktu, že stopa matice je suma vlastních čísel včetně násobností, získáme rovnici

$$0 = \mathrm{Tr}(A) = r + m_1\lambda_1 + m_2\lambda_2. \tag{47}$$

Její snadnou úpravou již získáme hledanou podmínku pro r

$$2r - r^2 + \sqrt{4r - 3}(m_1 - m_2) = 0 \tag{48}$$

Řešení rozdělíme na dva případy.

1. $\sqrt{4r - 3} \notin \mathbb{Q}$: potom $m_1 = m_2$ a tedy $r = 2$.

2. $\sqrt{4r-3} = s \in \mathbb{Q}$, což implikuje [1] $s \in \mathbb{N}$. Substitucí $4r-3 = s^2$ do rovnice 48 získáme

$$-s^4 + 2s^2 + 16(m_1 - m_2)s + 15 = 0. \tag{49}$$

Tudíž $s|15$. Pro jednotlivé hodnoty $s \in \{1, 3, 5, 15\}$, dostáváme $r \in \{1, 3, 7, 57\}$.

□

4.3 Silně regulární grafy

Dalším typem regulárních grafů jsou silně regulární grafy.

Definice r-regulární graf G se nazývá silně regulární, pokud existují $e, f \in \mathbb{N}$ taková, že:

- každá hrana $uv \in E(G)$ se vyskytuje právě v e trojúhelnících (tj. $|N(u) \cap N(v)| = e$) a zároveň
- každá nehrana $uv \notin E(G)$ se vyskytuje právě v f třešničkách (tj. $|N(u) \cap N(v)| = f$).

Poznámka 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 ($e = 0$, f velikost partity). Nejmenším nebipartitním silně regulárním grafem je pětiúhelník ($e = 0$, $f = 1$).

Věta Nechť G je silně regulární graf s parametry (r, e, f) na n vrcholech. Potom:

(a) $f - e = 1$, $n = 2r + 1$, $r = 2f$ nebo

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

Důkaz Technika tohoto důkazu je stejná jako u předchozí věty o Mooreových grafech.

Matici souslednosti grafu G označíme A. Její druhá mocnina má na diagonále r. Mimo diagonálu má buď hodnotu e pro případ kdy v A byla jednička (e trojúhelníků), nebo hodnotu f, pokud v A byla nula (f třešniček). Vidíme tedy vztah:

$$A^2 = rI + eA + f(J - I - A), \tag{50}$$

kde E je jednotková matice a J je matice samých jedniček. Úpravou dostaneme polynomiální vztah

$$p(A) = A^2 + (f - e)A + (f - r)E = fJ. \tag{51}$$

Dále platí, že pro $\lambda \in \mathrm{Sp}(A)$ je $p(\lambda) \in Sp(fJ)$. Spektrum fJ známe: obsahuje fn s násobností 1 a 0 s násobností $n - 1$.

[1] Odmocnina z přirozeného čísla je vždy přirozené číslo, či iracionální číslo, nikdy zlomek.

Protože G je r-regulární, tak je r také jeho vlastním číslem. Dosadíme tedy r do p:

$$p(r) = r^2 + (f-e)r + (f-r) \tag{52}$$
$$p(r) = r^2 + fr - er + f - r + 1 - 1 \tag{53}$$
$$p(r) = (r^2 - er + 1) + f(r+1) - (r+1) \tag{54}$$
$$p(r) = (r^2 - er + 1) + (r+1)(f-1). \tag{55}$$

Protože $f > 0$, tak platí $(r+1)(f-1) \geq 0$. Navíc zřejmě $e < r$, tudíž $r^2 - er + 1 > 0$. Jediné vlastní číslo, které toto splňuje je fn, proto

$$p(r) = fn \tag{56}$$

Nyní zbývá vyřešit případ, kdy $p(\lambda) = 0$. Řešení této kvadratické rovnice je

$$\lambda_{1,2} = \frac{e - f \pm s}{2}, \qquad s = \sqrt{(f-e)^2 - 4(f-r)}. \tag{57}$$

Násobnosti těchto kořenů označíme m_1, m_2. Jejich součet je zřejmě roven $n-1$. Využitím faktu, že stopa matice je suma vlastních čísel včetně násobností, získáme rovnici

$$0 = \mathrm{Tr}(A) = r + m_1\lambda_1 + m_2\lambda_2, \tag{58}$$

kterou upravíme

$$0 = r + \frac{m_1}{2}(e - f + s) + \frac{m_2}{2}(e - f - s) \tag{59}$$
$$0 = 2r + (e-f)(m_1 + m_2) + s(m_1 - m_2). \tag{60}$$

Řešení rozdělíme na dva případy.

1. $s \notin \mathbb{Q}$: potom $m_1 = m_2$. Potom se rovnice zjednoduší

$$0 = 2r + 2m_1(e-f) \tag{61}$$
$$m_1 = \frac{r}{f-e}. \tag{62}$$

Z toho vidíme, že

$$(f-e)|r, \quad f - e > 0, \quad n = 1 + 2m_1 = 1 + \frac{2r}{f-e}. \tag{63}$$

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

Po dosazení $f - e = 1$ do poslední rovnice 63 vidíme, že $n = 2r + 1$.
Po dosazení téhož do polynomu p a použitím vztahu 56 dostáváme

$$r^2 + r + (f - r) = f(2r+1). \tag{64}$$

Z toho již snadnou úpravou získáme hledané rovnosti

$$r = 2f, \qquad n = 4f + 1. \tag{65}$$

2. $s \in \mathbb{Q}$, což implikuje $s \in \mathbb{N}$. Vezmeme vztah pro násobnosti vlastních čísel a vztah 56 pro n

$$m_2 = n - 1 - m_1 = \frac{r^2 - er + 1 + (r+1)(f-1)}{f} - 1 - m_1. \tag{66}$$

Dosadíme do rovnice 60. Dostaneme:

$$0 = 2r + m_1(e - f + s) + (\frac{r^2 - er + 1 + (r+1)(f-1)}{f} - 1 - m_1)(e - f - s) \tag{67}$$

Což dále upravíme

$$m_1(-(e - f + s) + (e - f - s)) = 2r + \frac{1}{f}((r^2 - er + rf - r + f) - f)(e - f - s), \tag{68}$$

$$m_1(-2s) = 2r + \frac{1}{f}(r^2 - er + fr - r)(e - f - s), \tag{69}$$

$$m_1 = \frac{1}{2sf}(-2rf + r(r - e + f - 1)(-e + f + s)), \tag{70}$$

$$m_1 = \frac{r}{2sf}(r - 1 + f - e)(s + f - e) - 2f). \tag{71}$$

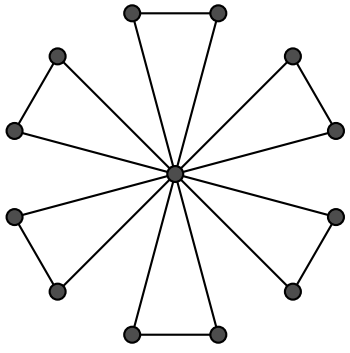
Protože m_1 je násobnost vlastního čísla λ_1, tak se jedná o přirozené číslo.

□

Věta (Friendship theorem) Nechť každí dva lidé mají právě jednoho společného známého. Pak existuje jeden (starosta), který zná všechny.

Neboli: nechť pro každé dva různé vrcholy $u, v \in V(G)$ platí $|N(u) \cap N(v)| = 1$. Potom existuje vrchol $c \in V$ takový, že $N(c) \cup \{c\} = V$.

Poznámka Friendship theorem tvrdí, že takový graf musí vypadat jako mlýn (hromádka trojúhelníků, které se stýkají v jednom centrálním vrcholu), viz obrázek 72.



