Text k přednášce z Lineární algebry I a II

Milan Hladík

19. ledna 2012

Toto je stručný text k přednáškám Lineární algebra I a II pro první ročník studia informatiky na Matematicko-fyzikální fakultě Univerzity Karlovy v Praze. Slouží jako doplněk ke studiu, rozhodně však není plnohodnotnou učebnicí.

Tento text vznikl mj. i proto, že žádná současná učebnice nekopíruje přesně sylabus přednášky. Nejblíže je [Tůma, 2003], pěkná skripta jsou [Rohn, 2004], kniha [Bečvář, 2005], nebo matematičtěji laděná kniha [Bican, 2009]. Anglicky psané knihy, které stojí za doporučení, jsou [Gareth, 2001], [Meyer, 2000], [Strang, 1988]. Na stránkách J. Matouška [Matoušek, 2010] je možno nalézt přibližný podrobný sylabus přednášky, stejně jako „Šestnáct miniatur“, šestnáct aplikací lineární algebry.

Základ tohoto textu jsem začal psát během zimního semestru roku 2010. Děkuji všem, kteří nějakým způsobem pomohli k vylepšení textu. Jmenovitě, za opravy chyb děkuji studentům: Jan Tomášek, Jakub Suchý, Martin Polák, Tomáš Novella, Tomáš Musil, Petr Babička a Antonín Tomeček. Za podnětné připomínky děkuji Jaroslavu Horáčkovi.

Případné připomínky a chyby zasílejte prosím na adresu hladik@kam.mff.cuni.cz.

Obsah

Kapitola 1

Úvod

Zde si připomeneme některé poznatky, které by čtenář měl znát, anebo jsou mimo hlavní proud tohoto textu, ale nějak se ho dotýkají.

1.1 Polynomy

Reálným polynomem stupně n je funkce $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, kde $a_0, \ldots, a_n \in \mathbb{R}$ a $a_n \neq 0$. Kromě reálných polynomů můžeme uvažovat polynomy s komplexními koeficienty, popř. nad jinými číselnými obory (o tom až později).

Polynomy můžeme sčítat, odčítat, násobit a dělit se zbytkem. Buďte $p(x) = a_n x^n + \cdots + a_1 x + a_0$, $q(x) = b_m x^m + \cdots + b_1 x + b_0$ dva polynomy a nechť bez újmy na obecnosti $n \geq n$. Pak máme operace

- Sčítání:

$$p(x) + q(x) = a_n x^n + \cdots + a_{m+1}x^{m+1} + (a_m + b_m)x^m + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

- Násobení:

$$p(x)q(x) = a_n b_m x^{n+m} + \cdots + (a_k b_0 + a_{k-1}b_1 + \cdots + a_0 b_k)x^k + \cdots + a_0 b_0,$$

  kde a_k pro $k > n$ a b_k pro $k > m$ definujeme jako 0.

- Dělení se zbytkem: Existuje polynom $r(x)$ stupně $n - m$ a polynom $s(x)$ stupně menšího než m tak, že $p(x) = r(x)q(x) + s(x)$. Zde $r(x)$ představuje podíl a $s(x)$ zbytek.

Kořeny

Kořen polynomu $p(x)$ je taková hodnota $x^* \in \mathbb{R}$, že $p(x^*) = 0$. Například, $p(x) = x^2 - 1$ má kořeny 1 a -1. Polynom $p(x) = x^2 + 1$ nemá reálný kořen, ale má dva komplexní, i a $-i$. Gaussova základní věta algebry z roku 1799 říká, že aspoň jeden kořen vždy existuje.

Věta 1.1 (Základní věta algebry)**.** *Každý polynom s komplexními koeficienty má alespoň jeden komplexní kořen.*

Důkaz. Důkazů existuje celá řada a žádný není zcela elementární. Myšlenkově snadno uchopitelný je důkaz autorů Melane & Birkhof a základní idea je následující. Uvažujme obraz kružnice v komplexní rovině se středem v počátku a poloměrem r při zobrazení $x \mapsto p(x)$. Je-li r hodně blízko nuly, je obrazem uzavřená křivka kolem bodu a_0. Naopak, je-li r dost velké, pak $p(x) \approx a_n x^n$ a obrazem křivka probíhající přibližně kolem kružnice se středem v počátku a poloměrem $a_n r^n$. Postupným spojitým zvětšováním r od nuly nakonec musí někde obraz protnout počátek, což odpovídá kořenu. □

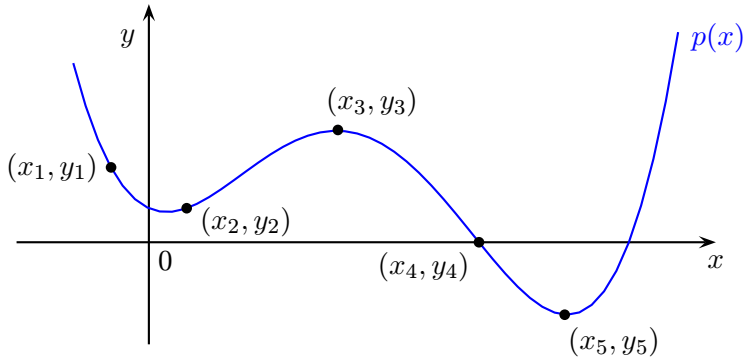
Je-li x_1 kořen polynomu $p(x)$, pak $p(x)$ je dělitelný $(x - x_1)$ beze zbytku a podíl je polynom stupně $n - 1$. Ten má podle základní věty algebry kořen x_2, opět můžeme beze zbytku dělit $x - x_2$ atd. až snížíme stupeň polynomu na nulu. Každý polynom tudíž lze zapsat jako $p(x) = a_n(x - x_1)\ldots(x - x_n)$,

kde $x_1, \ldots, x_n$ jsou jeho kořeny. Dalším důsledkem je, že polynom stupně n má právě n kořenů, pokud započítáváme i násobnosti.

Nyní víme, že každý polynom má kořen, ale zatím není jasné jak ho určit. Kořeny polynomů druhého stupně snadno najdeme podle známého vzorečku $x_{1,2} = \frac{1}{2a_2}(-a_1 \pm \sqrt{a_1^2 - 4a_2a_0})$. Pro kořeny polynomu třetího stupně existují také vzorce, tzv. Cardanovy, ale již mnohem komplikovanější. Důležitým zjištěním bylo, když roku 1824 přišel Abel na veřejnost s tím, že pro polynomy stupňů vyšších než 4 obecně žádný vzoreček na výpočet kořenů nemůže existovat. Veškeré praktické metody jsou tedy pouze iterační, kdy kořeny pouze aproximujeme, ale v jistém iteračním procesu aproximaci vylepšujeme na libovolnou přesnost.

Interpolace

Polynomy mají široké použití a najdeme je v mnoha situacích. Jedno využití je při interpolaci bodů. Mějme v rovině $n+1$ bodů $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)$, kde $x_i \neq x_j$ pro $i \neq j$. Cílem je najít polynom $p(x)$ procházející těmito body. Následující věta dává explicitní vyjádření hledaného polynomu, i když ne přímo v základním tvaru. Více v Sekci 3.6.



Věta 1.2 (Lagrangeův interpolační polynom)**.** *Body prochází polynom* $p(x) = \sum_{j=0}^{n} y_j p_j(x)$*, kde* $p_j(x) = \prod_{i=0, i\neq j}^{n} \frac{1}{x_j - x_i}(x - x_i)$.

Důkaz. Stačí dosadit jednotlivé body a ukázat rovnost $p(x_k) = y_k$, $k = 0, 1, \ldots, n$. Ta platí, protože $p_j(x_k) = 1$ pro $j = k$, a $p_j(x_k) = 0$ pro $j \neq k$. □

Kapitola 2

Soustavy rovnic

2.1 Základní pojmy

Soustavy lineárních rovnic patří mezi základní (algebraické) úlohy a setkáme se s nimi skoro všude – pokud nějaký problém nevede na soustavu rovnic přímo, tak se často objeví jako podproblém.

Příklad 2.1 ([Meyer, 2000])**.** Nejstarší zaznamenaná úloha na soustavy rovnic: čínská kniha Chiu-chang Suan-shu (ca 200 př.n.l.):

> *Tři snopy dobrého obilí, dva snopy průměrného a jeden podřadného se prodávají celkem za 39 dou. Dva snopy dobrého obilí, tři průměrného a jeden podřadného se prodávají za 34 dou. Jeden snop dobrého obilí, dva průměrného a tři podřadného se prodávají za 26 dou. Jaká je cena za jeden snop dobrého / průměrného / podřadného obilí?*

Zapsáno dnešní matematikou, dostáváme soustavu rovnic

$$\begin{aligned} 3x + 2y + z &= 39, \\ 2x + 3y + z &= 34, \\ x + 2y + 3z &= 26, \end{aligned}$$

kde x, y, z jsou neznámé pro ceny za jeden snop dobrého / průměrného / podřadného obilí. □

Soustavy rovnic budeme zapisovat maticově, proto si nejprve zavedeme pojem *matice*.

Definice 2.2 (Matice)**.** Reálná *matice* typu $m \times n$ je obdélníkové schema

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Prvek na pozici (i, j) matice A značíme: a_{ij} nebo A_{ij}.
Množinu všech reálných matic typu $m \times n$ značíme $\mathbb{R}^{m \times n}$; podobně pro komplexní, racionální, atd.
Je-li $m = n$, potom matici nazýváme *čtvercovou*.

Definice 2.3 (Vektor)**.** Reálný n-rozměrný (aritmetický) *vektor* je matice typu $n \times 1$

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Množina všech n-rozměrných vektorů se značí $\mathbb{R}^n$ (namísto $\mathbb{R}^{n \times 1}$).

Definice 2.4 ($*$ notace)**.**
i-tý řádek matice A se značí: $A_{i*} = (a_{i1}, a_{i2}, \ldots, a_{in})$.
j-tý sloupec matice A se značí: $A_{*j} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \ldots \\ a_{nj} \end{pmatrix}$.

Definice 2.5 (Soustava lineárních rovnic)**.** Mějme soustavu m lineárních rovnic o n neznámých

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2, \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m. \end{aligned} \tag{2.1}$$

Pak zavedeme následující pojmy: *Řešením* rozumíme každý vektor x vyhovující všem rovnicím. *Matice soustavy* je matice

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

a *rozšířená matice soustavy* je

$$(A \mid b) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{array}\right).$$

Poznamenejme, že rozšířená matice soustavy plně popisuje soustavu rovnic; řádky odpovídají rovnicím a sloupce nalevo proměnným.

Poznámka 2.6 (Geometrický význam soustavy rovnic)**.** Pro jednoduchost uvažujme nejprve případ $m = n = 2$, tedy dvě rovnice o dvou neznámých

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 &= b_1, \\ a_{21}x_1 + a_{22}x_2 &= b_2. \end{aligned}$$

První rovnice popisuje přímku v $\mathbb{R}^2$, druhá také. Řešení soustavy leží tedy v průniku obou přímek. Podobně pro $n = 3$, každá rovnice popisuje rovinu v prostoru $\mathbb{R}^3$ a řešení představuje průnik těchto rovin. Obecně pro libovolné n, rovnice určují tzv. nadroviny (srov. kapitola 7) řešení soustavy hledáme v jejich průniku.

Definice 2.7 (Elementární řádkové úpravy)**.** Elementární řádkové úpravy jsou

1. vynásobení i-tého řádku číslem $\alpha \neq 0$ (tj. vynásobí se všechny prvky řádku),
2. přičtení α-násobku j-tého řádku k i-tému, přičemž $i \neq j$,
3. výměna i-tého a j-tého řádku.

Poznámka 2.8. Ve skutečnosti výše zmíněné úpravy nejsou zas tak elementární. U druhé řádkové úpravy si vystačíme jen s $\alpha = 1$ a třetí úprava lze simulovat pomocí předchozích dvou (zkuste si to!).

Věta 2.9. *Elementární řádkové operace zachovávají množinu řešení soustavy.*

Důkaz. Triviální. □

2.2 Gaussova eliminace

Nyní se přesuňme k tomu jak soustavy rovnic řešit. Ukážeme si dvě metody, jejichž základem je transformace rozšířené matice soustavy pomocí elementárních úprav na jednodušší matici, ze které řešení snadno vyčteme. Ten jednodušší tvar matice se nazývá *odstupňovaný tvar matice*, v angličtině „row echelon form“ (REF).

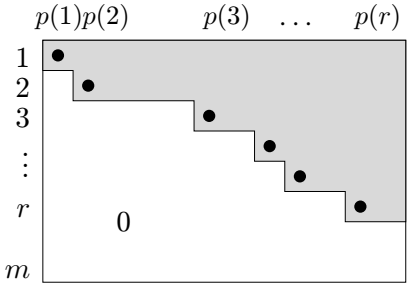
Definice 2.10 (Odstupňovaný tvar matice)**.** Matice $A \in \mathbb{R}^{m\times n}$ je v řádkově odstupňovaném tvaru pokud existuje r takové, že platí

- řádky $1, \dots, r$ jsou nenulové (tj. každý obsahuje aspoň jednu nenulovou hodnotu),
- řádky $r+1, \dots, m$ jsou nulové,

a navíc označíme-li $p(i) = \min\{j;\, a_{ij} \neq 0\}$, tak platí

- $p(1) < p(2) < \cdots < p(r)$.

K odstupňovanému tvaru se vztahují některé zásadní pojmy: Pozice $(1, p(1))$, $(2, p(2))$, $\dots$, $(r, p(r))$ se nazývají *pivoty*, sloupce $p(1)$, $p(2)$, $\dots p(r)$ se nazývají *bázické* a ostatní sloupce *nebázické* (význam bude zřejmý později).



Schematické znázornění odstupňovaného tvaru. Pivoty jsou pozice černých teček.

Každou matici lze převést elementárními řádkovými úpravami do odstupňovaného tvaru. *Hodností* matice A rozumíme počet nenulových řádků po převodu do odstupňovaného tvaru (tj. číslo r) a značíme $\operatorname{rank}(A)$. I když odstupňovaný tvar není jednoznačný, pozice pivotů jednoznačné jsou (ukážeme si později ve Větě 3.34). Proto je pojem hodnosti dobře definován.

Následující algoritmus převede matici do odstupňovaného tvaru; důkaz správnosti se udělá matematickou indukcí podle počtu sloupců a rozborem. Pochopitelně, existují i různé varianty.

Algoritmus 2.11 (REF(A))**.** Buď $A \in \mathbb{R}^{m\times n}$.

1: $i := 1$, $j := 1$,
2: **if** $a_{kl} = 0$ pro všechna $k \geq i$ a $l \geq j$ **then** konec,
3: $j := \min\{l;\, l \geq j,\ a_{kl} \neq 0$ pro nějaké $k \geq i\}$, //přeskočíme nulové podsloupečky
4: urči $a_{kj} \neq 0$, $k \geq i$ a vyměň řádky A_{i*} a A_{k*}, //nyní je na pozici pivota hodnota $a_{ij} \neq 0$
5: pro všechna $k > i$ polož $A_{k*} := A_{k*} - \frac{a_{kj}}{a_{ij}} A_{i*}$, //2. elementární úprava
6: polož $i := i+1$, $j := j+1$, a jdi na krok 2.

Algoritmus skončí po nejvýše $\min(m, n)$ iteracích hlavního cyklu. Celkem neurčitě jsme definovali index k v kroku 4. Teoreticky si můžeme zvolit libovolně, v praxi se doporučuje kandidát s maximální absolutní hodnotou, tzv. *parciální pivotizace*, protože je stabilnější.

Příklad 2.12. Ukázka převodu matice na odstupňovaný tvar

$$\begin{pmatrix} \textcircled{2} & 2 & -1 & 5 \\ 4 & 5 & 0 & 9 \\ 0 & 1 & 2 & 2 \\ 2 & 4 & 3 & 7 \end{pmatrix} \sim \begin{pmatrix} \textcircled{2} & 2 & -1 & 5 \\ 0 & 1 & 2 & -1 \\ 0 & 1 & 2 & 2 \\ 2 & 4 & 3 & 7 \end{pmatrix} \sim \begin{pmatrix} 2 & 2 & -1 & 5 \\ 0 & \textcircled{1} & 2 & -1 \\ 0 & 1 & 2 & 2 \\ 0 & 2 & 4 & 2 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 2 & 2 & -1 & 5 \\ 0 & \textcircled{1} & 2 & -1 \\ 0 & 0 & 0 & 3 \\ 0 & 2 & 4 & 2 \end{pmatrix} \sim \begin{pmatrix} 2 & 2 & -1 & 5 \\ 0 & 1 & 2 & -1 \\ 0 & 0 & 0 & \textcircled{3} \\ 0 & 0 & 0 & 4 \end{pmatrix} \sim \begin{pmatrix} 2 & 2 & -1 & 5 \\ 0 & 1 & 2 & -1 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

□

Teď už máme vše připraveno na Gaussovu eliminaci.

Algoritmus 2.13 (Gaussova eliminace[1])**.** Buď dána soustava rovnic $(A \mid b)$. Převeď ji na odstupňovaný tvar $(A' \mid b')$. Rozlišme tři situace:

(A) Poslední sloupec je bázický (tj. $\operatorname{rank}(A) < \operatorname{rank}(A \mid b)$)

V tomto případě soustava nemá řešení: Označme $r = \operatorname{rank}(A \mid b)$, pak r-tý řádek soustavy (v REF tvaru) má tvar

$$0x_1 + 0x_2 + \ldots 0x_n = b'_r.$$

Vzhledem k tomu, že $b'_r \neq 0$, neboť je to pivot, soustava nemůže mít řešení.

(B) Poslední sloupec je nebázický (tj. $\operatorname{rank}(A) = \operatorname{rank}(A' \mid b')$).

V tomto případě soustava má aspoň jedno řešení. Jestli má jediné, nebo nekonečně mnoho rozlišíme dole. Používáme značení $r = \operatorname{rank}(A' \mid b')$.

(B1) Nechť $r = n$. Potom existuje jediné řešení, které najdeme tzv. *zpětnou substitucí*:

$$\textbf{for } k = n \textbf{ down to } 1 \textbf{ do } x_k \coloneqq \frac{b'_k - \sum_{j=k+1}^{n} a'_{kj} x_j}{a'_{kk}}$$

Důkaz. Soustava v odstupňovaném tvaru má rovnicovou podobu

$$\begin{aligned} a'_{11}x_1 + a'_{12}x_2 + \ldots + a'_{1n}x_n &= b'_1, \\ a'_{22}x_2 + \ldots + a'_{2n}x_n &= b'_2, \\ &\vdots \\ a'_{kk}x_k + \ldots + a'_{kn}x_n &= b'_k, \\ &\vdots \\ a'_{nn}x_n &= b'_n \end{aligned}$$

(popřípadě ještě nějaké rovnice typu $0x_1 + \ldots + 0x_n = 0$, které lze vynechat). Hodnotu neznámé x_n spočítáme z poslední rovnice, tu dosadíme do předposlední a dopočítáme x_{n-1} atd. až nakonec spočítáme hodnotu x_1. Máme tedy jediné řešení, které je dobře definované, neboť $a_{kk} \neq 0$. □

(B2) Nechť $r < n$. Potom existuje nekonečně mnoho řešení[2], které popíšeme parametricky. Jako *bázické proměnné* si označme ty, které odpovídají bázickým sloupcům, tj. $x_{p(1)}, x_{p(2)}, \ldots, x_{p(r)}$, a jako *nebázické proměnné* ty zbývající. Potom nebázické proměnné budou parametry, které mohou nabývat libovolnou reálnou hodnotu a pomocí nich dopočítáme bázické proměnné opět zpětnou substitucí:

$$\textbf{for } k = r \textbf{ down to } 1 \textbf{ do } x_{p(k)} \coloneqq \frac{b'_{p(k)} - \sum_{j=p(k)+1}^{n} a'_{kj} x_j}{a'_{kp(k)}}.$$

Příklad 2.14. Vyřešme Gaussovou eliminací následující soustavu. Nejprve převedeme rozšířenou matici soustavy na odstupňovaný tvar

$$\left(\begin{array}{cccc|c} 2 & 2 & -1 & 5 & 1 \\ 4 & 5 & 0 & 9 & 3 \\ 0 & 1 & 2 & 2 & 4 \\ 2 & 4 & 3 & 7 & 7 \end{array}\right) \underset{\sim}{REF} \left(\begin{array}{cccc|c} 2 & 2 & -1 & 5 & 1 \\ 0 & 1 & 2 & -1 & 1 \\ 0 & 0 & 0 & 3 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Zpětná substituce:

[1] Carl Friedrich Gauss, z r. 1810.

