Aplikace lineární algebry v kombinatorice

2. ledna 2013

Obsah

Hamingovy kódy.

Příklad 1:

Město, v něm spolky. Velikost každého spolku je lichá, průniky jsou sudé. Kolik tam může být spolků? Určitě alespoň tolik, jako lidí (jednočlenné spolky).

Na druhou stranu to ale nejde lépe. Vezmeme charakteristické vektory. Ty musí být lineárně nezávislé.

☺

Máme ramseyovu teorii.

Nyní, udělejme $|X| = n$ a $\left(V = \begin{pmatrix} X \\ 3 \end{pmatrix}, E = \{uv; |u \cap v| = 1\}\right) = G$.
$w(G) \leq n$, $A \subseteq V, |A| = m; A_1, A_2 \ldots, A_n \subseteq X, |A_i \cap A_j| = 1 \Rightarrow m \leq n$.

2-vzdálenostní množiny: Máme v rovině body, chceme je rozmístit tak, aby jich množina obsahovala co nejméně různých vzdáleností.

Věta 1 *Označíme-li maximální počet bodů v n-rozměrném prostoru prostoru tak, že mají jen dvě vzdálenost, jako $m(n)$, potom:*

$$\frac{n \cdot (n+1)}{2} \leq m(n) \leq \frac{(n+1) \cdot (n+4)}{2}$$

Důkaz:
Dolní tak, že vezmeme body, co mají samé nuly a dvě jedničky. Potom jen vzdálenosti 2 a $\sqrt{2}$. Těch je zřejmě jen tolik, jako dolní odhad, ale jen pokud bereme ty vektory jako součást prostoru o dimenze $n+1$. Ale protože splňují rovnici $\sum x_i = 2$, což je podprostor (sice nevíme souřadnice uvnitř něj, ale to nevadí).

Odhad zhora. Máme množinu $A_1, \ldots, A_m \in E_n$. $d(A_i, A_j) \in \{a, b\}$. Definujme si $F(x, y) = (d^2(x, y) - a^2)(d^2(x, y) - b^2)$. Vpravo dostanu vždy nulu. Nyní zafixujme jeden argument ($f_i(x) = F(A_i, x)$). Množina funkcí do reálných čísel je vektorový prostor. Je třeba dokázat, že toto je lineárně nezávislé. Kdyby byly závislé, tak umím sestavit nulovou funkci. To je ale spor, protože dostávám všude nulu, kromě sebe sama, to je nenula.

Máme tedy m funkcí, což je ale menší, než dimenze prostoru, ve kterém žijí. Ale to jsou polynomy 4. stupně. Popíšeme generátory toho podprostoru. Pak už se upočítá dimenze.

☻

Mějme úplňák, chceme rozdělit jeho hrany tak, že dostáváme úplné bipartitní grafy (ty množiny musí být disjunktní, ale nemusí to pokrývat celé).

Věta 2 *Pokud to tak je, potom počet úplných bipartitních grafů je alespoň* $n-1$.

Důkaz:
Dokazuje se stejně, sčítáním nad $\mathbb{Z}_2$.

☻

Věta 3 $\forall G \exists$ *rozklad na dvě disjunktní* V_1, V_2 *takové, že* $G[V_1], G[V_2]$ *jsou eulerovské (všechno je sudé).*

Důkaz:
Mám množinu $M \subseteq T^n$, ortogonální doplněk $M^\perp$.

☻

Lemma 1

$$M \subseteq GF(2)^n \Rightarrow 1 \in \left\langle M \cup M^\perp \right\rangle$$

Důkaz:
Pokud $\langle M \rangle \cap M^\perp$ obsahuje jen 0. Potom $dim(M) = k, dim(M^\perp) = n-k$ a tedy z toho vyvodíme, že $\langle M \rangle \cup M^\perp = GF(2)^n$, tedy i 1.

Pokud $\exists u \in \langle M \rangle \cup M^\perp$, potom $\forall u \perp \langle M \rangle, u \perp u$. Tedy ale $\langle u, u \rangle = 0 = \sum u_i = \langle u, 1 \rangle$ a tedy $1 \perp u$.

☻

$G = (V, E), E = \{e_1, \ldots, e_n\}, GF(2)^n$ jsou podgrafy grafu G.

Když máme podprostor kružnic M, $M^\perp$ je prostor řezů.

Celý graf je tedy v součtu obou.

$\forall G \exists V_1, V_2$ disjunktní takové, že $V = V_1 \cup V_2$.

Komplexní matice se nazývá ***normální***, když komutuje s hermitovskou transpozicí.

A má ortonormální bázi z vlastních vektorů $\Leftrightarrow$ je normalní.

