Lineární prostory nad $\mathbb{R}$

Odpřednesenou látku naleznete v kapitolách 1.1–1.4 skript *Abstraktní a konkrétní lineární algebra*.

Co je definice?

Co je hypotéza?

Co je (matematická) věta? Lemma? Tvrzení?

Co je důkaz?

Více např. v textech

1. J. Velebil, *Velmi jemný úvod do matematické logiky*
2. Larry W. Cusick, *How to write proofs*

Neformálně

Lineární prostor (nad $\mathbb{R}$) je kolekce jakýchkoli objektů (těm budeme říkat vektory), které mezi sebou můžeme sčítat a každý z nich můžeme vynásobit skalárem (v našem případě prvkem $\mathbb{R}$). Sčítání vektorů a násobení skalárem se musí řídit jistými zákonitostmi.

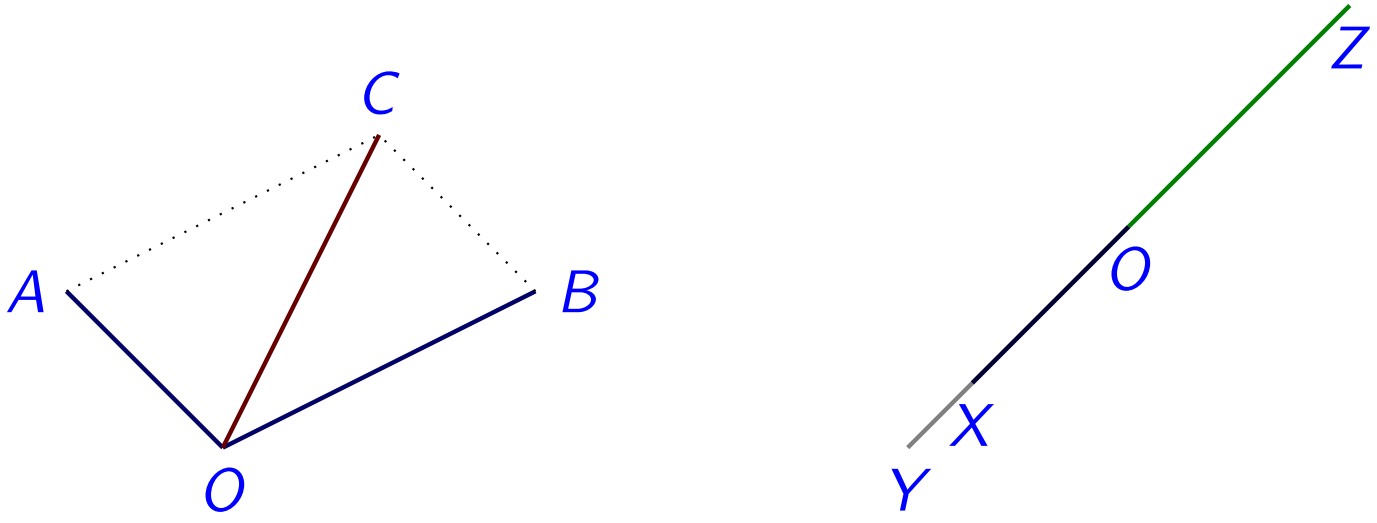
Příklady

1. Vektory v rovině (fyzikální, případně geometrická intuice).
2. Reálné polynomy (značení: $\mathbb{R}[x]$).
3. n-tice reálných čísel (značení: $\mathbb{R}^n$, $n \geq 0$).[a]
4. Komplexní čísla (značení: $\mathbb{C}$).
5. Řada dalších příkladů...

[a] Důležité: Prvky $\mathbb{R}^n$ budeme psát jako n-tice do sloupců.

Příklad (orientované úsečky v rovině)

Dvě operace:



sčítání: $OC = OA + OB$
násobení skalárem: $OY = \sqrt{2} \cdot OX$, $OZ = -\sqrt{2} \cdot OX$

Sčítání orientovaných úseček a násobení orientované úsečky reálným skalárem splňují jisté axiomy.

Definice (lineární prostor nad $\mathbb{R}$)

Lineární prostor (nad $\mathbb{R}$) je množina L spolu se dvěma funkcemi

$$+ : L \times L \to L, \quad \cdot : \mathbb{R} \times L \to L$$

pro které platí následující:

1. Vlastnosti sčítání:
   1. Existuje $\vec{o} \in L$ tak, že pro vš. $\vec{x} \in L$ platí: $\vec{x} + \vec{o} = \vec{o} + \vec{x} = \vec{x}$ (existence nulového vektoru).
   2. Pro vš. $\vec{x}, \vec{y}, \vec{z} \in L$ platí: $(\vec{x} + \vec{y}) + \vec{z} = \vec{x} + (\vec{y} + \vec{z})$ (asociativita sčítání vektorů).
   3. Pro vš. $\vec{x}, \vec{y} \in L$ platí: $\vec{x} + \vec{y} = \vec{y} + \vec{x}$ (komutativita sčítání vektorů).
   4. Pro vš. $\vec{x} \in L$ existuje právě jeden $\vec{y} \in L$ tak, že $\vec{x} + \vec{y} = \vec{o}$ (existence opačného vektoru, značíme $\vec{y} = -\vec{x}$).

Definice (lineární prostor nad $\mathbb{R}$), pokrač.

2. Vlastnosti násobení skalárem:
   1. Pro vš. $\vec{x} \in L$ platí: $1 \cdot \vec{x} = \vec{x}$ (násobení jednotkovým skalárem).
   2. Pro vš. $a, b \in \mathbb{R}$ a vš. $\vec{x} \in L$ platí: $a \cdot (b \cdot \vec{x}) = (a \cdot b) \cdot \vec{x}$ (asociativita násobení skalárem).
3. Distributivní zákony:
   1. Pro vš. $a, b \in \mathbb{R}$ a vš. $\vec{x} \in L$ platí: $(a + b) \cdot \vec{x} = a \cdot \vec{x} + b \cdot \vec{x}$ (distributivita součtu skalárů).
   2. Pro vš. $a \in \mathbb{R}$ a vš. $\vec{x}, \vec{y} \in L$ platí: $a \cdot (\vec{x} + \vec{y}) = a \cdot \vec{x} + a \cdot \vec{y}$ (distributivita součtu vektorů).

Poznámka

Axiomy tří typů: chování operace $+$, chování operace $\cdot$ a vzájemný vztah obou operací.

Jednoduché důsledky definice

Ať L je lineární prostor. Potom:

1. Nulový vektor je jednoznačně určen.
2. Pro vš. $\vec{x} \in L$ platí: $0 \cdot \vec{x} = \vec{o}$.
3. Opačný vektor k $\vec{x} \in L$ je vektor $(-1) \cdot \vec{x}$.
4. Pro vš. $a \in \mathbb{R}$ platí: $a \cdot \vec{o} = \vec{o}$.

Důkaz.

1. Ať existují $\vec{o_1}, \vec{o_2}$ tak, že pro vš. $\vec{x} \in L$ platí: $\vec{x} + \vec{o_1} = \vec{o_1} + \vec{x} = \vec{x}$ a $\vec{x} + \vec{o_2} = \vec{o_2} + \vec{x} = \vec{x}$. Pak $\vec{o_1} = \vec{o_1} + \vec{o_2} = \vec{o_2}$.
2. Pro vš. $\vec{x} \in L$ platí: $\vec{x} = 1 \cdot \vec{x} = (1 + 0) \cdot \vec{x} = 1 \cdot \vec{x} + 0 \cdot \vec{x} = \vec{x} + 0 \cdot \vec{x}$. Tudíž $0 \cdot \vec{x}$ musí být nulový vektor.

Důkaz (pokrač.)

3. Platí: $\vec{x} + (-1) \cdot \vec{x} = 1 \cdot \vec{x} + (-1) \cdot \vec{x} = (1 - 1) \cdot \vec{x} = 0 \cdot \vec{x} = \vec{o}$.
4. Platí: $a \cdot \vec{o} = a \cdot (0 \cdot \vec{o}) = (a \cdot 0) \cdot \vec{o} = 0 \cdot \vec{o} = \vec{o}$.

■

Velmi důležitý důsledek definice

Ať L je lineární prostor, $a \in \mathbb{R}$, $\vec{x} \in L$. Pak $a \cdot \vec{x} = \vec{o}$ právě tehdy, když $a = 0$ nebo $\vec{x} = \vec{o}$.

Důkaz.

Díky předchozímu stačí dokázat pouze implikaci zleva doprava. Ať $a \cdot \vec{x} = \vec{o}$ a $a \neq 0$. Potom existuje a^{-1}. Tudíž $\vec{o} = a^{-1} \cdot \vec{o} = a^{-1} \cdot (a \cdot \vec{x}) = (a^{-1} \cdot a) \cdot \vec{x} = 1 \cdot \vec{x} = \vec{x}$. ■

Povšimněme si, čeho využívá předchozí tvrzení:

Pro vš. $a \in \mathbb{R}$ platí: a^{-1} existuje, jakmile $a \neq 0$.

Další příklady a protipříklady

1. $L = (0, +\infty)$. Operace sčítání vektorů: $x \oplus y := x \cdot y$. Násobení skalárem: $\alpha \odot x := x^\alpha$. Pak L je lineární prostor.
2. L je jakákoli jednoprvková množina. Pak L (spolu s evidentními operacemi) je lineární prostor. Říkáme mu triviální lineární prostor. Nutně: $L = \{\vec{o}\}$.
3. $L = \mathbb{R}^2$. Operace: $\begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} c \\ d \end{pmatrix} := \begin{pmatrix} a+d \\ b+c \end{pmatrix}$, $\alpha \cdot \begin{pmatrix} a \\ b \end{pmatrix} := \begin{pmatrix} \alpha a \\ \alpha b \end{pmatrix}$. Nejde o lineární prostor.

Role reálných skalárů

Lze $\mathbb{R}$ nahradit jiným „číselným oborem“?

Se skaláry je třeba umět následující: rozumné sčítání, násobení.

Abstraktní pojem: skaláry musí tvořit strukturu $\mathbb{F}$, které se říká těleso.

To vede k pojmu lineární prostor nad tělesem $\mathbb{F}$. Více v příští přednášce.

Poznámka

Abstrakce v lineární algebře má tedy dva stupně:

1. Lineární prostor nad $\mathbb{R}$ abstrahuje (například) prostor orientovaných úseček.
2. Lineární prostor nad $\mathbb{F}$ abstrahuje dále: roli skalárů převezmou prvky tělesa $\mathbb{F}$.

Jaký nejobecnější výpočet lze v lineárním prostoru vykonat?

1. Například můžeme sečíst čtyři vektory: $\vec{x} + \vec{y} + \vec{z} + \vec{w}$.
   Díky asociativitě sčítání nemusíme psát závorky.
2. Například můžeme násobek vektoru opět vynásobit: $b \cdot (a \cdot \vec{x})$.
   Díky axiomům jde opět o násobek $(b \cdot a) \cdot \vec{x}$.
3. Obecněji, můžeme sčítat konečně mnoho násobků vektorů.
   To znamená: je-li dán konečný seznam vektorů $(\vec{x}_1, \ldots, \vec{x}_n)$ a konečný seznam skalárů[a] $(a_1, \ldots, a_n)$, lze utvořit lineární kombinaci

$$a_1 \cdot \vec{x}_1 + a_2 \cdot \vec{x}_2 + a_3 \cdot \vec{x}_3 + \ldots + a_n \cdot \vec{x}_n$$

   značenou také $\displaystyle\sum_{i=1}^{n} a_i \cdot \vec{x}_i$ nebo $\displaystyle\sum_{i \in \{1,\ldots,n\}} a_i \cdot \vec{x}_i$

[a] Těmto skalárům říkáme koeficienty lineární kombinace.

Definice

Seznam (také: skupina) vektorů je buď prázdná posloupnost () nebo konečná posloupnost $(\vec{x}_1, \ldots, \vec{x}_n)$.

Pozor: je rozdíl mezi seznamem a množinou

$(\vec{x}_1, \vec{x}_2, \vec{x}_3) \neq (\vec{x}_3, \vec{x}_2, \vec{x}_1)$ *vs.* $\{\vec{x}_1, \vec{x}_2, \vec{x}_3\} = \{\vec{x}_3, \vec{x}_2, \vec{x}_1\}$

$(\vec{x}_1, \vec{x}_1, \vec{x}_2) \neq (\vec{x}_1, \vec{x}_2)$ *vs.* $\{\vec{x}_1, \vec{x}_1, \vec{x}_2\} = \{\vec{x}_1, \vec{x}_2\}$

Definice (lineární kombinace konečného seznamu vektorů)

Pro seznam vektorů tvaru

1. () definujeme $\vec{o}$ jako jeho (jedinou možnou) lineární kombinaci (s prázdným seznamem koeficientů).
2. $(\vec{x}_1, \ldots, \vec{x}_n)$ je vektor $\sum_{i=1}^{n} a_i \cdot \vec{x}_i$ jeho lineární kombinace (se seznamem koeficientů $(a_1, \ldots, a_n)$).

Zobecnění předchozího (zatím jen slogan)

Lineární kombinace seznamu $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ v $\mathbb{R}^n$ vytvářejí „rovný kus“ prostoru $\mathbb{R}^n$.
Tento „rovný kus“ prostoru $\mathbb{R}^n$ prochází počátkem a má směr $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$.

Příští přednášky: těmto „rovným kusům“ v $\mathbb{R}^n$ budeme říkat lineární podprostory $\mathbb{R}^n$.

Pochopitelně, v příštích přednáškách budeme pracovat daleko abstraktněji než v $\mathbb{R}^n$.

Slogan je reklamní heslo!

Na přednášce budeme zmiňovat řadu sloganů. Slogany mají sloužit k intuitivnímu pochopení. Slogany v žádném případě nemohou nahradit přesná znění definic, vět, atd.

Lineární prostory nad $\mathbb{F}$

Odpřednesenou látku naleznete v kapitolách 1.1–1.4 skript *Abstraktní a konkrétní lineární algebra*.

Minulá přednáška

Lineární prostor nad $\mathbb{R}$ jako zobecnění (například) prostoru orientovaných úseček v rovině.

Dnešní přednáška

1. Těleso $\mathbb{F}$ jako zobecnění reálných čísel.
2. Lineární prostor nad $\mathbb{F}$ jako zobecnění pojmu lineární prostor nad $\mathbb{R}$.
3. Důležité: povšmneme si, že důkazy typicky nesouvisí s konkrétními operacemi; souvisí s pouze s algebraickými vlastnostmi těchto operací.[a]

Od příště budeme pracovat s lineárními prostory nad obecným tělesem.

[a] Do jisté míry je tak dnešní přednáška „kopií“ přednášky předchozí. Algebra dovolí od příště takovou marnotratnost nedopustit.

Sčítání a násobení reálných čísel

Množina reálných čísel $\mathbb{R}$ je vybavena dvěma funkcemi

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \quad \cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

pro které platí následující:

1. Vlastnosti sčítání:
   1. Existuje $0 \in \mathbb{R}$ tak, že pro vš. $a \in \mathbb{R}$ platí: $a + 0 = 0 + a = a$ (existence nuly).
   2. Pro vš. $a, b, c \in \mathbb{R}$ platí: $(a + b) + c = a + (b + c)$ (asociativita sčítání).
   3. Pro vš. $a, b \in \mathbb{R}$ platí: $a + b = b + a$ (komutativita sčítání).
   4. Pro vš. $a \in \mathbb{R}$ existuje právě jedno $b \in \mathbb{R}$ tak, že $a + b = 0$ (existence opačného čísla, značíme $b = -a$).

Sčítání a násobení reálných čísel (pokrač.)

2. Vlastnosti násobení:
   1. Existuje $1 \in \mathbb{R}$ tak, že pro vš. $a \in \mathbb{R}$ platí: $1 \cdot a = a$ (existence jednotky).
   2. Pro vš. $a, b, c \in \mathbb{R}$ platí: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (asociativita násobení).
   3. Pro vš. $a, b \in \mathbb{R}$ platí: $a \cdot b = b \cdot a$ (komutativita násobení).
3. Provázanost sčítání a násobení:
   1. Pro vš. $a, b, c \in \mathbb{R}$ platí: $a \cdot (b + c) = a \cdot b + a \cdot c$ (levý distributivní zákon).
   2. Pro vš. $a, b, c \in \mathbb{R}$ platí: $(b + c) \cdot a = b \cdot a + c \cdot a$ (pravý distributivní zákon).
4. Test invertibility: pro vš. $a \in \mathbb{R}$ platí: $a \neq 0$ iff existuje a^{-1}.

Poznámka

Výše uvedené vlastnosti byly podstatné pro zavedení pojmu lineární prostor nad $\mathbb{R}$ (viz minulou přednášku).

Příklady: další „standardní“ sčítání a násobení

1. Standardní sčítání a násobení racionálních čísel: obě operace na množině $\mathbb{Q}$ splňují stejné vlastnosti jako standardní sčítání a násobení na množině $\mathbb{R}$.
2. Standardní sčítání a násobení komplexních čísel: obě operace na množině $\mathbb{C}$ splňují stejné vlastnosti jako standardní sčítání a násobení na množině $\mathbb{R}$.
3. Standardní sčítání a násobení celých čísel: obě operace na množině $\mathbb{Z}$ nesplňují stejné vlastnosti jako standardní sčítání a násobení na množině $\mathbb{R}$. Neplatí test invertibility: například $2 \neq 0$, ale 2^{-1} v $\mathbb{Z}$ neexistuje![a]

[a] Test invertibility v $\mathbb{R}$ byl v minulé přednášce podstatný! Množinu $\mathbb{Z}$ tedy jako množinu skalárů nebudeme moci použít.

Příklad: „nestandardní“ sčítání a násobení

1. Množina $\mathbb{Z}_2 = \{0, 1\}$ s operacemi:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

2. Množina $\mathbb{Z}_3 = \{0, 1, 2\}$ s operacemi:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Operace na množinách $\mathbb{Z}_2$ a $\mathbb{Z}_3$ splňují stejné vlastnosti jako standardní sčítání a násobení na množině $\mathbb{R}$.

Slogan pro těleso

Těleso $\mathbb{F}$ je kolekce jakýchkoli objektů (těm budeme říkat prvky tělesa $\mathbb{F}$), které mezi sebou můžeme sčítat a násobit. Sčítání a násobení v $\mathbb{F}$ splňují stejné vlastnosti jako standardní sčítání a násobení v $\mathbb{R}$.

Definice (těleso)

Těleso je množina $\mathbb{F}$, vybavena dvěma funkcemi

$$+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}, \quad \cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$$

pro které platí následující:

1. Vlastnosti sčítání:
   1. Existuje $0 \in \mathbb{F}$ tak, že pro vš. $a \in \mathbb{F}$ platí: $a + 0 = 0 + a = a$ (existence nuly).
   2. Pro vš. $a, b, c \in \mathbb{F}$ platí: $(a + b) + c = a + (b + c)$ (asociativita sčítání).
   3. Pro vš. $a, b \in \mathbb{F}$ platí: $a + b = b + a$ (komutativita sčítání).
   4. Pro vš. $a \in \mathbb{F}$ existuje právě jedno $b \in \mathbb{F}$ tak, že $a + b = 0$ (existence opačného čísla, značíme $b = -a$).

Definice tělesa (pokrač.)

2. Vlastnosti násobení:
   1. Existuje $1 \in \mathbb{F}$ tak, že pro vš. $a \in \mathbb{F}$ platí: $1 \cdot a = a$ (existence jednotky).
   2. Pro vš. $a, b, c \in \mathbb{F}$ platí: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (asociativita násobení).
   3. Pro vš. $a, b \in \mathbb{F}$ platí: $a \cdot b = b \cdot a$ (komutativita násobení).
3. Provázanost sčítání a násobení:
   1. Pro vš. $a, b, c \in \mathbb{F}$ platí: $a \cdot (b + c) = a \cdot b + a \cdot c$ (levý distributivní zákon).
   2. Pro vš. $a, b, c \in \mathbb{F}$ platí: $(b + c) \cdot a = b \cdot a + c \cdot a$ (pravý distributivní zákon).
4. Test invertibility: pro vš. $a \in \mathbb{F}$ platí: $a \neq 0$ iff existuje a^{-1}.

Příklady

1. Množiny $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ se standardním sčítáním a násobením jsou tělesa.
2. Množina $\mathbb{Z}$ se standardním sčítáním a násobením není těleso.
3. Množiny $\mathbb{Z}_2$ a $\mathbb{Z}_3$ jsou tělesa (sčítáme a násobíme jako zbytky po dělení 2, resp. 3).

   Obecněji:[a] množina $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, kde p je prvočíslo, je těleso, pokud čísla sčítáme a násobíme jako zbytky po dělení p.

[a] Toto dokážeme v přednášce 11B.

Definice (lineární prostor nad tělesem $\mathbb{F}$)

Lineární prostor nad tělesem $\mathbb{F}$ je množina L spolu se dvěma funkcemi

$$+ : L \times L \to L, \quad \cdot : \mathbb{F} \times L \to L$$

pro které platí následující:

1. Vlastnosti sčítání:
   1. Existuje $\vec{o} \in L$ tak, že pro vš. $\vec{x} \in L$ platí: $\vec{x} + \vec{o} = \vec{o} + \vec{x} = \vec{x}$ (existence nulového vektoru).
   2. Pro vš. $\vec{x}, \vec{y}, \vec{z} \in L$ platí: $(\vec{x} + \vec{y}) + \vec{z} = \vec{x} + (\vec{y} + \vec{z})$ (asociativita sčítání vektorů).
   3. Pro vš. $\vec{x}, \vec{y} \in L$ platí: $\vec{x} + \vec{y} = \vec{y} + \vec{x}$ (komutativita sčítání vektorů).
   4. Pro vš. $\vec{x} \in L$ existuje právě jeden $\vec{y} \in L$ tak, že $\vec{x} + \vec{y} = \vec{o}$ (existence opačného vektoru, značíme $\vec{y} = -\vec{x}$).

Definice (lineární prostor nad tělesem $\mathbb{F}$), pokrač.

2. Vlastnosti násobení skalárem:
   1. Pro vš. $\vec{x} \in L$ platí: $1 \cdot \vec{x} = \vec{x}$ (násobení jednotkovým skalárem).
   2. Pro vš. $a, b \in \mathbb{F}$ a vš. $\vec{x} \in L$ platí: $a \cdot (b \cdot \vec{x}) = (a \cdot b) \cdot \vec{x}$ (asociativita násobení skalárem).
3. Distributivní zákony:
   1. Pro vš. $a, b \in \mathbb{F}$ a vš. $\vec{x} \in L$ platí: $(a + b) \cdot \vec{x} = a \cdot \vec{x} + b \cdot \vec{x}$ (distributivita součtu skalárů).
   2. Pro vš. $a \in \mathbb{F}$ a vš. $\vec{x}, \vec{y} \in L$ platí: $a \cdot (\vec{x} + \vec{y}) = a \cdot \vec{x} + a \cdot \vec{y}$ (distributivita součtu vektorů).

Poznámka

Axiomy tří typů: chování operace $+$, chování operace $\cdot$ a vzájemný vztah obou operací.

Definice je formálně stejná jako pro lineární prostor nad $\mathbb{R}$. Jediná změna: těleso $\mathbb{R}$ je nahrazeno obecným tělesem $\mathbb{F}$.

Příklady lineárních prostorů nad obecným tělesem $\mathbb{F}$

1. Prostory $\mathbb{F}^n$ nad $\mathbb{F}$, $n \geq 1$. Vektory jsou uspořádané n-tice prvků $\mathbb{F}$, psané do sloupce. Skaláry jsou prvky tělesa $\mathbb{F}$.

   Například: v $(\mathbb{Z}_7)^2$ je vektor $\begin{pmatrix} 2 \\ 0 \end{pmatrix}$, v $\mathbb{Q}^3$ je vektor $\begin{pmatrix} 2.14 \\ -21.7 \\ 12 \end{pmatrix}$,

   v $\mathbb{C}^2$ je vektor $\begin{pmatrix} 2-4i \\ \sqrt{3}i \end{pmatrix}$, atd.

2. Prostory $\mathbb{F}[x]$ polynomů v neurčité x s koeficienty z tělesa $\mathbb{F}$. Skaláry jsou prvky tělesa $\mathbb{F}$, vektory jsou jednotlivé polynomy. Sčítání a násobení je definováno analogicky jako v $\mathbb{R}[x]$. Například: v $\mathbb{Z}_3[x]$ platí:

$$\begin{aligned} (2x+2)+(x+2) &= 1 \\ (2x+2)\cdot(x+2) &= 2x^2+1 \end{aligned}$$

Jednoduché důsledky definice

Ať L je lineární prostor. Potom:

1. Nulový vektor je jednoznačně určen.
2. Pro vš. $\vec{x} \in L$ platí: $0 \cdot \vec{x} = \vec{o}$.
3. Opačný vektor k $\vec{x} \in L$ je vektor $(-1) \cdot \vec{x}$.
4. Pro vš. $a \in \mathbb{R}$ platí: $a \cdot \vec{o} = \vec{o}$.

Důkaz.

1. Ať existují $\vec{o_1}, \vec{o_2}$ tak, že pro vš. $\vec{x} \in L$ platí: $\vec{x} + \vec{o_1} = \vec{o_1} + \vec{x} = \vec{x}$ a $\vec{x} + \vec{o_2} = \vec{o_2} + \vec{x} = \vec{x}$. Pak $\vec{o_1} = \vec{o_1} + \vec{o_2} = \vec{o_2}$.
2. Pro vš. $\vec{x} \in L$ platí: $\vec{x} = 1 \cdot \vec{x} = (1 + 0) \cdot \vec{x} = 1 \cdot \vec{x} + 0 \cdot \vec{x} = \vec{x} + 0 \cdot \vec{x}$. Tudíž $0 \cdot \vec{x}$ musí být nulový vektor.

Důkaz (pokrač.)

3. Platí: $\vec{x} + (-1) \cdot \vec{x} = 1 \cdot \vec{x} + (-1) \cdot \vec{x} = (1 - 1) \cdot \vec{x} = 0 \cdot \vec{x} = \vec{o}$.
4. Platí: $a \cdot \vec{o} = a \cdot (0 \cdot \vec{o}) = (a \cdot 0) \cdot \vec{o} = 0 \cdot \vec{o} = \vec{o}$.

■

Velmi důležitý důsledek definice

Ať L je lineární prostor, $a \in \mathbb{F}$, $\vec{x} \in L$. Pak $a \cdot \vec{x} = \vec{o}$ právě tehdy, když $a = 0$ nebo $\vec{x} = \vec{o}$.

Důkaz.

Díky předchozímu stačí dokázat pouze implikaci zleva doprava. Ať $a \cdot \vec{x} = \vec{o}$ a $a \neq 0$. Potom existuje a^{-1}. Tudíž $\vec{o} = a^{-1} \cdot \vec{o} = a^{-1} \cdot (a \cdot \vec{x}) = (a^{-1} \cdot a) \cdot \vec{x} = 1 \cdot \vec{x} = \vec{x}$. ■

Povšimněme si:

Důkazy jsou stejné, jako v minulé přednášce!

Jaký nejobecnější výpočet lze v lineárním prostoru vykonat?

1. Například můžeme sečíst čtyři vektory: $\vec{x} + \vec{y} + \vec{z} + \vec{w}$.
   Díky asociativitě sčítání nemusíme psát závorky.
2. Například můžeme násobek vektoru opět vynásobit: $b \cdot (a \cdot \vec{x})$.
   Díky axiomům jde opět o násobek $(b \cdot a) \cdot \vec{x}$.
3. Obecněji, můžeme sčítat konečně mnoho násobků vektorů.
   To znamená: je-li dán konečný seznam vektorů $(\vec{x}_1, \ldots, \vec{x}_n)$ a konečný seznam skalárů[a] $(a_1, \ldots, a_n)$, lze utvořit lineární kombinaci
   $$a_1 \cdot \vec{x}_1 + a_2 \cdot \vec{x}_2 + a_3 \cdot \vec{x}_3 + \ldots + a_n \cdot \vec{x}_n$$
   značenou také $\displaystyle\sum_{i=1}^{n} a_i \cdot \vec{x}_i$ nebo $\displaystyle\sum_{i \in \{1,\ldots,n\}} a_i \cdot \vec{x}_i$

[a] Těmto skalárům říkáme koeficienty lineární kombinace.

Definice

Seznam (také: skupina) vektorů je buď prázdná posloupnost () nebo konečná posloupnost $(\vec{x}_1, \ldots, \vec{x}_n)$.

Pozor: je rozdíl mezi seznamem a množinou

$(\vec{x}_1, \vec{x}_2, \vec{x}_3) \neq (\vec{x}_3, \vec{x}_2, \vec{x}_1)$ *vs.* $\{\vec{x}_1, \vec{x}_2, \vec{x}_3\} = \{\vec{x}_3, \vec{x}_2, \vec{x}_1\}$

$(\vec{x}_1, \vec{x}_1, \vec{x}_2) \neq (\vec{x}_1, \vec{x}_2)$ *vs.* $\{\vec{x}_1, \vec{x}_1, \vec{x}_2\} = \{\vec{x}_1, \vec{x}_2\}$

Definice (lineární kombinace konečného seznamu vektorů)

Pro seznam vektorů tvaru

1. () definujeme $\vec{o}$ jako jeho (jedinou možnou) lineární kombinaci (s prázdným seznamem koeficientů).
2. $(\vec{x}_1, \ldots, \vec{x}_n)$ je vektor $\sum_{i=1}^{n} a_i \cdot \vec{x}_i$ jeho lineární kombinace (se seznamem koeficientů $(a_1, \ldots, a_n)$).

Příklad (geometrický význam lineární kombinace)

Pro seznam $(\mathbf{a}_1)$ v $\mathbb{R}^2$

a seznam (2.5) reálných čísel je

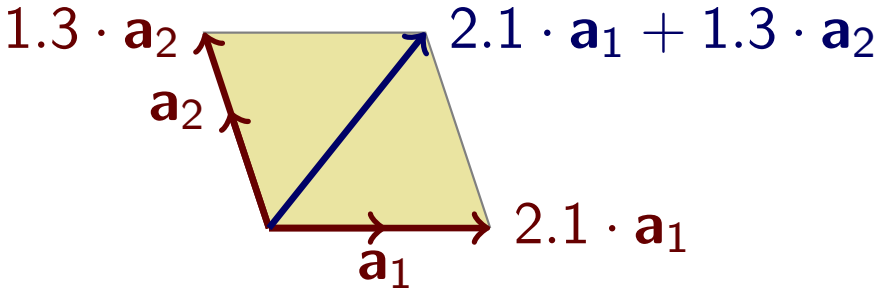
lineární kombinace.

Všechny možné lineární kombinace vektoru $\mathbf{a}_1$ vytvářejí v $\mathbb{R}^2$ přímku procházející počátkem (se směrem $\mathbf{a}_1$).

Příklad (geometrický význam lineární kombinace)

Pro seznam $(\mathbf{a}_1, \mathbf{a}_2)$ v $\mathbb{R}^3$

a seznam $(2.1, 1.3)$ reálných čísel je



Všechny možné lineární kombinace seznamu $(\mathbf{a}_1, \mathbf{a}_2)$ vytvářejí v $\mathbb{R}^3$ rovinu procházející počátkem (se směrem $(\mathbf{a}_1, \mathbf{a}_2)$).

Význam lineárních kombinací (zatím jen slogan)

Ať L je lineární prostor nad $\mathbb{F}$.
Lineární kombinace seznamu $(\vec{x}_1, \ldots, \vec{x}_n)$ v L vytvářejí „rovný kus“ prostoru L.
Tento „rovný kus“ prostoru L prochází počátkem $\vec{o}$ a má „směr“ $(\vec{x}_1, \ldots, \vec{x}_n)$.

Příští přednáška: těmto „rovným kusům“ v L budeme říkat lineární podprostory L.

Příklad (lineární kombinace a soustavy rovnic)

Existují koeficienty x, y v $\mathbb{Z}_7$ tak, že v $(\mathbb{Z}_7)^2$ platí rovnost

$$x \cdot \begin{pmatrix} 2 \\ 3 \end{pmatrix} + y \cdot \begin{pmatrix} 6 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 6 \end{pmatrix} \quad ?$$

Dva pohledy na tento problém:

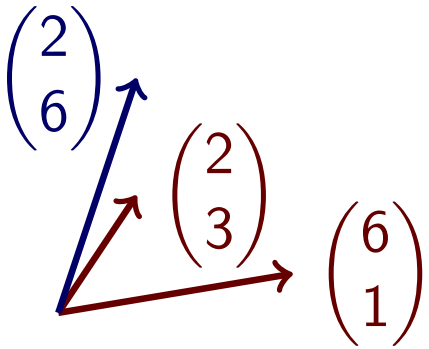
1. Hledáme prvky x, y v $\mathbb{Z}_7$ tak, že platí

$$\begin{aligned} 2x + 6y &= 2 \\ 3x + 1y &= 6 \end{aligned}$$

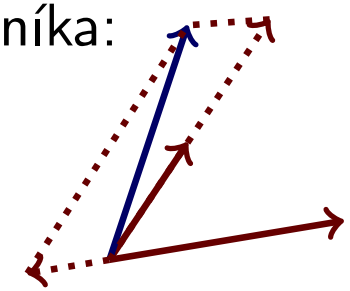
   To znamená: koeficienty lineární kombinace jsou řešením jisté soustavy lineárních rovnic nad $\mathbb{Z}_7$.

Příklad (lineární kombinace a soustavy rovnic, pokrač.)

2. Pro zadané vektory



hledáme „natažení“ červených vektorů tak, aby modrý vektor byl úhlopříčkou čtyřúhelníka:



Pozor: výše uvedený obrázek je „slogan“! Pracujeme totiž v $(\mathbb{Z}_7)^2$.

Zobecnění předchozího (zatím jen slogan)

Hledáme-li pro pevný seznam $(\mathbf{a}_1, \ldots, \mathbf{a}_s)$ a pevný vektor $\mathbf{b}$ v $\mathbb{F}^r$ reálné koeficienty $x_1, \ldots, x_s$ tak, aby platila rovnost

$$x_1 \cdot \mathbf{a}_1 + \ldots + x_s \cdot \mathbf{a}_s = \mathbf{b}$$

pak lze na tuto úlohu pohlížet dvěma způsoby:

1. Řešíme soustavu r lineárních rovnic o s neznámých.
2. Hledáme „natažení“ vektorů $\mathbf{a}_1, \ldots, \mathbf{a}_s$ pomocí skalárů $x_1, \ldots, x_s$ tak, aby vektor $\mathbf{b}$ tvořil úhlopříčku rovnoběžnostěnu.

Příští přednášky: druhý pohled na tuto úlohu nám dovolí vybudovat elegantní metodu řešení (Gaussovu eliminaci).

Lineární obal a lineární podprostor

Odpřednesenou látku naleznete v kapitolách 1.5 a 1.6 skript *Abstraktní a konkrétní lineární algebra*.

Minulá přednáška

1. Definice lineárního prostoru (nad obecným tělesem).
2. Lineární kombinace.

Dnešní přednáška

1. Lineární obal množiny vektorů.
2. Lineární podprostor lineárního prostoru.

Připomenutí

V lineárním prostoru můžeme zjednodušovat zápisy:

1. Píšeme: $-\vec{x}$ místo $(-1)\cdot\vec{x}$. Jde o opačný vektor k vektoru $\vec{x}$ (dokázáno minule).
2. Píšeme: $\vec{x}_1+\vec{x}_2+\cdots+\vec{x}_{n-1}+\vec{x}_n$ místo $(\ldots(\vec{x}_1+\vec{x}_2)+\cdots+\vec{x}_{n-1})+\vec{x}_n$. Důvod: asociativita sčítání vektorů.

Lineární kombinace seznamu $(\vec{x}_1,\ldots,\vec{x}_n)$ s koeficienty $a_1,\ \ldots,\ a_n$ z tělesa $\mathbb{F}$ je vektor $\displaystyle\sum_{i=1}^{n} a_i\cdot\vec{x}_i$.

Lineární kombinace prázdného seznamu () je nulový vektor.

Konečné a nekonečné množiny

Připomenutí:[a] množina přirozených čísel $\mathbb{N} = \{0, 1, 2, \dots\}$.

1. Množina M je konečná, když má přesně n prvků, kde n je nějaké přirozené číslo.

   To znamená: M je konečná, když buď

   $M = \emptyset$ (množina M má 0 prvků),

   nebo

   $M = \{x_1, \dots, x_n\}$, kde $n \geq 1$ je přirozené číslo (v tom případě má množina M n prvků).

2. Množina M je nekonečná, když není konečná.

   Například $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ jsou nekonečné množiny. Množina $\mathbb{R}[x]$ je nekonečná.

[a] Důležité: v této přednášce nula je přirozené číslo.

Definice (lineární obal množiny vektorů)

Ať M je jakákoli množina vektorů lineárního prostoru L. Lineární obal množiny vektorů M je množina $\mathrm{span}(M)$, definovaná takto:

$$\vec{x} \in \mathrm{span}(M) \quad \text{právě tehdy, když}^{a} \quad \vec{x} = \sum_{i=1}^{n} a_i \cdot \vec{x}_i$$

pro nějaké $n \geq 0$, nějaká $a_1, \ldots, a_n \in \mathbb{F}$ a nějaká $\vec{x}_1, \ldots, \vec{x}_n \in M$.

[a] Pozor: prázdná lineární kombinace je rovna vektoru $\vec{o}$.

Ujasnění si definice $\mathrm{span}(M)$

$\vec{x} \in \mathrm{span}(M)$ právě tehdy, když existuje nějaký seznam S vektorů z množiny M tak, že $\vec{x}$ je roven nějaké lineární kombinaci seznamu S.

To jest: $\mathrm{span}(M)$ je množina všech možných lineárních kombinací, které lze z M utvořit.

Příklady (viz minulé přednášky)

1. Pro

   v $\mathbb{R}^2$ je $\mathrm{span}(\{\mathbf{a}_1\})$ přímka procházející počátkem se směrem $(\mathbf{a}_1)$.

2. Pro

   v $\mathbb{R}^3$ je $\mathrm{span}(\{\mathbf{a}_1, \mathbf{a}_2\})$ rovina procházející počátkem se směrem $(\mathbf{a}_1, \mathbf{a}_2)$.

   Pozor: pro

   v $\mathbb{R}^3$, lineární obal $\mathrm{span}(\{\mathbf{a}_1, \mathbf{a}_2\})$ není rovina! Jde opět o přímku. Jak poznat o co jde? Uvidíme příště.[a]

[a] Toto téma se zove lineární závislost a lineární nezávislost.

Uzávěrové vlastnosti lineárního obalu

1. Je-li $M \subseteq N$, potom $\mathrm{span}(M) \subseteq \mathrm{span}(N)$.
2. Pro vš. M platí: $M \subseteq \mathrm{span}(M)$.
3. Pro vš. M platí: $\mathrm{span}(\mathrm{span}(M)) \subseteq \mathrm{span}(M)$.

Důkaz.

Přednáška. ∎

Vysvětlení uzávěrových vlastností (slogan)

Lineárními kombinacemi tvoříme „rovné kusy“ lineárního prostoru (viz minulou přednášku).

Množina $\mathrm{span}(M)$ je tedy „zabalení“ množiny M tak, aby výsledkem byl „co nejmenší rovný kus“, který obsahuje M.

Definice (lineární podprostor)

Ať W je podmnožina lineárního prostoru L. Řekneme, že W je lineární podprostor lineárního prostoru L, když platí $\operatorname{span}(W) \subseteq W$.

Slogan pro lineární podprostor

Podprostor je „dobrá“ podmnožina prostoru. Žádnou lineární kombinací nelze z lineárního podprostoru „utéct“.

Tvrzení

1. $\operatorname{span}(M)$ je vždy lineární podprostor. Jde o nejmenší podprostor, který obsahuje množinu M.
2. Množina M je lineární podprostor právě tehdy, když $\operatorname{span}(M) = M$.

Důkaz.

Přednáška.

Tvrzení

Ať L je lineární prostor. Podmnožina $W \subseteq L$ je lineárním podprostorem prostoru L právě tehdy, když platí:

1. $\vec{o}$ je prvkem W (uzavřenost W na nulový vektor).
2. $\vec{x} + \vec{y}$ je prvkem W, pro každé $\vec{x}, \vec{y} \in W$ (uzavřenost W na součet vektorů).
3. $a \cdot \vec{x}$ je prvkem W, pro každé $a \in \mathbb{F}$ a každé $\vec{x} \in W$ (uzavřenost W na skalární násobek).

Důkaz.

Přednáška. ■

Další slogan pro lineární podprostor

Lineární podprostor vždy obsahuje nulový vektor a „vydrží“ operace součtu a skalárního násobku.

Důležité

Ať W je lineární podprostor lineárního prostoru L. Potom množina W sama o sobě je lineárním prostorem, pokud sčítání vektorů ve W a násobení vektoru skalárem ve W definujeme stejně jako v prostoru L.

Obrácené tvrzení ale neplatí: například $W = \{\begin{pmatrix} x \\ 1 \end{pmatrix} \mid x \in \mathbb{R}\}$ není lineárním podprostorem $\mathbb{R}^2$. Ale množina W spolu s operacemi

$$\begin{pmatrix} x \\ 1 \end{pmatrix} \oplus \begin{pmatrix} x' \\ 1 \end{pmatrix} = \begin{pmatrix} x + x' \\ 1 \end{pmatrix} \qquad a \odot \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} a \cdot x \\ 1 \end{pmatrix}$$

tvoří lineární prostor nad $\mathbb{R}$.

Příklady

1. Každý lineární prostor je sám svým podprostorem.
2. Množina $\{\vec{o}\}$ je vždy lineárním podprostorem.[a]
3. $\mathbb{R}^3$ je lineární prostor (operace jsou definovány po složkách).
   1. $W_1 = \{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \mid z = 0\}$ je lineárním podprostorem $\mathbb{R}^3$.
   2. $W_2 = \{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \mid z = 1\}$ není lineárním podprostorem $\mathbb{R}^3$.

      Pozor! Na množině W_2 lze definovat strukturu lineárního prostoru (cvičení).

[a] Tomuto podprostoru říkáme triviální podprostor.

Příklady (pokrač.)

4. Označme jako $\mathbb{R}^{\leq 3}[x]$ množinu všech reálných polynomů stupně maximálně 3 a jako $\mathbb{R}^{\leq 136}[x]$ množinu všech reálných polynomů stupně maximálně 136.
   Potom $\mathbb{R}^{\leq 3}[x]$ je lineární podprostor lineárního prostoru $\mathbb{R}^{\leq 136}[x]$.

   Obecněji: Ať $\mathbb{F}$ je těleso. Označme jako $\mathbb{F}^{\leq n}[x]$ množinu všech polynomů nad $\mathbb{F}$ stupně maximálně n, $n \geq 0$.
   Jakmile $n \leq m$, je $\mathbb{F}^{\leq n}[x]$ lineární podprostor lineárního prostoru $\mathbb{F}^{\leq m}[x]$.
5. Pro každé $n \geq 0$ je $\mathbb{F}^{\leq n}[x]$ lineární podprostor lineárního prostoru $\mathbb{F}[x]$.

Vlastnosti lineárních podprostorů

Ať L je lineární prostor.

1. Průnik libovolného systému $\{W_i \mid i \in I\}$ podprostorů prostoru L je lineárním podprostorem prostoru L.
2. Sjednocení systému $\{W_i \mid i \in I\}$ lineárních podprostorů prostoru L obecně lineárním podprostorem prostoru L není.

Důkaz.

Přednáška. ■

Definice (spojení lineárních podprostorů)

Ať $\{W_i \mid i \in I\}$ je systém lineárních podprostorů prostoru L. Lineárnímu podprostoru $\operatorname{span}(\bigcup_{i\in I} W_i)$ prostoru L říkáme spojení podprostorů W_i, $i \in I$, a značíme jej[a]

$$\bigvee_{i\in I} W_i$$

[a] V případě dvou podprostorů používáme i značení $W_1 \vee W_2$.

Klasifikace lineárních podprostorů prostoru $\mathbb{R}^3$

Všechny podprostory $\mathbb{R}^3$ jsou buď

1. Jednoprvková množina obsahující pouze počátek.

nebo

2. Každá přímka procházející počátkem.

nebo

3. Každá rovina procházející počátkem.

nebo

4. Celá množina $\mathbb{R}^3$.

Důkaz.

V každém z uvedených bodů je lineární podprostor prostoru $\mathbb{R}^3$. To, že žádné jiné lineární podprostory prostoru $\mathbb{R}^3$ neexistují, ukážeme později.[a] ■

[a] Budeme k tomu potřebovat pojem dimense.

Lineární závislost a nezávislost

Odpřednesenou látku naleznete v kapitole 3.1 skript *Abstraktní a konkrétní lineární algebra*.

Minulé přednášky

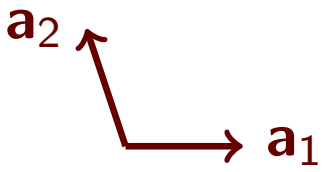
1. Lineární kombinace.
2. Definice lineárního obalu.
3. Definice lineárního podprostoru.

Dnešní přednáška

1. Lineární závislost/nezávislost seznamu a množiny vektorů v lineárním prostoru.

Připomenutí

1. Pro



   v $\mathbb{R}^3$ je $\operatorname{span}(\{\mathbf{a}_1, \mathbf{a}_2\})$ rovina procházející počátkem se směrem $(\mathbf{a}_1, \mathbf{a}_2)$.

2. Pro

   v $\mathbb{R}^3$, lineární obal $\operatorname{span}(\{\mathbf{a}_1, \mathbf{a}_2\})$ rovina není.

   V množině $\{\mathbf{a}_1, \mathbf{a}_2\}$ je (například) vektor $\mathbf{a}_2$ „zbytečný vzhledem k tvorbě lineárních kombinací“.[a]

   Platí totiž $\operatorname{span}(\{\mathbf{a}_1, \mathbf{a}_2\}) = \operatorname{span}(\{\mathbf{a}_1\})$.

[a] Za chvíli budeme říkat, že množina $\{\mathbf{a}_1, \mathbf{a}_2\}$ je lineárně závislá.

Definice

Lineární kombinace $a_1 \cdot \vec{x}_1 + \cdots + a_n \cdot \vec{x}_n$ je triviální, pokud $a_1 = a_2 = \cdots = a_n = 0$.
V opačném případě je lineární kombinace $a_1 \cdot \vec{x}_1 + \cdots + a_n \cdot \vec{x}_n$ netriviální.

Poznámky

1. Triviální lineární kombinace je vždy rovna nulovému vektoru: rovnost $0 \cdot \vec{x}_1 + \cdots + 0 \cdot \vec{x}_n = \vec{o}$ platí, protože $0 \cdot \vec{x} = \vec{o}$, pro jakýkoli vektor $\vec{x}$ (dokázáno minule).
2. I netriviální lineární kombinace může být rovna nulovému vektoru: například $\vec{x} - \vec{x} = \vec{o}$, pro jakýkoli vektor $\vec{x}$.
3. Lineární kombinaci, která dává nulový vektor, také říkáme nulová kombinace.[a]

[a] Pozor: triviální kombinace je vždy nulová. Nulová kombinace nemusí být triviální.

Definice (lineární nezávislost seznamu vektorů)

Řekneme, že seznam S vektorů je lineárně nezávislý, pokud platí jedna z podmínek:

1. Seznam S je prázdný.
2. Seznam S je tvaru $(\vec{x}_1, \ldots, \vec{x}_n)$ a platí: kdykoli $a_1 \cdot \vec{x}_1 + \cdots + a_n \cdot \vec{x}_n = \vec{o}$, pak $a_1 = a_2 = \cdots = a_n = 0$.

Řekneme, že seznam S je lineárně závislý, pokud není lineárně nezávislý.

Příklady

1. Prázdný seznam () je vždy lineárně nezávislý.
2. Seznam $(\vec{o})$ je vždy lineárně závislý.
3. Seznam, ve kterém se opakuje vektor, je vždy lineárně závislý.

Příklad

Nulová lineární kombinace $x_1 \cdot \mathbf{a}_1 + \dots x_s \cdot \mathbf{a}_s = \mathbf{o}$ v $\mathbb{F}^r$, kde

$$\mathbf{a}_1 = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{r1} \end{pmatrix}, \dots, \quad \mathbf{a}_s = \begin{pmatrix} a_{1s} \\ a_{2s} \\ \vdots \\ a_{rs} \end{pmatrix}$$

kóduje soustavu r lineárních rovnic

$$\begin{aligned} x_1 a_{11} + x_2 a_{12} + \dots + x_s a_{1s} &= 0 \\ x_1 a_{21} + x_2 a_{22} + \dots + x_s a_{2s} &= 0 \\ &\vdots \\ x_1 a_{r1} + x_2 a_{r2} + \dots + x_s a_{rs} &= 0 \end{aligned}$$

o s neznámých nad $\mathbb{F}$.

Seznam $(\mathbf{a}_1, \dots, \mathbf{a}_s)$ je lineárně nezávislý právě tehdy, když tato soustava má pouze triviální řešení $x_1 = x_2 = \dots = x_s = 0$.

Definice (lineární nezávislost množiny vektorů)

Ať M je množina vektorů v lineárním prostoru L. Řekneme, že M je lineárně nezávislá, pokud platí jedna z následujících podmínek:

1. Množina M je prázdná.
2. $M = \{\vec{x}_1, \dots, \vec{x}_n\}$ je neprázdná konečná množina a navíc platí: kdykoli $a_1 \cdot \vec{x}_1 + \cdots + a_n \cdot \vec{x}_n = \vec{o}$, pak $a_1 = a_2 = \cdots = a_n = 0$.
3. M je nekonečná množina a každá její konečná podmnožina je lineárně nezávislá.

Řekneme, že množina M je lineárně závislá, pokud není lineárně nezávislá.

Praktický test lineární nezávislosti neprázdné množiny M

Musí platit následující implikace:

> Ať $a_1 \cdot \vec{x}_1 + \cdots + a_n \cdot \vec{x}_n = \vec{o}$, kde $n > 0$ je přirozené číslo, vektory $\vec{x}_1, \dots, \vec{x}_n$ jsou z M a skaláry $a_1, \dots, a_n$ jsou z $\mathbb{F}$. Potom $a_1 = a_2 = \cdots = a_n = 0$.

Příklady

1. $\{\vec{o}\}$ je lineárně závislá množina v jakémkoli lineárním prostoru L.

   Obecněji: ať $\vec{o} \in M$, potom M je lineárně závislá množina.

2. Množina $\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$ je lineárně nezávislá množina v $\mathbb{R}^3$.

   Obecněji: definujte pro $i = 1, \dots, n$, vektor $\mathbf{e}_i \in \mathbb{R}^n$ jako n-tici mající na i-té posici 1 a všude jinde 0. Potom $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ je lineárně nezávislá množina v $\mathbb{R}^n$.

3. Nekonečná množina $\{1, x, x^2, x^3, \dots\}$ je lineárně nezávislá množina v prostoru polynomů $\mathbb{R}[x]$.

Příklady (pokrač.)

4. Množina $\left\{ \begin{pmatrix} 1 \\ -7 \\ 3 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 8 \\ -9 \end{pmatrix} \right\}$ je lineárně závislá množina v $\mathbb{R}^3$.

   Důvod:

$$2 \cdot \begin{pmatrix} 1 \\ -7 \\ 3 \end{pmatrix} + 3 \cdot \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix} + 1 \cdot \begin{pmatrix} 1 \\ 8 \\ -9 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Tvrzení

Ať M je lineárně nezávislá množina vektorů v lineárním prostoru L. Jakmile $N \subseteq M$, je i N lineárně nezávislá množina vektorů.

Důkaz.

Přednáška. ■

Slogan

Ubereme-li z lineárně nezávislé množiny vektorů nějaké vektory, je výsledná množina opět lineárně nezávislá.

Tvrzení

Ať M je lineárně závislá množina vektorů v lineárním prostoru L. Jakmile N je množina vektorů z L a platí $M \subseteq N$, je i N lineárně závislá množina vektorů.

Důkaz.

Přednáška. ■

Slogan

Přidáme-li do lineárně závislé množiny vektorů nějaké vektory, je výsledná množina opět lineárně závislá.

Věta (charakterisace lineárně nezávislých množin)

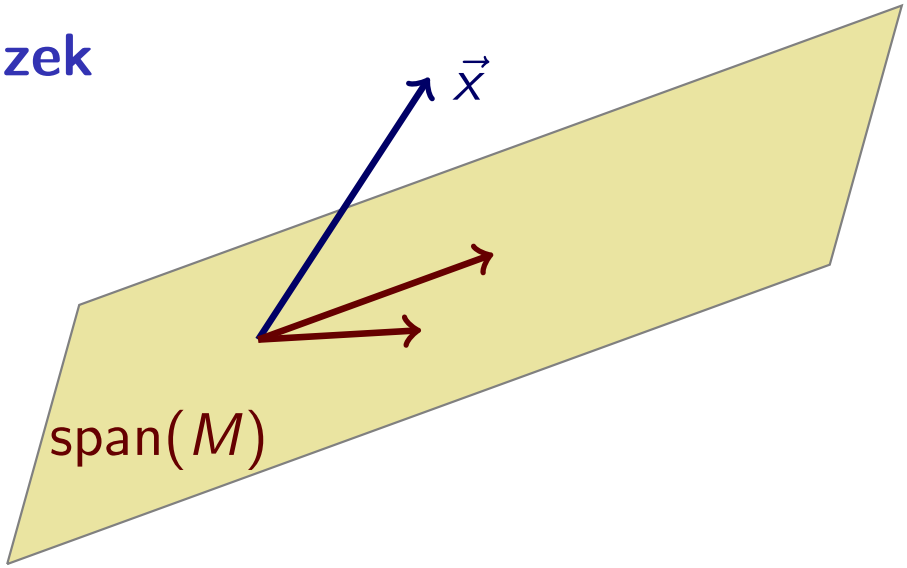
Pro množinu M vektorů z lineárního prostoru L jsou následující podmínky ekvivalentní:

1. Množina M je lineárně nezávislá.
2. Pro každý vektor $\vec{x} \notin \operatorname{span}(M)$ je množina $M \cup \{\vec{x}\}$ lineárně nezávislá.

Důkaz.

Přednáška. ■

Ilustrační obrázek



Věta (charakterisace lineárně závislých množin)

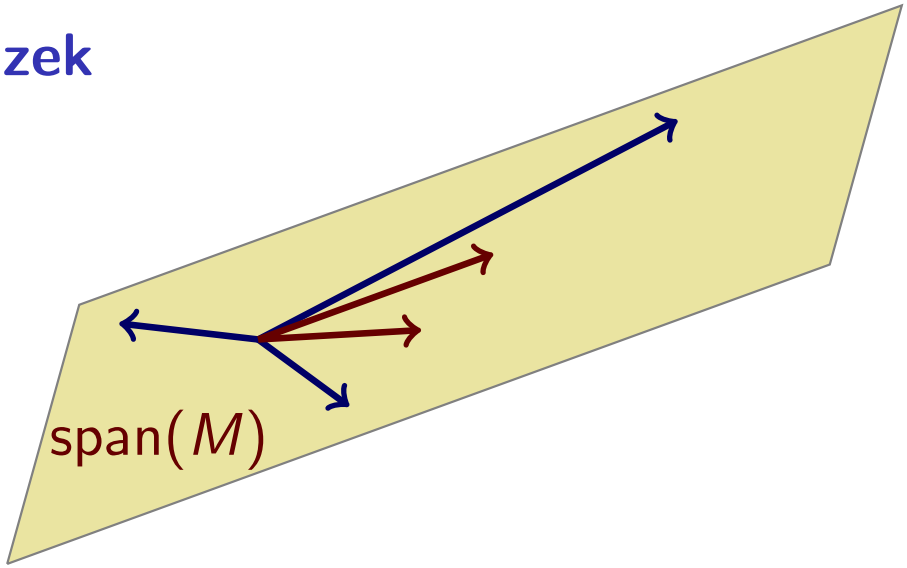
Pro množinu M vektorů z lineárního prostoru L jsou následující podmínky ekvivalentní:

1. Množina M je lineárně závislá.
2. Existuje $\vec{v} \in M$ tak, že $\operatorname{span}(M \setminus \{\vec{v}\}) = \operatorname{span}(M)$.

Důkaz.

Přednáška. ∎

Ilustrační obrázek



Báze a dimense

Odpřednesenou látku naleznete v kapitolách 3.1–3.3 a 3.6 skript *Abstraktní a konkrétní lineární algebra*.

Minulé přednášky

1. Lineární kombinace, lineární závislost/nezávislost.
2. Lineární obal seznamu/množiny vektorů.

Dnešní přednáška

1. Báze lineárního (pod)prostoru.

   Intuitivní význam: báze je výběr systému souřadnicových os.
2. Dimense lineárního (pod)prostroru.

   Intuitivní význam: dimense je počet souřadnicových os.

Připomenutí

Množina M je konečná, pokud buď $M = \emptyset$ nebo $M = \{x_1, \ldots, x_n\}$ pro nějaké přirozené číslo $n \geq 1$. Množina M je nekonečná, když není konečná.

Definice (množina generátorů)

Ať W je lineární podprostor prostoru L. Řekneme, že množina G generuje W, když platí $\operatorname{span}(G) = W$. (Říkáme také: G je množina generátorů podprostoru W.)

Definice (konečně generovaný podprostor)

Řekneme, že lineární podprostor W prostoru L je konečně generovaný, když existuje konečná množina jeho generátorů. (To jest, když platí $\operatorname{span}(G) = W$ pro nějakou konečnou množinu G.)

Příklady

1. Pro každý prostor L platí: L je množina generátorů prostoru L.

   Množina generátorů L prostoru L obecně není konečná a je vždy lineárně závislá (například: $\mathbb{R}^2$ je nekonečná lineárně závislá množina generátorů prostoru $\mathbb{R}^2$).

2. Jak $\emptyset$, tak $\{\vec{o}\}$ jsou konečné množiny generátorů triviálního prostoru $\{\vec{o}\}$. Důvody: $\mathrm{span}(\emptyset) = \{\vec{o}\}$ (minulé přednášky) a $\mathrm{span}(\{\vec{o}\}) = \{\vec{o}\}$.
   Všimněme si:
   1. $\emptyset$ je lineárně nezávislá množina generátorů prostoru $\{\vec{o}\}$.
   2. $\{\vec{o}\}$ je lineárně závislá množina generátorů prostoru $\{\vec{o}\}$.

3. Konečná množina $G = \{\begin{pmatrix} -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\}$ generuje „osu prvního a třetího kvadrantu“ prostoru $\mathbb{R}^2$. Množina G je lineárně závislá.

Definice (báze)

Lineárně nezávislé množině B, která generuje prostor L, říkáme báze prostoru L. Je-li B konečná, pak seznamu prvků B říkáme uspořádaná báze.

Slogan pro bázi

Báze prostoru je „nejúspornější“ množina generátorů.

Příklady

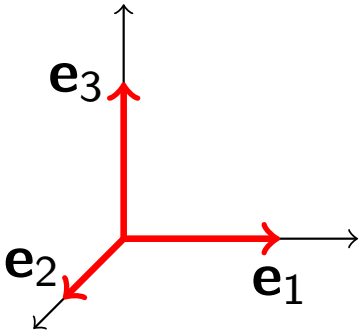
1. $\emptyset$ je báze triviálního prostoru $\{\vec{o}\}$.
2. Každá z množin $\{\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}3\\-4\end{pmatrix}\}$, $\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\}$ tvoří bázi prostoru $\mathbb{R}^2$.
3. Množina $\{1, x, x^2, x^3, \dots\}$ tvoří bázi prostoru $\mathbb{R}[x]$ všech reálných polynomů.

Příklad (kanonická báze prostoru $\mathbb{F}^n$, $n \geq 1$)

Ať $\mathbb{F}$ je jakékoli těleso. Označme jako $K_n = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$ následující seznam vektorů v $\mathbb{F}^n$, $n \geq 1$:

$\mathbf{e}_i$ má jedničku na i-té posici, všude jinde nuly.

Potom K_n je uspořádaná báze prostoru $\mathbb{F}^n$.
Této uspořádané bázi K_n říkáme kanonická báze prostoru $\mathbb{F}^n$.
(Také: standardní báze.)
Příklad: kanonická báze K_3 v $\mathbb{R}^3$.



$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad \mathbf{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Příklad: Fourierova báze pro $n = 4$ (varianta této báze je používána v JPEG)

Pro $w = e^{\frac{2\pi i}{4}} = i$, je seznam $(\vec{f_0}, \vec{f_1}, \vec{f_2}, \vec{f_3})$, kde

$$\vec{f_0} = \begin{pmatrix} w^0 \\ w^0 \\ w^0 \\ w^0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad \vec{f_1} = \begin{pmatrix} w^0 \\ w^1 \\ w^2 \\ w^3 \end{pmatrix} = \begin{pmatrix} 1 \\ i \\ -1 \\ -i \end{pmatrix}$$

$$\vec{f_2} = \begin{pmatrix} w^0 \\ w^2 \\ w^4 \\ w^6 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \quad \vec{f_3} = \begin{pmatrix} w^0 \\ w^3 \\ w^6 \\ w^9 \end{pmatrix} = \begin{pmatrix} 1 \\ -i \\ -1 \\ i \end{pmatrix}$$

uspořádaná báze lineárního prostoru $\mathbb{C}^4$ nad tělesem $\mathbb{C}$.

Tvrzení (Existence báze pro konečně generované prostory)

Každý konečně generovaný prostor L má konečnou bázi.
Navíc: všechny možné báze prostoru L mají stejný počet prvků.

Myšlenka důkazu

První tvrzení: víme, že $\mathrm{span}(G) = L$, kde G je konečná. Lze postupovat dvěma způsoby:

(I) „Přidávat“ do prázdné množiny „důležité“ vektory z G.

(II) „Ubírat“ z G „zbytečné“ vektory.

Detaily: přednáška.

Druhé tvrzení: Exchange Lemma (viz skripta, Lemma 3.2.10 a cvičení).

Definice (prostor konečné dimense)

Lineární prostor L má dimensi n (značíme: $\dim(L) = n$), když existuje báze B prostoru L, která má n prvků,[a] kde n je přirozené číslo.

[a] A tudíž, podle předchozího, všechny báze prostoru L mají n prvků.