[2] Toto platí pokud pracujeme nad reálnými čísly. Nad konečnými tělesy (sekce 4.3) se postupuje stejně, ale počet řešení bude konečný.

1. $x_4 = 1$
2. x_3 je volná (nebázická) proměnná
3. $x_2 = 1 + x_4 - 2x_3 = 2 - 2x_3$
4. $x_1 = \frac{1}{2}(1 - 5x_4 + x_3 - 2x_2) = -4 + \frac{5}{2}x_3$

Všechna řešení jsou tvaru

$$(-4 + \tfrac{5}{2}x_3, 2 - 2x_3, x_3, 1), \text{ kde } x_3 \in \mathbb{R},$$

resp.

$$(-4, 2, 0, 1) + x_3(\tfrac{5}{2}, -2, 1, 0), \text{ kde } x_3 \in \mathbb{R}.$$

Z posledního vyjádření je patrno, že množina řešení představuje přímku v $\mathbb{R}^4$ se směrnicí $(\frac{5}{2}, -2, 1, 0)$ a procházející bodem $(-4, 2, 0, 1)$. □

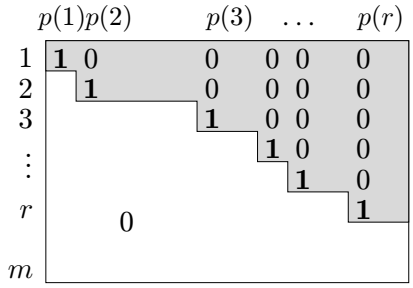
2.3 Gauss–Jordanova eliminace

Druhý algoritmus, který si uvedeme, je Gauss–Jordanova eliminace. Namísto odstupňovaného tvaru používá ještě specifičtější redukovaný odstupňovaný tvar, v angličtině „reduced row echelon form“ (RREF).

Definice 2.15 (Redukovaný odstupňovaný tvar matice)**.** Matice $A \in \mathbb{R}^{m\times n}$ je v redukovaném řádkově odstupňovaném tvaru pokud je v REF tvaru a navíc platí

- $a_{1p(1)} = a_{2p(2)} = \cdots = a_{rp(r)} = 1$,
- pro každé $i = 1, \ldots, r$ je $a_{1p(i)} = a_{2p(i)} = \cdots = a_{i-1,p(i)} = 0$.

Schematické znázornění redukovaného odstupňovaného tvaru. Narozdíl od REF, pivoty jsou navíc znormovány na jedničku a nad nimi jsou samé nuly.



Algoritmus, který převede libovolnou matici do RREF tvaru je podobný tomu pro REF. Jediná změna je v kroku 5, který nahradíme dvěma novými.

Algoritmus 2.16 (RREF(A))**.** Buď $A \in \mathbb{R}^{m\times n}$.

1: $i \coloneqq 1$, $j \coloneqq 1$,

2: **if** $a_{kl} = 0$ pro všechna $k \geq i$ a $l \geq j$ **then** konec,

3: $j \coloneqq \min\{l;\ l \geq j,\ a_{kl} \neq 0$ pro nějaké $k \geq i\}$, //přeskočíme nulové podsloupečky

4: urči $a_{kj} \neq 0$, $k \geq i$ a vyměň řádky A_{i*} a A_{k*}, //nyní je na pozici pivota hodnota $a_{ij} \neq 0$

5: polož $A_{i*} \coloneqq \frac{1}{a_{ij}} A_{i*}$, //nyní je na pozici pivota hodnota $a_{ij} = 1$

6: pro všechna $k \neq i$ polož $A_{k*} \coloneqq A_{k*} - a_{kj}A_{i*}$, //2. elementární úprava

7: polož $i \coloneqq i + 1$, $j \coloneqq j + 1$, a jdi na krok 2.

Příklad 2.17. Ukázka převodu matice na redukovaný odstupňovaný tvar

$$\begin{pmatrix} \textcircled{2} & 2 & -1 & 5 \\ 4 & 5 & 0 & 9 \\ 0 & 1 & 2 & 2 \\ 2 & 4 & 3 & 7 \end{pmatrix} \sim \begin{pmatrix} \textcircled{1} & 1 & -0.5 & 2.5 \\ 4 & 5 & 0 & 9 \\ 0 & 1 & 2 & 2 \\ 2 & 4 & 3 & 7 \end{pmatrix} \sim \begin{pmatrix} \textcircled{1} & 1 & -0.5 & 2.5 \\ 0 & 1 & 2 & -1 \\ 0 & 1 & 2 & 2 \\ 2 & 4 & 3 & 7 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 1 & -0.5 & 2.5 \\ 0 & \textcircled{1} & 2 & -1 \\ 0 & 1 & 2 & 2 \\ 0 & 2 & 4 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -2.5 & 3.5 \\ 0 & \textcircled{1} & 2 & -1 \\ 0 & 1 & 2 & 2 \\ 0 & 2 & 4 & 2 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 0 & -2.5 & 3.5 \\ 0 & \textcircled{1} & 2 & -1 \\ 0 & 0 & 0 & 3 \\ 0 & 2 & 4 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -2.5 & 3.5 \\ 0 & 1 & 2 & -1 \\ 0 & 0 & 0 & \textcircled{3} \\ 0 & 0 & 0 & 4 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 0 & -2.5 & 3.5 \\ 0 & 1 & 2 & -1 \\ 0 & 0 & 0 & \textcircled{1} \\ 0 & 0 & 0 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -2.5 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

□

Gauss–Jordanova eliminace pak funguje následujícím způsobem.

Algoritmus 2.18 (Gauss–Jordanova eliminace[3])**.** Buď dána soustava rovnic $(A \mid b)$. Převeď ji na redukovaný odstupňovaný tvar $(A' \mid b')$. Rozlišme tři situace:

(A) Poslední sloupec je bázický (tj. $\operatorname{rank}(A) < \operatorname{rank}(A \mid b)$)

V tomto případě soustava nemá řešení, důkaz analogický.

(B) Poslední sloupec je nebázický a $r = n$. Potom existuje jediné řešení, a to $(x_1, \ldots, x_n) = (b'_1, \ldots, b'_n)$.

Důkaz. Soustava v RREF tvaru má rovnicovou podobu

$$\begin{aligned} x_1 &= b'_1, \\ x_2 &= b'_2, \\ &\vdots \\ x_n &= b'_n \end{aligned}$$

(opět tam mohou být ještě nějaké rovnice typu $0x_1 + \ldots + 0x_n = 0$, které nemusíme uvažovat). Rovnice nám přímo určují řešení. □

(B2) Poslední sloupec je nebázický a $r < n$. Potom existuje nekonečně mnoho řešení, které popíšeme parametricky. Označme si nebázické proměnné x_i, $i \in N$, kde $N = \{1, \ldots, n\} \setminus \{p(1), \ldots, p(r)\}$. Opět, nebázické proměnné budou parametry, které mohou nabývat libovolnou reálnou hodnotu a pomocí nich dopočítáme bázické proměnné opět zpětnou substitucí:

$$\textbf{for } k = r \textbf{ down to } 1 \textbf{ do } x_{p(k)} := b'_{p(k)} - \sum_{j \in N, j > p(k)} a'_{kj} x_j.$$

Poznámka 2.19 (Frobeniova věta)**.** Při odvozování Gaussovy a Gauss-Jordanovy eliminace jsme jako důsledek dostali důležitou větu lineární algebry nazývanou Frobeniova věta[4]:

[3] Wilhelm Jordan, z r. 1887.

[4] V angličtině větu nazývají Rouché–Capelliho věta, v Rusku Kronecker–Capelliho věta a ve Španělsku Rouché–Frobeniova věta. Můžete se setkat i s názvem Rouché-Fonteného věta. Inu, jiný kraj, jiný mrav.

Soustava $(A \mid b)$ má (aspoň jedno) řešení právě tehdy když $\operatorname{rank}(A) = \operatorname{rank}(A \mid b)$.

Později, v kapitole věnované vektorovým prostorům k tomu získáme ještě jiný náhled.

Poznámka 2.20 (Gaussova versus Gauss-Jordanova eliminace)**.** Čtenář se může ptát, proč jsme si uváděli dvě poměrně podobné metody na řešeni soustav rovnic. Gaussova eliminace má výhodu v tom, že je ca o 50% rychlejší než ta druhá, na druhou stranu Gauss-Jordanovu eliminaci (či spíše RREF tvar) budeme potřebovat při invertování matic (sekce 3.3).

Kapitola 3

Matice

3.1 Základní operace s maticemi

Definice 3.1 (Rovnost)**.** Dvě matice se rovnají, $A = B$, pokud mají stejné rozměry $m \times n$ a $A_{ij} = B_{ij}$ pro všechna i, j.

Definice 3.2 (Součet)**.** Buď $A, B \in \mathbb{R}^{m\times n}$. Pak $A+B$ je matice typu $m\times n$ s prvky $(A+B)_{ij} = A_{ij}+B_{ij}$.

Definice 3.3 (Násobek)**.** Buď $\alpha \in \mathbb{R}$ a $A \in \mathbb{R}^{m\times n}$. Pak αA je matice typu $m \times n$ s prvky $(\alpha A)_{ij} = \alpha A_{ij}$.

Výše zmíněné operace umožňují zavést přirozeně i odčítání jako $A - B := A + (-1)B$.

Speciální maticí je nulová matice, jejíž všechny prvky jsou nuly. Značíme ji 0 či $0_{m\times n}$ pro zdůraznění rozměru.

Věta 3.4 (Vlastnosti součtu a násobků matic)**.** *Platí následující vlastnosti; α, β jsou čísla a A, B, C matice vhodných rozměrů.*

(1) $A + B = B + A$ *... (komutativita)*
(2) $(A + B) + C = A + (B + C)$ *... (asociativita)*
(3) $A + 0 = A$
(4) $A + (-1)A = 0$
(5) $\alpha(\beta A) = (\alpha\beta)A$
(6) $1A = A$
(7) $\alpha(A + B) = \alpha A + \alpha B$ *... (distributivita)*
(8) $(\alpha + \beta)A = \alpha A + \beta A$ *... (distributivita)*

Důkaz. Důkaz vlastností je vesměs triviální, ale je vhodný pro procvičení formálního přístupu. Základní idea důkazů je redukce dané vlastnosti na odpovídající vlastnost reálných čísel. Dokážeme vlastnost (1), zbytek necháváme čtenáři.

(1) Nejprve ověříme, že $A + B$ i $B + A$ mají stejný typ. Pak ukážeme $(A + B)_{ij} = A_{ij} + B_{ij} = B_{ij} + A_{ij} = (B + A)_{ij}$, tedy odpovídající si prvky jsou shodné. □

Násobení matic je definováno na první pohled trochu neobvykle.

Definice 3.5 (Součin)**.** Buď $A \in \mathbb{R}^{m\times p}$ a $B \in \mathbb{R}^{p\times n}$. Pak AB je matice typu $m \times n$ s prvky $(AB)_{ij} = \sum_{k=1}^{p} A_{ik}B_{kj}$.

Příklad 3.6 (Násobení matic)**.** Buď

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 0 & 1 \\ 2 & 2 & 2 & 2 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 2 & 2 \\ 1 & 2 & 1 & 3 \\ 1 & 2 & 1 & 0 \end{pmatrix}.$$

Mnemotechnická pomůcka pro násobení matic AB:

$$\begin{array}{c|c} & \begin{pmatrix} 1 & 1 & \mathbf{1} & 1 \\ 1 & 0 & \mathbf{2} & 2 \\ 1 & 2 & \mathbf{1} & 3 \\ 1 & 2 & \mathbf{1} & 0 \end{pmatrix} \\ \hline \begin{pmatrix} 1 & 2 & 3 & 4 \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ 2 & 2 & 2 & 2 \end{pmatrix} & \begin{pmatrix} 10 & 15 & 12 & 14 \\ 2 & 2 & \textcircled{\mathbf{3}} & 2 \\ 8 & 10 & 10 & 12 \end{pmatrix} \end{array}$$

□

Důležitou maticí je *jednotková matice*. Značí se I či I_n a je to čtvercová matice řádu n s prvky $I_{ij} = 1$ pro $i = j$ a $I_{ij} = 0$ jinak. Je to tedy matice s jedničkami na diagonále a s nulami jinde. *Jednotkový vektor* e_i je pak i-tý sloupec jednotkové matice, tj. $e_i = I_{*i}$.

Věta 3.7 (Vlastnosti součinu matic)**.** *Platí následující vlastnosti; α je číslo a A, B, C matice vhodných rozměrů.*

(1) $(AB)C = A(BC)$ *... (asociativita)*
(2) $A(B + C) = AB + AC$ *... (distributivita)*
(3) $(A + B)C = AC + BC$ *... (distributivita)*
(4) $\alpha(AB) = (\alpha A)B = A(\alpha B)$
(5) $I_m A = AI_n = A$, *kde* $A \in \mathbb{R}^{m\times n}$

Důkaz. Opět dokážeme jen vlastnost (1), ostatní necháváme za domácí cvičení.

(1) Buď $A \in \mathbb{R}^{m\times p}$, $B \in \mathbb{R}^{p\times r}$ a $C \in \mathbb{R}^{r\times n}$. Pak AB má typ $m \times r$, BC má typ $p \times n$ a oba součiny $(AB)C$, $A(BC)$ mají typ $m \times n$. Nyní ukážeme, že odpovídající si prvky jsou shodné. Na pozici (i, j) jest

$$((AB)C)_{ij} = \sum_{k=1}^{p} (AB)_{ik}C_{kj} = \sum_{k=1}^{p} \left(\sum_{l=1}^{r} A_{il}B_{lk} \right) C_{kj} = \sum_{k=1}^{p}\sum_{l=1}^{r} A_{il}B_{lk}C_{kj}$$
$$(A(BC))_{ij} = \sum_{l=1}^{r} A_{il}(BC)_{lj} = \sum_{l=1}^{r} A_{il} \left(\sum_{k=1}^{p} B_{lk}C_{kj} \right) = \sum_{l=1}^{r}\sum_{k=1}^{p} A_{il}B_{lk}C_{kj}$$

Vidíme, že oba výrazy jsou shodné až na pořadí sčítanců. Ale protože sčítání reálných čísel je komutativní, tak jsou hodnoty stejné. □

Poznámka 3.8. Součin matic obecně není komutativní! Pro mnoho matic je $AB \neq BA$. Najděte takový příklad!

Definice 3.9 (Transpozice)**.** Buď $A \in \mathbb{R}^{m\times n}$. Pak *transponovaná matice* má typ $n \times m$, značí se A^T a je definovaná $(A^T)_{ij} \coloneqq a_{ji}$.

Příklad 3.10. Transpozice vlastně znamená překlopení dle hlavní diagonály, např.

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}, \quad A^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}.$$

□

Věta 3.11 (Vlastnosti transpozice)**.** *Platí následující vlastnosti; α je číslo a A, B matice vhodných rozměrů.*

(1) $(A^T)^T = A$
(2) $(A + B)^T = A^T + B^T$
(3) $(\alpha A)^T = \alpha A^T$
(4) $(AB)^T = B^T A^T$

Důkaz. Triviální z definice. □

Definice 3.12 (Symetrická matice)**.** Matice $A \in \mathbb{R}^{n\times n}$ je *symetrická* pokud $A = A^T$.

Symetrická matice je tedy symetrická dle hlavní diagonály, např. je to O_n, I_n nebo $\left(\begin{smallmatrix}1 & 2\\ 2 & 3\end{smallmatrix}\right)$. Součet symetrických matic stejného řádu je zase symetrická matice (dokažte!), ale pro součin už to obecně neplatí (najděte protipříklad!).

Existuje celá řada speciálních typů matic. Mezi ty nejpoužívanější patří např.:

- *Diagonální matice.* Matice $A \in \mathbb{R}^{n\times n}$ je diagonální pokud $a_{ij} = 0$ pro všechna $i \neq j$. Tedy diagonální matice má na diagonále libovolné prvky a mimo ni jsou nuly. Příklad: jednotková matice I, nulová matice 0.
- *Horní trojúhelníková matice.* Matice $A \in \mathbb{R}^{n\times n}$ je horní trojúhelníková pokud $a_{ij} = 0$ pro všechna $i > j$. Tedy horní trojúhelníková matice má pod diagonálou nuly. Podobně se zavádí i *dolní trojúhelníková matice.*

Vraťme se na chvíli k aritmetickým vektorům. Transpozice a součin vektorů jakožto matic o jednom sloupci nám pomůže zavést známý skalární součin a normu vektoru. Buď $x, y \in \mathbb{R}^n$. Pak *skalární součin* x, y je

$$x^T y = \sum_{i=1}^{n} x_i y_i$$

(formálně je to matice 1×1, ale ztotožníme ji s reálným číslem). *Vnější součin* x, y je matice

$$xy^T = \begin{pmatrix} x_1y_1 & x_1y_2 & \dots & x_1y_n \\ \vdots & \vdots & & \vdots \\ x_ny_1 & x_ny_2 & \dots & x_ny_n \end{pmatrix}.$$

Standardní norma vektoru $x \in \mathbb{R}^n$ lze pak zavést jako

$$\|x\| = \sqrt{x^T x} = \sqrt{\textstyle\sum_{i=1}^{n} x_i^2}$$

Obecnější definice skalárního součinu a normy přijde později (Kapitola 8).

V následující větě si uvedeme ještě nějaké vlastnosti maticového násobení, které občas budeme využívat. První dvě vlastnosti říkají, co je výsledkem násobení matice s jednotkovým vektorem, další dvě ukazují jak snadno získat řádek či sloupec součinu matic a poslední dvě dávají jiný pohled na násobení matice s vektorem.

Věta 3.13. *Buď $A \in \mathbb{R}^{m\times p}$, $B \in \mathbb{R}^{p\times n}$, $x \in \mathbb{R}^p$ a $y \in \mathbb{R}^m$. Pak platí:*

(1) $Ae_j = A_{*j}$

(2) $e_i^T A = A_{i*}$

(3) $(AB)_{*j} = AB_{*j}$

(4) $(AB)_{i*} = A_{i*}B$

(5) $Ax = \sum_{j=1}^{p} x_j A_{*j}$

(6) $y^T A = \sum_{i=1}^{m} y_i A_{i*}$

Důkaz. Jednoduché z definice. Pro ilustraci si uvedeme jen některá tvrzení:

(1) $(Ae_j)_i = \sum_{k=1}^{n} a_{ik}(e_j)_k = \sum_{k\neq j}^{n} a_{ik} \cdot 0 + a_{ij} \cdot 1 = a_{ij}$.

(3) S využitím první vlastnosti, $(AB)_{*j} = (AB)e_j = A(Be_j) = AB_{*j}$.

