Lineární algebra pro pokročilé

Martin Černý, Hanka Salavcová

kam.mff.cuni.cz/∼cerny
cerny@kam.mff.cuni.cz

October 25, 2023

Vektorové prostory abstraktně

$(\mathbb{R}^n, +, \cdot)$ ... standardní vektorový prostor

Cíl: *Obecnější* definice pomocí struktur

1. **množina prvků** S

2. **operace** $\circ_1, \circ_2, \ldots, \circ_k$
   - $\circ_i : S^r \to S$
     - ***arita*** r operace $\circ_i$
     - $r = 1$ ... *unární operace*
     - $r = 2$ ... *binární operace*
       1. $+ : \mathbb{R}^2 \to \mathbb{R}$ ... binární operace sčítání
       2. $\cdot : \mathbb{R}^2 \to \mathbb{R}$ ... binární operace násobení
       3. $^2 : \mathbb{R}^1 \to \mathbb{R}$ ... unární operace druhá mocnina
       4. druhá odmocnina? není definovaná na reálných číslech

STRUKTURA $\mathbb{S} = (S, \circ_1, \circ_2, \ldots, \circ_k, R_1, R_2, \ldots, R_\ell)$

1. **množina prvků** S
2. **operace** $\circ_1, \circ_2, \ldots, \circ_k$
   - $\circ_i : S^r \to S$
     - ***arita*** r operace $\circ_i$
3. **relace** $R_1, R_2, \ldots, R_\ell$
   - $R_i \subseteq S^t$
     - ***arita*** t relace R_i
     1. $< \subseteq \mathbb{R}^2$ ... uspořádání reálných čísel
        - $(a, b) \in <$ ... a je menší než b
     2. $E \subseteq \binom{V}{2}$ ... hrany grafu
        - $(u, v) \in E$ ... orientovaná hrana mezi u a v

Matematická struktura

Matematická struktura je $\mathbb{S} = (S, \circ_1, \circ_2, \ldots, \circ_k, R_1, R_2, \ldots, R_\ell)$, kde

1. S je nosná množina.
2. $\circ_1, \circ_2, \ldots, \circ_k$ jsou operace arit $r_1, r_2, \ldots, r_k$,
3. $R_1, R_2, \ldots, R_\ell$ jsou relace arit $t_1, t_2, \ldots, t_\ell$.

Pro $k = 0$ mluvíme o *struktuře bez operací*,
a pro $\ell = 0$ mluvíme o *struktuře bez relací*.

Matematická podstruktura

Podstrukturu $\mathbb{S}'$ struktury $\mathbb{S} = (S, \circ_1, \circ_2, \ldots, \circ_k, R_1, R_2, \ldots, R_\ell)$ určuje

1. podmnožina $S' \subseteq S$,
2. uzavřenost na operace $\circ_1, \circ_2, \ldots, \circ_k$,
3. restrikce $R_1, R_2, \ldots, R_\ell$ na S'.

- $\mathbb{N} = (N, +, \cdot)$
  - přirozená čísla s binárními operacemi sčítání a násobení
  - odčítání není korektní operace $\implies$ rozdíl není definovaný
- $\mathbb{Z} = (Z, +, \cdot)$
  - celá čísla s binárními operacemi sčítání a násobení
  - podstruktury: $\mathbb{N}$, $\{0\} \subseteq Z$, sudá/lichá čísla, …
- $\mathbb{G} = (V, E)$
  - graf s množinou vrcholů V a množinou hran E
  - E je *symetrická* relace: $(u, v) \in E \implies (v, u) \in E$

standardní vektorový prostor

$(\mathbb{R}^n, +, \cdot)$

1. $\mathbb{R}^n$ … n-tice reálných čísel
2. $+ : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$
   - sčítání po složkách
3. $\cdot : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$
   - násobení skalárem

abstraktní vektorový prostor

$(V, \oplus, \otimes)$

1. V … množina *vektorů*
2. $\oplus : V \times V \to V$
   - *vlastnosti* sčítání
3. $\otimes : \mathbb{R} \times V \to V$
   - *vlastnosti* násobení

ABSTRAKTNÍ DEFINICE - OPERACE SČÍTÁNÍ

Pro operaci sčítání $\oplus$ platí

1. ***komutativita***: pro každé $\mathbf{u}, \mathbf{v} \in V$,

$$\mathbf{u} \oplus \mathbf{v} = \mathbf{v} \oplus \mathbf{u}$$

2. ***asociativita***: pro každé $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$,

$$(\mathbf{u} \oplus \mathbf{v}) \oplus \mathbf{w} = \mathbf{u} \oplus (\mathbf{v} \oplus \mathbf{w})$$