$A_1, A_2, \ldots, A_n$ mají společnou ortonormální bázi z vlastních vektorů $\Leftrightarrow$ jsou normální a $\forall i, j; A_i A_j = A_j A_i$.

$A = A^* \Leftrightarrow A$ je normální a reálná.

$A = A^* \Rightarrow A^*A = AA^*$ a je normalní, potom $\exists XX^* = E; X^*AX = D$ (s vlastními čísly), $D^* = D \Rightarrow$ všechny prvky jsou reálné.

Důsledek 1 *G je graf, A_G je matice sousednosti. Potom A_G má n vlastních čísel (součet jak algebraických tak geometrických násobností) a všechna jsou reálná.*

Věta 4 (Moorova) *Mějme d-regulární graf bez C_4, K_3. Určitě $n \geq 1 + d^2$ (počítání vrstev). Pokud je zde rovnost, graf se nazývá **Moorův**. Takových je málo.*

Důkaz:
A je matice sousednosti. $\lambda_{\max} = d$. A^2 má na diagonále dčka, mezi sousedy je určitě 0, jinak 1. Tedy, $A^2/J - A + (d-1) \cdot E$. Z toho se odvodí, že existuje jen málo vlastních čísel.

☻

Věta 5

$$\lambda_1 + \ldots + _n = 0$$

Věta 6 *Pro $d \notin \{0, 1, 2, 3, 7, 57\}$ neexistuje moorův graf.*

1 Silně regulární grafy

Graf G je (d, e, f)-***silně regulární***, pokud je:

- Je d-regulární.
- Každá hrana leží v e trojúhelnících ($\forall xy \in E; |N(x) \cap N(y)| = e$).
- $\forall xy \notin e; x \neq y; |N(x) \cap N(y)| = f$
- Není to úplný graf.

Věta 7 *Jestliže existuje (d, e, f) silně regulární graf s n vrcholy, potom:*

- $f = e + 1, d = 2f, n = 2d + 1$
- *nebo* $(e - f)^2 - 4(f - d) = s^2$ *a* $\frac{d}{2s}((d - 1 + f - e)(s + f - e) - 2) \in \mathbb{N}$.

Důkaz:
Nechť A je matice sousednosti. Matice A má na diagonále d (vždy tam a zpět). Na hranách jsou e a kde nejsou hrany, tam kde nejsou je f. Tedy: $A^2 = dE + eA + f(J - E - A)$. Tedy, $A^2 + A(f - e) + (f - d) = fJ$.

Všechny vlastní čísla dostaneme jako kořeny $p(x) = x^2 + (f - e)x + (f - d)$.

d je největší vlastní číslo.

Součet vlastních čísel je totéž jako její stopa.

☻

Věta 8 (Friendship theorem) *Nechť každí dva lidé mají právě jednoho společného přítele, potom existuje superpřítel.*

Důkaz:
Máme množinový systém $\mu = \{N(x); x \in V\}$. $x \cap y \Rightarrow |N(x) \cap N(y)| = 1$. Ať jsou nebo nejsou spojeny hranou, tak mají právě jeden průnikový prvek. To jsou dva axiomy projektivní roviny (je splněna i 4 body v obecné poloze? – ne, nemůže nastat všichni na jedné přímce, ale může nastat jeden, ostatní na přímce).

Tedy, pokud není superpřítel, tak máme konečnou projektivní rovinu. Máme tedy její řád a to je zde $m = 1$. Máme tedy $m + 1, 1, 1$ silně regulární graf o $m^2 + m + 1$ vrcholech. První možnost nastat nemůže, druhá $s^2 = 4m, s = 2t, m = t^2$. Po dosazení do druhé rovnice to nevyjde.

☻

2 Proplétání vlastních čísel

Máme matici A, její vlastní čísla $\lambda_1 \geq a_2 \ldots \geq a_n$ a k tomu vlastní vektory u_i, které tvoří ortonormální bázi.

Lemma 2

$$x \in span\{u_1, \ldots, u_k\} \Rightarrow x^* A x \geq \lambda_k x^* x$$

Důkaz:

$$\begin{aligned} x &= \sum_{i=1}^{k} \alpha_i u_i \\ x^* A(\sum \alpha_i u_i) &= \end{aligned}$$

$$
\begin{aligned}
x^*(\sum \alpha_i A u_i) &= \\
x^*(\sum \alpha_i \lambda_i u_i) &= \\
\sum \alpha_j^* u_j^* \alpha_i \lambda_i u_i \geq \sum \alpha_i^* \alpha_i \lambda_k &= \\
\lambda_k x^* x &
\end{aligned}
$$

☻

Důsledek 2

$$\lambda_i = \max_{x \neq 0} \frac{x^* A x}{x^* x}$$

Nechť matici B dostaneme z A vyškrtnutím i-tého řádku a i-tého sloupce $span(B) = \mu_1 \geq_2 \ldots \geq \mu_{n-1}$.