(5) Levá strana: $(Ax)_i = \sum_{j=1}^{p} a_{ij}x_j$, pravá strana: $(\sum_{j=1}^{p} x_j A_{*j})_i = \sum_{j=1}^{p} x_j (A_{*j})_i = \sum_{j=1}^{p} x_j a_{ij}$. □

Poznámka 3.14. Soustavu lineárních rovnic (2.1) můžeme maticově zapsat také takto: $Ax = b$, kde $x = (x_1, \dots, x_n)^T$ je vektor proměnných, $b \in \mathbb{R}^m$ vektor pravých stran a $A \in \mathbb{R}^{m\times n}$ matice soustavy.

Poznámka 3.15 (Blokové násobení matic)**.** Občas je výhodné použít tzv. blokové násobení matic, tj. matice rozdělíme do několika bloků (podmatic) a pak se matice násobí jako by byly podmatice obyčejná čísla. Např. pokud matice A, B rozdělíme na 4 podmatice, pak

$$AB = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{pmatrix}.$$

Zde je nutné si dát pozor, aby podmatice $A_{11}, \ldots, B_{22}$ měly vhodné rozměry a součiny v pravé části rovnosti dávaly smysl.

Poznámka 3.16 (Rychlé násobení matic)**.** Pokud násobíme dvě čtvercové matice řádu n, tak nás výpočet stojí řádově n^3 aritmetických operací. Na první pohled se může zdát, že výpočet nelze výrazně urychlit. Nicméně německý matematik Volker Strassen přišel r. 1969 s algoritmem, který potřebuje řádově pouze $n^{\log_2 7} \approx n^{2.807}$ operací. Strassenův algoritmus využívá právě rozdělení matic do bloků a chytrého přeuspořádání. Vývoj šel dál, Coppersmith–Winogradův algoritmus z r. 1990 snížil výpočetní složitost na řádově $n^{2.376}$. Poznamenejme ale, že tyto rychlé algoritmy se uplatní pouze pro velké n, protože skryté koeficienty u řádových odhadů jsou poměrně vysoké. Jaká je nejmenší možná asymptotická složitost je stále otevřený problém. Zajímavé také je, že násobení matic má stejnou asymptotickou složitost jako maticová inverze probíraná v Sekci 3.3, tedy oba problémy jsou na sebe efektivně převoditelné.

3.2 Regulární matice

Definice 3.17 (Regulární matice)**.** Buď $A \in \mathbb{R}^{n\times n}$. Matice A je *regulární* pokud soustava $Ax = 0$ má jediné řešení $x = 0$. V opačném případě se nazývá *singulární*.

Jiný ekvivalentní pohled na regulární matice je, že $Ax \neq 0$ pro všechna $x \neq 0$. Typickým příkladem regulární matice je I_n a singulární matice 0.

Věta 3.18. *Buď $A \in \mathbb{R}^{n\times n}$. Pak následující je ekvivalentní:*

(1) A je regulární,

(2) $RREF(A) = I$,

(3) $\operatorname{rank}(A) = n$.

Důkaz. Plyne z rozboru Gauss–Jordanovy eliminace. □

Nyní si ukážeme, že nulová pravá strana soustavy z definice regulární matice není tak podstatná.

Věta 3.19. *Buď $A \in \mathbb{R}^{n\times n}$. Pak následující je ekvivalentní:*

(1) A je regulární,

(2) pro nějaké $b \in \mathbb{R}^n$ má soustava $Ax = b$ jediné řešení,

(3) pro každé $b \in \mathbb{R}^n$ má soustava $Ax = b$ jediné řešení.

Důkaz. Plyne z rozboru Gauss–Jordanovy eliminace a Věty 3.18. □

Podívejme se na základní vlastnosti regulárních matic. Součet regulárních matic nemusí být regulární matice, vezměme např. $I + (-I) = 0$. Součin ale regularitu zachovává.

Věta 3.20. *Buďte $A, B \in \mathbb{R}^{n\times n}$ regulární matice. Pak AB je také regulární.*

Důkaz. Buď x řešení soustavy $ABx = 0$. Chceme ukázat, že x musí být nulový vektor. Označme si $y \coloneqq Bx$. Pak soustava lze přepsat na $Ay = 0$ a z regularity A je $y = 0$, neboli $Bx = 0$. Z regularity B je $x = 0$. □

Vraťme se k elementárním řádkovým úpravám. Ukážeme si, že jdou reprezentovat maticově, a že tyto matice jsou regulární. To, že jdou reprezentovat maticově, znamená, že výsledek úpravy na matici A je EA pro nějakou matici E. Jak najít tuto matici? Pomůže nám uvědomíme-li si, že aplikací dané úpravy na I dostaneme $EI = E$, tedy matici reprezentující danou úpravy dostaneme tak, že tuto úpravy provedeme na jednotkovou matici. Ale pozor! To je pouze nutná podmínka jak by taková matice měla vypadat. To, že to skutečně funguje, se musí dokázat pro každou úpravu zvlášť (důkaz necháváme na cvičení):

1. Vynásobení i-tého řádku číslem $\alpha \neq 0$ lze reprezentovat vynásobením zleva maticí
$$E_i(\alpha) = I + (\alpha - 1)e_i e_i^T = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \alpha & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}.$$

2. Přičtení α-násobku j-tého řádku k i-tému, přičemž $i \neq j$, lze reprezentovat vynásobením zleva maticí
$$E_{ij}(\alpha) = I + \alpha e_i e_j^T = \begin{array}{c} \\ \\ \\ i \\ \\ \\ \end{array} \begin{array}{c} \begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ & \ddots & \ddots & & \vdots \\ & & 1 & \ddots & \vdots \\ & \alpha & & \ddots & 0 \\ & & & & 1 \end{pmatrix} \\ j \end{array}.$$

3. Výměna i-tého a j-tého řádku jde reprezentovat vynásobením zleva maticí
$$E_{ij} = I + (e_j - e_i)(e_i - e_j)^T = \begin{array}{c} \\ i \\ \\ j \\ \\ \end{array} \begin{array}{c} \begin{pmatrix} 0 & 1 \\ & \\ 1 & 0 \end{pmatrix} \\ \begin{array}{cc} i & j \end{array} \end{array}.$$

Snadno se ukáže, že matice elementárních operací jsou regulární (dokažte!).

Maticově jdou reprezentovat nejenom elementární řádkové úpravy, ale také celá transformace převodu matice na odstupňovaný tvar.

Věta 3.21. *Buď $A \in \mathbb{R}^{m\times n}$. Pak $RREF(A) = QA$ pro nějakou regulární matici $Q \in \mathbb{R}^{n\times n}$.*

Důkaz. $RREF(A)$ získáme aplikací konečně mnoha elementárních řádkových úprav. Nechť jdou reprezentovat maticemi $E_1, E_2, \dots, E_k$. Pak $RREF(A) = E_k \dots E_2 E_1 A = QA$, kde $Q = E_k \dots E_2 E_1$. Protože matice $E_1, E_2, \dots, E_k$ jsou regulární, i jejich součin Q je regulární. □

Věta 3.22. *Každá regulární matice $A \in \mathbb{R}^{n\times n}$ se dá vyjádřit jako součin konečně mnoha elementárních matic.*

Důkaz. Pokud k elementárními úpravami dokážu dovést matici A na jednotkovou I_n, pak jistými k elementárními úpravami mohu převést naopak I_n na A. Je to tím, že každá elementární úprava má svojí inverzní, která vykonává opačnou úpravu. Tudíž existují matice $E_1, \dots, E_k$ elementárních úprav tak, že $A = E_k \dots E_2 E_1 I_n = E_k \dots E_2 E_1$. □

3.3 Inverzní matice

Motivace pro inverzní matice: Matice umíme sčítat, odečítat, násobit, tak nešly by i dělit? Ukážeme si, že něco jako dělení lze zavést, ale jen pro regulární matice.

Definice 3.23. Buď $A \in \mathbb{R}^{n\times n}$. Pak A^{-1} je *inverzní* maticí k A pokud splňuje $AA^{-1} = A^{-1}A = I_n$.

Které matice mají inverzi? Pouze a jen ty regulární.

Věta 3.24 (O existenci inverzní matice)**.** *Buď $A \in \mathbb{R}^{n\times n}$. Je-li A regulární, pak k ní existuje inverzní matice, a je určená jednoznačně. Naopak, existuje-li k A inverzní, pak A musí být regulární.*

Důkaz. 1. „Existence.“ Z předpokladu regularity matice A plyne, že soustava $Ax = e_j$ má (jediné) řešení pro každé $j = 1, \dots, n$, označme je x_j, $j = 1, \dots, n$. Vytvořme matici A^{-1} tak, aby její sloupce byly vektory $x_1, \dots, x_n$, to jest, $A^{-1} = (x_1|x_2|\dots|x_n)$. Ukážeme, že tato matice je hledaná inverze. Rovnost $AA^{-1} = I$ ukážeme po sloupcích. Buď $j \in \{1, \dots, n\}$, pak

$$(AA^{-1})_{*j} = A(A^{-1})_{*j} = Ax_j = e_j = I_{*j}.$$

Druhou rovnost dokážeme trochu trikem. Uvažme výraz

$$A(A^{-1}A - I) = AA^{-1}A - A = AI - A = 0.$$

Matice $A(A^{-1}A - I)$ je tedy nulová a její j-tý sloupec je nulový vektor: $A(A^{-1}A - I)_{*j} = 0$. Z regularity matice A dostáváme, že $(A^{-1}A - I)_{*j} = 0$. Protože to platí pro každé $j \in \{1, \dots, n\}$, je $A^{-1}A - I = 0$, neboli $A^{-1}A = I$.

2. „Jednoznačnost.“ Nechť pro nějakou matici B platí $AB = BA = I$. Pak

$$B = BI = B(AA^{-1}) = (BA)A^{-1} = IA^{-1} = A^{-1},$$

tedy B už musí být automaticky rovno naší zkonstruované matici A^{-1}.

3. „Naopak.“ Nechť pro A existuje inverzní matice. Buď x řešení soustavy $Ax = 0$. Pak $x = Ix = (A^{-1}A)x = A^{-1}(Ax) = A^{-1}0 = 0$. Tedy A je regulární. □

Uvědomme si, že první část důkazu nám dává i návod jak inverzní matici spočítat pomocí n soustav lineárních rovnic. Později (Věta 3.27) si ukážeme lepší metodu.

Pomocí inverzních matic snadno dokážeme následující větu, kterou bychom přímo z definice bez vybudovaného aparátu jen těžko dokazovali.

Věta 3.25. *Je-li A regulární, pak A^T je regulární.*

Důkaz. Je-li A regulární, pak existuje inverzní matice a platí $AA^{-1} = A^{-1}A = I_n$. Po transponování všech stran rovností dostaneme $(AA^{-1})^T = (A^{-1}A)^T = I_n^T$, neboli $(A^{-1})^T A^T = A^T(A^{-1})^T = I_n$. Vidíme, že matice A^T má inverzní (rovnou $(A^{-1})^T$) a je tudíž regulární. Navíc dostáváme i pěkný vztah $(A^T)^{-1} = (A^{-1})^T$. □

Ukážeme si, že dvě rovnosti $AA^{-1} = I_n$, $A^{-1}A = I_n$ z definice inverzní matice jsou zbytečný přepych a k jejímu určení stačí jen jedna z nich.

Věta 3.26 (Jedna rovnost stačí)**.** *Buďte $A, B \in \mathbb{R}^{n\times n}$.*

1. Je-li $BA = I$, pak A je regulární a $B = A^{-1}$.

2. Je-li $AB = I$, pak A je regulární a $B = A^{-1}$.

Důkaz. 1. „Regularita.“ Pokud x řeší soustavu $Ax = 0$, pak $x = Ix = (BA)x = B(Ax) = B0 = 0$, tedy A je regulární.

1. „Inverze.“ Nyní víme, že A je regulární a tudíž má inverzi A^{-1}. Proto $B = BI = B(AA^{-1}) = (BA)A^{-1} = IA^{-1} = A^{-1}$.

2. „Regularita.“ Transponujme obě strany rovnosti $AB = I$ a máme $B^T A^T = I$. Podle první části věty, kterou jsme již dokázali, je A^T regulární a dle věty 3.25 je i $(A^T)^T = A$ regulární.

2. „Inverze.“ Analogicky využijeme dokázané regularity A k odvození $B = IB = (A^{-1}A)B = A^{-1}(AB) = A^{-1}I = A^{-1}$. □

Věta 3.27 (Výpočet inverzní matice). *Buď $A \in \mathbb{R}^{n\times n}$. Nechť matice $(A \,|\, I_n)$ typu $n \times 2n$ má RREF tvar $(I_n \,|\, B)$. Pak $B = A^{-1}$. Netvoří-li první část RREF tvaru jednotkovou matici, pak A je singulární.*

Důkaz. Je-li $RREF(A \,|\, I_n) = (I_n \,|\, B)$, potom dle Věty 3.21 existuje regulární matice Q taková, že $(I_n \,|\, B) = Q(A \,|\, I_n)$, neboli po roztrženi na dvě části $I_n = QA$ a $B = QI_n$. První rovnost říká $Q = A^{-1}$ a druhá $B = Q = A^{-1}$.

Netvoří-li první část RREF tvaru jednotkovou matici, pak $RREF(A) \neq I_n$ a tudíž A není regulární. □

Příklad 3.28. Buď $A = \begin{pmatrix} 1 & 1 & 3 \\ 0 & 2 & -1 \\ 3 & 5 & 7 \end{pmatrix}$. Inverzní matici spočítáme takto:

$$(A \,|\, I_3) = \left(\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 0 & 2 & -1 & 0 & 1 & 0 \\ 3 & 5 & 7 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 0 & 2 & -1 & 0 & 1 & 0 \\ 0 & 2 & -2 & -3 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 0 & 1 & -0.5 & 0 & 0.5 & 0 \\ 0 & 2 & -2 & -3 & 0 & 1 \end{array}\right)$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 3.5 & 1 & -0.5 & 0 \\ 0 & 1 & -0.5 & 0 & 0.5 & 0 \\ 0 & 0 & -1 & -3 & -1 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -9.5 & -4 & 3.5 \\ 0 & 1 & 0 & 1.5 & 1 & -0.5 \\ 0 & 0 & 1 & 3 & 1 & -1 \end{array}\right) = \left(I_3 \,|\, A^{-1}\right)$$

Tedy máme $A^{-1} = \begin{pmatrix} -9.5 & -4 & 3.5 \\ 1.5 & 1 & -0.5 \\ 3 & 1 & -1 \end{pmatrix}$. □

Shrňme základní vlastnosti inverzních matic. Poznamenejme, že pro inverzi součtu dvou matic není znám žádný jednoduchý vzoreček.

Věta 3.29 (Vlastnosti inverzní matice). *Buďte $A, B \in \mathbb{R}^{n\times n}$ regulární. Pak:*

(1) $(A^{-1})^{-1} = A$,
(2) $(A^{-1})^T = (A^T)^{-1}$,
(3) $(\alpha A)^{-1} = \frac{1}{\alpha}A^{-1}$ *pro* $\alpha \neq 0$,
(4) $(AB)^{-1} = B^{-1}A^{-1}$.

Důkaz.
(1) Z rovnosti $A^{-1}A = I$ máme, že inverzní matice k A^{-1} je právě A.
(2) Bylo ukázáno v důkazu Věty 3.25.
(3) Plyne z $(\alpha A)(\frac{1}{\alpha}A^{-1}) = \frac{\alpha}{\alpha}AA^{-1} = I$.
(4) Plyne z $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I$. □

Pomocí inverzních matic můžeme elegantně vyjádřit řešení soustavy rovnic s regulární maticí. V praxi se ovšem tento výpočet nepoužívá, neboť je časově dražší než Gaussova eliminace.

Věta 3.30 (Soustava rovnic a inverzní matice). *Buď $A \in \mathbb{R}^{n\times n}$ regulární. Pak řešení soustavy $Ax = b$ je dáno vzorcem $x = A^{-1}b$.*

Důkaz. Protože A je regulární, má soustava jediné řešení x. Platí $x = Ix = (A^{-1}A)x = A^{-1}(Ax) = A^{-1}b$. □

Příklad 3.31. Jak se změní množina řešení soustavy $Ax = b$ když obě strany vynásobíme maticí Q, tj. přejdeme k soustavě $QAx = Qb$? A jak se změní když Q je regulární? □

Přestože jsme zmínili, že pro inverzi součtu matic není znám žádný jednoduchý vzoreček, ve speciálním případě to možné je. Tím speciálním případem je tzv. *rank-one update*, tedy situace, kdy jedna matice má hodnost 1. Tato formule tedy umožňuje rychle přepočítat inverzní matici, pokud původní matici „málo“ změníme, např. změny jsou jen v jednom řádku či jednom sloupci (pak b resp. c je jednotkový vektor).

Věta 3.32 (Sherman–Morrisonova formule[1]). *Buď $A \in \mathbb{R}^{n\times n}$ regulární a $b, c \in \mathbb{R}^n$. Pokud $c^T A^{-1} b = -1$, tak $A + bc^T$ je singulární, jinak*

$$(A + bc^T)^{-1} = A^{-1} - \frac{1}{1 + c^T A^{-1} b} A^{-1} bc^T A^{-1}.$$

Důkaz. V případě $c^T A^{-1} b = -1$ máme $(A+bc^T)A^{-1}b = AA^{-1}b + bc^T A^{-1}b = b(1 + c^T A^{-1}b) = 0$. Protože $b \neq 0$ a vzhledem k regularitě A je $A^{-1}b \neq 0$, musí matice$(A + bc^T)$ být singulární.

Pokud $c^T A^{-1} b \neq -1$, dostáváme:

$$\begin{aligned}(A + bc^T) &\left(A^{-1} - \frac{1}{1 + c^T A^{-1} b} A^{-1} bc^T A^{-1}\right) \\ &= I_n + bc^T A^{-1} - \frac{1}{1 + c^T A^{-1} b} bc^T A^{-1} - \frac{1}{1 + c^T A^{-1} b} b(c^T A^{-1} b)c^T A^{-1} \\ &= I_n + \Big(1 - \frac{1}{1 + c^T A^{-1} b} - \frac{c^T A^{-1} b}{1 + c^T A^{-1} b}\Big) bc^T A^{-1} = I_n + 0 \cdot bc^T A^{-1} = I_n.\end{aligned}$$

□

3.4 Jednoznačnost RREF

Abychom dokázali jednoznačnost RREF tvaru, ukážeme si nejprve pomocné tvrzení.

Lemma 3.33. *Buďte $A, B \in \mathbb{R}^{m\times n}$ matice v RREF tvaru, a nechť platí $A = QB$ pro nějakou regulární matici Q. Potom $A = B$.*

Důkaz. Matematickou indukcí podle n, tj. počtu sloupců.

Je-li $n = 1$, pak nastane jedna z možností: buď $B = 0$ nebo $B = e_1$. V prvním případě je $A = QB = Q0 = 0 = B$. V druhém případě je $QB \neq 0$ díky regularitě Q, tedy $A = e_1$.

Indukční krok $n \leftarrow n - 1$. Rozdělme matice A, B na podmatice $m \times (n-1)$ a poslední sloupec takto: $A = (A' \,|\, a)$, $B = (B' \,|\, b)$. Zřejmě A', B' jsou také v RREF tvaru. Rovnost $A = QB$ lze rozepsat jako $A' = QB'$ a $a = Qb$. První z rovností nám díky indukčnímu předpokladu dává $A' = B'$, takže zbývá dokázat $a = b$.