Příklady

1. Platí: $\dim(\mathbb{R}^n) = n$, $n \geq 0$.
2. Obecněji: pro jakékoli těleso $\mathbb{F}$ platí $\dim(\mathbb{F}^n) = n$, $n \geq 0$.
3. Platí: $\dim(\{\vec{o}\}) = 0$.
4. Prostor $\mathbb{R}[x]$ všech reálných polynomů nemá konečnou dimensi.
5. Podprostor $\mathbb{R}^{\leq 3}[x]$ (polynomy stupně nejvýše 3) prostoru $\mathbb{R}[x]$ má dimensi 4. Uspořádaná báze je např. $(x^3, x^2, x, 1)$.

Poznámka

Ať $\dim(L) = n$ a ať M je podmnožina L, která má m prvků.

1. Je-li M lineárně nezávislá, pak $m \leq n$.
2. Ať $m = n$. M je lineárně nezávislá právě tehdy, když platí $\mathrm{span}(M) = L$.

Důsledek (klasifikace lineárních podprostorů $\mathbb{R}^3$)

Lineární podprostory prostoru $\mathbb{R}^3$ jsou přesně tvaru $\mathrm{span}(M)$, kde M (zaměření podprostoru) je lineárně nezávislá podmnožina $\mathbb{R}^3$:

1. Počátek $\{\vec{o}\}$ (když M má nula prvků).
2. Přímky procházející počátkem (když M má jeden prvek).
3. Roviny procházející počátkem (když M má dva prvky).
4. Celé $\mathbb{R}^3$ (když M má tři prvky).

Zobecnění: klasifikace[a] lineárních podprostorů prostoru $\mathbb{R}^n$ (dokonce na lineární podprostory prostoru $\mathbb{F}^n$).

[a] To je náročnější na představu, ale geometrický význam je podobný jako pro lineární podprostory prostoru $\mathbb{R}^3$.

Připomenutí (Téma 2A)

Podprostoru $\mathrm{span}(W_1 \cup W_2)$ říkáme spojení podprostorů W_1 a W_2.
Značení: $W_1 \vee W_2$.

Věta (rovnost dvou lineárních podprostorů)

Ať W_1, W_2 jsou lineární podprostory prostoru L konečné dimense.
Potom $W_1 = W_2$ právě tehdy, když platí rovnost
$\dim(W_1) = \dim(W_2) = \dim(W_1 \vee W_2)$.[a]

---

[a] Důkaz: domácí cvičení. Postupujte následovně:

1. Ať $W_1 = W_2$. Potom $W_1 \vee W_2 = W_1$. Tudíž platí rovnost $\dim(W_1) = \dim(W_2) = \dim(W_1 \vee W_2)$.
2. Ať $\dim(W_1) = \dim(W_2) = \dim(W_1 \vee W_2)$. Protože $W_1 \subseteq W_1 \vee W_2$ a oba podprostory mají stejnou dimensi, platí $W_1 = W_1 \vee W_2$.
   Rovnost $W_2 = W_1 \vee W_2$ se dokáže analogicky.
   Celkově: $W_1 = W_1 \vee W_2 = W_2$, hotovo.

Důsledek (důležitý pro Frobeniovu větu, téma 6A)

Ať W je lineární podprostor prostoru L konečné dimense. Pro vektor $\vec{v}$ jsou následující podmínky ekvivalentní:[a]

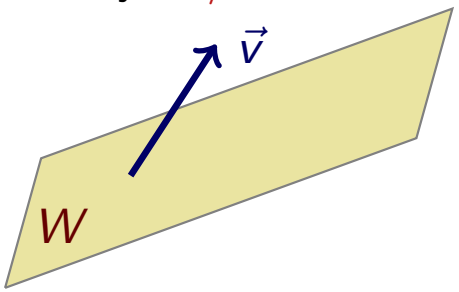
1. $\vec{v} \in W$
2. $\dim(W) = \dim(W \vee \mathrm{span}(\vec{v}))$

---

[a] Důkaz: domácí cvičení. Postupujte následovně:

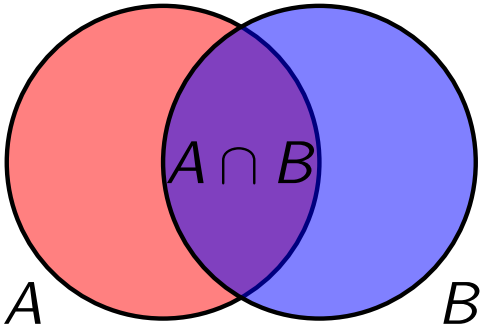
1. Dokažte: $\vec{v} \in W$ iff $\mathrm{span}(\vec{v}) \subseteq W$ iff $W = W \vee \mathrm{span}(\vec{v})$.
2. Použijte větu z předchozí stránky: $W = W \vee \mathrm{span}(\vec{v})$ iff $\dim(W) = \dim(W \vee \mathrm{span}(\vec{v})) = \dim(\underbrace{W \vee (W \vee \mathrm{span}(\vec{v}))}_{=W \vee \mathrm{span}(\vec{v})})$.

Měl by pomoci obrázek situace, kdy $\vec{v} \notin W$:



Připomenutí (princip inkluse a exkluse)

Ať A a B jsou konečné množiny.



Označíme-li počet prvků množin A, B, $A \cap B$ a $A \cup B$ jako $\mathrm{card}(A)$, $\mathrm{card}(B)$, $\mathrm{card}(A \cap B)$ a $\mathrm{card}(A \cup B)$, potom platí rovnost

$$\mathrm{card}(A \cup B) + \mathrm{card}(A \cap B) = \mathrm{card}(A) + \mathrm{card}(B)$$

Věta (o dimensi spojení a průniku)

Ať je L lineární prostor konečné dimense. Potom, pro libovolné lineární podprostory W_1, W_2, platí rovnost
$\dim(W_1 \vee W_2) + \dim(W_1 \cap W_2) = \dim(W_1) + \dim(W_2)$.

Důkaz.

Přednáška. ■

Slogan pro větu o dimensi spojení a průniku

Jde o „princip inkluse a exkluse“ pro lineární prostory konečné dimense. Dimense hraje roli počtu prvků.[a]

[a] Znovu upozorňujeme: slogan je reklamní heslo, nikoli skutečnost.

Věta (za předpokladu (AC))

Každý lineární prostor L má bázi.

Důkaz.

Náročný: nebudeme dokazovat. ■

Poznámka

Předpoklad (AC). Zkratka (AC) znamená Axiom of Choice, česky: axiom výběru.
Jedná se o tvrzení: kartézský součin libovolného systému neprázdných množin je neprázdná množina.[a]
Tvrzení (AC) je nezávislé na základních axiomech teorie množin.
Srovnejte s axiomem o rovnoběžkách z geometrie.

[a] Ve skriptech je použita ekvivalentní formulace (AC), tzv. Zornovo Lemma.

Pozor: stejný prostor nad různými tělesy má různé vlastnosti

1. Množina $\mathbb{C}$ všech komplexních čísel je
   1. lineární prostor dimense 1 nad tělesem $\mathbb{C}$,
   2. lineární prostor dimense 2 nad tělesem $\mathbb{R}$.
2. Množina $\mathbb{R}$ všech reálných čísel je
   1. lineární prostor dimense 1 nad tělesem $\mathbb{R}$,
   2. lineární prostor nekonečné dimense nad tělesem $\mathbb{Q}$.[a]

[a] Nepovinné: takzvaná Hamelova báze reálných čísel, viz Příklad 3.6.5 skript.

Důsledek: měli bychom vždy psát, nad jakým tělesem o lineárním prostoru mluvíme!

Souřadnice vzhledem k uspořádané bázi a komutativní diagramy

Odpřednesenou látku naleznete v kapitolách 3.1–3.3 a 2.2 skript *Abstraktní a konkrétní lineární algebra*.

Minulá přednáška

1. Báze lineárního (pod)prostoru.

   Intuitivní význam: báze je výběr systému souřadnicových os.

2. Dimense lineárního (pod)prostroru.

   Intuitivní význam: dimense je počet souřadnicových os.

Dnešní přednáška

1. Souřadnice vektoru vzhledem k uspořádané bázi.

   Intuitivní význam: souřadnice vektoru udávají „úseky“ vektoru na jednotlivých souřadnicových osách.

2. Ukážeme velmi užitečný pohled na zobrazení (funkce): kalkulus komutativních diagramů.

Věta (existence souřadnic vzhledem k uspořádané bázi)

Ať seznam $B = (\vec{b}_1, \dots, \vec{b}_n)$ tvoří bázi lineárního prostoru L. Pro každý vektor $\vec{x}$ v L existuje jediný seznam $(a_1, \dots, a_n)$ prvků $\mathbb{F}$ tak, že $\vec{x} = a_1 \cdot \vec{b}_1 + \dots + a_n \cdot \vec{b}_n$.

Důkaz.

Přednáška. ■

Definice (souřadnice vzhledem k uspořádané bázi)

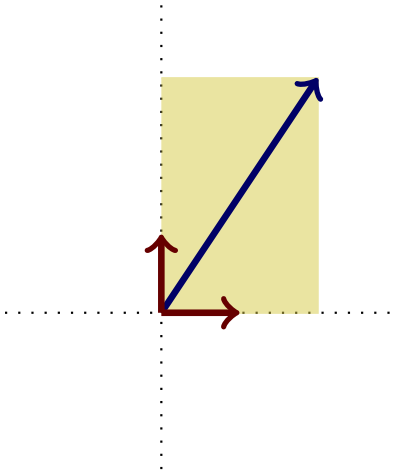
Seznamu $(a_1, \dots, a_n)$ z předchozí věty říkáme souřadnice vektoru $\vec{x}$ vzhledem k uspořádané bázi $B = (\vec{b}_1, \dots, \vec{b}_n)$. Značení:[a]

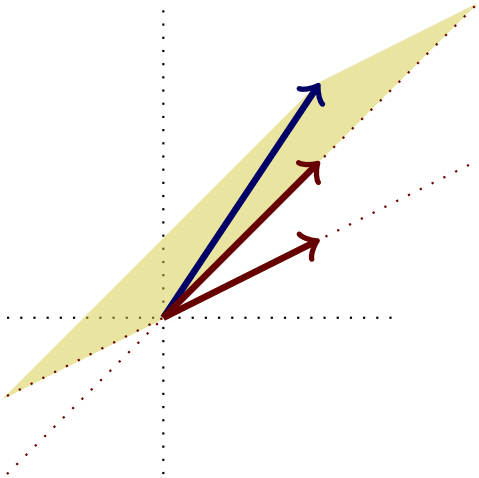
$$\mathbf{coord}_B(\vec{x}) = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

[a] Tj, souřadnice vektoru $\vec{x}$ chápeme jako další vektor: vektor souřadnic v $\mathbb{F}^n$.

Příklad (souřadnice stejného vektoru k různým bázím)

Seznamy $K_2 = (\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix})$, $B = (\begin{pmatrix}2\\1\end{pmatrix}, \begin{pmatrix}2\\2\end{pmatrix})$ jsou uspořádané báze prostoru $\mathbb{R}^2$. (Seznam K_2 je kanonická báze prostoru $\mathbb{R}^2$.)





$$\mathbf{coord}_{K_2}\begin{pmatrix}2\\3\end{pmatrix} = \begin{pmatrix}2\\3\end{pmatrix} \qquad \mathbf{coord}_{B}\begin{pmatrix}2\\3\end{pmatrix} = \begin{pmatrix}-1\\2\end{pmatrix}$$

$$\begin{pmatrix}2\\3\end{pmatrix} = 2\cdot\begin{pmatrix}1\\0\end{pmatrix} + 3\cdot\begin{pmatrix}0\\1\end{pmatrix} \qquad \begin{pmatrix}2\\3\end{pmatrix} = -1\cdot\begin{pmatrix}2\\1\end{pmatrix} + 2\cdot\begin{pmatrix}2\\2\end{pmatrix}$$

Důležitá vlastnost kanonické báze

Připomenutí: prostor $\mathbb{F}^n$ nad $\mathbb{F}$ má kanonickou bázi $K_n = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$, kde

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \quad \mathbf{e}_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Ať $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ je vektor v $\mathbb{F}^n$. Potom $\mathbf{coord}_{K_n}(\mathbf{x}) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.

Příklad (souřadnice stejného vektoru k různým bázím)

Seznamy

$$B_1 = (1, x, x^2) \qquad B_2 = (x^2, x, 1)$$

jsou uspořádané báze lineárního prostoru $\mathbb{R}^{\leq 2}[x]$ reálných polynomů stupně nejvýše 2.

Platí:

$$\mathbf{coord}_{B_1}(3x^2-2x+4) = \begin{pmatrix} 4 \\ -2 \\ 3 \end{pmatrix} \qquad \mathbf{coord}_{B_2}(3x^2-2x+4) = \begin{pmatrix} 3 \\ -2 \\ 4 \end{pmatrix}$$

$$3x^2-2x+4 = 4\cdot 1+(-2)\cdot x+3\cdot x^2, \quad 3x^2-2x+4 = 3\cdot x^2+(-2)\cdot x+4\cdot 1$$

Tvrzení (linearita výpočtu souřadnic)

Ať B je (jakákoli) konečná uspořádaná báze lineárního prostoru L. Potom pro zobrazení $\vec{x} \mapsto \mathbf{coord}_B(\vec{x})$ platí:[a]

1. $\mathbf{coord}_B(\vec{x} + \vec{y}) = \mathbf{coord}_B(\vec{x}) + \mathbf{coord}_B(\vec{y})$.
2. $\mathbf{coord}_B(a \cdot \vec{x}) = a \cdot \mathbf{coord}_B(\vec{x})$.

[a] Tyto dvě vlastnosti jsou velmi důležité. Příště je budeme studovat abstraktně (vedou k pojmu lineárního zobrazení).

Důkaz.

Přednáška. ■

Důsledek: důležitá vlastnost každé uspořádané báze

Ať $B = (\vec{b}_1, \ldots, \vec{b}_n)$ je jakákoli uspořádaná báze prostoru L.
Potom platí:

$$\mathbf{coord}_B(\vec{b}_1) = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ \mathbf{coord}_B(\vec{b}_2) = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \ \mathbf{coord}_B(\vec{b}_n) = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Obecně platí:

$$\mathbf{coord}_B\left(\sum_{i=1}^{n} a_i \cdot \vec{b}_i\right) = \sum_{i=1}^{n} a_i \cdot \mathbf{coord}_B(\vec{b}_i) = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

Několik připomenutí

1. Zadat zobrazení (také: funkci) $f : X \to Y$ znamená: pro každé $x \in X$ zadat právě jedno $y \in Y$. Toto y značíme $f(x)$ (funkční hodnota v x).
   Píšeme[a] i $x \mapsto f(x)$, $f : x \mapsto f(x)$.
2. Pro zobrazení $f : X \to Y$, $g : Y \to Z$ značíme $g \cdot f : X \to Z$ složené zobrazení $x \mapsto g(f(x))$.

[a] Důležité je rozlišovat: šipka $f : X \to Y$ versus šipka s patkou $x \mapsto f(x)$.

Poznámky

- Slova *funkce* a *zobrazení* znamenají totéž.
- Skládání zobrazení značíme stejně jako násobení (tj. tečkou). Uvidíme později, že skládání zobrazení skutečně je jistý druh násobení.

Několik připomenutí (pokrač.)

3. Přesná definice zobrazení $f : A \to B$ zní:

   Zobrazení $f : A \to B$ je podmnožina $A \times B$ taková, že pro všechna $a \in A$ existuje právě jedno $b \in B$ tak, že $(a, b) \in f$.

   Potom lze dokázat:

   1. Pro libovolnou množinu B existuje právě jedno zobrazení $f : \emptyset \to B$.
   2. Pro libovolnou množinu A existuje právě jedno zobrazení $f : A \to \{b\}$.
   3. Je-li A neprázdná množina, pak neexistuje zobrazení $f : A \to \emptyset$.

Několik připomenutí (pokrač.)

4. Komutativní trojúhelník:

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "h"'] & & Y \arrow[dl, "g"] \\ & Z & \end{tikzcd}$$

znamená $h = g \cdot f$, tj. $h(x) = g(f(x))$ pro všechna $x \in X$.

5. Komutativní čtverec:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "g"'] & B \arrow[d, "h"] \\ X \arrow[r, "k"'] & Y \end{tikzcd}$$

znamená $h \cdot f = k \cdot g$, tj. $h(f(x)) = k(g(x))$ pro všechna $x \in A$.

Několik připomenutí (pokrač.)

6. „Slepování“ komutativních diagramů:[a]

jestliže
$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "a"'] & B \arrow[d, "b"] \\ X \arrow[r, "x"'] & Y \end{tikzcd}$$
a
$$\begin{tikzcd} B \arrow[r, "g"] \arrow[d, "b"'] & C \arrow[d, "c"] \\ Y \arrow[r, "y"'] & Z \end{tikzcd}$$
jsou komutativní,

pak je i
$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "a"'] \arrow[rr, bend left, "g\cdot f"] & B \arrow[r, "g"] \arrow[d, "b"] & C \arrow[d, "c"] \\ X \arrow[r, "x"'] \arrow[rr, bend right, "y\cdot x"'] & Y \arrow[r, "y"'] & Z \end{tikzcd}$$
komutativní.

[a] Důležité: projděte si podrobně Příklady 2.2.1–2.2.3 skript.

Několik připomenutí (pokrač.)

7. „Trhání“ komutativních diagramů:[a]

Jestliže je

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "a"'] \arrow[rr, bend left, "g\cdot f"] & B \arrow[r, "g"] \arrow[d, "b"] & C \arrow[d, "c"] \\ X \arrow[r, "x"'] \arrow[rr, bend right, "y\cdot x"'] & Y \arrow[r, "y"'] & Z \end{tikzcd}$$

komutativní,

pak ani

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "a"'] & B \arrow[d, "b"] \\ X \arrow[r, "x"'] & Y \end{tikzcd}$$

ani

$$\begin{tikzcd} B \arrow[r, "g"] \arrow[d, "b"'] & C \arrow[d, "c"] \\ Y \arrow[r, "y"'] & Z \end{tikzcd}$$

komutativní být nemusí.

[a] Důležité: projděte si podrobně Příklady 2.2.1–2.2.3 skript.

Několik připomenutí (pokrač.)

8. Zobrazení $f : X \to Y$ je prosté (také: injektivní nebo injekce), když z rovnosti $f(x_1) = f(x_2)$ plyne $x_1 = x_2$.
9. Zobrazení $f : X \to Y$ je na (také: surjektivní nebo surjekce), když pro každé $y \in Y$ existuje x tak, že $f(x) = y$.
10. Zobrazení $f : X \to Y$ je bijekce (také: vzájemně jednoznačné), když f je injekce a surjekce současně.

Známá fakta

1. Identita na X, tj. $\mathrm{id}_X : X \to X$, kde $\mathrm{id}_X : x \mapsto x$, je bijekce.
2. Platí $h \cdot (g \cdot f) = (h \cdot g) \cdot f$ a $\mathrm{id}_Y \cdot f = f = f \cdot \mathrm{id}_X$, kdykoli je skládání definováno.
3. Složení injekcí je injekce, složení surjekcí je surjekce, složení bijekcí je bijekce.
4. $f : X \to Y$ je bijekce právě tehdy, když existuje jednoznačně určené[a] $g : Y \to X$ tak, že $g \cdot f = \mathrm{id}_X$ a $f \cdot g = \mathrm{id}_Y$.

[a] Tomuto jednoznačně určenému zobrazení se říká inverse zobrazení f a značí se také f^{-1}.

Lineární zobrazení

Odpřednesenou látku naleznete v kapitolách 2.1, 2.2 a 4 skript *Abstraktní a konkrétní lineární algebra*.

Minulé přednášky

1. Báze lineárního prostoru a souřadnice vektoru vzhledem ke konečné uspořádané bázi.

Dnešní přednáška

1. Lineární zobrazení $\mathbf{f} : L_1 \longrightarrow L_2$ zobecňuje zobrazení $\vec{x} \mapsto \mathbf{coord}_B(\vec{x})$, dané konečnou uspořádanou bází B.
2. Zavedeme pojem matice lineárního zobrazení z $\mathbb{F}^s$ do $\mathbb{F}^r$ (vzhledem ke kanonickým bázím).

Velmi důležité připomenutí

Vektory z prostoru $\mathbb{F}^n$ píšeme jako sloupce.

Definice (lineární zobrazení)

Ať L_1, L_2 jsou lineární prostory nad $\mathbb{F}$. Zobrazení $\mathbf{f} : L_1 \longrightarrow L_2$, pro které platí $\mathbf{f}(\vec{x} + \vec{x}') = \mathbf{f}(\vec{x}) + \mathbf{f}(\vec{x}')$ a $\mathbf{f}(a \cdot \vec{x}) = a \cdot \mathbf{f}(\vec{x})$ pro vš. a z $\mathbb{F}$, pro vš. $\vec{x}$, $\vec{x}'$ z L_1, říkáme lineární zobrazení z L_1 do L_2.

Příklady

1. Ať L má uspořádanou bázi B o n prvcích. Zobrazení $\mathbf{coord}_B : L \longrightarrow \mathbb{F}^n$ je lineární (minulá přednáška).
2. Řada dalších...

Poznámka (princip superposice)

$\mathbf{f} : L_1 \longrightarrow L_2$ je lineární právě tehdy, když platí rovnost

$$\mathbf{f}(\sum_{i=1}^{n} a_i \cdot \vec{x}_i) = \sum_{i=1}^{n} a_i \cdot \mathbf{f}(\vec{x}_i)$$

pro vš. a_i z $\mathbb{F}$ a vš. $\vec{x}_i$ z L_1.

Tvrzení (základní algebraické vlastnosti lineárních zobrazení)

1. Složení lineárních zobrazení je lineární. Identita je lineární zobrazení.
2. Jsou-li $\mathbf{f} : L_1 \longrightarrow L_2$ a $\mathbf{g} : L_1 \longrightarrow L_2$ lineární zobrazení, pak i zobrazení
   1. $\mathbf{f} + \mathbf{g}$ je lineární, kde $(\mathbf{f} + \mathbf{g})(\vec{x}) = \mathbf{f}(\vec{x}) + \mathbf{g}(\vec{x})$.
   2. $a \cdot \mathbf{f}$ je lineární (a je skalár z $\mathbb{F}$), kde $(a \cdot \mathbf{f})(\vec{x}) = a \cdot \mathbf{f}(\vec{x})$.

Důkaz.

Přednáška. ■

Důsledek (lineární prostor lineárních zobrazení)

Pro pevné lineární prostory L_1 a L_2 nad $\mathbb{F}$ je množina všech lineárních zobrazení z L_1 do L_2 lineární prostor nad $\mathbb{F}$. Tento prostor značíme $\mathrm{Lin}(L_1, L_2)$.

Věta (lineární zobrazení je určeno hodnotami na bázi)

Ať B je báze[a] lineárního prostoru L_1, ať L_2 je libovolný lineární prostor. Pak zadat

1. libovolné zobrazení $h : B \longrightarrow L_2$,

je totéž jako zadat

2. lineární zobrazení $\mathbf{f} : L_1 \longrightarrow L_2$.

[a] Připomenutí (téma 3A): každý lineární prostor má bázi.

Důkaz.

Pro prostory konečné dimense: princip superposice.

Pro obecné prostory: mírně složitější. ■

Příklad (popis libovolného lineárního zobrazení $\mathbf{f} : \mathbb{F}^s \longrightarrow \mathbb{F}^r$)

Připomenutí: $K_s = (\mathbf{e}_1, \dots, \mathbf{e}_s)$ je kanonická báze prostoru $\mathbb{F}^s$.
Zadat lineární zobrazení $\mathbf{f} : \mathbb{F}^s \longrightarrow \mathbb{F}^r$ znamená zadat seznam s (ne nutně různých) hodnot

$$\mathbf{f}(\mathbf{e}_1) = \mathbf{a}_1 = \begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \\ \vdots \\ a_{r1} \end{pmatrix}, \mathbf{f}(\mathbf{e}_2) = \mathbf{a}_2 = \begin{pmatrix} a_{12} \\ a_{22} \\ a_{32} \\ \vdots \\ a_{r2} \end{pmatrix}, \dots, \mathbf{f}(\mathbf{e}_s) = \mathbf{a}_s = \begin{pmatrix} a_{1s} \\ a_{2s} \\ a_{3s} \\ \vdots \\ a_{rs} \end{pmatrix}$$

v lineárním prostoru $\mathbb{F}^r$.
Tomuto seznamu říkáme matice (o r řádcích a s sloupcích).

Definice (matice)

Matice $\mathbf{A}$ nad $\mathbb{F}$ o r řádcích a s sloupcích je tabulka[a]

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1s} \\ a_{21} & a_{22} & \dots & a_{2s} \\ \vdots & & & \\ a_{r1} & a_{r2} & \dots & a_{rs} \end{pmatrix}$$

[a] Budeme také používat položkový zápis $\mathbf{A} = (a_{ij})_{i=1,\dots,r,j=1,\dots,s}$ nebo sloupcový zápis $\mathbf{A} = (\mathbf{a}_1, \dots, \mathbf{a}_s)$.
Nebudeme používat: matice typu $r \times s$, rozměrů $r \times s$, atd., případně ještě horší značení $n \times m$. (Nebo $m \times n$?)

Poznámka

Matici $\mathbf{A} = (\mathbf{a}_1, \dots, \mathbf{a}_s)$ o r řádcích a s sloupcích budeme ztotožňovat s lineárním zobrazením

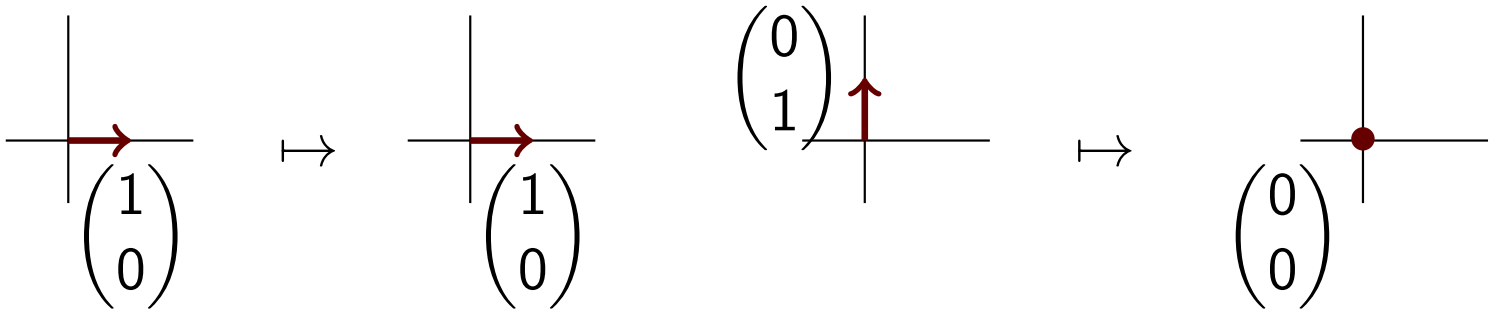
$$\mathbf{A} : \mathbf{e}_j \mapsto \mathbf{a}_j, \quad j = 1, \dots, s$$

z prostoru $\mathbb{F}^s$ do prostoru $\mathbb{F}^r$, a budeme psát $\mathbf{A} : \mathbb{F}^s \longrightarrow \mathbb{F}^r$.

Příklad (matice základních lineárních transformací v $\mathbb{R}^2$)

Kanonická báze $K_2 = (\mathbf{e}_1, \mathbf{e}_2)$ v $\mathbb{R}^2$. Matice některých lineárních zobrazení z $\mathbb{R}^2$ do $\mathbb{R}^2$ (vzhledem ke K_2) jsou:

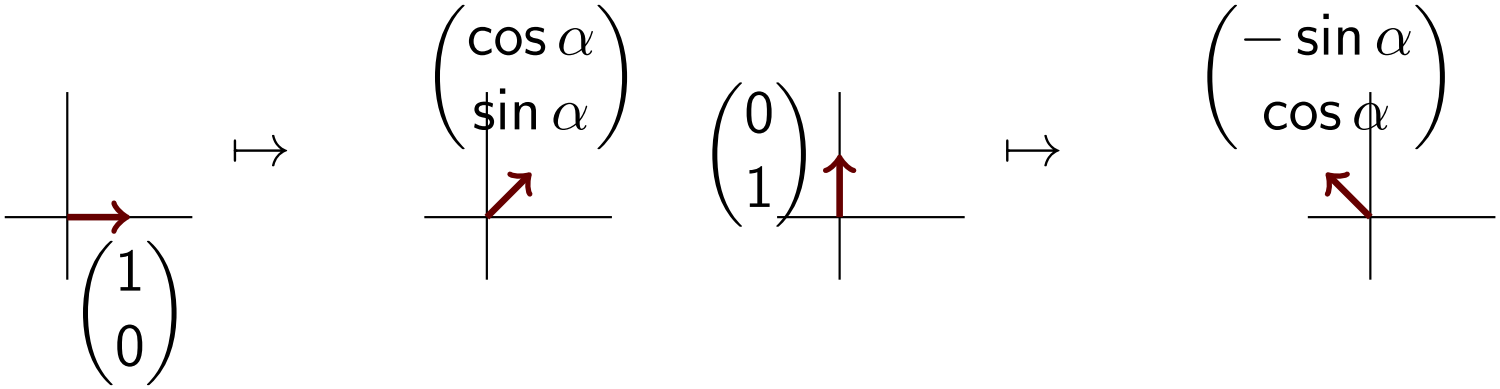
1. Projekce na osu x je ztotožněna s maticí $\mathbf{P}_x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.



Analogicky: projekce na osu y je ztotožněna s maticí $\mathbf{P}_y = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

Příklad (matice základních lineárních transformací v $\mathbb{R}^2$, pokrač.)

2. Rotace (o úhel α) je ztotožněna s maticí
$$\mathbf{R}_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}.$$



3. Změna měřítka ($a \neq 0$ a $b \neq 0$) je ztotožněna s maticí $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. Pro $a = 1$, $b = -1$ dostaneme reflexi: $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Příklad (matice základních lineárních transformací v $\mathbb{R}^2$, pokrač.)

4. Zkosení[a] (také: shear) je ztotožněno s maticí

$$\mathbf{S}_{a,b} = \begin{pmatrix} 1 & b \\ a & 1 \end{pmatrix}$$

kde $a, b \in \mathbb{R}$.

[a] Speciální typy zkosení (nad obecným tělesem) budou hrát důležitou roli při řešení soustav rovnic.

Co už nyní víme?

Například diagram

$$\mathbb{R}^2 \xrightarrow{\mathbf{R}_\alpha} \mathbb{R}^2 \xrightarrow{\mathbf{P}_x} \mathbb{R}^2$$

znamená následující: nejprve otočte o úhel α, potom proveďte projekci na osu x.

Značit se to musí $\mathbf{P}_x \cdot \mathbf{R}_\alpha$ (jde o skládání lineárních zobrazení). Co ale „násobení tabulek“ znamená? Odpověď: jde o novou matici.

Jak novou matici najít?

$$\mathbf{e}_j \mapsto j\text{-tý sloupec matice } \mathbf{R}_\alpha \mapsto ???$$

1. Násobení (skládání) matic: příští přednáška (téma 4B).
2. Zbytek dnešní přednášky: jak obecná matice $\mathbf{A} : \mathbb{F}^s \longrightarrow \mathbb{F}^r$ „zachází“ s obecným vektorem z prostoru $\mathbb{F}^s$?

Tvrzení (výpočet hodnoty matice A v obecném vektoru x)

Pro matici $\mathbf{A} : \mathbb{F}^s \longrightarrow \mathbb{F}^r$ se sloupcovým zápisem $(\mathbf{a}_1, \ldots, \mathbf{a}_s)$ a pro vektor $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_s \end{pmatrix}$ platí

$$\mathbf{A} : \mathbf{x} \mapsto \sum_{j=1}^{s} x_j \cdot \mathbf{a}_j$$

Důkaz.

Protože $\mathbf{A} : \mathbf{e}_j \mapsto \mathbf{a}_j$, tak $\mathbf{A} : \sum_{j=1}^{s} x_j \cdot \mathbf{e}_j \mapsto \sum_{j=1}^{s} x_j \cdot \mathbf{a}_j$. ■

Značení (násobení matice vektorem)

Vektor $\sum_{j=1}^{s} x_j \cdot \mathbf{a}_j$ značíme $\mathbf{A} \cdot \mathbf{x}$.

Příklad (rotace vektoru v $\mathbb{R}^2$)

Rotace (o úhel α): $\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$. Potom součin

$$\begin{aligned} \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} &= x_1 \cdot \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} + x_2 \cdot \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix} \\ &= \begin{pmatrix} x_1 \cos\alpha - x_2 \sin\alpha \\ x_1 \sin\alpha + x_2 \cos\alpha \end{pmatrix} \end{aligned}$$

dává výsledek otočení vektoru $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ o úhel α.

Například pro $\alpha = \frac{\pi}{4}$:

$$\begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \frac{\sqrt{2}}{2} - x_2 \frac{\sqrt{2}}{2} \\ x_1 \frac{\sqrt{2}}{2} + x_2 \frac{\sqrt{2}}{2} \end{pmatrix} = \frac{\sqrt{2}}{2} \cdot \begin{pmatrix} x_1 - x_2 \\ x_1 + x_2 \end{pmatrix}$$

Poznámka (další význam zápisu $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$)

Zápis $\mathbf{A} \cdot \mathbf{x}$ pro $\mathbf{x}$ v $\mathbb{F}^s$, kóduje hodnotu lineárního zobrazení $\mathbf{A} : \mathbb{F}^s \longrightarrow \mathbb{F}^r$ v bodě $\mathbf{x}$.

Zvolme pevné $\mathbf{b}$ v $\mathbb{F}^r$. Hledejme všechna $\mathbf{x}$ v $\mathbb{F}^s$ taková, že $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$. Na tento problém se lze dívat dvěma způsoby:

1. Hledáme vzor bodu $\mathbf{b}$ při lineárním zobrazení $\mathbf{A} : \mathbb{F}^s \longrightarrow \mathbb{F}^r$.
2. Řešíme soustavu lineárních rovnic.
   Počet sloupců matice $\mathbf{A}$ je počet neznámých, počet řádků matice $\mathbf{A}$ je počet rovnic v soustavě.

Příklad

$$\begin{pmatrix} 1 & 0 & -3 & 4 \\ 2 & 7 & 6 & 3 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 24 \\ 8 \end{pmatrix} \quad \text{je} \quad \begin{aligned} x_1 \qquad\quad - 3x_3 + 4x_4 &= 24 \\ 2x_1 + 7x_2 + 6x_3 + 3x_4 &= \ \ 8 \end{aligned}$$

Algebra matic

Odpřednesenou látku naleznete v kapitolách 2.1, 2.2 a 4 skript *Abstraktní a konkrétní lineární algebra*.

Minulá přednáška

1. Pojem lineárního zobrazení z $\mathbb{F}^s$ do $\mathbb{F}^r$ a jeho maticový zápis (vzhledem ke kanonickým bázím).

Dnešní přednáška

1. Zavedeme základní algebraické operace s maticemi.
2. V příští přednášce vše zobecníme pro prostory konečných dimensí; zavedeme pojem matice lineárního zobrazení (vzhledem k pevně zvoleným bázím).

Velmi důležité připomenutí

Vektory z prostoru $\mathbb{F}^n$ píšeme jako sloupce.

Již víme: $\mathrm{Lin}(\mathbb{F}^s, \mathbb{F}^r)$ je lineární prostor nad $\mathbb{F}$.

Jak se operace v $\mathrm{Lin}(\mathbb{F}^s, \mathbb{F}^r)$ projeví na „manipulaci s tabulkami“? Použijeme sloupcový zápis matic.

Pro $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_s)$ a $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_s)$ a skalár a z $\mathbb{F}$ je:

1. $\mathbf{A} + \mathbf{B} : \mathbb{F}^s \longrightarrow \mathbb{F}^r$ matice se sloupcovým zápisem $(\mathbf{a}_1 + \mathbf{b}_1, \ldots, \mathbf{a}_s + \mathbf{b}_s)$. Zápis $\mathbf{A} + \mathbf{B}$ čteme součet matic $\mathbf{A}$ a $\mathbf{B}$.
2. $a \cdot \mathbf{A} : \mathbb{F}^s \longrightarrow \mathbb{F}^r$ je matice se sloupcovým zápisem $(a \cdot \mathbf{a}_1, \ldots, a \cdot \mathbf{a}_s)$. Zápis $a \cdot \mathbf{A}$ čteme součin skaláru a a matice $\mathbf{A}$.

Nulový vektor[a] v lineárním prostoru $\mathrm{Lin}(\mathbb{F}^s, \mathbb{F}^r)$ je matice $\mathbf{O}_{s,r} = \underbrace{(\mathbf{o}, \ldots, \mathbf{o})}_{s\text{-krát}}$, kde $\mathbf{o}$ je nulový vektor v $\mathbb{F}^r$.

[a] Říkáme také: nulová matice.

Příklad: výpočty v $\mathrm{Lin}(\mathbb{R}^3, \mathbb{R}^2)$

1. Příklad součtu:

$$\begin{pmatrix} 5 & 3 & 6 \\ -1 & 0 & 7 \end{pmatrix} + \begin{pmatrix} 2 & 5 & -2 \\ 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 7 & 8 & 4 \\ 0 & 4 & 10 \end{pmatrix}$$

2. Příklad skalárního násobku:

$$(-2) \cdot \begin{pmatrix} -3 & 1 & 2 \\ 2 & 6 & 4 \end{pmatrix} = \begin{pmatrix} 6 & -2 & -4 \\ -4 & -12 & -8 \end{pmatrix}$$

3. Nulový vektor v v $\mathrm{Lin}(\mathbb{R}^3, \mathbb{R}^2)$ je:

$$\mathbf{O}_{3,2} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Poznámky k součtu matic a ke skalárnímu násobku matic

Sčítání matic a skalární násobení skalárem jsou operace v lineárním prostoru $\mathrm{Lin}(\mathbb{F}^s, \mathbb{F}^r)$. Přirozená čísla s a r jsou pevná. Proto:

1. Sčítat můžeme pouze matice stejných rozměrů. Pro matice různých rozměrů není sčítání definováno.

   Sloupcový zápis součtu

   $$(\mathbf{a}_1, \ldots, \mathbf{a}_s) + (\mathbf{b}_1, \ldots, \mathbf{b}_s) = (\mathbf{a}_1 + \mathbf{b}_1, \ldots, \mathbf{a}_s + \mathbf{b}_s)$$

   dává okamžitě „položkový návod“: chcete-li sečíst dvě matice stejných rozměrů, sečtěte položky na odpovídajících posicích.

2. Sloupcový zápis skalárního násobku

   $$a \cdot (\mathbf{a}_1, \ldots, \mathbf{a}_s) = (a \cdot \mathbf{a}_1, \ldots, a \cdot \mathbf{a}_s)$$

   dává okamžitě „položkový návod“: chcete-li matici vynásobit skalárem, vynásobte tímto skalárem každou položku matice.

Vlastnosti součtu matic a skalárního násobku matic

Protože $\mathrm{Lin}(\mathbb{F}^s, \mathbb{F}^r)$ je lineární prostor nad $\mathbb{F}$, platí:

1. $\mathbf{A} + \mathbf{O}_{s,r} = \mathbf{O}_{s,r} + \mathbf{A} = \mathbf{A}$, pro vš. $\mathbf{A}$ z $\mathrm{Lin}(\mathbb{F}^s, \mathbb{F}^r)$.
2. $\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$, pro vš. $\mathbf{A}$, $\mathbf{B}$ z $\mathrm{Lin}(\mathbb{F}^s, \mathbb{F}^r)$.
3. $\mathbf{A} + (\mathbf{B} + \mathbf{C}) = (\mathbf{A} + \mathbf{B}) + \mathbf{C}$, pro vš. $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ z $\mathrm{Lin}(\mathbb{F}^s, \mathbb{F}^r)$.
4. Pro každé $\mathbf{A}$ z $\mathrm{Lin}(\mathbb{F}^s, \mathbb{F}^r)$ existuje právě jedno[a] $\mathbf{B}$ z $\mathrm{Lin}(\mathbb{F}^s, \mathbb{F}^r)$ tak, že $\mathbf{A} + \mathbf{B} = \mathbf{O}_{s,r}$.
5. $1 \cdot \mathbf{A} = \mathbf{A}$ pro vš. $\mathbf{A}$ z $\mathrm{Lin}(\mathbb{F}^s, \mathbb{F}^r)$.
6. $a \cdot (b \cdot \mathbf{A}) = (a \cdot b) \cdot \mathbf{A}$ pro vš. a, b z $\mathbb{F}$ a vš. $\mathbf{A}$ z $\mathrm{Lin}(\mathbb{F}^s, \mathbb{F}^r)$.
7. $a \cdot (\mathbf{A} + \mathbf{B}) = a \cdot \mathbf{A} + a \cdot \mathbf{B}$ pro vš. a z $\mathbb{F}$ a pro vš. $\mathbf{A}$, $\mathbf{B}$ z $\mathrm{Lin}(\mathbb{F}^s, \mathbb{F}^r)$.
8. $(a + b) \cdot \mathbf{A} = a \cdot \mathbf{A} + b \cdot \mathbf{A}$ pro vš. a, b z $\mathbb{F}$ a pro vš. $\mathbf{A}$ z $\mathrm{Lin}(\mathbb{F}^s, \mathbb{F}^r)$.

---

[a] Tomuto jednoznačně určenému $\mathbf{B}$ říkáme opačná matice k matici $\mathbf{A}$ a značíme ji $-\mathbf{A}$.

Připomenutí značení (téma 4A)

Matice $\mathbf{A}$ se sloupcovým zápisem $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_s)$ je lineární zobrazení z $\mathbb{F}^s$ do $\mathbb{F}^r$, dané předpisem

$$\mathbf{e}_j \mapsto \mathbf{a}_j, \quad j = 1, \ldots, s$$

Princip superposice dává

$$\sum_{j=1}^{s} x_j \cdot \mathbf{e}_j \mapsto \sum_{j=1}^{s} x_j \cdot \mathbf{a}_j$$

Pro $\mathbf{x} = \sum_{j=1}^{s} x_j \cdot \mathbf{e}_j$ značíme $\sum_{j=1}^{s} x_j \cdot \mathbf{a}_j$ jako $\mathbf{A} \cdot \mathbf{x}$.

Proto

$$\mathbf{A} : \mathbf{x} \mapsto \mathbf{A} \cdot \mathbf{x}$$

Definice (součin matic)

Pro situaci[a]

$$\begin{array}{ccccc} \mathbb{F}^s & \xrightarrow{\mathbf{A}} & \mathbb{F}^p & \xrightarrow{\mathbf{B}} & \mathbb{F}^r \\ \mathbf{e}_j & \longmapsto & \mathbf{a}_j & \longmapsto & \mathbf{B}\cdot\mathbf{a}_j \end{array}$$

je $\mathbf{B}\cdot\mathbf{A}$ matice,[b] jejíž j-tý sloupec je $\mathbf{B}\cdot\mathbf{a}_j$, kde $\mathbf{a}_j$ je j-tý sloupec matice $\mathbf{A}$. Ve sloupcovém zápisu tedy platí
$\mathbf{B}\cdot\mathbf{A} = (\mathbf{B}\cdot\mathbf{a}_1, \dots, \mathbf{B}\cdot\mathbf{a}_s)$.

Matici $\mathbf{B}\cdot\mathbf{A}$ říkáme součin matic $\mathbf{B}$ a $\mathbf{A}$.

---

[a] Diagram okamžitě dává rozměrovou zkoušku pro součin matic $\mathbf{B}\cdot\mathbf{A}$: počet řádků matice $\mathbf{A}$ musí být roven počtu sloupců matice $\mathbf{B}$. Jindy součin matic nedefinujeme, protože by skládání nedávalo smysl.

[b] Položkový zápis součinu $\mathbf{B}\cdot\mathbf{A}$: pro $\mathbf{A} = (a_{kj})_{k=1,\dots,p,j=1,\dots,s}$ a $\mathbf{B} = (b_{ik})_{i=1,\dots,r,k=1,\dots,p}$ je $\mathbf{B}\cdot\mathbf{A}$ matice s položkami $(c_{ij})_{i=1,\dots,r,j=1,\dots,s}$, kde

$$c_{ij} = \sum_{k=1}^{p} b_{ik}\cdot a_{kj}$$

Příklad (matice složených lineárních transformací v $\mathbb{R}^2$)

Projekce na osu x: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, rotace (o úhel α): $\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$.

Součin matic

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ 0 & 0 \end{pmatrix}$$

je matice lineárního zobrazení „nejprve otočte o úhel α, potom spočtěte projekci na osu x“.

Součin matic

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \cos\alpha & 0 \\ \sin\alpha & 0 \end{pmatrix}$$

je matice lineárního zobrazení „nejprve spočtěte projekci na osu x, potom otočte o úhel α“.

Příklad (reflexe podle osy, která svírá úhel α s osou x)

Jde o složené zobrazení: nejdříve rotace o úhel $-\alpha$, potom reflexe, nakonec rotace o úhel α.

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix} =$$

$$\begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}$$

Poznámka

Analogicky lze vytvořit matice základních lineárních transformací v $\mathbb{R}^n$, $n \geq 3$. Aplikace: matematická analýza, fyzika, grafika.[a]

[a] Důležité: projděte si podrobně Příklady 4.1.6 a 4.2.9 skript.

Vlastnosti operací s maticemi

1. Pro součin platí asociativní zákon $\mathbf{C} \cdot (\mathbf{B} \cdot \mathbf{A}) = (\mathbf{C} \cdot \mathbf{B}) \cdot \mathbf{A}$, kdykoli jsou jednotlivé součiny definovány.
2. Obecně neplatí komutativní zákon $\mathbf{B} \cdot \mathbf{A} = \mathbf{A} \cdot \mathbf{B}$ (i když jsou oba součiny definovány).
3. Pro každé n definujeme jednotkovou matici[a] $\mathbf{E}_n : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ takto: $\mathbf{E}_n = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$, kde $\mathbf{e}_1, \ldots, \mathbf{e}_n$ jsou vektory kanonické báze $\mathbb{F}^n$.

   Potom pro každou matici $\mathbf{A} : \mathbb{F}^s \longrightarrow \mathbb{F}^r$ platí: $\mathbf{E}_r \cdot \mathbf{A} = \mathbf{A} = \mathbf{A} \cdot \mathbf{E}_s$.

[a] Matice $\mathbf{E}_n$ je maticí identického lineárního zobrazení $\mathbf{id} : \mathbb{F}^n \longrightarrow \mathbb{F}^n$.

Důkaz.

Okamžitě z vlastností lineárních zobrazení. ■

Příklad (popis obrazu projekce na osu x v $\mathbb{R}^2$)

Ať $\mathbf{P}_x : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ je projekce na osu x, ztotožněná s maticí $\mathbf{P}_x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Zajímá nás, zda vektor $\mathbf{b} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ je projekcí nějakého vektoru $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$. To lze zjistit algebrou matic:

$$\mathbf{P}_x \cdot \mathbf{x} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ 0 \end{pmatrix} \neq \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \mathbf{b}$$

Žádný vektor $\mathbf{x}$, jehož projekce na osu x je vektor $\mathbf{b}$, neexistuje.

To ale znamená: soustava rovnic $\mathbf{P}_x \cdot \mathbf{x} = \mathbf{b}$ nemá řešení!

Příklad (popis vzoru projekce na osu x v $\mathbb{R}^2$)

Ať $\mathbf{P}_x : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ je projekce na osu x, ztotožněná s maticí $\mathbf{P}_x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Pro vektor $\mathbf{b} = \begin{pmatrix} 3 \\ 0 \end{pmatrix}$ nás zajímají všechny vektory $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, které se na $\mathbf{b}$ projekcí zobrazí. To lze zjistit algebrou matic:

$$\mathbf{P}_x \cdot \mathbf{x} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \end{pmatrix} = \mathbf{b}$$

Řešením soustavy rovnic $\mathbf{P}_x \cdot \mathbf{x} = \mathbf{b}$ je množina všech vektorů $\mathbf{x}$ tvaru $\begin{pmatrix} 3 \\ x_2 \end{pmatrix}$, kde x_2 je libovolné reálné číslo.[a]

[a] Řešení lze napsat i ve tvaru $\begin{pmatrix} 3 \\ 0 \end{pmatrix} + \mathrm{span}(\begin{pmatrix} 0 \\ 1 \end{pmatrix})$. Jak uvidíme, tento druhý způsob zápisu řešení bude mít mnohé výhody.

Příklad (projekce na osu x v $\mathbb{R}^2$ není invertibilní)

Ať $\mathbf{P}_x : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ je projekce na osu x, ztotožněná s maticí $\mathbf{P}_x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Existují matice $\mathbf{A} : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ a $\mathbf{B} : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ takové, že

$$\begin{tikzcd} \mathbb{R}^2 \arrow[r, "\mathbf{A}"] \arrow[rr, bend right, "\mathbf{E}_2"'] & \mathbb{R}^2 \arrow[r, "\mathbf{P}_x"] & \mathbb{R}^2 \end{tikzcd} \quad \text{a} \quad \begin{tikzcd} \mathbb{R}^2 \arrow[r, "\mathbf{P}_x"] \arrow[rr, bend right, "\mathbf{E}_2"'] & \mathbb{R}^2 \arrow[r, "\mathbf{B}"] & \mathbb{R}^2 \end{tikzcd} \quad ?$$

Intuice: žádné takové matice neexistují, protože matice jsou lineární zobrazení.

Jak intuici dokázat? Algebrou matic!

Příklad (projekce na osu x v $\mathbb{R}^2$ není invertibilní, pokrač.)

Ptáme se, zda existují matice $\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ takové, že platí rovnosti

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{a} \quad \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Takové matice neexistují, protože

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} b_{11} & 0 \\ b_{21} & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Důsledek

Nenulovost čtvercové matice $\mathbf{A}$ typu $n \times n$ nezaručuje existenci matic $\mathbf{X}$ a $\mathbf{Y}$, které by řešily rovnice $\mathbf{A} \cdot \mathbf{X} = \mathbf{E}_n$ a $\mathbf{Y} \cdot \mathbf{A} = \mathbf{E}_n$.

Proč nás to zajímá?

Otázka řešitelnosti obecných maticových rovnic $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$ a $\mathbf{Y} \cdot \mathbf{A} = \mathbf{C}$ je důležitá. Proč?
Jde o zobecnění řešení soustav lineárních rovnic.

Lineární zobrazení, část 2

Odpřednesenou látku naleznete v kapitolách 2.3, 3.4 a 9.1 skript *Abstraktní a konkrétní lineární algebra*.

Minulá přednáška

1. Matice $\mathbf{A} = (\mathbf{a}_1, \dots, \mathbf{a}_s)$ (sloupcový zápis matice, každý sloupec $\mathbf{a}_j$ je vektor z $\mathbb{F}^r$) je ztotožněna s lineárním zobrazením $\mathbf{A} : \mathbb{F}^s \to \mathbb{F}^r$, $\mathbf{e}_j \mapsto \mathbf{a}_j$.

   Operace s maticemi odpovídají operacím s lineárními zobrazeními.

Dnešní přednáška

1. Pojmy jádro, obraz, defekt a hodnost lineárního zobrazení.

   Tyto pojmy umožní jemnější klasifikaci lineárních zobrazení.
2. Pojem matice obecného lineárního zobrazení $\mathbf{f} : L_1 \to L_2$ vzhledem k obecným uspořádaným bázím. Prostory L_1 a L_2 musí mít konečnou dimensi.

Připomenutí (témata 4A a 3B)

1. Ať L_1, L_2 jsou lineární prostory nad $\mathbb{F}$. Zobrazení $\mathbf{f} : L_1 \to L_2$, pro které platí $\mathbf{f}(\vec{x} + \vec{x}') = \mathbf{f}(\vec{x}) + \mathbf{f}(\vec{x}')$ a $\mathbf{f}(a \cdot \vec{x}) = a \cdot \mathbf{f}(\vec{x})$ pro vš. a z $\mathbb{F}$ a vš. $\vec{x}$, $\vec{x}'$ z L_1, říkáme lineární zobrazení z L_1 do L_2.
2. Zápis $\mathbf{A} : \mathbb{F}^s \to \mathbb{F}^r$ znamená[a] $\mathbf{A} : \mathbf{e}_j \mapsto j$-tý sloupec $\mathbf{A}$. Tudíž platí $\mathbf{x} \mapsto \mathbf{A} \cdot \mathbf{x}$, pro všechna $\mathbf{x}$ z $\mathbb{F}^s$.
3. Trojúhelník

$$\begin{tikzcd} \mathbb{F}^s \arrow[rr, "\mathbf{B}\cdot\mathbf{A}"] \arrow[dr, "\mathbf{A}"'] & & \mathbb{F}^r \\ & \mathbb{F}^p \arrow[ur, "\mathbf{B}"'] & \end{tikzcd}$$

   je komutativní.

[a] V terminologii dnešní přednášky: $\mathbf{A} : \mathbb{F}^s \to \mathbb{F}^r$ je maticí zobrazení $\mathbf{A} : \mathbf{e}_j \mapsto j$-tý sloupec $\mathbf{A}$ vzhledem ke kanonické bázi. Ale nepředbíhejme 😜

Definice (speciální vlastnosti lineárních zobrazení)

Lineárnímu zobrazení $\mathbf{f} : L_1 \to L_2$ říkáme:

1. monomorfismus, je-li $\mathbf{f}$ injektivní (také: prosté) zobrazení.
2. epimorfismus, je-li $\mathbf{f}$ surjektivní (také: na) zobrazení.
3. isomorfismus, je-li $\mathbf{f}$ bijektivní (také: prosté a na) zobrazení.[a]

[a] Ekvivalentně: k zobrazení $\mathbf{f}$ existuje inversní zobrazení $\mathbf{f}^{-1}$ a toto inversní zobrazení je opět lineární.

Tvrzení

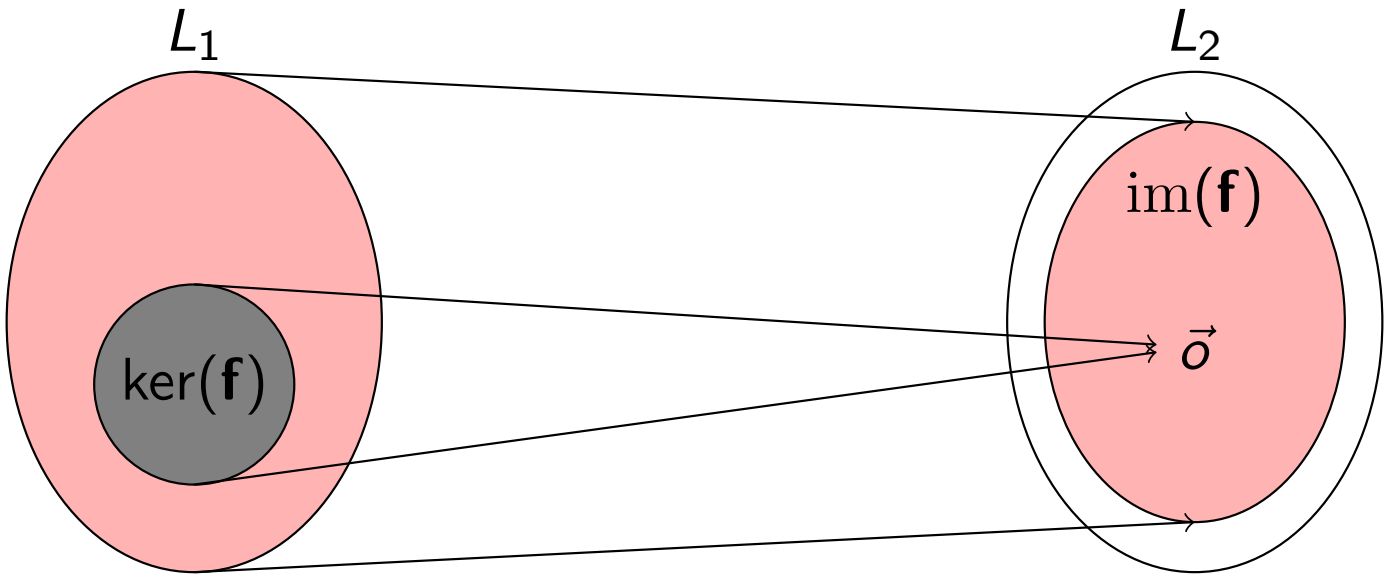
Složení monomorfismů/epimorfismů/isomorfismů je monomorfismus/epimorfismus/isomorfismus. Identita je isomorfismus.

Důkaz.

Přednáška.

Definice (obraz a jádro)

Ať $\mathbf{f} : L_1 \to L_2$ je lineární zobrazení. Množině $\ker(\mathbf{f}) = \{\vec{x} \mid \mathbf{f}(\vec{x}) = \vec{o}\}$ říkáme jádro $\mathbf{f}$, množině $\mathrm{im}(\mathbf{f}) = \{\mathbf{f}(\vec{x}) \mid \vec{x} \text{ z } L_1\}$ říkáme obraz $\mathbf{f}$.



Slogany (tj. reklamní hesla, nikoli skutečnost)

Jádro $\mathbf{f}$ říká, jak moc je $\mathbf{f}$ monomorfismus.
Obraz $\mathbf{f}$ říká, jak moc je $\mathbf{f}$ epimorfismus.

Tvrzení

Ať $\mathbf{f} : L_1 \to L_2$ je lineární zobrazení. Pak $\ker(\mathbf{f})$ je podprostor L_1, $\mathrm{im}(\mathbf{f})$ je podprostor L_2.[a]

[a] Obecněji: $\{\mathbf{f}(\vec{w}) \mid \vec{w} \in W\}$ je podprostor L_2, pro jakýkoli podprostor W prostoru L_1.

Důkaz.

Přednáška. ∎

Definice (defekt a hodnost lineárního zobrazení)

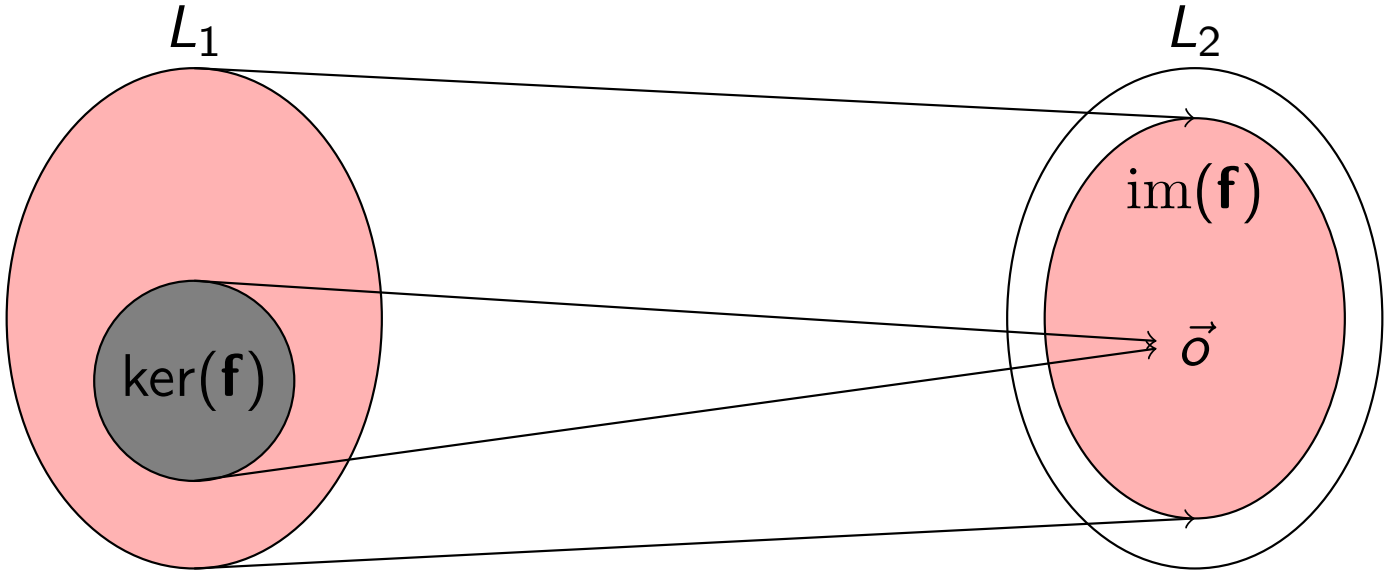
Ať $\mathbf{f} : L_1 \to L_2$ je lineární zobrazení, ať prostor L_1 má konečnou dimensi. Číslu $\mathrm{def}(\mathbf{f}) = \dim(\ker(\mathbf{f}))$ říkáme defekt lineárního zobrazení $\mathbf{f}$ a číslu $\mathrm{rank}(\mathbf{f}) = \dim(\mathrm{im}(\mathbf{f}))$ říkáme hodnost (také: rank) lineárního zobrazení $\mathbf{f}$.

Tvrzení (Věta o dimensi jádra a obrazu)

Ať $\mathbf{f} : L_1 \to L_2$ je lineární zobrazení, ať prostor L_1 má konečnou dimensi. Pak $\mathrm{def}(\mathbf{f}) + \mathrm{rank}(\mathbf{f}) = \dim(L_1)$.

Důkaz.

Bez důkazu (důkaz je například ve skriptech, Věta 3.3.6).



$\mathrm{def}(\mathbf{f}) = \dim(\ker(\mathbf{f}))$ $\qquad$ $\mathrm{rank}(\mathbf{f}) = \dim(\mathrm{im}(\mathbf{f}))$ ■

Tvrzení (charakterisace monomorfismů)

Ať $\mathbf{f} : L_1 \to L_2$ je lineární zobrazení, ať prostor L_1 má konečnou dimensi. Pak je ekvivalentní:

1. $\mathbf{f}$ je monomorfismus.
2. $\mathrm{def}(\mathbf{f}) = 0$.
3. $\mathbf{f}$ respektuje lineární nezávislost (tj. obraz lineárně nezávislé množiny je opět lineárně nezávislá množina).

Důkaz.

Přednáška. ■

Důsledek (monomorfismy a soustavy rovnic)

$\mathbf{A} : \mathbb{F}^s \to \mathbb{F}^r$ je monomorfismus právě tehdy, když soustava $\mathbf{A} \cdot \mathbf{x} = \mathbf{o}$ má pouze triviální řešení.