šestilopatkový mlýn

(72)

Důkaz Pro spor předpokládejme, že takový vrchol c neexistuje. Nejprve si všimněme, že podmínka na množství sousedů implikuje, že G neobsahuje čtyřúhelník.

Nejdříve ukážeme, že G je regulárním grafem. Vezměme libovolné dva vrcholy u, v, které spolu nesousedí a označme $w_1, ..., w_k$ sousedy vrcholu u. Každý vrchol w_i musí mít jednoho společného souseda z_i s vrcholem v. Vrcholy z_i musí být různé, jinak by vznikl čtyřúhelník $(u, w_i, z_i = z_j, w_j)$. Vrchol v má tedy také alespoň k sousedů. Symetrickou úvahou pak dostáváme rovnost $deg(u) = deg(v)$.

Vrcholy u a v mají právě jednoho společného souseda c. Bez újmy na obecnosti můžeme předpokládat, že je to $c = w_1$. Jakýkoliv jiný vrchol $w \in V(G)$ již sousedí nanejvýše s jedním z vrcholů u a v (jinak by vznikl čtyřúhelník). Zopakováním předchozí úvahy pro vrchol se kterým w nesousedí vidíme $deg(w) = deg(u) = deg(v)$. Nakonec w_1 nemůže podle předpokladu být spojen se všemi vrcholy, proto i pro něj platí $deg(w_1) = deg(u) = deg(v)$.

Všechny vrcholy tedy mají stejný stupeň a graf G je k-regulární. Dokonce je silně regulární ($e = f = 1$).

Nyní se podíváme na sledy délky 2. Od každého vrcholu $x \in V$ jich vede k^2, protože G je k-regulární. Navíc z vrcholu x vede do každého jiného vrcholu $y \in V$ právě jedna cesta délky 2 ($e = f = 1$). Sledů z x do x je přesně k. Dostáváme tedy vztah, ze kterého vyjádříme počet vrcholů:

$$k^2 = (n-1) + k \tag{73}$$

$$n = k^2 - k + 1. \tag{74}$$

V dalším kroku zopakuje již známý postup pro hledání polynomiálního vztahu vlastních čísel. Matici souslednosti grafu G označíme A. Z rozboru sledů délky 2 provedeném v předchozím kroku vidíme, že matice A^2 má na diagonále k a všude mimo diagonálu jedničky. Dostáváme tedy vztah

$$A^2 = J + (k-1)I. \tag{75}$$

Vlastními čísly matice A^2 jsou tedy $n + (k-1) = k^2$ s násobností 1 a $k-1$ s násobností $n-1$. Vlastní čísla matice A^2 jsou druhými mocninami vlastních čísel matice A. Tudíž matice A má vlastní čísla k s násobností 1 a $\pm\sqrt{k-1}$ s násobnostmi m_1, m_2. Použitím vztahu pro stopu matice dostáváme:

$$0 = \mathrm{Tr}(A) = k + (m_1 - m_2)\sqrt{k-1}. \tag{76}$$

To upravíme do tvaru

$$k^2 = (m_2 - m_1)^2(k-1), \tag{77}$$

z něhož plyne, že $k - 1 | k^2$. To je však možné pouze pro $k = 1, 2$. Jinak totiž $k-1$ dělí $k^2 - 1$, nemůže tedy dělit zároveň k.

Hodnotě $k = 1$ odpovídá po dosazení do rovnice 74 graf K_1. Hodnotě $k = 2$ odpovídá graf K_3. Oba splňují jak předpoklady, tak závěr věty. Pro jakýkoliv jiný graf nastává spor, tudíž musel vrchol c sousedit se všemi ostatními. □

4.4 Rayleighův princip a proplétání

Věta (Rayleighův princip) Nechť A je matice $n \times n$ s ortonormální bazí z vlastních vektorů x_i a vlastními čísly $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. Potom:

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

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

$$\begin{aligned} x^* A x = x^*(Ax) = x^* \left(A \cdot \sum_{i=1}^{k} \alpha_i x_i \right) = x^* \left(\sum_{i=1}^{k} \alpha_i A x_i \right) = x^* \left(\sum_{i=1}^{k} \alpha_i \lambda_i x_i \right) = \\ = \sum_{i=1}^{k} \alpha_i \lambda_i x^* x_i = \sum_{i=1}^{k} \alpha_i \lambda_i \left(\sum_{j=1}^{k} \alpha_j x_j \right)^* x_i = \sum_{i=1}^{k} \alpha_i \lambda_i (\alpha_i x_i)^* x_i = \\ = \sum_{i=1}^{k} \lambda_i \underbrace{\alpha_i \overline{\alpha_i}}_{\geq 0} \geq \sum_{i=1}^{k} \lambda_k \alpha_i \overline{\alpha_i} = \lambda_k \sum_{i=1}^{k} \alpha_i \overline{\alpha_i} = \lambda_k x^* x \end{aligned}$$

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:

$$\lambda_1 \geq \mu_1 \geq \lambda_2 \geq \cdots \geq \mu_{n-1} \geq \lambda_n \tag{78}$$

Důkaz Dokazujeme $\lambda_k \geq \mu_k \geq \lambda_{k+1}$. 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):

$$S_1 := \mathcal{L}\{x_k, \ldots, x_n\} \subseteq \mathbb{C}^n \tag{79}$$
$$S_2 := \mathcal{L}\{y_1, \ldots, y_k\} \subseteq \mathbb{C}^n \tag{80}$$

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:

$$\mu_k \leq \frac{y^* B y}{y^* y} = \frac{x^* A x}{x^* x} \leq \lambda_k \tag{81}$$

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 $S^TS = I$. Definujeme $B := S^TAS$ 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 Rayleighův princip podobně jako v předchozím tvrzení. Všimneme si, že:

$$x \in \mathcal{L}\{S^Tx_k, \ldots, S^Tx_n\}^\perp \Leftrightarrow Sx \in \mathcal{L}\{x_k, \ldots, x_n\}^\perp \tag{82}$$

Stačí si opět vzít vhodný prvek x z průniku:

$$x \in \mathcal{L}\{S^Tx_k, \ldots, S^Tx_n\}^\perp \cap \mathcal{L}\{y_1, \ldots, y_k\} \tag{83}$$

A můžeme použít Reileighův princip:

$$\lambda_k \geq \frac{(Sx)^TASx}{(Sx)^TSx} = \frac{x^TBx}{x^Tx} \geq \mu_k \tag{84}$$

$$\tag{85}$$

Navíc platí, že pokud $\lambda_i = \mu_i$, potom:

$$\frac{x^TBx}{x^Tx} = \lambda_i \quad \Rightarrow \quad x^TBx = x^Tx\lambda_i \quad \Rightarrow \quad Bx = \lambda_i x \tag{86}$$

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 $\widetilde{S}$ matici incidence blokové A:

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

$\widetilde{S} \cdot \widetilde{S}^T$ = diagonální matice $(x_1, x_2, \ldots, x_m) = D$

$S := \widetilde{S} \cdot D^{-\frac{1}{2}}$

$\widetilde{B} = S^TAS$

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:

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

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

„$\Rightarrow$“ 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[2], 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 $\left\{\rho P_G^k\right\}_k$ konverguje $\Leftrightarrow$ G není bipartitní.

Důkaz

[2]Někdy též zvaná „stacionární“.