Věta 9 *Potom* $\lambda_1 \geq \mu_1 \geq \lambda_2 \geq \ldots \mu_{n-1} \geq \lambda_n$.

Důkaz:
$\forall k; \lambda_k \geq \mu_k \geq \lambda_{k+1}$. $S_1 = span\{u_k, u_{k+1}, \ldots, u_n\}$, $S_1 = span\{v_1, v_2, \ldots, v_k\}$ Doplníme na i-té místo nuly abychom dostali $v_1', z_2' \ldots$. $S_3 = \{v_1', v_2', \ldots\}$. $dimS_1 + dimS_3 = n+1$. To je $dim(S_1+S_3)+dim(S_1 \cap S_3)$. Tedy $dimS_1 \cap S_3 \geq 1$, tedy existuje tam alespoň jeden nenulový vektor, ale na i-tém místě má 0, takže tuto pozici nepotřebuji. Z toho vykopu $x^*Ax = y^*By$, z toho vykopu že $\mu_k \leq \lambda_k$.

Tu druhou zvolím $S_1 = span\{u_1, u_2, \ldots, u_{k+1}\}$, $S_2 = span\{v_k, \ldots, v_{n-1}\}$ a obdobně.

☻

Důsledek 3 *Tentokrát vyškrtneme k řádků a odpovídajících k sloupců, takže máme* $\mu_1 \geq \ldots \geq \mu_{n-k}$ *Potom platí, že* $\lambda_i \geq \mu_i$ *a* $\mu_i \geq \lambda_{i+k}$.

Důkaz:
Škrtáme postupně.

☻

Věta 10 *G graf. Potom* $\alpha(G) \leq \min\{|i; \lambda_i \leq 0|, |i; \lambda_i \geq 0|\}$.

Důkaz:
Vezmeme matici sousednosti, uspořádejme je tak, že v levém horním rohu

jsou nezávislá množina, ta matice je nulová. Vyhodím ty vrcholy, co nejsou v nezávislé množině, zbyde mi α nul jako vlastní čísla. Tedy, $\lambda_{1,2,...\alpha} \geq 0$ a $0 \geq \lambda_{n,n-1,...,n-\alpha+1}$.

☻

Věta 11 *G je d-regulární, potom $\alpha(G) \leq n \cdot \frac{-\lambda_n}{d-\lambda_n}$.*

Důkaz:
Vezmeme A matici sousednosti a J samých jedniček. $AJ = d \cdot J = JA$. Tedy existuje společná ortonormální báze složená z vlastních vektorů. $X^*X = E, X^*AX = D$. U J máme jedno číslo n a jinak nuly. Nechť $C = A - \frac{1}{n}(d - \lambda_n) J$. $X^*CXX^*AX - \frac{1}{n}(d - \lambda_n) X^*JX$. C má dvakrát λ_n.
Provedeme podobný trik jako předtím, B je podmatice odpovídající λ, její vlastní čísla jsou nuly, a $-\frac{\alpha}{n}(d - \lambda_n) \geq \lambda_n$.

☻

Důsledek 4 $\chi(G) \geq 1 + \frac{\lambda_1}{|\lambda_n|}$

Důkaz:
V každé barvě je nejvýše α prvků.

☻

Věta 12 *Toto platí i pro obecné grafy.*

Lemma 3 $\lambda_1 \geq$ *průměrný stupeň G.*

Důkaz:
TODO: Cvičení

☻

Věta 13 $\chi(G) \leq 1 + \lambda_1$.

Důkaz:
Každý graf obsahuje kritický graf pro tu barevnost jako indukovaný podgraf. Minimální stupeň je $\delta(G) \geq \chi(G) - 1$, jinak bych ten menší mohl vyhodit, obarvil a dobarvil podle toho, co zbyde. Průměrný stupeň je alespoň $\chi - 1$, tedy $\lambda_{max}^{G'} \geq \chi - 1$, tedy $\lambda_1 \geq \lambda_{max}^{G'}$.

☻

3 Shanonova kapacita grafu

Úplný součin grafů je takový graf $G \boxtimes H$, že: $V := V(G) \times V(H)$ a hrana $(v_1, u_1), (v_2, u_2)$ tam je když $v_1 = v_2 \vee v_1 v_2 \in E_1$ a totéž pro u (s tím, že nebereme smyčky).