Tvrzení (charakterisace isomorfismů)

Ať $\mathbf{f} : L_1 \to L_2$ je lineární zobrazení, ať prostor L_1 má konečnou dimensi. Pak je ekvivalentní:

1. $\mathbf{f}$ je isomorfismus.
2. $\mathbf{f}$ je monomorfismus a epimorfismus současně.
3. $\mathrm{def}(\mathbf{f}) = 0$ a $\mathrm{im}(\mathbf{f}) = L_2$ současně.
4. $\mathrm{def}(\mathbf{f}) = 0$ a $\dim(L_1) = \dim(L_2)$.
5. $\mathbf{f}$ respektuje lineární nezávislost (tj. obraz lineárně nezávislé množiny je opět lineárně nezávislá množina) a každá rovnice $\mathbf{f}(\vec{x}) = \vec{b}$ má alespoň jedno řešení.

Důkaz.

Přednáška. ■

Důsledek (isomorfismy a soustavy rovnic)

$\mathbf{A} : \mathbb{F}^s \to \mathbb{F}^r$ je isomorfismus právě tehdy, když $s = r$ a každá soustava $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$ má právě jedno řešení.

Definice (regulární a singulární matice)

Matice $\mathbf{A} : \mathbb{F}^n \to \mathbb{F}^n$ typu je regulární (také: invertibilní, také: isomorfismus), pokud existuje jednoznačně určená matice $\mathbf{A}^{-1}$ taková, že platí rovnosti $\mathbf{A}^{-1} \cdot \mathbf{A} = \mathbf{E}_n = \mathbf{A} \cdot \mathbf{A}^{-1}$. Matici $\mathbf{A}^{-1}$ říkáme inverse matice $\mathbf{A}$.
Matice $\mathbf{A} : \mathbb{F}^n \to \mathbb{F}^n$ je singulární, pokud není regulární.

Příklad (rotace o úhel α v $\mathbb{R}^2$ je isomorfismus)

$$\mathbf{R}_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

je regulární (invertibilní) matice.[a]

[a] Inversním zobrazením rotace o úhel α je rotace o úhel $-\alpha$.

Důsledek (isomorfismy prostorů konečné dimense)

Ať $\dim(L_1) = \dim(L_2) = n$. Potom je, pro lineární zobrazení $\mathbf{f} : L_1 \to L_2$, ekvivalentní:

1. $\mathbf{f}$ je monomorfismus.
2. $\mathbf{f}$ je epimorfismus.
3. $\mathbf{f}$ je isomorfismus.

Tvrzení (důležité)

Ať $B = (\vec{b}_1, \ldots, \vec{b}_n)$ je uspořádaná báze prostoru L. Potom výpočet souřadnic v bázi B

$$\mathbf{coord}_B : L \to \mathbb{F}^n, \quad \vec{x} \mapsto \mathbf{coord}_B(\vec{x})$$

je isomorfismus.

Důkaz.

Přednáška. ■

Poznámka (důležitá)

Protože isomorfní lineární prostory se z abstraktního hlediska nijak neliší, vidíme: až na isomorfismus neexistují jiné konečně dimensionální lineární prostory nad $\mathbb{F}$ než prostory tvaru $\mathbb{F}^n$.

Definice (matice lineárního zobrazení)

Ať $\mathbf{f} : L_1 \to L_2$ je lineární zobrazení, ať $B = (\vec{b}_1, \ldots, \vec{b}_s)$ a $C = (\vec{c}_1, \ldots, \vec{c}_r)$ jsou uspořádané báze prostorů L_1 a L_2. Matice zobrazení $\mathbf{f}$ (vzhledem k B a C) je taková matice $\mathbf{A_f}$, pro kterou platí

$$\begin{tikzcd}
\mathbb{F}^s \arrow[r, "\mathbf{x} \mapsto \mathbf{A_f} \cdot \mathbf{x}"] & \mathbb{F}^r \\
L_1 \arrow[u, "\mathbf{coord}_B"] \arrow[r, "\mathbf{f}"'] & L_2 \arrow[u, "\mathbf{coord}_C"']
\end{tikzcd}$$

neboli:

$$\begin{tikzcd}
\mathbf{coord}_B(\vec{x}) \arrow[r, mapsto] & \mathbf{A_f} \cdot \mathbf{coord}_B(\vec{x}) = \mathbf{coord}_C(\mathbf{f}(\vec{x})) \\
\vec{x} \arrow[u, mapsto] \arrow[r, mapsto] & \mathbf{f}(\vec{x}) \arrow[u, mapsto]
\end{tikzcd}$$

pro každý vektor $\vec{x}$.

Tvrzení (výpočet matice lineárního zobrazení)

Ať $\mathbf{f} : L_1 \to L_2$ je lineární zobrazení, ať $B = (\vec{b}_1, \dots, \vec{b}_s)$ a $C = (\vec{c}_1, \dots, \vec{c}_r)$ jsou uspořádané báze prostorů L_1 a L_2. Potom matice $\mathbf{A_f}$ má r řádků a s sloupců. Navíc j-tý sloupec matice $\mathbf{A_f}$ je tvořen souřadnicemi $\mathbf{coord}_C(\mathbf{f}(\vec{b}_j))$, zapsanými do sloupce.

Důkaz.

$$\begin{tikzcd}
\mathbf{e}_j \arrow[rrr, mapsto] & & & j\text{-tý sloupec } \mathbf{A_f} = \mathbf{coord}_C(\mathbf{f}(\vec{b}_j)) \\
& \mathbb{F}^s \arrow[r, "\mathbf{x} \mapsto \mathbf{A_f} \cdot \mathbf{x}"] & \mathbb{F}^r & \\
& L_1 \arrow[u, "\mathbf{coord}_B"] \arrow[r, "\mathbf{f}"'] & L_2 \arrow[u, "\mathbf{coord}_C"'] & \\
\vec{b}_j \arrow[uuu, mapsto] \arrow[rrr, mapsto] & & & \mathbf{f}(\vec{b}_j) \arrow[uuu, mapsto]
\end{tikzcd}$$

Věta (matice složeného zobrazení)

Ať L_1, L_2, L_3 mají uspořádané báze $B = (\vec{b}_1, \ldots, \vec{b}_s)$, $C = (\vec{c}_1, \ldots, \vec{c}_p)$ a $D = (\vec{d}_1, \ldots, \vec{d}_r)$. Ať $\mathbf{f} : L_1 \to L_2$ a $\mathbf{g} : L_2 \to L_3$ jsou lineární zobrazení s maticemi $\mathbf{A_f}$ (vzhledem k B a C) a $\mathbf{A_g}$ (vzhledem k C a D). Potom $\mathbf{g} \cdot \mathbf{f} : L_1 \to L_3$ má matici $\mathbf{A_g} \cdot \mathbf{A_f}$ (vzhledem k B a D).

Důkaz.

$$\begin{tikzcd}
\mathbb{F}^s \arrow[r, "\mathbf{x} \mapsto \mathbf{A_f} \cdot \mathbf{x}"] \arrow[rr, bend left, "\mathbf{x} \mapsto \mathbf{A_g} \cdot \mathbf{A_f} \cdot \mathbf{x}"] & \mathbb{F}^p \arrow[r, "\mathbf{x} \mapsto \mathbf{A_g} \cdot \mathbf{x}"] & \mathbb{F}^r \\
L_1 \arrow[u, "\mathbf{coord}_B"] \arrow[r, "\mathbf{f}"'] \arrow[rr, bend right, "\mathbf{g} \cdot \mathbf{f}"'] & L_2 \arrow[u, "\mathbf{coord}_C"'] \arrow[r, "\mathbf{g}"'] & L_3 \arrow[u, "\mathbf{coord}_D"']
\end{tikzcd}$$

Věta (matice isomorfismu)

Ať L_1, L_2 mají uspořádané báze $B = (\vec{b}_1, \dots, \vec{b}_n)$, $C = (\vec{c}_1, \dots, \vec{c}_n)$. Ať lineární zobrazení $\mathbf{f} : L_1 \to L_2$ je isomorfismus s maticí zobrazení $\mathbf{A_f}$ (vzhledem k B a C). Potom existuje jednoznačně určená matice $\mathbf{A_f}^{-1}$ splňující rovnosti $\mathbf{A_f}^{-1} \cdot \mathbf{A_f} = \mathbf{E}_n = \mathbf{A_f} \cdot \mathbf{A_f}^{-1}$. Matice $\mathbf{A_f}^{-1}$ je matice $\mathbf{A}_{\mathbf{f}^{-1}}$ inversního zobrazení $\mathbf{f}^{-1}$ (vzhledem k C a B).[a]

[a] Tj. regulární (invertibilní) matice jsou přesně matice isomorfismů.

Důkaz.

$$\begin{tikzcd}
\mathbb{F}^n \arrow[r, "\mathbf{x} \mapsto \mathbf{A_f} \cdot \mathbf{x}"] \arrow[rr, bend left, "\mathbf{x} \mapsto \mathbf{x}"] & \mathbb{F}^n \arrow[r, "\mathbf{x} \mapsto (\mathbf{A}_{\mathbf{f}^{-1}}) \cdot \mathbf{x}"] & \mathbb{F}^n \\
L_1 \arrow[u, "\mathbf{coord}_B"] \arrow[r, "\mathbf{f}"'] \arrow[rr, bend right, "\mathbf{id}"'] & L_2 \arrow[u, "\mathbf{coord}_C"'] \arrow[r, "\mathbf{f}^{-1}"'] & L_1 \arrow[u, "\mathbf{coord}_B"']
\end{tikzcd}$$

Proto $\mathbf{A_f}^{-1} \cdot \mathbf{A_f} = \mathbf{E}_n$. Druhá rovnost analogicky. ■

Příklad (výpočet matice pro derivování)

$\mathbb{F}^{\leq 3}[x]$ je prostor polynomů stupně ≤ 3 nad tělesem $\mathbb{F}$. Báze $B = (x^3, x^2, x^1, 1)$. Zobrazení

$$\begin{aligned} &\mathbf{der} : \mathbb{F}^{\leq 3}[x] \to \mathbb{F}^{\leq 3}[x], \\ &(a_3x^3 + a_2x^2 + a_1x + a_0) \mapsto (3a_3x^2 + 2a_2x + a_1) \end{aligned}$$

je lineární a má následující matici vzhledem k B:

$$\mathbf{A_{der}} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Matice pro druhou derivaci: spočítáme součin $\mathbf{A_{der}} \cdot \mathbf{A_{der}}$, atd.

Příklad (matice zobrazení vzhledem k nekanonické bázi)

Lineární zobrazení $\mathbf{f} : \mathbb{R}^2 \to \mathbb{R}^2$ je dáno hodnotami

$$\mathbf{f}(\begin{pmatrix} 1 \\ -1 \end{pmatrix}) = 2 \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad \text{a} \quad \mathbf{f}(\begin{pmatrix} 1 \\ 1 \end{pmatrix}) = \frac{1}{3} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Zobrazení $\mathbf{f}$ tedy:

1. „Prodlužuje“ $2\times$ měřítko v ose druhého a čtvrtého kvadrantu.
2. „Zkracuje“ $3\times$ měřítko v ose prvního a třetího kvadrantu.

Vzhledem k nekanonické bázi $B = (\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix})$ má tedy $\mathbf{f}$ matici

$$\mathbf{A_f} = \begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{3} \end{pmatrix}$$

Jak spočítat matici $\mathbf{B_f}$ zobrazení $\mathbf{f}$ vzhledem ke kanonické bázi K_2?

Příklad (pokrač.)

Myšlenka řešení: hledaná matice $\mathbf{B_f}$ musí splňovat rovnici $\mathbf{B_f} = \mathbf{S} \cdot \mathbf{A_f} \cdot \mathbf{T}$, kde

$$\begin{tikzcd}
\mathbb{R}^2 \arrow[r, "\mathbf{x} \mapsto \mathbf{T} \cdot \mathbf{x}"] \arrow[rrr, bend left, "\mathbf{x} \mapsto \mathbf{B_f} \cdot \mathbf{x}"] & \mathbb{R}^2 \arrow[r, "\mathbf{x} \mapsto \mathbf{A_f} \cdot \mathbf{x}"] & \mathbb{R}^2 \arrow[r, "\mathbf{x} \mapsto \mathbf{S} \cdot \mathbf{x}"] & \mathbb{R}^2 \\
L_1 \arrow[u, "\mathbf{coord}_{K_2}"] \arrow[r, "\mathbf{id}"'] \arrow[rrr, bend right, "\mathbf{f}"'] & L_1 \arrow[u, "\mathbf{coord}_B"] \arrow[r, "\mathbf{f}"'] & L_2 \arrow[u, "\mathbf{coord}_B"] \arrow[r, "\mathbf{id}"'] & L_2 \arrow[u, "\mathbf{coord}_{K_2}"']
\end{tikzcd}$$

Jak najít matice $\mathbf{S}$ a $\mathbf{T}$? Jednoduše: jsou to matice identického zobrazení, navíc evidentně platí $\mathbf{T} = \mathbf{S}^{-1}$.

Příklad (pokrač.)

Platí (díky tomu, co jsme již dokázali)

$$\mathbf{S} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \qquad \mathbf{T} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

a tedy

$$\mathbf{B_f} = \mathbf{S} \cdot \mathbf{A_f} \cdot \mathbf{T} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{7}{6} & -\frac{5}{6} \\ -\frac{5}{6} & \frac{7}{6} \end{pmatrix}$$

Příští přednáška (téma 5B)

Konceptuální hledání (analogií) matic $\mathbf{T}$ a $\mathbf{S}$: takzvané matice transformace souřadnic.

Transformace souřadnic

Odpřednesenou látku naleznete v kapitolách 9.2 a 9.3 skript *Abstraktní a konkrétní lineární algebra*.

Minulá přednáška

1. Lineární zobrazení.
2. Výpočet souřadnic vzhledem k bázi je lineární zobrazení.
3. Matice libovolného lineárního zobrazení mezi lineárními prostory konečné dimense vzhledem k pevně zvoleným bázím.

Dnešní přednáška

1. Matice transformace souřadnic v jedné bázi na souřadnice ve druhé bázi. Jde opět o matici jistého lineárního zobrazení.
2. Uvidíme, že pro stále více problémů je třeba se naučit řešit maticové soustavy.[a]

[a] Řadu příkladů tedy v této přednášce nedopočítáme až do konce.

Příští přednáška

1. Koncepčně čistý a geometricky jasný způsob řešení soustav lineárních rovnic, maticových rovnic, atd.

Připomenutí (výpočet matice lineárního zobrazení)

Ať $\mathbf{f} : L_1 \to L_2$ je lineární zobrazení, ať $B = (\vec{b}_1, \ldots, \vec{b}_s)$ a $C = (\vec{c}_1, \ldots, \vec{c}_r)$ jsou uspořádané báze prostorů L_1 a L_2. Potom matice $\mathbf{A_f}$ má r řádků a s sloupců a j-tý sloupec matice $\mathbf{A_f}$ je tvořen souřadnicemi $\mathbf{coord}_C(\mathbf{f}(\vec{b}_j))$, zapsanými do sloupce.

$$
\begin{tikzcd}
\mathbf{e}_j \arrow[rrr, mapsto] & & & j\text{-tý sloupec } \mathbf{A_f} = \mathbf{coord}_C(\mathbf{f}(\vec{b}_j)) \\
& \mathbb{F}^s \arrow[r, "\mathbf{x} \mapsto \mathbf{A_f} \cdot \mathbf{x}"] & \mathbb{F}^r & \\
& L_1 \arrow[u, "\mathbf{coord}_B"] \arrow[r, "\mathbf{f}"'] & L_2 \arrow[u, "\mathbf{coord}_C"'] & \\
\vec{b}_j \arrow[uuu, mapsto] \arrow[rrrr, mapsto] & & & \mathbf{f}(\vec{b}_j) \arrow[uuu, mapsto]
\end{tikzcd}
$$

Definice (matice transformace souřadnic)

Ať $B = (\vec{b}_1, \dots, \vec{b}_n)$ a $C = (\vec{c}_1, \dots, \vec{c}_n)$ jsou uspořádané báze prostoru L. Matici[a] $\mathbf{T}_{B \mapsto C}$, která splňuje

$$\begin{tikzcd}
\mathbf{e}_j \arrow[rrr, mapsto] & & & j\text{-tý sloupec } \mathbf{T}_{B\mapsto C} = \mathbf{coord}_C(\vec{b}_j) \\
& \mathbb{F}^n \arrow[r, "\mathbf{x}\mapsto\mathbf{T}_{B\mapsto C}\cdot\mathbf{x}"] & \mathbb{F}^n & \\
& L \arrow[u, "\mathbf{coord}_B"] \arrow[r, "\mathbf{id}"'] & L \arrow[u, "\mathbf{coord}_C"'] & \\
\vec{b}_j \arrow[uuu, mapsto] \arrow[rrrr, mapsto] & & & & \vec{b}_j \arrow[uuu, mapsto]
\end{tikzcd}$$

říkáme matice transformace souřadnic z báze B do báze C (také: matice transformace souřadnic v bázi B na souřadnice v bázi C).

[a] Všimněte si značení: v dolním indexu $\mathbf{T}_{B \mapsto C}$ je šipka s patkou (bázi B „posíláme“ na bázi C).

Poznámky (základní vlastnosti matice transformace souřadnic)

1. Platí $\mathbf{T}_{B\mapsto C}\cdot\mathbf{coord}_B(\vec{x}) = \mathbf{coord}_C(\vec{x})$, pro každý vektor $\vec{x}$ v L. To plyne přímo z definice matice $\mathbf{T}_{B\mapsto C}$:

$$\begin{tikzcd}
\mathbb{F}^n \arrow[r, "\mathbf{x}\mapsto\mathbf{T}_{B\mapsto C}\cdot\mathbf{x}"] & \mathbb{F}^n \\
L \arrow[u, "\mathbf{coord}_B"] \arrow[r, "\mathbf{id}"'] & L \arrow[u, "\mathbf{coord}_C"']
\end{tikzcd}$$

2. Matice $\mathbf{T}_{B\mapsto C}$ je vždy regulární. Platí $(\mathbf{T}_{B\mapsto C})^{-1} = \mathbf{T}_{C\mapsto B}$. To plyne z toho, že $\mathbf{id} : L \to L$ je isomorfismus.

Poznámky (základní vlastnosti matice transformace, pokrač.)

3. Platí $\mathbf{T}_{B\mapsto B} = \mathbf{E}_n$. To je triviální:

$$\begin{tikzcd}
\mathbb{F}^n \arrow[r, "\mathbf{x}\mapsto\mathbf{x}"] & \mathbb{F}^n \\
L \arrow[u, "\mathbf{coord}_B"] \arrow[r, "\mathbf{id}"'] & L \arrow[u, "\mathbf{coord}_B"']
\end{tikzcd}$$

4. Platí $\mathbf{T}_{B\mapsto D} = \mathbf{T}_{C\mapsto D} \cdot \mathbf{T}_{B\mapsto C}$. To plyne z vlastností matice složeného zobrazení:

$$\begin{tikzcd}
\mathbb{F}^n \arrow[r, "\mathbf{x}\mapsto\mathbf{T}_{B\mapsto C}\cdot\mathbf{x}"] \arrow[rr, bend left, "\mathbf{x}\mapsto\mathbf{T}_{C\mapsto D}\cdot\mathbf{T}_{B\mapsto C}\cdot\mathbf{x}"] & \mathbb{F}^n \arrow[r, "\mathbf{x}\mapsto\mathbf{T}_{C\mapsto D}\cdot\mathbf{x}"] & \mathbb{F}^n \\
L \arrow[u, "\mathbf{coord}_B"] \arrow[r, "\mathbf{id}"'] \arrow[rr, bend right, "\mathbf{id}"'] & L \arrow[u, "\mathbf{coord}_C"'] \arrow[r, "\mathbf{id}"'] & L \arrow[u, "\mathbf{coord}_D"']
\end{tikzcd}$$

Příklad (přepočet souřadnic vzhledem k jiné bázi)

V prostoru $\mathbb{R}^{\leq 3}[x]$ nad $\mathbb{R}$ máme uspořádané báze $B = (x^3, x^2, x, 1)$ a $C = ((x-1)^3, (x-1)^2, x-1, 1)$.

Pro polynom $p(x) = -3x^2 + 6x + 3$ z $\mathbb{R}^{\leq 3}[x]$ hledáme $\mathbf{coord}_C(p(x))$. Víme, že $\mathbf{coord}_C(p(x)) = \mathbf{T}_{B \mapsto C} \cdot \mathbf{coord}_B(p(x))$.

Protože $\mathbf{coord}_B(p(x)) = \begin{pmatrix} 0 \\ -3 \\ 6 \\ 3 \end{pmatrix}$, stačí tedy znát[a] matici $\mathbf{T}_{B \mapsto C}$.

$$\mathbf{T}_{B \mapsto C} = (\mathbf{T}_{C \mapsto B})^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ 3 & -2 & 1 & 0 \\ -1 & 1 & -1 & 1 \end{pmatrix}^{-1}$$

[a] Uvidíme později, že pro nalezení matice $(\mathbf{T}_{C \mapsto B})^{-1}$ lze využít blokový tvar Gaussovy eliminace:

$$(\mathbf{T}_{C \mapsto B} \mid \mathbf{E}_n) \sim \cdots \sim (\mathbf{E}_n \mid (\mathbf{T}_{C \mapsto B})^{-1})$$

Příklad (přepočet souřadnic vzhledem k jiné bázi)

Jsou dány tři konečné báze B, C a D prostoru L. Spočtěte $\mathbf{coord}_B(4 \cdot \vec{x} + 12 \cdot \vec{y} + 3 \cdot \vec{z})$, pokud znáte $\mathbf{coord}_B(\vec{x})$, $\mathbf{coord}_C(\vec{y})$ a $\mathbf{coord}_D(\vec{z})$.

$$\mathbf{coord}_B(4 \cdot \vec{x} + 12 \cdot \vec{y} + 3 \cdot \vec{z}) =$$

$$4 \cdot \mathbf{coord}_B(\vec{x}) + 12 \cdot \mathbf{coord}_B(\vec{y}) + 3 \cdot \mathbf{coord}_B(\vec{z}) =$$

$$4 \cdot \mathbf{coord}_B(\vec{x}) + 12 \cdot \mathbf{T}_{C \mapsto B} \cdot \mathbf{coord}_C(\vec{y}) + 3 \cdot \mathbf{T}_{D \mapsto B} \cdot \mathbf{coord}_D(\vec{z}).$$

Poznámka (konceptuální výpočet $\mathbf{T}_{B\mapsto C}$ v prostoru $\mathbb{F}^n$)

Ať $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ a $C = (\mathbf{c}_1, \dots, \mathbf{c}_n)$ jsou libovolné báze prostoru $\mathbb{F}^n$.

Připomenutí: kanonická (také: standardní) báze $K_n = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ prostoru $\mathbb{F}^n$.

1. Je snadné nalézt matice $\mathbf{T}_{B\mapsto K_n}$ a $\mathbf{T}_{C\mapsto K_n}$.
   1. Do j-tého sloupce $\mathbf{T}_{B\mapsto K_n}$ napíšeme souřadnice $\mathbf{b}_j$ v kanonické bázi K_n.
   2. Do j-tého sloupce $\mathbf{T}_{C\mapsto K_n}$ napíšeme souřadnice $\mathbf{c}_j$ v kanonické bázi K_n.
2. $\mathbf{T}_{B\mapsto C} = \mathbf{T}_{K_n\mapsto C} \cdot \mathbf{T}_{B\mapsto K_n} = (\mathbf{T}_{C\mapsto K_n})^{-1} \cdot \mathbf{T}_{B\mapsto K_n}$.

Stačí tedy vyřešit[a] maticovou rovnici $\mathbf{T}_{C\mapsto K_n} \cdot \mathbf{X} = \mathbf{T}_{B\mapsto K_n}$.

---

[a] Uvidíme později, že pro nalezení matice $(\mathbf{T}_{C\mapsto K_n})^{-1} \cdot \mathbf{T}_{B\mapsto K_n}$ lze využít blokový tvar Gaussovy eliminace:

$$(\mathbf{T}_{C\mapsto K_n} \mid \mathbf{T}_{B\mapsto K_n}) \sim \cdots \sim (\mathbf{E}_n \mid (\mathbf{T}_{C\mapsto K_n})^{-1} \cdot \mathbf{T}_{B\mapsto K_n})$$

Příklad (nalezení báze, známe-li matici transformace)

$B = \left(\begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -2 \\ 1 \\ -2 \end{pmatrix}, \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix} \right)$ je báze lineárního prostoru $\mathbb{R}^3$. Tedy

$\mathbf{T}_{B \mapsto K_3} = \begin{pmatrix} 1 & -2 & 2 \\ 1 & 1 & -1 \\ 2 & -2 & 1 \end{pmatrix}$, kde K_3 je kanonická báze $\mathbb{R}^3$.

Nalezněte bázi $C = \left(\begin{pmatrix} c_{11} \\ c_{21} \\ c_{31} \end{pmatrix}, \begin{pmatrix} c_{12} \\ c_{22} \\ c_{32} \end{pmatrix}, \begin{pmatrix} c_{13} \\ c_{23} \\ c_{33} \end{pmatrix} \right)$ lineárního prostoru

$\mathbb{R}^3$ tak, aby platila rovnost $\mathbf{T}_{B \mapsto C} = \begin{pmatrix} -4 & 3 & 1 \\ 11 & 4 & 1 \\ 2 & 10 & 1 \end{pmatrix}$.

Příklad (pokrač.)

Protože C je báze a protože K_3 je kanonická báze, víme, že platí:

$$\begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{23} & c_{32} & c_{33} \end{pmatrix} = \mathbf{T}_{C \mapsto K_3}$$

Protože platí $\mathbf{T}_{C \mapsto K_3} = \mathbf{T}_{B \mapsto K_3} \cdot \mathbf{T}_{C \mapsto B} = \mathbf{T}_{B \mapsto K_3} \cdot (\mathbf{T}_{B \mapsto C})^{-1}$, dosadíme a spočítáme

$$\begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} = \begin{pmatrix} 1 & -2 & 2 \\ 1 & 1 & -1 \\ 2 & -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} -4 & 3 & 1 \\ 11 & 4 & 1 \\ 2 & 10 & 1 \end{pmatrix}^{-1}$$

Věta (změna matice zobrazení při změně bází)

Ať $\mathbf{f} : L_1 \to L_2$ je lineární zobrazení, $\dim(L_1) = n$, $\dim(L_2) = m$.
Ať B a B' jsou báze prostoru L_1 a ať C a C' jsou báze prostoru L_2.
Jestliže $\mathbf{A_f}$ je matice $\mathbf{f}$ vzhledem k B a C, pak součin
$\mathbf{T}_{C \mapsto C'} \cdot \mathbf{A_f} \cdot \mathbf{T}_{B' \mapsto B}$ je matice $\mathbf{f}$ vzhledem k B' a C'.

Důkaz.

$$\begin{tikzcd}
\mathbb{F}^n \arrow[r, "\mathbf{x} \mapsto \mathbf{T}_{B' \mapsto B} \cdot \mathbf{x}"] \arrow[rrr, bend left, "\mathbf{x} \mapsto \mathbf{T}_{C \mapsto C'} \cdot \mathbf{A_f} \cdot \mathbf{T}_{B' \mapsto B} \cdot \mathbf{x}"] & \mathbb{F}^n \arrow[r, "\mathbf{x} \mapsto \mathbf{A_f} \cdot \mathbf{x}"] & \mathbb{F}^m \arrow[r, "\mathbf{x} \mapsto \mathbf{T}_{C \mapsto C'} \cdot \mathbf{x}"] & \mathbb{F}^m \\
L_1 \arrow[u, "\mathbf{coord}_{B'}"] \arrow[r, "\mathbf{id}"'] \arrow[rrr, bend right, "\mathbf{f}"'] & L_1 \arrow[u, "\mathbf{coord}_B"'] \arrow[r, "\mathbf{f}"'] & L_2 \arrow[u, "\mathbf{coord}_C"] \arrow[r, "\mathbf{id}"'] & L_2 \arrow[u, "\mathbf{coord}_{C'}"']
\end{tikzcd}$$

■

Výpočet matice lineárního zobrazení $\mathbf{f} : L_1 \to L_2$ vzhledem k libovolným bázím

Ať $B = (\vec{b}_1, \ldots, \vec{b}_n)$ je báze L_1 a $C = (\vec{c}_1, \ldots, \vec{c}_m)$ je báze prostoru L_2.

Předpokládejme, že matice $\mathbf{A_f}$ zobrazení $\mathbf{f} : L_1 \to L_2$ vzhledem k jistým bázím $easy_n = (\vec{d}_1, \ldots, \vec{d}_n)$ a $easy_m = (\vec{k}_1, \ldots, \vec{k}_m)$ prostorů L_1 a L_2 se snadno určí.

1. Matice transformací souřadnic $\mathbf{T}_{B \mapsto easy_n}$ a $\mathbf{T}_{C \mapsto easy_m}$ se také určí snadno:
   1. Do j-tého sloupce matice $\mathbf{T}_{B \mapsto easy_n}$ napíšeme souřadnice vektoru $\vec{b}_j$ vzhledem k bázi $easy_n$.
   2. Do j-tého sloupce matice $\mathbf{T}_{C \mapsto easy_m}$ napíšeme souřadnice vektoru $\vec{c}_j$ vzhledem k bázi $easy_m$.
2. Platí: $\mathbf{T}_{easy_m \mapsto C} = (\mathbf{T}_{C \mapsto easy_m})^{-1}$.
3. Součin matic $\mathbf{T}_{easy_m \mapsto C} \cdot \mathbf{A_f} \cdot \mathbf{T}_{B \mapsto easy_n}$ je matice zobrazení $\mathbf{f}$ vzhledem k bázím B a C.

Příklad (matice zobrazení vzhledem k nestandardní bázi)

Nalezněte matici $\mathbf{A}$ zobrazení $\mathbf{der} : \mathbb{R}^{\leq 3}[x] \to \mathbb{R}^{\leq 3}[x]$ vzhledem k bázi $C = (x^3 + 3x^2, 3x^2 + 4x - 23, x - 1, 42)$.
Víme, že **der** má následující matici vzhledem k $B = (x^3, x^2, x, 1)$:

$$\mathbf{A}_{\mathbf{der}} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Platí:

$$\mathbf{T}_{C \mapsto B} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 3 & 3 & 0 & 0 \\ 0 & 4 & 1 & 0 \\ 0 & -23 & -1 & 42 \end{pmatrix}$$

Tedy: $\mathbf{A} = \mathbf{T}_{B \mapsto C} \cdot \mathbf{A}_{\mathbf{der}} \cdot \mathbf{T}_{C \mapsto B} = (\mathbf{T}_{C \mapsto B})^{-1} \cdot \mathbf{A}_{\mathbf{der}} \cdot \mathbf{T}_{C \mapsto B}$.

Závěrečné poznámky k transformaci souřadnic

1. Jakoukoli čvercovou regulární matici $\mathbf{T}$ typu $n \times n$ nad $\mathbb{F}$ lze považovat za matici transformace souřadnic $\mathbf{T}_{B \mapsto K_n}$, kde K_n je kanonická báze prostoru $\mathbb{F}^n$ a báze B je tvořena sloupci matice $\mathbf{T}$.
2. Je-li $\mathbf{A_f}$ matice zobrazení $\mathbf{f} : L_1 \to L_2$ vzhledem k bázím B a C, pak matice zobrazení $\mathbf{f}$ vzhledem k nějakým bázím B' a C' má tvar $\mathbf{S} \cdot \mathbf{A_f} \cdot \mathbf{T}$, pro nějaké regulární matice $\mathbf{S}$ a $\mathbf{T}$.

   Speciální případ: $L_1 = L_2$, $B = C$ a $B' = C'$. Pak matice $\mathbf{A_f}$ přejde na matici tvaru $\mathbf{T}^{-1} \cdot \mathbf{A_f} \cdot \mathbf{T}$, pro nějakou regulární matici $\mathbf{T}$.

Poznámky (pokrač.)

3. Řekneme, že dvě matice $\mathbf{A}$ a $\mathbf{B}$ typu $n \times n$ nad $\mathbb{F}$ jsou si podobné (značení: $\mathbf{A} \approx \mathbf{B}$), pokud platí rovnost $\mathbf{B} = \mathbf{T}^{-1} \cdot \mathbf{A} \cdot \mathbf{T}$, pro nějakou regulární matici $\mathbf{T}$.

   Podobné matice jsou tedy ty, které popisují stejné lineární zobrazení, každá matice jej vyjadřuje v jiné bázi. To využijeme při hledání vlastních hodnot lineárních zobrazení (později).

Příklad (Připomenutí příkladu z minulé přednášky)

Lineární zobrazení $\mathbf{f} : \mathbb{R}^2 \to \mathbb{R}^2$ je dáno hodnotami

$$\mathbf{f}(\begin{pmatrix} 1 \\ -1 \end{pmatrix}) = 2 \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad \text{a} \quad \mathbf{f}(\begin{pmatrix} 1 \\ 1 \end{pmatrix}) = \frac{1}{3} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Zobrazení $\mathbf{f}$ tedy:

1. „Prodlužuje“ $2\times$ měřítko v ose druhého a čtvrtého kvadrantu.
2. „Zkracuje“ $3\times$ měřítko v ose prvního a třetího kvadrantu.

Příklad (pokrač.)

Vzhledem k nekanonické bázi $B = \left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right)$ lineárního prostoru $\mathbb{R}^2$ má zobrazení $\mathbf{f}$ matici

$$\mathbf{A_f} = \begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{3} \end{pmatrix}$$

Vzhledem ke kanonické bázi K_2 lineárního prostoru $\mathbb{R}^2$ má zobrazení $\mathbf{f}$ matici[a]

$$\mathbf{B_f} = \begin{pmatrix} \frac{7}{6} & -\frac{5}{6} \\ -\frac{5}{6} & \frac{7}{6} \end{pmatrix}$$

Platí: $\mathbf{A_f} \approx \mathbf{B_f}$.

Matice $\mathbf{A_f}$ je „přehlednější“ než matice $\mathbf{B_f}$ (matice $\mathbf{A_f}$ vypovídá okamžitě o geometrické povaze zobrazení $\mathbf{f}$).

[a] Minulá přednáška.

GEM a soustavy lineárních rovnic, část 1

Odpřednesenou látku naleznete v kapitole 6 skript *Abstraktní a konkrétní lineární algebra*.

Minulé přednášky

1. Matice jako (speciální) lineární zobrazení. Obecná lineární zobrazení lze representovat maticí (vzhledem k zadaným bázím).
2. Algebra matic (sčítání matic, násobení matic skalárem, násobení matic mezi sebou).
3. Zápis $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$ kóduje soustavu lineárních rovnic.

Dnešní přednáška

1. Gaussova eliminační metoda (GEM) jako universální a systematická metoda řešení soustav lineárních rovnic (nad $\mathbb{F}$).

Příští přednáška

1. Maticové rovnice.
2. Hledání soustav, které mají zadané řešení.

Připomenutí (maticový zápis soustavy lineárních rovnic)

Zápis $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$, kde $\mathbf{A}$ je matice typu $r \times s$ nad $\mathbb{F}$, $\mathbf{x}$ je v $\mathbb{F}^s$ a $\mathbf{b}$ je v $\mathbb{F}^r$, kóduje soustavu lineárních rovnic nad $\mathbb{F}$.

Terminologie: $\mathbf{A}$ je matice soustavy, $\mathbf{b}$ je pravá strana rovnice, $\mathbf{x}$ je vektor neznámých. Matice $(\mathbf{A} \mid \mathbf{b})$ (také: $(\mathbf{a}_1, \ldots, \mathbf{a}_s \mid \mathbf{b})$) je rozšířená matice soustavy.
Například

$$\begin{pmatrix} 2 & -4 & 4 \\ 2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 12 \\ -42 \end{pmatrix}$$

je zápis soustavy

$$\begin{array}{rcrcrcr} 2x_1 & - & 4x_2 & + & 4x_3 & = & 12 \\ 2x_1 & & & + & x_3 & = & -42 \end{array}$$

nad $\mathbb{R}$.

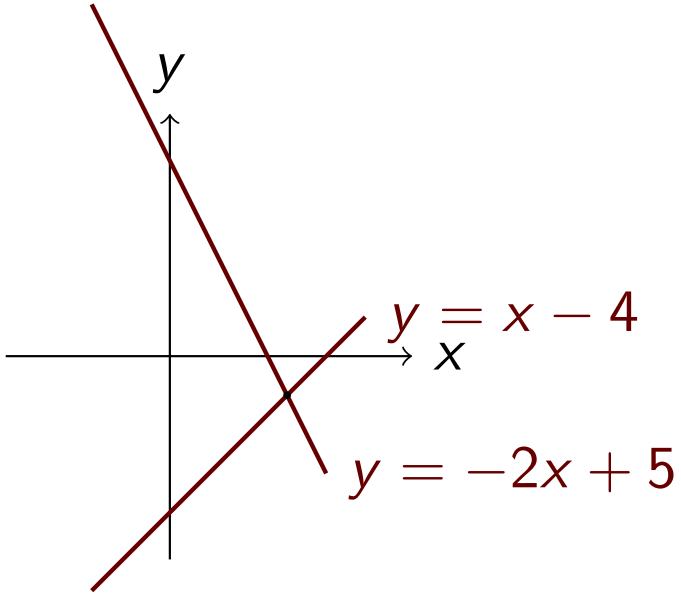
Připomenutí (dva pohledy na řešení soustav)

Pro soustavu

$$\left(\begin{array}{cc|c} 1 & -1 & 4 \\ 2 & 1 & 5 \end{array}\right)$$

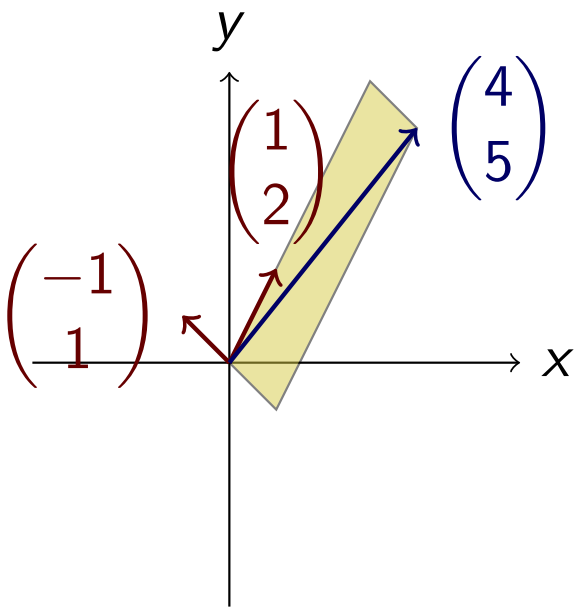
nad $\mathbb{R}$ je řešení

1. Průsečík dvou přímek: $x - y = 4$ a $2x + y = 5$:



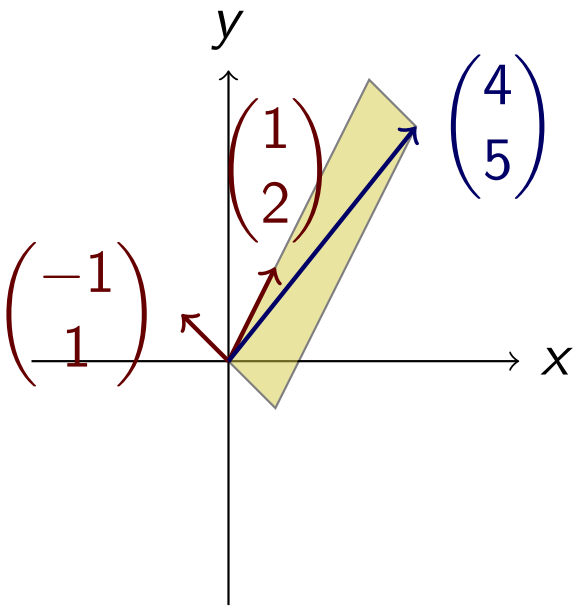
Připomenutí (dva pohledy na řešení soustav, pokrač.)

2. Pravá strana je lineární kombinací sloupců matice soustavy
$$\left(\begin{array}{cc|c} 1 & -1 & 4 \\ 2 & 1 & 5 \end{array}\right)$$

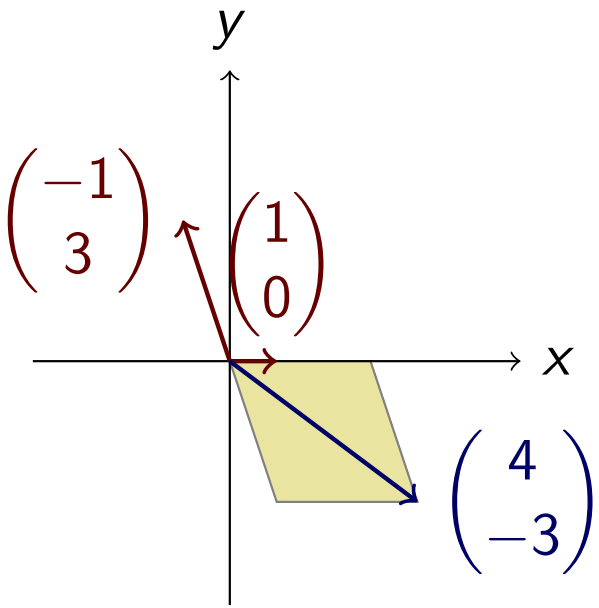


Řešení jsou koeficienty této lineární kombinace.

Výhoda druhého pohledu na řešení soustav



lze převést isomorfismem na



Koeficienty lineární kombinace situace napravo se najdou snadno.

Gaussova eliminační metoda je přesně postupné převádění vhodnými isomorfismy do příjemné polohy!

Ve zbytku přednášky

1. Nejprve se zaměříme na problém řešení soustav tvaru $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$.

   Konvence: Nebude-li řečeno jinak, je soustava $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$ ve zbytku přednášky soustavou r rovnic o s neznámých nad $\mathbb{F}$.

   Soustavy budeme většinou zapisovat rozšířenou maticí $(\mathbf{A} \mid \mathbf{b})$ nebo $(\mathbf{a}_1, \ldots, \mathbf{a}_s \mid \mathbf{b})$.

   Zformulujeme a dokážeme důležitý výsledek: Frobeniovu větu o řešitelnosti soustav lineárních rovnic.
2. Poté vyřešíme obecný problém maticových rovnic $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$.
3. Jako technický prostředek použijeme Gaussovu eliminační metodu (zkráceně: GEM). GEM převádí matice (a tím i soustavy) na „příjemný“ tvar.

Definice (horní blokový tvar matice)

Matice **M** je v horním blokovém tvaru, jsou-li splněny následující dvě podmínky:[a]

1. Každý nenulový řádek matice **M** je nad jakýmkoli řádkem samých nul.
2. Každý pivot (tj. nenulová položka první zleva) jakéhokoli nenulového řádku matice **M** je vždy více napravo než pivot předchozího řádku.

[a] Pozorování: **M** je v horním blokovém tvaru iff $(\mathbf{M} \mid \mathbf{o})$ je v horním blokovém tvaru.

Příklad

$$\begin{pmatrix} \mathbf{3} & -1 & 4 & 6 & 1 & 5 & 32 \\ 0 & 0 & \mathbf{6} & 2 & 3 & -4 & -1 \\ 0 & 0 & 0 & \mathbf{12} & 2 & 8 & 14 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Je v horním blokovém tvaru.

$$\begin{pmatrix} \mathbf{31} & 10 & 14 & 16 & -23 & 15 & 32 \\ 0 & 0 & \mathbf{23} & 2 & 3 & -4 & -1 \\ 0 & 0 & \mathbf{42} & 12 & 2 & 8 & 14 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{15} \end{pmatrix}$$

Není v horním blokovém tvaru.

Věta (Gaussova eliminační metoda (GEM) nad $\mathbb{F}$)

Jakoukoli matici $\mathbf{M}$ nad $\mathbb{F}$ lze konečným počtem tzv. řádkových elementárních úprav převést na horní blokový tvar.
Řádkové elementární úpravy jsou tří typů:

(I) Přičtení skalárního násobku řádku matice k jinému řádku matice.

(II) Prohození dvou řádků v matici.

(III) Vynásobení řádku matice nenulovým skalárem.

Důkaz.

Nebudeme dělat (viz skripta, Věta 6.3.10.). ■

Poznámky

GEM: použití řádkových elementárních úprav dané matice s cílem zapsat danou matici v horním blokovém tvaru. Při dosažení tohoto tvaru říkáme, že GEM skončila.

Příklad (Přičtení skalárního násobku řádku k řádku)

Ať $\mathbf{M} = \begin{pmatrix} 2 & 3 & 5 & 8 \\ 4 & 1 & 7 & 3 \\ 5 & 2 & 6 & 4 \end{pmatrix}$ a ať $\mathbf{P} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix}$.

Platí

$$\mathbf{P} \cdot \mathbf{M} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 & 5 & 8 \\ 4 & 1 & 7 & 3 \\ 5 & 2 & 6 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 5 & 8 \\ 4 & 1 & 7 & 3 \\ 11 & 11 & 21 & 28 \end{pmatrix} \begin{matrix} R_1 \\ R_2 \\ R_3 + 3R_1 \end{matrix}$$

Tudíž: přičtení skalárního násobku řádku k danému řádku je dáno isomorfismem $\mathbf{P} : \mathbb{R}^3 \to \mathbb{R}^3$, aplikovaným na čtveřici vektorů $\mathbf{M} = (\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3, \mathbf{m}_4)$ z $\mathbb{R}^3$.

Příklad (prohození dvou řádků v matici)

Ať $\mathbf{M} = \begin{pmatrix} 2 & 3 & 5 & 8 \\ 4 & 1 & 7 & 3 \\ 5 & 2 & 6 & 4 \end{pmatrix}$ a ať $\mathbf{P} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

Platí

$$\mathbf{P} \cdot \mathbf{M} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 & 5 & 8 \\ 4 & 1 & 7 & 3 \\ 5 & 2 & 6 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 2 & 6 & 4 \\ 4 & 1 & 7 & 3 \\ 2 & 3 & 5 & 8 \end{pmatrix} \begin{matrix} R_3 \\ R_2 \\ R_1 \end{matrix}$$

Tudíž: prohození dvou řádků je dáno isomorfismem $\mathbf{P} : \mathbb{R}^3 \to \mathbb{R}^3$, aplikovaným na čtveřici vektorů $\mathbf{M} = (\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3, \mathbf{m}_4)$ z $\mathbb{R}^3$.

Příklad (Vynásobení řádku matice nenulovým skalárem)

Ať $\mathbf{M} = \begin{pmatrix} 2 & 3 & 5 & 8 \\ 4 & 1 & 7 & 3 \\ 5 & 2 & 6 & 4 \end{pmatrix}$ a ať $\mathbf{P} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -5 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Platí

$$\mathbf{P} \cdot \mathbf{M} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -5 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 & 5 & 8 \\ 4 & 1 & 7 & 3 \\ 5 & 2 & 6 & 4 \end{pmatrix} = \begin{array}{c} \begin{pmatrix} 2 & 3 & 5 & 8 \\ -20 & -5 & -35 & -15 \\ 5 & 2 & 6 & 4 \end{pmatrix} \end{array} \begin{array}{l} R_1 \\ -5R_2 \\ R_3 \end{array}$$

Tudíž: vynásobení řádku matice nenulovým skalárem je dáno isomorfismem $\mathbf{P} : \mathbb{R}^3 \to \mathbb{R}^3$, aplikovaným na čtveřici vektorů $\mathbf{M} = (\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3, \mathbf{m}_4)$ z $\mathbb{R}^3$.

Definice (ekvivalentní soustavy)

Řekneme, že soustavy $(\mathbf{A} \mid \mathbf{b})$ a $(\mathbf{A}' \mid \mathbf{b}')$ r rovnic o s neznámých jsou ekvivalentní[a] (značení: $(\mathbf{A} \mid \mathbf{b}) \sim (\mathbf{A}' \mid \mathbf{b}')$), když pro každý vektor $\mathbf{x}$ z $\mathbb{F}^s$ platí: $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$ právě tehdy, když $\mathbf{A}' \cdot \mathbf{x} = \mathbf{b}'$.

[a] Slogan: Ekvivalentní soustavy stejných rozměrů mají stejná řešení.

Tvrzení (základní vlastnosti ekvivalence soustav)

Platí:

1. $(\mathbf{A} \mid \mathbf{b}) \sim (\mathbf{A} \mid \mathbf{b})$.
2. Jestliže $(\mathbf{A} \mid \mathbf{b}) \sim (\mathbf{A}' \mid \mathbf{b}')$, pak $(\mathbf{A}' \mid \mathbf{b}') \sim (\mathbf{A} \mid \mathbf{b})$.
3. Jestliže $(\mathbf{A} \mid \mathbf{b}) \sim (\mathbf{A}' \mid \mathbf{b}')$ a $(\mathbf{A}' \mid \mathbf{b}') \sim (\mathbf{A}'' \mid \mathbf{b}'')$, pak $(\mathbf{A} \mid \mathbf{b}) \sim (\mathbf{A}'' \mid \mathbf{b}'')$.

Ať $\mathbf{P} : \mathbb{F}^r \to \mathbb{F}^r$ je jakýkoli isomorfismus. Potom platí

1. $(\mathbf{A} \mid \mathbf{b}) \sim (\mathbf{P} \cdot \mathbf{A} \mid \mathbf{P} \cdot \mathbf{b})$.
2. $\mathrm{rank}((\mathbf{A} \mid \mathbf{b})) = \mathrm{rank}((\mathbf{P} \cdot \mathbf{A} \mid \mathbf{P} \cdot \mathbf{b}))$.

Důkaz.

Přednáška.

Shrnutí

Ať $\mathbf{M}$ je jakákoli nad $\mathbb{F}$ o r řádcích. Potom platí:

1. Každá elementární úprava matice $\mathbf{M}$ je dána součinem $\mathbf{P} \cdot \mathbf{M}$ pro vhodný „elementární“ isomorfismus $\mathbf{P} : \mathbb{F}^r \to \mathbb{F}^r$.
2. Je-li matice $\mathbf{M}'$ horním blokovým tvarem[a] matice $\mathbf{M}$, pak
   1. Existuje isomorfismus $\mathbf{P} : \mathbb{F}^r \to \mathbb{F}^r$ tak, že $\mathbf{M}' = \mathbf{P} \cdot \mathbf{M}$ a $\mathbf{P} = \mathbf{P}_k \cdot \ldots \cdot \mathbf{P}_1$, kde k je nějaké přirozené číslo a $\mathbf{P}_1, \ldots, \mathbf{P}_k$ jsou „elementární“ isomorfismy.
   2. Platí $\mathrm{rank}(\mathbf{M}) = \mathrm{rank}(\mathbf{M}')$ a $\mathrm{def}(\mathbf{M}) = \mathrm{def}(\mathbf{M}')$.

Speciálně: pro $\mathbf{M}$ ve tvaru $(\mathbf{A} \mid \mathbf{b})$ lze elementárními úpravami převést každou soustavu na horní blokový tvar $(\mathbf{A}' \mid \mathbf{b}')$. Navíc platí $(\mathbf{A} \mid \mathbf{b}) \sim (\mathbf{A}' \mid \mathbf{b}')$.

---

[a] Důležité: nikdy jsme neříkali, že při elementárních úpravách lze vyškrtávat nulové řádky. Vyškrtávat nulové řádky při GEM nebudeme; matice $\mathbf{M}$ a $\mathbf{M}'$ musí mít stejné rozměry!

Důsledky

1. Pro každou matici $\mathbf{M}$ platí $\mathrm{rank}(\mathbf{M}) = \mathrm{rank}(\mathbf{M}^T)$, kde $\mathbf{M}^T$ je transponovaná matice[a] k matici $\mathbf{M}$.
2. Hodnost matice $\mathbf{M}$ je rovna počtu nenulových řádků v horním blokovém tvaru po skončení GEM.
3. Defekt matice $\mathbf{M}$ je roven počtu sloupců matice $\mathbf{M}$ mínus hodnost matice $\mathbf{M}$.

---

[a] Matice $\mathbf{M}^T$ má jako své sloupce původní řádky matice $\mathbf{M}$ zapsané ve stejném pořadí. Například pro

$$\mathbf{M} = \begin{pmatrix} 2 & 4 & -1 \\ 3 & 1 & 7 \end{pmatrix}$$

je

$$\mathbf{M}^T = \begin{pmatrix} 2 & 3 \\ 4 & 1 \\ -1 & 7 \end{pmatrix}$$

Věta (Frobenius)

1. Soustava $(\mathbf{A} \mid \mathbf{b})$ má řešení právě tehdy, když platí rovnost $\mathrm{rank}(\mathbf{A}) = \mathrm{rank}(\mathbf{A} \mid \mathbf{b})$.
2. Pokud $(\mathbf{A} \mid \mathbf{b})$ má řešení, potom lze říci následující:[a]

   Zvolme jakékoli $\mathbf{p}$, splňující rovnost $\mathbf{A} \cdot \mathbf{p} = \mathbf{b}$.
   Potom $\mathbf{A} \cdot \mathbf{x}_0 = \mathbf{b}$ platí právě tehdy, když $\mathbf{x}_0 = \mathbf{p} + \mathbf{x}_h$ pro nějaké $\mathbf{x}_h$ z $\ker(\mathbf{A})$.

[a] Budeme používat i zkrácený a přehledný zápis: množinu všech řešení lze napsat jako $\mathbf{p} + \ker(\mathbf{A}) = \{\mathbf{p} + \mathbf{x}_h \mid \mathbf{x}_h \in \ker(\mathbf{A})\}$, kde $\mathbf{A} \cdot \mathbf{p} = \mathbf{b}$.

Důkaz.

1. $(\mathbf{A} \mid \mathbf{b})$ má řešení právě tehdy, když $\mathbf{b}$ je v $\mathrm{im}(\mathbf{A})$. To nastane právě tehdy, když $\mathrm{rank}(\mathbf{A}) = \mathrm{rank}(\mathbf{A} \mid \mathbf{b})$. Viz str 12, téma 3A.
2. Triviální.

Základní myšlenky řešení soustavy $(\mathbf{A} \mid \mathbf{b})$

1. $\ker(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{A} \cdot \mathbf{x} = \mathbf{o}\}$ je lineární podprostor prostoru $\mathbb{F}^s$. Tudíž pro vyřešení $\mathbf{A} \cdot \mathbf{x} = \mathbf{o}$ stačí najít bázi $\ker(\mathbf{A})$. Tato báze má přesně $\mathrm{def}(\mathbf{A})$ prvků.

   Jakékoli bázi prostoru $\ker(\mathbf{A})$ budeme říkat fundamentální systém soustavy s maticí $\mathbf{A}$.

2. Soustavě $(\mathbf{A} \mid \mathbf{o})$ budeme říkat homogenní soustava příslušná k matici $\mathbf{A}$.

   Jakékoli řešení homogenní soustavy je tedy lineární kombinací prvků fundamentálního systému.

3. Jakékoli řešení soustavy lze vyjádřit ve tvaru $\mathbf{p} + \mathbf{x}_h$, kde $\mathbf{x}_h$ je v $\ker(\mathbf{A})$ a $\mathbf{p}$ je jakékoli řešení původní soustavy (takzvané partikulární řešení).

Jak vyřešit homogenní soustavu $(\mathbf{A} \mid \mathbf{o})$

1. GEM: $(\mathbf{A} \mid \mathbf{o}) \sim (\mathbf{A}' \mid \mathbf{o})$.
2. Víme: $\mathrm{rank}(\mathbf{A}) = \mathrm{rank}(\mathbf{A}')$ a matice $\mathbf{A}'$ je v horním blokovém tvaru. Tudíž známe defekt matice $\mathbf{A}$: $d = \mathrm{def}(\mathbf{A}) = s - \mathrm{rank}(\mathbf{A}) = s - \mathrm{rank}(\mathbf{A}')$.
3. Báze prostoru $\ker(\mathbf{A})$ musí mít d prvků. Tudíž d hodnot v každém řešení lze zvolit (jde o posice, na kterých nejsou pivoty matice $\mathbf{A}'$). Touto volbou zajistíme lineární nezávislost. Dalších $s - d$ hodnot lze spočíst z nenulových rovnic v soustavě $(\mathbf{A}' \mid \mathbf{o})$ zpětným dosazením.

Jak nalézt partikulární řešení soustavy $(\mathbf{A} \mid \mathbf{b})$

1. GEM: $(\mathbf{A} \mid \mathbf{b}) \sim (\mathbf{A}' \mid \mathbf{b}')$.
2. d hodnot v partikulárním řešení lze zvolit (jde o posice, na kterých nejsou pivoty matice $\mathbf{A}'$).
3. Zpětné dopočtení z nenulových rovnic soustavy $(\mathbf{A}' \mid \mathbf{b}')$.

Příklad (ukázka systematického řešení soustavy nad $\mathbb{R}$)

Nad $\mathbb{R}$ vyřešte: $2x_1 + 3x_2 - 4x_3 = 2$ (maticově: $\left(\begin{array}{ccc|c} 2 & 3 & -4 & 2 \end{array}\right)$).
Pro matici soustavy $\mathbf{A} = \begin{pmatrix} 2 & 3 & -4 \end{pmatrix}$ platí rovnosti $\mathrm{rank}(\mathbf{A}) = 1$ a $\mathrm{def}(\mathbf{A}) = 2$. Pivot je na první posici: volit budeme vždy druhou a třetí položku, první položku dopočteme.

1. Příslušná homogenní rovnice: $\left(\begin{array}{ccc|c} 2 & 3 & -4 & 0 \end{array}\right)$.

   Fundamentální systém: $\begin{pmatrix} -\frac{3}{2} \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}$.

2. Partikulární řešení pro $\left(\begin{array}{ccc|c} 2 & 3 & -4 & 2 \end{array}\right)$: $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

3. Celkové řešení: $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \mathrm{span}\left\{ \begin{pmatrix} -\frac{3}{2} \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 4 \\ 0 \\ 1 \end{pmatrix} \right\}$.

Příklad (geometrický význam postupu řešení soustavy)

Rovnice $2x_1 + 3x_2 - 4x_3 = 2$ v $\mathbb{R}^3$ popisuje rovinu ρ v prostoru $\mathbb{R}^3$. Tato rovina ρ je v obecné poloze (rovina ρ neprochází počátkem, protože $2 \neq 0$).

1. Homogenní rovnice $2x_1 + 3x_2 - 4x_3 = 0$ je paralelní posunutí roviny ρ tak, aby výsledná rovina ρ_h procházela počátkem.

   Fundamentální systém $\mathbf{x}_1$, $\mathbf{x}_2$ je systém souřadnic v rovině ρ_h.
2. Partikulární řešení rovnice $2x_1 + 3x_2 - 4x_3 = 2$ je libovolný bod $\mathbf{p}$ v původní rovině ρ.
3. Zápis $\mathbf{p} + \operatorname{span}\{\mathbf{x}_1, \mathbf{x}_2\}$ obecného řešení vyjadřuje opětovné paralelní posunutí roviny ρ_h zpět do roviny ρ.

Poznámka

Stejnou geometrickou představu je třeba mít pro řešení obecné soustavy $(\mathbf{A} \mid \mathbf{b})$ nad $\mathbb{F}$.

Příklad (systematické řešení komplikovanější soustavy nad $\mathbb{R}$)

$$\left(\begin{array}{cccc|c} 1 & 3 & 2 & 0 & 3 \\ 1 & 1 & 1 & -1 & 5 \\ 2 & 8 & 5 & 3 & 7 \\ 3 & 9 & 6 & 2 & 12 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 3 & 2 & 0 & 3 \\ 0 & -2 & -1 & -1 & 2 \\ 0 & 2 & 1 & 3 & 1 \\ 0 & 0 & 0 & 2 & 3 \end{array}\right) \begin{array}{l} R_1 \\ R_2 - R_1 \\ R_3 - 2R_1 \\ R_4 - 3R_1 \end{array}$$

$$\sim \left(\begin{array}{cccc|c} 1 & 3 & 2 & 0 & 3 \\ 0 & 1 & \frac{1}{2} & \frac{1}{2} & -1 \\ 0 & 0 & 0 & 2 & 3 \\ 0 & 0 & 0 & 2 & 3 \end{array}\right) \begin{array}{l} R_1 \\ -1/2R_2 \\ R_3 + R_2 \\ R_4 \end{array}$$

$$\sim \left(\begin{array}{cccc|c} 1 & 3 & 2 & 0 & 3 \\ 0 & 1 & \frac{1}{2} & \frac{1}{2} & -1 \\ 0 & 0 & 0 & 1 & \frac{3}{2} \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \begin{array}{l} R_1 \\ R_2 \\ 1/2R_3 \\ R_4 - R_3 \end{array}$$

Důležité: povšimněme si značení řádkových úprav; úpravy budeme vždy takto vyznačovat.

Příklad (pokrač.)

Po skončení GEM $\left(\begin{array}{cccc|c} 1 & 3 & 2 & 0 & 3 \\ 0 & 1 & \frac{1}{2} & \frac{1}{2} & -1 \\ 0 & 0 & 0 & 1 & \frac{3}{2} \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$ jsou pivoty na čtvrté, druhé a první posici. Tyto položky v řešení budeme dopočítávat, třetí položku řešení budeme volit.

Řešení je: $\begin{pmatrix} \frac{33}{4} \\ -\frac{7}{4} \\ 0 \\ \frac{3}{2} \end{pmatrix} + a \cdot \begin{pmatrix} -\frac{1}{2} \\ -\frac{1}{2} \\ 1 \\ 0 \end{pmatrix}$, kde $a \in \mathbb{R}$.

Zkrácený zápis: $\begin{pmatrix} \frac{33}{4} \\ -\frac{7}{4} \\ 0 \\ \frac{3}{2} \end{pmatrix} + \operatorname{span}\left(\begin{pmatrix} -\frac{1}{2} \\ -\frac{1}{2} \\ 1 \\ 0 \end{pmatrix}\right)$.

Řešením soustavy je přímka v $\mathbb{R}^4$.

GEM a soustavy lineárních rovnic, část 2

Odpřednesenou látku naleznete v kapitolách 6 a 7.1 skript *Abstraktní a konkrétní lineární algebra*.

Minulá přednáška

1. Gaussova eliminační metoda (GEM) jako universální a systematická metoda řešení soustav lineárních rovnic (nad $\mathbb{F}$).

