Lineární algebra v kombinatorice

Alexander „Olin“ Slávik

Abstrakt. Lineární algebra je bezesporu jedním ze základních kamenů vysokoškolské matematiky. Velmi dobře ji však můžeme uplatnit i v některých elementárních kombinatorických úlohách. Příspěvek stručně seznamuje se základními lineárně-algebraickými fakty a ukazuje typické úlohy, u kterých je možné tato pozorování s výhodou aplikovat.

Stručný úvod do lineární algebry

Ze střední školy známe definici vektorů jakožto uspořádaných dvojic či trojic reálných čísel. Lineární algebra tento koncept zobecňuje dvěma směry: jednak jako vektory chápeme prvky libovolného *vektorového prostoru*, jednak může na místě reálných čísel vystupovat libovolné *těleso*. Obě tyto algebraické struktury jsou přirozenými zobecněními – požadavky na ně kladené jsou takové, aby se „chovaly“ podobně jako zmíněný středoškolský příklad. Pro úplnost uvedeme formální definice.

Definice. Množinu $\mathbb{F}$ spolu s binárními operacemi $+$ a $\cdot$ a „význačnými“ prvky 0 a 1 nazveme *(komutativním) tělesem*, pokud pro všechna $x, y, z \in \mathbb{F}$ platí následující vztahy:

(i) $x + y = y + x$,
(ii) $x + 0 = x$,
(iii) $x \cdot y = y \cdot x$,
(iv) $x \cdot 1 = x$,
(v) $x \cdot (y + z) = x \cdot y + x \cdot z$,
(vi) existuje prvek $-x \in \mathbb{F}$ takový, že $x + -x = 0$,
(vii) je-li $x \neq 0$, pak existuje prvek $x^{-1} \in \mathbb{F}$ takový, že $x \cdot x^{-1} = 1$.

Běžnými tělesy jsou například racionální, reálná či komplexní čísla (se standardními operacemi); jiným příkladem jsou tělesa $\mathbb{Z}_p$ pro p prvočíslo, kde se sčítá a násobí modulo p.

Definice. Nechť $\mathbb{F}$ je těleso, V libovolná množina, $+\colon V \times V \to V$ a $\cdot\colon \mathbb{F} \times V \to V$ binární operace takové, že pro všechna $a, b \in \mathbb{F}$, $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ platí

(i) existuje prvek $\mathbf{o} \in V$ takový, že pro všechna $\mathbf{v} \in V$ je $\mathbf{v} + \mathbf{o} = \mathbf{v}$,
(ii) existuje $\mathbf{w} \in V$ takový, že $\mathbf{v} + \mathbf{w} = \mathbf{o}$, značíme $\mathbf{w} = -\mathbf{v}$,
(iii) je $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$,
(iv) $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$,
(v) $a \cdot (b \cdot \mathbf{v}) = (a \cdot b) \cdot \mathbf{v}$,
(vi) $1 \cdot \mathbf{v} = \mathbf{v}$,
(vii) $a \cdot (\mathbf{v} + \mathbf{w}) = a \cdot \mathbf{v} + a \cdot \mathbf{w}$,
(viii) $(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$.

Pak čtveřici $(V, +, \cdot, \mathbf{o})$ nazveme *vektorovým* (či *lineárním*) *prostorem nad* $\mathbb{F}$. Prvky tělesa $\mathbb{F}$ se někdy nazývají *skaláry*.

Pro každé těleso $\mathbb{F}$ a $n \in \mathbb{N}$ můžeme „vybavit“ množinu $\mathbb{F}^n$ strukturou vektorového prostoru tak, že sčítání vektorů a násobení skaláry definujeme po složkách, dostaneme tak tzv. *aritmetický vektorový prostor*. Jinými příklady jsou např. prostor všech posloupností prvků $\mathbb{F}$ či obecněji prostor všech funkcí z nějaké množiny M do $\mathbb{F}$.[1]

V následujícím bude vždy V vektorový prostor nad tělesem $\mathbb{F}$.