Označme r počet pivotů matice A' a nechť jsou ve sloupcích $p_1, \ldots, p_r$. Pak pro každé $i = 1, \ldots, r$ je $e_i = A'_{*p_i} = QB'_{*p_i} = Qe_i = Q_{*i}$. Tedy prvních r sloupců matice Q je tvořeno jednotkovými sloupci. Nyní uvažme dvě možnosti: buď je poslední sloupec matice B bázický nebo ne. Pokud není, pak $b_{r+1} = \ldots = b_m = 0$ a tedy $b = \sum_{j=1}^m b_j e_j = \sum_{j=1}^r b_j e_j = \sum_{j=1}^r b_j Q_{*j} = \sum_{j=1}^m b_j Q_{*j} = Qb = a$. Naopak, je-li poslední sloupec B bázický, pak $b = e_{r+1}$. Tvrdíme, že v tomto případě je také $a = e_{r+1}$. Jinak, pokud $a_{r+1} = \ldots = a_m = 0$ (poslední sloupec A je nebázický) a tudíž $a \neq b$, pak $Qa = \sum_{j=1}^m a_j Q_{*j} = \sum_{j=1}^r a_j Q_{*j} + \sum_{j=r+1}^m 0 Q_{*j} = \sum_{j=1}^r a_j e_j = a$. Tedy $Qa = a = Qb$, z čehož máme $Q(a - b) = 0$ a díky regularitě Q je $a = b$, což je spor. □

Věta 3.34 (Jednoznačnost RREF). *RREF tvar matice je jednoznačně určen.*

Důkaz. Buď $A \in \mathbb{R}^{m\times n}$ a nechť má dva různé RREF tvary A_1 a A_2. Podle Věty 3.21 existují regulární matice Q_1, Q_2 takové, že $Q_1 A = A_1$, $Q_2 A = A_2$. Pak máme $A = Q_1^{-1} A_1 = Q_2^{-1} A_2$, a tedy $A_1 = Q_1 Q_2^{-1} A_2$. Protože $Q_1 Q_2^{-1}$ je regulární, podle Lemmatu 3.33 dostáváme $A_1 = A_2$, což je spor. □

Poznámka 3.35. Předchozí věta je důležitá mj. z toho důvodu, že ospravedlňuje definici hodnosti matice jako počet pivotů RREF tvaru matice (viz sekce 2.2). Nyní je tedy pojem hodnosti dobře definován.

Věta říká také to, že ačkoli REF tvar jednoznačný není, tak pozice pivotů a tvar samotný (až na numerické hodnoty) jednoznačný jest.

[1] Nazývána podle amerických statistiků se jmény Jack Sherman a Winifred J. Morrison, kteří ji odvodili v letech 1949–50. Nezávisle na nich byla objevena řadou jiných osobností, např. obecnější tvar odvodil Max Woodbury v r. 1950.

3.5 Ještě k soustavám rovnic

3.5.1 Numerická stabilita při řešení soustav

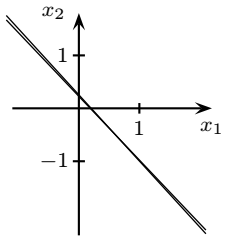
Na závěr kapitol věnovaných soustavám rovnic a maticím se zmiňme jak je to s numerickým řešením soustav lineárních rovnic. Přestože Gaussova eliminace představuje teoreticky kvalitní nástroj na řešení soustav, při numerickém řešení na počítačích dochází k zaokrouhlovacím chybám a vypočtený výsledek se může diametrálně lišit od správného řešení. Tato nestabilita se nazývá *špatná podmíněnost*. Přestože to je spíš vlastnost dané soustavy než Gaussovy eliminace, jiné metody se dokáží s případnou nestabilitou vypořádat trochu lépe.

Příklad 3.36. Uvažujme dvě soustavy, které se liší v jediném koeficientu podle toho zda jsme zaokrouhlili číslo $\frac{2}{30}$ nahoru či dolů (na tři desetinná místa).

$$\begin{aligned} 0.835x_1 + 0.667x_2 &= 0.168 \\ 0.333x_1 + 0.266x_2 &= \mathbf{0.067} \end{aligned} \qquad \begin{aligned} 0.835x_1 + 0.667x_2 &= 0.168 \\ 0.333x_1 + 0.266x_2 &= \mathbf{0.066} \end{aligned}$$

Zatímco první soustava má řešení $(x_1, x_2) = (1, -1)$, ta druhá má řešení $(x_1, x_2) = (-666, 834)$.

Geometrická představa je průsečík dvou téměř identických přímek, takže malá změna v datech znamená potencionálně velkou změnu v průsečíku.



□

Příklad 3.37. Jiným, typickým příkladem špatně podmíněných matic jsou tzv. Hilbertovy matice. Hilbertova matice H_n řádu n je definována $(H_n)_{ij} = \dfrac{1}{i+j-1}$, $i, j = 1, \ldots .n$. Např.

$$H_3 = \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} \end{pmatrix}.$$

Uvažujme soustavu $H_n x = b$, kde $b = H_n e$. Řešení soustavy je $x = e = (1, \ldots, 1)^T$, a protože H_n je regulární, je to jediné řešení. Jak se se soustavou vypořádá počítač? Výpočty v Matlabu (R 2008b), double precision 52 bitů $\sim 10^{-16}$ v roce 2009 ukázaly:

n	řešení
8	$x_i = 1$
10	$x_i \in [0.9995,\ 1.0003]$
12	$x_i \in [0.8246,\ 1.1500]$
14	$x_i \in [-45.4628,\ 53.3428]$

□

Příklad 3.38 (Parciální pivotizace)**.** Nyní si ukážeme, že parciální pivotizace často vede k přesnějšímu řešení, i když ani ta samozřejmě není všelék. Řešíme soustavu v aritmetice s přesností na 3 číslice:

$$\begin{aligned} 10^{-3}x_1 - x_2 &= 1, \\ 2x_1 + x_2 &= 0. \end{aligned}$$

Bez pivotizace:

$$\left(\begin{array}{cc|c} \mathbf{10^{-3}} & -1 & 1 \\ 2 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{cc|c} \mathbf{1} & -1000 & 1000 \\ 2 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & -1000 & 1000 \\ 0 & \mathbf{2000} & -2000 \end{array}\right)$$
$$\sim \left(\begin{array}{cc|c} 1 & -1000 & 1000 \\ 0 & \mathbf{1} & -1 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & -1 \end{array}\right).$$

Parciální pivotizace:

$$\left(\begin{array}{cc|c} 10^{-3} & -1 & 1 \\ \mathbf{2} & 1 & 0 \end{array}\right) \sim \left(\begin{array}{cc|c} \mathbf{2} & 1 & 0 \\ 10^{-3} & -1 & 1 \end{array}\right) \sim \cdots \sim \left(\begin{array}{cc|c} 1 & 0 & \frac{1}{2} \\ 0 & 1 & -1 \end{array}\right).$$

Pro porovnání, skutečné řešení je $(\frac{1000}{2001}, -\frac{2000}{2001})$ □

3.5.2 LU rozklad

LU rozklad je rozklad čtvercové matice $A \in \mathbb{R}^{n\times n}$ na součin $A = LU$, kde L je dolní trojúhelníková matice s jedničkami na diagonále a U horní trojúhelníková matice.

LU rozklad úzce souvisí s odstupňovaným tvarem matice. V zasadě, U je odstupňovaný tvar A a matici L můžeme získat z elementárních úprav. Pokud z elementárních úprav používáme pouze násobení řádku nenulovým číslem a přičtení násobku řádku k nějakému pod ním (tedy bez prohazování řádků), tak matice takovýchto úprav jsou dolní trojúhelníkové a jejich inverze taky. Tudíž nám dají dohromady hledanou matici L. Základní algoritmus tedu může být:

Převeď A na odstupňovaný tvar U: tedy $E_k \dots E_1 A = U$, z čehož $A = \underbrace{E_1^{-1} \dots E_k^{-1}}_{L} U$.

Uvědomíme-li si jak se invertuje matice elementární úpravy, lze L konstruovat velice efektivně a dokonce obě matice L a U můžeme udržovat v jedné matici.

Příklad 3.39. Např.:

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 4 & 1 & 7 \\ -6 & -2 & -12 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 3 \\ \textcircled{2} & -1 & 1 \\ -6 & -2 & -12 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 3 \\ \textcircled{2} & -1 & 1 \\ \textcircled{-3} & 1 & -3 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 3 \\ \textcircled{2} & -1 & 1 \\ \textcircled{-3} & \textcircled{-1} & -2 \end{pmatrix}.$$

Tedy

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 4 & 1 & 7 \\ -6 & -2 & -12 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ -3 & -1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 & 3 \\ 0 & -1 & 1 \\ 0 & 0 & -2 \end{pmatrix} = LU.$$

□

Algoritmus se dá adaptovat i na případ když při elementárních úpravách musíme někde prohodit řádky. Pak dostaneme LU rozklad matice vniklé z A prohozením nějakých řádků. Obecně totiž ne pro pro každou matici LU rozklad existuje (např. pro $A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$), ale po vhodném proházení řádků už ano.

Lu rozklad má široké uplatnění. Například pro invertování matic: $A^{-1} = U^{-1}L^{-1}$, pro počítání determinantu $\det(A) = \det(L)\det(U)$ (viz kapitola 9) nebo pro řešení soustav rovnic.

Příklad 3.40. Použití LU rozkladu pro řešení soustavy $Ax = b$ (tedy $LUx = b$):

(1) Najdi LU rozklad matice A, tj. $A = LU$,

(2) vyřeš soustavu $Ly = b$ dopřednou substitucí,

(3) vyřeš soustavu $Ux = y$ zpětnou substitucí.

Například pro soustavu s maticí z Příkladu 3.39

$$(A \mid b) = \left(\begin{array}{ccc|c} 2 & 1 & 3 & -1 \\ 4 & 1 & 7 & 5 \\ -6 & -2 & -12 & -2 \end{array}\right).$$

Krok (2)

$$(L \mid b) = \left(\begin{array}{ccc|c} 1 & 0 & 0 & -1 \\ 2 & 1 & 0 & 5 \\ -3 & -1 & 1 & -2 \end{array}\right) \rightarrow y = (-1, 7, 2)^T.$$

Krok (3)

$$(U \mid y) = \left(\begin{array}{ccc|c} 2 & 1 & 3 & -1 \\ 0 & -1 & 1 & 7 \\ 0 & 0 & -2 & 2 \end{array}\right) \rightarrow x = (5, -8, -1)^T.$$

□

3.5.3 Iterativní metody

Kromě přímých metod typu Gaussovy eliminace na řešení soustav lineárních rovnic existují i iterativní metody, které od počátečního vektoru postupně konvergují k řešení soustavy. Výhoda iterativních metod je menší citlivost k zaokrouhlovacím chybám, a menší časové a paměťové nároky pro velké a řídké soustavy (řídké soustavy mají jen malý zlomek hodnot nenulových, většina jsou nuly).

Jedna ze základních iterativních metod je Gauss–Seidelova metoda, ukážeme si ji na konkrétním příkladu.

Příklad 3.41. Uvažujme soustavu

$$\left.\begin{array}{c} 6x + 2y - z = 4 \\ x + 5y + z = 3 \\ 2x + y + 4z = 27 \end{array}\right\} \quad \begin{array}{l} x = \frac{1}{6}(4 - 2y + z) \\ y = \frac{1}{5}(3 - x - z) \\ z = \frac{1}{4}(27 - 2x - y) \end{array}$$

Zvolme počáteční hodnoty $x^{(0)} = y^{(0)} = z^{(0)} = 1$. Iterační krok je pak:

$$\begin{aligned} x^{(i)} &= \tfrac{1}{6}(4 - 2y^{(i-1)} + z^{(i-1)}), \\ y^{(i)} &= \tfrac{1}{5}(3 - x^{(i)} - z^{(i-1)}), \\ z^{(i)} &= \tfrac{1}{4}(27 - 2x^{(i)} - y^{(i)}). \end{aligned}$$

Průběh:

iterace	$x^{(i)}$	$y^{(i)}$	$z^{(i)}$
0	1	1	1
1	0.5	0.3	6.425
2	1.6375	-1.0125	6.184375
3	2.034896	-1.043854	5.993516
4	2.013537	-1.001411	5.993584
5	1.999401	-0.998597	5.999949
6	1.999624	-0.999895	6.000212

□

3.6 Aplikace

Interpolace polynomem

Vraťme se nyní k problému interpolace bodů polynomem. Lagrangeova Věta 1.2 nám sice dává explicitní vyjádření polynomu, ale polynom není v základním tvaru. Navíc nevíme, jestli takovýto polynom má nejmenší možný stupeň a jestli je jednoznačný.

Mějme body $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)$, kde $x_i \neq x_j$ pro $i \neq j$ a hledejme interpolační polynom ve

tvaru $p(x) = a_n x^n + \cdots + a_1 x + a_0$. Pokud dosadíme dané body, dostáváme soustavu rovnic

$$\begin{aligned} a_n x_0^n + \cdots + a_1 x_0 + a_0 &= 0, \\ a_n x_1^n + \cdots + a_1 x_1 + a_0 &= 0, \\ &\vdots \\ a_n x_n^n + \cdots + a_1 x_n + a_0 &= 0. \end{aligned}$$

Rovnic je $n+1$ a proměnných také, jsou to koeficienty $a_n, \ldots, a_0$. Máme tedy soustavu rovnic se čtvercovou maticí, nazývanou Vandermondova[2)]. Proto jsme také hledali polynom $p(x)$ stupně n; polynom menšího stupně by nemusel existovat (více rovnic než proměnných) a naopak polynom vyššího stupně by nemusel být jednoznačný (více proměnných než rovnic). Jak si ukážeme, naše čtvercová matice je regulární a proto polynom stupně n vždy existuje a je určený jednoznačně. Polynom pak získáme pomocí Věty 1.2 nebo vyřešením soustavy rovnic.

Regularita matice soustavy se ukáže následujícími elementárními úpravami. Nejprve ke každému sloupci kromě posledního přičteme x_n násobek sloupce napravo a pak i-tý řádek vydělíme číslem $x_{i-1} - x_n$. Až na poslední řádek a sloupec dostaneme Vandermondovu matici menšího řádu, kterou upravujeme rekursivně dále.

$$\begin{pmatrix} x_0^n & \ldots & x_0^2 & x_0 & 1 \\ x_1^n & \ldots & x_1^2 & x_1 & 1 \\ \vdots & \vdots & & & \vdots \\ x_n^n & \ldots & x_n^2 & x_n & 1 \end{pmatrix} = \begin{pmatrix} (x_0 - x_n)x_0^{n-1} & \ldots & (x_0 - x_n)x_0 & x_0 - x_n & 1 \\ (x_1 - x_n)x_1^{n-1} & \ldots & (x_1 - x_n)x_1 & x_1 - x_n & 1 \\ \vdots & \vdots & & & \vdots \\ (x_n - x_n)x_1^{n-1} & \ldots & (x_n - x_n)x_1 & x_1 - x_n & 1 \end{pmatrix}$$

$$= \begin{pmatrix} x_0^{n-1} & \ldots & x_0 & 1 & \frac{1}{x_0 - x_n} \\ x_1^{n-1} & \ldots & x_1 & 1 & \frac{1}{x_1 - x_n} \\ \vdots & \vdots & & & \vdots \\ x_{n-1}^{n-1} & \ldots & x_{n-1} & 1 & \frac{1}{x_{n-1} - x_n} \\ 0 & \ldots & 0 & 0 & 1 \end{pmatrix} = \cdots = \begin{pmatrix} 1 & & & \\ 0 & \ddots & & \\ \vdots & \ddots & \ddots & \\ 0 & \ldots & 0 & 1 \end{pmatrix}.$$

Diskrétní a rychlá Fourierova transformace

Nyní máme v zásadě dvě možné reprezentace polynomu $p(x)$, první je základní tvar $p(x) = a_n x^n + \cdots + a_1 x + a_0$ a druhá je seznamem funkčních hodnot v $n+1$ různých bodech. Mezi těmito reprezentacemi můžeme snadno přecházet. Z první na druhou si stačí zvolit libovolných $n+1$ bodů a spočítat funkční hodnoty a druhý směr jsme rozebírali nahoře.

Která reprezentace je výhodnější? Každá na něco jiného. Dejme tomu, že chceme umět efektivně sčítat a násobit polynomy. V první reprezentaci je sčítání jednoduché, stojí nás to řádově n aritmetických operací, ale pronásobit polynomy dá trochu zabrat, to už stojí řádově n^2 aritmetických operací. V druhé reprezentaci stojí sčítání i násobení řádově n, pokud známe funkční hodnoty polynomů ve stejných bodech. Toto by nás mohlo inspirovat k tomu násobit polynomy v základním tvaru tak, že si spočítáme funkční hodnoty ve vhodných bodech, pronásobíme a převedeme zpět. A skutečně, pokud se zvolí vhodné body, lze transformaci mezi reprezentacemi implementovat tak, že stojí řádově $n \log n$ aritmetických operací, a tolik řádově stojí i výsledné násobení polynomů. Těmto transformacím se říká Fourierova transformace, viz [Tůma, 2003, kap. 15].

Umět rychle násobit polynomy je velmi důležité. Například i obyčejné násobení reálných čísel v desetinném rozvoji si lze představit jako násobení polynomů.

[2)] Podle francouzského matematika Alexandre–Théophile Vandermonde (1735–1796).

Kapitola 4

Grupy a tělesa

Tato kapitola je věnovaná základním algebraickým strukturám jako jsou grupy a tělesa. Jsou to abstraktní pojmy zobecňující dobře známé obory reálných (racionálních, komplexních) čísel s operacemi sčítáni a násobení.

4.1 Grupy

Pojem grupy zavedl francouzský matematik Èvariste Galois (1811–1832) při budování teorie řešitelnosti hledání kořenů polynomů. Pro kořeny polynomů stupně alespoň 5 neexistuje obecně žádný vzoreček, ale Galoisova teorie dává návod jak to otestovat pro konkrétní polynom, tj. jestli kořeny daného polynomu jdou vyjádřit pomocí základních aritmetických operací a odmocnin.

Grupy mají však mnohem širší použití. Díky své obecnosti a abstraktnosti je můžeme najít v různých oborech: fyzika (Lieovy grupy), architektuře (Friezovy grupy), geometrii a molekulární chemii (symetrické grupy) aj.

Definice 4.1 (Grupa)**.** Buď $\circ : G^2 \mapsto G$ binární operace na množině G. Pak *grupou* je dvojice $(G, \circ)$ splňující:

1. $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$ (asociativita),
2. $\exists e \in G\ \forall a \in G : e \circ a = a \circ e = a$ (existence neutrálního prvku),
3. $\forall a \in G\ \exists b \in G : a \circ b = b \circ a = e$ (existence inverzního prvku).

Abelovou (komutativní) grupou je taková grupa, která navíc splňuje:

4. $\forall a, b \in G\ a \circ b = b \circ a$ (komutativita).

Výše zmíněné podmínky se také občas nazývají axiomy. Poznamenejme, že implicitně je v definici grupy schovaná podmínka uzavřenosti: $\forall a, b \in G : a \circ b \in G$. Pokud je operací $\circ$ sčítání, většinou se značí neutrální prvek 0 a inverzní $-a$, pokud jde o násobení, neutrální prvek se označuje 1 a inverzní a^{-1}.

Příklad 4.2. Ukažme si nějaké příklady grup.

- Dobře známé $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.
- Grupy matic $(\mathbb{R}^{m \times n}, +)$.
- Celá čísla $\{0, 1, \ldots, n-1\}$ a sčítání modulo n, značení $(\mathbb{Z}_n, +)$.
- Známé obory s násobením, např. $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$.
- Množina reálných polynomů proměnné x se sčítáním.

Výše zmíněné grupy jsou Abelovy. Dvě důležité neabelovské grupy jsou

- Zobrazení na množině s operací skládání, např. rotace v $\mathbb{R}^n$ podle počátku nebo později probírané permutace,
- Regulární matice s násobením.