Dnešní přednáška

1. Lineární maticové rovnice.
2. Hledání soustav, které mají zadané řešení.

Příklad

Nalezněte všechny matice $\mathbf{X}$, které splňují rovnost[a] $\mathbf{R}_\alpha \cdot \mathbf{X} = \mathbf{X} \cdot \mathbf{R}_\alpha$, kde $\mathbf{R}_\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ je matice rotace o úhel α, $\alpha \in [0; 2\pi)$.

Rozměrová zkouška: musí platit $\mathbf{X} : \mathbb{R}^2 \to \mathbb{R}^2$.

Rešeními jsou například matice $\mathbf{E}_2$, $\mathbf{O}_{2,2}$ a $\mathbf{R}_\alpha$.

Jak nalézt všechna řešení? Předvedeme universální metodu.

1. Označme $\mathbf{X} = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$. Potom

$$\mathbf{R}_\alpha \cdot \mathbf{X} = \begin{pmatrix} \cos\alpha \cdot x_{11} - \sin\alpha \cdot x_{21} & \cos\alpha \cdot x_{12} - \sin\alpha \cdot x_{22} \\ \sin\alpha \cdot x_{11} + \cos\alpha \cdot x_{21} & \sin\alpha \cdot x_{12} + \cos\alpha \cdot x_{22} \end{pmatrix} \text{ a}$$

$$\mathbf{X} \cdot \mathbf{R}_\alpha = \begin{pmatrix} \cos\alpha \cdot x_{11} + \sin\alpha \cdot x_{12} & -\sin\alpha \cdot x_{11} + \cos\alpha \cdot x_{12} \\ \cos\alpha \cdot x_{21} + \sin\alpha \cdot x_{22} & -\sin\alpha \cdot x_{21} + \cos\alpha \cdot x_{22} \end{pmatrix}.$$

[a] Geometrický význam: hledáme všechny transformace $\mathbf{X}$ roviny, které jsou záměnné s rotací o úhel α.

Příklad (pokrač.)

2. Rovnost $\mathbf{R}_\alpha \cdot \mathbf{X} = \mathbf{X} \cdot \mathbf{R}_\alpha$ je ekvivalentní rovnosti $\mathbf{R}_\alpha \cdot \mathbf{X} - \mathbf{X} \cdot \mathbf{R}_\alpha = \mathbf{O}_{2,2}$. Stačí tedy vyřešit soustavu čtyř rovnic

$$\begin{array}{rrrrcl}
 & -\sin\alpha \cdot x_{21} & -\sin\alpha \cdot x_{12} & & = & 0 \\
\sin\alpha \cdot x_{11} & & & -\sin\alpha \cdot x_{22} & = & 0 \\
\sin\alpha \cdot x_{11} & & & -\sin\alpha \cdot x_{22} & = & 0 \\
 & \sin\alpha \cdot x_{21} & +\sin\alpha \cdot x_{12} & & = & 0
\end{array}$$

V maticovém zápisu (po skončení GEM) máme řešit soustavu

$$\left(\begin{array}{cccc|c}
\sin\alpha & 0 & 0 & -\sin\alpha & 0 \\
0 & \sin\alpha & \sin\alpha & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0
\end{array}\right)$$

v závislosti na parametru $\alpha \in [0; 2\pi)$.

Příklad (pokrač.)

3. Pro $\sin\alpha = 0$ má soustava tvar

$$\left(\begin{array}{cccc|c} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

a tudíž řešení je tvaru $\mathbf{X} = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$, kde x_{11}, x_{21}, x_{12} a x_{22} jsou libovolná reálná čísla.

Závěr: s rotací o úhel 0 nebo π je záměnná libovolná transformace roviny.

Příklad (pokrač.)

4. Pro $\sin\alpha \neq 0$ má soustava tvar

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

a řešení $\operatorname{span}\left(\begin{pmatrix} 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}\right)$.

Závěr: s rotací $\mathbf{R}_\alpha$ o úhel $\alpha \notin \{0, \pi\}$ jsou záměnné transformace roviny tvaru $\mathbf{X} = a \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + b \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, kde a, b jsou libovolná reálná čísla.

Poznámky

1. Předchozí metoda (rozměrová zkouška pro hledanou matici $\mathbf{X}$ a následné řešení velké soustavy rovnic) je universální metodou pro řešení maticových rovnic, kde neznámá matice $\mathbf{X}$ vystupuje pouze v první mocnině.

   Jak už to u universálních metod bývá: v některých případech je taková metoda zbytečně zdlouhavá.

2. Předvedeme speciální metodu řešení maticových rovnic tvaru[a] $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$.

[a] Protože rovnost $\mathbf{X} \cdot \mathbf{A} = \mathbf{B}$ je ekvivalentní rovnosti $\mathbf{A}^T \cdot \mathbf{X}^T = \mathbf{B}^T$, získáme tak i metodu pro řešení rovnic tvaru $\mathbf{X} \cdot \mathbf{A} = \mathbf{B}$. Musíme ovšem obezřetně zacházet s transposicemi matic.

Převod maticové rovnice na více soustav lineárních rovnic

Maticovou rovnici $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$, kde matice $\mathbf{A} : \mathbb{F}^s \to \mathbb{F}^r$, a matice $\mathbf{B} : \mathbb{F}^p \to \mathbb{F}^r$, převedeme na p soustav

$$\mathbf{A} \cdot \mathbf{x} = \mathbf{b}_1, \quad \ldots, \quad \mathbf{A} \cdot \mathbf{x} = \mathbf{b}_p$$

kde $\mathbf{B} = (\mathbf{b}_1 \ \mathbf{b}_2 \ \ldots \ \mathbf{b}_p)$.

1. Každou takovou soustavu $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}_i$ vyřešíme předešlými postupy.[a]
2. Řešení $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$ existuje právě tehdy, když každá soustava $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}_i$ má řešení.
3. Pokud má každá soustava $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}_i$ řešení, pak „sesazením“ všech řešení $\mathbf{x}_1, \ldots \mathbf{x}_s$ jednotlivých soustav dostaneme řešení původní maticové rovnice: $\mathbf{X} = (\mathbf{x}_1 \ \mathbf{x}_2 \ \ldots \ \mathbf{x}_p)$.

[a] Jak uvidíme, lze takový systém soustav řešit simultánně.

Příklad

Nad $\mathbb{R}$ vyřešte rovnici $\begin{pmatrix} 1 & 2 & 1 \\ 1 & -3 & 2 \end{pmatrix} \cdot \mathbf{X} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.

Protože $\mathbf{X} : \mathbb{R}^2 \to \mathbb{R}^3$, máme řešit dvě soustavy:

$$\begin{pmatrix} 1 & 2 & 1 \\ 1 & -3 & 2 \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 1 \\ 1 & -3 & 2 \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

Obě soustavy mají stejnou matici soustavy, lze je tedy řešit simultánně:

1. Simultánní GEM:

$$\left(\begin{array}{ccc|cc} 1 & 2 & 1 & 2 & 1 \\ 1 & -3 & 2 & 1 & 2 \end{array}\right) \sim \left(\begin{array}{ccc|cc} 1 & 2 & 1 & 2 & 1 \\ 0 & -5 & 1 & -1 & 1 \end{array}\right) \begin{array}{l} R_1 \\ R_2 - R_1 \end{array}$$

   Podle Frobeniovy věty mají obě soustavy řešení.

Příklad (pokrač.)

2. Zápis $\left(\begin{array}{ccc|cc} 1 & 2 & 1 & 2 & 1 \\ 0 & -5 & 1 & -1 & 1 \end{array}\right)$ kóduje dvě soustavy s řešeními (v pořadí soustav zleva doprava):

$$\begin{pmatrix} 3 \\ 0 \\ -1 \end{pmatrix} + \operatorname{span}\left(\begin{pmatrix} -7 \\ 1 \\ 5 \end{pmatrix}\right) \quad \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + \operatorname{span}\left(\begin{pmatrix} -7 \\ 1 \\ 5 \end{pmatrix}\right)$$

3. „Sesazení řešení dohromady“: celkové řešení je tvaru

$$\mathbf{X} = \begin{pmatrix} 3-7a & -7b \\ a & b \\ -1+5a & 1+5b \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 0 \\ -1 & 1 \end{pmatrix} + a \cdot \begin{pmatrix} -7 & 0 \\ 1 & 0 \\ 5 & 0 \end{pmatrix} + b \cdot \begin{pmatrix} 0 & -7 \\ 0 & 1 \\ 0 & 5 \end{pmatrix}$$

kde a, b jsou libovolná reálná čísla.

Poznámka

Víme, že pro regulární matici $\mathbf{A} : \mathbb{F}^n \to \mathbb{F}^n$ má soustava $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$ jediné řešení, a sice $\mathbf{X} = \mathbf{A}^{-1} \cdot \mathbf{B}$.

Toto jediné řešení lze nalézt postupem, kterému se někdy říká Gaussova-Jordanova eliminace: eleminace řádkovými úpravami nekončí po dosažení horní trojúhelníkové matice, ale pokračujuje nulováním i nad hlavní diagonálou.

Získáváme tak postup

$$(\mathbf{A} \mid \mathbf{B}) \sim \cdots \sim (\mathbf{E}_n \mid \mathbf{A}^{-1} \cdot \mathbf{B})$$

Speciálně: pro regulární $\mathbf{A} : \mathbb{F}^n \to \mathbb{F}^n$ lze nalézt $\mathbf{A}^{-1}$ postupem

$$(\mathbf{A} \mid \mathbf{E}_n) \sim \cdots \sim (\mathbf{E}_n \mid \mathbf{A}^{-1})$$

Více viz cvičení a skripta, Příklad 6.4.12.

Příklad

Nad $\mathbb{R}$ nalezněte (jakoukoli) soustavu tvaru $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$, která má řešení

$$\begin{pmatrix} 3 \\ 2 \\ 6 \end{pmatrix} + \operatorname{span}\left(\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 4 \end{pmatrix} \right)$$

Myšlenky postupu:

1. Zadané řešení tvoří rovinu v $\mathbb{R}^3$, která prochází bodem $\begin{pmatrix} 3 \\ 2 \\ 6 \end{pmatrix}$ a má „směr“ určený vektory $\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 4 \end{pmatrix}$.
2. Tudíž: hledanou soustavu očekáváme ve tvaru $(a_1 \ a_2 \ a_3 \mid b)$, neboli $a_1 x + a_2 y + a_3 z = b$.
   Jak najít soustavu $(a_1 \ a_2 \ a_3 \mid b)$ systematicky?

Příklad, pokrač.

Podle Frobeniovy věty je

$$\begin{pmatrix}3\\2\\6\end{pmatrix} + \operatorname{span}\left(\begin{pmatrix}1\\2\\0\end{pmatrix}, \begin{pmatrix}2\\0\\4\end{pmatrix}\right)$$

řešením soustavy $\mathbf{A}\cdot\mathbf{x} = \mathbf{b}$, kde

1. Vektory $\begin{pmatrix}1\\2\\0\end{pmatrix}$, $\begin{pmatrix}2\\0\\4\end{pmatrix}$ jsou lineárně nezávislé; tvoří tudíž fundamentální systém soustavy $\mathbf{A}\cdot\mathbf{x} = \mathbf{o}$, kde $\operatorname{def}(\mathbf{A}) = 2$ a $\mathbf{A}$ má tři sloupce. To umožní nalézt $\mathbf{A} = (a_1\ a_2\ a_3)$.
2. Vektor $\begin{pmatrix}3\\2\\6\end{pmatrix}$ je partikulární řešení soustavy $\mathbf{A}\cdot\mathbf{x} = \mathbf{b}$, neboli $\mathbf{A}\cdot\begin{pmatrix}3\\2\\6\end{pmatrix} = \mathbf{b}$. Matici $\mathbf{A}$ známe, můžeme dopočítat $\mathbf{b} = (b)$.

Příklad, pokrač.

3. Nalezení **A**:
   1. Protože má platit $(a_1\ a_2\ a_3) \cdot \begin{pmatrix} 2 \\ 0 \\ 4 \end{pmatrix} = 0$, musí platit $(2\ 0\ 4) \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = 0.$
   2. Protože má platit $(a_1\ a_2\ a_3) \cdot \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} = 0$, musí platit $(1\ 2\ 0) \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = 0$

Tudíž $\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$ je fundamentální systém soustavy $\left(\begin{array}{ccc|c} 2 & 0 & 4 & 0 \\ 1 & 2 & 0 & 0 \end{array}\right)$, neboli (např.) $\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ -1 \end{pmatrix}$ a $\mathbf{A} = (2\ \ -1\ \ -1)$.

Příklad, pokrač.

4. Nalezení $\mathbf{b}$. Protože $\mathbf{A} = (2 \;\; -1 \;\; -1)$ a $\mathbf{A} \cdot \begin{pmatrix} 3 \\ 2 \\ 6 \end{pmatrix} = \mathbf{b}$, je $b = -2$.
5. Závěr: hledaná soustava je (například) $(2 \;\; -1 \;\; -1 \mid -2)$.

Poznámky

1. Předchozí příklad nalezl obecnou rovnici roviny z jejího parametrického zadání. Postup využíval platnosti Frobeniovy věty a základních vlastností matic.
2. Očekáváme: podobný postup bude fungovat pro nalezení soustavy $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$ nad tělesem $\mathbb{F}$, která má řešení

$$\mathbf{p} + \operatorname{span}(\mathbf{x}_1, \ldots, \mathbf{x}_d)$$

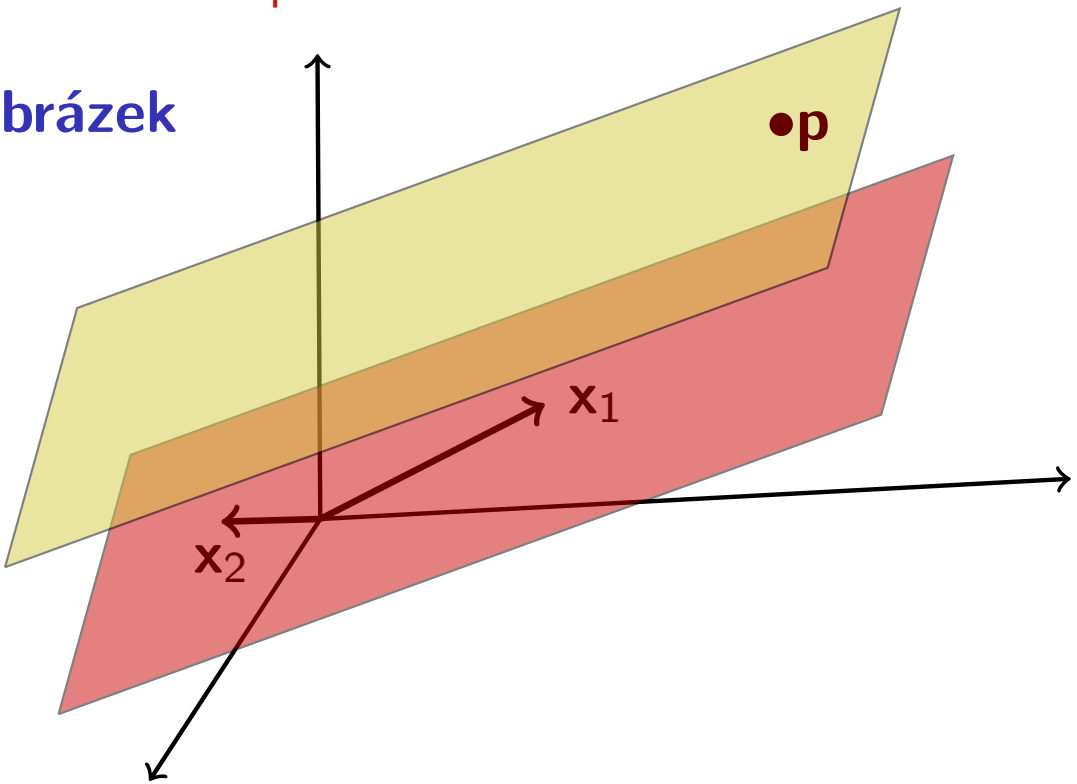
kde vektory $\mathbf{x}_1, \ldots, \mathbf{x}_d$ jsou lineárně nezávislé.

Definice

Zápisu $\mathbf{p} + \mathrm{span}(\mathbf{x}_1, \ldots, \mathbf{x}_d)$ v $\mathbb{F}^s$, kde vektory $\mathbf{x}_1, \ldots, \mathbf{x}_d$ jsou lineárně nezávislé, říkáme afinní podprostor dimense d v prostoru $\mathbb{F}^s$.[a] Seznamu $(\mathbf{x}_1, \ldots, \mathbf{x}_d)$ říkáme směr (také: zaměření) tohoto podprostoru.

[a] Také: d-dimensionální plocha v $\mathbb{F}^s$.

Ilustrační obrázek



Tvrzení

Ke každému d-dimensionálnímu afinnímu podprostoru $\mathbf{p} + \operatorname{span}(\mathbf{x}_1, \ldots, \mathbf{x}_d)$ v $\mathbb{F}^s$ existuje alespoň jedna soustava tvaru $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$, která má $\mathbf{p} + \operatorname{span}(\mathbf{x}_1, \ldots, \mathbf{x}_d)$ jako množinu řešení.

Důkaz.

Podrobně na přednášce; hlavní myšlenky jsou:

1. Musí platit $\mathbf{A} \cdot \mathbf{x}_i = \mathbf{o}$ pro $i = 1, \ldots, d$ a $\mathbf{A} \cdot \mathbf{p} = \mathbf{b}$.
2. Označme $\mathbf{X} = (\mathbf{x}_1, \ldots, \mathbf{x}_d)$. Protože seznam $(\mathbf{x}_1, \ldots, \mathbf{x}_d)$ je lineárně nezávislý, platí $d = \operatorname{rank}(\mathbf{X}) = \operatorname{rank}(\mathbf{X}^T)$. Soustava[a] $\mathbf{X}^T \cdot \mathbf{a} = \mathbf{o}$ má $s - d$ prvků ve svém fundamentálním systému. Označme tento systém jako $(\mathbf{a}_1, \ldots, \mathbf{a}_{s-d})$.
3. Známe $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_{s-d})^T$ a dopočteme $\mathbf{b}$ z rovnice $\mathbf{A} \cdot \mathbf{p} = \mathbf{b}$.

[a] Pozor: matici $\mathbf{X}^T$ známe, neznámá je označena jako $\mathbf{a}$.

Příklad

Nad $\mathbb{R}$ nalezněte (jakoukoli) soustavu tvaru $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$, která má řešení

$$\begin{pmatrix} 1 \\ 1 \\ -2 \\ 0 \\ 2 \end{pmatrix} + \operatorname{span}\left(\begin{pmatrix} 2 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right)$$

1. Označme $\mathbf{X} = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 2 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, potom $\mathbf{X}^T = \begin{pmatrix} 2 & 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 \\ -1 & 2 & 0 & 0 & 1 \end{pmatrix}$. Platí $3 = \operatorname{rank}(\mathbf{X}) = \operatorname{rank}(\mathbf{X}^T)$.
2. Matice $\mathbf{A}$ má jako řádky fundamentální systém soustavy $\mathbf{X}^T \cdot \mathbf{a} = \mathbf{o}$. Protože $\operatorname{rank}(\mathbf{X}^T) = 3$, bude mít matice $\mathbf{A}$ dva lineárně nezávislé řádky.

Příklad (pokrač.)

3. Fundamentální systém soustavy $\mathbf{X}^T \cdot \mathbf{a} = \mathbf{o}$, neboli homogenní soustavy

$$\left(\begin{array}{ccccc|c} 2 & 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 & 0 \\ -1 & 2 & 0 & 0 & 1 & 0 \end{array}\right), \text{ je například } \begin{pmatrix} -1/2 \\ -1/4 \\ 5/4 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1/2 \\ -1/4 \\ -3/4 \\ 0 \\ 1 \end{pmatrix}.$$

Užitečný trik:[a] proto je i $4 \cdot \begin{pmatrix} -1/2 \\ -1/4 \\ 5/4 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -2 \\ -1 \\ 5 \\ 4 \\ 0 \end{pmatrix}$, $4 \cdot \begin{pmatrix} 1/2 \\ -1/4 \\ -3/4 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ -3 \\ 0 \\ 4 \end{pmatrix}$

fundamentální systém soustavy $\mathbf{X}^T \cdot \mathbf{a} = \mathbf{o}$.

Můžeme tedy psát: $\mathbf{A} = \begin{pmatrix} -2 & -1 & 5 & 4 & 0 \\ 2 & -1 & -3 & 0 & 4 \end{pmatrix}$.

[a] Fundamentální systém tvoří bázi jádra matice soustavy. A nenulové skalární násobky prvků jakékoli báze opět tvoří bázi.

Příklad (pokrač.)

4. Dopočteme $\mathbf{b}$ z rovnice $\mathbf{A} \cdot \begin{pmatrix} 1 \\ 1 \\ -2 \\ 0 \\ 2 \end{pmatrix} = \mathbf{b}$.

$$\text{Tudíž } \mathbf{b} = \begin{pmatrix} -2 & -1 & 5 & 4 & 0 \\ 2 & -1 & -3 & 0 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ -2 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} -13 \\ 15 \end{pmatrix}.$$

Odpověď: 3-dimensionální afinní podprostor v $\mathbb{R}^5$

$$\begin{pmatrix} 1 \\ 1 \\ -2 \\ 0 \\ 2 \end{pmatrix} + \operatorname{span}\left(\begin{pmatrix} 2 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right)$$

je řešením soustavy $\left(\begin{array}{ccccc|c} -2 & -1 & 5 & 4 & 0 & -13 \\ 2 & -1 & -3 & 0 & 4 & 15 \end{array} \right)$ nad $\mathbb{R}$.

Závěrečné poznámky

1. GEM je sice universální metodou řešení soustav lineárních rovnic, nad $\mathbb{R}$ (nebo $\mathbb{C}$) je však numericky nestabilní.

   V praxi je pro řešení (zvláště velkých) soustav lineárních rovnic nad $\mathbb{R}$ (nebo $\mathbb{C}$) nutno použít jiné metody (například iterační Gaussovu-Seidelovu metodu,[a] a jiné). Tyto metody jsou mimo sylabus standardní přednášky z lineární algebry.

2. Jak řešit soustavy s parametrem? GEM je universální metodou! Při řešení soustav s parametrem pomocí GEM musíme být velmi opatrní na provádění elementárních úprav.

   Pro soustavy se čtvercovou maticí vyvineme později další metodu řešení (kombinaci GEM a Cramerovy věty).

3. Nepovinné: Nad $\mathbb{R}$ lze mít i další geometrický pohled na GEM (tzv. Householderovy reflexe).

[a] Viz Poznámku 6.4.7 skript.

Determinant: část 1

Odpřednesenou látku naleznete v kapitolách 8.1 a 8.2 skript *Abstraktní a konkrétní lineární algebra*.

Minulé přednášky

1. GEM.
2. Regularita a singularita čtvercových matic.

Dnešní přednáška

1. Determinant čtvercové matice: test regularity matice.
   Determinant má ale především geometrický význam.
2. Bude nutné připomenout základní fakta o permutacích.
   Použijeme grafickou notaci pro permutace: strunové diagramy.
3. Základní metody výpočtu determinantu: z definice a pomocí GEM.

Příští přednáška

1. Hlubší poznatky o determinantech.
2. Aplikace determinantu na řešení čtvercových soustav lineárních rovnic.

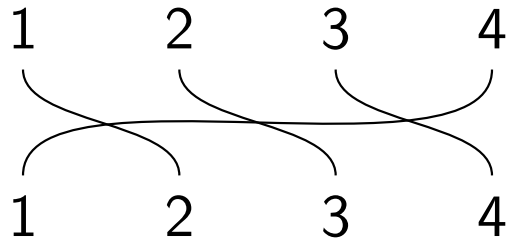
Definice (permutace)

Permutace množiny $\{1, 2, \ldots, n\}$ je jakákoli bijekce $\pi : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Zápisy permutací

1. Výčtem: $\pi : \quad 1 \mapsto 2, \quad 2 \mapsto 3, \quad 3 \mapsto 4, \quad 4 \mapsto 1.$
2. Tabulkou:[a] $\pi = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$
3. Strunovým diagramem:[b]

$\pi =$

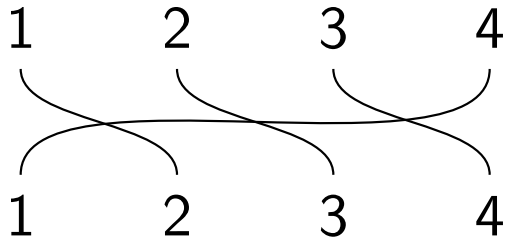


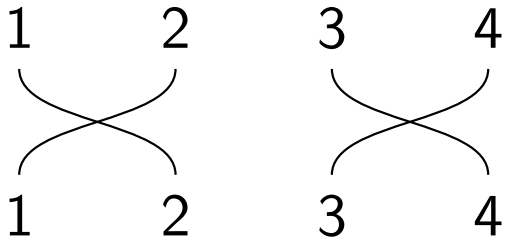
Strunový diagram čteme odshora dolů.

[a] Upozornění: tato tabulka není matice ve smyslu našeho předmětu.
[b] Řešené příklady na strunové diagramy naleznete v kapitole 8.1 skript.

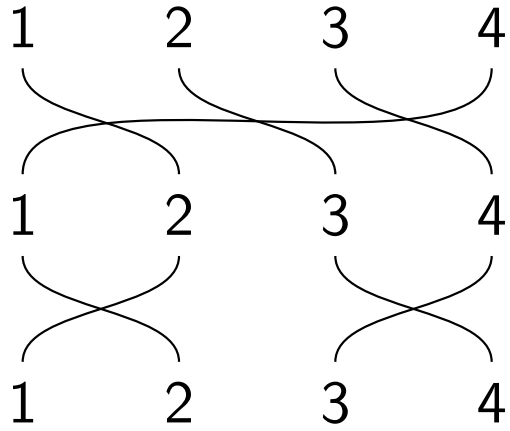
Grafické skládání permutací

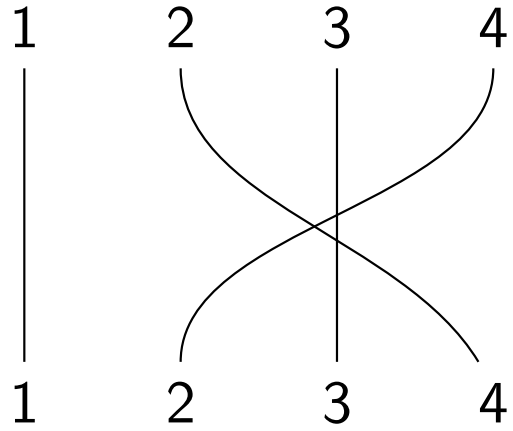
Například:

$\pi =$ 

$\sigma =$ 

Spočteme nejdříve π a potom σ (směrem shora dolů):

$\sigma \cdot \pi =$ 

$=$ 

Definice (symetrická grupa permutací)

Množině všech permutací množiny $\{1, 2, \ldots, n\}$, spolu s výše uvedenou operací skládání $\cdot$, říkáme symetrická grupa permutací n-prvkové množiny. Značení: S_n.

Tvrzení (vlastnosti skládání permutací)

Skládání $\cdot$ v S_n je asociativní, má neutrální prvek (říkáme mu jednotková (také: triviální) permutace, značíme id_n), každá permutace má inversi vzhledem ke skládání $\cdot$ (značení a terminologie: π^{-1} je inversní permutace k permutaci π).

Důkaz.

Plyne okamžitě z vlastností bijekcí. ∎

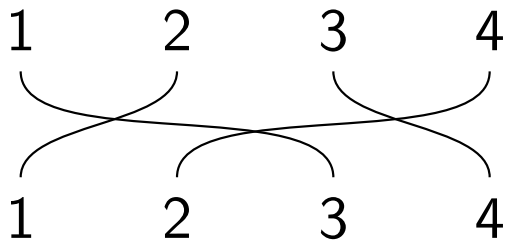
Definice (znaménko permutace)

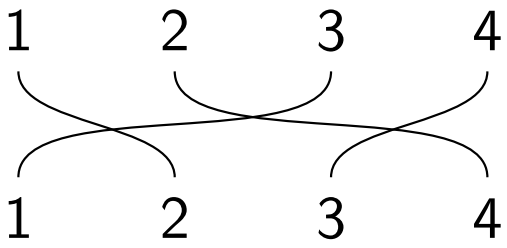
Ať π je permutace množiny $\{1, \ldots, n\}$. Znaménko permutace π je číslo $\operatorname{sign} \pi$, které je definováno takto:

$$\operatorname{sign} \pi = \begin{cases} +1, & \text{pokud strunový diagram } \pi \\ & \text{obsahuje sudý počet překřížení strun} \\ & \text{(v tomto případě říkáme, že } \pi \text{ je sudá permutace),} \\ -1, & \text{pokud strunový diagram } \pi \\ & \text{obsahuje lichý počet překřížení strun} \\ & \text{(v tomto případě říkáme, že } \pi \text{ je lichá permutace).} \end{cases}$$

Příklad

Pro permutace

$\pi =$ 

$\pi^{-1} =$ 

platí: $\operatorname{sign} \pi = -1 = \operatorname{sign}(\pi^{-1})$.

Tvrzení (znaménka speciálních permutací)

1. Pro identickou permutaci id_n v S_n platí $\mathrm{sign}(\mathrm{id}_n) = 1$.
2. Pro libovolné permutace σ a π v S_n platí $\mathrm{sign}(\sigma \cdot \pi) = (\mathrm{sign}\,\sigma) \cdot (\mathrm{sign}\,\pi)$.
3. Ať π je permutace v S_n. Pak platí $\mathrm{sign}\,\pi = \mathrm{sign}(\pi^{-1})$.
4. Ať π je permutace v S_n. Označte jako σ permutaci v S_n vzniklou z π prohozením dvou hodnot. Potom $\mathrm{sign}\,\sigma = -\,\mathrm{sign}\,\pi$.

Důkaz.

Přednáška (strunové diagramy). ∎

Definice (determinant čtvercové matice)

Pro matici $\mathbf{A}$ typu $n \times n$ nad $\mathbb{F}$ definujeme determinant jako skalár

$$\det(\mathbf{A}) = \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{\pi(1),1} \cdot a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n}$$

Často se píše i $|\mathbf{A}|$ místo $\det(\mathbf{A})$.

„Šachový význam“ součinu $a_{\pi(1),1} \cdot a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n}$

1. Ať π je permutace v S_n.
   Pokud na políčka $a_{\pi(1),1}$, $a_{\pi(2),2}$, $\ldots$, $a_{\pi(n),n}$ rozestavíme věže, pak se navzájem neohrožují.[a]
2. Obráceně: n navzájem se neohrožujících věží na „šachovnici“ $(a_{i,j})$ určuje permutaci π v S_n a tím i jeden součin $a_{\pi(1),1} \cdot a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n}$.

[a] Připomenutí: Položka $a_{\pi(j),j}$ matice $\mathbf{A}$ je položka v j-tém sloupci na $\pi(j)$-tém řádku.

Příklad (Sarrusovo pravidlo pro matice 3×3)

Na množině $\{1, 2, 3\}$ existuje přesně šest následujících permutací:

$$\pi_0 = \begin{array}{ccc} 1 & 2 & 3 \\ | & | & | \\ 1 & 2 & 3 \end{array} \qquad \pi_2 = \begin{array}{ccc} 1 & 2 & 3 \\ \diagdown & \diagdown & \diagdown \\ 1 & 2 & 3 \end{array} \qquad \pi_4 = \begin{array}{ccc} 1 & 2 & 3 \\ \diagup & \diagup & \diagdown \\ 1 & 2 & 3 \end{array}$$

$$\pi_1 = \begin{array}{ccc} 1 & 2 & 3 \\ \diagup & \diagdown & | \\ 1 & 2 & 3 \end{array} \qquad \pi_3 = \begin{array}{ccc} 1 & 2 & 3 \\ | & \diagup & \diagdown \\ 1 & 2 & 3 \end{array} \qquad \pi_5 = \begin{array}{ccc} 1 & 2 & 3 \\ \diagup & | & \diagdown \\ 1 & 2 & 3 \end{array}$$

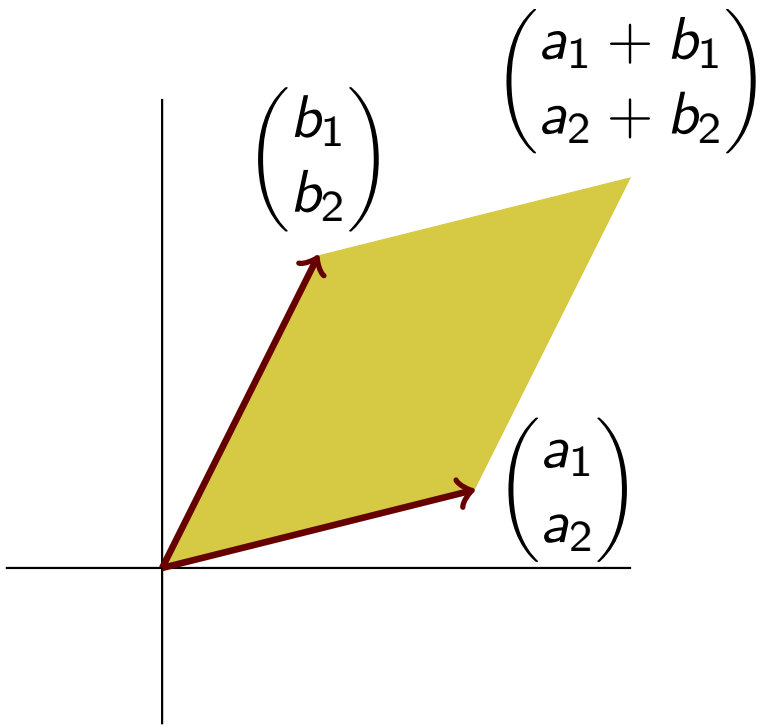
Tudíž:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \cdot a_{22} \cdot a_{33} + a_{21} \cdot a_{32} \cdot a_{13} + a_{31} \cdot a_{12} \cdot a_{23}$$

$$- a_{21} \cdot a_{12} \cdot a_{33} - a_{11} \cdot a_{32} \cdot a_{23} - a_{31} \cdot a_{22} \cdot a_{13}$$

Geometrický význam determinantu matice 2×2 nad $\mathbb{R}$

Determinant $\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}$ je velikost $P(\mathbf{a}, \mathbf{b})$ orientované plochy

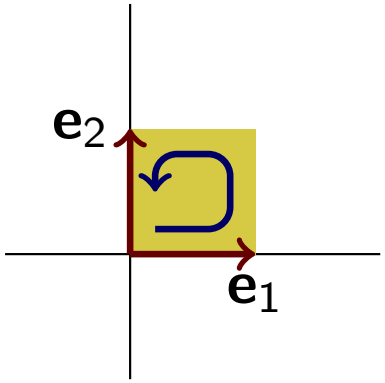


kde $\mathbf{a} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ a $\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$.

Geometrie determinantu (pokrač.)

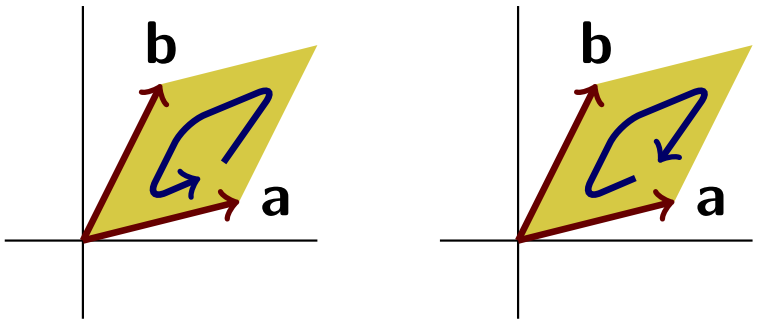
Vlastnosti velikosti $P(\mathbf{a}, \mathbf{b})$ orientované plochy jsou:

1. $P(\mathbf{e}_1, \mathbf{e}_2) = 1$. Tato rovnost zavádí jednotku plochy a orientaci prostoru $\mathbb{R}^2$: při pohybu kolem počátku jsme zvolili směr proti směru hodinových ručiček — první je vektor $\mathbf{e}_1$, vektor $\mathbf{e}_2$ je druhý.



Geometrie determinantu (pokrač.)

2. $P(\mathbf{a}, \mathbf{b}) = -P(\mathbf{b}, \mathbf{a})$. Tato rovnost vystihuje, jak chápeme orientaci velikosti plochy: změnou pořadí vektorů **a**, **b** změníme znaménko velikosti plochy.



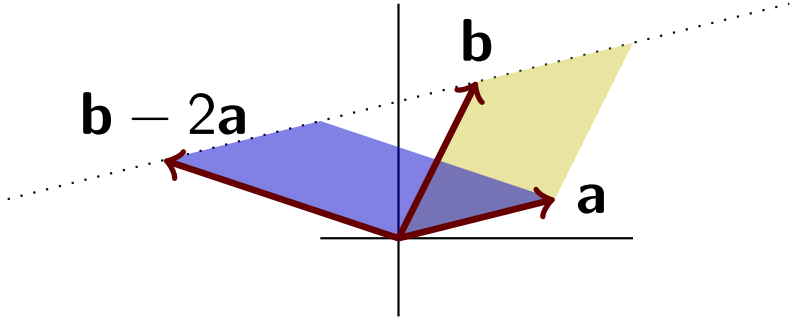
$$P(\mathbf{a}, \mathbf{b}) \quad = \quad -P(\mathbf{b}, \mathbf{a})$$

Geometrie determinantu (pokrač.)

3. Výpočet hodnoty $P(\mathbf{a}, \mathbf{b})$ je lineární v každé položce, tj. pro libovolná reálná čísla a_1, a_2, b_1, b_2 a libovolné vektory $\mathbf{a}$, $\mathbf{b}$, $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{b}_1$, $\mathbf{b}_2$ platí rovnosti

$$\begin{aligned} P(a_1 \cdot \mathbf{a}_1 + a_2 \cdot \mathbf{a}_2, \mathbf{b}) &= a_1 \cdot P(\mathbf{a}_1, \mathbf{b}) + a_2 \cdot P(\mathbf{a}_2, \mathbf{b}) \\ P(\mathbf{a}, b_1 \cdot \mathbf{b}_1 + b_2 \cdot \mathbf{b}_2) &= b_1 \cdot P(\mathbf{a}, \mathbf{b}_1) + b_2 \cdot P(\mathbf{a}, \mathbf{b}_2) \end{aligned}$$

Důležitý důsledek: platí rovnosti $P(\mathbf{a}, \mathbf{b}) = P(\mathbf{a}, \mathbf{b} + a \cdot \mathbf{a})$ a $P(\mathbf{a}, \mathbf{b}) = P(\mathbf{a} + b \cdot \mathbf{b}, \mathbf{b})$ pro a, b reálná.
Například:



$$P(\mathbf{a}, \mathbf{b}) = P(\mathbf{a}, \mathbf{b} - 2\mathbf{a})$$

Zobecnění (geometrický význam determinantu)

Determinant $\det(\mathbf{A})$ matice $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_n)$ typu $n \times n$ nad $\mathbb{F}$ je velikost $V(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ orientovaného objemu rovnoběžnostěnu v prostoru $\mathbb{F}^n$. Rovnoběžnostěn je určen vektory $\mathbf{a}_1, \ldots, \mathbf{a}_n$ (v tomto pořadí).

Platí:

1. $V(\mathbf{e}_1, \ldots, \mathbf{e}_n) = 1$.
2. $V(\mathbf{a}_1, \ldots, \mathbf{a}_n) = \operatorname{sign} \pi \cdot V(\mathbf{a}_{\pi(1)}, \ldots, \mathbf{a}_{\pi(n)})$, kde π je libovolná permutace v S_n.
3. $V(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ je lineární v každé souřadnici zvlášť.

Výše uvedené tři vlastnosti funkce

$$V : \underbrace{\mathbb{F}^n \times \cdots \times \mathbb{F}^n}_{n\text{-krát}} \to \mathbb{F}$$

určují pojem determinantu jednoznačně.

Tvrzení (determinant transponované matice)

Platí: $\det(\mathbf{A}) = \det(\mathbf{A}^T)$.

Důkaz.

$$\begin{aligned}
\det(\mathbf{A}) &= \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{\pi(1),1} \cdot a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n} \\
&= \sum_{\pi^{-1} \in S_n} \operatorname{sign} \pi^{-1} \cdot a_{1,\pi^{-1}(1)} \cdot a_{2,\pi^{-1}(2)} \cdot \ldots \cdot a_{n,\pi^{-1}(n)} \\
&= \sum_{\pi \in S_n} \operatorname{sign} \pi \cdot a_{1,\pi(1)} \cdot a_{2,\pi(2)} \cdot \ldots \cdot a_{n,\pi(n)} \\
&= \det(\mathbf{A}^T)
\end{aligned}$$

Využili jsme jednoduchého faktu: platí rovnosti
$\{\pi \mid \pi \in S_n\} = S_n = \{\pi^{-1} \mid \pi \in S_n\}$. ■

Důsledky (výpočet determinantu a GEM)

1. Prohození dvou řádků mění znaménko determinantu.
2. Vynásobení jednoho řádku nenulovým skalárem a změní determinant a-krát.
3. Přičtení lineární kombinace ostatních řádků k řádku nezmění hodnotu determinantu.

Tvrzení (determinant horní trojúhelníkové matice)

Ať $\mathbf{A}$ je horní trojúhelníková matice. Potom $\det(\mathbf{A})$ = součin prvků na hlavní diagonále matice.

Důsledek (opatrný výpočet determinantu pomocí GEM)

$\det(\mathbf{A})$ lze počítat pomocí GEM: je nutné si ovšem poznamenat typy úprav (a tudíž i případné změny hodnoty determinantu).

Příklad (výpočet determinantu pomocí GEM)

$$\begin{vmatrix} 2 & 3 & 1 \\ 3 & 1 & 4 \\ -2 & 16 & 3 \end{vmatrix} = -\frac{1}{2}\begin{vmatrix} 2 & 3 & 1 \\ -6 & -2 & -8 \\ -2 & 16 & 3 \end{vmatrix}\begin{matrix} R_1 \\ -2R_2 \\ R_3 \end{matrix} =$$

$$= -\frac{1}{2}\begin{vmatrix} 2 & 3 & 1 \\ 0 & 7 & -5 \\ 0 & 19 & 4 \end{vmatrix}\begin{matrix} R_1 \\ R_2 + 3R_1 \\ R_3 + R_1 \end{matrix} =$$

$$= \frac{1}{2}\cdot\frac{1}{7}\begin{vmatrix} 2 & 3 & 1 \\ 0 & 7 & -5 \\ 0 & -133 & -28 \end{vmatrix}\begin{matrix} R_1 \\ R_2 \\ -7R_3 \end{matrix} =$$

$$= \frac{1}{2}\cdot\frac{1}{7}\begin{vmatrix} 2 & 3 & 1 \\ 0 & 7 & -5 \\ 0 & 0 & -123 \end{vmatrix}\begin{matrix} R_1 \\ R_2 \\ R_3 + 19R_2 \end{matrix} =$$

$$= \frac{2\cdot 7\cdot(-123)}{2\cdot 7} = -123$$

Věta (invertibilita matice pomocí determinantu)

Pro matici $\mathbf{A}$ typu $n \times n$ nad $\mathbb{F}$ platí: $\mathbf{A}$ je regulární právě tehdy, když $\det(\mathbf{A}) \neq 0$.

Důkaz.

Bez důkazu (viz např. Důsledek 8.4.4 skript). ■

Poznámky k výpočtu $\det(\mathbf{A})$

1. Výpočet z definice: časově náročný. Je zapotřebí se vyznat v S_n (má $n!$ prvků).
2. Výpočet pomocí GEM: méně náročný (řádově n^3 kroků). Pozor! Nad $\mathbb{R}$ a $\mathbb{C}$ je GEM numericky nestabilní. Navíc (při ručním výpočtu) je zapotřebí GEM provádět opatrně.
3. Jiný způsob výpočtu? Ano: rozvoj podle řádku nebo sloupce (rekursivní výpočet). Příště.

Jiný způsob zavedení determinantu (nepovinné)

Determinant lze zavést pomocí vnější mocniny[a] lineárního prostoru, viz kapitolu 5 skript.

Výhody tohoto přístupu:

1. Okamžitý geometrický vhled do pojmu determinant a snadné důkazy vlastností determinantu.
2. Determinant je možno počítat pro libovolná lineární zobrazení, ne jen pro matice.
3. Pojem vnější mocniny vede rychle ke geometrické algebře, která umožňuje elegantní a rychlé výpočty v počítačové grafice, viz například knihu

   L. Dorst, D. Fontijne, S. Mann, *Geometric algebra for Computer Science*, Elsevier, 2007

[a] Na první pohled myšlenka vnější mocniny vypadá velmi divoce. Tato myšlenka je ale velmi přirozená a je stejně stará jako lineární algebra: v roce 1844 s ní přišel Hermann Grassmann (1808–1887).

Determinant, část 2

Odpřednesenou látku naleznete v kapitolách 8.3 a 8.4 skript *Abstraktní a konkrétní lineární algebra*.

Minulá přednáška

1. Definice determinantu čtvercové matice (s použitím permutací).
2. Základní metody výpočtu determinantu:
   1. Z definice: nutnost znalosti S_n.
   2. Pomocí GEM: nutnost opatrného provádění GEM.
3. Čtvercová matice $\mathbf{A}$ je regulární právě tehdy, když $\det(\mathbf{A}) \neq 0$.

Dnešní přednáška

1. Věta o rozvoji determinantu podle sloupce.[a]
2. Hlubší poznatky o determinantu.
3. Aplikace determinantu na řešení čtvercových soustav lineárních rovnic (Cramerova věta). Ukážeme geometrický význam Cramerovy věty.

[a] Víme: $\det(\mathbf{A}^T) = \det(\mathbf{A})$. Takže determinant půjde rozvíjet i podle řádku.

Připomenutí

Determinant $\det(\mathbf{A})$ čtvercové matice $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_n)$ je lineární v každém sloupci. Speciálně: protože $\mathbf{a}_j = \sum_{i=1}^{n} a_{ij} \cdot \mathbf{e}_i$ (kde $\mathbf{a}_j$ je j-tý sloupec matice $\mathbf{A}$), platí rovnost:[a]

$$\det(\mathbf{A}) = \sum_{i=1}^{n} a_{ij} \cdot \underbrace{\det(\mathbf{a}_1, \ldots, \mathbf{a}_{j-1}, \mathbf{e}_i, \mathbf{a}_{j+1}, \ldots, \mathbf{a}_n)}_{\text{Značení: } A_{ij}.}$$

Například (zvolili jsme $j = 2$, tj. rozvíjíme podle druhého sloupce):

$$\begin{vmatrix} -2 & 4 & 5 \\ 3 & 6 & 7 \\ 7 & -2 & 5 \end{vmatrix} = 4 \cdot \underbrace{\begin{vmatrix} -2 & 1 & 5 \\ 3 & 0 & 7 \\ 7 & 0 & 5 \end{vmatrix}}_{A_{12}} + 6 \cdot \underbrace{\begin{vmatrix} -2 & 0 & 5 \\ 3 & 1 & 7 \\ 7 & 0 & 5 \end{vmatrix}}_{A_{22}} - 2 \cdot \underbrace{\begin{vmatrix} -2 & 0 & 5 \\ 3 & 0 & 7 \\ 7 & 1 & 5 \end{vmatrix}}_{A_{32}}$$

[a] Této rovnosti se říká (Laplaceův) rozvoj determinantu podle j-tého sloupce.

Definice

Determinantu $A_{ij} = \det(\mathbf{a}_1, \ldots, \mathbf{a}_{j-1}, \mathbf{e}_i, \mathbf{a}_{j+1}, \ldots, \mathbf{a}_n)$ říkáme algebraický doplněk posice (i, j) v matici $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_n)$.

Věta (praktický výpočet algebraického doplňku)

Ať $\mathbf{A}$ je matice typu $n \times n$ nad $\mathbb{F}$, $n \geq 2$. Označme jako $\mathbf{A}_{ij}$ matici typu $(n-1) \times (n-1)$ vzniklou z matice $\mathbf{A}$ vynecháním i-tého řádku a j-tého sloupce. Potom[a] $A_{ij} = (-1)^{i+j} \cdot \det(\mathbf{A}_{ij})$.

[a] Pozor: nezapomeňte na znaménko posice (i, j): $A_{ij} = (-1)^{i+j} \cdot \det(\mathbf{A}_{ij})$.

Důkaz.

Bez důkazu (viz např. Lemma 8.3.4 ve skriptech). ■

Pozorování

Rozvoj determinantu podle sloupce umožňuje rekursivní výpočet determinantu! Důvod: pro $\mathbf{A}$ typu $n \times n$ jsou algebraické doplňky jedotlivých posic determinanty matic typu $(n-1) \times (n-1)$.

Příklad (determinant rozvojem podle třetího sloupce)

$$\begin{vmatrix} 1 & 2 & 0 & 1 \\ 2 & 7 & 6 & 3 \\ 5 & 2 & 0 & 3 \\ 3 & 2 & 5 & 1 \end{vmatrix} = 0 \cdot \underbrace{(-1)^{1+3} \cdot \begin{vmatrix} 2 & 7 & 3 \\ 5 & 2 & 3 \\ 3 & 2 & 1 \end{vmatrix}}_{A_{13}}$$

$$+ 6 \cdot \underbrace{(-1)^{2+3} \cdot \begin{vmatrix} 1 & 2 & 1 \\ 5 & 2 & 3 \\ 3 & 2 & 1 \end{vmatrix}}_{A_{23}}$$

$$+ 0 \cdot \underbrace{(-1)^{3+3} \cdot \begin{vmatrix} 1 & 2 & 1 \\ 2 & 7 & 3 \\ 3 & 2 & 1 \end{vmatrix}}_{A_{33}}$$

$$+ 5 \cdot \underbrace{(-1)^{4+3} \cdot \begin{vmatrix} 1 & 2 & 1 \\ 2 & 7 & 3 \\ 5 & 2 & 3 \end{vmatrix}}_{A_{43}}$$

Poznámky k výpočtu determinantu rozvojem podle sloupce

1. Protože $\det(\mathbf{A}) = \det(\mathbf{A}^T)$, lze determinant počítat i rozvojem podle řádku.
2. Rekursivní výpočet determinantu (tj. výpočet rozvojem podle sloupce nebo řádku) má složitost $n!$ — je tudíž obecně výpočetně pomalý.
3. Výpočet determinantu rozvojem je vhodný pro řídké matice (matice, obsahující hodně nul).

Definice (adjungovaná matice)

Pro matici $\mathbf{A}$ typu $n \times n$ je její adjungovaná matice $\mathrm{adj}(\mathbf{A})$ transponovaná matice algebraických doplňků posic v matici $\mathbf{A}$.

Příklad (nad $\mathbb{R}$)

Pro $\mathbf{A} = \begin{pmatrix} 2 & 7 \\ 5 & 3 \end{pmatrix}$ je $\mathrm{adj}(\mathbf{A}) = \begin{pmatrix} 3 & -7 \\ -5 & 2 \end{pmatrix}$.

Cramerova věta (o vztahu matice a adjungované matice)

Ať $\mathbf{A}$ je matice typu $n \times n$ nad $\mathbb{F}$, $n \geq 2$. Potom platí rovnosti:

$$\mathbf{A} \cdot \mathrm{adj}(\mathbf{A}) = \det(\mathbf{A}) \cdot \mathbf{E}_n = \mathrm{adj}(\mathbf{A}) \cdot \mathbf{A}$$

Pro regulární $\mathbf{A}$ tedy platí $\mathbf{A}^{-1} = \det(\mathbf{A})^{-1} \cdot \mathrm{adj}(\mathbf{A})$.

Důkaz.

1. Každý prvek na hlavní diagonále matice $\mathbf{A} \cdot \mathrm{adj}(\mathbf{A})$ má hodnotu $\det(\mathbf{A})$. To plyne z rozvoje determinantu podle sloupce.
2. Každý prvek mimo hlavní diagonálu matice $\mathbf{A} \cdot \mathrm{adj}(\mathbf{A})$ má hodnotu 0. To plyne z rozvoje determinantu, aplikovaného na matici se dvěma stejnými řádky.

Tudíž $\mathbf{A} \cdot \mathrm{adj}(\mathbf{A}) = \det(\mathbf{A}) \cdot \mathbf{E}_n$. Druhá rovnost se dokáže analogicky. ∎

Příklad (inverse pomocí adjungované matice)

Pro $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 7 \\ 4 & 2 & 1 \end{pmatrix}$ nad $\mathbb{R}$ je $\det(\mathbf{A}) = 6$. Víme, že inverse matice $\mathbf{A}$ existuje.

1. Matice algebraických doplňků posic v matici $\mathbf{A}$ je $\begin{pmatrix} -10 & 26 & -12 \\ 4 & -11 & 6 \\ 2 & -1 & 0 \end{pmatrix}$.

   Proto $\operatorname{adj}(\mathbf{A}) = \begin{pmatrix} -10 & 26 & -12 \\ 4 & -11 & 6 \\ 2 & -1 & 0 \end{pmatrix}^T = \begin{pmatrix} -10 & 4 & 2 \\ 26 & -11 & -1 \\ -12 & 6 & 0 \end{pmatrix}$.

2. Celkově $\mathbf{A}^{-1} = 6^{-1} \cdot \begin{pmatrix} -10 & 4 & 2 \\ 26 & -11 & -1 \\ -12 & 6 & 0 \end{pmatrix}$.

Doporučení (sanity check)

Při výpočtu $\operatorname{adj}(\mathbf{A})$ je možná rozumné nejprve spočítat matici algebraických doplňků a potom ji transponovat.

Výhodnost a vhodnost výpočtu $\mathbf{A}^{-1}$ pomocí $\mathrm{adj}(\mathbf{A})$

1. Pro obecné (velké) matice je výpočet nevýhodný. Vyžaduje spočítat velké množství determinantů.
2. Pro velké a řídké matice (tj. pro matice obsahující velké množství nulových položek) může jít o výhodný výpočet.
3. Výpočet je výhodný pro matice typu 2×2.
   Ať $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ je regulární (tj., ať $\det(\mathbf{A}) = ad - bc \neq 0$).
   Potom
   $$\mathbf{A}^{-1} = (ad-bc)^{-1} \cdot \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}^T = (ad-bc)^{-1} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$
4. Poznámka: některé aplikace (například v kryptografii) vyžadují práci s maticemi nad ještě obecnější strukturou než je těleso. Pak je výpočet $\mathbf{A}^{-1}$ pomocí $\mathrm{adj}(\mathbf{A})$ často jediná možnost.

Věta (základní strukturální vlastnosti determinantu)

Funkce det : $\underbrace{\mathbb{F}^n \times \ldots \mathbb{F}^n}_{n\text{-krát}} \to \mathbb{F}$ má následující vlastnosti:

1. $\det(\mathbf{E}_n) = 1$.
2. $\det(\mathbf{B} \cdot \mathbf{A}) = \det(\mathbf{B}) \cdot \det(\mathbf{A})$.
3. Pro regulární $\mathbf{A}$ je $\det(\mathbf{A}^{-1}) = (\det(\mathbf{A}))^{-1}$.
4. $\det(a \cdot \mathbf{A}) = a^n \cdot \det(\mathbf{A})$, kde a je libovolný skalár.[a]

[a] Pozor: rovnost $\det(\mathbf{A} + \mathbf{B}) = \det(\mathbf{A}) + \det(\mathbf{B})$ obecně neplatí.

Důkaz.

1. Víme z minulé přednášky.
2. Bez důkazu (viz např. Tvrzení 8.2.19 ve skriptech).
3. Pro regulární $\mathbf{A}$ platí rovnosti
   $1 = \det(\mathbf{E}_n) = \det(\mathbf{A} \cdot \mathbf{A}^{-1}) = \det(\mathbf{A}) \cdot \det(\mathbf{A}^{-1})$.
   Takže $\det(\mathbf{A}^{-1}) = (\det(\mathbf{A}))^{-1}$.
4. Plyne z toho, že determinant je v každém sloupci lineární.

Definice (soustava se čtvercovou maticí)

Rovnici $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$, kde $\mathbf{A}$ je matice typu $n \times n$ nad $\mathbb{F}$, říkáme soustava se čtvercovou maticí.

Tvrzení (řešení čtvercové soustavy s regulární maticí)

Ať $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$ je soustava se čtvercovou maticí. Tato soustava má jediné řešení právě tehdy, když $\mathbf{A}$ je regulární matice. V tomto případě je toto jediné řešení tvaru $\mathbf{A}^{-1} \cdot \mathbf{b}$.

Důkaz.

Regularita matice $\mathbf{A}$ znamená přesně to, že $\mathbf{A} : \mathbb{F}^n \to \mathbb{F}^n$ je isomorfismus. To znamená přesně to, že pro každé $\mathbf{b}$ existuje právě jedno $\mathbf{x}$ takové, že $\mathbf{A} : \mathbf{x} \mapsto \mathbf{b}$, neboli $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$. ■

Cramerova věta o řešení regulárních soustav (také: Cramerovo pravidlo pro řešení regulárních soustav)

Ať $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$ je soustava se čtvercovou regulární maticí nad $\mathbb{F}$.
Potom j-tá položka jediného řešení $\mathbf{x} = \mathbf{A}^{-1} \cdot \mathbf{b}$ je tvaru

$$x_j = \det(\mathbf{A})^{-1} \cdot \det(\mathbf{a}_1, \ldots, \mathbf{a}_{j-1}, \mathbf{b}, \mathbf{a}_{j+1}, \ldots, \mathbf{a}_n)$$

Důkaz.

Víme: $\mathbf{x} = \mathbf{A}^{-1} \cdot \mathbf{b} = \det(\mathbf{A})^{-1} \cdot \mathrm{adj}(\mathbf{A}) \cdot \mathbf{b}$. Takže

$$\det(\mathbf{A}) \cdot \mathbf{x} = \mathrm{adj}(\mathbf{A}) \cdot \mathbf{b}$$

Proto $\det(\mathbf{A}) \cdot x_j$ je součin j-tého řádku matice $\mathrm{adj}(\mathbf{A})$ se sloupcem $\mathbf{b}$.
Ten součin je roven $\det(\mathbf{a}_1, \ldots, \mathbf{a}_{j-1}, \mathbf{b}, \mathbf{a}_{j+1}, \ldots, \mathbf{a}_n)$. ■

Příklad (použití Cramerovy věty)

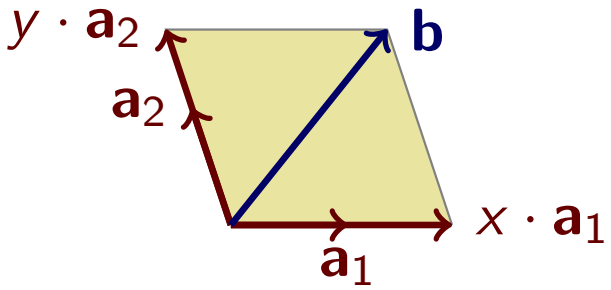
Pro soustavu $\left(\begin{array}{cc|c} 2 & 4 & 1 \\ -3 & 5 & 6 \end{array}\right)$ nad $\mathbb{R}$ platí $\begin{vmatrix} 2 & 4 \\ -3 & 5 \end{vmatrix} = 22 \neq 0$. Lze tedy použít Cramerovu větu:

1. První položka jediného řešení je: $\dfrac{\begin{vmatrix} 1 & 4 \\ 6 & 5 \end{vmatrix}}{\begin{vmatrix} 2 & 4 \\ -3 & 5 \end{vmatrix}} = \dfrac{-19}{22}$.
2. Druhá položka jediného řešení je: $\dfrac{\begin{vmatrix} 2 & 1 \\ -3 & 6 \end{vmatrix}}{\begin{vmatrix} 2 & 4 \\ -3 & 5 \end{vmatrix}} = \dfrac{15}{22}$.

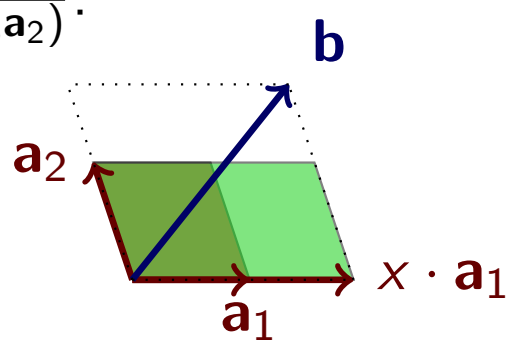
Jediné řešení: $\begin{pmatrix} \dfrac{-19}{22} \\ \\ \dfrac{15}{22} \end{pmatrix}$.

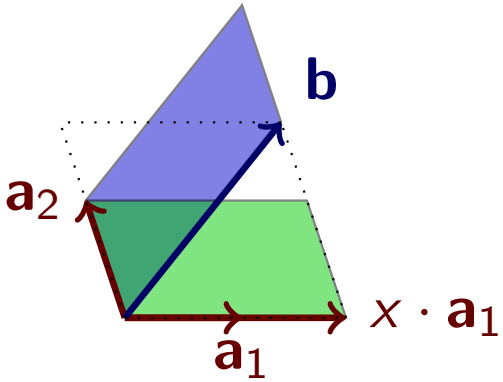
Geometrie Cramerovy věty pro soustavy 2×2 nad $\mathbb{R}$

Pro regulární soustavu $(\mathbf{a}_1, \mathbf{a}_2 \mid \mathbf{b})$ platí podle Cramerovy věty $\frac{\det(\mathbf{b},\mathbf{a}_2)}{\det(\mathbf{a}_1,\mathbf{a}_2)} \cdot \mathbf{a}_1 + \frac{\det(\mathbf{a}_1,\mathbf{b})}{\det(\mathbf{a}_1,\mathbf{a}_2)} \cdot \mathbf{a}_2 = \mathbf{b}$. Co to opravdu znamená?[a]



Ale $x \cdot \det(\mathbf{a}_1, \mathbf{a}_2) = \det(x \cdot \mathbf{a}_1, \mathbf{a}_2) = \det(\mathbf{b}, \mathbf{a}_2)$, takže platí $x = \frac{\det(\mathbf{b},\mathbf{a}_2)}{\det(\mathbf{a}_1,\mathbf{a}_2)}$:





Podobnou úvahu lze provést pro $y = \frac{\det(\mathbf{a}_1,\mathbf{b})}{\det(\mathbf{a}_1,\mathbf{a}_2)}$.