Definice. Je-li W podmnožinou V, pak nazveme W *podprostorem* V, pokud pro libovolná $\mathbf{v}, \mathbf{w} \in V$ a $a, b \in \mathbb{F}$ platí $a\mathbf{v} + b\mathbf{w} \in W$.

Pro kombinatorické úvahy (a nejen pro ty) budou kruciální pojmy lineární (ne)závislosti, generování a dimenze. Ponořme se tedy opět do světa definic.

Definice. Nechť M je podmnožinou V. *Lineárním obalem* M rozumíme množinu

$$\langle M \rangle = \{a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k \mid k \in \mathbb{N}, a_i \in \mathbb{F}, \mathbf{v}_i \in M \text{ pro } i \leq k\}.$$

Snadno nahlédneme, že $\langle M \rangle$ je podprostor V; je to nejmenší podprostor V, který obsahuje množinu M. Je-li $\langle M \rangle = V$, pak řekneme, že M *generuje* V.

Definice. Řekneme, že vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in V$ jsou *lineárně nezávislé*, pokud je splněna následující podmínka: kdykoliv skaláry $a_1, a_2, \ldots, a_k \in \mathbb{F}$ splňují $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k = 0$, pak již $a_1 = a_2 = \cdots = a_k = 0$. V opačném případě jsou vektory *lineárně závislé*. Množinu $M \subseteq V$ nazveme lineárně nezávislou, pokud je každá (konečná) sada vektorů z této množiny lineárně nezávislá.

Definice. Množinu $M \subseteq V$, která je současně lineárně nezávislá a generuje V, nazveme *bazí* V.

Pozorování. *Množina $B \subseteq V$ je bazí V právě tehdy, když každý vektor z V lze jednoznačně zapsat ve tvaru $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k$, kde $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in B$ a $a_1, a_2 \ldots, a_k \in \mathbb{F}$.*

[1] Pokud chápeme uspořádané n-tice jako funkce z množiny $\{1, \ldots, n\}$, pak do tohoto konceptu zapadá i aritmetický vektorový prostor.

Věta. *Každý vektorový prostor má nějakou bázi; přesněji, každou lineárně nezávislou množinu lze doplnit na bázi. Všechny báze daného vektorového prostoru mají stejnou velikost (mohutnost) – toto číslo nazveme dimenzí prostoru a budeme značit* $\dim V$.

Dále už omezíme své úvahy pouze na aritmetické vektorové prostory.

Definice. *Skalární součin* vektorů $\mathbf{v} = (v_1, \ldots, v_n), \mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{F}^n$ definujeme předpisem

$$\mathbf{v} \cdot \mathbf{w} = v_1 w_1 + v_2 w_2 + \cdots + v_n w_n.$$

V kombinatorických aplikacích budeme konfrontováni zpravidla s vektorovými prostory konečné dimenze (tedy s konečnou bazí). V těchto situacích bude ústředním nástrojem následující pozorování:

Pozorování. *Kdykoliv máme sadu více jak n vektorů z $\mathbb{F}^n$, pak jsou již nutně lineárně závislé. Na druhou stranu, kdykoliv máme sadu méně jak n vektorů z $\mathbb{F}^n$, pak již nutně existuje vektor na tyto všechny kolmý.*

Úlohy

Úloha 1. V obdélníkovém sále s r řadami po s sedadlech ($r > s$) na některá místa zasedli lidé. Dokažte, že můžeme vybrat některé řady (nejméně jednu) tak, aby v každém sloupci sedadel byl počet lidí sedících v těchto vybraných řadách sudý.

Úloha 2. V tabulce 5×5 jsou zapsána celá čísla. Je dovoleno vybrat libovolný čtverec 3×3 nebo 2×2 a zvětšit v něm všechna čísla o 1. Je vždy možné postupným prováděním těchto operací dostat tabulku, v níž jsou všechna čísla dělitelná 2011?

