NDMI028 Aplikace lineární algebry v kombinatorice
Handout No. 3

Princip ortogonality a ortogonálních doplňků podprostorů, prostor cyklů grafu
20. říjen 2020

Ortogonalita a ortogonální doplněk podprostoru

Definice: V této přednášce uvažujeme konečná tělesa a podtělesa tělesa reálných čísel (tedy dnes T nebude těleso komplexních čísel), vektorové prostory budou n-tice prvků tělesa (tedy $\mathcal{V} = T^n$) a *skalární součin* vektorů $x, y \in T^n$ bude standardní skalární součin

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i.$$

Vektory x, y se nazývají *ortogonální* pokud $\langle x, y \rangle = 0$.
Ortogonální doplněk $M^\perp$ množiny vektorů $M \subseteq T^n$ je množina vektorů ortogonálních na všechny vektory z M, tedy $M^\perp = \{y : \forall_{x \in M} \langle x, y \rangle = 0\}$.

Vlastnosti ortogonálního doplňku: Jsou-li $\mathcal{A}, \mathcal{B}$ podprostory T^n, pak

- $\dim(\mathcal{A}^\perp) = n - \dim(\mathcal{A})$,
- $(\mathcal{A}^\perp)^\perp = \mathcal{A}$,
- $(\mathcal{A} \cap \mathcal{B})^\perp = \mathcal{A}^\perp + \mathcal{B}^\perp$,
- $(\mathcal{A} \cup \mathcal{B})^\perp = \mathcal{A}^\perp \cap \mathcal{B}^\perp$.

Je-li $M \subseteq T^n$, pak $M^\perp = \langle M \rangle^\perp$ a $(\mathcal{M}^\perp)^\perp = \langle M \rangle$.

Poznámky: Vše výše uvedené je nejlépe vidět, hledíme-li na ortogonální doplněk jako na řešení homogenní soustavy lineárních rovnic, přičemž řádky matice této soustavy budou vektory z $\mathcal{A}$ (stačí vzít nějakou bázi).
Uvědomte si rozdíl konečných těles od reálných čísel – nad konečným tělesem může být nenulový vektor ortogonální sám na sebe, nad reálnými čísly nikoliv.

Mohutnosti množinových systémů podruhé

Věta (sudo-sudoměsta): Nechť $A_1, A_2, \ldots, A_k$ jsou různé podmnožiny n-prvkové množiny X takové, že každá má sudý počet prvků a každé dvě z nich mají sudý počet společných prvků. Potom $k \leq 2^{\lfloor \frac{n}{2} \rfloor}$. Navíc tento odhad je těsný, pro každé n existuje sudo-sudoměsto s $2^{\lfloor \frac{n}{2} \rfloor}$ množinami.

Důkaz: Pro jednoduchost zápisu ztotožníme množiny s jejich charakteristickými vektory, tedy chápeme $A_i \in \{0,1\}^n = GF(2)^n$. Označme $M = \{A_1, \ldots, A_k\}$. Podmínka na sudo-sudoměsto říká, že $\langle A_i, A_j \rangle = 0$ pro všechna i, j, a tedy $M \subseteq M^\perp$. Tudíž $\dim(\langle M \rangle) \leq n - \dim(\langle M \rangle)$, neboli $2 \cdot \dim(\langle M \rangle) \leq n$, z čehož plyne $\dim(\langle M \rangle) \leq \lfloor \frac{n}{2} \rfloor$. Proto $|M| \leq |\langle M \rangle| = 2^{\dim(\langle M \rangle)} \leq 2^{\lfloor \frac{n}{2} \rfloor}$.
Pro konstrukci seskupme prvky množiny X do $\lfloor \frac{n}{2} \rfloor$ dvojic a vytvořme množiny A_i všemi možnými způsoby tak, že prvky každé dvojice buď oba patří nebo oba nepatří do A_i.

Otázky k zamyšlení:
1. **Maximální města** Pro která $x, y \in \{\text{sudo,licho}\}$ je pravda, že každá dvě maximální (co do inkluze) x-y-města na stejné množině X mají stejný počet množin?
2. **Mod-q města** Pro přirozené číslo q nazveme Mod-q-město množinový systém takový, že mohutnost žádné množiny není dělitelná číslem q, zatímco mohutnost průniku libovolných dvou různých množin z tohoto systému číslem q dělitelná je. Dokažte, že pro každé číslo q existuje přirozené číslo $c(q)$ takové, že každé Mod-q město na n-prvkové množině X má nejvýše $c(q) \cdot n$ množin.
3. Ukažte, že $c(p^t) = 1$ pro každé prvočíslo p a libovolné t.