[a] Analogicky lze postupovat pro regulární soustavy větších rozměrů a nad libovolným tělesem (musíme ovšem kreslit rovnoběžnostěny).

Příklad (vyřešte nad $\mathbb{R}$, $p \in \mathbb{R}$ je parametr)

$$(\mathbf{A} \mid \mathbf{b}) = \left(\begin{array}{ccc|c} 2 & -p & -1 & 3 \\ 1 & -7 & -5 & 0 \\ -1 & 3 & p & -1 \end{array}\right), \det(\mathbf{A}) = (p-2)\cdot(p-17).$$

1. $\det(\mathbf{A}) \neq 0$ právě tehdy, když $p \notin \{2, 17\}$.
   V tomto případě existuje jediné řešení. Toto jediné řešení lze nalézt pomocí GEM nebo pomocí Cramerovy věty.

   Řešení: $\begin{pmatrix} \dfrac{26}{17-p} \\ \dfrac{3}{17-p} \\ \dfrac{1}{17-p} \end{pmatrix}$, $p \notin \{2, 17\}$.

Příklad (pokrač.)

2. $p = 2$. Řešíme soustavu $\left(\begin{array}{rrr|r} 2 & -2 & -1 & 3 \\ 1 & -7 & -5 & 0 \\ -1 & 3 & 2 & -1 \end{array}\right)$.

   Řešení: $\begin{pmatrix} \frac{5}{3} \\ 0 \\ \frac{1}{3} \end{pmatrix} + \operatorname{span}(\begin{pmatrix} 1 \\ 3 \\ -4 \end{pmatrix})$, pro $p = 2$.

3. $p = 17$. Řešíme soustavu $\left(\begin{array}{rrr|r} 2 & -17 & -1 & 3 \\ 1 & -7 & -5 & 0 \\ -1 & 3 & 17 & -1 \end{array}\right)$.

   Řešení pro $p = 17$ neexistuje (Frobeniova věta).

Doporučení

Pro čtvercové soustavy s parametrem doporučujeme použít kombinaci Cramerovy věty a GEM. Výpočet pak má dvě fáze:

1. Cramerova věta pro ty parametry, pro které je matice soustavy regulární.
2. GEM pro ty parametry, pro které je matice soustavy singulární.

Vlastní hodnoty a vlastní vektory

Odpřednesenou látku naleznete v kapitolách 10.1, 10.3 a 10.4 skript *Abstraktní a konkrétní lineární algebra*.

Minulé přednášky

1. Matice lineárních zobrazení mezi prostory konečných dimensí.
2. Matice transformace souřadnic.

Dnešní přednáška

1. Budeme studovat obecná lineární zobrazení $\mathbf{f} : L \to L$, kde L má konečnou dimensi.
   Zjistíme, pro které vektory $\vec{x}$ platí $\mathbf{f}(\vec{x}) = \lambda \cdot \vec{x}$ (tzv homotetie — to je to nejjednodušší lineární zobrazení z L do L).
2. Budeme se snažit změnit bázi L tak, aby ve směrech vektorů nové báze bylo zobrazení $\mathbf{f} : L \to L$ homotetií (obecně pro každý směr různou). Ne vždy to půjde.

Příští přednáška

1. Diagonalisace matic nad $\mathbb{R}$ a nad $\mathbb{C}$.
2. Dvě aplikace diagonalisace: řešení rekurentních rovnic a funkce matic.[a]

[a] Tyto dvě aplikace nebudou zkoušeny!

Příklad (equilibrium stochastických procesů)

Pro matici $\mathbf{A} = \begin{pmatrix} 0.3 & 0.7 \\ 0.8 & 0.2 \end{pmatrix}$ nalezněte alespoň jeden nenulový vektor $\mathbf{q}$ tak, aby platila rovnost[a] $\mathbf{A} \cdot \mathbf{q} = \mathbf{q}$.

To je snadné: $\begin{pmatrix} 0.3 & 0.7 \\ 0.8 & 0.2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, protože řádkové součty matice $\mathbf{A}$ jsou 1. Tudíž $\mathbf{q} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

[a] Stejnou (ale komplikovaněji zadanou) úlohu řeší algoritmus `PageRank`, viz například K. Bryan a A. Leise, The $ 25,000,000,000 eigenvector: The linear algebra behind Google, *SIAM Rev.* 48.3 (2006), 569–581, nebo Dodatek F skript.

Co dělat pro obecnou matici A?

Měli jsme štěstí („hezký“ tvar matice $\mathbf{A}$, takovým maticím se říká řádkově stochastické). Jak ale postupovat pro obecnou matici $\mathbf{A}$?

Příklad (equilibrium stochastických procesů, znovu a jinak)

Pro matici $\mathbf{A} = \begin{pmatrix} 0.3 & 0.7 \\ 0.8 & 0.2 \end{pmatrix}$ nalezneme všechna nenulová řešení všech soustav tvaru $\mathbf{A} \cdot \mathbf{x} = \lambda \cdot \mathbf{x}$, kde $\lambda \in \mathbb{R}$ je neznámé.

Přepsáním soustavy $\mathbf{A} \cdot \mathbf{x} = \lambda \cdot \mathbf{x}$ na $(\mathbf{A} - \lambda \cdot \mathbf{E}_2) \cdot \mathbf{x} = \mathbf{o}$ zjistíme, co je třeba udělat:

1. Matice $\mathbf{A} - \lambda \cdot \mathbf{E}_2$ musí být singulární. Jedině tehdy bude mít rovnice $(\mathbf{A} - \lambda \cdot \mathbf{E}_2) \cdot \mathbf{x} = \mathbf{o}$ nenulové řešení.

   To jest: hledáme všechna λ taková, aby $\det(\mathbf{A} - \lambda \cdot \mathbf{E}_2) = 0$.

   To znamená vyřešit rovnici $\det(\mathbf{A} - x \cdot \mathbf{E}_2) = 0$.
2. Pro konkrétní hodnoty λ nalezneme nenulové řešení soustavy $(\mathbf{A} - \lambda \cdot \mathbf{E}_2) \cdot \mathbf{x} = \mathbf{o}$ pomocí GEM.

Příklad (equilibrium stochastických procesů, pokrač.)

$$\det(\mathbf{A}-x\cdot\mathbf{E}_2) = \begin{vmatrix} 0.3-x & 0.7 \\ 0.8 & 0.2-x \end{vmatrix} = (0.3-x)\cdot(0.2-x)-0.56 =$$
$$= x^2 - 0.5x - 0.5 = (x-1)\cdot(x+0.5) = 0.$$

Soustava $(\mathbf{A} - x\cdot\mathbf{E}_2)\cdot\mathbf{x} = \mathbf{o}$ pro

1. $x = 1$ má tvar $\left(\begin{array}{cc|c} -0.7 & 0.7 & 0 \\ 0.8 & -0.8 & 0 \end{array}\right)$ a řešení[a] $\mathrm{span}(\begin{pmatrix} 1 \\ 1 \end{pmatrix})$.

   To znamená: $\mathbf{A}\cdot\mathbf{x} = \mathbf{x}$ pro všechna $\mathbf{x}$ ze $\mathrm{span}(\begin{pmatrix} 1 \\ 1 \end{pmatrix})$.

2. $x = -0.5$ má tvar $\left(\begin{array}{cc|c} 0.8 & 0.7 & 0 \\ 0.8 & 0.7 & 0 \end{array}\right)$ a řešení[b] $\mathrm{span}(\begin{pmatrix} -7 \\ 8 \end{pmatrix})$.

   To znamená: $\mathbf{A}\cdot\mathbf{x} = -0.5\cdot\mathbf{x}$ pro všechna $\mathbf{x}$ ze $\mathrm{span}(\begin{pmatrix} -7 \\ 8 \end{pmatrix})$.

[a] To jsme již věděli.
[b] To je nová informace.

Příklad (equilibrium stochastických procesů, pokrač.)

Co jsme se vlastně dozvěděli a k čemu je to dobré?

1. V souřadnicovém systému $B = \left(\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}-7\\8\end{pmatrix}\right)$ se matice $\mathbf{A}$ stane diagonální maticí $D(1;-0.5) = \begin{pmatrix}1 & 0\\0 & -0.5\end{pmatrix}$.

   Opravdu:

$$\underbrace{\begin{pmatrix}1 & -7\\1 & 8\end{pmatrix}}_{\mathbf{T}_{B\mapsto K_2}} \cdot \underbrace{\begin{pmatrix}1 & 0\\0 & -0.5\end{pmatrix}}_{D(1;-0.5)} = \begin{pmatrix}1 & 3.5\\1 & -4\end{pmatrix} = \underbrace{\begin{pmatrix}0.3 & 0.7\\0.8 & 0.2\end{pmatrix}}_{\mathbf{A}} \cdot \underbrace{\begin{pmatrix}1 & -7\\1 & 8\end{pmatrix}}_{\mathbf{T}_{B\mapsto K_2}}$$

   tudíž

$$\underbrace{\begin{pmatrix}1 & 0\\0 & -0.5\end{pmatrix}}_{D(1;-0.5)} = \underbrace{\begin{pmatrix}1 & -7\\1 & 8\end{pmatrix}^{-1}}_{\mathbf{T}_{K_2\mapsto B}} \cdot \underbrace{\begin{pmatrix}0.3 & 0.7\\0.8 & 0.2\end{pmatrix}}_{\mathbf{A}} \cdot \underbrace{\begin{pmatrix}1 & -7\\1 & 8\end{pmatrix}}_{\mathbf{T}_{B\mapsto K_2}}$$

Příklad (equilibrium stochastických procesů, pokrač.)

2. Díky předchozímu vidíme, že zadáme-li rekurentní proces

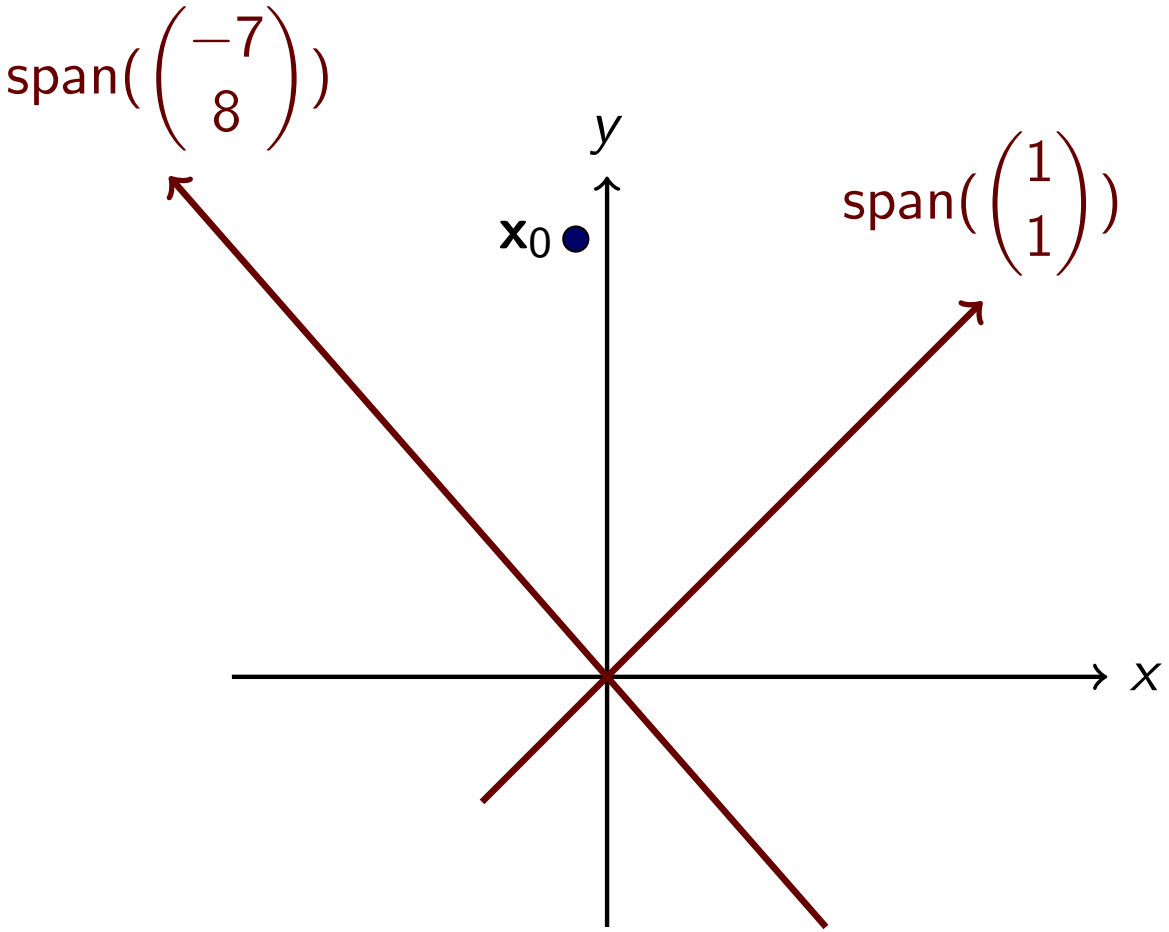
$$\mathbf{x}_0 \text{ libovolný vektor z } \mathbb{R}^2, \quad \mathbf{A} \cdot \mathbf{x}_k = \mathbf{x}_{k+1}, \ k \geq 0,$$

pak se posloupnost vektorů $\mathbf{x}_0$, $\mathbf{x}_1$, $\mathbf{x}_2$, ... chová následovně:

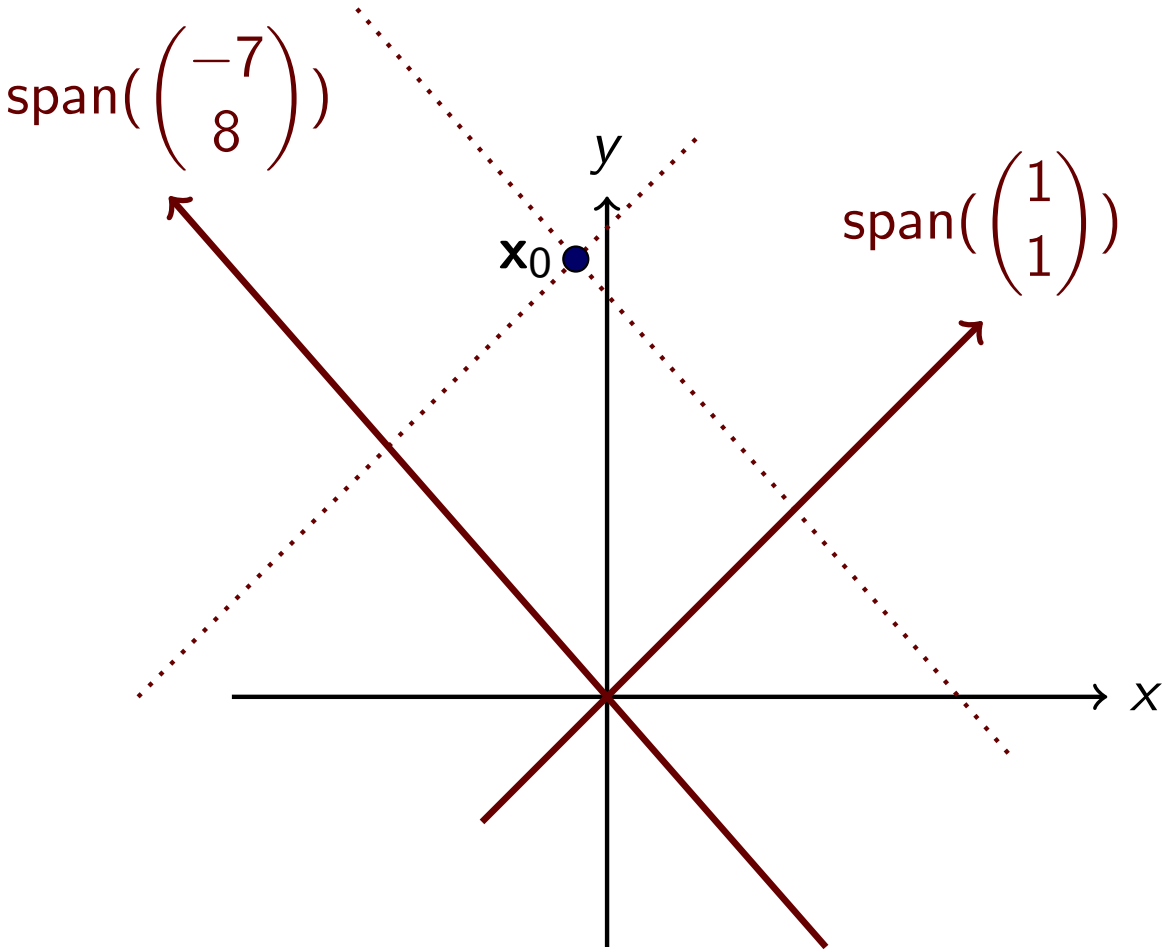
1. Je-li $\mathbf{x}_0$ na přímce $\mathrm{span}(\begin{pmatrix} 1 \\ 1 \end{pmatrix})$, jde o posloupnost $\mathbf{x}_0$, $\mathbf{x}_0$, $\mathbf{x}_0$, ...
2. Je-li $\mathbf{x}_0$ na přímce $\mathrm{span}(\begin{pmatrix} -7 \\ 8 \end{pmatrix})$, jde o posloupnost $\mathbf{x}_0$, $-0.5 \cdot \mathbf{x}_0$, $(-0.5)^2 \cdot \mathbf{x}_0$, $(-0.5)^3 \cdot \mathbf{x}_0$, ...
3. Je-li $\mathbf{x}_0 = a \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + b \cdot \begin{pmatrix} -7 \\ 8 \end{pmatrix}$, tedy jestliže platí rovnost $\mathbf{coord}_B(\mathbf{x}_0) = \begin{pmatrix} a \\ b \end{pmatrix}$, potom $\mathbf{coord}_B(\mathbf{x}_n) = \begin{pmatrix} a \\ (-0.5)^n \cdot b \end{pmatrix}$.

Diagonalisací matice $\mathbf{A}$ tedy získáváme o rekurentním procesu úplný přehled.

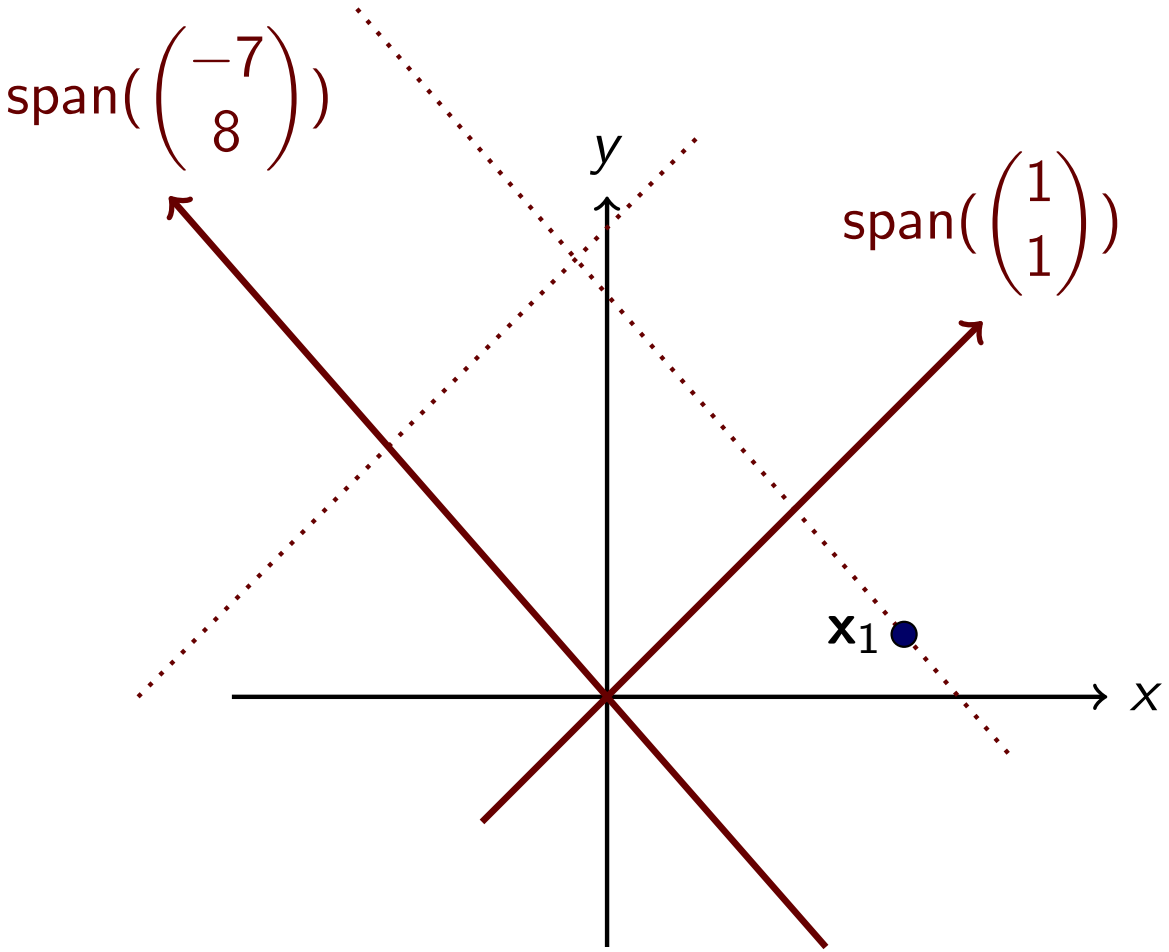
Příklad (equilibrium stochastických procesů, pokrač.)



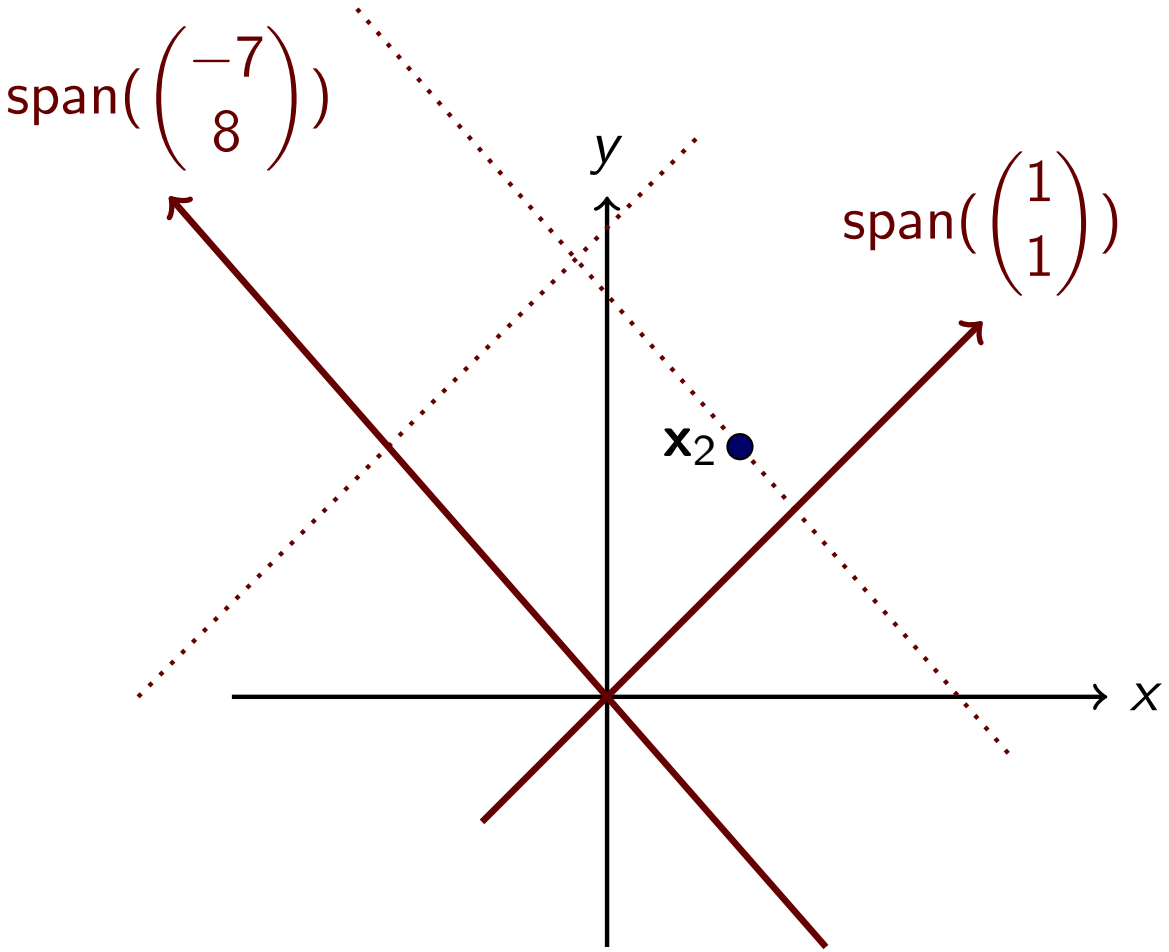
Příklad (equilibrium stochastických procesů, pokrač.)



Příklad (equilibrium stochastických procesů, pokrač.)



Příklad (equilibrium stochastických procesů, pokrač.)



Shrnutí dosavadních úvah

1. Pokud pro obecnou matici $\mathbf{A} : \mathbb{F}^n \to \mathbb{F}^n$ najdeme bázi B, ve které $\mathbf{A}$ je diagonální maticí, získáme v nové bázi úplný přehled o maticích tvaru $\mathbf{A}^k$, kde $k \geq 0$.

   To je důležité například v následujících oblastech:

   1. Teorie dynamických systémů.
   2. Ekonomie (například tzv. Leontiefův input-output model).
   3. Složitost rekursivních algoritmů (řešení rekurentních rovnic, viz příští přednášku).
   4. Geometrie kvadratických útvarů, viz kapitolu 14.1 skript.
   5. Funkce matic, viz příští přednášku.
   6. Atd.

   Hledání diagonální matice k matici $\mathbf{A}$ se říká diagonalisace matice $\mathbf{A}$. Ne vždy zadanou matici diagonalisovat půjde.

2. Problém diagonalisace lze zformulovat (a řešit) pro obecná lineární zobrazení $\mathbf{f} : L \to L$, kde L má konečnou dimensi.

Definice

Pro lineární zobrazení $\mathbf{f} : L \to L$ je λ v $\mathbb{F}$ vlastní hodnotou (také: vlastním číslem), pokud existuje nenulový vektor $\vec{x}$, splňující rovnost $\mathbf{f}(\vec{x}) = \lambda \cdot \vec{x}$.
Každému takovému nenulovému vektoru $\vec{x}$ říkáme vlastní vektor příslušný hodnotě λ.

Pozorování

Ať $\mathbf{f} : L \to L$ je lineární zobrazení.

1. Pro libovolné λ v $\mathbb{F}$ platí: $\{\vec{x} \mid \mathbf{f}(\vec{x}) = \lambda \cdot \vec{x}\} = \ker(\mathbf{f} - \lambda \cdot \mathbf{id})$. Tudíž vlastní vektory příslušné hodnotě λ tvoří podprostor L.[a]
2. λ je vlastní hodnota $\mathbf{f}$ právě tehdy, když $\mathrm{eigen}(\lambda, \mathbf{f})$ je netriviální prostor.

[a] Říkáme mu vlastní podprostor příslušný λ, značíme jej $\mathrm{eigen}(\lambda, \mathbf{f})$. Důvod: vlastní hodnotě se říká eigenvalue, vlastnímu vektoru eigenvector, vlastnímu podprostoru eigenspace. Německy: eigen=vlastní.

Připomenutí (základní vlastnosti podobnosti matic)

Řekneme, že dvě matice $\mathbf{A}$ a $\mathbf{B}$ typu $n \times n$ nad $\mathbb{F}$ jsou si podobné (značení: $\mathbf{A} \approx \mathbf{B}$), pokud platí rovnost $\mathbf{B} = \mathbf{T}^{-1} \cdot \mathbf{A} \cdot \mathbf{T}$, pro nějakou regulární matici $\mathbf{T}$.

Podobné matice jsou maticemi stejného lineárního zobrazení, ale vzhledem k jiné bázi.

Platí:

1. $\mathbf{A} \approx \mathbf{A}$.
2. Jestliže $\mathbf{A} \approx \mathbf{B}$, potom $\mathbf{B} \approx \mathbf{A}$.
3. Jestliže $\mathbf{A} \approx \mathbf{B}$ a $\mathbf{B} \approx \mathbf{C}$, potom $\mathbf{A} \approx \mathbf{C}$.

Definice (charakteristický polynom čtvercové matice)

Ať $\mathbf{A}$ je matice typu $n \times n$ nad $\mathbb{F}$, $n \geq 1$. Výrazu $\det(\mathbf{A} - x\mathbf{E}_n)$ říkáme charakteristický polynom matice $\mathbf{A}$ (značení: $\mathrm{char}_{\mathbf{A}}(x)$).

Poznámky (pro matice typu $n \times n$ nad $\mathbb{F}$)

1. $\mathrm{char}_{\mathbf{A}}(x)$ je polynom stupně n. Tudíž má v $\mathbb{F}$ nanejvýš n kořenů (i s násobnostmi). Pro matici $\mathbf{A} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ nad $\mathbb{R}$ nemá polynom $\mathrm{char}_{\mathbf{A}}(x)$ v $\mathbb{R}$ žádný kořen.
2. Jestliže $\mathbf{A} \approx \mathbf{B}$, potom $\mathrm{char}_{\mathbf{A}}(x) = \mathrm{char}_{\mathbf{B}}(x)$.[a]
   Důvod:

$$\det(\mathbf{B} - x\mathbf{E}_n) = \det(\mathbf{T}^{-1}\mathbf{A}\mathbf{T} - x\mathbf{E}_n) = \det(\mathbf{T}^{-1}\mathbf{A}\mathbf{T} - \mathbf{T}^{-1}x\mathbf{T}) = \det(\mathbf{T}^{-1}(\mathbf{A} - x\mathbf{E}_n)\mathbf{T}) = \det(\mathbf{T}^{-1})\det(\mathbf{A} - x\mathbf{E}_n)\det(\mathbf{T}) = \det(\mathbf{A} - x\mathbf{E}_n).$$

[a] Pozor: obrácená implikace neplatí, viz dále.

Tvrzení

Ať $\mathbf{f} : L \to L$ je lineární zobrazení, $\dim(L) = n$. Označme jako $\mathbf{A_f}$ matici $\mathbf{f}$ vzhledem k jakékoli bázi prostoru L. Potom λ v $\mathbb{F}$ je vlastní hodnotou $\mathbf{f}$ právě tehdy, když $\det(\mathbf{A_f} - \lambda \mathbf{E}_n) = 0$.

Důkaz.

Protože L má dimensi n, je λ vlastní hodnotou $\mathbf{f}$ právě tehdy, když $\mathrm{def}(\mathbf{f} - \lambda \mathbf{id}) > 0$. To nastane právě tehdy, když matice $\mathbf{A_f} - \lambda \mathbf{E}_n$ je singulární. ■

Poznámka

Předchozí tvrzení nezávisí na volbě báze prostoru L a tím pádem nezávisí na volbě matice $\mathbf{A_f}$.

Připomenutí: změnou báze změníme matici $\mathbf{A_f}$ na matici $\mathbf{T}^{-1} \cdot \mathbf{A_f} \cdot \mathbf{T}$, pro nějakou regulární matici $\mathbf{T}$.

Příklad (matice mohou mít stejné vlastní hodnoty, ale různé vlastní podprostory)

Ať $\mathbf{A} = \begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \\ -4 & 4 & -1 \end{pmatrix}$ je matice nad $\mathbb{R}$.

Potom $\mathrm{char}_{\mathbf{A}}(x) = -(x-3)^2 \cdot (x-2)$.

1. Pro dvojnásobnou vlastní hodnotu $\lambda = 3$:

$$\mathrm{eigen}(3, \mathbf{A}) = \ker(\mathbf{A} - 3\mathbf{E}_3) = \mathrm{span}\left(\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}\right).$$

2. Pro jednonásobnou vlastní hodnotu $\lambda = 2$:

$$\mathrm{eigen}(2, \mathbf{A}) = \ker(\mathbf{A} - 2\mathbf{E}_3) = \mathrm{span}\left(\begin{pmatrix} -2 \\ 1 \\ 4 \end{pmatrix}\right).$$

Příklad (pokrač.)

Pozor! Pro $\mathbf{B} = \begin{pmatrix} 2 & 4 & -3 \\ -1 & 10 & -6 \\ -1 & 8 & -4 \end{pmatrix}$ je $\mathrm{char}_{\mathbf{B}}(x) = \mathrm{char}_{\mathbf{A}}(x)$. Ale

$\mathrm{eigen}(3, \mathbf{B}) = \mathrm{span}(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix})$ a $\mathrm{eigen}(2, \mathbf{B}) = \mathrm{span}(\begin{pmatrix} 0 \\ 3 \\ 4 \end{pmatrix})$.

Tedy: **A** a **B** mají stejná vlastní čísla (i s násobnostmi), ale různé vlastní podprostory.

Problém diagonalisace

Pro matici $\mathbf{A}$ typu $n \times n$ nad $\mathbb{F}$ chceme rozhodnout, zda $\mathbf{A} \approx \mathbf{D}$,[a] kde $\mathbf{D} = D(\lambda_1; \lambda_2; \ldots; \lambda_n)$ je diagonální matice

$$\begin{pmatrix} \lambda_1 & 0 & 0 & \ldots & 0 \\ 0 & \lambda_2 & 0 & \ldots & 0 \\ 0 & 0 & \lambda_3 & \ldots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \ldots & \lambda_n \end{pmatrix}$$

nebo ve sloupcovém zápisu

$$(\lambda_1 \cdot \mathbf{e}_1, \lambda_2 \cdot \mathbf{e}_2, \lambda_3 \cdot \mathbf{e}_3, \ldots, \lambda_n \cdot \mathbf{e}_n)$$

[a] Přesněji: $\mathbf{A} = \mathbf{T} \cdot \mathbf{D} \cdot \mathbf{T}^{-1}$, kde $\mathbf{T}$ je regulární matice.

Myšlenka nalezení matic T a D v rovnici $\mathbf{A} = \mathbf{T} \cdot \mathbf{D} \cdot \mathbf{T}^{-1}$

Ať $\mathbf{D} = D(\lambda_1; \ldots; \lambda_n)$.

1. Rovnost $\mathbf{A} = \mathbf{T} \cdot \mathbf{D} \cdot \mathbf{T}^{-1}$ platí právě tehdy, když platí rovnost $\mathbf{A} \cdot \mathbf{T} = \mathbf{T} \cdot \mathbf{D}$ a matice $\mathbf{T}$ je regulární.
2. Pro regulární matici $\mathbf{T} = (\mathbf{t}_1, \ldots, \mathbf{t}_n)$ platí rovnost $\mathbf{A} \cdot \mathbf{T} = \mathbf{T} \cdot \mathbf{D}$ právě tehdy, když platí rovnosti $\mathbf{A} \cdot \mathbf{t}_j = \lambda_j \cdot \mathbf{t}_j$ pro všechna $j = 1, \ldots, n$.

Shrnuto: rovnost $\mathbf{A} = \mathbf{T} \cdot D(\lambda_1, \ldots, \lambda_n) \cdot \mathbf{T}^{-1}$ platí právě tehdy, když platí následující dvě podmínky:

- $\mathbf{A} \cdot \mathbf{t}_j = \lambda_j \cdot \mathbf{t}_j$ pro všechna $j = 1, \ldots, n$.
  To jest: j-tý sloupec $\mathbf{t}_j$ matice $\mathbf{T}$ je vlastní vektor příslušný vlastní hodnotě λ_j matice $\mathbf{A}$.
- Matice $\mathbf{T} = (\mathbf{t}_1, \ldots, \mathbf{t}_n)$ je regulární.

Pozorování

Dva vlastní vektory, příslušející dvěma různým vlastním hodnotám, jsou lineárně nezávislé.
Platí-li

$$\mathbf{A} \cdot \mathbf{t}_{j_1} = \lambda_{j_1} \cdot \mathbf{t}_{j_1} \quad \text{a} \quad \mathbf{A} \cdot \mathbf{t}_{j_2} = \lambda_{j_2} \cdot \mathbf{t}_{j_2}$$

pak z rovnosti $a_1 \cdot \mathbf{t}_{j_1} + a_2 \cdot \mathbf{t}_{j_2} = \mathbf{o}$ plyne

$$\begin{aligned} \mathbf{o} &= (\mathbf{A} - \lambda_{j_2} \cdot \mathbf{E}) \cdot \mathbf{o} \\ &= (\mathbf{A} - \lambda_{j_2} \cdot \mathbf{E}) \cdot (a_1 \cdot \mathbf{t}_{j_1} + a_2 \cdot \mathbf{t}_{j_2}) \\ &= a_1 \cdot \underbrace{(\mathbf{A} - \lambda_{j_2} \cdot \mathbf{E}) \cdot \mathbf{t}_{j_1}}_{\neq \mathbf{o}} + a_2 \cdot \underbrace{(\mathbf{A} - \lambda_{j_2} \cdot \mathbf{E}) \cdot \mathbf{t}_{j_2}}_{= \mathbf{o}} \end{aligned}$$

tedy $a_1 = 0$.
Rovnost $a_2 = 0$ se dokáže analogicky.

Problém

Existuje dostatek lineárně nezávislých vlastních vektorů pro stejnou vlastní hodnotu?

Věta (charakterisace diagonalisovatelných matic nad $\mathbb{F}$)

Pro matici $\mathbf{A}$ typu $n \times n$ nad $\mathbb{F}$ jsou následující podmínky ekvivalentní:

1. $\mathbf{A}$ je diagonalisovatelná, tj $\mathbf{A} \approx \mathbf{D}$ pro nějakou diagonální matici $\mathbf{D}$.
2. Charakteristický polynom $\mathrm{char}_{\mathbf{A}}(x)$ lze v $\mathbb{F}$ rozložit na součin lineárních faktorů a platí: násobnost λ jako kořene $\mathrm{char}_{\mathbf{A}}(x)$ je rovna $\dim(\mathrm{eigen}(\lambda, \mathbf{A}))$.[a]

[a] Násobnosti λ jako kořene $\mathrm{char}_{\mathbf{A}}(x)$ se někdy říká algebraická násobnost λ, číslu $\dim(\mathrm{eigen}(\lambda, \mathbf{A}))$ se někdy říká geometrická násobnost λ.

Důkaz.

Bez důkazu (nemáme vybudovanou teorii polynomů nad obecným tělesem $\mathbb{F}$). Pro zájemce: Věta 10.4.8 skript. ■

Příklad (nad $\mathbb{R}$)

Matice $\mathbf{A} = \begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \\ -4 & 4 & -1 \end{pmatrix}$ a $\mathbf{B} = \begin{pmatrix} 2 & 4 & -3 \\ -1 & 10 & -6 \\ -1 & 8 & -4 \end{pmatrix}$ splňují:

1. $\mathrm{char}_{\mathbf{A}}(x) = \mathrm{char}_{\mathbf{B}}(x) = -(x-3)^2 \cdot (x-2)$.
2. Protože $\dim(\mathrm{eigen}(3, \mathbf{A})) = 2$ a $\dim(\mathrm{eigen}(2, \mathbf{A})) = 1$, platí $\mathbf{A} \approx \mathbf{D}$ pro nějakou diagonální matici $\mathbf{D}$.
3. Protože $\dim(\mathrm{eigen}(3, \mathbf{B})) = 1$ a $\dim(\mathrm{eigen}(2, \mathbf{B})) = 1$, neplatí $\mathbf{B} \approx \mathbf{D}$ pro žádnou diagonální matici $\mathbf{D}$.

Ukázali jsme (mimo jiné): $\mathbf{A} \not\approx \mathbf{B}$, přestože $\mathrm{char}_{\mathbf{A}}(x) = \mathrm{char}_{\mathbf{B}}(x)$.

Příklad

Pro matici $\mathbf{A} = \begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \\ -4 & 4 & -1 \end{pmatrix}$ nad $\mathbb{R}$ platí $\mathrm{char}_{\mathbf{A}}(x) = -(x-3)^2 \cdot (x-2)$

a $\mathbf{A} = \mathbf{T} \cdot \mathbf{D} \cdot \mathbf{T}^{-1}$, kde $\mathbf{D} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ a $\mathbf{T} = \begin{pmatrix} 1 & -1 & -2 \\ 1 & 0 & 1 \\ 0 & 1 & 4 \end{pmatrix}$.

Matice $\mathbf{A}$ v kanonické bázi odpovídá lineárnímu zobrazení

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} 5x - 2y + 2z \\ -x + 4y - z \\ -4x + 4y - z \end{pmatrix}$$

Vzhledem k bázi $\left(\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -2 \\ 1 \\ 4 \end{pmatrix} \right)$ jde o podstatně jednodušší zobrazení

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} 3x \\ 3y \\ 2z \end{pmatrix}$$

Diagonalisace matic

Odpřednesenou látku naleznete v kapitolách 10.1, 10.3 a 10.4 skript *Abstraktní a konkrétní lineární algebra*.

Minulá přednáška

1. Pojmy vlastní hodnota a vlastní vektor lineárního zobrazení.
2. Věta o diagonalisovatelnosti čtvercových matic nad $\mathbb{C}$.

Dnešní přednáška

1. Diagonalisovatelnost matic nad $\mathbb{C}$ a nad $\mathbb{R}$.
2. Dvě aplikace: řešení rekurentních rovnic a funkce matic.[a]

[a] Tyto dvě aplikace nebudou zkoušeny!

Připomenutí důležité vlastnosti tělesa $\mathbb{C}$

Každý polynom $p(x)$ v $\mathbb{C}[x]$ stupně n má přesně n kořenů (počítaných i s násobnostmi).[a]

[a] Této vlastnosti tělesa $\mathbb{C}$ se říká algebraická uzavřenost.

1. Komplexní číslo λ je kořen polynomu $p(x) \in \mathbb{C}[x]$ násobnosti k, pokud platí rovnost $p(x) = (x - \lambda)^k \cdot q(x)$ pro $q(x) \in \mathbb{C}[x]$ a $q(\lambda) \neq 0$.
2. Speciálně: číslo λ má jako kořen $p(x)$ násobnost nula právě tehdy, když λ není kořenem polynomu $p(x)$.

Důsledek (téma 8B, tvar věty o diagonalisaci pro $\mathbb{F} = \mathbb{C}$)

Pro čtvercovou matici $\mathbf{A}$ nad $\mathbb{C}$ jsou následující podmínky ekvivalentní:

1. Matice $\mathbf{A}$ diagonalisovatelná.
2. Pro každé komplexní číslo λ platí: násobnost λ jako kořene polynomu $\mathrm{char}_{\mathbf{A}}(x)$ je rovna $\dim(\mathrm{eigen}(\lambda, \mathbf{A}))$.

Příklad

Pauliho matice[a] jsou následující tři matice nad $\mathbb{C}$:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Všechny tyto matice jsou diagonalisovatelné:

1. Matice Z již diagonální je.

---

[a] Jde o důležitý příklad v kvantové mechanice a kvantovém počítání. Matice X, Y a Z jsou operátory spinu ve směrech os x, y, z a značívají se též

σ_x (také: σ_1) $\quad$ σ_y (také: σ_2) $\quad$ σ_z (také: σ_3)

Užitečná početní cvičení: platí rovnosti

1. $\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = -i \cdot \sigma_1\sigma_2\sigma_3 = \mathbf{E}_2$.
2. $\{\sigma_j, \sigma_k\} = 2\delta_{jk}\mathbf{E}_2$, kde $\{\sigma_j, \sigma_k\} = \sigma_j\sigma_k + \sigma_k\sigma_j$ je tzv Poissonova závorka a δ_{jk} je Kroneckerův symbol.
3. $[\sigma_j, \sigma_k] = \sum_{l=1}^{3} 2i\epsilon_{jkl}\sigma_l$, kde $[\sigma_j, \sigma_k] = \sigma_j\sigma_k - \sigma_k\sigma_j$ je tzv komutátor a ϵ_{jkl} je Levi-Civitův symbol.

Příklad (pokrač.)

2. Diagonalisace matice $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

   Platí $\mathrm{char}_X(x) = x^2 - 1 = (x-1)\cdot(x+1)$.

   Vlastní hodnoty a vlastní vektory matice X jsou: $\lambda_1 = 1$, $\mathbf{t}_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ a $\lambda_2 = -1$, $\mathbf{t}_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

   Tudíž
   $$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \approx \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
   a operátor X je diagonální v bázi $(\mathbf{t}_1, \mathbf{t}_2)$.

Příklad (pokrač.)

3. Diagonalisace matice $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$.

   Platí $\mathrm{char}_Y(x) = x^2 - 1 = (x-1)\cdot(x+1)$.

   Vlastní hodnoty a vlastní vektory matice Y jsou: $\lambda_1 = 1$, $\mathbf{v}_1 = \begin{pmatrix} -i \\ 1 \end{pmatrix}$ a $\lambda_2 = -1$, $\mathbf{v}_2 = \begin{pmatrix} i \\ 1 \end{pmatrix}$.

   Tudíž
   $$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \approx \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
   a operátor Y je diagonální v bázi $(\mathbf{v}_1, \mathbf{v}_2)$.

Jordanův tvar čtvercové matice (nepovinné)

Ať $\mathbf{A}$ je matice typu $n \times n$ nad $\mathbb{F}$ taková, že polynom $\mathrm{char}_{\mathbf{A}}(x)$ lze rozložit na součin lineárních faktorů.[a]
Potom lze dokázat, že $\mathbf{A}$ je „téměř diagonalisovatelná“. Přesněji: platí $\mathbf{A} \approx \mathbf{J}$, kde

$$\mathbf{J} = \begin{pmatrix} \mathbf{J}_1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{J}_2 & \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{J}_3 & \mathbf{0} & \dots & \mathbf{0} \\ \vdots & & & & & \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{J}_n \end{pmatrix}$$

[a] To platí například pro libovolnou matici nad $\mathbb{C}$.

Jordanův tvar čtvercové matice (nepovinné, pokrač.)

$$\mathbf{J}_i = \begin{pmatrix} \lambda_i & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & \lambda_i & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & \lambda_i & 1 & 0 & \dots & 0 \\ \vdots & & & & & & \\ 0 & 0 & 0 & 0 & 0 & \dots & \lambda_i \end{pmatrix}$$

Matici $\mathbf{J}_i$ říkáme Jordanova buňka. Na diagonále je vlastní hodnota λ_i matice $\mathbf{A}$. Rozměr matice $\mathbf{J}_i$ je roven násobnosti vlastní hodnoty λ jako kořene $\mathrm{char}_{\mathbf{A}}(x)$.

Příklad

Ať $\mathbf{A} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ je regulární matice nad $\mathbb{R}$. Potom platí:

1. $\mathrm{char}_{\mathbf{A}}(x) = (a - x)^2 + b^2 = x^2 - 2ax + (a^2 + b^2)$.
   Diskriminant tohoto výrazu je $-4b^2$.

   Matice $\mathbf{A}$ je tedy nad $\mathbb{R}$ diagonalisovatelná pouze v případě $b = 0$.

   V tomto případě ale $\mathbf{A}$ už je diagonální: $\mathbf{A} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ a musí platit $a \neq 0$, protože $\mathbf{A}$ je regulární.

   Matice $\mathbf{A}$ je tedy maticí změny měřítka (změna je stejná na obou souřadnicových osách).

Příklad (pokrač.)

2. V případě $b \neq 0$ matice $\mathbf{A} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ není nad $\mathbb{R}$ diagonalisovatelná.

   Matice $\mathbf{A}$ (chápaná jako matice nad $\mathbb{C}$) má vlastní hodnoty $\lambda_1 = a + bi$ a $\lambda_2 = a - bi$, protože
   $\mathrm{char}_{\mathbf{A}}(x) = x^2 - 2ax + (a^2 + b^2) = (x - (a + ib)) \cdot (x - (a - ib))$.

   Označme $r = |\lambda_1| = |\lambda_2| = \sqrt{a^2 + b^2}$. Dále označme jako α úhel[a] mezi vektory $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ a $\begin{pmatrix} a \\ b \end{pmatrix}$.

   Potom
   $$\mathbf{A} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$
   To jest: $\mathbf{A}$ je rotace o úhel α, následovaná změnou měřítka.

[a] Úhlu α se říká argument komplexního čísla $a + bi$. Platí tedy rovnost $a + bi = r \cdot (\cos\alpha + i \sin\alpha) = r \cdot e^{i\alpha}$.

Tvrzení (klasifikace regulárních transformací roviny)

Ať $\mathbf{M} : \mathbb{R}^2 \to \mathbb{R}^2$ je regulární a ať nemá 2-násobnou vlastní hodnotu. Pak $\mathbf{M}$ je podobná buď

1. matici $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, kde $a \neq b$ jsou z $\mathbb{R}$ a $a \cdot b \neq 0$,

nebo

2. matici $\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$, kde $r > 0$ a $\alpha \in [0; 2\pi)$.

Slogan

Regulární transformace roviny bez 2-násobných vlastních hodnot jsou pouze dvou typů:

1. Změny měřítka (změna měřítka je na každé souřadnicové ose jiná).
2. Rotace následované změnou měřítka stejnou na obou souřadnicových osách.

Důkaz (klasifikace regulárních transformací roviny).

1. V případě, kdy $\mathbf{M}$ je diagonalisovatelná nad $\mathbb{R}$, má $\mathbf{M}$ dvě různé reálné vlastní hodnoty a, b. Tudíž $\mathbf{M} \approx \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, kde $a \cdot b \neq 0$, protože $\mathbf{M}$ je regulární.
2. V případě, kdy $\mathbf{M}$ nad $\mathbb{R}$ diagonalisovatelná není, má $\mathrm{char}_{\mathbf{M}}(x)$ komplexní kořen $\lambda = a + bi$, kde $b \neq 0$.
   Označme jako $\mathbf{v}$ komplexní vlastní vektor příslušný vlastní hodnotě λ. Označme jako $\mathbf{T}$ matici se sloupci $\mathbf{t}_1 = \mathrm{Re}(\mathbf{v})$ (vektor reálných částí položek vektoru $\mathbf{v}$) a $\mathbf{t}_2 = \mathrm{Im}(\mathbf{v})$ (vektor imaginárních částí položek vektoru $\mathbf{v}$).
   Potom platí rovnost $\mathbf{M} = \mathbf{T} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \mathbf{T}^{-1}$.
   Nyní stačí použít předchozí příklad. ■

Výpočet mocnin diagonalisovatelné matice

Pro diagonalisovatelnou matici $\mathbf{A}$ typu $n \times n$ nad $\mathbb{F}$ platí:
$\mathbf{A} = \mathbf{T} \cdot \mathbf{D} \cdot \mathbf{T}^{-1}$ pro nějakou regulární matici $\mathbf{T}$.

Tudíž: $\mathbf{A}^2 = \mathbf{A} \cdot \mathbf{A} = (\mathbf{T} \cdot \mathbf{D} \cdot \mathbf{T}^{-1}) \cdot (\mathbf{T} \cdot \mathbf{D} \cdot \mathbf{T}^{-1}) = \mathbf{T} \cdot \mathbf{D}^2 \cdot \mathbf{T}^{-1}$.

Obecně: $\mathbf{A}^k = \mathbf{T} \cdot \mathbf{D}^k \cdot \mathbf{T}^{-1}$, pro všechna přirozená čísla $k \geq 0$.

Protože mocniny diagonální matice lze počítat velmi rychle, lze rychle počítat i mocniny diagonalisovatelných matic.

Ukážeme dvě aplikace umocňování:

1. Řešení lineárních homogenních rekurentních rovnic.
   To je důležité při analýze složitosti rekursivních algoritmů.
2. Základní myšlenku funkcí matice.
   To je důležité ve fyzice, grafice, kvantovém počítání, ...

Příklad (Fibonacciho posloupnost)

Hledáme posloupnost čísel $F(n)$, splňující lineární rekurentní rovnici $F(n+2) = F(n+1) + F(n)$, pro všechna př. č. $n \geq 0$.

Cíl: chceme explicitní vzorec pro $F(n)$, $n \geq 0$.

Evidentně: známe-li $F(0)$ a $F(1)$, známe všechna $F(n)$.[a]

1. Vytvoříme generující matici $\mathbf{F} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ pro kterou platí:
$$\mathbf{F} \cdot \begin{pmatrix} F(0) \\ F(1) \end{pmatrix} = \begin{pmatrix} F(1) \\ F(2) \end{pmatrix}, \text{ obecně } \mathbf{F}^n \cdot \begin{pmatrix} F(0) \\ F(1) \end{pmatrix} = \begin{pmatrix} F(n) \\ F(n+1) \end{pmatrix}.$$
2. Matice $\mathbf{F}$ je diagonalisovatelná nad $\mathbb{R}$: $\lambda_1 = \frac{1+\sqrt{5}}{2}$, $\lambda_2 = \frac{1-\sqrt{5}}{2}$
$$\mathbf{D} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = \mathbf{T}^{-1} \cdot \mathbf{F} \cdot \mathbf{T}, \quad \mathbf{T} = \begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix}, \quad \mathbf{F}^n = \mathbf{T} \cdot \mathbf{D}^n \cdot \mathbf{T}^{-1}$$

[a] Požadavkům $F(0) = x_0$ a $F(1) = x_1$ se říká počáteční podmínka. Pro klasickou Fibonacciho posloupnost jde o $F(0) = 1$, $F(1) = 1$.

Příklad (Fibonacciho posloupnost, pokrač.)

3. $\begin{pmatrix} F(n) \\ F(n+1) \end{pmatrix} = \mathbf{T} \cdot \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} \cdot \mathbf{T}^{-1} \cdot \begin{pmatrix} F(0) \\ F(1) \end{pmatrix} =$
$\begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix} \cdot \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} \cdot \frac{1}{\lambda_2-\lambda_1} \cdot \begin{pmatrix} \lambda_2 & -1 \\ -\lambda_1 & 1 \end{pmatrix} \cdot \begin{pmatrix} F(0) \\ F(1) \end{pmatrix} =$
$\frac{1}{\lambda_2-\lambda_1} \cdot \begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix} \cdot \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} \cdot \begin{pmatrix} \lambda_2 & -1 \\ -\lambda_1 & 1 \end{pmatrix} \cdot \begin{pmatrix} F(0) \\ F(1) \end{pmatrix}$

   Takže: $F(n) = \frac{\lambda_1^n \cdot \lambda_2 - \lambda_2^n \cdot \lambda_1}{\lambda_2-\lambda_1} \cdot F(0) + \frac{-\lambda_1^n + \lambda_2^n}{\lambda_2-\lambda_1} \cdot F(1)$

   V klasickém případě (tj když $F(0) = F(1) = 1$), je

$$\begin{aligned} F(n) &= \frac{\lambda_1^n \cdot \lambda_2 - \lambda_2^n \cdot \lambda_1}{\lambda_2 - \lambda_1} + \frac{-\lambda_1^n + \lambda_2^n}{\lambda_2 - \lambda_1} = \\ &= \lambda_1^n \cdot \frac{\lambda_2 - 1}{\lambda_2 - \lambda_1} + \lambda_2^n \cdot \frac{1 - \lambda_1}{\lambda_2 - \lambda_1} \end{aligned}$$

Poznámky (lineární homogenní rekurence k-tého řádu)

Obdobným způsobem lze řešit jakoukoli homogenní lineární rekurentní rovnici k-tého řádu: hledáme posloupnost $X(n)$ prvků $\mathbb{F}$, které splňují

$$X(n+k) = a_1 X(n+k-1) + a_2 X(n+k-2) + \dots a_k X(n)$$

pro všechna přirozená čísla $n \geq 0$, kde $a_1, \dots, a_k$ jsou v $\mathbb{F}$.

Jediné, co potřebujeme, je diagonalisovatelnost generující matice.

1. Řešení rekurentních rovnic hraje zásadní úlohu při analýze složitosti rekursivních algoritmů.
2. Podobné postupy fungují i pro lineární homogenní diferenciální rovnice k-tého řádu. Viz Dodatek O skript.

Příklad (exponenciála matice)

Víme, že funkce e^x má Taylorův rozvoj $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$.

Pro čtvercovou diagonalisovatelnou matici $\mathbf{X} = \mathbf{T} \cdot \mathbf{D} \cdot \mathbf{T}^{-1}$ definujeme

$$e^{\mathbf{X}} = \sum_{i=0}^{\infty} \frac{\mathbf{X}^n}{n!} = \sum_{i=0}^{\infty} \frac{\mathbf{T} \cdot \mathbf{D}^n \cdot \mathbf{T}^{-1}}{n!} = \mathbf{T} \cdot \underbrace{\left(\sum_{i=0}^{\infty} \frac{\mathbf{D}^n}{n!} \right)}_{=e^{\mathbf{D}}} \cdot \mathbf{T}^{-1}$$

Konvergenci této řady musíme chápat ve smyslu normy.[a]

Lze ukázat, že matice $e^{\mathbf{D}}$ je diagonální, a že platí $e^{\mathbf{D}} = (\delta_{ij} \cdot e^{d_{ij}})$.

[a] To je velmi technický pojem, nebudeme o něm mluvit. Více například v knize Roger A. Horn, Charles J. Johnson, *Matrix analysis*, Cambridge University Press, 2012, nebo v přednášce A0B01PAN (Pokročilá analýza), nebo v kapitole 13.2 skript. Analogicky exponenciále lze postupovat pro obecnou funkci $f : \mathbb{R} \to \mathbb{R}$ (případně $f : \mathbb{C} \to \mathbb{C}$), která má Taylorův rozvoj.

Abstraktní skalární součin

Odpřednesenou látku naleznete v kapitolách 12.1 a 12.2 skript *Abstraktní a konkrétní lineární algebra*.

Dnešní přednáška

1. V této přednášce (a ve všech přednáškách týkajících se skalárního součinu) se zaměříme na lineární prostory nad $\mathbb{R}$.[a]
2. Skalární součin zavedeme axiomaticky. Odvodíme geometrický význam skalárního součinu.[b]

   Axiomatické zavedení skalárního součinu nám umožní převést známé významy z $\mathbb{R}^n$ (kolmost, délka vektoru, atd) do obecných lineárních prostorů se skalárním součinem.

[a] Velmi málo řekneme i o lineárních prostorech nad $\mathbb{C}$. Důvod: fyzika a kvantové počítání.

[b] Slogan: skalární součin je míra „odchylky“ dvou vektorů.

Příští přednáška

1. Popis obecných skalárních součinů v prostorech $\mathbb{R}^n$.

Definice (reálný skalární součin)

Ať L je lineární prostor nad $\mathbb{R}$. Funkci $\langle - \mid - \rangle : L \times L \to \mathbb{R}$ říkáme skalární součin,[a] pokud platí následující, pro libovolné vektory $\vec{x}$, $\vec{y}$:

1. Komutativita: $\langle \vec{x} \mid \vec{y} \rangle = \langle \vec{y} \mid \vec{x} \rangle$.
2. Linearita ve druhé souřadnici: zobrazení $\langle \vec{x} \mid - \rangle : L \to \mathbb{R}$ je lineární.
3. Positivní definitnost: $\langle \vec{x} \mid \vec{x} \rangle \geqslant 0$, $\langle \vec{x} \mid \vec{x} \rangle = 0$ iff $\vec{x} = \vec{o}$.

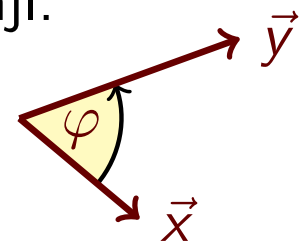
[a] Naše značení pro skalární součin je obvyklé ve fyzice (tzv bra-ket notation nebo Diracova notace) a má jisté výhody. Značení $\vec{x} \cdot \vec{y}$ pro skalární součin nebudeme používat! Důvod: přetížení značky $\cdot$ pro součin.

Poznámka (skalární součin pro prostory nad $\mathbb{C}$)

V případě lineárního prostoru nad $\mathbb{C}$ mluvíme o skalárním součinu, pokud $\langle - \mid - \rangle : L \times L \to \mathbb{C}$ je positivně definitní, lineární ve druhé souřadnici a místo komutativity platí rovnost $\langle \vec{x} \mid \vec{y} \rangle = \overline{\langle \vec{y} \mid \vec{x} \rangle}$.

Příklady skalárních součinů

1. Skalární součin v prostoru orientovaných úseček: $\langle \vec{x} \mid \vec{y} \rangle = \|\vec{x}\| \cdot \|\vec{y}\| \cdot \cos\varphi$, kde $\|\vec{x}\|$ a $\|\vec{y}\|$ jsou délky úseček $\vec{x}$ a $\vec{y}$ a φ je úhel, který svírají:[a]



   Tento skalární součin splňuje všechny tři požadované vlastnosti: je komutativní, lineární ve druhé souřadnici a positivně definitní.

---

[a] Důležitá poznámka: v další části přednášky ukážeme, že pro libovolný skalární součin je možné definovat pojmy délky $\|\vec{x}\|$ vektoru $\vec{x}$ (také: normy vektoru $\vec{x}$) a úhlu φ mezi dvěma vektory tak, že platí rovnost $\langle \vec{x} \mid \vec{y} \rangle = \|\vec{x}\| \cdot \|\vec{y}\| \cdot \cos\varphi$.

V prostoru s obecným skalárním součinem se tudíž budeme moci „chovat stejně“ jako v klasické geometrii. Bude tak například platit Pythagorova věta, a podobně.

Příklady skalárních součinů (pokrač.)

2. Standardní skalární součin v $\mathbb{R}^n$: $\langle \mathbf{x} \mid \mathbf{y} \rangle = \mathbf{x}^T \cdot \mathbf{y} = \sum_{i=1}^{n} x_i \cdot y_i$.
3. Standardní skalární součin není jediný skalární součin v $\mathbb{R}^n$. Například[a] $\left\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \middle| \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle = x_1 y_1 + x_2 y_1 + x_1 y_2 + 2 x_2 y_2$ je skalární součin v $\mathbb{R}^2$. (Jde o úmorné, ale užitečné cvičení.)
4. Standardní skalární součin v $\mathbb{C}^n$: $\langle \mathbf{x} \mid \mathbf{y} \rangle = \sum_{i=1}^{n} \overline{x_i} \cdot y_i$.

   Pozor! Platí rovnost $\langle \mathbf{x} \mid \mathbf{y} \rangle = \overline{\langle \mathbf{y} \mid \mathbf{x} \rangle}$, nikoli $\langle \mathbf{x} \mid \mathbf{y} \rangle = \langle \mathbf{y} \mid \mathbf{x} \rangle$.