Příklady negrup:

- $(\mathbb{N}, +)$, $(\mathbb{Z}, -)$, $(\mathbb{R} \setminus \{0\}, :)$, ... □

Věta 4.3 (Základní vlastnosti v grupě)**.** *Pro prvky grupy $(G, \circ)$ platí následující vlastnosti.*

(1) $a \circ c = b \circ c$ implikuje $a = b$ (krácení).

(2) Neutrální prvek e je určen jednoznačně.

(3) Pro každé $a \in G$ je inverzní prvek určen jednoznačně.

(4) Rovnice $a \circ x = b$ má právě jedno řešení pro každé $a, b \in G$.

Důkaz.

(1)
$$\begin{aligned} a \circ c &= b \circ c && / \circ c^{-1} \\ a \circ (c \circ c^{-1}) &= b \circ (c \circ c^{-1}) \\ a \circ e &= b \circ e \\ a &= b \end{aligned}$$

(2) Existují-li dva různé neutrální prvky e_1, e_2, pak $e_1 = e_1 \circ e_2 = e_2$, což je spor.

(3) Existují-li k $a \in G$ dva různé inverzní prvky a_1, a_2, pak $a \circ a_1 = e = a \circ a_2$ a z vlastnosti krácení dostáváme $a_1 = a_2$, což je spor.

(4) Vynásobme rovnost zleva prvkem a^{-1} a dostaneme jediného kandidáta $x = a^{-1} \circ b$. Dosazením ověříme, že rovnost splňuje. □

Tak jako množiny doprovází pojem podmnožina, tak nelze mluvit o grupách a nezmínit podgrupy.

Definice 4.4 (Podgrupa)**.** *Podgrupou* grupy $(G, \circ)$ je grupa $(H, \circ)$ taková, že $H \subseteq G$. Značení: $(H, \circ) \leq (G, \circ)$.

Jinými slovy, se stejně definovanou operací splňuje H vlastnosti uzavřenost a existence neutrálního a inverzního prvku. To jest, pro každé $a, b \in H$ je $a \circ b \in H$, dále $e \in H$, a pro každé $a \in H$ je $a^{-1} \in H$.

Příklad 4.5.

- Každá grupa $(G, \circ)$ má dvě triviální podgrupy: sama sebe $(G, \circ)$ a $(\{e\}, \circ)$.
- $(\mathbb{N}, +) \not\leq (\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$. □

4.2 Permutace

Důležitým příkladem grup je takzvaná symetrická grupa permutací, proto si povíme něco více o permutacích. Připomeňme, že vzájemně jednoznačné zobrazení (bijekce) $f : X \mapsto Y$ je zobrazení, které je prosté (žádné dva různé prvky se nezobrazí na jeden) a „na“ (pokryje celou množinu Y).

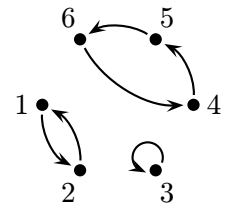
Definice 4.6 (Permutace)**.** *Permutací* na konečné množině X je vzájemně jednoznačné zobrazení $p : X \mapsto X$.

Většinou budeme uvažovat $X = \{1, \ldots, n\}$. Množina všech permutací na $\{1, \ldots, n\}$ se pak značí S_n. Zadání permutace:

- tabulkou

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$$

- grafem



- rozložením na cykly

$$p = (1,2)(3)(4,5,6) \text{ resp. redukovaně } p = (1,2)(4,5,6).$$

Příkladem jednoduché, ale důležité, permutace je *transpozice* $= (i,j)$, tj. permutace s jedním cyklem délky 2 prohazující dva prvky. Jednodušší už je jenom identita id zobrazující každý prvek na sebe.

Inverzní permutace a skládání permutací je definováno stejně jako pro jiná zobrazení:

Definice 4.7 (Inverzní permutace)**.** Buď $p \in S_n$. *Inverzní permutací* k p je permutace p^{-1} definovaná $p^{-1}(i) = j$ pokud $p(j) = i$.

Příklad 4.8. $(i,j)^{-1} = (i,j)$, $(i,j,k)^{-1} = (k,j,i)$, ... □

Definice 4.9 (Skládání permutací)**.** Buďte $p, q \in S_n$. *Složená permutace* $p \circ q$ je permutace definovaná $(p \circ q)(i) = p(q(i))$.

Příklad 4.10. $id \circ p = p \circ id = p$, $p \circ p^{-1} = p^{-1} \circ p = id$, ... □

Skládání permutací je asociativní (jako každé zobrazení), ale komutativní obecně není. Např. pro $p = (1,2)$, $q = (1,3,2)$ máme $p \circ q = (1,3)$, ale $q \circ p = (2,3)$.

Významná charakteristika permutace je tzv. znaménko.

Definice 4.11 (Znaménko permutace)**.** Nechť se permutace $p \in S_n$ skládá z k cyklů. Pak *znaménko permutace* je číslo $\operatorname{sgn}(p) = (-1)^{n-k}$.

Příklad 4.12. $\operatorname{sgn}(id) = 1$, $\operatorname{sgn}((i,j)) = -1$, ... □

Znaménko je vždy 1 nebo -1. Podle toho se též označují permutace jako *sudé* (co mají znaménko 1) a *liché* (ty se znaménkem -1).

Věta 4.13 (O znaménku složení permutace a transpozice)**.** *Buď $p \in S_n$ a $t = (i,j)$ transpozice. Pak* $\operatorname{sgn}(p) = -\operatorname{sgn}(t \circ p) = -\operatorname{sgn}(p \circ t)$.

Důkaz. Dokážeme $\operatorname{sgn}(p) = -\operatorname{sgn}(t \circ p)$, druhá rovnost je analogická. Permutace p se skládá z několika cyklů. Rozlišme dva případy:

Nechť i, j jsou částí stejného cyklu, označme jej $(i, u_1, \ldots, u_r, j, v_1, \ldots, v_s)$. Pak

$$(i,j) \circ (i, u_1, \ldots, u_r, j, v_1, \ldots, v_s) = (i, u_1, \ldots, u_r)(j, v_1, \ldots, v_s),$$

tedy počet cyklů se zvýší o jedna.

Nechť i, j náleží do dvou různých cyklů, např. $(i, u_1, \ldots, u_r)(j, v_1, \ldots, v_s)$. Pak

$$(i,j) \circ (i, u_1, \ldots, u_r)(j, v_1, \ldots, v_s) = (i, u_1, \ldots, u_r, j, v_1, \ldots, v_s),$$

tedy počet cyklů se sníží o jedna.

V každém případě se počet cyklů změní o jedna a tudíž i výsledné znaménko. □

Věta 4.14. *Každou permutaci lze rozložit na složení transpozic.*

Důkaz. Rozložíme na transpozice postupně všechny cykly permutace. Libovolný cyklus $(u_1, \ldots, u_r)$ se rozloží

$$(u_1, \ldots, u_r) = (u_1, u_2) \circ (u_2, u_3) \circ (u_3, u_4) \circ \ldots \circ (u_{r-1}, u_r).$$ □

Poznamenejme, že rozklad na transpozice není jednoznačný, dokonce ani počet transpozic ne. Pouze jejich parita zůstane stejná.

Výše zmíněné vlastnosti mají řadu pěkných důsledků.

Důsledek 4.15. *Platí* $\operatorname{sgn}(p) = (-1)^r$*, kde* r *je počet transpozic při rozkladu* p *na transpozice.*

Důkaz. Je to důsledek věty 4.13. Vyjdeme z identity, která je sudá. Každá transpozice mění znaménko, tedy výsledné znaménko bude $(-1)^r$. □

Důsledek 4.16. *Buď* $p, q \in S_n$*. Pak* $\operatorname{sgn}(p \circ q) = \operatorname{sgn}(p)\operatorname{sgn}(q)$.

Důkaz. Nechť p se dá rozložit na r_1 transpozic a q na r_2 transpozic. Pak $\operatorname{sgn}(p \circ q) = (-1)^{r_1+r_2} = (-1)^{r_1}(-1)^{r_2} = \operatorname{sgn}(p)\operatorname{sgn}(q)$. □

Důsledek 4.17. *Buď* $p \in S_n$*. Pak* $\operatorname{sgn}(p) = \operatorname{sgn}(p^{-1})$.

Důkaz. Platí $1 = \operatorname{sgn}(id) = \operatorname{sgn}(p \circ p^{-1}) = \operatorname{sgn}(p)\operatorname{sgn}(p^{-1})$, tedy p, p^{-1} musí mít stejné znaménko. □

Poznámka 4.18. Kromě počtu cyklů a počtu transpozic jde znaménko permutace p zavést také např. pomocí počtu inverzí. Inverzí zde rozumíme uspořádanou dvojici (i, j) takovou, že $i < j$ a $p(i) > p(j)$. Označíme-li počet inverzí permutace p jako $I(p)$, pak platí $\operatorname{sgn}(p) = (-1)^{I(p)}$.

Poznámka 4.19. Vraťme se zpět ke grupám. $(S_n, \circ)$ tvoří nekomutativní grupu, tzv. *symetrickou grupu*. Hraje důležitou roli v algebře, protože se dá ukázat, že každá grupa je isomorfní nějaké symetrické grupě či její podgrupě (Cayleyova reprezentace).

Když už mluvíme o podgrupách $(S_n, \circ)$, pěkným příkladem je podgrupa sudých permutací.

Symetrické grupy a znaménko permutace se využije také při analýze hlavolamů jako je Loydova patnáctka nebo Rubikova kostka.

4.3 Tělesa

Algebraická tělesa nám zobecňují třídu tradičních oborů jako je třeba množina reálných čísel na abstraktní množinu se dvěma operacemi a řadou vlastností. To nám umožní pracovat s maticemi (sčítat, násobit, invertovat, řešit soustavy rovnic, ...) nad jinými obory než jen nad $\mathbb{R}$.

Definice 4.20 (Těleso)**.** *Tělesem* je množina $\mathbb{T}$ spolu se dvěma komutativními binárními operacemi $+$ a $\cdot$ splňující

1. $(\mathbb{T}, +)$ je Abelova grupa, neutrální prvek značíme 0 a inverzní k a pak $-a$,
2. $(\mathbb{T} \setminus \{0\}, \cdot)$ je Abelova grupa, neutrální prvek značíme 1 a inverzní k a pak a^{-1},
3. $\forall a, b, c \in \mathbb{T}$: $a(b + c) = ab + ac$ (distributivita).

Těleso se občas zavádí bez komutativity násobení a tělesu s komutativním násobením se pak říká komutativní těleso nebo pole, ale pro naše účely budeme komutativitu automaticky předpokládat. Podobně jako podgrupy můžeme zavést i pojem podtěleso jako podmnožinu tělesa, která se stejně definovanými operacemi tvoří těleso.

Příklad 4.21. Příkladem nekonečných těles je např. $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$. Množina celých čísel $\mathbb{Z}$ ale těleso netvoří, protože chybí inverzní prvky pro násobení, (např. když invertujeme hezkou celočíselnou matici, tak často vycházejí zlomky a tím pádem se dostáváme mimo obor $\mathbb{Z}$). Těleso netvoří ani čísla reprezentovaná na počítači v aritmetice s pohyblivou desetinnou čárkou – jednak nejsou operace sčítání a násobení uzavřené (pokud by výsledkem bylo hodně velké či hodně malé číslo), a jednak nejsou ani asociativní (díky zaokrouhlování). Konečná tělesa prozkoumáme později. □

Řadu pěkných vlastností zdědí těleso z vlastností příslušných grup $(\mathbb{T}, +)$ a $(\mathbb{T} \setminus \{0\}, \cdot)$. Např. distributivita zprava $(b + c)a = ba + ca$ plyne z levé distributivity a komutativity násobení. Některé specifické vlastnosti uvádíme v následující větě.

Věta 4.22 (Základní vlastnosti v tělese)**.** *Pro prvky tělesa platí následující vlastnosti.*

(1) $0a = 0$,

(2) $ab = 0$ *implikuje, že* $a = 0$ *nebo* $b = 0$.

Důkaz.

(1)
$$\begin{aligned} 0a = (0+0)a &= 0a + 0a && / + (-0a) \\ (-0a) + 0a = (0+0)a &= (-0a) + 0a + 0a \\ 0 &= 0 + 0a \\ 0 &= 0a \end{aligned}$$

(2) Jeli $a = 0$, pak věta platí. Je-li $a \neq 0$, pak existuje a^{-1} a pronásobením zleva dostaneme $a^{-1}ab = a^{-1}0$, neboli $1b = 0$. □

Druhá vlastnost (a její důkaz) předchozí věty mj. říkají, že při rozhodování zda nějaká struktura tvoří těleso nemusíme ověřovat uzavřenost násobení na $\mathbb{T} \setminus \{0\}$ (žádné dva nenulové prvky se nevynásobí na nulu), tato vlastnost vyplývá z ostatních. Stačí tedy jen uzavřenost na $\mathbb{T}$, což bývá snáze vidět.

Podívejme se teď na konečná tělesa. Zaveďme množinu $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ a operace $+$ a $\cdot$ modulo n. Snadno nahlédneme, že $\mathbb{Z}_2$ a $\mathbb{Z}_3$ je těleso, ale $\mathbb{Z}_4$ už není, neboť prvek 2 nemá inverzi 2^{-1}. Tento výsledek můžeme zobecnit.

Lemma 4.23. *Buď* p *prvočíslo a* $0 \neq a \in \mathbb{Z}_p$. *Pak* $\{0, 1, \ldots, p-1\} = \{0a, 1a, \ldots, (p-1)a\}$.

Důkaz. Sporem předpokládejme, že $ak = al$ pro nějaké $k, l \in \mathbb{Z}_p$, $k \neq l$. Pak dostáváme $a(k-l) = 0$, tudíž buď a nebo $k-l$ je dělitelné p. To znamená buď $a = 0$ nebo $k - l = 0$. Ani jedna možnost ale nastat nemůže, což je spor. □

Věta 4.24. $\mathbb{Z}_n$ *je těleso právě tehdy když* n *je prvočíslo.*

Důkaz. Je-li n složené, pak $n = pq$, kde $1 < p, q < n$. Kdyby $\mathbb{Z}_n$ bylo těleso, pak $pq = 0$ implikuje podle věty 4.22 buď $p = 0$ nebo $q = 0$, ale ani jedno neplatí.

Je-li n prvočíslo, pak se snadno ověří všechny axiomy z definice tělesa. Jediný pracnější může být existence inverze a^{-1} pro libovolné $a \neq 0$. To ale nahlédneme snadno z Lemmatu 4.23. Protože $\{0, 1, \ldots, n-1\} = \{0a, 1a, \ldots, (n-1)a\}$, musí být v množině napravo prvek 1 a tudíž existuje $b \in \mathbb{Z}_n$ tak, že $ab = 1$. □

Poznámka 4.25. Soustavy rovnic a operace s maticemi jsme zaváděli nad tělesem reálných čísel. Nicméně nic nám nebrání rozšířit tyto pojmy a pracovat nad jakýmkoli jiným tělesem. Jediné vlastnosti reálných čísel, který jsme používali, jsou přesně ty, které se vyskytují v definici tělesa. Proto platí postupy a věty z předchozích kapitol i když pracujeme nad libovolným tělesem.

Příklad 4.26 (Těleso $\mathbb{Z}_5$)**.** Operace nad $\mathbb{Z}_5$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Inverzní prvky:

x	0	1	2	3	4
$-x$	0	4	3	2	1

x	0	1	2	3	4
x^{-1}	–	1	3	2	4

Výpočet inverzní matice nad $\mathbb{Z}_5$

$$(A\,|\,I_3) = \left(\begin{array}{ccc|ccc} 1&2&3&1&0&0\\ 2&0&4&0&1&0\\ 3&3&4&0&0&1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1&2&3&1&0&0\\ 0&1&3&3&1&0\\ 0&2&0&2&0&1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1&0&2&0&3&0\\ 0&1&3&3&1&0\\ 0&0&4&1&3&1 \end{array}\right) \sim$$
$$\sim \left(\begin{array}{ccc|ccc} 1&0&2&0&3&0\\ 0&1&3&3&1&0\\ 0&0&1&4&2&4 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1&0&0&2&4&2\\ 0&1&0&1&0&3\\ 0&0&1&4&2&4 \end{array}\right) = \left(I_3\,|\,A^{-1}\right)$$

□

Nyní víme, že existují tělesa o velikostech odpovídajícím prvočíslům. Existují však tělesa jiných velikostí?

Věta 4.27. *Existují konečná tělesa právě o velikostech p^n, kde p je prvočíslo a $n \geq 1$.*

Důkaz vynecháme, ale ukážeme základní myšlenku jak sestrojit těleso o velikosti p^n. Takové těleso se značí $\mathrm{GF}(p^n)$[1)] a jeho prvky jsou polynomy stupně nanejvýš $n-1$ s koeficienty v tělese $\mathbb{Z}_p$. Sčítání je definováno analogicky jako pro reálné polynomy. Násobí se modulo ireducibilní polynom stupně n, kde ireducibilní znamená nerozložitelný na součin dvou polynomů stupně aspoň jedna (takový polynom vždy existuje).

Příklad 4.28 (Těleso GF(8))**.** Množina má za prvky polynomy stupňů nanejvýš dva s koeficienty v $\mathbb{Z}_2$

$$\mathrm{GF}(8) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}.$$

Sčítání je definované

$$(a_2x^2 + a_1x + a_0) + (b_2x^2 + b_1x + b_0) = (a_2+b_2)x^2 + (a_1+b_1)x + (a_0+b_0),$$

např. $(x+1) + (x^2+x) = x^2+1$. Uvažme ireducibilní polynom např. x^3+x+1. Pak násobíme modulo tento polynom, např. $x^2 \cdot x = -x-1 = x+1$, nebo $x^2 \cdot (x^2+1) = -x = x$. □

Definice 4.29 (Charakteristika tělesa)**.** *Charakteristika tělesa* $\mathbb{T}$ je nejmenší n takové, že $\underbrace{1+1+\cdots+1}_{n} = 0$. Pokud takové n neexistuje pak ji definujeme jako 0.

Věta 4.30. *Charakteristika tělesa je buď nula nebo prvočíslo.*

Důkaz. Protože $0 \neq 1$, tak charakteristika nemůže být 1. Pokud je charakteristika složené číslo $n = pq$, pak $0 = \underbrace{1+1+\cdots+1}_{n=pq} = (\underbrace{1+\cdots+1}_{p})(\underbrace{1+\cdots+1}_{q})$, tedy součet p nebo q jedniček dá nulu, což je spor s minimalitou n. □

Příklad 4.31. Pokud charakteristika tělesa $\mathbb{T}$ není 2, tak můžeme zavést něco jako průměr. Označme symbolem 2 hodnotu $1+1$ a pak pro libovolné $a, b \in \mathbb{T}$ má číslo $p = \frac{1}{2}(a+b)$ má vlastnost $a - p = p - b$. (Viz důkaz Věty 7.2 či Příklad 12.4.)

Tedy např. zatímco v Z_2 průměr 0 a 1 nelze zadefinovat, tak v tělese Z_5 je průměr 0 a 1 číslo 3. □

Další užitečný výsledek je *Malá Fermatova věta*[2)], používá se např. pro pravděpodobnostní test prvočíselnosti velkých čísel. Často se uvádí ve znění, že $a^{p-1} \equiv 1 \mod p$, tedy, že čísla a^{p-1} a 1 mají stejný zbytek při dělení číslem p. V jazyce konečných těles větu formulujeme takto:

Věta 4.32 (Malá Fermatova věta)**.** *Buď p prvočíslo a $0 \neq a \in \mathbb{Z}_p$. Pak $a^{p-1} = 1$ v tělese $\mathbb{Z}_p$.*

Důkaz. Podle Lemmatu 4.23 je $\{0, 1, \ldots, p-1\} = \{0a, 1a, \ldots, (p-1)a\}$. Protože $0 = 0a$, tak dostáváme $\{1, \ldots, p-1\} = \{1a, \ldots, (p-1)a\}$. Tudíž $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = (1a) \cdot (2a) \cdot (3a) \cdot \ldots \cdot (p-1)a$. Zkrácením obou stran čísly $1, 2, \ldots, p-1$ získáme požadovanou rovnost $1 = a \cdot \ldots \cdot a$. □

[1)] GF = Galois field, tedy Galoisovo těleso.