Prostor cyklů grafu

Pro tento paragraf zafixujeme (libovolný) graf $G = (V, E)$ a budeme uvažovat jeho napnuté podgrafy, tj. podgrafy $H = (V(H), E(H))$ takové, že $V(H) = V$ a $E(H) \subseteq E$. Každý takový podgraf H ztotožníme s charakteristickým vektorem jeho množiny hran jako podmnožiny množiny E, tedy chápeme $H \in GF(2)^E$. Množinu všech napnutých podgrafů grafu G označíme $\mathcal{V}_G$.

Tvrzení: $\mathcal{V}_G$ je vektorový prostor nad $GF(2)$, přičemž sčítání vektorů odpovídá symetrické diferenci množin hran.

Definice: Označme $\mathcal{E}_G$ množinu všech napnutých podgrafů grafu G, jejichž všechny stupně jsou sudé (takové grafy budeme nazývat *Eulerovské*). Označme $\mathcal{B}_G$ množinu všech elementárních řezů grafu G, tj. množinu všech grafů $B_A = (V, \{xy : x \in A, y \in V \setminus A, xy \in E\})$ pro $A \subseteq V$.

Věta: Jak $\mathcal{E}_G$, tak $\mathcal{B}_G$ jsou vektorové podprostory $\mathcal{V}_G$. Přitom platí $\mathcal{E}_G^\perp = \mathcal{B}_G$ a $\mathcal{B}_G^\perp = \mathcal{E}_G$. Je-li graf G souvislý, je $\dim(\mathcal{B}_G) = |V| - 1$, a tedy $\dim(\mathcal{E}_G) = |E| - |V| + 1$. (Prostor $\mathcal{E}_G$ se nazývá prostor cyklů grafu G, prostor $\mathcal{B}_G$ je jeho prostor řezů.)

Důkaz: Ukážeme, že prostor řezů je generován hvězdami, tj. podgrafy $B_{\{u\}}, u \in V$, a dále, že libovolný napnutý podgraf je Eulerovský právě tehdy, když je ortogonální ke všem hvězdám. Je-li G souvislý, pak libovolných $|V| - 1$ hvězd je lineárně nezávislých.

Otázky k zamyšlení:
1. Odvoďte vzorec pro dimenzi prostoru cyklů nesouvislého grafu, v závislosti na počtu komponent souvislosti.
2. Ukažte, že pro rovinný graf je prostor cyklů generován jeho stěnovými kružnicemi.

Seidelův switching

Definice: Operace *Seidelův switching* provedena na graf G a jeho vrchol v vymění všechny hrany a nehrany z vrcholu v vycházející, formálně $S(G, v) = (V(G), (E(G) \cup \{vx : vx \notin E(G)\}) \setminus \{vx : vx \in E(G)\})$. Grafy G a H na stejné množině vrcholů jsou *Seidelovsky ekvivalentní*, pokud lze G převést na H nějakou posloupností Seidelových switchingů, v tom případě píšeme $G \sim H$. Píšeme $G \approx H$ pokud existuje graf H' izomorfní grafu H takový, že $G \sim H'$.

Příklad: Ekviangulární systémy přímek v prostoru.

Pozorování: Dva grafy na dané množině vrcholů V jsou Seidelovsky ekvivalentní, právě když leží ve stejné lineární množině ve faktorprostoru $\mathcal{V}_{K_V}/\mathcal{B}_{K_V}$. Proto je tříd ekvivalence při Seidelově switchingu přesně tolik, jako Eulerovských grafů na dané množině vrcholů.

Rozklad grafu na dva Eulerovské podgrafy

Lemma: Pro každý podprostor M prostoru $GF(2)^n$ platí, že $\mathbf{1} \in M + M^\perp$. (Symbolem $\mathbf{1}$ značíme vektor složený ze samých jedniček.)

Důkaz: Pro každý vektor $x \in M \cap M^\perp$ je $\langle x, x\rangle = 0$. Nad $GF(2)$ ale platí $\langle x, x\rangle = \langle x, \mathbf{1}\rangle$, a tedy $\mathbf{1} \in (M \cap M^\perp)^\perp = M + M^\perp$.

Věta: Pro každý graf G existuje podmnožina vrcholů $A \subseteq V(G)$ taková, že $G[A]$ i $G[V \setminus A]$ jsou Eulerovské grafy (tj. mají všechny stupně sudé).

Důkaz: Aplikujte předchozí lemma na prostor $GF(2)^{E(G)} = \mathcal{V}_G$ a jeho podprostor $M = \mathcal{E}_G$. Uvědomte si, že v tomto prostoru je $\mathbf{1} = G$.