[a] K tomuto skalárnímu součinu se vrátíme koncem této přednášky. Po příští přednášce budeme schopni (téměř) okamžitě uvidět, že jde o skalární součin. Budeme také schopni popsat všechny možné skalární součiny v prostoru $\mathbb{R}^n$.

Tvrzení (nerovnost Cauchy-Schwarz-Bunyakovski)

Platí $|\langle \vec{x} \mid \vec{y} \rangle| \leqslant \sqrt{\langle \vec{x} \mid \vec{x} \rangle} \cdot \sqrt{\langle \vec{y} \mid \vec{y} \rangle}$.

Důkaz.

Platí $0 \leqslant \langle \vec{x} + a\vec{y} \mid \vec{x} + a\vec{y} \rangle = \underbrace{\langle \vec{x} \mid \vec{x} \rangle}_{C} + a\,\underbrace{2\langle \vec{x} \mid \vec{y} \rangle}_{B} + a^2\,\underbrace{\langle \vec{y} \mid \vec{y} \rangle}_{A}$, pro každé $a \in \mathbb{R}$.

Tudíž $B^2 - 4AC \leqslant 0$, neboli $B^2 \leqslant 4AC$. Z toho nerovnost $|\langle \vec{x} \mid \vec{y} \rangle| \leqslant \sqrt{\langle \vec{x} \mid \vec{x} \rangle} \cdot \sqrt{\langle \vec{y} \mid \vec{y} \rangle}$ plyne okamžitě. ■

Jednoduchý, ale důležitý důsledek: úhel mezi vektory

Pro nenulové $\vec{x}$, $\vec{y}$ platí $-1 \leqslant \underbrace{\dfrac{\langle \vec{x} \mid \vec{y} \rangle}{\sqrt{\langle \vec{x} \mid \vec{x} \rangle} \cdot \sqrt{\langle \vec{y} \mid \vec{y} \rangle}}}_{=\cos\varphi \text{ pro jediné } \varphi \in [0;\pi]} \leqslant 1$. Úhlu φ říkáme úhel mezi vektory $\vec{x}$ a $\vec{y}$.

Definice (norma vektoru)

Normu vektoru $\vec{x}$ definujeme[a] jako $\|\vec{x}\| = \sqrt{\langle \vec{x} \mid \vec{x} \rangle}$.

[a] Nerovnost C-S-B tedy můžeme zapsat jako $|\langle \vec{x} \mid \vec{y} \rangle| \leqslant \|\vec{x}\| \cdot \|\vec{y}\|$.

Tvrzení (vlastnosti normy)

Platí:

1. $\|\vec{x}\| \geqslant 0$, $\|\vec{x}\| = 0$ iff $\vec{x} = \vec{o}$.
2. $\|a \cdot \vec{x}\| = |a| \cdot \|\vec{x}\|$.
3. Trojúhelníková nerovnost: $\|\vec{x} + \vec{y}\| \leqslant \|\vec{x}\| + \|\vec{y}\|$.

Důkaz.

Jediná netriviální vlastnost je trojúhelníková nerovnost. Upravujte: $\|\vec{x} + \vec{y}\|^2 = \langle \vec{x} + \vec{y} \mid \vec{x} + \vec{y} \rangle = \|\vec{x}\|^2 + 2\langle \vec{x} \mid \vec{y} \rangle + \|\vec{y}\|^2$ a použijte nerovnost Cauchy-Schwarz-Bunyakovski:
$\|\vec{x}\|^2 + 2\langle \vec{x} \mid \vec{y} \rangle + \|\vec{y}\|^2 \leqslant \|\vec{x}\|^2 + 2\|\vec{x}\| \cdot \|\vec{y}\| + \|\vec{y}\|^2 = (\|\vec{x}\| + \|\vec{y}\|)^2$.
Celkově: $\|\vec{x} + \vec{y}\|^2 \leqslant (\|\vec{x}\| + \|\vec{y}\|)^2$, tedy $\|\vec{x} + \vec{y}\| \leqslant \|\vec{x}\| + \|\vec{y}\|$. ■

Důsledek

Pro nenulová $\vec{x}$, $\vec{y}$ platí rovnost $\langle \vec{x} \mid \vec{y} \rangle = \|\vec{x}\| \cdot \|\vec{y}\| \cdot \cos\varphi$.

Poznámka

Předchozí důsledek je stejná rovnost, která platí pro „klasický“ skalární součin v prostoru orientovaných úseček!

Definice (ortogonalita vektorů)

Pokud $\langle \vec{x} \mid \vec{y} \rangle = 0$, mluvíme o ortogonálních (také: navzájem kolmých) vektorech.

Několik poznámek o ortogonalitě

1. Neřekli jsme, že vektory $\vec{x}$ a $\vec{y}$ jsou na sebe kolmé, pokud svírají úhel $\frac{\pi}{2}$. Taková úvaha platí pouze pro nenulové vektory. Chceme ovšem hovořit i o nulovém vektoru, proto jsme definovali kolmost rovností $\langle \vec{x} \mid \vec{y} \rangle = 0$.

Několik poznámek o ortogonalitě (pokrač.)

2. Pozor: nulový vektor $\vec{o}$ je kolmý na každý vektor $\vec{x}$.
   Důvod: z definice skalárního součinu víme, že zobrazení

$$\langle \vec{x} \mid - \rangle : L \to \mathbb{R}$$

   je lineární. Proto $\langle \vec{x} \mid - \rangle$ musí poslat nulový vektor na nulový vektor, neboli musí platit rovnost

$$\langle \vec{x} \mid \vec{o} \rangle = 0$$

   Obráceně: jestliže $\vec{x}$ je kolmý na každý vektor, pak $\vec{x} = \vec{o}$.
   Důvod: podle předpokladu je $\langle \vec{x} \mid \vec{x} \rangle = 0$. Z definice skalárního součinu plyne, že $\vec{x} = \vec{o}$.

Několik poznámek o ortogonalitě (pokrač.)

3. Chceme-li pro nějaký vektor $\vec{x}$ ověřit, že $\langle \vec{x} \mid \vec{v} \rangle = 0$ pro každý vektor $\vec{v}$ ze $\mathrm{span}(M)$, stačí ověřit, že platí $\langle \vec{x} \mid \vec{m} \rangle = 0$ pro všechny vektory $\vec{m}$ z M.

   Důvod: pro obecný vektor $\vec{v}$ ze $\mathrm{span}(M)$ nastane jedna ze dvou situací:

   1. $\vec{v} = \vec{o}$. Pak $\langle \vec{x} \mid \vec{v} \rangle = 0$.
   2. $\vec{v} = \sum_{i=1}^{n} a_i \cdot \vec{m}_i$ pro nějaká a_i z $\mathbb{R}$ a nějaká $\vec{m}_i$ z M. Pak
   $$\langle \vec{x} \mid \vec{v} \rangle = \langle \vec{x} \mid \sum_{i=1}^{n} a_i \cdot \vec{m}_i \rangle = \sum_{i=1}^{n} a_i \cdot \langle \vec{x} \mid \vec{m}_i \rangle$$

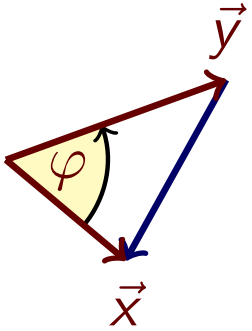
   Jestliže tedy je $\langle \vec{x} \mid \vec{m}_i \rangle = 0$ pro každé i, platí $\langle \vec{x} \mid \vec{v} \rangle = 0$.

   Slogan: ortogonalitu stačí ověřovat pouze pro množinu generátorů podprostoru.

Ortogonalitou se budeme podrobněji zabývat v příštích přednáškách.

Příklady (geometrie prostoru se skalárním součinem)

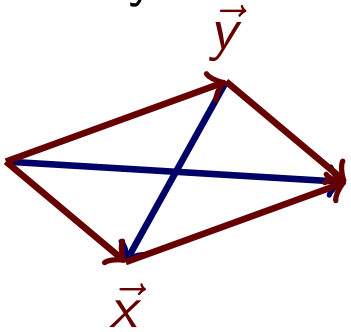
1. Kosinová věta: Nenulové vektory $\vec{x}$ a $\vec{y}$ určují trojúhelník



Platí: $\|\vec{x}-\vec{y}\|^2 = \|\vec{x}\|^2 + \|\vec{y}\|^2 - \underbrace{2\cdot\langle\vec{x}\mid\vec{y}\rangle}_{2\cdot\|\vec{x}\|\cdot\|\vec{y}\|\cdot\cos\varphi}$.

Případu, kdy $\langle\vec{x}\mid\vec{y}\rangle = 0$, se říká Pythagorova věta.

2. Rovnoběžníková rovnost: Dva nenulové vektory $\vec{x}$ a $\vec{y}$ určují strany rovnoběžníka s úhlopříčkami $\vec{x}-\vec{y}$ a $\vec{x}+\vec{y}$.



Platí: $\|\vec{x}-\vec{y}\|^2 + \|\vec{x}+\vec{y}\|^2 = 2(\|\vec{x}\|^2 + \|\vec{y}\|^2)$.

Upravujte:

$$\|\vec{x}-\vec{y}\|^2 + \|\vec{x}+\vec{y}\|^2 = \langle\vec{x}-\vec{y}\mid\vec{x}-\vec{y}\rangle + \langle\vec{x}+\vec{y}\mid\vec{x}+\vec{y}\rangle = \dots$$

Poznámky (vztah skalárního součinu, normy a metriky)

Skalární součin indukuje normu a ta indukuje metriku (také: distanci) na množině L. Jde o funkci $d : L \times L \to \mathbb{R}$, která splňuje:

1. $d(\vec{x}, \vec{y}) \geqslant 0$, rovnost nastává právě tehdy, když $\vec{x} = \vec{y}$.
2. $d(\vec{x}, \vec{y}) = d(\vec{y}, \vec{x})$.
3. $d(\vec{x}, \vec{y}) \leqslant d(\vec{x}, \vec{z}) + d(\vec{z}, \vec{y})$.

Stačí definovat $d(\vec{x}, \vec{y}) = \|\vec{x} - \vec{y}\|$.
O prostoru L s metrikou d mluvíme jako o metrickém lineárním prostoru.
Pro lineární prostory platí:[a] skalární součin $\rightsquigarrow$ norma $\rightsquigarrow$ metrika.

---

[a] Obrácené implikace neplatí. Například $d(x, y) = \begin{cases} 1, & \text{když } x \neq y, \\ 0, & \text{když } x = y, \end{cases}$ je metrika na $\mathbb{R}$, která nevznikla z žádné normy na $\mathbb{R}$ (tj $\|x\| = d(0, x)$ není norma). Norma $\left\| \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right\| = |x_1| + |x_2|$ na $\mathbb{R}^2$ nevznikla z žádného skalárního součinu na $\mathbb{R}^2$, protože nesplňuje rovnoběžníkovou rovnost.

Poznámka

Předchozí úvahy říkají, že prostory se skalárním součinem se chovají tak, jak jsme zvyklí z klasické geometrie. Další příklad ukazuje, že klasická geometrie nemusí být vždy vhodná.

Příklad (nikoli positivně definitní „skalární součin“)

Na $\mathbb{R}^4$ definujte $\left\langle \begin{pmatrix} t \\ x \\ y \\ z \end{pmatrix} \middle| \begin{pmatrix} t' \\ x' \\ y' \\ z' \end{pmatrix} \right\rangle = -tt' + xx' + yy' + zz'$. Protože $\left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \middle| \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\rangle = -1$, nejde o positivně definitní „skalární součin“.

Tento „skalární součin“ je velmi důležitý v teorii relativity. Příslušnému pojmu „vzdálenosti“ vektorů $\mathbf{x}$ a $\mathbf{y}$ v $\mathbb{R}^4$ se říká Lorentzova metrika Minkowského časoprostoru.[a]

[a] V tomto časoprostoru je rychlost světla c rovna 1.

Příklad (Lorentzova transformace)

Pohyb podsvětelnou rychlostí v ve směru osy x v Minkowského časoprostoru je lineární zobrazení $\mathbf{L} : \mathbb{R}^4 \to \mathbb{R}^4$, pro které platí

$$\begin{aligned} t' &= \gamma \cdot (t - vx) \\ x' &= \gamma \cdot (x - vt) \\ y' &= y \\ z' &= z \end{aligned} \qquad \text{kde } 0 \leqslant v < c = 1 \text{ a } \gamma = \frac{1}{\sqrt{1 - v^2}}.$$

Vzhledem ke kanonické bázi $\mathbb{R}^4$ má zobrazení $\mathbf{L}$ matici

$$\mathbf{\Lambda} = \begin{pmatrix} \gamma & -v \cdot \gamma & 0 & 0 \\ -v \cdot \gamma & \gamma & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \cosh \varphi & -\sinh \varphi & 0 & 0 \\ -\sinh \varphi & \cosh \varphi & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

kde $\varphi = \ln(\gamma(1 + v))$. Pohyb ve směru osy x podsvětelnou rychlostí v v Minkowského časoprostoru lze tedy interpretovat jako rotaci (v rovině dané osami t a x) o úhel φ v hyperbolické geometrii.

Příklad (rotace a standardní skalární součin)

Připomenutí: rotace o úhel α je $\mathbf{R}_\alpha : \mathbb{R}^2 \to \mathbb{R}^2$, kde[a]

$$\mathbf{R}_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

Potom platí:

$$\begin{aligned} \langle \mathbf{R}_\alpha \cdot \mathbf{x} \mid \mathbf{R}_\alpha \cdot \mathbf{y} \rangle &= (\mathbf{R}_\alpha \cdot \mathbf{x})^T \cdot (\mathbf{R}_\alpha \cdot \mathbf{y}) \\ &= \mathbf{x}^T \cdot \mathbf{R}_\alpha^T \cdot \mathbf{R}_\alpha \cdot \mathbf{y} \\ &= \mathbf{x}^T \cdot \mathbf{R}_\alpha^{-1} \cdot \mathbf{R}_\alpha \cdot \mathbf{y} \\ &= \mathbf{x}^T \cdot \mathbf{y} \\ &= \langle \mathbf{x} \mid \mathbf{y} \rangle \end{aligned}$$

Tudíž platí: $\|\mathbf{x}\| = \|\mathbf{R}_\alpha \cdot \mathbf{x}\|$ a $\|\mathbf{x} - \mathbf{y}\| = \|\mathbf{R}_\alpha \cdot \mathbf{x} - \mathbf{R}_\alpha \cdot \mathbf{y}\|$.

Ukázali jsme: rotace zachovává standardní skalární součin, normu a metriku.

[a] Povšimněme si: $\mathbf{R}_\alpha^T = \mathbf{R}_\alpha^{-1}$.

Tvrzení

Pro matici $\mathbf{A} : \mathbb{R}^n \to \mathbb{R}^n$ jsou následující podmínky ekvivalentní:

1. $\mathbf{A}$ zachovává standardní skalární součin v $\mathbb{R}^n$.
2. $\mathbf{A}$ je regulární a platí $\mathbf{A}^T = \mathbf{A}^{-1}$.

Důkaz.

Z (1) plyne (2):[a] $\delta_{ij} = \langle \mathbf{e}_i \mid \mathbf{e}_j \rangle = \langle \mathbf{A} \cdot \mathbf{e}_i \mid \mathbf{A} \cdot \mathbf{e}_j \rangle = \mathbf{e}_i^T \cdot \mathbf{A}^T \cdot \mathbf{A} \cdot \mathbf{e}_j$, takže $\mathbf{A}^T \cdot \mathbf{A} = \mathbf{E}_n$.
Ze (2) plyne (1):
$\langle \mathbf{A} \cdot \mathbf{x} \mid \mathbf{A} \cdot \mathbf{y} \rangle = \mathbf{x}^T \cdot \mathbf{A}^T \cdot \mathbf{A} \cdot \mathbf{y} = \mathbf{x}^T \cdot \mathbf{A}^{-1} \cdot \mathbf{A} \cdot \mathbf{y} = \mathbf{x}^T \cdot \mathbf{y} = \langle \mathbf{x} \mid \mathbf{y} \rangle$. ■

[a] Připomenutí: pro Kroneckerův symbol δ platí $\delta_{ij} = 0$ pro $i \neq j$ a $\delta_{ii} = 1$.

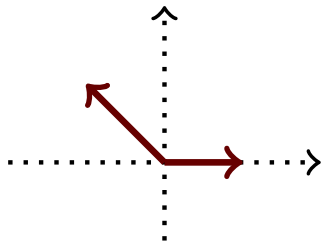
Poznámka (základní transformace prostoru $\mathbb{R}^2$)

Projekce na osy a změna měřítka nezachovávají standardní skalární součin! Rotace zachovává standardní skalární součin (viz předchozí příklad). Reflexe podle os x a y standardní skalární součin zachovávají.

Příklad (netradiční skalární součin v $\mathbb{R}^2$)

Pro $\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \rangle = x_1y_1 + x_2y_1 + x_1y_2 + 2x_2y_2$ v $\mathbb{R}^2$ platí rovnost $\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mid \begin{pmatrix} -1 \\ 1 \end{pmatrix} \rangle = 0$.

To znamená, že náš skalární součin „vidí“ vektory $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix}$ jako navzájem kolmé:



To může být velmi praktické. Jak tedy rozpoznat obecný skalární součin? Všimněme si, že náš součin je zadán jistou maticí **G**:

$$\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \rangle = \begin{pmatrix} x_1 & x_2 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}}_{\mathbf{G}} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = x_1y_1 + x_2y_1 + x_1y_2 + 2x_2y_2$$

Co dál?

Budeme chtít pochopit, které matice $\mathbf{G}$ zadávají skalární součiny v prostoru $\mathbb{R}^n$.

Uvidíme, že skalární součiny v $\mathbb{R}^n$ přesně odpovídají maticím, kterým říkáme positivně definitní.

Charakterisace skalárních součinů v $\mathbb{R}^n$

Odpřednesenou látku naleznete v kapitolách 12.1, 12.2 a 12.3 skript *Abstraktní a konkrétní lineární algebra*.

Dnešní přednáška

1. V této přednášce (a ve všech přednáškách týkajících se skalárního součinu) se zaměříme na lineární prostory nad $\mathbb{R}$.
2. Charakterisace matic, které zadávají skalární součiny v prostoru $\mathbb{R}^n$.
3. Konstrukce skalárních součinů požadovaných vlastností.

Příští přednášky ke skalárnímu součinu

1. Ortogonální báze a ortonormální báze.
2. Ortogonalisační proces a ortonormalisační proces.
3. Ortogonální projekce a ortogonální rejekce.

Připomenutí (dva různé skalární součiny v $\mathbb{R}^2$)

1. Standardní skalární součin:

$$\left\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \middle| \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle = x_1 y_1 + x_2 y_2 = \begin{pmatrix} x_1 & x_2 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{\mathbf{E}_2} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

2. „Nezvyklý“ skalární součin:

$$\left\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \middle| \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle = x_1 y_1 + x_2 y_1 + x_1 y_2 + 2 x_2 y_2 = \begin{pmatrix} x_1 & x_2 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}}_{\mathbf{G}} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

V obou případech je součin zadán jistou maticí typu 2×2. Je to náhoda?

Co dál?

Ukážeme, že skalární součiny v $\mathbb{R}^n$ odpovídají přesně těm čtvercovým maticím, kterým říkáme positivně definitní.

Definice (positivně definitní matice)

Řekneme, že matice $\mathbf{G}$ typu $n \times n$ nad $\mathbb{R}$ je positivně definitní, když existuje matice $\mathbf{R}$ s lineárně nezávislými sloupci tak, že $\mathbf{G} = \mathbf{R}^T \cdot \mathbf{R}$.

Poznámky

1. Protože $\mathbf{G}^T = (\mathbf{R}^T \cdot \mathbf{R})^T = \mathbf{R}^T \cdot \mathbf{R} = \mathbf{G}$, je každá positivně definitní matice $\mathbf{G}$ symetrická.

Poznámky (pokrač.)

2. Positivně definitní matice $\mathbf{G}$ zobecňují kladná reálná čísla: matice $\mathbf{R}$ je „druhá odmocnina“[a] matice $\mathbf{G}$.

   Opravdu: Matice $\mathbf{G} = (g)$ typu 1×1 je positivně definitní právě tehdy, když $g > 0$.

   1. Ať $\mathbf{G} = (g) = \mathbf{R}^T \cdot \mathbf{R}$. Pak $\mathbf{R} = \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}$ a platí $g = r_1^2 + \cdots + r_n^2$.

      Protože jediný sloupec $\mathbf{R}$ musí být lineárně nezávislý, je $g > 0$.
   2. Je-li $g > 0$, platí $(g) = (\sqrt{g})^T \cdot (\sqrt{g})$. Protože $\sqrt{g} > 0$, je jediný sloupec matice $\mathbf{R} = (\sqrt{g})$ lineárně nezávislý. Matice $\mathbf{G}$ je tudíž positivně definitní.

[a] Jde jen o slogan: matice $\mathbf{R}$ není určena jednoznačně. Například platí $(4) = (2)^T \cdot (2) = \begin{pmatrix} 2 \\ 0 \end{pmatrix}^T \cdot \begin{pmatrix} 2 \\ 0 \end{pmatrix}$.

Věta (charakterisace positivně definitních matic)

Pro matici $\mathbf{G} = (g_{ij})_{i=1,\dots,n, j=1,\dots,n}$ nad $\mathbb{R}$ jsou následující podmínky ekvivalentní:

1. $\mathbf{G}$ je positivně definitní.
2. Matice $\mathbf{G}$ je symetrická a determinanty všech matic $\mathbf{G}_k = (g_{ij})_{i=1,\dots,k, j=1,\dots,k}$, kde $1 \leqslant k \leqslant n$, jsou kladné.[a]
3. Matice $\mathbf{G}$ je symetrická a nerovnost $\mathbf{x}^T \cdot \mathbf{G} \cdot \mathbf{x} \geqslant 0$ platí pro všechna $\mathbf{x}$ z $\mathbb{R}^n$ (rovnost platí pouze pro $\mathbf{x} = \mathbf{o}$).
4. Matice $\mathbf{G}$ je symetrická a $\mathrm{char}_{\mathbf{G}}(x)$ má všechny kořeny reálné a kladné.
5. Existuje regulární matice $\mathbf{R}$ tak, že platí $\mathbf{G} = \mathbf{R}^T \cdot \mathbf{R}$.

[a] Tento test positivní definitnosti budete využívat v analýze pro určování lokálních minim funkcí více proměnných.

Důkaz.

Bez důkazu (je těžký, pro zájemce: Tvrzení 12.3.4 skript). ■

Poznámka o Choleskyho faktorisaci — nepovinné

1. Připomenutí definice: $\mathbf{G}$ je positivně definitní právě tehdy, když $\mathbf{G} = \mathbf{R}^T \cdot \mathbf{R}$, kde $\mathbf{R}$ má lineárně nezávislé sloupce.
2. Předchozí věta: $\mathbf{G}$ je positivně definitní právě tehdy, když $\mathbf{G} = \mathbf{R}^T \cdot \mathbf{R}$, kde $\mathbf{R}$ je regulární.
3. Zesílení věty: $\mathbf{G}$ je positivně definitní právě tehdy, když $\mathbf{G} = \mathbf{R}^T \cdot \mathbf{R}$, kde $\mathbf{R}$ je regulární v horním blokovém tvaru.

Rovnosti $\mathbf{G} = \mathbf{R}^T \cdot \mathbf{R}$ pro regulární matici $\mathbf{R}$ v horním blokovém tvaru se říká Choleskyho faktorisace matice $\mathbf{G}$. Příklad Choleskyho faktorisace:

$$\begin{pmatrix} 1 & 2 & 8 \\ 2 & 8 & 12 \\ 8 & 12 & 27 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 3 \\ 0 & 0 & 3 \end{pmatrix}^T \cdot \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 3 \\ 0 & 0 & 3 \end{pmatrix}$$

Choleskyho faktorisaci lze nalézt algoritmem, viz skripta, Příklad 12.3.6. Tento algoritmus je nepovinný.

Příklady

1. Protože $\mathbf{E}_n = \mathbf{E}_n^T \cdot \mathbf{E}_n$, je jednotková matice $\mathbf{E}_n$ positivně definitní.

   Připomeňme: $\mathbf{E}_n$ zadává standardní skalární součin $\langle \mathbf{x} \mid \mathbf{y} \rangle = \mathbf{x}^T \cdot \mathbf{E}_n \cdot \mathbf{y} = \mathbf{x}^T \cdot \mathbf{y}$ v $\mathbb{R}^n$.

2. Matice $\mathbf{G} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ je positivně definitní podle předchozí věty: $\mathbf{G}$ je symetrická a platí nerovnosti $\det(\mathbf{G}_1) = \det(1) > 0$ a $\det(\mathbf{G}_2) = \det(\mathbf{G}) > 0$.

   Připomeňme: $\mathbf{G}$ zadává „nezvyklý“ skalární součin $\langle \mathbf{x} \mid \mathbf{y} \rangle = \mathbf{x}^T \cdot \mathbf{G} \cdot \mathbf{y}$ v $\mathbb{R}^2$.

Příklady (pokrač.)

3. Matice

$$\mathbf{G} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

není positivně definitní podle předchozí věty: platí $\det(\mathbf{G}_1) < 0$, $\det(\mathbf{G}_2) < 0$, $\det(\mathbf{G}_3) < 0$, $\det(\mathbf{G}_4) < 0$.

Připomeňme (minulá přednáška): $\mathbf{G}$ zadává „skalární součin“ $\langle \mathbf{x} \mid \mathbf{y} \rangle = \mathbf{x}^T \cdot \mathbf{G} \cdot \mathbf{y}$ v Minkowského časoprostoru $\mathbb{R}^4$.

Věta (obecný tvar skalárního součinu v $\mathbb{R}^n$)

1. Ať $\mathbf{G}$ je positivně definitní matice typu $n \times n$ nad $\mathbb{R}$. Potom maticový součin

$$\mathbf{x}^T \cdot \mathbf{G} \cdot \mathbf{y}$$

   definuje skalární součin v $\mathbb{R}^n$.

2. Každý skalární součin $\langle - \mid - \rangle$ v $\mathbb{R}^n$ definuje positivně definitní[a] matici $\mathbf{G} = (g_{ij})_{i=1,\dots,n, j=1,\dots,n}$, kde $g_{ij} = \langle \mathbf{e}_i \mid \mathbf{e}_j \rangle$. Potom platí rovnost $\langle \mathbf{x} \mid \mathbf{y} \rangle = \mathbf{x}^T \cdot \mathbf{G} \cdot \mathbf{y}$.

---

[a] Matici $\mathbf{G}$ říkáme metrický tensor (také: Gramova matice) skalárního součinu $\langle - \mid - \rangle$.

Důkaz.

Přednáška. ■

Příklad (popis všech skalárních součinů v $\mathbb{R}^2$)

Matice $\mathbf{G} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ je positivně definitní právě tehdy, když platí:

1. $\mathbf{G}$ je symetrická matice, tj. když platí $c = b$.
2. $\det(\mathbf{G}_1) = a > 0$ a $\det(\mathbf{G}_2) = \det(\mathbf{G}) = ad - b^2 > 0$.

To znamená: výraz

$$ax_1y_1 + b(x_1y_2 + x_2y_1) + dx_2y_2$$

zadává skalární součin $\left\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle$ v $\mathbb{R}^2$ právě tehdy, když platí nerovnosti $a > 0$ a $ad - b^2 > 0$.

Příklad (jednotková kružnice pro skalární součin v $\mathbb{R}^2$)

Pro positivně definitní[a] matici $\mathbf{G} = \begin{pmatrix} a & b \\ b & d \end{pmatrix}$ a příslušný skalární součin $\langle - \mid - \rangle$ je množina[b]

$$\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid \| \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \| = 1 \}$$

jednotková kružnice. Rovnice této kružnice je

$$ax_1^2 + 2bx_1x_2 + dx_2^2 = 1$$

a my ukážeme, že v bázi vlastních vektorů matice $\mathbf{G}$, jde o elipsu.

---

[a] Připomenutí: platí $a > 0$ a $ad - b^2 > 0$.

[b] Připomenutí: $\| - \|$ je norma vytvořená skalárním součinem $\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \rangle = \begin{pmatrix} x_1 & x_2 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ b & d \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$.

Příklad (jednotková kružnice, pokrač.)

1. Positivně definitní matice $\mathbf{G} = \begin{pmatrix} a & b \\ b & d \end{pmatrix}$ má charakteristický polynom $\mathrm{char}_{\mathbf{G}}(x) = x^2 - (a+d)x + (ad - b^2)$ s diskriminantem $D = (a-d)^2 + 4b^2 \geqslant 0$.
2. V případě $D = (a-d)^2 + 4b^2 = 0$ platí $b = 0$ a $a = d > 0$.

   Pak matice $\mathbf{G}$ je diagonální, vlastní vektory jsou $\mathbf{e}_1$ a $\mathbf{e}_2$ a v bázi $(\mathbf{e}_1, \mathbf{e}_2)$ má rovnice jednotkové kružnice tvar

$$x_1^2 + x_2^2 = \left(\frac{1}{\sqrt{a}}\right)^2$$

Příklad (jednotková kružnice, pokrač.)

3. V případě $D = (a-d)^2 + 4b^2 > 0$ rozlišíme dva případy:
   1. $b = 0$. Pak $\mathbf{G}$ je diagonální a $a \neq d$. Vlastní vektory $\mathbf{G}$ jsou $\mathbf{e}_1$ a $\mathbf{e}_2$ a v bázi $(\mathbf{e}_1, \mathbf{e}_2)$ má rovnice jednotkové kružnice tvar
   $$\left(\frac{x_1}{\sqrt{d}}\right)^2 + \left(\frac{x_2}{\sqrt{a}}\right)^2 = \left(\frac{1}{\sqrt{ad}}\right)^2$$
   protože $d > 0$, neboť $\mathbf{G}$ je positivně definitní. Jde tedy o elipsu.
   2. $b \neq 0$. Matice $\mathbf{G}$ pak má dvě různé kladné vlastní hodnoty
   $$\lambda_1 = \frac{a+d+\sqrt{D}}{2} \qquad \lambda_2 = \frac{a+d-\sqrt{D}}{2}$$
   V bázi $(\mathbf{v}_1, \mathbf{v}_2)$ vlastních vektorů má rovnice jednotkové kružnice tvar
   $$\left(\frac{t_1}{\sqrt{\lambda_2}}\right)^2 + \left(\frac{t_2}{\sqrt{\lambda_1}}\right)^2 = \left(\frac{1}{\sqrt{\lambda_1\lambda_2}}\right)^2$$
   Jde tedy o elipsu.

Připomenutí

Minulá přednáška: každý skalární součin vytváří normu.
Je-li $\langle - \mid - \rangle$ skalární součin na $\mathbb{R}^n$, pak

1. vektory $\mathbf{x}$ a $\mathbf{y}$ jsou ortogonální (také: navzájem kolmé), pokud $\langle \mathbf{x} \mid \mathbf{y} \rangle = 0$,
2. norma (také: velikost) vektoru $\mathbf{x}$ je $\|\mathbf{x}\| = \sqrt{\langle \mathbf{x} \mid \mathbf{x} \rangle}$,
3. vektor $\mathbf{x}$ je normovaný, pokud $\|\mathbf{x}\| = 1$.

Tvrzení (kanonická báze $\mathbb{R}^n$ a standardní skalární součin v $\mathbb{R}^n$)

Pro standardní skalární součin $\langle \mathbf{x} \mid \mathbf{y} \rangle = \mathbf{x}^T \cdot \mathbf{y}$ a kanonickou bázi $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ v $\mathbb{R}^n$ platí:[a] $\langle \mathbf{e}_i \mid \mathbf{e}_j \rangle = \mathbf{e}_i^T \cdot \mathbf{e}_j = \delta_{ij} = \begin{cases} 0, & \text{pro } i \neq j \\ 1, & \text{pro } i = j \end{cases}$.

[a] Takovým bázím budeme říkat ortonormální a obecně je budeme studovat příště. To jest: vektory takové báze jsou na sebe navzájem kolmé a každý vektor takové báze má normu 1.

Věta (každou bázi $\mathbb{R}^n$ lze považovat za ortonormální)

Ať $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ je jakákoli uspořádaná báze $\mathbb{R}^n$. Potom existuje jediný skalární součin $\langle - \mid - \rangle$ takový, že $\langle \mathbf{b}_i \mid \mathbf{b}_j \rangle = \delta_{ij}$.

Důkaz.

Označme $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$, připomenutí (téma 5B):
$\mathbf{T}_{B \mapsto K_n} \cdot \mathbf{e}_i = \mathbf{b}_i$, čili $\mathbf{T}_{K_n \mapsto B} \cdot \mathbf{b}_i = \mathbf{e}_i$, pro vš $i = 1, \ldots, n$.

1. Existence hledaného skalárního součinu.
   Definujte $\mathbf{G} = (\mathbf{T}_{K_n \mapsto B})^T \cdot \mathbf{T}_{K_n \mapsto B}$. Potom matice $\mathbf{G}$ je positivně definitní a platí

$$\begin{aligned}
\langle \mathbf{b}_i \mid \mathbf{b}_j \rangle &= \mathbf{b}_i^T \cdot \mathbf{G} \cdot \mathbf{b}_j \\
&= \underbrace{\mathbf{b}_i^T \cdot (\mathbf{T}_{K_n \mapsto B})^T}_{=(\mathbf{T}_{K_n \mapsto B} \cdot \mathbf{b}_i)^T = \mathbf{e}_i^T} \cdot \underbrace{\mathbf{T}_{K_n \mapsto B} \cdot \mathbf{b}_j}_{=\mathbf{e}_j} \\
&= \mathbf{e}_i^T \cdot \mathbf{e}_j = \delta_{ij}
\end{aligned}$$

Důkaz (pokrač.)

2. Jednoznačnost hledaného skalárního součinu.
   Ať $\mathbf{b}_i^T \cdot \mathbf{G}_1 \cdot \mathbf{b}_j = \mathbf{b}_i^T \cdot \mathbf{G}_2 \cdot \mathbf{b}_j = \delta_{ij}$. Ukážeme $\mathbf{G}_1 = \mathbf{G}_2$.

   Opravdu: platí $\mathbf{b}_i^T \cdot (\mathbf{G}_1 - \mathbf{G}_2) \cdot \mathbf{b}_j = 0$ pro vš. i, j.

   To znamená $(\mathbf{T}_{B \mapsto K_n} \cdot \mathbf{e}_i)^T \cdot (\mathbf{G}_1 - \mathbf{G}_2) \cdot (\mathbf{T}_{B \mapsto K_n} \cdot \mathbf{e}_j) = 0$ pro vš. i, j, neboli $\mathbf{e}_i^T \cdot (\mathbf{T}_{B \mapsto K_n})^T \cdot (\mathbf{G}_1 - \mathbf{G}_2) \cdot \mathbf{T}_{B \mapsto K_n} \cdot \mathbf{e}_j = 0$ pro vš. i, j.

   Ukázali jsme rovnost $(\mathbf{T}_{B \mapsto K_n})^T \cdot (\mathbf{G}_1 - \mathbf{G}_2) \cdot \mathbf{T}_{B \mapsto K_n} = \mathbf{O}_{n,n}$.

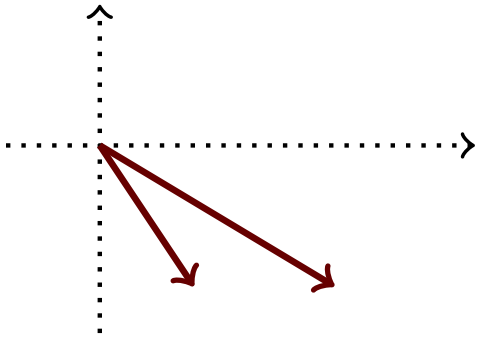
   Protože $\mathbf{T}_{B \mapsto K_n}$ i $(\mathbf{T}_{B \mapsto K_n})^T$ jsou regulární, platí $\mathbf{G}_1 - \mathbf{G}_2 = \mathbf{O}_{n,n}$.

   Tudíž $\mathbf{G}_1 = \mathbf{G}_2$.

Příklad

Najděte skalární součin v $\mathbb{R}^2$ takový, aby vektory $\begin{pmatrix} 2 \\ -3 \end{pmatrix}$ a $\begin{pmatrix} 5 \\ -3 \end{pmatrix}$ byly navzájem kolmé a každý měl normu 1.

Obrázek:



Skalární součin nalezneme podle předchozího tvrzení:

1. Pro $\mathbf{T}_{B \mapsto K_n} = \begin{pmatrix} 2 & 5 \\ -3 & -3 \end{pmatrix}$ je[a] $\mathbf{T}_{K_n \mapsto B} = (\mathbf{T}_{B \mapsto K_n})^{-1} = \frac{1}{9} \cdot \begin{pmatrix} -3 & -5 \\ 3 & 2 \end{pmatrix}$ a $\mathbf{G} = (\mathbf{T}_{K_n \mapsto B})^T \cdot \mathbf{T}_{K_n \mapsto B} = \frac{1}{81} \cdot \begin{pmatrix} 18 & 21 \\ 21 & 29 \end{pmatrix}$.

[a] Matici $\mathbf{T}_{K_n \mapsto B}$ nalezneme nejrychleji pomocí adjungované matice.

Příklad (pokrač.)

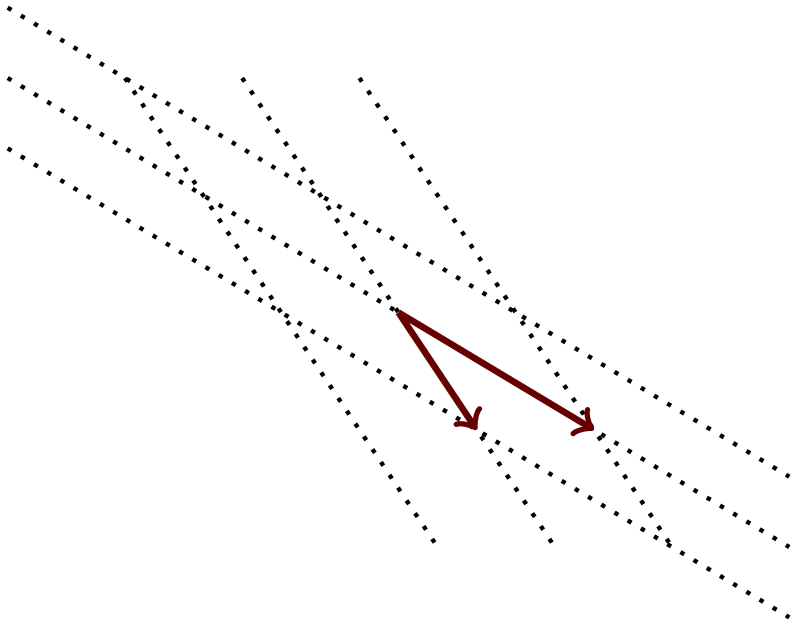
2. Hledaný skalární součin je
$$\left\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle = \frac{18}{81} \cdot x_1 y_1 + \frac{21}{81} \cdot x_1 y_2 + \frac{21}{81} \cdot x_2 y_1 + \frac{29}{81} \cdot x_2 y_2.$$
3. $\left\langle \begin{pmatrix} 2 \\ -3 \end{pmatrix} \mid \begin{pmatrix} 5 \\ -3 \end{pmatrix} \right\rangle =$
$$\frac{18}{81} \cdot 2 \cdot 5 + \frac{21}{81} \cdot 2 \cdot (-3) + \frac{21}{81} \cdot (-3) \cdot 5 + \frac{29}{81} \cdot (-3) \cdot (-3) = 0.$$
4. $\left\langle \begin{pmatrix} 2 \\ -3 \end{pmatrix} \mid \begin{pmatrix} 2 \\ -3 \end{pmatrix} \right\rangle =$
$$\frac{18}{81} \cdot 2 \cdot 2 + \frac{21}{81} \cdot 2 \cdot (-3) + \frac{21}{81} \cdot (-3) \cdot 2 + \frac{29}{81} \cdot (-3) \cdot (-3) = 1.$$
5. $\left\langle \begin{pmatrix} 5 \\ -3 \end{pmatrix} \mid \begin{pmatrix} 5 \\ -3 \end{pmatrix} \right\rangle =$
$$\frac{18}{81} \cdot 5 \cdot 5 + \frac{21}{81} \cdot 5 \cdot (-3) + \frac{21}{81} \cdot (-3) \cdot 5 + \frac{29}{81} \cdot (-3) \cdot (-3) = 1.$$

K čemu jsou takové výpočty dobré?

Skalární součin

$$\left\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle = \frac{18}{81} \cdot x_1 y_1 + \frac{21}{81} \cdot x_1 y_2 + \frac{21}{81} \cdot x_2 y_1 + \frac{29}{81} \cdot x_2 y_2$$

z předchozího příkladu „vidí“



jako jednotkovou pravoúhlou síť.

Co zatím v $\mathbb{R}^n$ umíme

Pro zadanou bázi $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ prostoru $\mathbb{R}^n$ umíme sestrojit skalární součin $\langle - \mid - \rangle$ v $\mathbb{R}^n$ tak, že $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ je ortonormální báze vzhledem k $\langle - \mid - \rangle$.

Příště se v $\mathbb{R}^n$ naučíme

Pro zadanou bázi $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ prostoru $\mathbb{R}^n$ a zadaný skalární součin $\langle - \mid - \rangle$ v $\mathbb{R}^n$ nalezneme novou bázi $(\mathbf{c}_1, \ldots, \mathbf{c}_n)$, která je ortonormální vzhledem k $\langle - \mid - \rangle$.

Hledaná báze bude navíc splňovat rovnost $\operatorname{span}(\mathbf{b}_1, \ldots, \mathbf{b}_k) = \operatorname{span}(\mathbf{c}_1, \ldots, \mathbf{c}_k)$ pro všechna $k = 1, \ldots, n$.

K tomu bude zapotřebí zavedení nových pojmů: ortogonální projekce a ortogonální rejekce.

Ortogonalisace a ortogonální projekce

Odpřednesenou látku naleznete v kapitole 12.4 skript *Abstraktní a konkrétní lineární algebra*.

Minulé přednášky

1. Definice skalárního součinu v lineárních prostorech nad $\mathbb{R}$.
2. Úplný popis skalárních součinů v prostoru $\mathbb{R}^n$.

Dnešní přednáška

1. V této přednášce (a ve všech přednáškách týkajících se skalárního součinu) se zaměříme na lineární prostory nad $\mathbb{R}$.
2. Ortogonální báze a ortonormální báze.
3. Ortogonální projekce. Ortogonalisace a ortonormalisace.

Příští přednáška

1. Hlubší poznatky o ortogonálních projekcích.
2. Metoda nejmenších čtverců.[a]

[a] Budeme se věnovat pouze nejjednodušší formě metody nejmenších čtverců v $\mathbb{R}^n$ se standardním skalárním součinem. Vše je podrobně popsáno ve výtahu z příští přednášky. Viz také Dodatek C skript.

Připomenutí vlastností ortogonality (minulé přednášky)

Platí-li $\langle \vec{x} \mid \vec{y} \rangle = 0$, říkáme, že vektory $\vec{x}$ a $\vec{y}$ jsou ortogonální (také: navzájem kolmé).

1. Pozor: nulový vektor $\vec{o}$ je kolmý na každý vektor $\vec{x}$.
   Obráceně: jestliže $\vec{x}$ je kolmý na každý vektor, pak $\vec{x} = \vec{o}$.
2. Abychom ukázali, že rovnost $\langle \vec{x} \mid \vec{v} \rangle = 0$ platí pro každý vektor $\vec{v}$ ze $\mathrm{span}(M)$, stačí ukázat, že všechny vektory $\vec{m}$ z M platí rovnost $\langle \vec{x} \mid \vec{m} \rangle = 0$.

   Speciální případ výše uvedeného je:[a]

   Ať $(\vec{b}_1, \ldots, \vec{b}_k)$ je báze lineárního podprostoru W lineárního prostoru L. Jestliže platí $\langle \vec{x} \mid \vec{b}_i \rangle = 0$ pro všechna $i = 1, \ldots, k$, potom platí $\langle \vec{x} \mid \vec{w} \rangle = 0$ pro všechny vektory $\vec{w}$ z W.

[a] Tento speciální případ několikrát (bez dalších komentářů) v dnešní přednášce použijeme.

Tvrzení (lineární nezávislost ortogonální množiny vektorů)

Ať M je jakákoli množina nenulových vektorů s vlastností $\langle \vec{x} \mid \vec{y} \rangle = 0$ pro jakékoli různé vektory $\vec{x}$, $\vec{y}$ z M.[a] Pak M je lineárně nezávislá množina.

[a] Takové množině říkáme ortogonální množina.

Důkaz.

Ať $\{\vec{x}_1, \ldots, \vec{x}_n\}$ je jakákoli konečná podmnožina M. Ať $\sum_{i=1}^{n} a_i \cdot \vec{x}_i = \vec{o}$. Pro libovolné pevné $i_0 \in \{1, \ldots, n\}$ platí:

$$0 = \langle \vec{x}_{i_0} \mid \vec{o} \rangle = \langle \vec{x}_{i_0} \mid \sum_{i=1}^{n} a_i \cdot \vec{x}_i \rangle = \sum_{i=1}^{n} a_i \cdot \langle \vec{x}_{i_0} \mid \vec{x}_i \rangle = a_{i_0} \cdot \langle \vec{x}_{i_0} \mid \vec{x}_{i_0} \rangle.$$

Protože $\vec{x}_{i_0} \neq \vec{o}$, platí $\langle \vec{x}_{i_0} \mid \vec{x}_{i_0} \rangle \neq 0$. Proto $a_{i_0} = 0$. ■

Několik sloganů

1. Jestliže $\dim(L) = n$, potom každá ortogonální množina v L má nejvýše n prvků.

   Slogan: v prostoru dimense n může existovat maximálně n navzájem na sebe kolmých nenulových vektorů.

2. Ortogonální množině v L, která tvoří bázi L, říkáme ortogonální báze.

   Slogan:[a] ortogonální báze je pravoúhlý souřadnicový systém.

3. Každou bázi $(\vec{b}_1, \ldots, \vec{b}_n)$ lze normalisovat: v bázi $\left(\frac{\vec{b}_1}{\|\vec{b}_1\|}, \ldots, \frac{\vec{b}_n}{\|\vec{b}_n\|}\right)$ mají všechny vektory normu 1.

   Slogan: normální báze má jednotkové úseky na jednotlivých souřadnicových osách.

[a] Pozor: jde jen o slogan. Víme, že například leckterý skalární součin v rovině může jako ortogonální vidět vektory, které „ve skutečnosti“ nesvírají pravý úhel.

Definice (ortonormální báze, čili normální a ortogonální báze)

Bázi $(\vec{b}_1, \ldots, \vec{b}_n)$ prostoru se skalárním součinem, která splňuje rovnost $\langle \vec{b}_i \mid \vec{b}_j \rangle = \delta_{ij}$,[a] říkáme ortonormální.

[a] Kroneckerův symbol δ splňuje: $\delta_{ii} = 1$, $\delta_{ij} = 0$ pro $i \neq j$.

Poznámky

1. Kanonická báze $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ prostoru $\mathbb{R}^n$ je ortonormální vzhledem ke standardnímu skalárnímu součinu.
2. Pro jakoukoli bázi $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ prostoru $\mathbb{R}^n$ existuje jednoznačně určený skalární součin, ve kterém je tato báze ortonormální (viz minulou přednášku).

   Stejnou větu lze dokázat pro obecné prostory nad $\mathbb{R}$ konečné dimense. To dokazovat nebudeme.
3. Ortonormální báze jsou důležité: umožňují „zpříjemnit“ řadu výpočtů. Viz dále.

Tvrzení (výpočet souřadnic v ortonormální bázi)

Ať $B = (\vec{b}_1, \dots, \vec{b}_n)$ je ortonormální báze prostoru se skalárním součinem. Pak[a] $\vec{x} = \sum_{i=1}^{n} \langle \vec{b}_i \mid \vec{x} \rangle \cdot \vec{b}_i$, čili $\mathbf{coord}_B(\vec{x}) = \begin{pmatrix} \langle \vec{b}_1 \mid \vec{x} \rangle \\ \vdots \\ \langle \vec{b}_n \mid \vec{x} \rangle \end{pmatrix}$.

[a] Tato rovnost je konečně-dimensionální variantou rozvoje ve Fourierovu řadu.

Důkaz.

Definujeme: $\vec{y} = \sum_{i=1}^{n} \langle \vec{b}_i \mid \vec{x} \rangle \cdot \vec{b}_i$. Musíme ukázat: $\vec{y} = \vec{x}$.

Pro libovolné pevné $i_0 \in \{1, \dots, n\}$ platí:

$$\langle \vec{b}_{i_0} \mid \vec{y} \rangle = \langle \vec{b}_{i_0} \mid \sum_{i=1}^{n} \langle \vec{b}_i \mid \vec{x} \rangle \cdot \vec{b}_i \rangle = \sum_{i=1}^{n} \langle \vec{b}_i \mid \vec{x} \rangle \cdot \langle \vec{b}_{i_0} \mid \vec{b}_i \rangle = \langle \vec{b}_{i_0} \mid \vec{x} \rangle.$$

Takže $\langle \vec{b}_{i_0} \mid \vec{x} - \vec{y} \rangle = 0$, pro libovolné pevné $i_0 \in \{1, \dots, n\}$.
Kdyby $\vec{x} - \vec{y} \neq \vec{o}$, byla by $(n+1)$-prvková množina nenulových vektorů $\{\vec{x} - \vec{y}, \vec{b}_1, \dots, \vec{b}_n\}$ lineárně nezávislá.
To není možné: proto je $\vec{y} = \vec{x}$. ∎

Důsledek (skalární součin v ortonormální bázi)

Ať $B = (\vec{b}_1, \dots, \vec{b}_n)$ je ortonomální báze prostoru se skalárním součinem. Pak platí:[a] $\langle \vec{x} \mid \vec{y} \rangle = \sum_{i=1}^{n} \langle \vec{b}_i \mid \vec{x} \rangle \cdot \langle \vec{b}_i \mid \vec{y} \rangle$.

[a] Podle předchozího to znamená: $\langle \vec{x} \mid \vec{y} \rangle = \mathbf{x}^T \cdot \mathbf{y}$, kde $\mathbf{coord}_B(\vec{x}) = \mathbf{x}$ a $\mathbf{coord}_B(\vec{y}) = \mathbf{y}$. Slogan: skalární součin v ortonormální bázi se počítá jako standardní skalární součin souřadnic. Jde o konečně-dimensionální variantu Parsevalovy rovnosti z teorie Fourierových řad.

Důkaz.

$$\langle \vec{x} \mid \vec{y} \rangle = \langle \sum_{i=1}^{n} \langle \vec{b}_i \mid \vec{x} \rangle \cdot \vec{b}_i \mid \sum_{j=1}^{n} \langle \vec{b}_j \mid \vec{y} \rangle \cdot \vec{b}_j \rangle =$$

$$\sum_{i=1}^{n} \sum_{j=1}^{n} \langle \vec{b}_i \mid \vec{x} \rangle \cdot \langle \vec{b}_j \mid \vec{y} \rangle \cdot \langle \vec{b}_i \mid \vec{b}_j \rangle = \sum_{i=1}^{n} \sum_{j=1}^{n} \langle \vec{b}_i \mid \vec{x} \rangle \cdot \langle \vec{b}_j \mid \vec{y} \rangle \cdot \delta_{ij} =$$

$$\sum_{i=1}^{n} \langle \vec{b}_i \mid \vec{x} \rangle \cdot \langle \vec{b}_i \mid \vec{y} \rangle.$$

Poznámka pro ty, kteří chtějí vidět souvislosti (nepovinné)

Předchozí dvě tvrzení (výpočet souřadnic v ortonormální bázi a výpočet skalárního součinu v ortonormální bázi) jsou pouhou instancí toho, že pro ortonormální bázi $B = (\vec{b}_1, \dots, \vec{b}_n)$ prostoru L tvoří seznam

$$B^* = (\langle \vec{b}_1 \mid - \rangle, \dots, \langle \vec{b}_n \mid - \rangle)$$

bázi duálního prostoru L^*, která je duální bází k bázi B.

Více se lze dozvědět v kapitole 3.5 skript.

Zde se objevují výhody Diracovy (také: bra-ket) notace pro skalární součin. Ve fyzice se vektor $\vec{x}$ často píše jako $|\vec{x}\rangle$ (čteme: ket $\vec{x}$). Příslušný kovektor se píše jako $\langle \vec{x}|$ (čteme: bra $\vec{x}$). Skalární součin $\langle \vec{x} \mid \vec{y} \rangle$ je pak aplikací kovektoru $\langle \vec{x}|$ na vektor $|\vec{y}\rangle$. Tudíž $\langle \vec{x} \mid \vec{y} \rangle$ je bra-ket[a] $\vec{x}$ a $\vec{y}$.

[a] Samozřejmě: bra-ket je jazyková hříčka, správně by mělo být bracket.

Další důsledek (úhly vektoru se souřadnicovými osami)

Ať $B = (\vec{b}_1, \ldots, \vec{b}_n)$ je ortonormální báze prostoru se skalárním součinem. Ať vektor $\vec{x}$ je nenulový. Potom pro úhel φ_{i_0}, který vektor $\vec{x}$ svírá se souřadnicovou osou $\vec{b}_{i_0}$, platí rovnost[a]

$\cos\varphi_{i_0} = \dfrac{\langle \vec{b}_{i_0} \mid \vec{x} \rangle}{\|\vec{x}\|}$. Navíc platí $\displaystyle\sum_{i=1}^{n} \cos^2\varphi_i = 1$.

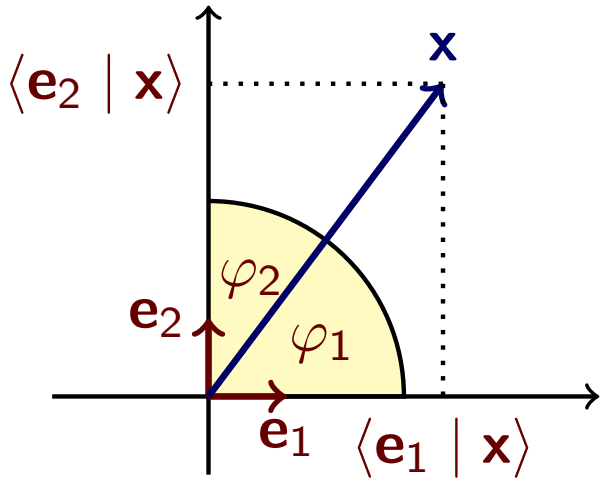
[a] Všimněme si: tvrdíme, že $\langle \vec{b}_{i_0} \mid \vec{x} \rangle$, tj. i_0-tá souřadnice vektoru $\vec{x}$ vzhledem k bázi B, se počítá jako součin $\|\vec{x}\| \cdot \cos\varphi_{i_0}$. To je zobecnění známého faktu z elementární geometrie roviny (viz další stranu).

Důkaz.

Protože $\langle \vec{b}_{i_0} \mid \vec{x} \rangle = \underbrace{\|\vec{b}_{i_0}\|}_{=1} \cdot \|\vec{x}\| \cdot \cos\varphi_{i_0}$, platí $\cos\varphi_{i_0} = \dfrac{\langle \vec{b}_{i_0} \mid \vec{x} \rangle}{\|\vec{x}\|}$.

Dále: $$\sum_{i=1}^{n} \cos^2\varphi_i = \sum_{i=1}^{n} \frac{\langle \vec{b}_i \mid \vec{x} \rangle^2}{\|\vec{x}\|^2} = \frac{\displaystyle\sum_{i=1}^{n} \langle \vec{b}_i \mid \vec{x} \rangle^2}{\|\vec{x}\|^2} = \frac{\langle \vec{x} \mid \vec{x} \rangle}{\|\vec{x}\|^2} = 1. \quad \blacksquare$$

Předchozí tvrzení v rovině s ortonormální bází $(\mathbf{e}_1, \mathbf{e}_2)$



$$\cos\varphi_1 = \frac{\text{orientovaná délka přilehlé odvěsny}}{\text{délka přepony}} = \frac{\langle \mathbf{e}_1 \mid \mathbf{x} \rangle}{\|\mathbf{x}\|}$$

$$\cos\varphi_2 = \frac{\text{orientovaná délka přilehlé odvěsny}}{\text{délka přepony}} = \frac{\langle \mathbf{e}_2 \mid \mathbf{x} \rangle}{\|\mathbf{x}\|}$$

$$\varphi_1 + \varphi_2 = \frac{\pi}{2}, \text{ čili } \cos\varphi_2 = \cos\left(\frac{\pi}{2} - \varphi_1\right) = \sin\varphi_1$$

Tudíž $\cos^2\varphi_1 + \cos^2\varphi_2 = \cos^2\varphi_1 + \sin^2\varphi_1 = 1$.

Projekce na přímku a rejekce přímkou

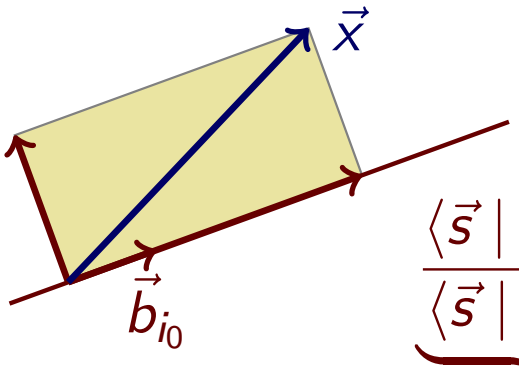
Ať $\vec{s}$ je nenulový vektor v prostoru se skalárním součinem. Potom pro každý vektor $\vec{x}$ platí:

1. Vektor $\frac{\langle \vec{s} | \vec{x} \rangle}{\langle \vec{s} | \vec{s} \rangle} \cdot \vec{s}$ leží na přímce span($\vec{s}$).
2. Vektor $\vec{x} - \frac{\langle \vec{s} | \vec{x} \rangle}{\langle \vec{s} | \vec{s} \rangle} \cdot \vec{s}$ je kolmý na přímku span($\vec{s}$).

$$\langle \vec{s} \mid \vec{x} - \frac{\langle \vec{s} \mid \vec{x} \rangle}{\langle \vec{s} \mid \vec{s} \rangle} \cdot \vec{s} \rangle = \langle \vec{s} \mid \vec{x} \rangle - \frac{\langle \vec{s} \mid \vec{x} \rangle}{\langle \vec{s} \mid \vec{s} \rangle} \cdot \langle \vec{s} \mid \vec{s} \rangle = 0$$

Dostáváme tedy ortogonální rozklad[a] vektoru $\vec{x}$:

$$\underbrace{\vec{x} - \frac{\langle \vec{s} \mid \vec{x} \rangle}{\langle \vec{s} \mid \vec{s} \rangle} \cdot \vec{s}}_{\text{ortogonální rejekce přímkou span}(\vec{s})}$$

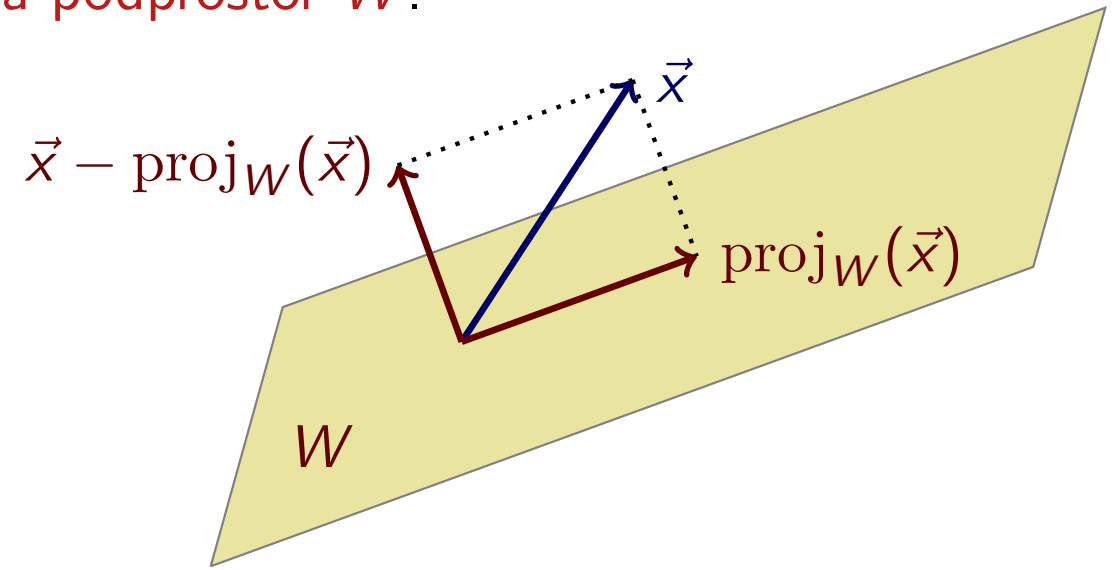


$$\underbrace{\frac{\langle \vec{s} \mid \vec{x} \rangle}{\langle \vec{s} \mid \vec{s} \rangle} \cdot \vec{s}}_{\text{ortogonální projekce na přímku span}(\vec{s})}$$

[a] Slovník: projekce=promítnutí, rejekce=odmítnutí.