3. ***existence nulového prvku***: $\exists\ \mathbf{o} \in V$, že pro každý $\mathbf{u} \in V$,

$$\mathbf{o} \oplus \mathbf{u} = \mathbf{u}$$

4. ***existence inverzního prvku***: pro každý $\mathbf{u} \in V$, existuje $-\mathbf{u} \in V$,

$$\mathbf{u} \oplus (-\mathbf{u}) = \mathbf{o}$$

Jednoznačnost nulového prvku

Nulový prvek $\mathbf{o}$ je určen jednoznačně.

Důkaz: sporem

- $\exists\, \hat{\mathbf{o}} \in V : \hat{\mathbf{o}} \neq \mathbf{o}$
- z definice: $\mathbf{o} = \mathbf{o} + \hat{\mathbf{o}} = \hat{\mathbf{o}}$

Jednoznačnost inverzního prvku

Pro každý $\mathbf{u} \in V$ je $-\mathbf{u}$ určen jednoznačně.

Důkaz: sporem

- $\exists\, -\mathbf{u}_1, -\mathbf{u}_2 \in V : -\mathbf{u}_1 \neq -\mathbf{u}_2$
- $\mathbf{u} \oplus -\mathbf{u}_1 = \mathbf{u} \oplus -\mathbf{u}_2$
- $\mathbf{o} \oplus -\mathbf{u}_1 = \mathbf{o} \oplus -\mathbf{u}_2$
  - přičtením $-\mathbf{u}_1$ zleva
- $-\mathbf{u}_1 = -\mathbf{u}_2$

ABSTRAKTNÍ DEFINICE - OPERACE NÁSOBENÍ A DISTRIBUTIVITA

Pro operaci násobení $\otimes$ platí

1. ***asociativita***: pro každé $\alpha, \beta \in \mathbb{R}$, $\mathbf{u} \in V$,
$$(\alpha\beta)\mathbf{u} = \alpha(\beta\mathbf{u})$$
2. ***násobení jedničkou***: pro každý $\mathbf{u} \in V$,
$$1 \otimes \mathbf{u} = \mathbf{u}$$

Propojení $\oplus$ a $\otimes$ ***distributivitou***

1. ***násobení skalárem***: pro každé $\alpha, \beta \in \mathbb{R}$, $\mathbf{u} \in V$,
$$(\alpha + \beta)\mathbf{u} = (\alpha\mathbf{u}) \oplus (\beta\mathbf{u})$$
2. ***součtu vektorů***: pro každé $\alpha \in \mathbb{R}$, $\mathbf{u}, \mathbf{v} \in V$,
$$\alpha(\mathbf{u} \oplus \mathbf{v}) = \alpha\mathbf{u} \oplus \alpha\mathbf{v}$$

Abstraktní definice vektorového prostoru

Vektorový prostor je libovolná struktura $(V, \oplus, \otimes)$ splňující výše zmíněné vlastnosti daných operací. Pokud pracujeme s takto definovanými vektory, můžeme vyžít pouze těchto vlastností (a jejich důsledků, které vyvodíme).

- *Je tato definice obecnější?* **Není**

Isomorfismus vektorových prostorů

Všechny vektorové prostory se liší od $(\mathbb{R}^n, +, \cdot)$ pouze přejmenováním prvků.

Důkaz: *později*

Abstraktní definice vektorového prostoru

Vektorový prostor je libovolná struktura $(V, \oplus, \otimes)$ splňující výše zmíněné vlastnosti daných operací. Pokud pracujeme s takto definovanými vektory, můžeme využít pouze těchto vlastností (a jejich důsledků, které vyvodíme).