[2)] Malá Fermatova věta byla formulována francouzským právníkem a amatérským matematikem Pierre de Fermatem r. 1640. Velká Fermatova věta z r. 1637 pak říká, že neexistují přirozená čísla x, y, z splňující rovnici $x^n + y^n = z^n$ pro $n > 2$. Tato věta zůstávala dlouho jako otevřený problém bez důkazu až ji r. 1993 dokázal britský matematik Andrew Wiles.

4.4 Aplikace

Konečná tělesa se používají např. v kódování a šifrování. Na závěr této sekce si ukážeme praktické využití těles právě v kódování, viz [Tůma, 2003, kap. 11]. Jinou ukázkou použití je tzv. „Secret sharing“, viz [Tůma, 2003, kap. 4].

Příklad 4.33 (Samoopravné kódy – Hammingův kód $(7,4,3)$)**.** Hammingův kód $(7,4,3)$ spočívá v rozdělení přenosových dat na sekvence o čtyřech bitech, které zakódujeme na sedm bitů, které přeneseme. Tento kód umí detekovat a opravit jednu přenosovou chybu.

Vstupní 4 bity (= čtyři čísla v $\mathbb{Z}_2$) zakódujeme na 7 vynásobením tzv. generující maticí $H \in \mathbb{Z}_2^{7\times 4}$,

$$\text{např.: } Ha = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \mathbf{0} \\ \mathbf{1} \\ \mathbf{1} \\ \mathbf{0} \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \mathbf{0} \\ 0 \\ \mathbf{1} \\ \mathbf{1} \\ \mathbf{0} \end{pmatrix} = b.$$

Příjemce používá detekční matici $D \in \mathbb{Z}_2^{3\times 7}$. Kontrola po přijetí: $Db = 0$ znamená vše v pořádku (nebo více jak dvě chyby v přenosu), jinak nastala přenosová chyba a víme kde,

$$\text{např.: } Db = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \ldots \text{v pořádku.}$$

$$\text{např.: } Db = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ \mathbf{0} \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \ldots \text{chyba na pozici } 110_2 = 6.$$

□

Kapitola 5

Vektorové prostory

Vektorové prostory nám zobecňují dobře známý prostor aritmetických vektorů $\mathbb{R}^n$. Stejně jako u grup a těles je zavedeme pomocí abstraktních axiomů.

Vektorové prostory byly zavedeny „zapomenutým“ německým filosofem Hermannem Grassmannem (1809–1877), kterého znovuobjevil italský matematik Giuseppe Peano (1858–1932). Současné verze definice pochází od německého matematika Hermanna Weyla (1885–1955).

Poznamenejme, že v některých odvětvích se vektorové prostory označují také jako *lineární prostory*.

5.1 Základní pojmy

Definice 5.1 (Vektorový prostor)**.** Buď $\mathbb{T}$ těleso s neutrálními prvky 0 pro sčítání a 1 pro násobení. *Vektorovým prostorem nad tělesem* $\mathbb{T}$ rozumíme množinu V s operacemi sčítání vektorů $+ : V^2 \mapsto V$, násobení vektoru skalárem $\cdot : T \times V \mapsto V$ splňující pro každé $\alpha, \beta \in \mathbb{T}$ a $u, v \in V$:

1. $(V, +)$ je Abelova grupa, neutrální prvek značíme o a inverzní k v pak $-v$,
2. $\alpha(\beta v) = (\alpha\beta)v$ (asociativita),
3. $1v = v$
4. $(\alpha + \beta)v = \alpha v + \beta v$ (distributivita),
5. $\alpha(u + v) = \alpha u + \alpha v$ (distributivita).

Vektory budeme značit latinkou a jejich násobky (skaláry) řeckými písmeny. Vektory píšeme bez šipek, tedy v, a ne $\vec{v}$.

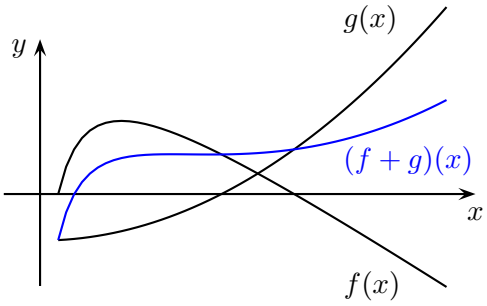
Příklad 5.2. Příklady vektorových prostorů:

- Aritmetický prostor $\mathbb{R}^n$ nad $\mathbb{R}$, či obecněji $\mathbb{T}^n$ nad $\mathbb{T}$, kde $\mathbb{T}$ je libovolné těleso; n-tice prvků z tělesa $\mathbb{T}$ sčítáme a násobíme skalárem podobně jako u $\mathbb{R}^n$.
- Prostor matic $\mathbb{R}^{m\times n}$ nad $\mathbb{R}$, či obecněji $\mathbb{T}^{m\times n}$ nad $\mathbb{T}$.
- Prostor všech reálných polynomů proměnné x, značíme $\mathcal{P}$.
- Prostor všech reálných polynomů proměnné x stupně nanejvýš n, značíme $\mathcal{P}^n$.
  - Sčítání:
$$(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) + (b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0) = \\ (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$
  - Násobení skalárem $\alpha \in \mathbb{R}$:
$$\alpha(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) = (\alpha a_n)x^n + (\alpha a_{n-1})x^{n-1} + \cdots + (\alpha a_1)x + (\alpha a_0)$$
  - Nulový vektor: 0

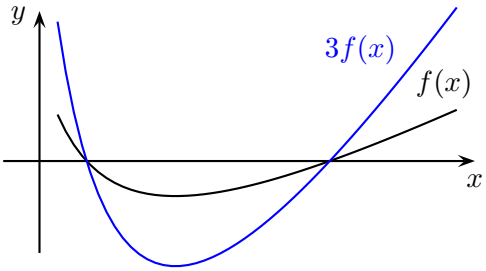
– Opačný vektor:

$$-(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) = (-a_n)x^n + (-a_{n-1})x^{n-1} + \cdots + (-a_1)x + (-a_0)$$

- Prostor všech reálných funkcí $f : \mathbb{R} \mapsto \mathbb{R}$, značíme $\mathcal{F}$.



Součet vektorů.



Vynásobení vektoru skalárem.

□

Věta 5.3 (Základní vlastnosti vektorů)**.** *V prostoru V nad $\mathbb{T}$ platí:*

(1) $\forall v \in V : 0v = o$,

(2) $\forall \alpha \in \mathbb{T} : \alpha o = o$,

(3) $\forall v \in V\ \forall \alpha \in \mathbb{T} : \alpha v = o$ *implikuje, že* $\alpha = 0$ *nebo* $v = o$,

(4) $\forall v \in V : (-1)v = -v$.

Důkaz. Analogicky jako u vlastností v tělese. □

5.2 Podprostory

Definice 5.4 (Podprostor)**.** Buď V vektorový prostor nad $\mathbb{T}$. Pak $U \subseteq V$ je *podprostorem* V pokud nad $\mathbb{T}$ tvoří vektorový prostor nad T se stejně definovanými operacemi. Značení: $U \Subset V$.

Jinými slovy, U musí obsahovat nulový vektor a splňovat uzavřenost na obě operace. To jest, pro každé $u, v \in U$ je $u + v \in U$, a pro každé $\alpha \in \mathbb{T}$ a $u \in U$ je $\alpha u \in U$.

Příklad 5.5. Příklady vektorových podprostorů:

- Dva triviální podprostory prostoru V jsou: V a $\{o\}$.
- $\mathcal{P}^n \Subset \mathcal{P} \Subset \mathcal{F}$.
- Symetrické matice v $\mathbb{R}^{n\times n}$.
- $\mathbb{Q}^n$ nad $\mathbb{Q}$ je podprostorem $\mathbb{R}^n$ nad $\mathbb{Q}$, ale není podprostorem $\mathbb{R}^n$ nad $\mathbb{R}$.
- Jsou-li U, V podprostory W, a platí $U \subseteq V$, pak $U \Subset V$. □

Nyní si ukážeme, že průnik libovolného systému (i nekonečného nespočetného) podprostorů je zase podprostor. Pro sjednocení tato vlastnost obecně neplatí (najděte protipříklad).

Věta 5.6 (Průnik podprostorů)**.** *Buď V vektorový prostor nad $\mathbb{T}$, a mějme V_i, $i \in I$ libovolný systém podprostorů V. Pak $\bigcap_{i\in I} V_i$ je opět podprostor V.*

Důkaz. Stačí ověřit tři vlastnosti: Protože $o \in V_i$ pro každé $i \in I$, musí být i v jejich průniku. Uzavřenost na sčítání: Buď $u, v \in \bigcap_{i\in I} V_i$, tj. pro každé $i \in I$ je $u, v \in V_i$, tedy i $u + v \in V_i$. Proto $u + v \in \bigcap_{i\in I} V_i$. Analogicky uzavřenost na násobky: Buď $\alpha \in \mathbb{T}$ a $v \in \bigcap_{i\in I} V_i$, tj. pro každé $i \in I$ je $v \in V_i$, tedy i $\alpha v \in V_i$. Proto $\alpha v \in \bigcap_{i\in I} V_i$. □

Tato vlastnost nás opravňuje k následující definici.

Definice 5.7 (Lineární obal)**.** Buď V vektorový prostor nad $\mathbb{T}$, a $W \subseteq V$. Pak *lineární obal* W, značený $\operatorname{span}(W)$, je průnik všech podprostorů V obsahujících W, to jest $\operatorname{span}(W) = \bigcap_{U:W\subseteq U\in V} U$.

Z jiného pohledu, lineární obal množiny W je tedy nejmenší (co do inkluze) prostor obsahující W. Ještě k terminologii: Říkáme, že W *generuje* prostor $\operatorname{span}(W)$, a prvky množiny W jsou *generátory* prostoru $\operatorname{span}(W)$. Prostor je *konečně generovaný* pokud je generovaný nějakou konečnou množinou.

Příklad 5.8. Příklady lineárních obalů:

- $\operatorname{span}\{(1,0)^T\}$ je přímka v rovině, konkrétně osa x_1. Je to tedy konečně generovaný podprostor $\mathbb{R}^2$.
- $\operatorname{span}\{(1,0)^T, (2,0)^T\}$ je totéž.
- $\operatorname{span}\{(1,1)^T, (1,2)^T\}$ je celá rovina $\mathbb{R}^2$.
- $\operatorname{span}\{\} = \{o\}$. □

Proč jsme označili obal jako lineární? Odpověď se nazývá vyjádření lineárního obalu pomocí lineárních kombinací.

Definice 5.9 (Lineární kombinace)**.** Buď V vektorový prostor nad $\mathbb{T}$ a $v_1 \ldots, v_n \in V$. Pak *lineární kombinací* rozumíme výraz typu $\sum_{i=1}^n \alpha_i v_i = \alpha_1 v_1 + \cdots + \alpha_n v_n$, kde $\alpha_1, \ldots, \alpha_n \in \mathbb{T}$.

Poznámka 5.10. Vyjádření typu $v_1, \ldots, v_n$ jsme doposud používali výhradně pro jednotlivé složky aritmetického vektoru $v = (v_1, \ldots, v_n)$. Nicméně, nyní ho budeme používat spíše pro n nějakých vektorů. Význam by však měl být vždy jasný z kontextu.

Věta 5.11. *Buď V vektorový prostor nad $\mathbb{T}$, a mějme $v_1, \ldots, v_n \in V$. Pak*

$$\operatorname{span}\{v_1, \ldots, v_n\} = \{\textstyle\sum_{i=1}^n \alpha_i v_i;\ \alpha_1, \ldots, \alpha_n \in \mathbb{T}\}\,. \tag{5.1}$$

Důkaz. Inkluze „$\supseteq$“. $\operatorname{span}\{v_1, \ldots, v_n\}$ je podprostor V obsahující vektory $v_1, \ldots, v_n$, tedy musí být uzavřený na násobky a součty. Tudíž obsahuje i násobky $\alpha_i v_i$, $i = 1, \ldots, n$, a také jejich součet $\sum_{i=1}^n \alpha_i u_i$.

Inkluze „$\subseteq$“. Stačí ukázat, že množina napravo ve výrazu (5.1) je vektorový podprostor V obsahující vektory $v_1, \ldots, v_n$, a proto je jednou z množin, jejichž průnikem $\operatorname{span}\{v_1, \ldots, v_n\}$ vzniklo. Pro každé i je vektor v_i v této množině obsažen, stačí vzít lineární kombinaci s $\alpha_i = 1$ a $\alpha_j = 0$, $j \neq i$. Nulový vektor rovněž obsahuje, vezměme lineární kombinaci s nulovými koeficienty. Uzavřenost na součty: vezměme libovolné dva vektory této množiny, $u = \sum_{i=1}^n \beta_i v_i$, $u' = \sum_{i=1}^n \beta'_i v_i$. Pak $u + u' = \sum_{i=1}^n \beta_i v_i + \sum_{i=1}^n \beta'_i v_i = \sum_{i=1}^n (\beta_i + \beta'_i) v_i$, což je prvek množiny. Podobně pro násobky, buď $\alpha \in \mathbb{T}$, pak $\alpha u = \alpha \sum_{i=1}^n \beta_i v_i = \sum_{i=1}^n (\alpha\beta_i) v_i$, což opět náleží do množiny. □

Příklad 5.12. Trochu jiný pohled na soustavu rovnic $Ax = b$. Výraz Ax je vlastně lineární kombinace sloupců matice A, takže řešit soustavu znamená hledat lineární kombinaci sloupců, která dá b. Řešení tedy existuje pokud b náleží do podprostoru generovaného sloupci matice A. □

5.3 Lineární nezávislost

Motivací pro tuto podkapitolu je snaha najít pro daný konečně generovaný podprostor minimální (co do počtu i co do inkluze) množinu generátorů, což vede k pojmu báze. Rovněž budeme chtít zavést v prostorech pojmy jako souřadnice, souřadný systém a dimenze.

Definice 5.13 (Lineární nezávislost)**.** Buď V vektorový prostor nad $\mathbb{T}$ a $v_1 \ldots, v_n \in V$. Pak vektory $v_1 \ldots, v_n$ se nazývají *lineárně nezávislé* pokud rovnost $\sum_{i=1}^n \alpha_i v_i = o$ nastane pouze pro $\alpha_1 = \cdots = \alpha_n = 0$. V opačném případě jsou vektory *lineárně závislé*.

Tedy vektory $v_1 \ldots, v_n$ jsou lineárně závislé pokud existují $\alpha_1, \ldots, \alpha_n \in \mathbb{T}$, ne všechna nulová a taková, že $\sum_{i=1}^n \alpha_i v_i = o$.

Lineární nezávislost se dá zobecnit i na nekonečné množiny vektorů, nicméně s nekonečny bývá trochu potíž (např. co se myslí nekonečnou řadou?), takže se to musí obejít, třeba tak, že každá konečná podmnožina je lineárně nezávislá. V našem výkladu se ale omezíme pouze na konečný případ.

Příklad 5.14. Příklady lineárně (ne)závislých vektorů v $\mathbb{R}^2$:

- $(1,0)$ je lineárně nezávislý,
- $(1,0)$, $(2,0)$ jsou lineárně závislé,
- $(1,1)$, $(1,2)$ jsou lineárně nezávislé,
- $(0,0)$ je lineárně závislý,
- prázdná množina je lineárně nezávislá. □

Příklad 5.15. Definice lineární nezávislosti trochu připomíná definici regularity (df. 3.17). Není to náhoda, sloupce regulární matice (a potažmo i řádky) představují další příklad lineárně nezávislých vektorů. □

Věta 5.16. *Buď V vektorový prostor nad $\mathbb{T}$, a mějme $v_1, \ldots, v_n \in V$. Pak vektory $v_1 \ldots, v_n$ jsou lineárně závislé právě tehdy když existuje $k \in \{1, \ldots, n\}$ takové, že $v_k = \sum_{i \neq k} \alpha_i v_i$ pro nějaké $\alpha_1, \ldots, \alpha_n \in \mathbb{T}$, to jest $v_k \in \operatorname{span}\{v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n\}$.*

Důkaz. Implikace „⇒“. Jsou-li vektory $v_1, \ldots, v_n$ lineárně závislé, pak existuje jejich netriviální lineární kombinace rovna nule, tj. $\sum_{i=1}^{n} \beta_i v_i = o$ pro $\beta_1, \ldots, \beta_n \in \mathbb{T}$ a $\beta_k \neq 0$ pro nějaké $k \in \{1, \ldots, n\}$. Vyjádříme si k-tý člen $\beta_k v_k = -\sum_{i \neq k} \beta_i v_i$, a po zkrácení dostáváme požadovaný předpis $v_k = \sum_{i \neq k} (-\beta_k^{-1} \beta_i) v_i$.

Implikace „⇐“. Je-li $v_k = \sum_{i \neq k} \alpha_i v_i$, pak $v_k - \sum_{i \neq k} \alpha_i v_i = o$, což je požadovaná netriviální kombinace rovna nule, neboť koeficient u v_k je $1 \neq 0$. □

Věta nám dává i jinou charakterizaci lineární závislosti.

Důsledek 5.17. *Buď V vektorový prostor nad $\mathbb{T}$, a mějme $v_1, \ldots, v_n \in V$. Pak vektory $v_1 \ldots, v_n$ jsou lineárně závislé právě tehdy když existuje $k \in \{1, \ldots, n\}$ takové, že*

$$\operatorname{span}\{v_1, \ldots, v_n\} = \operatorname{span}\{v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n\}. \tag{5.2}$$

Důkaz. Implikace „⇒“. Jsou-li vektory $v_1, \ldots, v_n$ lineárně závislé, pak podle Věty 5.16 existuje $k \in \{1, \ldots, n\}$ takové, že $v_k = \sum_{i \neq k} \alpha_i v_i$ pro nějaké $\alpha_1, \ldots, \alpha_n \in \mathbb{T}$. Inkluze $\supseteq$ v (5.2) je splněna triviálně, zaměříme se na tu opačnou. Libovolný vektor $u \in \operatorname{span}\{v_1, \ldots, v_n\}$ se dá vyjádřit

$$u = \sum_{i=1}^{n} \beta_i v_i = \beta_k v_k + \sum_{i \neq k} \beta_i v_i = \beta_k \Big(\sum_{i \neq k} \alpha_i v_i \Big) + \sum_{i \neq k} \beta_i v_i = \sum_{i \neq k} (\beta_k \alpha_i + \beta_i) v_i$$

Tedy $u \in \operatorname{span}\{v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n\}$ a máme $\operatorname{span}\{v_1, \ldots, v_n\} \subseteq \operatorname{span}\{v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n\}$.

Implikace „⇐“. Pokud platí rovnost (5.2), tak $v_k \in \operatorname{span}\{v_1, \ldots, v_n\} = \operatorname{span}\{v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n\}$ a podle Věty 5.16 jsou vektory $v_1, \ldots, v_n$ lineárně závislé. □

Věta mj. říká i to, že vektory jsou lineárně závislé právě tehdy když odebráním nějakého (ale ne libovolného) z nich se jejich lineární obal nezmenší. Tedy mezi nimi je nějaký nadbytečný. U lineárně nezávislého systému je tomu naopak: Odebráním libovolného z nich se jejich lineární obal ostře zmenší. Tedy mezi nimi není žádný nadbytečný.