Zobecnění: projekce na podprostor a rejekce podprostorem

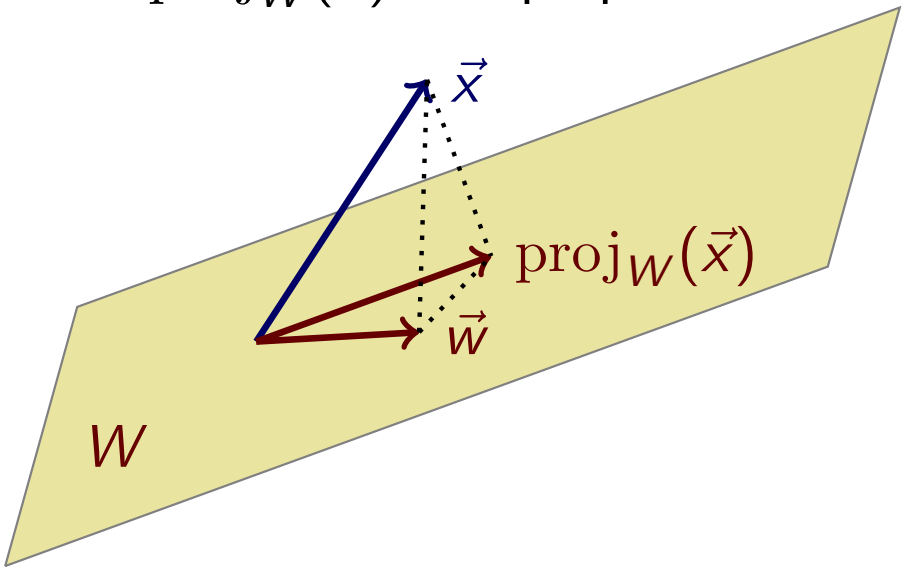
Ať W je podprostor lineárního prostoru L se skalárním součinem, ať $\vec{x}$ je libovolný vektor v L.
Vektoru $\mathrm{proj}_W(\vec{x})$, který leží ve W a pro který je $\vec{x} - \mathrm{proj}_W(\vec{x})$ kolmý na všechny vektory z W, říkáme ortogonální projekce vektoru $\vec{x}$ na podprostor W.



Vektoru $\vec{x} - \mathrm{proj}_W(\vec{x})$ budeme říkat ortogonální rejekce vektoru $\vec{x}$ podprostorem W a budeme jej značit $\mathrm{rej}_W(\vec{x})$.

Ortogonální rejekce je „nejkratší“ ze všech rejekcí

Pro jakýkoli vektor $\vec{x}$, který neleží ve W, a pro jakýkoli vektor $\vec{w}$, který ve W leží, vzniká pravoúhlý trojúhelník s odvěsnami $\mathrm{proj}_W(\vec{x}) - \vec{w}$ a $\vec{x} - \mathrm{proj}_W(\vec{x})$, a s přeponou $\vec{x} - \vec{w}$.



Díky Pythagorově větě tedy pro všechny vektory $\vec{w}$ z W platí[a]

$$\|\vec{x}-\mathrm{proj}_W(\vec{x})\|^2 \leq \|\vec{x}-\mathrm{proj}_W(\vec{x})\|^2 + \underbrace{\|\mathrm{proj}_W(\vec{x}) - \vec{w}\|^2}_{\geq 0} = \|\vec{x}-\vec{w}\|^2$$

[a] Na této nerovnosti je založena metoda nejmenších čtverců, viz cvičení a příští přednáška, nebo Dodatek C skript.

Věta (ortogonální projekce na podprostor s ortogonální bází)

Ať $M = \{\vec{u}_1, \ldots, \vec{u}_k\}$ je konečná neprázdná ortogonální množina vektorů. Označme $W = \mathrm{span}(M)$. Pro libovolný vektor $\vec{x}$ platí

$$\mathrm{proj}_W(\vec{x}) = \sum_{i=1}^{k} \frac{\langle \vec{u}_i \mid \vec{x} \rangle}{\langle \vec{u}_i \mid \vec{u}_i \rangle} \cdot \vec{u}_i \left(\text{tj. } \mathrm{proj}_W(\vec{x}) = \sum_{i=1}^{k} \mathrm{proj}_{\mathrm{span}(\vec{u}_i)}(\vec{x}) \right)$$

ortogonální projekce vektoru $\vec{x}$ na podprostor W.

Důkaz.

Evidentně: $\mathrm{proj}_W(\vec{x})$ leží ve W.
Pro každé $i_0 = 1, \ldots, k$ platí $\langle \vec{u}_{i_0} \mid \vec{x} - \mathrm{proj}_W(\vec{x}) \rangle = 0$, protože:

$$\langle \vec{u}_{i_0} \mid \vec{x} - \mathrm{proj}_W(\vec{x}) \rangle = \langle \vec{u}_{i_0} \mid \vec{x} \rangle - \langle \vec{u}_{i_0} \mid \mathrm{proj}_W(\vec{x}) \rangle =$$

$$\langle \vec{u}_{i_0} \mid \vec{x} \rangle - \langle \vec{u}_{i_0} \mid \sum_{i=1}^{k} \frac{\langle \vec{u}_i \mid \vec{x} \rangle}{\langle \vec{u}_i \mid \vec{u}_i \rangle} \cdot \vec{u}_i \rangle =$$

$$\langle \vec{u}_{i_0} \mid \vec{x} \rangle - \sum_{i=0}^{k} \frac{\langle \vec{u}_i \mid \vec{x} \rangle}{\langle \vec{u}_i \mid \vec{u}_i \rangle} \cdot \langle \vec{u}_{i_0} \mid \vec{u}_i \rangle = \langle \vec{u}_{i_0} \mid \vec{x} \rangle - \langle \vec{u}_{i_0} \mid \vec{x} \rangle = 0. \quad \blacksquare$$

Ortogonalisační proces (Gram-Schmidt)

Každou bázi $B = (\vec{b}_1, \dots, \vec{b}_n)$ prostoru se skalárním součinem lze převést na bázi $C = (\vec{c}_1, \dots, \vec{c}_n)$ s následujícími vlastnostmi:

1. C je ortogonální, tj $\langle \vec{c}_i \mid \vec{c}_j \rangle = 0$ pro $i \neq j$.
2. Pro každé $k \in \{1, \dots, n\}$ platí $\operatorname{span}\{\vec{b}_1, \dots, \vec{b}_k\} = \operatorname{span}\{\vec{c}_1, \dots, \vec{c}_k\}$.

Důkaz.

Definujeme[a]

$$\vec{c}_1 := \vec{b}_1, \quad \vec{c}_{k+1} := \underbrace{\vec{b}_{k+1} - \mathrm{proj}_{\operatorname{span}\{\vec{c}_1,\dots,\vec{c}_k\}}(\vec{b}_{k+1})}_{\text{rejekce vektoru } \vec{b}_{k+1} \text{ podprostorem } \operatorname{span}\{\vec{c}_1,\dots,\vec{c}_k\}}$$

Díky definici je splněno $\operatorname{span}\{\vec{b}_1, \dots, \vec{b}_k\} = \operatorname{span}\{\vec{c}_1, \dots, \vec{c}_k\}$, pro každé $k \in \{1, \dots, n\}$.
První podmínka je splněna z definice ortogonální rejekce. ■

[a] Slogan: Gram-Schmidt je posloupnost postupných ortogonálních rejekcí.

Poznámka (ortonormalisační proces)

Pokud je $C = (\vec{c}_1, \ldots, \vec{c}_n)$ ortogonální báze[a] prostoru L, je seznam $(\frac{\vec{c}_1}{\|\vec{c}_1\|}, \ldots, \frac{\vec{c}_n}{\|\vec{c}_n\|})$ ortonormální báze prostoru L (tj je ortogonální a norma každého prvku je 1):

$$\langle \frac{\vec{c}_i}{\|\vec{c}_i\|} \mid \frac{\vec{c}_j}{\|\vec{c}_j\|} \rangle = \frac{1}{\|\vec{c}_i\| \cdot \|\vec{c}_j\|} \cdot \langle \vec{c}_i \mid \vec{c}_j \rangle = \delta_{ij}$$

Každou konečnou bázi B v prostoru se skalárním součinem tedy lze ortonormalisovat:

1. Nejprve provedeme Gram-Schmidtův ortogonalisační proces na bázi B. Dostaneme ortogonální bázi C.
2. Ortogonální bázi C znormalisujeme výše uvedeným postupem.

[a] Evidentně pro každé i platí $\|\vec{c}_i\| \neq 0$, protože C je báze.

Příklad (ortogonalisace vektorů — Gram-Schmidt)

Vektory $\mathbf{b}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$, $\mathbf{b}_2 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$ a $\mathbf{b}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$ jsou lineárně nezávislé v $\mathbb{R}^4$. Příslušnou bázi $(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3)$ podprostoru W dimense 3 označíme B.

Báze B není ortogonální vzhledem ke standardnímu skalárnímu součinu v $\mathbb{R}^4$. Bázi B nyní ortogonalisujeme. Výsledné vektory v nové (ortogonální) bázi označíme $\mathbf{c}_1$, $\mathbf{c}_2$, $\mathbf{c}_3$. Budeme postupovat Gram-Schmidtovou metodou.

1. První vektor: $\mathbf{c}_1 = \mathbf{b}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$.

Příklad (pokrač.)

2. Druhý vektor: spočteme

$$\mathbf{b}_2 - \mathrm{proj}_{\mathsf{span}\{\mathbf{c}_1\}}(\mathbf{b}_2) = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} - \tfrac{3}{4} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} -\frac{3}{4} \\ \frac{1}{4} \\ \frac{1}{4} \\ \frac{1}{4} \end{pmatrix}.$$

Užitečný trik: protože skalární násobek nemění ortogonalitu,

položíme $\mathbf{c}_2 = 4 \cdot \begin{pmatrix} -\frac{3}{4} \\ \frac{1}{4} \\ \frac{1}{4} \\ \frac{1}{4} \end{pmatrix} = \begin{pmatrix} -3 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$

Tím se zbavíme pozdějších nepříjemných výpočtů se zlomky.

Příklad (pokrač.)

3. Třetí vektor: spočteme

$$\mathbf{b}_3 - \mathrm{proj}_{\mathsf{span}\{\mathbf{c}_1,\mathbf{c}_2\}}(\mathbf{b}_3) = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} - \tfrac{2}{4} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} - \tfrac{2}{12} \cdot \begin{pmatrix} -3 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -\frac{2}{3} \\ \frac{1}{3} \\ \frac{1}{3} \end{pmatrix}$$

Opět se zbavíme zlomků: $\mathbf{c}_3 = 3 \cdot \begin{pmatrix} 0 \\ -\frac{2}{3} \\ \frac{1}{3} \\ \frac{1}{3} \end{pmatrix} = \begin{pmatrix} 0 \\ -2 \\ 1 \\ 1 \end{pmatrix}$.

Výpočet je u konce: seznam $(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$ je hledaná ortogonální báze.

Příklad (normalisace ortogonální báze)

Normalisace ortogonální báze $\mathbf{c}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$, $\mathbf{c}_2 = \begin{pmatrix} -3 \\ 1 \\ 1 \\ 1 \end{pmatrix}$,

$\mathbf{c}_3 = \begin{pmatrix} 0 \\ -2 \\ 1 \\ 1 \end{pmatrix}$ podprostoru W v prostoru $\mathbb{R}^4$ se standardním skalárním součinem je tvořena vektory

$$\frac{\mathbf{c}_1}{\|\mathbf{c}_1\|} = \frac{1}{2} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad \frac{\mathbf{c}_2}{\|\mathbf{c}_2\|} = \frac{1}{\sqrt{12}} \cdot \begin{pmatrix} -3 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad \frac{\mathbf{c}_3}{\|\mathbf{c}_3\|} = \frac{1}{\sqrt{6}} \cdot \begin{pmatrix} 0 \\ -2 \\ 1 \\ 1 \end{pmatrix}$$

Projekce na podprostor, u kterého neznáme ortogonální bázi

1. V obecném případě je vždy možno nejprve obecnou bázi ortogonalisovat (Gram-Schmidt) a poté použít vzorec pro projekci na podprostor s ortogonální bází.
2. V případě $\mathbb{R}^n$ lze využít znalosti metrického tensoru, viz další přednášku.

Ortogonální projekce a metoda nejmenších čtverců

Odpřednesenou látku naleznete v kapitole 12.4 a Dodatku C skript *Abstraktní a konkrétní lineární algebra*.

Minulá přednáška

1. Ortogonalisační proces (Gram-Schmidt).
2. Ortogonální projekce a ortogonální rejekce.
3. Ortogonální projekce na podprostor s ortogonální bází.

Dnešní přednáška

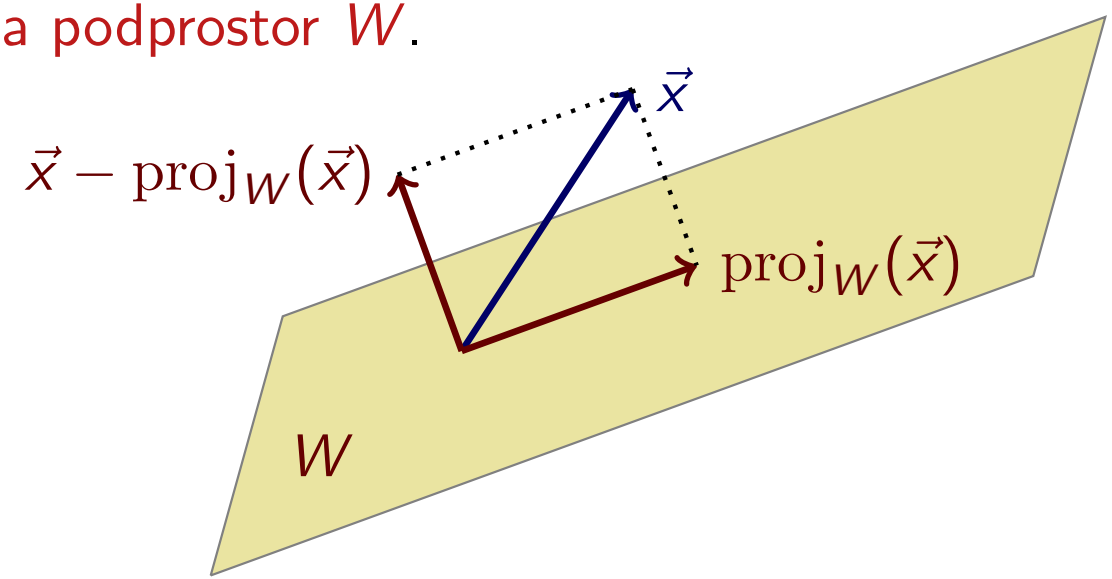
V této přednášce se zaměříme pouze na lineární prostory $\mathbb{R}^n$ nad $\mathbb{R}$.

1. Výpočet matice ortogonální projekce na podprostor (s libovolnou bází) v $\mathbb{R}^n$.
2. Charakterisace matic ortogonálních projekcí v $\mathbb{R}^n$.
3. Aplikace projekcí na řešení soustav lineárních rovnic (metoda nejmenších čtverců).[a]

[a] Budeme se věnovat pouze nejjednodušší formě metody nejmenších čtverců v $\mathbb{R}^n$ se standardním skalárním součinem. Vše je podrobně popsáno v tomto výtahu z přednášky.

Připomenutí: projekce na podprostor a rejekce podprostorem

Ať W je podprostor lineárního prostoru L se skalárním součinem, ať $\vec{x}$ je libovolný vektor v L.
Vektoru $\mathrm{proj}_W(\vec{x})$, který leží ve W a pro který je $\vec{x} - \mathrm{proj}_W(\vec{x})$ kolmý na všechny vektory z W, říkáme ortogonální projekce vektoru $\vec{x}$ na podprostor W.

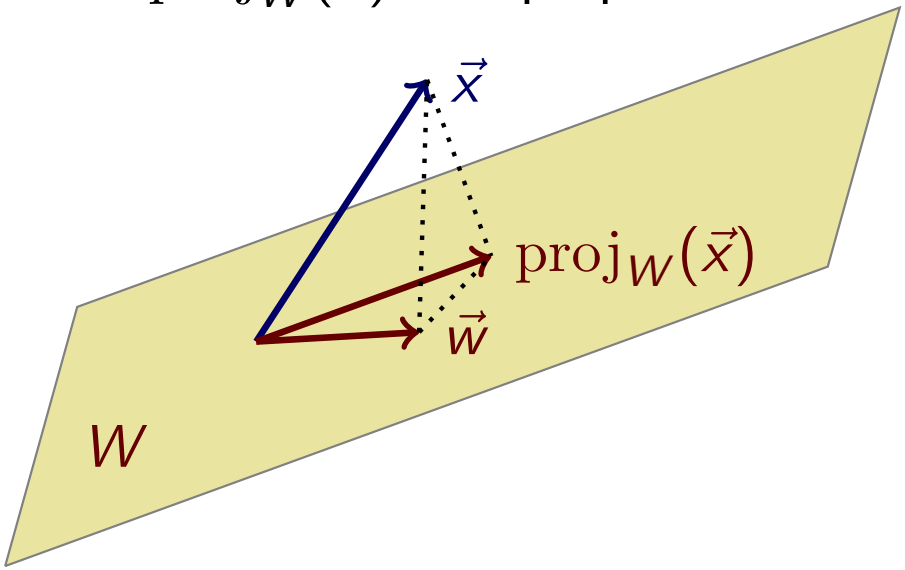


Vektoru $\vec{x} - \mathrm{proj}_W(\vec{x})$ říkáme ortogonální rejekce vektoru $\vec{x}$ podprostorem W a značíme jej $\mathrm{rej}_W(\vec{x})$.[a]

[a] Slovník: projekce=promítnutí, rejekce=odmítnutí.

Ortogonální rejekce je „nejkratší“ ze všech rejekcí

Pro jakýkoli vektor $\vec{x}$, který neleží ve W, a pro jakýkoli vektor $\vec{w}$, který ve W leží, vzniká pravoúhlý trojúhelník s odvěsnami $\mathrm{proj}_W(\vec{x}) - \vec{w}$ a $\vec{x} - \mathrm{proj}_W(\vec{x})$, a s přeponou $\vec{x} - \vec{w}$.



Díky Pythagorově větě tedy pro všechny vektory $\vec{w}$ z W platí[a]

$$\|\vec{x}-\mathrm{proj}_W(\vec{x})\|^2 \leq \|\vec{x}-\mathrm{proj}_W(\vec{x})\|^2 + \underbrace{\|\mathrm{proj}_W(\vec{x}) - \vec{w}\|^2}_{\geq 0} = \|\vec{x}-\vec{w}\|^2$$

[a] Na této nerovnosti je založena metoda nejmenších čtverců, viz cvičení a druhá část této přednášky.

Projekce na podprostor, u kterého neznáme ortogonální bázi

1. V obecném případě je vždy možno nejprve obecnou bázi ortogonalisovat (Gram-Schmidt) a poté použít vzorec pro projekci na podprostor s ortogonální bází.
2. V případě $\mathbb{R}^n$ lze využít znalosti metrického tensoru, viz níže.

Tvrzení

Ať W je podprostor prostoru $\mathbb{R}^n$ se skalárním součinem zadaným metrickým tensorem $\mathbf{G}$. Ať vektory $\mathbf{a}_1, \ldots, \mathbf{a}_k$ tvoří jakoukoli bázi podprostoru W. Označme jako $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_k)$ příslušnou matici. Potom[a]

$$\mathrm{proj}_W(\mathbf{x}) = \mathbf{A} \cdot (\mathbf{A}^T \cdot \mathbf{G} \cdot \mathbf{A})^{-1} \cdot \mathbf{A}^T \cdot \mathbf{G} \cdot \mathbf{x}$$

[a] Tento divoký vzorec má krotkou podobu pro standardní skalární součin: platí $\mathrm{proj}_W(\mathbf{x}) = \mathbf{A} \cdot (\mathbf{A}^T \cdot \mathbf{A})^{-1} \cdot \mathbf{A}^T \cdot \mathbf{x}$, protože $\mathbf{G} = \mathbf{E}_n$.

Důkaz.

Přednáška. ∎

Příklad (výpočet matice ortogonální projekce)

V prostoru $\mathbb{R}^3$ se standardním[a] skalárním součinem nalezněte matici projekce na rovinu $W = \operatorname{span}\left(\begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}\right)$. Víme: pro $\mathbf{A} = \begin{pmatrix}1 & 1\\1 & 1\\1 & 0\end{pmatrix}$, je $\mathbf{P}_W = \mathbf{A}\cdot(\mathbf{A}^T\cdot\mathbf{A})^{-1}\cdot\mathbf{A}^T$ matice ortogonální projekce na W.

$$\mathbf{P}_W = \begin{pmatrix}1 & 1\\1 & 1\\1 & 0\end{pmatrix}\cdot\begin{pmatrix}3 & 2\\2 & 2\end{pmatrix}^{-1}\cdot\begin{pmatrix}1 & 1 & 1\\1 & 1 & 0\end{pmatrix} = \frac{1}{2}\cdot\begin{pmatrix}1 & 1 & 0\\1 & 1 & 0\\0 & 0 & 2\end{pmatrix}.$$

Například projekci vektoru $\begin{pmatrix}-20\\4\\6\end{pmatrix}$ na W spočítáme součinem

$$\frac{1}{2}\cdot\begin{pmatrix}1 & 1 & 0\\1 & 1 & 0\\0 & 0 & 2\end{pmatrix}\cdot\begin{pmatrix}-20\\4\\6\end{pmatrix} = \begin{pmatrix}-8\\-8\\6\end{pmatrix} = 6\cdot\begin{pmatrix}1\\1\\1\end{pmatrix} + (-14)\cdot\begin{pmatrix}1\\1\\0\end{pmatrix}.$$

[a] Metrický tensor tedy je $\mathbf{G} = \mathbf{E}_3$.

Příklad (výpočet matice ortogonální projekce)

V prostoru $\mathbb{R}^2$ se skalárním součinem s metrickým tensorem[a] $\mathbf{G} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ spočtěte matici projekce na přímku $W = \operatorname{span}(\begin{pmatrix} 1 \\ 1 \end{pmatrix})$.

Víme: pro $\mathbf{A} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, je $\mathbf{P}_W = \mathbf{A} \cdot (\mathbf{A}^T \cdot \mathbf{G} \cdot \mathbf{A})^{-1} \cdot \mathbf{A}^T \cdot \mathbf{G}$ matice ortogonální projekce.

Tudíž je

$$\mathbf{P}_W = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \cdot ((1 \quad 1) \cdot \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix})^{-1} (1 \quad 1) \cdot \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \frac{1}{5} \cdot \begin{pmatrix} 2 & 3 \\ 2 & 3 \end{pmatrix}.$$

Například projekci vektoru $\begin{pmatrix} 4 \\ 6 \end{pmatrix}$ na W spočítáme součinem

$$\frac{1}{5} \cdot \begin{pmatrix} 2 & 3 \\ 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 6 \end{pmatrix} = \frac{1}{5} \cdot \begin{pmatrix} 26 \\ 26 \end{pmatrix} = \frac{26}{5} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

[a] Jde o nestandardní skalární součin: to znamená, že jde o ortogonální projekci vzhledem ke skalárnímu součinu $\langle \mathbf{x} \mid \mathbf{y} \rangle = \mathbf{x}^T \cdot \mathbf{G} \cdot \mathbf{y}$.

Věta (charakterisace matic ortogonálních projekcí)

Ať $\mathbb{R}^n$ je vybaven skalárním součinem $\langle - \mid - \rangle$ s metrickým tensorem $\mathbf{G}$. Pro matici $\mathbf{P} : \mathbb{R}^n \to \mathbb{R}^n$ je ekvivalentní:

1. $\mathbf{P}$ je matice ortogonální projekce na podprostor $\mathrm{im}(P)$ dimense k.
2. $\mathrm{rank}(\mathbf{P}) = k$ a platí $\mathbf{P}^2 = \mathbf{P}$ a $\langle \mathbf{P} \cdot \mathbf{x} \mid \mathbf{y} \rangle = \langle \mathbf{x} \mid \mathbf{P} \cdot \mathbf{y} \rangle$.

Důkaz.

Přednáška. ■

Poznámka

Pro standardní skalární součin v $\mathbb{R}^n$ (tj. pro $\mathbf{G} = \mathbf{E}_n$) lze druhou podmínku přeformulovat takto:

2. $\mathrm{rank}(\mathbf{P}) = k$ a platí $\mathbf{P}^2 = \mathbf{P}$ a $\mathbf{P}^T = \mathbf{P}$.

Úvaha o bodech na přímce

Ať $\{x_1, x_2, \ldots, x_n\}$ je alespoň dvouprvková množina reálných čísel. Body

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \ldots, \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

v $\mathbb{R}^2$ leží na přímce tvaru $y = ax + b$ právě tehdy, když soustava rovnic

$$\left(\begin{array}{cc|c} x_1 & 1 & y_1 \\ x_2 & 1 & y_2 \\ \vdots & \vdots & \vdots \\ x_n & 1 & y_n \end{array}\right)$$

nad $\mathbb{R}$ má řešení $\begin{pmatrix} a \\ b \end{pmatrix}$.

Důležité pozorování: protože $\{x_1, x_2, \ldots, x_n\}$ je alespoň dvouprvková množina reálných čísel, má matice výše uvedené soustavy hodnost 2.

Úvaha o bodech na přímce (pokrač.)

Ať $\{x_1, x_2, \ldots, x_n\}$ je alespoň dvouprvková množina reálných čísel.
Co dělat, když body

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \ldots, \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

v $\mathbb{R}^2$ na přímce tvaru $y = ax + b$ neleží?
Lze nalézt přímku tvaru $y = ax + b$, která je (pro zadané body) nejlepší možnou volbou?[a]
Důležité pozorování: soustava rovnic

$$\left(\begin{array}{cc|c} x_1 & 1 & y_1 \\ x_2 & 1 & y_2 \\ \vdots & \vdots & \vdots \\ x_n & 1 & y_n \end{array}\right)$$

řešení mít nemůže, hodnost matice soustavy je ale stále 2.

[a] Zatím nevíme, co myslíme slovem nejlepší. Pravděpodobně chceme minimalisovat chybu, které se dopustíme.

Příklad

Tři body $\begin{pmatrix}3\\6\end{pmatrix}, \begin{pmatrix}4\\9\end{pmatrix}, \begin{pmatrix}5\\10\end{pmatrix}$ v $\mathbb{R}^2$ na přímce neleží.[a]

Označme soustavu $\left(\begin{array}{cc|c} 3 & 1 & 6 \\ 4 & 1 & 9 \\ 5 & 1 & 10 \end{array}\right)$ jako $(\mathbf{A} \mid \mathbf{b})$.

Víme:

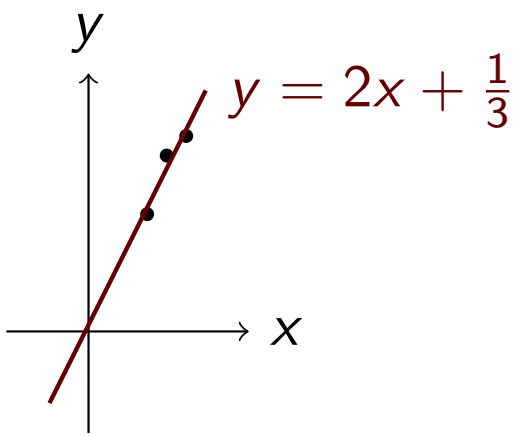
1. $(\mathbf{A} \mid \mathbf{b})$ nemá řešení, tj. vektor $\mathbf{b}$ neleží v prostoru $W = \mathrm{im}(\mathbf{A})$.
2. Sloupce matice $\mathbf{A}$ tvoří bázi prostoru W.
3. Soustava $(\mathbf{A}^T \cdot \mathbf{A} \mid \mathbf{A}^T \cdot \mathbf{b})$ má právě jedno řešení, protože $\mathbf{A}^T \cdot \mathbf{A}$ je positivně definitní (tudíž regulární).
   Označme toto řešení $\widehat{\mathbf{x}}$. Platí tedy $\widehat{\mathbf{x}} = (\mathbf{A}^T \cdot \mathbf{A})^{-1} \cdot \mathbf{A}^T \cdot \mathbf{b}$.
4. Matice $\mathbf{P}_W$ ortogonální projekce na W je tvaru $\mathbf{P}_W = \mathbf{A} \cdot (\mathbf{A}^T \cdot \mathbf{A})^{-1} \cdot \mathbf{A}^T$. Tudíž $\mathbf{A} \cdot \widehat{\mathbf{x}} = \mathbf{P}_W \cdot \mathbf{b}$.
5. Takže: $\|\mathrm{rej}_W(\mathbf{b})\|^2 = \|\mathbf{b} - \mathbf{A} \cdot \widehat{\mathbf{x}}\|^2 \leq \|\mathbf{b} - \mathbf{A} \cdot \mathbf{x}\|^2$ pro vš $\mathbf{x}$.
   To je ono: minimalisovali jsme čtverec chyby $\|\mathbf{b} - \mathbf{A} \cdot \mathbf{x}\|$.

[a] Body na první pohled „téměř“ leží na přímce $y = 2x$.

Příklad (pokrač.)

Vyřešíme tedy soustavu $(\mathbf{A} \mid \mathbf{b}) = \left(\begin{array}{cc|c} 3 & 1 & 6 \\ 4 & 1 & 9 \\ 5 & 1 & 10 \end{array}\right)$ metodou nejmenších čtverců.[a]

1. Soustava $(\mathbf{A}^T \cdot \mathbf{A} \mid \mathbf{A}^T \cdot \mathbf{b})$ má tvar $\left(\begin{array}{cc|c} 50 & 12 & 104 \\ 12 & 3 & 25 \end{array}\right)$ a má jediné řešení $\begin{pmatrix} 2 \\ 1/3 \end{pmatrix}$.
2. Hledaná přímka má tvar $y = 2x + \frac{1}{3}$.



[a] Řešením získáme „nejlepší možnou“ přímku, kterou lze proložit zadanými body. Říká se jí regresní přímka.

Příklad (pokrač.)

Vektor $\begin{pmatrix} 2 \\ 1/3 \end{pmatrix}$ není řešením soustavy $\left(\begin{array}{cc|c} 3 & 1 & 6 \\ 4 & 1 & 9 \\ 5 & 1 & 10 \end{array}\right)$.

Platí $\begin{pmatrix} 3 & 1 \\ 4 & 1 \\ 5 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1/3 \end{pmatrix} = \begin{pmatrix} 19/3 \\ 25/3 \\ 31/3 \end{pmatrix}$.

Čtverec chyby, které jsme se dopustili, je

$$\| \begin{pmatrix} 6 \\ 9 \\ 10 \end{pmatrix} - \begin{pmatrix} 19/3 \\ 25/3 \\ 31/3 \end{pmatrix} \|^2 = \| \begin{pmatrix} -1/3 \\ 2/3 \\ -1/3 \end{pmatrix} \|^2 = 6/9$$

a jde o nejmenší čtverec chyby.

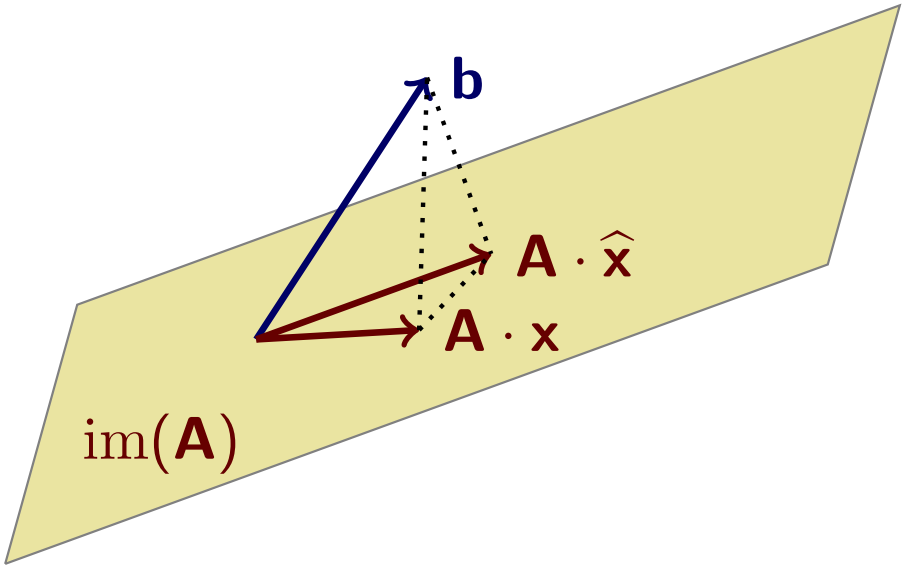
Řešení soustavy rovnic metodou nejmenších čtverců

Ať $(\mathbf{A} \mid \mathbf{b})$ je soustava nad $\mathbb{R}$, kde matice $\mathbf{A}$ má lineárně nezávislé sloupce. Řešení soustavy $(\mathbf{A} \mid \mathbf{b})$ metodou nejmenších čtverců probíhá následovně:

1. Protože $\mathbf{A}$ má lineárně nezávislé sloupce, je matice $\mathbf{A}^T \cdot \mathbf{A}$ positivně definitní, tedy regulární.
2. Soustava $(\mathbf{A}^T \cdot \mathbf{A} \mid \mathbf{A}^T \cdot \mathbf{b})$ má tedy jediné řešení, označme toto řešení $\widehat{\mathbf{x}} = (\mathbf{A}^T \cdot \mathbf{A})^{-1} \cdot \mathbf{A}^T \cdot \mathbf{b}$.
   Tomuto jedinému řešení $\widehat{\mathbf{x}}$ se říká řešení soustavy $(\mathbf{A} \mid \mathbf{b})$ metodou nejmenších čtverců.

   Má to následující důvod:
   1. Platí rovnost $\mathbf{A} \cdot \widehat{\mathbf{x}} = \mathbf{A} \cdot (\mathbf{A}^T \cdot \mathbf{A})^{-1} \cdot \mathbf{A}^T \cdot \mathbf{b}$. To znamená, že $\mathbf{A} \cdot \widehat{\mathbf{x}}$ je ortogonální projekce vektoru $\mathbf{b}$ na $\mathrm{im}(\mathbf{A})$.
   2. Protože ortogonální rejekce $\mathbf{b} - \mathbf{A} \cdot \widehat{\mathbf{x}}$ vektoru $\mathbf{b}$ podprostorem $\mathrm{im}(\mathbf{A})$ je „nejkratší“ rejekcí vektoru $\mathbf{b}$ podprostorem $\mathrm{im}(\mathbf{A})$, platí $\|\mathbf{b} - \mathbf{A} \cdot \widehat{\mathbf{x}}\|^2 \leq \|\mathbf{b} - \mathbf{A} \cdot \mathbf{x}\|^2$, pro každé $\mathbf{x}$.

Ilustrace řešení soustavy $(\mathbf{A} \mid \mathbf{b})$ metodou nejmenších čtverců



Pokud má matice soustavy $(\mathbf{A} \mid \mathbf{b})$ lineárně nezávislé sloupce, potom platí:

1. Soustava $(\mathbf{A} \mid \mathbf{b})$ má právě jedno řešení $\widehat{\mathbf{x}}$ metodou nejmenších čtverců.
2. Pro každé $\mathbf{x}$ platí nerovnost $\|\mathbf{b} - \mathbf{A} \cdot \widehat{\mathbf{x}}\|^2 \leq \|\mathbf{b} - \mathbf{A} \cdot \mathbf{x}\|^2$.

Příklad (řešení soustavy rovnic metodou nejmenších čtverců)

Soustava $(\mathbf{A} \mid \mathbf{b}) = \left(\begin{array}{cc|c} 1 & 1 & 2 \\ 1 & 1 & 3 \\ 1 & 0 & 2 \end{array}\right)$ nemá řešení (Frobeniova věta).

V našem případě: $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}$, $\mathbf{b} = \begin{pmatrix} 2 \\ 3 \\ 2 \end{pmatrix}$, $\mathbf{A}^T \cdot \mathbf{A} = \begin{pmatrix} 3 & 2 \\ 2 & 2 \end{pmatrix}$, $\mathbf{A}^T \cdot \mathbf{b} = \begin{pmatrix} 7 \\ 5 \end{pmatrix}$.

Soustava $\left(\begin{array}{cc|c} 3 & 2 & 7 \\ 2 & 2 & 5 \end{array}\right)$ má jediné řešení $\widehat{\mathbf{x}} = \begin{pmatrix} 2 \\ 0.5 \end{pmatrix}$.

Protože $\mathbf{A} \cdot \widehat{\mathbf{x}} = \begin{pmatrix} 2.5 \\ 2.5 \\ 2 \end{pmatrix}$, vektor $\widehat{\mathbf{x}}$ není řešením soustavy $(\mathbf{A} \mid \mathbf{b})$.

Ovšem jakýkoli jiný vektor $\mathbf{x}$ by „dopadl ještě hůře“. Pro všechny vektory $\mathbf{x}$ z $\mathbb{R}^2$ totiž platí nerovnost

$$0.5 = \|\mathbf{b} - \mathbf{A} \cdot \widehat{\mathbf{x}}\|^2 \leq \|\mathbf{b} - \mathbf{A} \cdot \mathbf{x}\|^2$$

Příklad (proložení paraboly)

Ať $\{x_1, x_2, \ldots, x_n\}$ je alespoň tříprvková množina reálných čísel. Body

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \ldots, \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

v $\mathbb{R}^2$ leží na parabole tvaru $y = ax^2 + bx + c$ právě tehdy, když soustava rovnic

$$\left(\begin{array}{ccc|c} x_1^2 & x_1 & 1 & y_1 \\ x_2^2 & x_2 & 1 & y_2 \\ \vdots & \vdots & \vdots & \vdots \\ x_n^2 & x_n & 1 & y_n \end{array}\right)$$

má řešení $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$.

Příklad (proložení paraboly, pokrač.)

Důležité pozorování: protože $\{x_1, x_2, \ldots, x_n\}$ je alespoň tříprvková množina reálných čísel, má matice soustavy

$$\left(\begin{array}{ccc|c} x_1^2 & x_1 & 1 & y_1 \\ x_2^2 & x_2 & 1 & y_2 \\ \vdots & \vdots & \vdots & \vdots \\ x_n^2 & x_n & 1 & y_n \end{array}\right)$$

hodnost 3.

Opravdu: ať x_i, x_j, x_k jsou tři navzájem různé hodnoty z množiny $\{x_1, x_2, \ldots, x_n\}$.

Potom

$$\begin{vmatrix} x_i^2 & x_i & 1 \\ x_j^2 & x_j & 1 \\ x_k^2 & x_k & 1 \end{vmatrix} = (x_i - x_k) \cdot (x_i - x_k) \cdot (x_j - x_k) \neq 0$$

Příklad (proložení paraboly, pokrač.)

Ať $\{x_1, x_2, \ldots, x_n\}$ je alespoň tříprvková množina reálných čísel. Body

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \ldots, \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

v $\mathbb{R}^2$ lze proložit parabolu $y = ax^2 + bx + c$, kde $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ je řešením soustavy rovnic

$$\left(\begin{array}{ccc|c} x_1^2 & x_1 & 1 & y_1 \\ x_2^2 & x_2 & 1 & y_2 \\ \vdots & \vdots & \vdots & \vdots \\ x_n^2 & x_n & 1 & y_n \end{array}\right)$$

metodou nejmenších čtverců.

Závěrečná poznámka

Řešení soustav metodou nejmenších čtverců má řadu aplikací. Je základem regresních metod v matematické statistice, viz například knihu

- Douglas C. Montgomery a George C. Runger, *Applied statistics and probability for engineers*, 3.ed, John Wiley & Sons, New York, 2003.

Historická poznámka

Autorem metody nejmenších čtverců je německý matematik Karl Friedrich Gauss (1777–1855). V roce 1801 Gauss tuto metodu použil pro predikci dráhy planetky Ceres, která 40 dní po objevení zmizela evropským astronomům za Sluncem. Gauss předpověděl polohu, kde se planetka za 10 měsíců opět objeví.

Uvedení do lineárních kódů

Odpřednesenou látku naleznete v dodatku I skript *Abstraktní a konkrétní lineární algebra*.

Dnešní přednáška

1. Základní geometrické myšlenky teorie lineárních kódů.
2. Generující a kontrolní matice lineárního podprostoru.

Dobré zdroje dalších informací

1. Richard Wesley Hamming (1915–1998): Bellovy laboratoře, ∼1946, technika pro opravu chyb na děrných štítcích
2. J. Adámek, *Foundations of coding*, John Wiley & Sons, New York, 1991
3. D. J. C. MacKay, *Information theory, inference and learning algorithms*, Cambridge Univ. Press, 2003
4. W. C. Huffman a V. Pless, *Fundamentals of error-correcting codes*, Cambridge Univ. Press, 2003

Příští přednáška

1. Základy ortogonální geometrie v prostorech tvaru $\mathbb{F}^n$ nad $\mathbb{F}$, kde $\mathbb{F}$ je obecné těleso.

Kódování versus šifrování

1. Kódování: dvě strany (Alice a Bob) si vyměňují zprávy. Při přenosu zpráv může dojít k poškození vyslané zprávy.

   Předpokládejme, že Alice píše Bobovi. Chceme umožnit Bobovi opravit poškozenou zprávu bez nutnosti zpětného dotazu Alice.

   Můžeme použít metody lineární algebry: lineární kódy.

2. Šifrování: dvě strany (Alice a Bob) si vyměňují zprávy. Při přenosu zpráv nemůže dojít k poškození vyslané zprávy, ale může dojít k odposlechu třetí stranou (ta se jmenuje Eve[a]).

   Předpokládejme, že Alice píše Bobovi. Chceme takovou komunikaci, kterou Eve nedokáže efektivně přečíst.

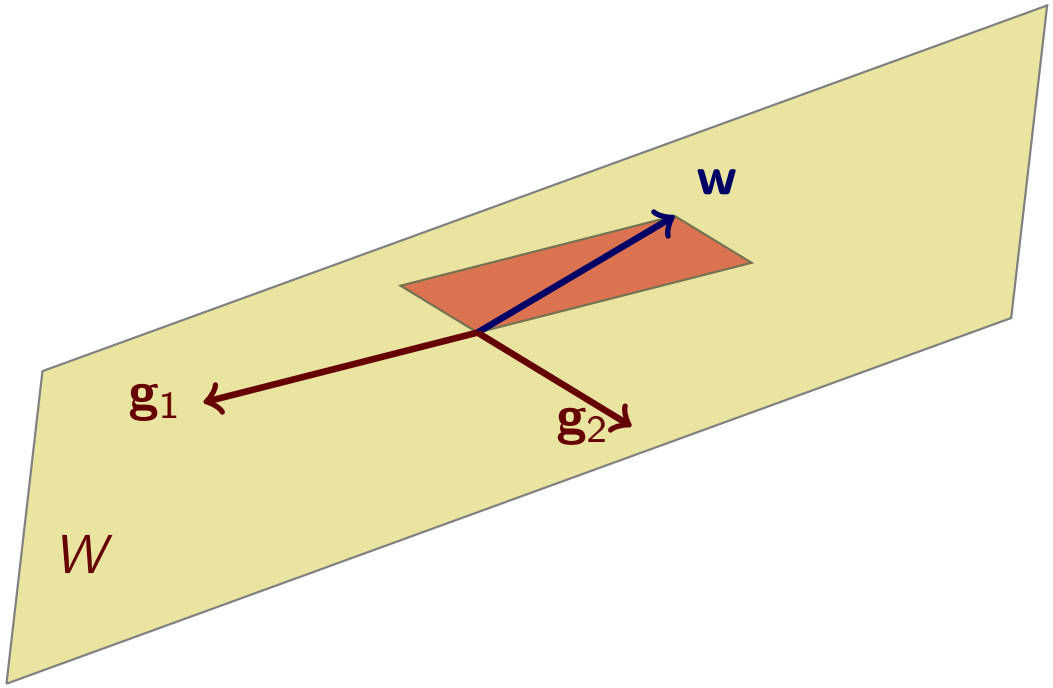
   K účinnému šifrování je třeba použít sofistikovaných metod. Viz např. J. Velebil, *Diskrétní matematika*, Praha, 2007.

[a] Z anglického *eavesdropper* — ten, kdo tajně naslouchá.

Rovina v $\mathbb{R}^3$ jako lineární kód

Rovina $x + y - z = 0$ je lineární podprostor W dimense 2 v $\mathbb{R}^3$.

1. Volbou uspořádané báze W lze generovat prvky W.
   1. W má usp. bázi (např.) $(\mathbf{g}_1, \mathbf{g}_2)$, kde $\mathbf{g}_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$, $\mathbf{g}_2 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$.
   2. Tudíž $\mathbf{w} \in W$ iff existují jednoznačně určená $a_1, a_2 \in \mathbb{R}$ tak, že $a_1 \cdot \mathbf{g}_1 + a_2 \cdot \mathbf{g}_2 = \mathbf{w}$. (Protože báze určuje systém souřadnic.)



Rovina v $\mathbb{R}^3$ jako lineární kód (pokrač.)

Rovina $x + y - z = 0$ je lineární podprostor W dimense 2 v $\mathbb{R}^3$.

3. Vektor $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ budeme považovat za vektor informačních bitů.

   Neboli: volbou a_1, a_2 lze vygenerovat $\mathbf{w} \in W$ takto:

$$\underbrace{\begin{pmatrix} 1 & 0 \\ 2 & 1 \\ 3 & 1 \end{pmatrix}}_{\text{generující matice } \mathbf{G}} \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} a_1 \\ 2a_1 + a_2 \\ 3a_1 + a_2 \end{pmatrix} = \mathbf{w}$$

   Vektor $\mathbf{w}$ Alice odešle Bobovi.

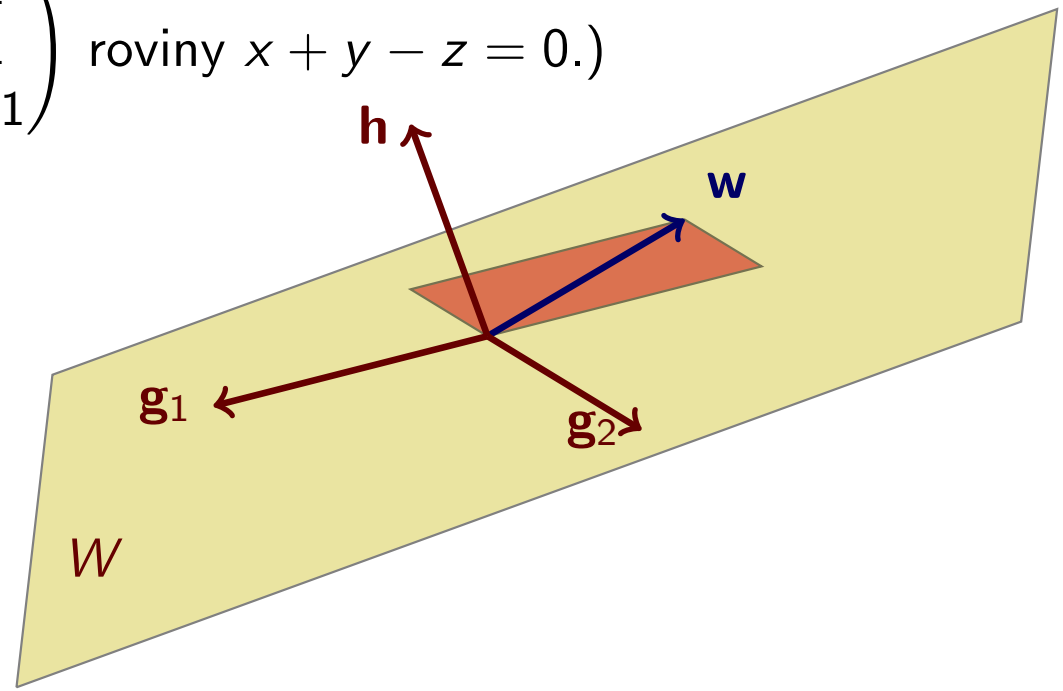
   Vektor $\mathbf{w}$ obsahuje redundantní informaci.[a] Tato redundantní informace chrání původní informační bity před poškozením.

[a] Podíl délky informace a celkové délky kódového slova (tzv information rate kódu) je tedy v našem případě $\frac{2}{3}$.

Rovina v $\mathbb{R}^3$ jako lineární kód (pokrač.)

Rovina $x + y - z = 0$ je lineární podprostor W dimense 2 v $\mathbb{R}^3$.

2. Volbou ortogonálního doplňku W lze testovat, zda vektory leží ve W.[a]
   1. W má ortogonální doplněk. Tudíž $\mathbf{w} \in W$ iff $\mathbf{h}^T \cdot \mathbf{w} = \mathbf{o}$. (Protože ortogonální doplněk je dán normálovým vektorem $\mathbf{h} = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}$ roviny $x + y - z = 0$.)



[a] Co je ortogonální doplněk vysvětlíme přesně v příští přednášce. Zatím se odvoláváme na intuici v $\mathbb{R}^3$.

Rovina v $\mathbb{R}^3$ jako lineární kód (pokrač.)

2. Neboli: syndrom s vektoru $\mathbf{v} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$, kde

$$s = \underbrace{\begin{pmatrix} 1 & 1 & -1 \end{pmatrix}}_{\text{kontrolní matice}} \cdot \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$$

určuje míru příslušnosti vektoru $\mathbf{v}$ do W.

Povšimněme si: syndrom s vektoru $\mathbf{v}$ je hodnota standardního skalárního součinu $\langle \mathbf{h} \mid \mathbf{v} \rangle = \mathbf{h}^T \cdot \mathbf{v}$ v $\mathbb{R}^3$.

Syndrom vektoru $\mathbf{v}$ je tedy nulový právě tehdy, když jsou vektory $\mathbf{v}$ a $\mathbf{h}$ ortogonální.[a]

[a] V příští přednášce zobecníme pojem ortogonality vzhledem ke standardnímu skalárnímu součinu z prostorů $\mathbb{R}^n$ na prostory tvaru $\mathbb{F}^n$, kde $\mathbb{F}$ je obecné těleso.

Rovina v $\mathbb{R}^3$ jako lineární kód (pokrač.)

Rovina $x + y - z = 0$ je lineární podprostor W dimense 2 v $\mathbb{R}^3$.

Generující a kontrolní matice: $\mathbf{G} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \\ 3 & 1 \end{pmatrix}$, $\mathbf{h}^T = \begin{pmatrix} 1 & 1 & -1 \end{pmatrix}$.

Alice z informace $\begin{pmatrix} 3 \\ 2 \end{pmatrix}$ vygeneruje kódové slovo $\mathbf{G} \cdot \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 3 \\ 8 \\ 11 \end{pmatrix}$ z prostoru W. Toto slovo odešle Bobovi.

Bob přijme slovo $\begin{pmatrix} 3 \\ 7 \\ 11 \end{pmatrix}$. Došlo k poškození? Bob spočte syndrom přijatého slova:

$$\mathbf{h}^T \cdot \begin{pmatrix} 3 \\ 7 \\ 11 \end{pmatrix} = -1$$

Syndrom je nenulový, k chybě došlo. Na jaké posici k chybě došlo? Jak ji opravit?

Nearest neighbour decoding

Pokud jsme nepřijali kódové slovo, chceme najít kódové slovo, které je (v nějakém smyslu) nejblíže[a] přijatému slovu. Přijaté slovo pak nahradíme tímto nejbližším kódovým slovem.

[a] Zatím jde jen o slogan; v příští přednášce zavedeme Hammingovu vzdálenost (kódových) slov.

Problémy při opravě v lineárních kódech nad $\mathbb{R}$

1. Základní problém při nearest neighbour decoding nad $\mathbb{R}$: reálných čísel je příliš mnoho.
2. Potřebujeme „konečné číselné obory“, které se chovají stejně jako $\mathbb{R}$. Neboli: potřebujeme obecná konečná tělesa.[a]

   Důvod: chceme použít lineární algebru.

[a] Potřebujeme dostatečnou zásobu konečných těles $\mathbb{F}$. Existence nekonečně mnoha konečných těles souvisí s existencí nekonečného počtu prvočísel — viz příští přednášku.

Příklad: kód 10-ISBN

Deset cifer: použity jsou symboly z množiny $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X\}$. Chápeme je jako zbytky po dělení číslem 11.

Příklad:

$$0-141-01878-X$$

kde jednotlivé skupiny znamenají:

1. 0 jazyk knihy (angličtina)
2. 141 nakladatelství (Penguin Mathematics)
3. 01878 číslo knihy, přidělené nakladatelstvím
4. X kontrolní bit

Obecně: kódové slovo kódu 10-ISBN je $x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}$, kde $\sum_{i=1}^{10} ix_i = 0$ jako zbytek po dělení číslem 11.

Kód 10-ISBN (pokrač.)

Kdy je řetězec $x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}$ kódem ISBN?
Právě tehdy, když jeho syndrom

$$\underbrace{(1,2,3,4,5,6,7,8,9,X)}_{\text{kontrolní matice } \mathbf{H}^T \text{ kódu 10-ISBN}} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \end{pmatrix}$$

je nula (počítáno jako zbytek po dělení číslem 11).[a]

[a] Povšimněme si: ISBN chápeme jako vektor v $(\mathbb{Z}_{11})^{10}$. Píšeme je tedy do sloupce.

Kód 10-ISBN (pokrač.)

Jak vytvořit kód ISBN?

Info o knize[a] = 9 bitů. Jak spočítat kontrolní bit?

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}}_{\text{generující matice } \mathbf{G} \text{ kódu 10-ISBN}} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \end{pmatrix}$$

počítáno jako zbytek po dělení číslem 11.

[a] Povšimněme si: informační bity chápeme jako vektor v $(\mathbb{Z}_{11})^9$. Píšeme je tedy do sloupce.

Kód 10-ISBN (pokrač.)

1. Kódy 10-ISBN = vektory v lineárním podprostoru W lineárního prostoru $(\mathbb{Z}_{11})^{10}$.
   Uspořádaná báze B prostoru W = sloupce matice $\mathbf{G}$.
   Dimense $W = 9$.
2. Info o knize = vektor souřadnic $\mathbf{a}$ vektoru $\mathbf{w}$ ve W vzhledem k uspořádané bázi B. Platí vztah $\mathbf{w} = \mathbf{G} \cdot \mathbf{a}$.
3. Test při příjmu slova $\mathbf{v}$ = výpočet syndromu $\mathbf{H}^T \cdot \mathbf{v}$ slova $\mathbf{v}$.
   Sloupce $\mathbf{H}$ = báze ortogonálního doplňku k W.

Kód 10-ISBN = lineární 11-kód délky 10 a dimense 9.

Kód 10-ISBN je schopen detekovat jednu chybu a prohození dvou pozic,[a] viz Příklad 3.3.2 textu *Diskrétní matematika*.

[a] To jsou běžné písařské chyby. 10-ISBN je starý kód, začíná být nahrazován kódem 13-ISBN.

Lineární podprostory prostoru $\mathbb{F}^n$ nad $\mathbb{F}$ (znovu a mírně jinak)

Ať W je lineární podprostor prostoru $\mathbb{F}^n$ nad $\mathbb{F}$. Víme, že platí $0 \leq \dim(W) \leq n$. Předpokládejme, že $\dim(W) = k > 0$.

1. Zvolme uspořádanou bázi $(\mathbf{g}_1, \ldots, \mathbf{g}_k)$ prostoru W. Označme jako $\mathbf{G} : \mathbb{F}^k \to \mathbb{F}^n$ matici se sloupcovým zápisem $(\mathbf{g}_1, \ldots, \mathbf{g}_k)$.

   Podle věty o dimensi jádra a obrazu platí $\mathrm{rank}(\mathbf{G}) = k$ a $\mathrm{def}(\mathbf{G}) = 0$. Navíc platí $\mathrm{im}(\mathbf{G}) = W$.

   Z toho okamžitě plyne:

   1. Pro jakoukoli volbu vektoru $\mathbf{a}$ z $\mathbb{F}^k$ je $\mathbf{G} \cdot \mathbf{a}$ vektor ve W.
   2. Vektor $\mathbf{w}$ z $\mathbb{F}^n$ leží ve W právě tehdy, když soustava rovnic $(\mathbf{G} \mid \mathbf{w})$ má právě jedno řešení (označme je $\mathbf{a}$).

      Toto jediné řešení $\mathbf{a}$ z $\mathbb{F}^k$ je vektor souřadnic vektoru $\mathbf{w}$ vzhledem k uspořádané bázi $(\mathbf{g}_1, \ldots, \mathbf{g}_k)$.

   Matici $\mathbf{G}$ říkáme generující matice[a] lineárního podprostoru W.

[a] Generující matice podprostoru W není jednoznačně určena: volbou jiné báze podprostoru W získáme jinou generující matici.

Lineární podprostory prostoru $\mathbb{F}^n$ nad $\mathbb{F}$ (pokrač.)

Ať W je lineární podprostor prostoru $\mathbb{F}^n$ nad $\mathbb{F}$ s uspořádanou bází $(\mathbf{g}_1, \ldots, \mathbf{g}_k)$, $k > 0$.

2. Protože $W = \mathrm{span}(\mathbf{g}_1, \ldots, \mathbf{g}_k)$, existuje soustava rovnic tvaru $(\mathbf{H}^T \mid \mathbf{o})$ tak, že řešení $(\mathbf{H}^T \mid \mathbf{o})$ je přesně W.[a]

   Podle Frobeniovy věty platí $\mathrm{rank}(\mathbf{H}^T) = n - k$ a $\mathrm{def}(\mathbf{H}^T) = k$.
   Víme, že rozměry $\mathbf{H}^T$ můžeme volit tak, aby platilo $\mathbf{H}^T : \mathbb{F}^n \to \mathbb{F}^{n-k}$.

Matici $\mathbf{H}^T$ říkáme kontrolní matice[b] lineárního podprostoru W.

Důvod: vektor $\mathbf{w}$ leží ve W právě tehdy, když $\mathbf{H}^T \cdot \mathbf{w} = \mathbf{o}$. Maticí $\mathbf{H}^T$ tedy kontrolujeme přítomnost vektoru v podprostoru W.

---

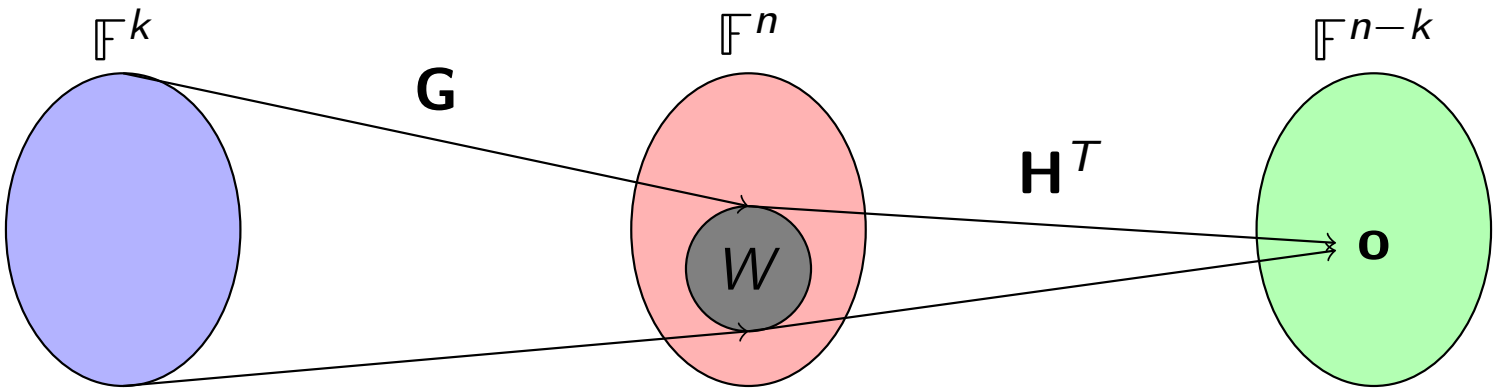
[a] Slogan: $\mathbf{H}$ je normála podprostoru W. To je důvod, proč píšeme v soustavě $(\mathbf{H}^T \mid \mathbf{o})$ matici soustavy jako transponovanou.

[b] Kontrolní matice podprostoru W není jednoznačně určena: volbou jiné soustavy rovnic získáme jinou kontrolní matici.

Základní vztah matic $\mathbf{G}$ a $\mathbf{H}^T$ pro lineární podprostor W

Platí

$$\begin{aligned}\{\mathbf{w} \in \mathbb{F}^n \mid \mathbf{G} \cdot \mathbf{a} = \mathbf{w} \text{ pro něj. } \mathbf{a} \text{ v } \mathbb{F}^k\} &= \mathrm{im}(\mathbf{G}) \\ &= W \\ &= \ker(\mathbf{H}^T) \\ &= \{\mathbf{w} \in \mathbb{F}^n \mid \mathbf{H}^T \cdot \mathbf{w} = \mathbf{o} \text{ v } \mathbb{F}^{n-k}\}\end{aligned}$$



Jinými slovy: $\mathbf{H}^T \cdot \mathbf{G} = \mathbf{O}_{k,n-k}$ a $\mathrm{rank}(\mathbf{G}) = \mathrm{def}(\mathbf{H}^T)$.

Co bude následovat v další přednášce?

1. V prostorech tvaru $\mathbb{F}^n$ zavedeme vztah ortogonality. To nám umožní mluvit přesně o generujících a kontrolních maticích lineárních podprostorů prostoru $\mathbb{F}^n$.
2. V prostorech tvaru $\mathbb{F}^n$ zavedeme pojem Hammingovy vzdálenosti vektorů. To nám později umožní zformulovat přesně metody detekce a opravy chyb v lineárních kódech.
3. Ukážeme, že existuje nekonečně mnoho konečných těles tvaru $\mathbb{Z}_p$, kde p je prvočíslo.

A co v následujících přednáškách?

Nahlédneme do teorie lineárních kódů.

1. Prostudujeme Hammingův $(7, 4)$-kód.
2. Ukážeme, jak Hammingova vzdálenost souvisí s detekcí a opravou chyb.
3. Ukážeme, jak vytvořit kontrolní matici z generující matice (a naopak).

Ortogonalita a Hammingova vzdálenost v $\mathbb{F}^n$

Odpřednesenou látku naleznete v dodatku I skript *Abstraktní a konkrétní lineární algebra*.

Dnešní přednáška

1. Konečná tělesa tvaru $\mathbb{Z}_p$, kde p je prvočíslo.
2. Základy ortogonální geometrie v $\mathbb{F}^n$, kde $\mathbb{F}$ je obecné těleso.
3. Hammingova vzdálenost v $\mathbb{F}^n$.

Příští přednáška

1. Základy kódování v prostorech $(\mathbb{Z}_p)^n$ nad $\mathbb{Z}_p$, kde p je prvočíslo.

Připomenutí (viz druhou přednášku) — definice tělesa

Množině $\mathbb{F}$ spolu se dvěma operacemi sčítání $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$, násobení $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$, říkáme těleso, pokud jsou splněny následující podmínky:

1. Axiomy pro sčítání: sčítání je komutativní, asociativní a má neutrální prvek 0. Každý prvek má opačný prvek vzhledem ke sčítání.
2. Axiomy pro násobení: násobení je komutativní, asociativní a má neutrální prvek 1.
3. Distributivní zákony:[a] platí $a \cdot (b + c) = a \cdot b + a \cdot c$ a $(b + c) \cdot a = b \cdot a + c \cdot a$.
4. Test invertibility: $a \neq 0$ právě tehdy, když existuje a^{-1}.