„⇒“ 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 vyjádříme distribuci po k iteracích: **TODO:** distribucí násobíme zleva, dále (levým) vlastním vektorem 1 není vektor jedniček, ale stabilní distribuce π ...

$$P_G^k \rho = P_G^k \sum_i a_i p_i = \sum_i P_G^k a_i p_i \tag{87}$$

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

$$\sum_i \lambda_i^k a_i p_i \tag{88}$$

TODO: P není matice sousednosti... 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:

$$\lim_{k\to\infty} \left(\lambda_1^k a_1 p_1 + \sum_{i>1} \lambda_i^k a_i p_i \right) = a_1 p_1 = \pi \tag{89}$$

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

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.

$$\|P_G^t \rho - \pi\|_2^2 = \left\| \sum_{i>1} \lambda_i^t a_i p_i \right\|_2^2 = \sum_{i>1} \lambda_i^{2t} \|a_i p_i\|_2^2 \tag{90}$$

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

$$\leq \mu^{2t} \sum_i \|a_i p_i\|_2^2 = \mu^{2t} \|\rho\|_2^2 \leq \mu^{2t} \tag{91}$$

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

$$\|P_G^t \rho - \pi\|_2 \leq \mu^t \tag{92}$$

$$\|P_G^t \rho - \pi\|_1 \leq \mu^t \sqrt{n} \tag{93}$$

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 $h_v(G) = \min\limits_{S\subseteq V, |S|\leq \frac{n}{2}} \frac{|N(S)\setminus S|}{|S|}$
- 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 $= d - \lambda_2$
- $\lambda = \max\{\lambda_2, -\lambda_n\}$ (druhé největší vlastní číslo v absolutní hodnotě)

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 $\lambda_2 \geq \frac{x^T A x}{x^T x}$ (Rayleighův 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) $\forall G$ d-regulární, $\forall S, T \subseteq V, S \cap T = \emptyset : |e(S,T) - \frac{d \cdot |S| \cdot |T|}{n}| \leq \lambda d \cdot \sqrt{|S| \cdot |T|}$

Důkaz Buďte χ_S, χ_T charakteristické vektory S a T. $u = (1, 1, \dots)$ je první vlastní vektor. $\chi_S^\perp$ značí vektor kolmý na u.

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

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

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 Samoopravné kódy

Definice Samoopravný kód C s parametry $(n, M)_q$ nad abecedou A je podmnožina A^n, kde $|A| = q$ a $|C| = M$. Prvkům množiny C říkáme kódová slova.

Nejčastěji A je konečné těleso $GF(q)$ o q prvcích nebo $A = \{0, \ldots, q-1\}$. Pokud C je vektorový podprostor nad tělesem A, pak C nazýváme lineárním kódem. Množinu A^n navíc vybavíme Hammingovou metrikou $d(\ ,\ )$. Pro dvě slova $x, y \in A^n$ se složkami x_i resp. y_i platí

$$d(x, y) = |\{i \mid x_i \neq y_i\}|.$$

Minimální vzdálenost kódu je pak definována jako $d = \min_{x \neq y \in C} d(x, y)$. Mluvíme pak o $(n, M, d)_q$ kódu.

Chceme, aby kód měl co největší minimální vzdálenost (při co největší mohutnosti). To souvisí s tím, že pokud vysíláme kódové slovo $c \in C$, může během přenosu dojít k chybám (uvažujeme pouze změnu složky nikoliv zkrácení délky) a druhá strana přijme slovo $y = c + e$, kde e je chybové slovo. Příjemce se pak snaží chybu detekovat a případně opravit y na nejbližší kódové slovo $c' \in C$ (vše je měřeno Hammingovou metrikou). Pokud kódová slova budou co nejdále od sebe, je detekce a oprava y na správné kódové slovo c (tj. $c = c'$) více pravděpodobná. Přesněji pokud počet chyb (což je počet nenulových složek chybového slova e) je $\leq d - 1$ je možné chybu detekovat (přijmeme-li nekódové slovo, víme, že nastala chyba). Pokud pokud počet chyb je $\leq \lfloor \frac{d-1}{2} \rfloor =: t$ je možné chybu opravit. Označme $N_t(c) = \{x \in A^n \mid d(c, x) \leq t\}$ okolí slova c do vzdálenosti t. Vidíme, že okolí $N_t(c)$ pro všechna $c \in C$ jsou disjunktní, kde C má minimální vzdálenost d a t je definováno výše.

Tvrzení (Hammingův odhad) Mějme $(n, M, d)_q$ kód C. Označme $t = \lfloor \frac{d-1}{2} \rfloor$. Pak

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

Důkaz Stačí si uvědomit, že okolí jsou disjunktní a obsahují všechny stejně slov (zde nezáleží na středu okolí). Dostáváme tak:

$$q^n \geq \sum_{c \in C} |N_t(c)| = M \cdot \sum_{i=0}^{t} \binom{n}{i} (q-1)^i.$$

□

Definice Kódy, která nabývají rovnosti v Hammingově odhadu nazýváme perfektními.

Nyní si ukážeme základní příklady perfektních kódů. Mezi ty triviální patří totální $(n, q^n, 1)$ kód obsahující všechna slova z A^n, opakovací $(n, 2, n)$ kód pro lichou délku n a jednoprvkový kód.

Každý lineární kód můžeme popsat jeho bází. Generující matice G o rozměrech $k \times n$ lineárního (n, q^k) kódů C nad $GF(q)$ má v řádcích zapsanou jeho bázi. Kontrolní matice lineárního kódu C je taková matice H o rozměrech $(n-k) \times n$, že $c \in C \Leftrightarrow Hc^T = 0$. Platí $HG^T = 0$. Lineární kód můžeme jednoznačně popsat jeho generující nebo kontrolní maticí.

Definice Hammingův kód $\mathcal{H}(r, q)$ je určen svojí kontrolní matici o rozměrech $r \times \frac{q^r-1}{q-1}$, která obsahuje ve sloupcích všechny po dvou lineárně nezávislé vektory nad $GF(q)$ délky r. Kód $\mathcal{H}(r, q)$ je 1-perfektní $(\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3)_q$ lineární kód.

Definice Uvažme matici $G' = (I_{12} \mid Q)$, kde Q je doplněk matice sousednosti dvacetistěnu. Matice G' generuje $(24, 12, 8)_2$ kód $\mathcal{G}_{24}$ nad $GF(2)$. Vynecháním libovolné fixní souřadnice kódových slov v $\mathcal{G}_{24}$ obdržíme $(23, 12, 7)_2$ kód $\mathcal{G}_{23}$. Kód $\mathcal{G}_{23}$ se nazývá binární Golayův 3-perfektní kód.

Definice Uvažme matici $G = (I_6 \mid Q)$, kde

$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 & 1 \\ 1 & 0 & 1 & 2 & 2 \\ 2 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \end{pmatrix}.$$

Matice G generuje $(11, 6, 5)_3$ kód $\mathcal{G}_{11}$ nad $GF(3)$. Kód $\mathcal{G}_{11}$ se nazývá ternární Golayův 2-perfektní kód.

7.2 Lloydova věta

Nyní směřujeme k charakterizující větě, která říká, že ve skutečnosti žádné jiné perfektní kódy než výše uvedené nad abecedou mohutnosti mocniny prvočísla neexistují. Důkaz, který uvedeme je kombinatorický. Jádro důkazu spočívá v důkazu Lloydovy věty, která dává silné omezení na existenci perfektních kódů.

Věta Definujme Lloydův polynom v proměnné x stupně t

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

Pokud existuje t-perfektní kód délky n nad abecedou mohutnosti q, pak $L_t(x)$ má t různých celočíselných kořenů mezi 1 a n.

K důkazu Lloydovy věty budeme potřebovat vlastnosti vzdálenostně regulárních grafů.