5.4 Báze

Definice 5.18 (Báze)**.** Buď V konečně generovaný vektorový prostor nad $\mathbb{T}$. Pak *bází* rozumíme jakýkoli lineárně nezávislý systém generátorů V.

Systémem rozumíme uspořádanou množinu, časem uvidíme, proč je uspořádání důležité (pro souřadnice atp.).

Proč bázi definujeme pouze pro konečně generované prostory? Pro nekonečně generované potřebujeme rozšířit pojem lineární nezávislosti na nekonečné množiny. To lze učinit pomocí nekonečných součtů (pak ale musíme mít na prostoru metriku, topologii či něco podobného) nebo, jak se to standardně dělá, to obejít pomocí konečných součtů. Každopádně si to trochu zjednodušíme a omezíme jen na konečně generované prostory.

Příklad 5.19. Příklady bází:

- V $\mathbb{R}^2$ máme bázi např. $e_1 = (1,0)^T$, $e_2 = (0,1)^T$. Jiná báze je $(7,5)^T$, $(2,3)^T$.
- V $\mathbb{R}^n$ máme např. bázi $e_1, \ldots, e_n$, říká se jí *kanonická*.
- V $\mathcal{P}^n$ je bází např. $1, x, x^2, \ldots, x^n$. Je to nejjednodušší, nikoliv však jediná možná. Užitečná je i Bernsteinova báze skládající se z vektorů $\binom{n}{i}x^i(1-x)^{n-i}$, používá se např. ve výpočetní geometrii pro aproximaci křivek procházejících danými body (tzv. Bézierovy křivky). □

Věta 5.20. *Nechť $v_1, \ldots, v_n$ je báze prostoru V. Pak pro každý vektor $u \in V$ existují jednoznačně určené koeficienty $\alpha_1, \ldots, \alpha_n \in \mathbb{T}$ takové, že $u = \sum_{i=1}^n \alpha_i v_i$.*

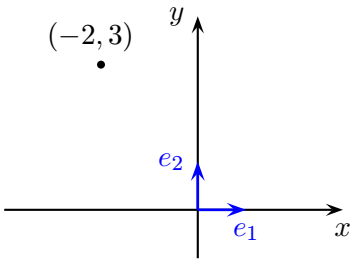
Důkaz. Vektory $v_1, \ldots, v_n$ tvoří bázi V, tedy každé $u \in V$ se dá vyjádřit jako $u = \sum_{i=1}^n \alpha_i v_i$ pro vhodné skaláry. Jednoznačnost ukážeme sporem. Nechť existuje i jiné vyjádření $u = \sum_{i=1}^n \beta_i v_i$. Potom $\sum_{i=1}^n \alpha_i v_i - \sum_{i=1}^n \beta_i v_i = u - u = o$, neboli $\sum_{i=1}^n (\alpha_i - \beta_i) v_i = o$. Protože $v_1, \ldots, v_n$ jsou lineárně nezávislé, musí $\alpha_i = \beta_i$ pro každé $i = 1 \ldots, n$. To je spor s tím, že vyjádření jsou různá. □

Díky zmíněné jednoznačnosti můžeme zavést pojem souřadnice.

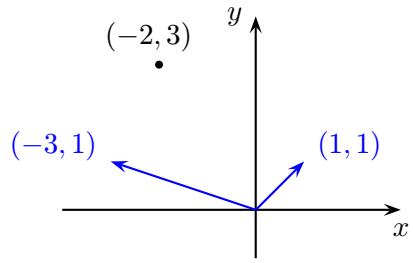
Definice 5.21 (Souřadnice)**.** Nechť $B = \{v_1, \ldots, v_n\}$ je báze prostoru V a nechť vektor $u \in V$ má vyjádření $u = \sum_{i=1}^n \alpha_i v_i$. Pak *souřadnicemi* vektoru $u \in V$ vzhledem k dané bázi rozumíme koeficienty $\alpha_1, \ldots, \alpha_n$ a vektor souřadnic značíme $[u]_B := (\alpha_1, \ldots, \alpha_n)^T$.

Pojem souřadnic je důležitější než se na první pohled zdá. Umožňuje totiž reprezentovat těžko uchopitelné vektory a (konečně generované) prostory pomocí souřadnic, tedy aritmetických vektorů. Každý vektor má určité souřadnice a naopak každá n-tice skalárů dává souřadnici nějakého vektoru. Existuje tedy vzájemně jednoznačný vztah mezi vektory a souřadnicemi, který později (Sekce 6.2) využijeme k tomu, abychom řadu (např. početních) problémů z prostoru V převedli do aritmetického prostoru, kde se pracuje snadněji.

Příklad 5.22. Souřadnice vektoru vzhledem k bázi v prostoru $\mathbb{R}^2$.



Souřadnice vektoru $(-2,3)$ vzhledem ke kanonické bázi: $[(-2,3)]_{\text{kan}} = (-2,3)$.



Souřadnice vektoru $(-2,3)$ vzhledem k bázi $B = \{(-3,1),(1,1)\}$: $[(-2,3)]_B = (\frac{5}{4}, \frac{7}{4})$.

□

Příklad 5.23. Pro každé $x \in \mathbb{R}^n$ je $[x]_{\text{kan}} = x$, kde kan značí kanonickou bázi. □

Příklad 5.24.

- Je-li $v_1, \ldots, v_n \in V$ systém generátorů V, pak každý vektor $u \in V$ lze vyjádřit jako lineární kombinaci vektorů $v_1, \ldots, v_n$ alespoň jedním způsobem.
- Jsou-li $v_1, \ldots, v_n \in V$ lineárně nezávislé, pak každý vektor $u \in V$ lze vyjádřit jako lineární kombinaci vektorů $v_1, \ldots, v_n$ nejvýše jedním způsobem.
- Je-li $v_1, \ldots, v_n \in V$ báze V, pak každý vektor $u \in V$ lze vyjádřit jako lineární kombinaci vektorů $v_1, \ldots, v_n$ právě jedním způsobem. □

Věta 5.25 (O existenci báze)**.** *Každý konečně generovaný vektorový prostor V má bázi.*

Důkaz. Definujme množinu $M = \{m \in \mathbb{N};\ \text{V má systém generátorů o } m \text{ prvcích}\}$. Z předpokladu je $M \neq \emptyset$ a zdola omezená množina, tedy má minimum m_0. Označme jemu odpovídající generátory $v_1 \ldots, v_{m_0}$. Jsou-li lineárně nezávislé, pak tvoří bázi a jsme hotovi. Jsou-li lineárně závislé, pak podle Důsledku 5.17 existuje index k tak, že

$$\operatorname{span}\{v_1, \ldots, v_{m_0}\} = \operatorname{span}\{v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_{m_0}\}.$$

To je ale spor s minimalitou m_0. □

Důkaz jen formalizuje to, že z konečné množiny generátorů prostoru V postupně odstraníme ty lineárně závislé až nám zbyde báze. Věta jde zobecnit pomocí axiomu výběru na libovolné prostory, ale to je nad rámec tohoto výkladu.

Nyní směřujeme k tomu, že pro daný konečně generovaný prostor jsou všechny jeho báze stejně velké, což povede k zavedení pojmu dimenze.

Věta 5.26 (Steinitzova věta o výměně[1])**.** *Buď V vektorový prostor V, buď $x_1, \ldots, x_m$ lineárně nezávislý systém ve V, a nechť $y_1, \ldots, y_n$ jsou generátory V. Pak platí*

(1) $m \leq n$,

(2) existují navzájem různé indexy $k_1, \ldots, k_{n-m}$ tak, že $x_1, \ldots, x_m, y_{k_1}, \ldots, y_{k_{n-m}}$ jsou generátory V.

Důkaz. Důkaz provedeme matematickou indukcí podle m. Je-li $m = 0$, pak tvrzení platí triviálně. Přejděme k indukčnímu kroku. Předpokládejme, že tvrzení platí pro $m-1$ a ukážeme, že platí i pro m.

Uvažujme vektory $x_1, \ldots, x_{m-1}$. Ty jsou lineárně nezávislé, a podle indukčního předpokladu je $m-1 \leq n$ a existují navzájem různé indexy $l_1, \ldots, l_{n-m+1}$ takové, že $x_1, \ldots, x_{m-1}, y_{l_1}, \ldots, y_{l_{n-m+1}}$ generují V. Kdyby $m - 1 = n$, pak jsou generátory prostoru V vektory $x_1, \ldots, x_{m-1}$, a dostáváme $x_m \in V = \operatorname{span}\{x_1, \ldots, x_{m-1}\}$, což je spor s lineární nezávislostí $x_1, \ldots, x_m$. Tudíž jsme dokázali první tvrzení $m \leq n$.

Pro důkaz druhé části uvažujme lineární kombinaci $x_m = \sum_{i=1}^{m-1} \alpha_i x_i + \sum_{j=1}^{n-m+1} \beta_j y_{l_j}$, což si můžeme dovolit díky tomu, že vektory v sumě generují V. Kdyby $\beta_1 = \cdots = \beta_{n-m+1} = 0$, pak dostáváme spor s lineární nezávislostí $x_1, \ldots, x_m$. Proto existuje k takové, že $\beta_k \neq 0$. Idea zbytku důkazu je vyměnit y_{l_k} za x_m. Z rovnosti si vyjádříme

$$y_{l_k} = \frac{1}{\beta_k}\Big(x_m - \sum_{i=1}^{m-1} \alpha_i x_i - \sum_{j=1, j\neq k}^{n-m+1} \beta_j y_{l_j}\Big).$$

Chceme dokázat, že $x_1, \ldots, x_m, y_{l_1}, \ldots, y_{l_{k-1}}, y_{l_{k+1}}, \ldots, y_{l_{n-m+1}}$ generují V. Vezměme libovolný vektor $x \in V$ a můžeme ho vyjádřit pro vhodné koeficienty γ_i, δ_j jako

$$\begin{aligned} x &= \sum_{i=1}^{m-1} \gamma_i x_i + \sum_{j=1}^{n-m+1} \delta_j y_{l_j} = \sum_{i=1}^{m-1} \gamma_i x_i + \sum_{j=1, j\neq k}^{n-m+1} \delta_j y_{l_j} + \frac{\delta_k}{\beta_k}\Big(x_m - \sum_{i=1}^{m-1} \alpha_i x_i - \sum_{j=1, j\neq k}^{n-m+1} \beta_j y_{l_j}\Big) \\ &= \sum_{i=1}^{m-1} \Big(\gamma_i - \frac{\delta_k}{\beta_k}\alpha_i\Big) x_i + \frac{\delta_k}{\beta_k} x_m + \sum_{j=1, j\neq k}^{n-m+1} \Big(\delta_j - \frac{\delta_k}{\beta_k}\beta_j\Big) y_{l_j}. \end{aligned}$$

□

Důsledek 5.27. *Všechny báze konečně generovaného vektorového prostoru V jsou stejně velké.*

Důkaz. Buďte $x_1, \ldots, x_m$ a $y_1, \ldots, y_n$ dvě báze prostoru V. Speciálně, $x_1, \ldots, x_m$ jsou lineárně nezávislé a $y_1, \ldots, y_n$ jsou generátory V, tedy $m \leq n$. Analogicky naopak, $y_1, \ldots, y_n$ jsou lineárně nezávislé a $x_1, \ldots, x_m$ generují V, tedy $n \leq m$. Dohromady dostáváme $m = n$. □

5.5 Dimenze

Každý konečně generovaný prostor má bázi (Věta 5.25) a všechny báze jsou stejně velké (Důsledek 5.27), což nás ospravedlňuje zavést jeho dimenzi jako velikost (libovolné) báze.

[1] V angličtině *replacement theorem*, autorem je matematik Ernst Steinitz (1871–1928) z dříve německého, dnes polského Slezska.

Definice 5.28 (Dimenze)**.** *Dimenze* konečně generovaného vektorového prostoru V je velikost jeho nějaké báze. Značíme $\dim V$.

Příklad 5.29. Příklady dimenzí:

- $\dim \mathbb{R}^n = n$, $\dim \mathbb{R}^{m\times n} = mn$, $\dim \{o\} = 0$, $\dim \mathcal{P}^n = n+1$,
- prostory $\mathcal{P}$, $\mathcal{F}$, a $\mathbb{R}^n$ nad $\mathbb{Q}$ nejsou konečně generované (jako by měly nekonečnou dimenzi). □

Věta 5.30 (Vztah počtu prvků systému k dimenzi)**.** *Buď V konečně generovaný vektorový prostor V. Pak platí*

(1) Nechť $x_1 \dots, x_m$ jsou lineárně nezávislé. Pak $m \le \dim V$. Pokud $m = \dim V$, potom $x_1 \dots, x_m$ je báze.

(2) Nechť $y_1 \dots, y_n$ jsou generátory V. Pak $n \ge \dim V$. Pokud $n = \dim V$, potom $y_1 \dots, y_n$ je báze.

Důkaz. Označme $d = \dim V$ a nechť $z_1, \dots, z_d$ je báze V.

(1) Protože $x_1 \dots, x_m$ jsou lineárně nezávislé, podle Steinitzovy věty 5.26 je $m \le d$. Pokud $m = d$, pak podle stejné věty lze systém $x_1 \dots, x_m$ doplnit o $d - m = 0$ vektorů na generátory prostoru V. Tedy jsou to nutně i generátory a tím i báze.

(2) Protože $y_1 \dots, y_n$ jsou generátory V, podle Steinitzovy věty 5.26 je $n \ge d$. Nechť $n = d$. Jsou-li $y_1 \dots, y_n$ lineárně nezávislé, pak tvoří bázi. Pokud jsou lineárně závislé, pak lze jeden vynechat a získat systém generátorů o velikosti $n - 1$ (Důsledek 5.17). Podle Steinitzovy věty by pak ale platilo $d \le n - 1$, což vede ke sporu. □

Na bázi sa dá tedy nahlížet jako na největší lineárně nezávislý systém, nebo taky jako na nejmenší systém generátorů (co do inkluze i co do počtu).

Věta 5.31 (Rozšíření lineárně nezávislého systému na bázi)**.** *Každý lineárně nezávislý systém konečně generovaného vektorového prostoru lze rozšířit na bázi.*

Důkaz. Nechť $x_1 \dots, x_m$ jsou lineárně nezávislé a $z_1, \dots, z_d$ je báze V. Podle Steinitzovy věty 5.26 existují indexy $k_1, \dots, k_{d-m}$ tak, že $x_1 \dots, x_m, z_{k_1}, \dots, z_{k_{d-m}}$ jsou generátory V. Jejich počet je d, tedy podle věty 5.30 je to báze V. □

Věta 5.32 (Dimenze podprostoru)**.** *Každý podprostor W konečně generovaného vektorového prostoru V je konečně generovaný a platí* $\dim W \le \dim V$. *Navíc, pokud* $\dim W = \dim V$, *tak $W = V$.*

Důkaz. Definujme množinu $M \coloneqq \{m \ge 0;\ W$ obsahuje lineárně nezávislý systém o velikosti $m\}$. Množina M je neprázdná, protože obsahuje o, a shora omezená, protože pro každý lineárně nezávislý systém $x_1 \dots, x_m$ ve W (a tím i ve V) podle Steinitzovy věty 5.26 platí $m \le \dim V$. Tedy $\dim V$ je horní mez na M, a proto M musí obsahovat maximum. Označme jej m^* a nechť mu odpovídá lineárně nezávislý systém $x_1 \dots, x_{m^*}$. Ukážeme, že tento systém tvoří bázi, a k tomu stačí ověřit, že generuje podprostor W. Kdyby tomu tak nebylo, pak by existoval vektor $x \in W$ takový že $x \notin \operatorname{span}(x_1 \dots, x_{m^*})$. Pak by vektory $x, x_1 \dots, x_{m^*}$ byly lineárně nezávislé, což je ve sporu s maximalitou m^*. Tudíž W je konečně generovaný a $\dim W = m^* \le \dim V$.

Pokud $\dim W = \dim V$, tak systém $x_1, \dots, x_{m^*}$ musí podle Věty 5.30 tvořit bázi V, a proto $W = V$. □

Příklad 5.33. Najděme všechny podprostory $\mathbb{R}^2$:

- dimenze 2: to je pouze $\mathbb{R}^2$ (z Věty 5.32),
- dimenze 1: ty jsou generovány jedním vektorem, tedy jsou to všechny přímky procházející počátkem,
- dimenze 0: to je pouze $\{o\}$. □

Víme, že sjednocení podprostorů obecně podprostor netvoří. Nicméně, můžeme sestrojit jeho lineární obal, tomu se říká spojení podprostorů a má následující ekvivalentní předpis.

Definice 5.34 (Spojení podprostorů)**.** Buďte U, V podprostory vektorového prostoru W. Pak *spojení podprostorů U, V* je definováno $U + V \coloneqq \{u + v;\ u \in U, v \in V\}$.

Věta 5.35 (Spojení podprostorů)**.** *Buďte U, V podprostory vektorového prostoru W. Pak*

$$U + V = \operatorname{span}(U \cup V).$$

Důkaz. Inkluze „$\subseteq$“: je triviální, neboť prostor $\operatorname{span}(U \cup V)$ je uzavřený na součty.

Inkluze „$\supseteq$“: Stačí ukázat, že $U + V$ obsahuje prostory U, V a že je podprostorem W. První část je zřejmá, pro druhou uvažujme $x_1, x_2 \in U + V$. Vektory se dají vyjádřit jako $x_1 = u_1 + v_1$, $u_1 \in U$, $v_1 \in V$, a $x_2 = u_2 + v_2$, $u_2 \in U$, $v_2 \in V$. Potom $x_1 + x_2 = u_1 + v_1 + u_2 + v_2 = (u_1 + u_2) + (v_1 + v_2) \in U + V$, což dokazuje uzavřenost na sčítání. Pro uzavřenost na násobky uvažujme $x = u + v \in U + V$, $u \in U$, $v \in V$ a skalár α. Pak $\alpha x = \alpha(u + v) = (\alpha u) + (\alpha v) \in U + V$. □

Příklad 5.36. $\mathbb{R}^2 = \operatorname{span}(e_1) + \operatorname{span}(e_2)$, $\mathbb{R}^3 = \operatorname{span}(e_1) + \operatorname{span}(e_2) + \operatorname{span}(e_3)$, $\mathbb{R}^3 = \operatorname{span}(e_1, e_2) + \operatorname{span}(e_3)$, $\mathbb{R}^2 = \operatorname{span}(1, 2) + \operatorname{span}(3, 4)$, ale i $\mathbb{R}^2 = \operatorname{span}(1, 2) + \operatorname{span}(3, 4) + \operatorname{span}(5, 6)$. □

Věta 5.37 (Dimenze spojení a průniku)**.** *Buďte U, V podprostory konečně generovaného vektorového prostoru W. Pak platí*

$$\dim(U + V) + \dim(U \cap V) = \dim U + \dim V. \tag{5.3}$$

Důkaz. $U \cap V$ je podprostor W, tedy má konečnou bázi $z_1, \ldots, z_p$. Podle Věty 5.31 ji můžeme rozšířit $z_1, \ldots, z_p, x_1 \ldots, x_m$ na bázi U. Podobně ji můžeme rozšířit $z_1, \ldots, z_p, y_1 \ldots, y_n$ na bázi V. Stačí když ukážeme, že vektory $z_1, \ldots, z_p$, $x_1 \ldots, x_m$, $y_1 \ldots, y_n$ dohromady tvoří bázi $U + V$, a rovnost (5.3) už bude platit. Nejprve ukážeme, že to jsou generátory, a pak, že jsou lineárně nezávislé.