- K čemu tedy zavádíme abstraktní definici?
  1. Nejpřirozenější definice
     - u VP polynomů těžko interpretovat násobení polynomů na n-ticích čísel
  2. Nemožnost konstrukce přejmenování
     - např. VP funkcí

1. $(\mathbb{C}, +, \cdot)$ prostor komplexních čísel
   - $\mathbb{C}$ ... komplexní čísla
   - $+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ ... sčítání komplexních čísel
   - $\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ ... násobení komplexních čísel
2. $(\mathcal{P}, +_{\mathcal{P}}, \cdot_{\mathcal{P}})$ prostor polynomů
   - $\mathcal{P}$ ... polynomy stupně k
     - $p(x) = a_0 + a_1 x + \cdots + a_k x^k \in \mathcal{P}$
   - $+_{\mathcal{P}} : \mathcal{P} \times \mathcal{P} \to \mathcal{P}$ ... sčítání polynomů
   - $\cdot_{\mathcal{P}} : \mathbb{R} \times \mathcal{P} \to \mathcal{P}$ ... násobení skalárem
3. $(\mathcal{F}, +_{\mathcal{F}}, \cdot_{\mathcal{F}})$ prostor funkcí
   - $\mathcal{F}$ ... funkce na intervalu $[0, 1]$
     - $f : [0, 1] \to \mathbb{R}$
   - $+\mathcal{F} : \mathcal{F} \times \mathcal{F} \to \mathcal{F}$ ... sčítání funkcí
   - $\cdot_{\mathcal{F}} : \mathbb{R} \times \mathcal{F} \to \mathcal{F}$ ... násobení skalárem

Vektorové podprostory a lineární obaly

Vektorové podprostory

- $\mathbb{V} = (V, \oplus, \otimes)$ ... vektorový prostor
- $\mathcal{P} = \{W \mid W \text{ je podprostor } \mathbb{V}\}$

Otázka: *Jakou strukturu tvoří* $\mathcal{P}$*?*

- $\implies$ ukážeme, že *úplný svaz*

$(X, \leq)$ ... **částečně uspořádaná množina**

- X ... množina prvků
- $\leq \subseteq X^2$ ... relace ***částečné uspořádání***
  1. ***reflexivita***: $a \in X \implies a \leq a$
     - *ostré uspořádání* $<$ splňuje *antireflexivitu*: $\nexists a \in X : a < a$
  2. ***antisymetrie***: $a, b \in X : a \leq b \wedge b \leq a \implies a = b$
     - jinak mezi a a b žádné uspořádání
  3. ***transitivita***: $a, b, c \in X : a \leq b \wedge b \leq c \implies a \leq c$
- Zkratka: $a < b$ pokud $a \leq b$ a $a \neq b$
- $(\mathbb{N}, \leq), (\mathbb{Q}, \leq), (\mathbb{R}, \leq)$ ... *lineární uspořádání*
  - **linearita:** pro každé a, b buď $a \leq b$ nebo $b \leq a$
- $(\mathbb{N}, |), (2^X, \subseteq)$ ... linearita platit nemusí ($2 \nmid 3 \wedge 3 \nmid 2$)

- ***y* je přímý následník *x***
  1. $x < y$
  2. neexistuje z, že $x < z < y$
     - $(\mathbb{N}, \leq)$ ... k je přímý následník $k - 1$
     - $(\mathbb{Q}, \leq), (\mathbb{R}, \leq)$ ... přímí následníci **neexistují**
- pro $x \leq y$ existuje ***řetěz přímých následníků*** $a_0, \ldots, a_k$:
  1. $x = a_0 < a_1 < \ldots < a_{k-1} < a_k = y$
  2. a_i je přímým následníkem a_{i-1}

O částečně uspořádaných množinách

V konečné množině X má každá dvojice porovnatelných prvků x, y řetěz přímých následníků.

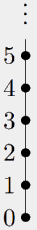
Důkaz:

1. buď y je přímým následníkem x
2. nebo existuje z, že $x < z < y$
   - 2.1 buď y je přímým následníkem z a ten zase x
   - 2.2 nebo existuje prvek mezi nimi ...

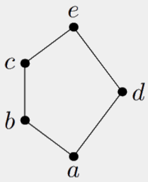
■ konečný počet prvků $\implies$ konečný argument

Hasseho diagram

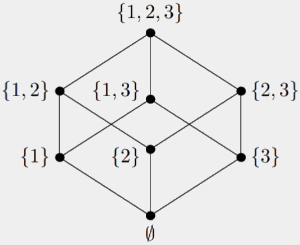
- reprezentuje prvky X jako body v rovině
    1. $x < y \implies$ bod x leží pod bodem y
    2. x, y spojíme úsečkou, pokud je y přímý následník x
    3. zbytek vztahů z transitivity



$(\mathbb{N}, \leq)$



$(\{a, b, c, d, e\}, \leq)$



$(2^{\{1,2,3\}}, \subseteq)$

- **podmínka**: pro každé $x < y$ existuje řetěz přímých následníků

- 2^E ... množina všech podmnožin pevné množiny E
- $\mathcal{X} \subseteq 2^E$ ... *množinový systém*

Částečné uspořádání množinového systému

Pro libovolný množinový systém $\mathcal{X}$ je struktura $(\mathcal{X}, \subseteq)$ částečně uspořádaná množina.