7.3 Vzdálenostně regulární grafy

Definice Uvažme graf $\Gamma = (V, E)$, že $V(G) = A^n$ a hrana mezi vrcholy u, v vede právě tehdy, když $d(u, v) = 1$, tedy liší se právě v jedné souřadnici. Kód v grafu Γ příslušející kódu C je pak podmnožina vrcholů, které odpovídají kódovým slovům C.

Graf Γ je speciálním případem vzdálenostně regulárního grafu. Poznatky z této sekce na závěr aplikujeme právě na Γ. Po celou dobu této podkapitoly pracujeme pouze s vzdálenostně regulárními grafy.

Definice Graf G je vzdálenostně regulární, pokud existují konstanty s_{hij} tak, že pro $\forall u, v \in V(G), d(u, v) = j$ je

$$|\{w : d(u, w) = h, d(w, v) = i\}| = s_{hij}.$$

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

Lemma Platí

$$z_{mi} = z_{m-1,i-1} \cdot s_{1,i-1,i} + z_{m-1,i} \cdot s_{1,i,i} + z_{m-1,i+1} \cdot s_{1,i+1,i},$$

kde 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 trojúhelníkové nerovnosti). V rovnici sčítáme vrcholy sousedící s u, které jsou ve vzdálenosti $i - 1$, i a $i + 1$ od v.

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

Definice Definujme vzdálenostní matice $A_0 = I, A_1 = A, A_2, \ldots, A_d$ grafu G. Sloupce a řádky jsou číslovány vrcholy grafu.

$$(A_i)_{uv} = \begin{cases} 1 & d(u, v) = i \\ 0 & \text{jinak} \end{cases}$$

Věta $\dim \mathcal{A}(G) = d + 1$, kde d je průměr G.[3] Bází $\mathcal{A}(G)$ jsou výše definované matice $A_0, A_1, A_2, \ldots, A_d$.

Důkaz Platí $A^m = \sum_{i=0}^{d} z_{mi} A_i$ pro libovolné $m \in \mathbb{N}$. Matice $A_0, A_1, A_2, \ldots, A_d$ tedy generují celý prostor $\mathcal{A}(G)$ a zároveň jsou lineárně nezávislé a proto $\dim \mathcal{A}(G) = d + 1$.

□

Definice Matice B_h je velikosti $(d + 1) \times (d + 1)$ a definujme ji předpisem

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

Navíc označme $B = B_1$.

Lemma Existuje homomorfismus vektorových prostorů $\widehat{\ } : \mathcal{A}(G) \to \widehat{\mathcal{A}(G)}$ takový, že $\widehat{A_h} = B_h$ pro $h = 0, \ldots, d$.

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

Důkaz Nejdříve si všimněme, co se děje v následujícím součinu matic:

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

V sumě je přičtena 1 pokaždé, když pro vrchol w platí, že $d(u,w) = h$ a $d(w,v) = i$, což je přesně definice s_{hij} pro $j = d(u,v)$. Máme tedy:

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

Což je vlastně lineární kombinace prvků z báze s koeficienty s_{hij}. Matici B_h obsahuje v i-tém řádku souřadnice $A_h A_i$ vzhledem k bázi $\{A_0, A_1, \ldots, A_d\}$, čili vektor $(s_{hi0}, \ldots, s_{hid})$. Hledaný homomorfismus je tedy transpozice regulární reprezentace levého násobení v $\mathcal{A}(G)$ vzhledem k $\{A_0, A_1, \ldots, A_d\}$. □

Lemma $B = B_1$ je tridiagonální matice. Všechny sloupcové součty jsou stejné a jsou rovny $k = s_{110}$. Navíc $s_{100} = 0$ a $s_{101} = 1$.

$$B = \begin{pmatrix} \ddots & & 0 \\ & \ddots & \\ 0 & & \ddots \end{pmatrix}$$

Důkaz Matice je tridiagonální, protože $s_{1,i,j}$ dává smysl jen pro $i \in \{j-1, j, j+1\}$ (z trojúhelníkové 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. □

Následující známy výsledek z teorie matic uvádíme bez důkazu.

Poznámka B je tridiagonální matice $\Rightarrow \forall$ její vlastní čísla jsou různá.

7.4 Charakteristické polynomy

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

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

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

7.5 Lloydova věta

Věta Pokud existuje t-perfektní kód s parametry (n, q), pak $L_t(x)$ (definice níže) má t různých celočíselných kořenů mezi 1 a n.

$$L_t(x) = \sum_{j=0}^{t} (-1)^j (q-1)^{t-j} \binom{x-1}{j} \binom{n-x}{t-j} \tag{94}$$

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.

7.6 Vzdálenostně regulární grafy

Definice Vzdálenostně regulární graf je regulární a $\exists s_{hij}$ takové, 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:

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

7.7 Reprezentace vzdálenostně regulárních grafů polynomy

Věta $\dim \mathcal{A}(G) = d + 1$, kde d je průměr G.[4]

Důkaz $A^m = \sum_{i=0}^{d} Z_{mi} A_i$
$i > m \Rightarrow Z_{mi} = 0$
$A^0 = Z_{0,0} \cdot A_0 = A_0$
$A^1 = Z_{1,0} \cdot A_0 + Z_{1,1} \cdot A_1 = A_1$
$A^2 = Z_{2,0} \cdot A_0 + Z_{2,1} \cdot A_1 + Z_{2,2} \cdot A_2$
$\vdots$
$A^d = Z_{d,0} \cdot A_0 + Z_{d,1} + \cdots + Z_{d,d} \cdot A_d$

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 $\dim \mathcal{A}(G) = d + 1$. □

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

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}:

$$(B_h)_{ij} := s_{hij} \tag{95}$$

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:

$$(A_h A_i)_{uv} = \sum_w (A_h)_{uw} \cdot (A_i)_{wv} = s_{hid(u,v)} \tag{96}$$

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)?

$$A_h A_i = \sum_{j=0}^{d} s_{hij} A_j \tag{97}$$

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) B_1 je tridiagonální matice. Všechny sloupcové součty jsou stejné a jsou rovny k.

$$B_1 = \begin{pmatrix} \ddots & \ddots & 0 \\ \ddots & \ddots & \ddots \\ 0 & \ddots & \ddots \end{pmatrix}$$

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 B_1 je tridiagonální matice $\Rightarrow \forall$ vlastní čísla jsou různá.

7.8 Charakteristické polynomy

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

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

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

Lemma (O charakteristickém polynomu) Nechť $\lambda_1, \ldots, \lambda_d \in \mathrm{Sp}(B_1)$ takové, že jsou různá od k . Potom pro $i = 1, \ldots, d$ platí:

$$v_o(\lambda_i) + \ldots + v_d(\lambda_i) = 0$$

neboli $v_o(\lambda) + \ldots + v_d(\lambda) = c \cdot (\lambda - \lambda_1) \cdot \ldots \cdot (\lambda - \lambda_d)$.

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

$$AA_i = \sum_{j=0}^{d} s_{1ij}A_j = s_{1,i,i-1}A_{i-1} + s_{1,i,i}A_i + s_{1,i,i+1}A_{i+1}$$

Tj. $v_i(A) = A_i$. Po aplikaci homomorfismu $\widehat{\ }$ dostáváme $v_i(B) = B_i$.