[a] Díky komutativitě násobení stačí požadovat platnost pouze jednoho z distributivních zákonů.

Počítání modulo číslo

Zvolme přirozené číslo $m \geq 2$. Sčítání a násobení definujeme na zbytcích po dělení číslem m. Množinu zbytků označíme $\mathbb{Z}_m$. Například: pro $m = 4$ je $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Tabulky sčítání a násobení v $\mathbb{Z}_4$ jsou:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Například (jako zbytky): $2 + 3 = 5 = 1$, $2 \cdot 3 = 6 = 2$ v $\mathbb{Z}_4$.

Pozor: $3^{-1} = 3$ (protože $3 \cdot 3 = 1$), ale 2^{-1} neexistuje.

Tedy $\mathbb{Z}_4$ není těleso. Důvod: existuje $a \neq 0$, pro které neexistuje a^{-1}. Test invertibility je jediný z axiomů tělesa, který je v $\mathbb{Z}_4$ porušen.

Věta

$\mathbb{Z}_m$ je těleso právě tehdy, když m je prvočíslo.[a]

[a] Viz také Tvrzení 1.2.2 skript.

Důkaz.

1. Je-li $m = a \cdot b$ složené číslo ($a > 1$ a $b > 1$), potom $a \cdot b = 0$ v $\mathbb{Z}_m$, takže ani a ani b nemají inversi v $\mathbb{Z}_m$.
2. Je-li m prvočíslo, ukážeme indukcí, že každé číslo a z množiny $\{1, \ldots, m-1\}$ má v $\mathbb{Z}_m$ inversi.
   1. Je-li $a = 1$, pak $a^{-1} = 1$.
   2. Ať a splňuje $1 < a \leq m - 1$. Předpokládejme, že každé číslo z množiny $\{1, \ldots, a-1\}$ má v $\mathbb{Z}_m$ inversi.
      Vydělme m číslem a se zbytkem: $m = q \cdot a + a'$, kde $a' < a$ je zbytek po dělení. Protože m je prvočíslo, platí $a' \geq 1$. Potom platí $0 = q \cdot a + a'$ v $\mathbb{Z}_m$.
      Takže v Z_m platí $a' = (-q) \cdot a$. Protože a' má podle indukčního předpokladu inversi, platí v $\mathbb{Z}_m$ rovnost $1 = \underbrace{(a'^{-1} \cdot (-q))}_{=a^{-1}} \cdot a$.

Příklady těles tvaru $\mathbb{Z}_p$, p prvočíslo

1. Těleso $\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

2. Těleso $\mathbb{Z}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Příklady těles tvaru $\mathbb{Z}_p$, p prvočíslo (pokrač.)

3. Násobení v tělese $\mathbb{Z}_{11}$ (vzpomeňte si na 10-ISBN):

$\cdot$	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Poznámky k existenci prvočísel

1. Množina $\mathbb{P}$ všech prvočísel je nekonečná množina. Hledání velkých prvočísel je ale velmi obtížné.
2. The Great Internet Mersenne Prime Search.
   Ke dni 9. 2. 2024 je největším známým prvočíslem číslo

$$2^{82\,589\,933} - 1 \quad \text{(GIMPS, 7. 12. 2018)}$$

   Má 24 862 048 cifer.[a] Viz například stránky:
   1. http://primes.utm.edu/primes/
   2. http://www.mersenne.org/
3. O některých testech prvočíselnosti se lze dočíst například v textu J. Velebil, *Diskrétní matematika*, Praha, 2007.

[a] Jak vypadá binární zápis tohoto prvočísla? Uvědomme si, že každé číslo tvaru $2^k - 1$ má ve svém binárním zápise k jedniček.

Úplný popis konečných těles

Tělesa tvaru $\mathbb{Z}_p$, kde p je prvočíslo, netvoří úplný seznam konečných těles.
Vytvoření úplného seznamu konečných těles vyžaduje rozumět výpočtům v okruhu $\mathbb{Z}_p[x]$ (okruh polynomů nad $\mathbb{Z}_p$) modulo polynom.

Více například v textu

J. Velebil, *Diskrétní matematika*, Praha, 2007.

Obecná konečná tělesa umožňují studium dalších aplikací:

1. Cyklické kódy.
2. Šifrování na eliptických křivkách.
3. A řadu dalších.

Připomenutí skalárního součinu v $\mathbb{R}^n$ nad $\mathbb{R}$

Skalární součin $\langle - \mid - \rangle$ v $\mathbb{R}^n$ je funkce tvaru

$$\langle - \mid - \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$$

která splňuje tři podmínky:

1. Pro vš. $\mathbf{x}$, $\mathbf{y}$ z $\mathbb{R}^n$ platí rovnost $\langle \mathbf{x} \mid \mathbf{y} \rangle = \langle \mathbf{y} \mid \mathbf{x} \rangle$.
2. Pro vš. $\mathbf{x}$ z $\mathbb{R}^n$ platí, že $\langle \mathbf{x} \mid - \rangle : \mathbb{R}^n \to \mathbb{R}$ je lineární zobrazení.
3. Pro vš. $\mathbf{x}$ z $\mathbb{R}^n$ platí $\langle \mathbf{x} \mid \mathbf{x} \rangle \geq 0$. Rovnost $\langle \mathbf{x} \mid \mathbf{x} \rangle = 0$ platí právě tehdy, když $\mathbf{x} = \mathbf{o}$.

Poznámka

Třetí podmínku šlo zformulovat, protože $\mathbb{R}$ je uspořádané těleso, tj. protože umíme rozpoznat nezáporná reálná čísla. Obecné těleso ale „rozumně“ uspořádat jít nemusí.[a]

[a] Např. těleso $\mathbb{C}$ uspořádat nelze, viz Příklad 1.3.8 skript. Viz také následující příklad.

Příklad (žádné konečné těleso $\mathbb{F}$ není uspořádané těleso)

Ať $\mathbb{F}$ je konečné těleso. V množině $\mathbb{F}$ nelze zadat podmnožinu $\mathbb{F}_+$ (množinu kladných prvků tělesa $\mathbb{F}$), která splňuje následující dvě podmínky:

1. Platí přesně jedna z podmínek $a = 0$, $a \in \mathbb{F}_+$, $-a \in \mathbb{F}_+$.
2. Jestliže $a \in \mathbb{F}_+$ a $b \in \mathbb{F}_+$, pak $a + b \in \mathbb{F}_+$ a $ab \in \mathbb{F}_+$.

Postupujeme sporem: ať taková množina $\mathbb{F}_+$ existuje.[a]
Protože $\mathbb{F}$ je konečná množina, existuje nejmenší kladné přirozené číslo n tak, že $\underbrace{1 + \cdots + 1}_{n\text{-krát}} = 0$.

Z axiomů pro $\mathbb{F}_+$ plyne, že platí $a^2 \in \mathbb{F}_+$ pro vš. $a \neq 0$.
Protože $1 = 1^2$, musí platit $1 \in \mathbb{F}_+$ a $\underbrace{1 + \cdots + 1}_{n\text{-krát}} \in \mathbb{F}_+$. To je spor.

[a] Množina $\mathbb{F}_+$ s těmito vlastnostmi umožňuje definovat uspořádání: $a < b$ iff $b - a \in \mathbb{F}_+$.

Tvrzení (vlastnosti zobrazení $\gamma : (\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x}^T \cdot \mathbf{y}$ pro $\mathbf{x}$, $\mathbf{y}$ z $\mathbb{F}^n$)

Ať $\mathbb{F}$ je jakékoli těleso. Zobrazení $\gamma : (\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x}^T \cdot \mathbf{y}$ z množiny $\mathbb{F}^n \times \mathbb{F}^n$ do množiny $\mathbb{F}$ se chová velmi podobně jako standardní skalární součin v $\mathbb{R}^n$. To jest, platí následující:

1. Pro vš. $\mathbf{x}$, $\mathbf{y}$ z $\mathbb{F}^n$ platí $\gamma(\mathbf{x}, \mathbf{y}) = \gamma(\mathbf{y}, \mathbf{x})$.
2. Pro vš. $\mathbf{x}$ z $\mathbb{F}^n$ je zobrazení $\gamma(\mathbf{x}, -) : \mathbb{F}^n \to \mathbb{F}$ lineární.

Podmínka

3. Rovnost $\gamma(\mathbf{x}, \mathbf{x}) = 0$ platí právě tehdy, když $\mathbf{x} = \mathbf{o}$.

ale obecně neplatí (protipříklad lze nalézt například v $(\mathbb{Z}_2)^2$).

Důkaz.

1. Protože $\gamma(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T \cdot \mathbf{y}$ a $\gamma(\mathbf{y}, \mathbf{x}) = \mathbf{y}^T \cdot \mathbf{x} = (\mathbf{x}^T \cdot \mathbf{y})^T$, platí[a] $\gamma(\mathbf{x}, \mathbf{y}) = \gamma(\mathbf{y}, \mathbf{x})$.

[a] Každá matice rozměrů 1×1 je totiž symetrická.

Důkaz (pokrač.).

2. Pro vš. $\mathbf{x}$ z $\mathbb{F}^n$ je zobrazení $\gamma(\mathbf{x}, -) : \mathbb{F}^n \to \mathbb{F}$ lineární, protože $\gamma(\mathbf{x}, a_1 \cdot \mathbf{y}_1 + a_2 \cdot \mathbf{y}_2) = \mathbf{x}^T \cdot (a_1 \cdot \mathbf{y}_1 + a_2 \cdot \mathbf{y}_2) = a_1 \cdot \mathbf{x}^T \cdot \mathbf{y}_1 + a_2 \cdot \mathbf{x}^T \cdot \mathbf{y}_2 = a_1 \cdot \gamma(\mathbf{x}, \mathbf{y}_1) + a_2 \cdot \gamma(\mathbf{x}, \mathbf{y}_2)$.
3. Pro $\mathbf{x} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ v $(\mathbb{Z}_2)^2$ platí $\gamma(\mathbf{x}, \mathbf{x}) = \mathbf{x}^T \cdot \mathbf{x} = 0$.

■

K čemu jsme použili positivní definitnost skalárních součinů?

Použili jsme ji pouze k důkazu C-S-B nerovnosti (tím pádem pro definici úhlu mezi vektory a pro definici normy a metriky vytvořené skalárním součinem).

Positivní definitnost jsme nepotřebovali pro definici ortogonality.

Připomenutí: vektory $\mathbf{x}$, $\mathbf{y}$ v $\mathbb{R}^n$ jsou ortogonální (vzhledem ke skalárnímu součinu $\langle - \mid - \rangle$), pokud platí $\langle \mathbf{x} \mid \mathbf{y} \rangle = 0$.

Definice (ortogonalita v $\mathbb{F}^n$)

Řekneme, že vektory $\mathbf{x}$, $\mathbf{y}$ z $\mathbb{F}^n$ jsou ortogonální[a] (také: navzájem na sebe kolmé), pokud platí $\mathbf{x}^T \cdot \mathbf{y} = 0$.

[a] Přesněji: v $\mathbb{F}^n$ jde o ortogonalitu vzhledem k $\gamma(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T \cdot \mathbf{y}$.
Slogan: ortogonalita v $\mathbb{F}^n$ zobecňuje ortogonalitu vzhledem ke standardnímu skalárnímu součinu v $\mathbb{R}^n$.

Definice (ortogonální doplněk lineárního podprostoru $\mathbb{F}^n$)

Pro lineární podprostor W prostoru $\mathbb{F}^n$ definujeme jeho ortogonální doplněk jako množinu

$$W^\perp = \{\mathbf{x} \in \mathbb{F}^n \mid \mathbf{w}^T \cdot \mathbf{x} = 0 \text{ pro všechna } \mathbf{w} \text{ z } W\}$$

Poznámka

Protože $\mathbf{w}^T \cdot \mathbf{x} = 0$ iff $\mathbf{x}^T \cdot \mathbf{w} = 0$, platí

$$W^\perp = \{\mathbf{x} \in \mathbb{F}^n \mid \mathbf{x}^T \cdot \mathbf{w} = 0 \text{ pro všechna } \mathbf{w} \text{ z } W\}$$

Věta (vlastnosti ortogonálního doplňku)

Ať W je lineární podprostor prostoru $\mathbb{F}^n$. Potom platí:

1. $W^\perp$ je opět lineární podprostor prostoru $\mathbb{F}^n$.
2. Je-li $\dim(W) = k$, pak $\dim(W^\perp) = n - k$.
3. Platí $(W^\perp)^\perp = W$.

Důkaz.

1.
   1. Pro všechna $\mathbf{w}$ z W platí $\mathbf{w}^T \cdot \mathbf{o} = 0$. Tudíž $\mathbf{o}$ je ve $W^\perp$.
   2. Jestliže $\mathbf{x}_1$ a $\mathbf{x}_2$ jsou ve $W^\perp$, pak
   $$\mathbf{w}^T \cdot (a_1 \cdot \mathbf{x}_1 + a_2 \cdot \mathbf{x}_2) = a_1 \cdot \underbrace{\mathbf{w}^T \cdot \mathbf{x}_1}_{=0} + a_2 \cdot \underbrace{\mathbf{w}^T \cdot \mathbf{x}_2}_{=0} = 0$$
   pro všechna $\mathbf{w}$ ve W. Ukázali jsme, že $W^\perp$ je uzavřen v $\mathbb{F}^n$ na tvorbu lineárních kombinací.

   Takže $W^\perp$ je lineární podprostor[a] prostoru $\mathbb{F}^n$.

[a] Elegantní důkaz téhož: $W^\perp = \bigcap_{\mathbf{w} \in W} \ker(\gamma(\mathbf{w}, -))$, kde $\gamma(\mathbf{w}, \mathbf{x}) = \mathbf{w}^T \cdot \mathbf{x}$.

Důkaz (pokrač.).

2. Označme jako $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ uspořádanou bázi W. Pro matici $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_k)$ platí: $\mathbf{x}$ je ve $W^\perp$ iff $\mathbf{A}^T \cdot \mathbf{x} = \mathbf{o}$ iff $\mathbf{x}$ je v $\ker(\mathbf{A}^T)$. Neboli: $W^\perp = \ker(\mathbf{A}^T)$.

   Protože $\mathrm{rank}(\mathbf{A}^T) = \mathrm{rank}(\mathbf{A}) = k$ a protože $\mathbf{A}^T : \mathbb{F}^n \to \mathbb{F}^k$, je $\mathrm{def}(\mathbf{A}^T) = n - k$ podle věty o dimensi jádra a obrazu.

   To znamená, že $\dim(W^\perp) = n - k$.

3. Zjevně platí $W \subseteq (W^\perp)^\perp$, protože každý vektor $\mathbf{w}$ z W je ortogonální ke každému vektoru z $W^\perp$.

   Je-li $\dim(W) = k$, je $\dim((W^\perp)^\perp) = n - (n - k) = k$.

   Proto $W = (W^\perp)^\perp$.

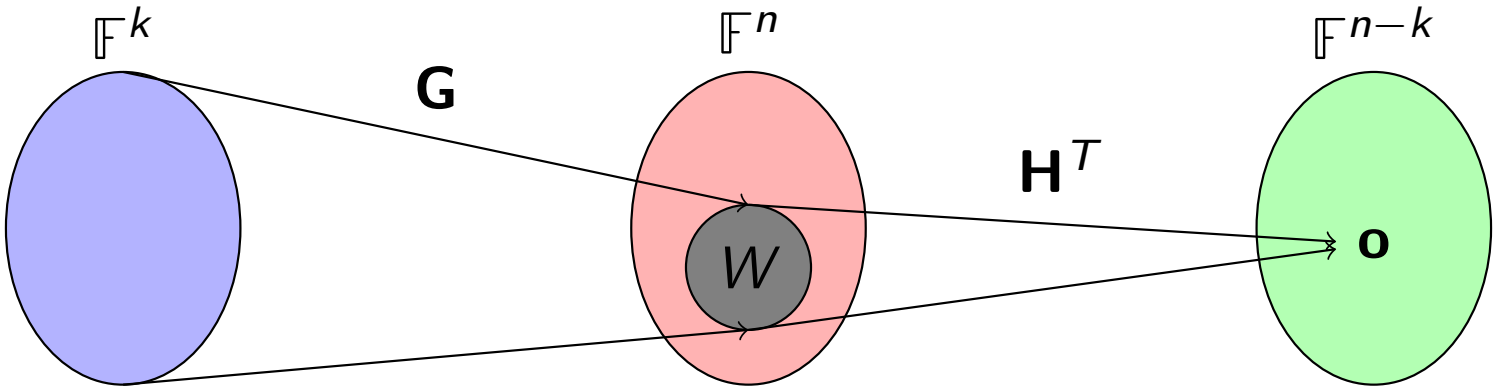
Příklad (rovnost $W = W^\perp$ může platit)

Pro podmnožinu $W = \{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\}$ lineárního prostoru $(\mathbb{Z}_2)^2$ platí:[a]

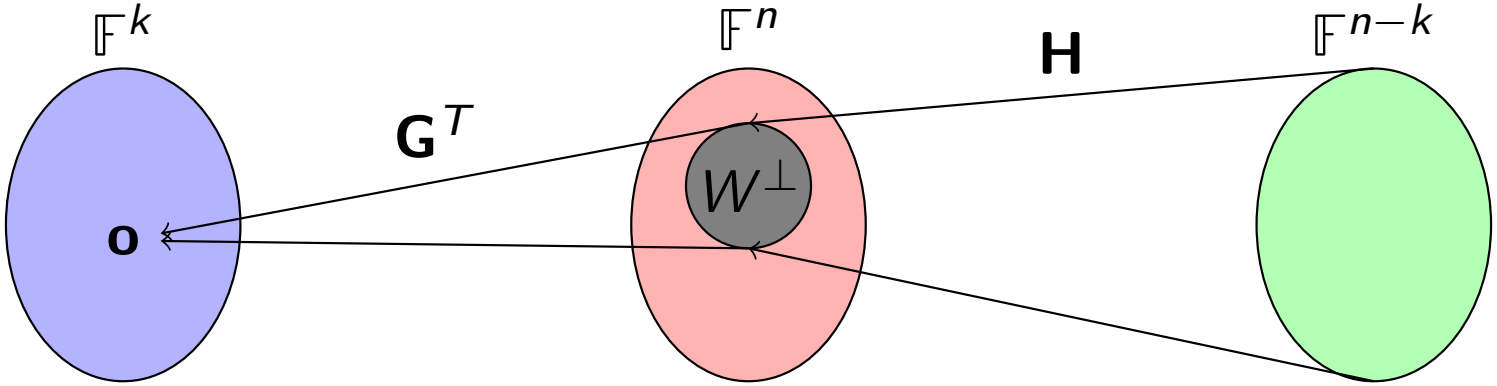
1. W je lineární podprostor prostoru $(\mathbb{Z}_2)^2$.
2. $W = \text{span}(\begin{pmatrix}1\\1\end{pmatrix})$, $\dim(W) = 1$.
3. $$\begin{aligned} W^\perp &= \{\begin{pmatrix}x_1\\x_2\end{pmatrix} \mid \begin{pmatrix}0\\0\end{pmatrix}^T \cdot \begin{pmatrix}x_1\\x_2\end{pmatrix} = 0 \text{ a současně } \begin{pmatrix}1\\1\end{pmatrix}^T \cdot \begin{pmatrix}x_1\\x_2\end{pmatrix} = 0\} \\ &= W \end{aligned}$$

[a] Pro zájemce (nepovinné): „absurdní“ rovnost $W = W^\perp$ je způsobena degenerovaností podprostoru W prostoru $(\mathbb{Z}_2)^2$. Všechny vektory podprostoru W jsou totiž na sebe navzájem kolmé.

Dualita generujících a kontrolních matic podprostoru



$$\mathrm{im}(\mathbf{G}) = W = \ker(\mathbf{H}^T)$$



$$\mathrm{im}(\mathbf{H}) = W^\perp = \ker(\mathbf{G}^T)$$

Definice (Hammingova vzdálenost v $\mathbb{F}^n$)

Pro vektory $\mathbf{x}$, $\mathbf{y}$ z $\mathbb{F}^n$ definujeme

$$d_H(\mathbf{x}, \mathbf{y}) = \text{ počet různých položek vektorů } \mathbf{x} \text{ a } \mathbf{y}$$

Přirozenému číslu $d_H(\mathbf{x}, \mathbf{y})$ říkáme Hammingova vzdálenost vektorů $\mathbf{x}$ a $\mathbf{y}$.

Poznámka

Pro všechny vektory $\mathbf{x}$, $\mathbf{y}$ z $\mathbb{F}^n$ platí $d_H(\mathbf{x}, \mathbf{y}) \leq n$.

Tvrzení (Hammingova vzdálenost je metrika na $\mathbb{F}^n$)

Pro všechny vektory $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ z $\mathbb{F}^n$ platí:

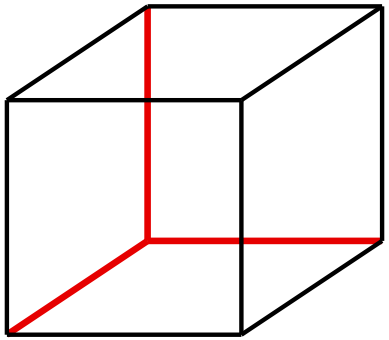
1. $d_H(\mathbf{x}, \mathbf{y}) \geq 0$, rovnost nastává právě tehdy, když $\mathbf{x} = \mathbf{y}$.
2. $d_H(\mathbf{x}, \mathbf{y}) = d_H(\mathbf{y}, \mathbf{x})$.
3. $d_H(\mathbf{x}, \mathbf{y}) \leq d_H(\mathbf{x}, \mathbf{z}) + d_H(\mathbf{z}, \mathbf{y})$.

Důkaz.

Důkaz plyne okamžitě z definice d_H. ∎

Příklad (Hammingova vzdálenost v $(\mathbb{Z}_2)^3$)

Osm vektorů $\begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}$ prostoru $(\mathbb{Z}_2)^3$ si lze představit jako vrcholy krychle (červené hrany jsou souřadnicové osy):



Hammingova vzdálenost dvou vektorů je pak délka nejkratší cesty po hranách krychle z jednoho vrcholu do druhého.

Podobnou představu lze mít o Hammingově vzdálenosti vektorů v prostoru $(\mathbb{Z}_2)^n$: vektory v $(\mathbb{Z}_2)^n$ jsou vrcholy n-dimensionální krychle.

Lineární kódy

Odpřednesenou látku naleznete v dodatku I skript *Abstraktní a konkrétní lineární algebra*.

Dnešní přednáška

1. Analýza Hammingova $(7,4)$-kódu.
2. Lineární kódy nad $\mathbb{Z}_p$.
3. Oprava a detekce chyb.
4. Syndrome decoding a nearest neighbour decoding.

Další možné doplňující informace

1. J. Adámek, *Foundations of coding*, John Wiley & Sons, 1991
2. D. J. C. MacKay, *Information theory, inference and learning algorithms*, Cambridge Univ. Press, 2003
3. W. C. Huffman a V. Pless, *Fundamentals of error-correcting codes*, Cambridge Univ. Press, 2003

Připomenutí (minulé přednášky):

Teorie lineárních prostorů nad obecným tělesem $\mathbb{F}$ byla vybudována.

Příkladem těles jsou $\mathbb{Z}_p$, kde p je prvočíslo.

To znamená:

1. Umíme určit bázi a dimensi podprostorů W lineárního prostoru $(\mathbb{Z}_p)^n$.
2. Umíme pracovat s maticemi nad $\mathbb{Z}_p$ a řešit soustavy lineárních rovnic nad $\mathbb{Z}_p$.

Navíc:

3. V prostoru $(\mathbb{Z}_p)^n$ rozumíme relaci ortogonality a Hammingově vzdálenosti.
4. V prostoru $(\mathbb{Z}_p)^n$ rozumíme generujícím a kontrolním maticím lineárních podprostorů.

Příklad (Hammingův $(7,4)$-kód)

V $(\mathbb{Z}_2)^7$ zvolme lineární podprostor W dimense 4 s bází danou vektory

$$\mathbf{g}_1 = \begin{pmatrix}1\\0\\0\\0\\0\\1\\1\end{pmatrix}, \mathbf{g}_2 = \begin{pmatrix}0\\1\\0\\0\\1\\0\\1\end{pmatrix}, \mathbf{g}_3 = \begin{pmatrix}0\\0\\1\\0\\1\\1\\0\end{pmatrix}, \mathbf{g}_4 = \begin{pmatrix}0\\0\\0\\1\\1\\1\\1\end{pmatrix}$$

Generující matice $\mathbf{G}$ podprostoru W je

$$\mathbf{G} = (\mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3, \mathbf{g}_4) = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\\0&1&1&1\\1&0&1&1\\1&1&0&1\end{pmatrix}$$

Příklad (Hammingův $(7,4)$-kód, pokrač.)

1. $\mathrm{rank}(\mathbf{G}) = 4$, tudíž máme k disposici 4 info bity.
2. Dimense ortogonálního doplňku $7 - 4 = 3$. Informace bude chráněna třemi bity (redundance).
3. Posílání zpráv: informace $\begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$ vytváří kódové slovo

$$\mathbf{G} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Pozorování: $\mathbf{G}$ je v blokovém tvaru $\left(\begin{array}{c} \mathbf{E}_4 \\ \hline \mathbf{B} \end{array}\right)$.[a]

[a] Takovým kódům se říká systematické: jsou v nich jasně odděleny informační a ochranné bity.

Příklad (Hammingův $(7,4)$-kód, pokrač.)

Kontrolní (Hammingova) matice

$$\mathbf{H}^T = \begin{pmatrix} \mathbf{h}_1^T \\ \mathbf{h}_2^T \\ \mathbf{h}_3^T \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Jde o ideální kód, pokud došlo nejvýše k jedné chybě:[a]

1. Odesláno $\mathbf{w}$, přijmeme $\mathbf{v}$ a předpokládáme, že došlo k nejvýše jedné chybě. Tj. $\mathbf{v} = \mathbf{w} + \mathbf{e}$ ($\mathbf{e}$ je error pattern). Víme, že $\mathbf{e}$ obsahuje nejvýše jednu jedničku.
2. Spočteme syndrom $\mathbf{s}$ slova $\mathbf{v}$: $\mathbf{s} = \mathbf{H}^T\mathbf{v} = \mathbf{H}^T\mathbf{e}$.
   1. Jestliže $\mathbf{s} = \mathbf{o}$, při přenosu nedošlo k chybě, tj. $\mathbf{e} = \mathbf{o}$, neboli $\mathbf{v} = \mathbf{w}$.
   2. Jestliže $\mathbf{s}$ je i-tý sloupec $\mathbf{H}^T$, je $\mathbf{e} = \mathbf{e}_i$. Došlo k chybě na i-tém místě. Opravíme ji: $\mathbf{w} = \mathbf{v} - \mathbf{e}_i$.
3. Isolujeme info bity.

[a] Jde dokonce o příklad tzv perfektního kódu pro opravu jedné chyby, viz příští přednášku.

Příklad (Hammingův $(7,4)$-kód, pokrač.)

Co se stane, pokud error pattern $\mathbf{e}$ obsahuje dvě jedničky? Tj., co nastane, pokud při přenosu došlo k právě dvěma chybám?

Spočteme syndrom $\mathbf{s}$ slova $\mathbf{v}$: $\mathbf{s} = \mathbf{H}^T\mathbf{v} = \mathbf{H}^T\mathbf{e}$.

Pokud jsou jedničky v $\mathbf{e}$ na místech i a j, je $\mathbf{H}^T\mathbf{e}$ součet i-tého a j-tého sloupce matice $\mathbf{H}^T$.

Připomeňme, že

$$\mathbf{H}^T = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Dvě chyby na první a druhé posici současně tedy nerozlišíme od jedné chyby na pouze třetí posici.

Problém návrhu lineárního kódu

Jak vyvážit následující požadavky? Chceme co největší opravné schopnosti kódu a co nejmenší počet kontrolních bitů.

Tyto požadavky jsou intuitivně protichůdné.

V plné obecnosti se nyní budeme věnovat dvěma tématům

1. Způsoby dekódování lineárních kódů.
2. Opravné a ochranné schopnosti lineárních kódů.

Obě témata mají jasnou geometrickou interpretaci.

Definice (lineární kód)

Ať p je prvočíslo. Lineární p-kód délky n a dimense k je lineární podprostor W prostoru $(\mathbb{Z}_p)^n$, $\dim(W) = k$, $0 \leq k \leq n$.
Terminologie:

1. Prvkům $(\mathbb{Z}_p)^n$ říkáme také slova, prvkům W kódová slova.[a]
2. Generující matice $\mathbf{G} : (\mathbb{Z}_p)^k \to (\mathbb{Z}_p)^n$ kódu W je (jakákoli) generující matice podprostoru W.
3. Vektoru $\mathbf{w} = \mathbf{G} \cdot \mathbf{a}$ říkáme kódové slovo určené vektorem informace $\mathbf{a}$ ze $(\mathbb{Z}_p)^k$.
4. Kontrolní matice $\mathbf{H}^T : (\mathbb{Z}_p)^n \to (\mathbb{Z}_p)^{n-k}$ je (jakákoli) kontrolní matice podprostoru W.
5. Součinu $\mathbf{s} = \mathbf{H}^T \cdot \mathbf{v}$ říkáme syndrom slova $\mathbf{v}$.

[a] Slova a kódová slova jsou vektory v $(\mathbb{Z}_p)^n$, píšeme je tedy do sloupce. Poznámky ke značení v jiné literatuře uvedeme na příští přednášce.

Geometrie error patternu a jeho syndromu

Ať W je lineární p-kód délky n a dimense k s generující maticí $\mathbf{G} = (\mathbf{g}_1, \ldots, \mathbf{g}_k)$ a kontrolní maticí $\mathbf{H}^T$. Zvolme jakékoli slovo $\mathbf{e}$ ze $(\mathbb{Z}_p)^n$ (tzv. error pattern) a označme $\mathbf{H}^T \cdot \mathbf{e} = \mathbf{s}$ syndrom slova $\mathbf{e}$.

Z lineární algebry okamžitě plyne:[a]

$\mathbf{e} + W$ je k-dimensionální plocha v $(\mathbb{Z}_p)^n$.

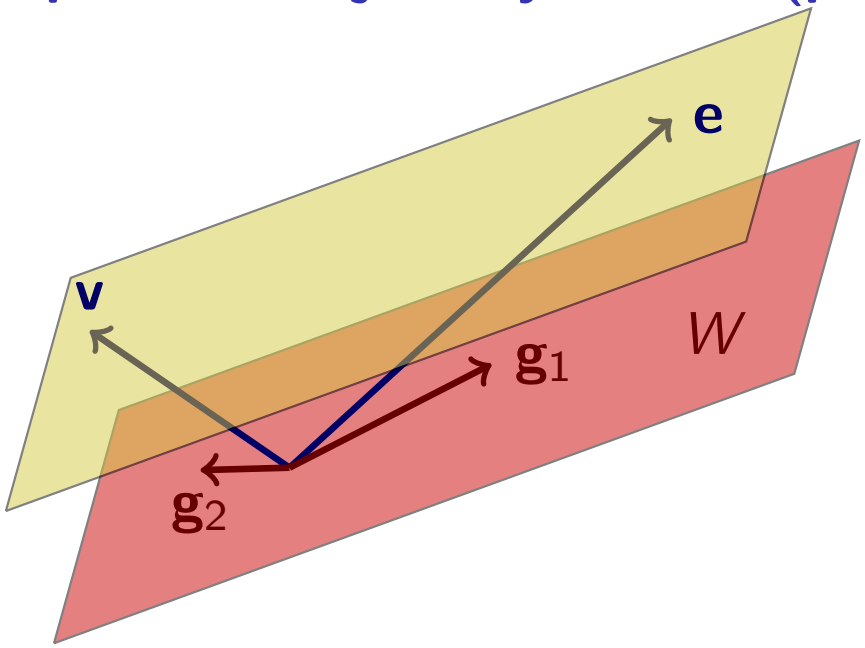
Tato plocha prochází bodem $\mathbf{e}$ a má směr $(\mathbf{g}_1, \ldots, \mathbf{g}_k)$.

Platí totiž, že $\mathbf{e} + W$ je přesně množina řešení soustavy $(\mathbf{H}^T \mid \mathbf{s})$.

Jiný pohled na totéž: $\mathbf{e} + W$ je přesně množina všech slov $\mathbf{v}$ ze $(\mathbb{Z}_p)^n$ se syndromem $\mathbf{s} = \mathbf{H}^T \cdot \mathbf{e}$.

[a] Připomeňte si přednášku 6B.

Geometrie error patternu a jeho syndromu (pokrač.)



k-dimensionální plocha $\mathbf{e} + W$ v $(\mathbb{Z}_p)^n$ je přesně množina všech slov $\mathbf{v}$ ze $(\mathbb{Z}_p)^n$ se syndromem $\mathbf{s}$.

Dekódovací strategie: přijmeme-li slovo $\mathbf{v}$, stačí nalézt $\mathbf{e}$ tak, aby $\mathbf{v}$ bylo v $\mathbf{e} + W$. Potom bylo odesláno slovo $\mathbf{w} = \mathbf{v} - \mathbf{e}$.

Problém této strategie: je pro $\mathbf{v}$ error pattern $\mathbf{e}$ určen jednoznačně? Není! Existuje ale „přirozená“ volba: ať $\mathbf{e}$ je „co nejblíže“ $\mathbf{o}$.

V úvahách o dekódování, opravách a detekci chyb budou hrát roli následující pojmy:

Definice (Hammingova váha slova a min. distance kódu)

1. Hammingova váha $w_H(\mathbf{v}) = d_H(\mathbf{v}, \mathbf{o})$ slova $\mathbf{v}$. Zjevně platí: $w_H(\mathbf{v}) =$ počet nenulových položek slova $\mathbf{v}$.
2. Minimální (Hammingova) distance kódu W
   $\mathrm{dist}(W) = \min\{w_H(\mathbf{w}) \mid \mathbf{w}$ je nenulové slovo ve $W\}$.

Poznámka (jiný vzorec pro minimální distanci kódu)

Platí: $\mathrm{dist}(W) = \min\{d_H(\mathbf{w}, \mathbf{w}') \mid \mathbf{w}, \mathbf{w}'$ jsou různá slova z $W\}$.

Opravdu: pro různá slova $\mathbf{w}$, $\mathbf{w}'$ z W je $\mathbf{w} - \mathbf{w}'$ nenulové slovo z W a platí $d_H(\mathbf{w}, \mathbf{w}') = w_H(\mathbf{w} - \mathbf{w}')$. Obráceně, pro nenulové slovo $\mathbf{w}$ z W je $w_H(\mathbf{w}) = d_H(\mathbf{w}, \mathbf{o})$ Hammingova vzdálenost dvou různých slov ve W.

Tvrzení

Ať $\mathbf{H}^T$ je kontrolní matice kódu W. Pro kladné přirozené číslo d jsou následující podmínky ekvivalentní:

1. Kód W má minimální distanci d.
2. Každých $d-1$ sloupců matice $\mathbf{H}^T$ je lineárně nezávislých a některých d sloupců matice $\mathbf{H}^T$ je lineárně závislých.

Důkaz.

Kód W obsahuje slovo $\mathbf{w}$ váhy $w > 0$ iff $\mathbf{H}^T \cdot \mathbf{w} = \mathbf{o}$ iff $w > 0$ sloupců $\mathbf{H}^T$ je lineárně závislých. ■

Důsledek (Singletonův odhad)

Ať W je kód délky n a dimense k. Potom $\mathrm{dist}(W) \leq n - k + 1$.

Důkaz.

Pro kontrolní matici $\mathbf{H}^T$ kódu W platí $\mathrm{rank}(\mathbf{H}^T) = n - k$. Tudíž $\mathrm{dist}(W) - 1 \leq n - k$. ■

Příklad (minimální distance Hammingova $(7,4)$-kódu)

Hammingův $(7,4)$-kód má kontrolní matici

$$\mathbf{H}^T = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Označme jako d minimální distanci tohoto kódu.

Singletonův odhad dává: $d - 1 \leq 7 - 4 + 1$, čili $d \leq 5$.

Ve skutečnosti platí $d = 3$.

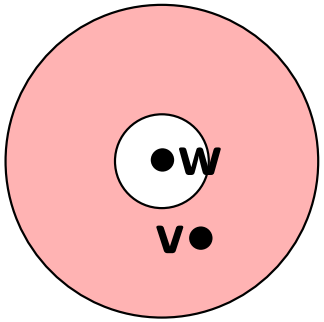
Proč? Například první tři sloupce matice $\mathbf{H}^T$ jsou lineárně závislé, jakákoli dvojice sloupců matice $\mathbf{H}^T$ je lineárně nezávislá.

Definice (detekce a oprava chyb)

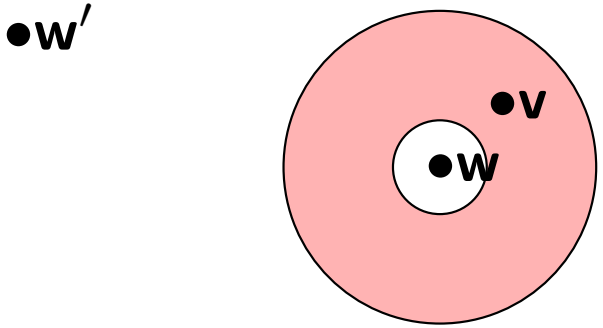
Ať W je lineární kód. Řekneme, že

1. W detekuje t chyb, pokud pro každé $\mathbf{w}$ ve W a každé $\mathbf{v}$ takové, že $1 \leq d_H(\mathbf{w}, \mathbf{v}) \leq t$, platí: $\mathbf{v}$ není ve W.
2. W opravuje t chyb, pokud pro každé $\mathbf{w}$ ve W a každé $\mathbf{v}$ takové, že $1 \leq d_H(\mathbf{w}, \mathbf{v}) \leq t$, platí: $d_H(\mathbf{w}, \mathbf{v}) < d_H(\mathbf{w}', \mathbf{v})$ pro všechna $\mathbf{w}'$ z W různá od $\mathbf{w}$.

Geometrie detekce a opravy chyb (slogany)



Detekce: slova nedaleko od kódového slova nejsou ve W.



Oprava: slova nedaleko od kódového slova jsou daleko od jiných slov z W.

Tvrzení

Kód W detekuje t chyb právě tehdy, když $\mathrm{dist}(W) > t$.

Důkaz.

1. Ať $\mathrm{dist}(W) \leq t$. Zvolme kódová slova $\mathbf{w}$, $\mathbf{w}'$ tak, že $d_H(\mathbf{w}, \mathbf{w}') = \mathrm{dist}(W)$. Potom $1 \leq d_H(\mathbf{w}, \mathbf{w}') \leq t$.

   To znamená, že nelze detekovat následujících t chyb: odesláno slovo $\mathbf{w}$, přijato slovo $\mathbf{w}'$.

2. Ať $\mathrm{dist}(W) > t$. Zvolme $\mathbf{w}$ ve W a $\mathbf{v}$ takové, že platí $1 \leq d_H(\mathbf{w}, \mathbf{v}) \leq t$.

   Potom $d_H(\mathbf{w}, \mathbf{v}) < \mathrm{dist}(W)$, takže $\mathbf{v}$ nemůže být kódové slovo.

■

Tvrzení

Kód W opravuje t chyb právě tehdy, když $\mathrm{dist}(W) > 2t$.

Důkaz.

1. Ať $\mathrm{dist}(W) \leq 2t$. Zvolme kódová slova $\mathbf{w}$, $\mathbf{w}'$ tak, že $d_H(\mathbf{w}, \mathbf{w}') = \mathrm{dist}(W)$ a označme jako $i_1, \ldots, i_r$ indexy položek, ve kterých se $\mathbf{w}$ a $\mathbf{w}'$ liší.
   Definujme $\mathbf{v}$ jako slovo, které má stejné položky jako $\mathbf{w}$, kromě položek $i_2, i_4, \ldots$, na kterých má stejné položky jako $\mathbf{w}'$.

   Potom $1 \leq d_H(\mathbf{w}, \mathbf{v}) \leq \frac{r}{2} \leq t$, ale $d_H(\mathbf{w}', \mathbf{v}) \leq d_H(\mathbf{w}, \mathbf{v})$.
2. Ať $\mathrm{dist}(W) > 2t$. Ať $\mathbf{w}$ je ve W a ať platí $1 \leq d_H(\mathbf{w}, \mathbf{v}) \leq t$.
   Pro jakékoli $\mathbf{w}'$ ve W platí $d_H(\mathbf{w}, \mathbf{w}') \geq \mathrm{dist}(W) > 2t$.
   To znamená, že $2t < d_H(\mathbf{w}, \mathbf{w}') \leq d_H(\mathbf{w}, \mathbf{v}) + d_H(\mathbf{v}, \mathbf{w}')$.

   Takže $d_H(\mathbf{w}', \mathbf{v}) > 2t - d_H(\mathbf{w}, \mathbf{v}) \geq 2t - t = t \geq d_H(\mathbf{w}, \mathbf{v})$.

Syndrome decoding

Ať W je lineární p-kód délky n a dimense k. Předpokládejme, že odeslané kódové slovo z W bylo přijato jako slovo $\mathbf{v}$ ze $(\mathbb{Z}_p)^n$.

Syndrome decoding je následující dekódovací procedura:

1. Spočteme syndrom $\mathbf{H}^T \cdot \mathbf{v} = \mathbf{s}$ slova $\mathbf{v}$.
2. Nalezneme takové řešení soustavy $(\mathbf{H}^T \mid \mathbf{s})$ tvaru $\mathbf{e} + W$, kde Hammingova váha $w_H(\mathbf{e})$ je nejmenší možná.[a]

   Předpokládáme, že bylo odesláno kódové slovo $\mathbf{w} = \mathbf{v} - \mathbf{e}$.

[a] Pokud je takových $\mathbf{e}$ více, vybereme některé z nich náhodně.

Kolik různých syndromů existuje?

Kontrolní matice W je lineární zobrazení $\mathbf{H}^T : (\mathbb{Z}_p)^n \to (\mathbb{Z}_p)^{n-k}$.
Slovo $\mathbf{s}$ je syndrom právě když $\mathbf{s}$ leží v $\mathrm{im}(\mathbf{H}^T)$.
Protože $\mathrm{rank}(\mathbf{H}^T) = n - k$, existuje celkem p^{n-k} různých syndromů.

Příklad (Hammingův $(7,4)$-kód a syndrome decoding)

Existuje 8 různých syndromů: $\mathbf{s}_0 = \begin{pmatrix}0\\0\\0\end{pmatrix}$, $\mathbf{s}_1 = \begin{pmatrix}0\\0\\1\end{pmatrix}$, $\mathbf{s}_2 = \begin{pmatrix}0\\1\\0\end{pmatrix}$,

$\mathbf{s}_3 = \begin{pmatrix}0\\1\\1\end{pmatrix}$, $\mathbf{s}_4 = \begin{pmatrix}1\\0\\0\end{pmatrix}$, $\mathbf{s}_5 = \begin{pmatrix}1\\0\\1\end{pmatrix}$, $\mathbf{s}_6 = \begin{pmatrix}1\\1\\0\end{pmatrix}$, $\mathbf{s}_7 = \begin{pmatrix}1\\1\\1\end{pmatrix}$.

Vyřešením příslušných soustav nalezneme 8 „nejmenších“ error

paterns: $\mathbf{e}_0 = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\end{pmatrix}$, $\mathbf{e}_1 = \begin{pmatrix}1\\0\\0\\0\\0\\0\\0\end{pmatrix}$, $\mathbf{e}_2 = \begin{pmatrix}0\\1\\0\\0\\0\\0\\0\end{pmatrix}$, $\ldots$, $\mathbf{e}_7 = \begin{pmatrix}0\\0\\0\\0\\0\\0\\1\end{pmatrix}$.

Vidíme, že syndrome decoding Hammingova $(7,4)$-kódu je korektní pro opravu nejvýše jedné chyby.[a]

[a] Dekódování již nelze nijak vylepšit, protože minimální distance tohoto kódu je 3.

Nearest neighbour decoding

Ať W je linární p-kód délky n a dimense k. Předpokládejme, že odeslané kódové slovo z W bylo přijato jako slovo $\mathbf{v}$ ze $(\mathbb{Z}_p)^n$.

Nearest neighbour decoding je následující dekódovací procedura:

1. Pokud je $\mathbf{v}$ kódové slovo, předpokládáme, že k žádné chybě nedošlo.

   Předpokládáme tedy, že bylo odesláno kódové slovo $\mathbf{v}$.

2. Pokud $\mathbf{v}$ kódové slovo není, nalezneme takové kódové slovo $\mathbf{w}$, pro které je Hammingova vzdálenost $d_H(\mathbf{v}, \mathbf{w})$ nejmenší.[a]

   Předpokládáme, že bylo odesláno kódové slovo $\mathbf{w}$.

[a] Pokud je takových kódových $\mathbf{w}$ slov více, vybereme některé z nich náhodně.

Tvrzení (syndrome decoding = nearest neighbour decoding)

Ať W je linární p-kód délky n a dimense k. Předpokládejme, že odeslané kódové slovo z W bylo přijato jako slovo $\mathbf{v}$ ze $(\mathbb{Z}_p)^n$. Potom množiny

$$\{\mathbf{w} \in W \mid \text{Hammingova vzdálenost } d_H(\mathbf{v}, \mathbf{w}) \text{ je nejmenší}\}$$

a

$$\{\mathbf{w} \in W \mid \text{Hammingova váha } w_H(\mathbf{v} - \mathbf{w}) \text{ je nejmenší}\}$$

jsou stejné.

To jest: syndrome decoding a nearest neighbour decoding jsou totožné procedury.

Důkaz.

Podle definice Hammingovy vzdálenosti platí pro libovolné vektory $\mathbf{x}$, $\mathbf{y}$ rovnost $d_H(\mathbf{x}, \mathbf{y}) = d_H(\mathbf{x} - \mathbf{y}, \mathbf{o}) = w_H(\mathbf{x} - \mathbf{y})$. ■

Perfektní lineární kódy

Odpřednesenou látku naleznete v dodatku I skript *Abstraktní a konkrétní lineární algebra*.

Minulé přednášky

1. Detekce a oprava chyb v lineárních kódech.
2. Hammingův $(7, 4)$-kód.

Dnešní přednáška

1. Kódy perfektní pro opravu t chyb.
2. Obecné Hammingovy kódy.
3. Jako aplikaci teorie kódů vyřešíme Hat Problem (nepovinné).

Další možné doplňující informace

1. J. Adámek, *Foundations of coding*, John Wiley & Sons, 1991
2. D. J. C. MacKay, *Information theory, inference and learning algorithms*, Cambridge Univ. Press, 2003

Definice (perfektní kód pro t chyb)

Řekneme, že lineární kód W délky n nad $\mathbb{Z}_p$ je perfektní pro t chyb, pokud pro každé $\mathbf{v}$ ze $(\mathbb{Z}_p)^n$ existuje právě jedno $\mathbf{w}$ z W tak, že $d_H(\mathbf{w}, \mathbf{v}) \leq t$.

Poznámky

1. Kód W je perfektní pro t chyb právě tehdy, když platí
$$(\mathbb{Z}_p)^n = \bigcup_{\mathbf{w} \in W} \mathrm{Ball}_t(\mathbf{w})$$
kde
$$\mathrm{Ball}_t(\mathbf{w}) = \{\mathbf{v} \in (\mathbb{Z}_p)^n \mid d_H(\mathbf{w}, \mathbf{v}) \leq t\}$$
je koule v $(\mathbb{Z}_p)^n$ se středem ve $\mathbf{w}$ a poloměrem t. Toto sjednocení je navíc disjunktní.[a]
Je-li W perfektní pro t chyb, pak $\mathrm{dist}(W) = 2t + 1$. Takže W opravuje t chyb.

[a] Slogan: kód W je perfektní pro t chyb právě tehdy, když $(\mathbb{Z}_p)^n$ lze pokrýt disjunktními koulemi se středy v kódových slovech a poloměrem t.

Poznámky (pokrač.)

2. Počet prvků jedné koule

$$\begin{aligned}\mathrm{Ball}_t(\mathbf{w}) &= \{\mathbf{v} \mid d_H(\mathbf{w},\mathbf{v}) = 0\} \cup \{\mathbf{v} \mid d_H(\mathbf{w},\mathbf{v}) = 1\} \cup \ldots \\ &\quad \cdots \cup \{\mathbf{v} \mid d_H(\mathbf{w},\mathbf{v}) = t-1\} \cup \{\mathbf{v} \mid d_H(\mathbf{w},\mathbf{v}) = t\}\end{aligned}$$

je roven součtu

$$\sum_{i=0}^{t} \underbrace{\binom{n}{i}}_{\substack{\text{výběr}\\ \text{lišících}\\ \text{se posic}}} \cdot \overbrace{(p-1)^i}^{\substack{\text{výběr}\\ \text{lišících}\\ \text{se znaků}}}, \quad \text{kde } \binom{n}{i} = \frac{n!}{i! \cdot (n-i)!}.$$

Poznámky (pokrač.)

3. Kód W je perfektní pro t chyb právě tehdy, když platí rovnost

$$p^n = (\text{počet slov ve } W) \cdot \sum_{i=0}^{t} \binom{n}{i} \cdot (p-1)^i$$

Víme-li navíc, že W má dimensi k, lze tuto rovnost psát jako

$$p^{n-k} = \sum_{i=0}^{t} \binom{n}{i} \cdot (p-1)^i$$

protože takové W obsahuje přesně p^k slov.

4. Pro obecný lineární kód W dimense k opravující t chyb platí pouze nerovnost

$$p^{n-k} \geq \sum_{i=0}^{t} \binom{n}{i} \cdot (p-1)^i$$

které se říká sphere-packing bound.

Poznámky

1. Klasifikace perfektních kódů nad $\mathbb{Z}_p$ existuje, jde však o těžký a hluboký výsledek. Viz například knihu
   - W. C. Huffman a V. Pless, *Fundamentals of error-correcting codes*, Cambridge Univ. Press, 2003
2. Uvidíme příklad třídy kódů, perfektních pro 1 chybu. Jde o třídu takzvaných Hammingových kódů.
3. Vesmírný program NASA používá perfektní kódy pro přenos fotografií z družic.

   Například sondy Voyager 1 a Voyager 2 používaly pro přenos fotografií Jupitera a Saturnu perfektní kód (Golay (24,12,8) code).

Definice (Hammingův kód)

Hammingův kód je kód nad $\mathbb{Z}_2$ délky $n = 2^m - 1$ s kontrolní maticí $\mathbf{H}^T$, která má m řádků a sloupce matice $\mathbf{H}^T$ přesně odpovídají binárním zápisům všech čísel $1, \ldots, 2^m - 1$, kde $m \geq 1$ je přirozené číslo.

Příklady

1. Kontrolní matice Hammingova kódu pro $m = 1$:
$$\mathbf{H}^T = (1)$$
Délka tohoto kódu je 1, dimense 0.[a] Inf. rate $= \frac{0}{1} = 0$.
2. Kontrolní matice Hammingova kódu pro $m = 2$:
$$\mathbf{H}^T = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$
Délka tohoto kódu je 3, dimense 1. Inf. rate $= \frac{1}{3} = 0.33\ldots$

[a] Jde tedy o triviální kód $(\mathbb{Z}_2)^0 = \{\mathbf{o}\}$, který není příliš použitelný.

Příklady (pokrač.)

3. Kontrolní matice Hammingova $(7,4)$-kódu (zde je $m = 3$):

$$\mathbf{H}^T = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

   Délka tohoto kódu je 7, dimense 4. Inf. rate $= \frac{4}{7} = 0.57\ldots$

4. Kontrolní matice Hammingova kódu pro $m = 4$:

$$\mathbf{H}^T = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

   Délka tohoto kódu je 15, dimense 11. Inf. rate $= \frac{11}{15} = 0.73\ldots$

5. Pro obecné $m \geq 1$ je délka příslušného Hammingova kódu $2^m - 1$, dimense je rovna $2^m - 1 - m$ a inf. rate je roven

$$\frac{2^m - 1 - m}{2^m - 1} = 1 - \frac{m}{2^m - 1}$$

Tvrzení

Ať W je Hammingův kód délky $n = 2^m - 1$, $m \geq 2$. Potom W je perfektní pro 1 chybu.

Důkaz.

Chceme ukázat rovnost

$$p^{n-k} = \sum_{i=0}^{t} \binom{n}{i} \cdot (p-1)^i$$

kde $p = 2$, $t = 1$, $n = 2^m - 1$ a $k = 2^m - 1 - m$.
Opravdu, platí:

$$\underbrace{\binom{2^m - 1}{0}}_{=1} + \underbrace{\binom{2^m - 1}{1}}_{=2^m-1} = 1 + 2^m - 1 = 2^m = 2^{n-k}$$

The Hat Problem (Todd Ebert, 1998)

Skupina vězňů hraje následující hru o svobodu:

1. Každý vězeň dostane buď černý nebo bílý klobouk (klobouky se rozdávájí náhodně s pravděpodobností 1/2).
2. Každý vidí barvy klobouků ostatních, barvu svého klobouku nevidí nikdo.
3. Skupina hraje jako tým. Vyhrají, pokud alespoň jeden uhodne správně barvu svého klobouku a nikdo ze skupiny nehádá špatně.
4. Před začátkem hry se vězni na strategii domlouvat mohou, po začátku hry spolu komunikovat nesmí.

Simple-minded strategie: hádejme náhodně, pravděpodobnost výhry je pak 1/2.

Existuje stategie lepší?

Ano: je-li $m \geq 2$, pak pro skupinu $n = 2^m - 1$ vězňů pomůže příslušný Hammingův kód.

Optimální vyhrávací strategie pro Hat Problem

Označme jako W Hammingův kód délky $n = 2^m - 1$, kde $m \geq 2$. Slova $\mathbf{v}$ ze $(\mathbb{Z}_2)^n$ budeme považovat za distribuci klobouků:

1. 0 v i-té položce slova $\mathbf{v}$ znamená: vězeň i má černý klobouk.
2. 1 v i-té položce slova $\mathbf{v}$ znamená: vězeň i má bílý klobouk.

Pro zadanou distribuci $\mathbf{v}$ definujme slovo $\mathbf{v}_i$ jako distribuci, která má shodné položky se slovem $\mathbf{v}$, kromě i-té položky, kde je 0.[a] Platí rovnost $\mathbf{v} = \mathbf{v}_i + a_i\mathbf{e}_i$, kde $a_i \in \mathbb{Z}_2$ je pevné.

Strategie i-tého vězně:

1. Jesliže $\mathbf{v}_i + b_i\mathbf{e}_i \notin W$ pro jakékoli b_i ze $\mathbb{Z}_2$, vězeň i mlčí.
2. Jesliže $\mathbf{v}_i + b_i\mathbf{e}_i \in W$ pro nějaké b_i ze $\mathbb{Z}_2$, vězeň i prohlásí, že má klobouk barvy $1 + b_i$.

[a] Slovo $\mathbf{v}_i$ je tedy definováno jako distribuce, kterou i-tý vězeň skutečně vidí a který předpokládá, že má černý klobouk.

Optimální vyhrávací strategie pro Hat Problem (pokrač.)

Strategie je dobře definovaná: nemůže současně platit $\mathbf{v}_i + 0 \cdot \mathbf{e}_i \in W$ a $\mathbf{v}_i + 1 \cdot \mathbf{e}_i \in W$.

Kdyby platilo $\mathbf{v}_i + 0 \cdot \mathbf{e}_i \in W$ a $\mathbf{v}_i + 1 \cdot \mathbf{e}_i \in W$, pak součet $(\mathbf{v}_i + 0 \cdot \mathbf{e}_i) + (\mathbf{v}_i + 1 \cdot \mathbf{e}_i) = \mathbf{e}_i$ leží ve W. To není možné, protože syndrom $\mathbf{e}_i$ je i-tý sloupec kontrolní matice $\mathbf{H}^T$ a ten je nenulový.[a]

1. Jestliže $\mathbf{v}$ není ve W, strategie dává vítězství.

   Pokud $\mathbf{v}$ není ve W, existuje jediné j tak, že $\mathbf{v} + \mathbf{e}_j$ je ve W. Hammingův kód je totiž perfektní pro 1 chybu. Vězeň j tedy správně uhodl barvu svého klobouku. Navíc všichni ostatní vězni museli mlčet: pro $i \neq j$ by v opačném případě muselo platit $\mathbf{v}_i + b_i \mathbf{e}_i \in W$ pro nějaké b_i.

[a] Připomenutí: kontrolní matice Hammingova kódu má ve sloupcích binární zápisy nenulových čísel $1, \ldots, 2^m - 1$.

Optimální vyhrávací strategie pro Hat Problem (pokrač.)

Protože $\mathbf{v} + \mathbf{e}_j = \mathbf{v}_i + a_i\mathbf{e}_i + \mathbf{e}_j \in W$ a $\mathbf{v}_i + b_i\mathbf{e}_i \in W$, platí $(\mathbf{v}_i + a_i\mathbf{e}_i + \mathbf{e}_j) + (\mathbf{v}_i + b_i\mathbf{e}_i) = (a_i + b_i)\mathbf{e}_i + \mathbf{e}_j \in W$.

Syndrom slova $(a_i + b_i)\mathbf{e}_i + \mathbf{e}_j$ je ale nenulový, to je spor.

2. Jestliže $\mathbf{v}$ je ve W, každý hádá špatně.

   Opravdu: pro každé i platí $\mathbf{v} = \mathbf{v}_i + a_i\mathbf{e}_i \in W$ a i-tý vězeň tedy prohlásí, že má klobouk barvy $1 + a_i$, ačkoli má ve skutečnosti klobouk barvy a_i.

Optimální vyhrávací strategie pro Hat Problem (pokrač.)

To znamená, že pravděpodobnost výhry při této strategii je přesně

$$1 - \frac{\text{počet slov ve } W}{\text{počet slov v } (\mathbb{Z}_2)^n} = 1 - \frac{2^{2^m-1-m}}{2^{2^m-1}} = 1 - \frac{1}{2^m}$$

1. Například pro $m = 2$ (tedy pro skupinu $n = 2^2 - 1 = 3$ vězňů) je pravděpodobnost výhry $3/4 = 0.75$.[a]
2. Pro $m = 3$ (tj. pro $n = 2^3 - 1 = 7$ vězňů) je pravděpodobnost výhry $7/8 = 0.875$.
3. Pro $m = 4$ (tj. pro $n = 2^4 - 1 = 15$ vězňů) je pravděpodobnost výhry $15/16 = 0.9375$.
4. Pro $m = 5$ (tj. pro $n = 2^5 - 1 = 31$ vězňů) je pravděpodobnost výhry $31/32 = 0.96875$.
5. Atd.

To je vždy lepší výsledek než simple-minded strategie (která dává vždy pravděpodobnost 1/2).

[a] Je užitečným cvičením si optimální strategii pro $m = 2$ vyzkoušet.

Důležité upozornění

V teorii lineárních kódů je zvykem psát vektory z $\mathbb{F}^n$ do řádku (na rozdíl od B6B01LAG). Co tím ztrácíme a co tím získáváme?

1. Vycvičeni dosavadním průběhem této přednášky, ztrácíme okamžitý geometrický přehled o tom, co se při kódování skutečně děje.
   Pro zájemce: ve skutečnosti geometrický přehled neztrácíme; pracujeme jen s kovektory místo s vektory, viz kapitolu 3.5 skript.
   To znamená, že kódování má jasnou geometrickou interpretaci v duálním prostoru.
2. Získáváme kompatibilitu s rozsáhlou literaturou o kódování.

Protože nám šlo jen o velmi krátký úvod do lineárních kódů, psali jsme vektory nadále do sloupců. Kdo bude číst jinou literaturu z kódování, bude velmi pravděpodobně muset všechny matice a maticové rovnice z teorie kódů transponovat.

Která lineární algebra je tedy ta „správná“?

1. Psaní vektorů z $\mathbb{F}^n$ do sloupců nám umožnilo chápat součin $\mathbf{A} \cdot \mathbf{x}$ jako funkční hodnotu lineárního zobrazení $\mathbf{A}$ v bodě $\mathbf{x}$. Chápání součinu $\mathbf{A} \cdot \mathbf{x}$ jako funkční hodnoty vedlo k přirozené geometrické interpretaci maticových výpočtů.

   To je ve shodě s tím, jak značíme funkční hodnoty ve zbytku matematiky: značku $f(x)$ chápeme jako funkční hodnotu funkce f v bodě x.

2. Při psaní vektorů z $\mathbb{F}^n$ do řádku bychom museli hodnotu lineárního zobrazení $\mathbf{A}$ v bodě $\mathbf{x}$ značit $\mathbf{x} \cdot \mathbf{A}$.

   Tento způsob uvažování o maticovém součinu je ve shodě s (menšinovým) názorem, že funkční hodnotu funkce f v bodě x bychom měli značit $(x)f$. Takovému značení funkčních hodnot se říká reverse Polish notation (RPN).

Proč jsme v přednášce zvolili „sloupcovou“ lineární algebru?

1. Protože na RPN nejsme zvyklí, zvolili jsme „sloupcovou“ lineární algebru. Je totiž ve shodě s tím, jak uvažujeme ve zbytku matematiky.
2. „Řádková“ lineární algebra navíc není ve svém značení úplně důsledná. Dochází tak k absurditám:[a] například soustava rovnic
$$\left(\begin{array}{cc|c} 2 & -1 & 3 \\ 4 & 7 & 11 \end{array}\right)$$
ze „sloupcové“ lineární algebry by se v „řádkové“ lineární algebře měla správně zapisovat
$$\left(\begin{array}{cc} 2 & 4 \\ -1 & 7 \\ \hline 3 & 11 \end{array}\right)$$
ale neděje se tak. „Řádková“ lineární algebra pro soustavy rovnic přebírá zápis „sloupcové“ lineární algebry!

[a] Vzpomeňte si, kolikrát se v textech z „řádkové“ lineární algebry objevuje rčení: „*. . . jednotlivé vektory nyní napíšeme do sloupců matice. . .*“

Závěrečné poznámky

1. Poslední čtyři přednášky byly pouze nahlédnutím do teorie kódů.
2. Skutečné studium teorie kódů vyžaduje zvládnutí dalších partií matematiky:
   1. Teorie informace.
   2. Teorie pravděpodobnosti.
   3. Teorie grup.
   4. A dalších...

   Více se lze dozvědět v doporučené (tj. nepovinné) literatuře.