Shanonova kapacita je

$$\sup \left\{ \alpha(G^k)^{\frac{1}{k}} \right\}$$

Pro 5-cyklus je to $\sqrt{5}$. Uděláme ortogonální reprezentaci grafu, každý vrchol dostane vektor, pokud mezi nimi není hrana, tak jsou na sebe kolmé.

Nejlepší reprezentace je taková, která jde do co nejmenšího kulového vrchlíku.

Definujme $\tau = \max_{c,|c|=1} \frac{1}{\langle c;v \rangle^2}$ (v je vektor vrcholu).

Lemma 4 $\alpha(G) \leq \tau(G)$

Důkaz:
Vezmeme si nezávislou, dáme libovolnou reprezentaci. Ta už musí udělat sama dostatečně veliký vrchlík.

☻

Lemma 5 *Máme grafy G, H a jejich reprezentace. Potom pro $G \boxtimes H$ existuje reprezentace taková, že $\tau(G \boxtimes H) = \tau(G) \cdot \tau(H)$.*

Máme vektory x, y. Potom ***tenzorový součin*** je $x \otimes y \in \mathbb{R}^{m \cdot n}$ a vyjde vynásobením každý s každým v lexikografickém pořadí opačně (tedy, od druhé souřadnice). Vyjde taky jako $x^T \times y$.

Pozorování 1 *Je to lineární operátor.*

Důkaz:
Stačí vzít tenzorový součin těch vektorů.

☻

Nyní už stačí vzít jen reprezentaci C_5, nasadit obě lemmata a je hotovo.

Věta 14 *Nechť P je reguární. Potom:*

$$Sp(A) = Sp(P \cdot A \cdot P^{-1})$$

Důkaz:
Roznásobením přes determinanty.

☻

Lemma 6 *Nechť $A \in \mathbb{C}^{n\times n}$ je hermitovská a $S \in \mathbb{C}^{m\times n}$, $m < n$, $SS^* = E$. Potom vlastní čísla SAS^* proplétají vlastní čísla A.*

Důkaz:
Vektory z S jsou na sebe kolmé. Lze rozšířit na ortonormální bázi R takové, že $RR^* = E$ (ale větší).

Nahradím tedy S za R. To odpovídá blokovému násobení matic, nalevo nahoře mám SAS^*. Tedy, vlastní čísla SAS^* problétají vlastní čísla RAR^*. Ale to má stejná vlastní čísla, jako A.

☻

Lemma 7 *Mám čtvercovou matici A nařezanou na bloky dlouhé $n_1, n_2, \ldots, n_m$. Získáme matici $B \in \mathbb{C}^{m\times m}$ tak, že vezmeme daný bloček, vše sečteme a vydělíme n_i.*

Vlastní čísla matice B problétají vlastní čísla A.

Důkaz:
Udělám matici $S \in \mathbb{C}^{m\times n}$. Takže mám řádků kolik je bloků a sloupečků kolik je sloupečků. Do prvního bloku přijdou jedničky na první řádek, do druhého na druhý, etc, jinak nuly.

Potom SS^* je matice $m \times m$. Na diagonále budou velikosti bloků, jinak nuly. SAS^* vychází součty prvků v celém bloku. Pohrajeme si a napasujeme předchozí lemma.

☻

Věta 15 *G je graf. Potom $\alpha(G) \leq n \cdot \frac{-\lambda_1\lambda_n}{\delta^2(G)-\lambda_1\lambda_n}$.*

Důkaz:
Nastěhuju si nezávislou jako nejnižší indexy. Rozdělím matici na 4 kusy, a spočítám B jako v minulém lemmatu. Vlevo nahoře mám 0, vpravo dole mě to nezajímá. Potom $b_{2,1} = b_{2,1} \cdot \frac{\alpha}{m-\alpha}$. Ta má vlastní čísla γ_1, γ_2 a proplétá vlastní čísla matice sousednosti.

☻

Věta 16 $\chi \geq 1 - \frac{\lambda_1}{\lambda_m}$

Důkaz:
Nařežeme na nezávislé množiny podle barev.

☻

4 Siedelův switching

Siedelův switching je operace na grafu, kdy si vyberu jeden vrchol, tomu vyměním/zneguji všechny jeho sousední hrany.

G H pokud mezi sebou jdou převádět postupným přepínáním.

To je ekvivalentní s tím, že všechny vrcholy nějaké množiny můžu switchnout (měním hrany jen mezi množinou a okolím). To je vidět.

To je totéž jako sčítání v $\mathbb{Z}_2$ s úplným bipartitním grafu (používajícím všechny vrcholy). Jde přeswitchovat, když existuje takový graf.