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

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

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

Důkaz

$$(TA)_{iu} = \sum_w T_{iw} A_{wu} = s_{i,1,d(u,z)}$$
$$(BT)_{iu} = \sum_j B_{ij} T_{ju} = s_{1,i,d(u,z)} = s_{i,1,d(u,z)}$$
$$TA = BT \quad \Rightarrow \quad TA^2 = BTA = B^2T \quad \Rightarrow \quad TA^m = B^mT$$
$$Tp(A) = p(B)T \quad \Rightarrow \quad TX = \widehat{X}T$$

□

Definice Definujme si pomocné polynomy:

$$x_i(\lambda) = v_0(\lambda) + \cdots + v_i(\lambda)$$
$$S_t = x_t(A) = A_0 + A_1 + \cdots + A_t$$

Kde S_t je matice, která označuje dvojce vrcholů jedničkou, pokud jsou vzdálené nanejvýš t (je to součet vzdálenostních matic do t).

Lemma Nechť C je perfektní kód v grafu G. Ať c je jeho charakteristický vektor C. 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 přímo z definice perfektního kódu. □

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

Důkaz Mějme $z_0 = z \in C$ a $z_1, z_2, \ldots, z_t \in C$ takové, že $d(z, z_i) = i$ pro $i = 1, 2, \ldots, t$. Platí $(T_{z_i} \cdot c)_j = \delta_{ij}$ (Kroneckerovo delta = 1 pro $i = j$, 0 jinak). Tedy vektory $T_{z_i} \cdot c$ pro $i = 0, 1, \ldots, t$ jsou lineárně nezávislé. Navíc dostáváme, že

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

$\overset{1}{=}$ plyne z lemma o zastřešování, $\overset{2}{=}$ plyne z předchozího lemmatu. Výsledný vektor je pro všechny volby 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. Pišme

$$u_i = T_{z_i} \cdot c - T_{z_0} \cdot c \qquad i = 1, 2, \ldots, t$$
$$\widehat{S}_t u_i = \widehat{S}_t T_{z_i} \cdot c - \widehat{S}_t T_{z_i} \cdot c = \begin{pmatrix} k_0 \\ \vdots \\ k_d \end{pmatrix} - \begin{pmatrix} k_0 \\ \vdots \\ k_d \end{pmatrix} = \vec{0} \quad \Rightarrow \quad u_i \in \operatorname{Ker} \widehat{S}_t$$

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

7.9 Důkaz Lloydovy věty

Zde začnou věci dávat větší smysl. Nejdříve dokážeme pomocí výše zmíněných lemmat 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 $\widehat{S}_t$:

$$\operatorname{Sp}(B) = \{k, \lambda_1, \ldots, \lambda_d\} \tag{98}$$

$$\operatorname{Sp}(\widehat{S}_t) = \{x_t(k), x_t(\lambda_1), \ldots, x_t(\lambda_d)\} \tag{99}$$

Z povídání o B (je tridiagonální) víme, že její vlastní čísla jsou různá. Dle pomocného lemmatu výše má $\widehat{S}_t$ dimenzi jádra alespoň t, a tedy 0 je její alespoň t-násobné vlastní číslo – tj. alespoň t hodnot z $\lambda_1, \ldots, \lambda_d$ jsou kořeny x_t (k není kořen x_t **TODO:** proč?). Stupeň x_t je nejvýše t (z definice), takže toto jsou všechny jeho kořeny **TODO:** proč není identicky nulový.

Dohromady tedy kořeny x_t jsou podmnožinou kořenů x_d (a žádné kořeny nejsou vícenásobné), takže x_t dělí x_d. □

Věta (Lloyd) Pokud existuje t-perfektní kód s parametry (n, q), pak $L_t(x)$ (definice níže) má t různých celočíselných kořenů mezi 1 a n.

$$L_t(x) = \sum_{j=0}^{t} (-1)^j (q-1)^{t-j} \binom{x-1}{j} \binom{n-x}{t-j} \tag{100}$$

Důkaz Nejprve definujme graf Γ: Jeho vrcholy jsou slova délky n nad abecedou velikosti q a hrany spojují právě slova lišící se v jednom znaku. Tento graf je vzdálenostně regulární s průměrem $d = n$. Speciálně budou užitečné následující jeho parametry[5]:

$$s_{1,i,i-1} = (q-1)(n+1-i) \tag{101}$$

$$s_{1,i,i} = (q-2)i \tag{102}$$

$$s_{1,i,i+1} = i+1 \tag{103}$$

Nyní bude naším cílem upočítat polynomy x_i. K tomu začneme od rekurzivního vzorce pro polynomy v_i, z něj spočteme jejich vytvořující funkci[6] $V(t) = \sum_{i=0}^{\infty} v_i(\lambda) t^i$ a od té dojdeme k vytvořující funkci $X(t) = \sum_{i=0}^{\infty} x_i(\lambda) t^i$ pro x_i. Začneme z definice v_i:

$$v_0(\lambda) = 1 \tag{104}$$

$$v_1(\lambda) = \lambda \tag{105}$$

$$s_{1,i,i-1} v_{i-1}(\lambda) + (s_{1,i,i} - \lambda) v_i(\lambda) + s_{1,i,i+1} v_{i+1}(\lambda) = 0 \quad \forall i \in \{1, \ldots, d\} \tag{106}$$

[5] Hodnoty těchto parametrů lze odvodit rozebráním, které pozice ve slově odpovídajícím vrcholu u mohu změnit a jak, abych získal w.

[6] Zde je dobré vědět, jak se to dělá, ale samotný výpočet je asi možné přeskočit.

Dosadíme za $s_{1,i,*}$:

$$(q-1)(n+1-i)v_{i-1}(\lambda) + ((q-2)i - \lambda)v_i(\lambda) + (i+1)v_{i+1} = 0 \tag{107}$$

Nyní bychom rádi dosadili V za v_i, abychom V upočítali, ale k tomu se potřebujeme zbavit i. Z vlastností vytvořujících funkcí víme:

$$\sum_{i=0}^{\infty} v_{i+1}(\lambda)x^i = \frac{V(x)-1}{x} \tag{108}$$

$$\sum_{i=0}^{\infty} iv_i(\lambda)x^i = x\frac{\mathrm{d}V(x)}{\mathrm{d}x} \tag{109}$$

$$\sum_{i=0}^{\infty} (i+1)v_{i+1}(\lambda)x^i = \frac{\mathrm{d}V(x)}{\mathrm{d}x} \tag{110}$$

$$\sum_{i=0}^{\infty} (i+2)v_{i+2}(\lambda)x^i = \frac{1}{x}\left(\frac{\mathrm{d}V(x)}{\mathrm{d}x} - \lambda\right) \tag{111}$$

Přepíšeme vztah pro v_i, aby platil od $i = 0$, dosadíme a upravíme:

$$(q-1)nv_i - (q-1)iv_i + (q-2)(i+1)v_{i+1} - \lambda v_{i+1} + (i+2)v_{i+2} = 0 \tag{112}$$

$$(q-1)nV(x) - (q-1)x\frac{\mathrm{d}V(x)}{\mathrm{d}x} + (q-2)\frac{\mathrm{d}V(x)}{\mathrm{d}x} - \lambda\frac{V(x)-\lambda}{x} + \frac{1}{x}\left(\frac{\mathrm{d}V(x)}{\mathrm{d}x} - \lambda\right) = 0 \tag{113}$$

$$V(x)\left((q-1)n - \frac{\lambda}{x}\right) - \frac{\mathrm{d}V(x)}{\mathrm{d}x}\left((1-q)x + (q-2) + \frac{1}{x}\right) + \frac{\lambda}{x} - \frac{\lambda}{x} = 0 \tag{114}$$

$$V(x)\left((1-q)nx - \lambda\right) - \frac{\mathrm{d}V(x)}{\mathrm{d}x}\left((q-1)x^2 + (q-2)x + 1\right) = 0 \tag{115}$$