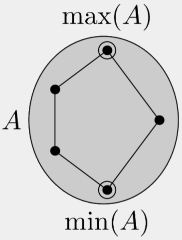
Důkaz:

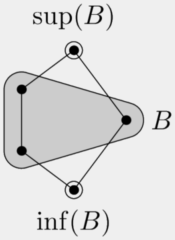
1. Reflexivita $A \subseteq A$
   - $x \in A \implies x \in A$
2. Antisymetrie $A \subseteq B \wedge B \subseteq A \implies A = B$
   - neplatilo by, kdyby existoval prvek z A mimo B, nebo naopak
   - díky $A \subseteq B$ a $B \subseteq A$ není možné
3. Transitivita $A \subseteq B \wedge B \subseteq C \implies A \subseteq C$
   - $x \in A \implies x \in B$, protože $A \subseteq B$
   - $x \in B \implies x \in C$, protože $B \subseteq C$

Úplný svaz

Částečně uspořádaná množina $(X, \leq)$ se nazývá ***úplný svaz***, pokud existuje ***infimum*** a ***supremum*** pro každou podmnožinu množiny X.

- $Y \subseteq X$
  - *minimum*: $\min(Y) := x \in Y$, že $\forall y \in Y$ platí $x \leq y$
  - *maximum*: $\max(Y) := x \in Y$, že $\forall y \in Y$ platí $y \leq x$
  - ***infimum***: $\inf(Y) := \max\{x \in X \mid \forall y \in Y \text{ platí } x \leq y\}$
  - ***supremum***: $\sup(Y) := \min\{x \in X \mid \forall y \in Y \text{ platí } y \leq x\}$





O infimum a supremu

Pokud pro $Y \subseteq X$ existuje minimum, existuje i infimum a $\min(Y) = \inf(Y)$. Podobně pokud existuje maximum, existuje i supremum a $\max(Y) = \sup(Y)$.

Důkaz: Minimum je infimum

1. dolní závora
   - $\forall y \in Y : \min(Y) \leq y$
2. největší dolní závora
   - x ... dolní závora
     - $\forall y \in Y : x \leq y$
   - $\min(Y) \in Y$
     - $x \leq \min(Y)$

- $\mathbb{V} = (V, \oplus, \otimes)$ ... vektorový prostor
- $\mathcal{P} = \{W | W$ je podprostorem $\mathbb{V}\}$
- $(\mathcal{P}, \subseteq)$ ... částečně uspořádaná množina

Vektorové podprostory tvoří úplný svaz

Částečně uspořádaná množina $(\mathcal{P}, \subseteq)$ je úplný svaz.

1. Nejprve zkonstruujeme infima
2. Poté zkonstruujeme suprema

Infima svazu vektorových podprostorů

$\mathcal{S} \subseteq \mathcal{P}$ ... podmnožina vektorových podprostorů

$$\inf(\mathcal{S}) = ???$$

- $\inf(\emptyset) = ???$
  - $\inf(\emptyset) = \mathbb{V}$
- $\emptyset \neq \mathcal{S} \subseteq \mathcal{P}$
  - pro každé $W \in \mathcal{S}$: $\inf(\mathcal{S}) \subseteq W$

Infima svazu vektorových podprostorů

Pro $\emptyset \neq \mathcal{S} \subseteq \mathcal{P}$ je $\inf(\mathcal{S}) = \bigcap_{W \in \mathcal{S}} W$.

Infima svazu vektorových podprostorů

Pro $\emptyset \neq \mathcal{S} \subseteq \mathcal{P}$ je $\inf(\mathcal{S}) = \bigcap_{W \in \mathcal{S}} W$.