Takže třídy ekvivalence lze získat tak, že vyfaktorizuji všechny grafy pomocí báze všech úplný bipartitních na všech vrcholech.

Věta 17 *Tříd ekvivalence je stejně jako eulerovských grafů.*

Důkaz:
Jsou to ortogonální doplňky.

☻

Lineární forma je zobrazení z vektorového prostoru do jeho tělesa, které jsou lineární. V^* je prostor těchto forem. Platí, že $dimV = dimV^*$.

Lemma 8 (Burnsidovo) *Mějme grupu G a množinu M. Potom akce grupy na množině je zobrazení $G \times M \to M$ takové, že jednička z G nechávají m napokoji a $(g \cdot h) \cdot m = g(h \cdot m)$.*

Potom prvky, které se dají dostat z jednoho prvku akcemi z G jsou ekvivalence.

5 Neexistence perfektních kódů

Máme abecedu Σ, $|\Sigma| = q$. Σ^n jsou slova, $d_H(x, y)$ je počet míst, na kterých se tato slova liší.

Vysílají se jen daná kódová slova.

Řekneme, že kód C opravuje t chyb, pokud kdykoliv dojde až k t chybám při přenosu, tak lze najít jednoznačně nejbližší kódové slovo.

Pozorování 2 *Vzdálenosti kódových slov jsou alespoň* $2d + 1$.

Důkaz:
Přes okolíčka a jejich průniky.

☻

Pozorování 3 d_H *je metrika.*

Důkaz:
Jen upočítat. Zajímavá je jen trojúhelníková nerovnost.

☻

Pozorování 4 *Nechť* $C \subseteq \Sigma^n$ *opravuje* t *chyb. Potom* $|C| \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i}$

Důkaz:
Velikosti okolíček.

☻

$C \subseteq \Sigma^n$ se nazývá ***t-perfektní*** s parametry q, n, t, pokud platí rovnost. Tedy, okolíčka tvoří rozklad.

Příklad 2:

Mějme q prvočíslo a matici $\mathbb{Z}_2^{k \times 2^k - 1}$, v ní všechny kromě nulového vektoru. A $C = \{x | Hx = 0\}$. C je 1-perfektní kód.

☺

Důkaz:
Opravuje jednu chybu. Sporem, najdeme vektor součet těchto dvou slov, ten musí být v C, ale nevyjde tam.

Počet slov bude velikost jádra.

☻

Věta 18 *$\exists(q,n,t)$-perfektní kód a $q=p^r$ (mocnina prvočísla). Potom* $\sum_{i=0}^{t}\binom{n}{i}(q-1)^i = q^k$.

Důkaz:
Je to celé číslo. Z toho vytlučeme, že je to mocnina p a z toho se už uspoří, že musí být i mocnina q.

☻

Důsledek 5 *Nechť $q=p^r$ a $\exists(q,n,1)$-perfektní kód, potom $n=\frac{q^k-1}{q-1}$.*

Důkaz:
Jen dosazení.

☻

Jsou kódy pro mocniny prvočísla a $t=1$, pro $n=11$ a $t=2$ a pro $n=23$ a $t=3$. Na mocninách prvočísla žádná jiná nejsou.

Ve složených se ví, že neexistují, kromě $t=1,2$, kde se neví.

Věta 19 (Podmínka pakování koulí) *$\exists(q,n,t)$-perfektní kód. Potom* $\sum_{i=0}^{t}\binom{n}{i}(q-1)^i \mid q^n$ *pro složená q a q^k pro $q=p^r$.*

Věta 20 *Pokud $\exists(q,n,t)$-perfektní kód, potom* $L_t(x)=\sum_{j=0}^{t}(-1)^j(q-1)^{t-1}\binom{x-1}{q}\binom{n-x}{t-j}$ *má t různých celočíselných kořenů mezi 1 a n.*

Věta 21 *Pro $q=p^r$ a $t\geq$ neexistují (n,q,t) perfektní kody s jinými parametry než s Hamingových a Golojových kódů.*

Důkaz:
Má t ruzných celočíselných kořenů.

TODO: Tady bylo hromada chlupatých výpočtů, které se použijí na omezení $t\leq 11, n\leq 495, q\leq 27$ a nacpe se na to počítač.

☻

Poznámka 1 *Pro $q = 2$ se přidá součit $\Pi(\sigma_i - 2)$, udělá se něco podobného.*

Tvrzení 1 $q = 2, t = 2$.

Důkaz:
Podmínka pakování koulí říká, že $1 + \binom{n}{1} + \binom{n}{2} = 2^{\alpha}$.