Nyní přeskupíme a zintegrujeme pomocí rozkladu na parciální zlomky:

$$\int \frac{\mathrm{d}V}{V} = \int \frac{(q-1)nx - \lambda}{(1-q)x^2 + (q-2)x + 1}\,\mathrm{d}x \tag{116}$$

$$\ln V + c = \int \frac{(n+\lambda)(q-1)}{q(1+x(q-1))}\,\mathrm{d}x + \int \frac{\lambda - n(q-1)}{q(1-x)}\,\mathrm{d}x \tag{117}$$

$$= \frac{(n+\lambda)(q-1)}{q}\int \frac{1}{1+x(q-1)}\,\mathrm{d}x + \frac{\lambda - n(q-1)}{q}\int \frac{1}{1-x}\,\mathrm{d}x \tag{118}$$

$$= \frac{(n+\lambda)(q-1)}{q}\frac{\ln(1+x(q-1))}{q-1} + \frac{\lambda - n(q-1)}{q}(-1)\ln(1-x) \tag{119}$$

$$= \frac{n+\lambda}{q}\ln(1+x(q-1)) - \frac{\lambda - n(q-1)}{q}\ln(1-x) \tag{120}$$

Nyní se zbavíme c – víme, že $V(x=0)=1$, takže $c=0$ – a logaritmů.

$$V = (1+x(q-1))^{\frac{n+\lambda}{q}}(1-x)^{\frac{n(q-1)-\lambda}{q}} \tag{121}$$

Hurá máme V, nyní chceme X – x_i je posloupnost částečných součtů v_i a jak si všichni dobře pamatujeme posloupnost částečných součtů získáme z vytvořující funkce jejím vynásobením vytvořující funkcí posloupnosti samých jedniček $J(x) = \sum_{i=0}^{\infty} x^i = \frac{1}{1-x}$:

$$X = VJ = (1+x(q-1))^{\frac{n+\lambda}{q}}(1-x)^{\frac{n(q-1)-\lambda}{q}-1} \tag{122}$$

Provedeme substituci $y = n - \frac{n+\lambda}{q}$ a rozvineme dle zobecněné binomické věty, abychom měli explicitně vyjádřený polynom x_t:

$$X(x) = (1+x(q-1))^{n-y}(1-x)^{y-1} \tag{123}$$

$$= \left(\sum_{i=0}^{\infty}\binom{n-y}{i}(q-1)^i x^i\right)\left(\sum_{i=0}^{\infty}\binom{y-1}{i}(-x)^i\right) \tag{124}$$

$$= \sum_{i=0}^{\infty}\left(\sum_{j=0}^{i}\binom{n-y}{j}(q-1)^j\binom{y-1}{i-j}(-1)^{i-j}\right)x^i \tag{125}$$

$$x_t(\lambda) = \sum_{j=0}^{t}\binom{n-y(\lambda)}{j}(q-1)^j\binom{y(\lambda)-1}{t-j}(-1)^{t-j} \tag{126}$$

Nyní zásadní trik: všimneme si, že když $y \in \{1,\ldots,n\}$, tak X (v uzavřeném tvaru) je polynom v x stupně $\leq n-1$ – tedy koeficient před x^t je 0 a $\lambda = n(q-1) - qy$ je kořenem x_n. Takto máme n různých kořenů x_n, a protože je to polynom stupně nejvýše n, jsou to všechny jeho kořeny. Z toho a aplikace Lloydovy věty pro vzdálenostně regulární grafy plyne, že $L_t(y)$ musí mít t různých kořenů mezi čísly 1 až n.

$$L_t(y) = \sum_{j=0}^{t}\binom{n-y}{j}(q-1)^j\binom{y-1}{t-j}(-1)^{t-j} \tag{127}$$

□

7.10 Charakterizace perfektních kódů

Pro každý kód C opravující t chyb platí nerovnost

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

označována také jako Sphere packing (dokázaná na začátku sekce). Pro perfektní kódy pak platí rovnost. Než se pustíme do charakterizace perfektních kódů nad abecedou velikosti mocniny prvočísla, dokážeme nutnou podmínku pro existenci takovýchto kódů.

Věta Nechť $q = p^r$, kde p je prvočíslo. Pak existuje $\alpha \in \mathbb{N}$ takové, že

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i = q^\alpha.$$

Důkaz Ze Sphere packingu dostaneme

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i = \frac{q^n}{|C|}. \tag{128}$$

Tedy, $|C|$ musí dělit $q^n = p^{rn}$ a $\frac{q^n}{|C|} = p^\beta$ pro nějaké $\beta \in \mathbb{N}$. Dále použijeme následující rovnost (jednoduše dokazatelnou indukcí)

$$\sum_{i=0}^{n} \binom{n}{i} (q-1)^i = q^n. \tag{129}$$

Když od sebe odečteme rovnice 129 a 128, dostaneme

$$q^n - p^\beta \equiv 0 \pmod{q-1},$$

z čehož vyplývá $p^\beta = q^\alpha$ pro nějaké $\alpha \in \mathbb{N}$. □

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 a q (Hammingův)

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

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

Důkaz je technicky náročný a budeme se jím zabývat po zbytek sekce. Po celou dobu budeme předpokládat, že q je mocnina nějakého prvočísla. Základem je Lloydova věta a právě dokázaná nutná podmínka pro existenci těchto kódů. Nejprve se pro malé hodnoty parametrů ukáže, zda pro dané hodnoty kódy existují či nikoli. Pak se pro obecný případ udělá horní odhad parametrů pomocí Lloydovy věty. A pro konečný počet případů, pro které by kódy mohly existovat, bylo dokázáno počítačem, že neexistují. Pro $t = 1$ ze Sphere packingu dostaneme $1 + n(q-1) = q^\alpha$, tedy $n = \frac{q^\alpha-1}{q-1}$, což jsou přesně velikosti Hammingových kódů. Dále budeme předpokládat, že $t \geq 2$.

Věta 2-perfektní kód existuje jen pro $q = 3$ (Golayův kód).

Důkaz neexistence 2-perfektního kódu nad jinou než tří prvkovou abecedou uvedeme jen pro $q = 2$.

Věta Pro $q = 2$ neexistuje 2-perfektní kód.

Důkaz Z dokázané nutné podmínky pro existenci perfektního kódu dostaneme:

$$1 + n + \binom{n}{2} = q^{\alpha} \tag{130}$$
$$2 + 2n + n(n-1) = q^{\alpha+1} \tag{131}$$
$$7 + (2n+1)^2 = q^{\alpha+3} \tag{132}$$

A dále pak z Lloydovy věty dostaneme:

$$L_2(x) = \binom{n-x}{2} - (x-1)(n-x) + \binom{x-1}{2}$$
$$2L_2(x) = n^2 + n + 2 + 4x^2 - 2(n+1)2x$$

Provedeme substituci $y = 2x$ a za $n^2 + n + 2$ dosadíme $q^{\alpha+1}$ (z rovnice 131):

$$p(y) = y^2 - 2(n+1)y + 2^{\alpha+1}$$

Z Vietových vzorců dostaneme pro kořeny y_1, y_2 polynomu p:

$$y_1 y_2 = 2^{\alpha+1} \tag{133}$$
$$y_1 + y_2 = 2n + 2 \tag{134}$$

Tedy $y_1 = 2^a, y_2 = 2^b$ pro nějaké $a, b \geq 0$, bez újmy na obecnosti $a \leq b$. Nyní rozebereme několik případů pro různé hodnoty a.

$a = 1$ Tedy $y_1 = 2$ a $y_2 = 2n$. Po dosazení do polynomu p dostaneme hodnoty $n = 1$ nebo $n = 2$, což jsou nesmyslné hodnoty pro kódy.