Důkaz:

- $U = \bigcap_{W \in \mathcal{S}} W$
- $U \in \mathcal{P}$
  - průnik podprostorů je opět podprostor
- podmínky z definice infima
  1. dolní závora
     - $U \subseteq W$ pro všechny $W \in \mathcal{S}$ z definice
  2. největší dolní závora
     - $X \subseteq W$ pro všechny $W \in \mathcal{S}$
     - $\implies X \subseteq \bigcap_{W \in \mathcal{S}} W = U$

$\mathcal{S} \subseteq \mathcal{P}$ ... podmnožina vektorových podprostorů

$$\sup(\mathcal{S}) = ???$$

Z definice:

1. $\mathcal{S} \subseteq \sup(\mathcal{S})$
   - $\forall W \in \mathcal{S} : W \subseteq \sup(\mathcal{S})$
2. nejmenší X, že $\mathcal{S} \subseteq X$

- *nejmenší z nadmnožin* $\implies$ *průnik přes všechny nadmnožiny*

Suprema svazu vektorových podprostorů

Pro $\mathcal{S} \subseteq \mathcal{P}$ je $\sup(\mathcal{S}) = \bigcap_{W \in \mathcal{P}, \mathcal{S} \subseteq W} W$.

Suprema svazu vektorových podprostorů

Pro $\mathcal{S} \subseteq \mathcal{P}$ je $\sup(\mathcal{S}) = \bigcap_{W \in \mathcal{P}, \mathcal{S} \subseteq W} W$.

Důkaz:

- $U = \bigcap_{W \in \mathcal{P}, \mathcal{S} \subseteq W} W$
- $U \in \mathcal{P}$
  - průnik podprostorů opět podprostor
- podmínky z definice suprema
  1. horní závora
     - $\mathcal{S} \subseteq W$ pro každý W účastnící se průniku, tedy $\mathcal{S} \subseteq U$
  2. nejmenší horní závora
     - pokud $\mathcal{S} \subseteq W$, potom W obsahuje U, tedy $U \subseteq W$

Úplný svaz vektorových podprostorů

Pro daný vektorový prostor, množina všech jeho vektorových podprostorů $\mathcal{P}$ uspořádaná inkluzí tvoří úplný svaz: Existuje infimum a supremum pro každou podmnožinu $\mathcal{S} \subseteq \mathcal{P}$.

Důkaz:

- $\inf(\emptyset) = \mathbb{V}$
- pro $\emptyset \neq \mathcal{S} \subseteq \mathcal{P}$ je $\inf(\mathcal{S}) = \bigcap_{X \in \mathcal{S}} X$
- pro $\mathcal{S} \subseteq \mathcal{P}$ je $\sup(\mathcal{S}) = \bigcap_{W \in \mathcal{P}, \mathcal{S} \subseteq W} W$

X ... množina vektorů

Cíl: $X \rightsquigarrow X'$ ... vektorový podprostor

1. odebráním prvků
   - nemusí být vektorový podprostor (např. $\mathbf{o} \notin X$)
2. přidáním prvků
   - *nejmenší* vektorový podprostor obsahující X
   - nejmenší do velikosti nedává úplně smysl
     - (netriviální podprostor je nekonečně velký)
   - nejmenší do inkluze

Lineární obal

Pro X je **lineární obal** $\mathcal{L}(X)$ do inkluze nejmenší vektorový podprostor W s vlastností $X \subseteq W$.

- z vlastností $(\mathcal{P}, \subseteq)$ dobře definovaný

Lineární obal

Pro X je **lineární obal** $\mathcal{L}(X)$ do inkluze nejmenší vektorový podprostor W s vlastností $X \subseteq W$.

Lineární obal

Platí $\mathcal{L}(X) = \inf\{W \mid W \in \mathcal{P}, X \subseteq W\} = \bigcap_{W \in \mathcal{P}, X \subseteq W} W$.

Důkaz: Zbývá dokázat první rovnost: *nejmenší = infimum*

- $\mathcal{U} = \{W \mid W \in \mathcal{P}, X \subseteq W\}$
  - $\inf(\mathcal{U})$ ... existuje
  - $\inf(\mathcal{U})$ ... (průnik je) vektorový podprostor
  - $X \subseteq \inf(\mathcal{U})$ ... X je obsaženo ve všech W
  - $\inf(\mathcal{U}) \subseteq W$ pro $X \subseteq W$ ... obsažen v každém kandidátovi

Lineární obal

Pro množinu vektorů X je ***lineární obal*** $\mathcal{L}(X)$ do inkluze nejmenší vektorový podprostor obsahující všechny vektory z X. Lineární obal X je roven průniku všech vektorových podprostorů obsahujících X.

- klíčovou roli hrají při definici *báze* vektorového podprostoru
  - $\implies$ *nejmenší* množina vektorů $X \subseteq W$, že $\mathcal{L}(X) = W$