Úloha 3. V řadě je N žárovek očíslovaných postupně 1 až N. *Krokem* rozumíme přepnutí tří žárovek, jejichž čísla a, b, c splňují $a + c = 2b$. Určete všechna N, pro něž lze konečnou posloupností kroků všechny žárovky zhasnout nezávisle na jejich počátečním stavu. (iKS)

Úloha 4. Nechť $a_1, a_2, \ldots, a_5$, $b_1, b_2, \ldots, b_5$ jsou ne nutně různá čísla z množiny $\{1, \ldots, 10\}$ taková, že $a_i \geq b_i$ pro $i \leq 5$. Dokažte, že potom existují celá čísla $\alpha_1, \ldots, \alpha_5$ ne všechna nulová taková, že

$$\binom{a_1}{b_1}^{\alpha_1} \binom{a_2}{b_2}^{\alpha_2} \binom{a_3}{b_3}^{\alpha_3} \binom{a_4}{b_4}^{\alpha_4} \binom{a_5}{b_5}^{\alpha_5} = 1.$$

Úloha 5. (Lindströmova věta, „baby“ verze) Jsou-li $A_1, \ldots, A_m$ podmnožiny množiny $\{1, \ldots, n\}$ a $m > n$, pak existují dvě disjunktní množiny $I_1, I_2 \subseteq \{1, \ldots, m\}$ (z nichž je alespoň jedna neprázdná) takové, že

$$\bigcup_{i \in I_1} A_i = \bigcup_{i \in I_2} A_i.$$

Úloha 6. (Lindströmova věta) Je-li navíc v předchozí úloze $m > n+1$, pak můžeme navíc požadovat, aby platilo

$$\bigcap_{i \in I_1} A_i = \bigcap_{i \in I_2} A_i.$$

Úloha 7. Nechť přirozená čísla k, n splňují $k < n$ a označme $S = \{1, \ldots, n\}$. Nechť $A_1, \ldots, A_k$ jsou neprázdné podmnožiny S. Dokažte, že je možné obarvit některé prvky S dvěma barvami, červenou a modrou, tak, aby byly splněny následující podmínky:

(i) každý prvek S je buď neobarvený, nebo je obarvený červeně, nebo je obarvený modře,
(ii) alespoň jeden prvek S je obarvený,
(iii) každá z množin A_i ($i \leq k$) je buď celá neobarvená, nebo se v ní vyskytuje alespoň jeden prvek od obou barev. (VJIMC 2009)

Úloha 8. Nechť $n \in \mathbb{N}$ je sudé a $A_1, \ldots, A_n \subseteq \{1, \ldots, n\}$ mají všechny sudý počet prvků. Dokažte, že existují dvě různá čísla $i, j \leq n$ taková, že $A_i \cup A_j$ má také sudý počet prvků.

Úloha 9. V PraSestánu žije $n \in \mathbb{N}$ obyvatel. Kolik nejvíce občanských sdružení mohou založit, pokud je legislativa v PraSestánu následující:

(i) každé sdružení musí mít lichý počet členů,
(ii) každá dvě sdružení musejí mít sudý počet společných členů?

Úloha 10. Kvůli příliš striktním zákonům proběhl v PraSestánu krvavý převrat. Aby se nový diktátor zalíbil lidu, vyhlásil pro občanská sdružení tato nová pravidla:

(i) každé sdružení musí mít nově sudý počet členů,
(ii) každá dvě sdružení musejí mít stále sudý počet společných členů,
(iii) žádná dvě sdružení nemohou mít tutéž členskou základnu.

Jaký je největší možný počet občanských sdružení v tomto případě?

Úloha 11. Souvislý graf má 100 vrcholů a 1000 hran. Kolika způsoby můžeme nějaké hrany vyhodit tak, aby každý vrchol výsledného grafu měl sudý stupeň?

Zdroje

(1) Lászlo Babai, Péter Frankl: *Linear algebra methods in combinatorics*, Dept. Comput. Sc., University of Chicago, 1992, Preliminary version 2