$a = 2$ Tedy $y_1 = 4$ a $y_2 = 2n - 2$. Stejným způsobem jako v předchozím bodu dosadíme do p a spočteme $n = 2$ nebo $n = 5$. Pro $n = 5$ dostaneme triviální opakovací kód.

$a \geq 3$ Z rovnice 134 a faktu, že $a, b \geq 3$ dostaneme pro nějaké k:

$$2n + 1 = 2^a + 2^b - 1 \tag{135}$$
$$= 8k - 1 \tag{136}$$
$$(2n+1)^2 = 64k^2 - 16k + 1 \tag{137}$$

A dosadíme do rovnice 132:

$$(2n+1)^2 = 2^{\alpha+3} - 7 \tag{138}$$

Pravá strana rovnice 137 modulo 16 se rovná 1, zatímco pravá strana rovnice 138 modulo 16 se rovná -7, což je spor, neboť by se pravé strany obou rovnic měly rovnat. Pro $a \geq 3$ tedy neexistuje žádný perfektní kód. □

Věta Pro $t \geq 3$ a $q > 2$ neexistuje t-perfektní kód nad abecedou s q znaky.

Důkaz této části je nejnáročnější, proto ho rozdělíme do několika lemmátek. Hlavní roli budou mít kořeny Lloydova polynomu, které si označíme $\sigma_1, \ldots, \sigma_t$ a pro které platí

$$2 < \sigma_1 < \cdots < \sigma_t < n.$$

Nerovnosti mezi kořeny máme z Lloydovy věty. Po dosazení čísel $0, 1$ a 2 do Lloydova polynomu, zjistíme, že ani jedno z těchto čísel není kořenem, tedy $2 < \sigma_1$.

Lemma Pro kořeny Lloyodova polynomu $\sigma_1, \ldots, \sigma_t$ platí:

1. $\prod_{i=1}^{t} \sigma_i = t! q^{\alpha - t}$
2. $\sum_{i=1}^{t} \sigma_i = \frac{t(n-t)(q-1)}{q} + \frac{t(t+1)}{2}$

Důkaz Nejprve si vyjádříme součin kořenů pomocí koeficientů Lloydova polynomu.

$$\begin{aligned} L_t(x) &= a_t x^t + \cdots + a_1 x + a_0 \\ &= a_t \Big(x^t + \frac{a_{t-1}}{a_t} x^{t-1} + \cdots + \frac{a_0}{a_t} \Big) \\ &= a_t (x - \sigma_1) \ldots (x - \sigma_t) \\ &= a_t \Big(x^t - \Big(\sum \sigma_i \Big) x^{t-1} + \cdots + (-1)^t \prod \sigma_i \Big) \end{aligned}$$

Tedy máme:

$$\prod_{i=1}^{t} \sigma_i = (-1)^t \frac{a_0}{a_t} \tag{139}$$

$$\sum_{i=1}^{t} \sigma_i = -1 \frac{a_{t-1}}{a_t} \tag{140}$$

Nyní spočítáme koeficienty a_0 a a_t:

$$\begin{aligned} a_0 &= L_t(0) = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i = q^\alpha \\ a_t &= \sum_{i=0}^{t} (-1)^i (q-1)^{t-i} \frac{1}{i!} (-1)^{t-i} \frac{1}{(t-i)!} \\ &= \frac{(-1)^t}{t!} \sum_{i=0}^{t} (q-1)^{t-i} \frac{t!}{i!(t-i)!} \\ &= \frac{(-1)^t}{t!} \big((q-1) + 1 \big)^t \end{aligned}$$

Pro poslední rovnost jsme použili binomickou větu. Po dosazení do rovnice 139 dostaneme rovnost pro součin kořenů Lloydova polynomu

$$\prod_{i=1}^{t} \sigma_i = (-1)^t \frac{q^\alpha}{\frac{(-1)^t}{t!} q^t} = t! q^{\alpha - t}.$$

Bez důkazu uvádíme

$$a_{t-1} = -\frac{(-q)^t}{t!} \Big(\frac{t(t+1)}{2} + \frac{t(n-t)(q-1)}{q} \Big).$$

Po dosazení do rovnice 140 dostaneme dokazovanou rovnost pro součet kořenů. □

Lemma $2\sigma_1 \leq \sigma_t$

Důkaz Definujme si funkci $f(x) = k \Leftrightarrow x = p^h k$, kde pro p platí $q = p^r$ a p je nesoudělné s k. Aplikujme f na součin kořenů:

$$\begin{aligned} f(\sigma_1) f(\sigma_2) \dots f(\sigma_t) &= f(\sigma_1 \sigma_2 \dots \sigma_t) = \\ &= f(t! q^{a-t}) = f(t!) \leq t! \end{aligned}$$

Uvažme nyní 2 možnosti:

1. Nechť existují $i \neq j$ takové, že $f(\sigma_i) = f(\sigma_j) = k$, pak:

   $$\sigma_i = p^{h_i} k$$
   $$\sigma_j = p^{h_j} k$$

   Bez újmy na obecnosti platí $\sigma_i < \sigma_j$ a pak tedy $h_i < h_j$ a $p\sigma_i \leq \sigma_j$. Když všechny nerovnosti dáme dohromady, dostaneme požadovaný výsledek

   $$\sigma_t \geq \sigma_j \geq p\sigma_i \geq 2\sigma_i \geq 2\sigma_1.$$

2. Nechť jsou tedy všechny $f(\sigma_i)$ různé. Jelikož je jejich součin menší než $t!$, pak se mezi $f(\sigma_1), \dots, f(\sigma_t)$ vyskytují všechna čísla $1, \dots, t$. Jelikož $t \geq 3$ a p je nesoudělné se všemi čísly $1, \dots, t$, tak $p > 3$. Evidentně musí existovat i, j taková, že:

   $$\sigma_i = p^{h_i}$$
   $$\sigma_j = 2p^{h_j}$$

   Rozebereme 2 možnosti:

   (a) Nechť $h_j \geq h_i$, pak $\sigma_t \geq \sigma_j = 2p^{h_j} \geq 2p^{h_i} = 2\sigma_i \geq 2\sigma_1$

   (b) Nechť $h_i > h_j$, pak $\sigma_t \geq \sigma_i = p^{h_i} \geq p^{h_j+1} = \frac{p}{2}\sigma_j \geq 2\sigma_j \geq 2\sigma_1$

□

Lemma $\sigma_1\sigma_t \leq \frac{8}{9}(\frac{\sigma_1+\sigma_t}{2})^2$
Důkaz Celou nerovnost vynásobíme σ_1^2,

$$\frac{\sigma_t}{\sigma_1} \leq \frac{8}{9}\Big(\frac{1+\frac{\sigma_1}{\sigma_t}}{2}\Big)^2.$$

Provedeme substituci $x = \frac{\sigma_t}{\sigma_1}$,

$$x \leq \frac{8}{9}\Big(\frac{1+x}{2}\Big)^2.$$

Po elementárních úpravách dostaneme

$$0 \leq \Big(x - \frac{1}{2}\Big)\Big(x - 2\Big).$$

Což platí, protože z předchozího lemmatu víme, že $x \geq 2$. □

Lemma $\prod_{i=1}^{t} \sigma_i \geq \frac{n^t(q-1)^t}{q^t}\big(1 - \frac{t(t-1)}{2n}\big)$
Důkaz Víme, že

$$\prod_{i=1}^{t} \sigma_i = t!q^{\alpha-t}.$$

Pravou stranu následně upravíme:

$$\begin{aligned}
\frac{t!}{q^t}q^\alpha &= \frac{t!}{q^t}\sum_{i=0}^{t}(q-1)^i\binom{n}{i} \\
&\geq \frac{t!}{q^t}(q-1)^t\frac{n(n-1)\dots(n-t+1)}{t!} \\
&= \frac{(q-1)^t}{q^t}n^t\Big(1-\frac{1}{n}\Big)\Big(1-\frac{2}{n}\Big)\dots\Big(1-\frac{t-1}{n}\Big)
\end{aligned}$$

Nyní použijeme vzoreček, který platí pro $x_1, \dots, x_k \in (0,1)$

$$\prod_{i=1}^{k}(1-x_i) \geq 1 - \sum_{i=1}^{k} x_i.$$

Po aplikaci na $(1-\frac{1}{n})(1-\frac{2}{n})\dots(1-\frac{t-1}{n})$, dostaneme dokazovaný odhad:

$$\begin{aligned}
\frac{t!}{q^t}q^\alpha &\geq \frac{n^t(q-1)^t}{q^t}\Big(1 - \sum_{i=1}^{t-1}\frac{i}{n}\Big) \\
&\geq \frac{n^t(q-1)^t}{q^t}\Big(1 - \frac{t(t-1)}{2n}\Big)
\end{aligned}$$

□

Lemma $\prod_{i=1}^{t} \sigma_i \leq \frac{8}{9} \frac{n^t (q-1)^t}{q^t}$

Důkaz Pro důkaz použijeme již dokázanou nerovnost $\sigma_1 \sigma_t \leq \frac{8}{9}(\frac{\sigma_1+\sigma_t}{2})^2$ a nerovnost mezi aritmetickým a geometrickým průměrem

$$\Big(\prod_{i=1}^{k} x_i\Big)^{\frac{1}{k}} \leq \frac{\sum_{i=1}^{k} x_i}{k}.$$

Odhadněme tedy součin kořenů:

$$\begin{aligned}(\sigma_1\sigma_t)(\sigma_2\sigma_3\ldots\sigma_{t-1}) &\leq \frac{8}{9}\Big(\frac{\sigma_1+\sigma_t}{2}\Big)^2\Big(\frac{\sigma_2+\cdots+\sigma_{t-1}}{t-2}\Big)^{t-2}\\ &\leq \frac{8}{9}\Big(\frac{2\frac{\sigma_1+\sigma_t}{2}+(t-2)\frac{\sigma_2+\cdots+\sigma_{t-1}}{t-2}}{t}\Big)^t\\ &= \frac{8}{9}\Big(\frac{\sigma_1+\cdots+\sigma_t}{t}\Big)^t\end{aligned}$$

Po dosazení již dokázaného vzorečku pro součet kořenů dostaneme odhad

$$\prod_{i=1}^{t} \sigma_i \leq \Big(\frac{(n-t)(q-1)}{q} + \frac{t+1}{2}\Big)^t.$$

Abychom dokázali lemma, potřebujeme tedy dokázat, že

$$\frac{(n-t)(q-1)}{q} + \frac{t+1}{2} \leq \frac{n(q-1)}{q}.$$

Po několika elementárních úpravách dostaneme nerovnost $6t+3q \leq 3tq$, která platí, protože $6t \leq 2tq$ (kvůli předpokladu $q \geq 3$) a $3q \leq tq$ (kvůli předpokladu $t \geq 3$). □

Lemma $n \leq \frac{9}{2}t(t-1)$

Důkaz Nerovnost vyplývá okamžitě z předchozích 2 lemmat. □

Lemma $n \geq q^{\lfloor \frac{t}{2} \rfloor}$

Důkaz Nejprve trochu počítání:

$$\begin{aligned}\prod_{i=1}^{t}(\sigma_i - 1) &= (-1)^t \frac{a_t}{a_t}\prod_{i=1}^{t}(1-\sigma_i)\\ &= (-1)^t \frac{L_t(1)}{a_t}\\ &= \Big(\frac{q-1}{q}\Big)^t (n-1)(n-2)\ldots(n-t)\end{aligned}$$

Jelikož jsou kořeny Lloydova polynomu celá čísla, celý součin je také celé číslo a tedy $p^{rt} = q^t$ musí dělit součin $\pi = (n-1)(n-2)\dots(n-t)$. Pokud bychom vyjádřili číslo π pomocí prvočíselného rozkladu, tak rt vyjadřuje počet výskytů prvočísla p v tomto rozkladu. Pokusme se tedy rt nějak odhadnout. Nechť $N_t = \{n-1, \dots, n-t\}$ a h je takové číslo, že p^h dělí nějaké číslo z N_t a p^{h+1} nedělí žádné z čísel z N_t. Nechť k je takové, že $k = fp^h \in N_t$. Když k číslo k budeme přičítat či odčítat číslo p dostaneme čísla dělitelné p, tedy $k+p, k-p, k+2p, k-2p$ atd. Takovýchto čísel z N_t je tedy $\lfloor \frac{t}{p} \rfloor$. Obecně když budeme přičítat odčítat mocninu p^i, dostaneme čísla dělitelné p^i a těch je $\lfloor \frac{t}{p^i} \rfloor$ v množině N_t. Počet výskytů p v rozkladu čísla π můžeme tedy odhadnout

$$rt \leq h + \left\lfloor \frac{t}{p} \right\rfloor + \left\lfloor \frac{t}{p^2} \right\rfloor + \left\lfloor \frac{t}{p^3} \right\rfloor + \dots$$

To dále můžeme upravit:

$$\begin{aligned} h &\geq rt - \sum_{i=1}^{\infty} \left\lfloor \frac{t}{p^i} \right\rfloor \geq rt - \frac{t}{p}\Big(\sum_{i=0}^{\infty} \frac{1}{p^i}\Big) \\ &= rt - \frac{t}{p}\Big(\frac{1}{1-\frac{1}{p}}\Big) = t\Big(r - \frac{1}{p-1}\Big) \\ &\geq \frac{rt}{2} \end{aligned}$$

Poslední nerovnost vychází z toho, že $r - \frac{1}{p-1} \geq \frac{r}{2}$, což se dá snadno ověřit rozborem případů pro $p > 2$ a $p = 2$. Nyní již můžeme odhadnou n a dokázat tak lemma

$$n > p^h \geq p^{\frac{rt}{2}} \geq q^{\lfloor \frac{t}{2} \rfloor}.$$

□

Lemma $t \leq 11, q \leq 27$ a $n \leq 495$.

Důkaz Když složíme předchozí 2 lemmata dohromady dostaneme nerovnost

$$\frac{9}{2}t(t-1) \geq n \geq q^{\lfloor \frac{t}{2} \rfloor} \geq 3^{\lfloor \frac{t}{2} \rfloor}.$$

Z nerovnosti $\frac{9}{2}t(t-1) \geq 3^{\lfloor \frac{t}{2} \rfloor}$ dostaneme odhad $t \leq 11$. Následně pak dosadíme za t a dostaneme, že $n \leq 495$. Při dosazení $t = 3$ (nejmenší možná hodnota t, kdy q dosahuje nejvyšší hodnoty) dostaneme odhad $q \leq 27$. □

Počítačem bylo ověřeno, že pro hodnoty $3 \leq t \leq 11, 3 \leq q \leq 27$ a $n \leq 495$ neexistují žádné perfektní kódy, kdy q je mocnina prvočísla. Charakterizace perfektních kódů nad abecedou, která má velikost mocninu prvočísla, je tedy hotová.

Pro zajímavost uvedeme, že pro q, které není mocninou prvočísla, neexistují perfektní kódy pro $t \geq 3$ a pro $t = 1, 2$ se to neví. Pro parametry, pro které existují perfektní kódy, existují i jiné perfektní kódy než Hammingovy a Golayovi.