„Generičnost.“ Buď $z \in U + V$, pak $z = u + v$, kde $u \in U, v \in V$. Vektor u lze vyjádřit $u = \sum_{i=1}^{p} \alpha_i z_i + \sum_{j=1}^{m} \beta_j x_j$ a podobně $v = \sum_{i=1}^{p} \gamma_i z_i + \sum_{k=1}^{n} \delta_k y_k$. Potom $z = u + v = \sum_{i=1}^{p} (\alpha_i + \gamma_i) z_i + \sum_{j=1}^{m} \beta_j x_j + \sum_{k=1}^{n} \delta_k y_k$, tedy z je lineární kombinací našich vektorů.

„Lineární nezávislost.“ Buď $\sum_{i=1}^{p} \alpha_i z_i + \sum_{j=1}^{m} \beta_j x_j + \sum_{k=1}^{n} \gamma_k y_k = o$, chceme ukázat, že všechny koeficienty musí být nulové. Označme $z \coloneqq \sum_{i=1}^{p} \alpha_i z_i + \sum_{j=1}^{m} \beta_j x_j = -\sum_{k=1}^{n} \gamma_k y_k$. Zřejmě $z \in U \cap V$, tedy lze vyjádřit $z = \sum_{i=1}^{p} \delta_i z_i$. Tím dostáváme $z = \sum_{i=1}^{p} \delta_i z_i = -\sum_{k=1}^{n} \gamma_k y_k$, neboli $\sum_{i=1}^{p} \delta_i z_i + \sum_{k=1}^{n} \gamma_k y_k = o$. Jediná lineární kombinace lineárních vektorů, která dá nulový vektor, je triviální, proto $\delta_i = 0\ \forall i$ a $\gamma_k = 0\ \forall k$. Dosazením do původní rovnosti dostaneme $\sum_{i=1}^{p} \alpha_i z_i + \sum_{j=1}^{m} \beta_j x_j = o$, a tudíž z lineární nezávislosti máme $\alpha_i = 0\ \forall i$ a $\beta_j = 0\ \forall j$. □

Poznámka 5.38 (Direktní součet podprostorů)**.** Je-li $U \cap V = \{o\}$, pak spojení podprostorů $W = U + V$ se nazývá *direktní součet* podprostorů U, V. Podmínka $U \cap V = \{o\}$ způsobí, že každý vektor $w \in W$ lze zapsat jediným způsobem ve tvaru $w = u + v$, kde $u \in U$ a $v \in V$. Nyní je např. $\mathbb{R}^2 = \operatorname{span}(e_1) + \operatorname{span}(e_2)$ nebo $\mathbb{R}^2 = \operatorname{span}(1, 2) + \operatorname{span}(3, 4)$ direktním součtem, ale $\mathbb{R}^2 = \operatorname{span}(1, 2) + \operatorname{span}(3, 4) + \operatorname{span}(5, 6)$ není.

5.6 Maticové prostory

Nyní se vrátíme zpátky k tématu, které jsme zdánlivě opustili, k teorii matic a skloubíme ji s vektorovými prostory. Oba obory se vzájemně obohatí: Vektorově prostorový pohled nám umožní jednoduše odvodit další vlastnosti matic, a naopak, postupy z maticové teorie nám poskytnou nástroje na testování lineární nezávislosti, určování dimenze atp.

Maticové prostory si zavedeme nad reálnými čísly, ale analogicky se chovají nad jakýmkoliv jiným tělesem.

Definice 5.39 (Maticové prostory)**.** Buď $A \in \mathbb{R}^{m \times n}$. Pak definujeme

1. sloupcový prostor $\mathcal{S}(A) \coloneqq \operatorname{span}\{A_{*1}, \ldots, A_{*n}\} = \{Ax;\ x \in \mathbb{R}^n\}$,
2. řádkový prostor $\mathcal{R}(A) \coloneqq \mathcal{S}(A^T) = \{A^T y;\ y \in \mathbb{R}^m\}$,
3. jádro $\operatorname{Ker}(A) \coloneqq \{x \in \mathbb{R}^n;\ Ax = o\}$.

Výše definované jsou vektorové prostory, speciálně $\mathcal{S}(A) \Subset \mathbb{R}^m$, a $\mathcal{R}(A), \operatorname{Ker}(A) \Subset \mathbb{R}^n$. Důkaz ponecháváme na rozmyšlení.

Maticově můžeme reprezentovat libovolný podprostor V prostoru $\mathbb{R}^n$. Stačí vzít nějaké jeho generátory $v_1, \ldots, v_m$ a sestavit matici $A \in \mathbb{R}^{m\times n}$ jejíž řádky tvoří právě vektory $v_1, \ldots, v_m$. Pak $V = \mathcal{R}(A)$. Podobně V můžeme vyjádřit jako sloupcový prostor vhodné matice z $R^{n\times m}$. Pokud tedy dokážeme dobře manipulovat s maticovými prostory, umožní nám to zacházet i s prostory $\mathbb{R}^n$. Jak si ukážeme později v Sekci 6.2, můžeme takto pracovat s libovolnými konečně generovanými prostory.

Podívejme se jak se mění maticové prostory, když matici násobíme zleva nějakou jinou maticí (to vlastně dělá Gaussova eliminace). Řádkové prostory jsou porovnatelné přímo, ale sloupcové se skládají z různě velkých vektorů. Nicméně, mezi sloupci je zachovává jakási lineárně závislostní vazba (pozor, lineární nezávislost se nemusí zachovávat).

Věta 5.40 (Prostory a násobení maticí zleva)**.** *Buď $A \in \mathbb{R}^{m\times n}$, $Q \in \mathbb{R}^{p\times m}$. Pak*

(1) $\mathcal{R}(QA) \Subset \mathcal{R}(A)$,

(2) Pokud $A_{*k} = \sum_{j\neq k} \alpha_j A_{*j}$ pro nějaké $k \in \{1, \ldots, n\}$, pak $(QA)_{*k} = \sum_{j\neq k} \alpha_j (QA)_{*j}$.

Důkaz.

(1) Stačí ukázat $\mathcal{R}(QA) \subseteq \mathcal{R}(A)$. Buď $x \in \mathcal{R}(QA)$, pak existuje $y \in \mathbb{R}^p$ takové, že $x = (QA)^T y = A^T Q^T y = A^T (Q^T y) \in \mathcal{R}(A)$.

(2) $(QA)_{*k} = QA_{*k} = Q(\sum_{j\neq k} \alpha_j A_{*j}) = \sum_{j\neq k} \alpha_j QA_{*j} = \sum_{j\neq k} \alpha_j (QA)_{*j}$. □

Pokud násobíme zleva regulární maticí, což je typický případ, tak můžeme odvodit silnější tvrzení.

Věta 5.41 (Prostory a násobení regulární maticí zleva)**.** *Buď $Q \in \mathbb{R}^{m\times m}$ regulární a $A \in \mathbb{R}^{m\times n}$. Pak*

(1) $\mathcal{R}(QA) = \mathcal{R}(A)$,

(2) Platí $A_{*k} = \sum_{j\neq k} \alpha_j A_{*j}$ pro nějaké $k \in \{1, \ldots, n\}$, právě tehdy když $(QA)_{*k} = \sum_{j\neq k} \alpha_j (QA)_{*j}$.

Důkaz.

(1) Podle Věty 5.40 je $\mathcal{R}(QA) \subseteq \mathcal{R}(A)$. Aplikujeme-li Větu 5.40 na matici (QA) násobenou zleva Q^{-1} dostaneme $\mathcal{R}(Q^{-1}QA) \subseteq \mathcal{R}(QA)$, tedy $\mathcal{R}(QA) = \mathcal{R}(A)$.

(2) Implikaci zleva doprava dostaneme z Věty 5.40. Obrácenou implikaci dostaneme z Věty 5.40 aplikované na matici (QA) násobenou zleva Q^{-1}. □

Důsledkem předchozí věty je, že pokud sloupce matice B jsou lineárně nezávislé, tak zůstanou i po pronásobení regulární maticí.

Tyto věty nám také usnadní dokázat nejdůležitější výsledek o maticových prostorech.

Věta 5.42 (Maticové prostory a RREF)**.** *Buď $A \in \mathbb{R}^{m\times n}$ a A^R její RREF tvar s pivoty na pozicích $(1, p_1), \ldots, (r, p_r)$. Pak*

(1) báze $\mathcal{R}(A)$ je tvořena nenulovými řádky A^R, tedy vektory $A^R_{1*}, \ldots, A^R_{r*}$,

(2) báze $\mathcal{S}(A)$ je tvořena sloupci $A_{*p_1}, \ldots, A_{*p_r}$,

(3) $\dim \mathcal{R}(A) = \dim \mathcal{S}(A) = \operatorname{rank}(A) = r$.

Důkaz. Víme z Věty 3.21, že $A^R = QA$ pro nějakou regulární matici Q.

(1) Podle Věty 5.41 je $\mathcal{R}(A) = \mathcal{R}(QA) = \mathcal{R}(A^R)$. Nenulové řádky A^R jsou lineárně nezávislé, tedy tvoří bázi $\mathcal{R}(A^R)$ i $\mathcal{R}(A)$.

(2) Nejprve ukážeme, že sloupce $A^R_{*p_1}, \ldots, A^R_{*p_r}$ tvoří bázi $\mathcal{S}(A^R)$. Tyto vektory jsou jistě lineárně nezávislé (jsou to jednotkové vektory). Generují $\mathcal{S}(A^R)$, neboť libovolný nebázický sloupec se dá vyjádřit jako lineární kombinace těch bázických:

$$A^R_{*j} = \sum_{i=1}^{m} a^R_{ij} e_i = \sum_{i=1}^{r} a^R_{ij} e_i = \sum_{i=1}^{r} a^R_{ij} A^R_{*p_i}.$$

Nyní použijeme Větu 5.41, která nám zaručí, že i $A_{*p_1}, \ldots, A_{*p_r}$ jsou lineárně nezávislé a generují ostatní sloupce, tedy tvoří bázi $\mathcal{S}(A)$.

(3) $\dim \mathcal{R}(A)$ je velikost báze $\mathcal{R}(A)$, tedy r, a podobně $\dim \mathcal{S}(A)$ je velikost báze $\mathcal{S}(A)$, také r. Navíc $r = \operatorname{rank}(A)$. □

Třetí vlastnost Věty 5.42 dává důležitý a netriviální důsledek pro hodnost matice a její transpozice, neboť

$$\operatorname{rank}(A) = \dim \mathcal{R}(A) = \dim \mathcal{S}(A) = \dim \mathcal{R}(A^T) = \operatorname{rank}(A^T).$$

Dostáváme tedy následující větu.

Věta 5.43. *Pro každou matici* $A \in \mathbb{R}^{m\times n}$ *je* $\operatorname{rank}(A) = \operatorname{rank}(A^T)$.

Tuto větu jsme nezmiňovali v kapitole 3, protože k jejímu dokázání potřebujeme netriviální poznatky z vektorových prostorů. A naopak, řadu charakteristik vektorových prostorů jako je určování dimenze, hledání báze atp. můžeme testovat pomocí známých postupů teorie matic. Spojují se nám tady dvě teorie a společně produkují zajímavé výsledky.

Věta 5.42 nám dává návod jak zjistit určité charakteristiky prostorů pomocí RREF tvaru matice. Stačí si dát aritmetické vektory do matice, převést do RREF tvaru a z něj pak vyčíst danou informaci. Pokud vektory nejsou z aritmetického prostoru $\mathbb{R}^n$, pak je potřeba na to jít oklikou, pomocí tzv. isomorfismu (sekce 6.2).

Příklad 5.44. Uvažujme prostor

$$V = \operatorname{span}\{(1,2,3,4,5)^T,\ (1,1,1,1,1)^T,\ (1,3,5,7,9)^T,\ (2,1,1,0,0)^T\}.$$

Nejprve sestavme matici, jejíž sloupce jsou rovny daným generátorům V, tedy $V = \mathcal{S}(A)$:

$$\begin{pmatrix} 1 & 1 & 1 & 2 \\ 2 & 1 & 3 & 1 \\ 3 & 1 & 5 & 1 \\ 4 & 1 & 7 & 0 \\ 5 & 1 & 9 & 0 \end{pmatrix} \overset{RREF}{\sim} \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Z RREF tvaru vidíme, že $\dim(V) = 3$, báze V je např.: $(1,2,3,4,5)^T$, $(1,1,1,1,1)^T$, $(2,1,1,0,0)^T$. Třetí z generátorů je závislý, a je roven dvojnásobku prvního minus druhý.

Nyní dejme generující vektory to řádků matice:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 5 & 7 & 9 \\ 2 & 1 & 1 & 0 & 0 \end{pmatrix} \overset{RREF}{\sim} \begin{pmatrix} 1 & 0 & 0 & -1 & -1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Opět z RREF tvaru vyčteme, že $\dim(V) = 3$, dostaneme ale jinou bázi: $(1,0,0,-1,-1)^T$, $(0,1,0,1,0)^T$, $(0,0,1,1,2)^T$. □

Věta 5.45 (O dimenzi jádra a hodnosti matice)**.** *Pro každou matici* $A \in \mathbb{R}^{m\times n}$ *platí*

$$\dim \operatorname{Ker}(A) + \operatorname{rank}(A) = n.$$

Důkaz. Buď $\dim \operatorname{Ker}(A) = k$ a $x_1, \ldots, x_k$ báze $\operatorname{Ker}(A)$. Rozšiřme ji na bázi $\mathbb{R}^n$ doplněním o vektory $x_{k+1}, \ldots, x_n$. Stačí ukázat, že vektory $Ax_{k+1}, \ldots, Ax_n$ tvoří bázi $\mathcal{S}(A)$, protože pak $\operatorname{rank}(A) = \dim \mathcal{S}(A) = n - k$ a rovnost z věty je splněna.

„Generičnost.“ Buď $y \in \mathcal{S}(A)$, pak $y = Ax$ pro nějaké $x \in \mathbb{R}^n$. Toto x lze vyjádřit $x = \sum_{i=1}^n \alpha_i x_i$. Dosazením

$$y = Ax = A\Big(\sum_{i=1}^n \alpha_i x_i\Big) = \sum_{i=1}^n \alpha_i A x_i = \sum_{i=k+1}^n \alpha_i (A x_i)$$

„Lineární nezávislost.“ Buď $\sum_{i=k+1}^n \alpha_i A x_i = o$. Pak $A\big(\sum_{i=k+1}^n \alpha_i x_i\big) = o$, čili $\sum_{i=k+1}^n \alpha_i x_i$ patří do jádra matice A. Proto $\sum_{i=k+1}^n \alpha_i x_i = \sum_{i=1}^k \beta_i x_i$ pro nějaké skaláry $\beta_1, \ldots, \beta_k$. Přepsáním rovnice dostáváme $\sum_{i=k+1}^n \alpha_i x_i + \sum_{i=1}^k (-\beta_i) x_i = o$ a vzhledem k lineární nezávislosti $x_1, \ldots, x_n$ je $\alpha_{k+1} = \ldots = \alpha_n = \beta_1 = \ldots = \beta_k = 0$. □

Příklad 5.46. Mějme

$$A = \begin{pmatrix} 2 & 4 & 4 & 4 \\ -3 & -4 & 2 & 0 \\ 5 & 7 & -2 & 1 \end{pmatrix} \overset{RREF}{\sim} \begin{pmatrix} 1 & 0 & -6 & -4 \\ 0 & 1 & 4 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Tedy $\dim \mathrm{Ker}\,(A) = 4 - 2 = 2$. Prostor $\mathrm{Ker}\,(A)$ představuje všechna řešení soustavy $Ax = o$ a ta jsou tvaru

$$(6x_3 + 4x_4, -4x_3 - 3x_4, x_3, x_4)^T,\ x_3, x_4 \in \mathbb{R},$$

neboli

$$x_3(6, -4, 1, 0)^T + x_4(4, -3, 0, 1)^T,\ x_3, x_4 \in \mathbb{R}.$$

Báze $\mathrm{Ker}\,(A)$ je tudíž $(6, -4, 1, 0)$, $(4, -3, 0, 1)$. A tato vlastnost platí vždy, tj. vektory získané tímto postupem představují bázi $\mathrm{Ker}\,(A)$. □

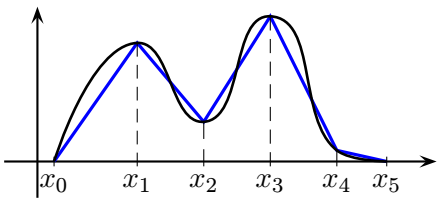
Další vlastnosti maticových prostorů si ukážeme v Důsledku 8.25.

5.7 Aplikace

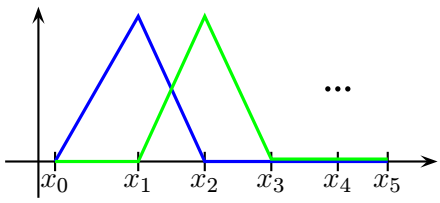
Příklad 5.47 (Metoda konečných prvků pro soustavy diferenciálních rovnic)**.** Fyzikální úlohy vedou často soustavy diferenciálních rovnic.

- strukturální analýza (elasticita těles, stabilita konstrukcí, ...)
- proudění tekutin a plynů (meteorologie, ...)
- ...

Cílem je najít funkci, která vyhovuje dané soustavě diferenciálních rovnic, přičemž v soustavě se vyskytuje neznámá funkce v derivaci (v první nebo i vyšších). Principem metody konečných prvků je diskretizace spojitého prostoru proměnných a aproximovat hledanou funkci funkcí po částech lineární.



Aproximace lineární lomenou funkcí.



Báze lineárních lomenek.

Po částech lineární funkce je lineární kombinací určitých základních lineárních lomených funkcí. Tyto lineární lomenky nám takto představují konečnou bázi prostoru po částech lineárních funkcí, a celý problém vede na soustavu lineárních rovnic. Tato soustava je obrovská (klidně řádu 10^6) a je tím větší, čím přesnější chceme mít řešení. Na druhou stranu, soustava je řídká, tj. pouze malá část koeficientů je nenulová. □

Kapitola 6

Lineární zobrazení

Definice 6.1 (Lineární zobrazení)**.** Buďte U, V vektorové prostory nad tělesem $\mathbb{T}$. Zobrazení $f : U \mapsto V$ je *lineární* pokud každé $x, y \in U$ a $\alpha \in \mathbb{T}$ platí:

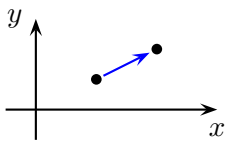
- $f(x + y) = f(x) + f(y)$,
- $f(\alpha x) = \alpha f(x)$.

Lineární zobrazení se též nazývá *homomorfismus*. Koho by zajímala zoologie latinských názvů druhů zobrazení, poznamenejme, že prosté zobrazení je *injektivní*, zobrazení „na“ je *surjektivní*, injektivní homomorfismus je *monomorfismus*, surjektivní homomorfismus je *epimorfismus*, homomorfismus množiny do sebe sama je *endomorfismus*, surjektivní a injektivní homomorfismus je *isomorfismus*, a isomorfní endomorfismus se nazývá *automorfismus*.

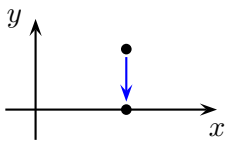
Příklad 6.2 (Příklady lineárních zobrazení)**.**

- $f : U \mapsto V$ definované $f(x) = o$,
- identita je zobrazení $id : U \mapsto U$ definované $id(x) = x$,
- $f : \mathbb{R}^n \mapsto \mathbb{R}^m$ definované $f(x) = Ax$, kde $A \in \mathbb{R}^{m \times n}$ je pevná matice,
- derivace z prostoru reálných diferencovatelných funkcí do prostoru funkcí $\mathcal{F}$. □

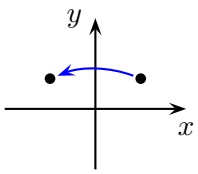
Příklad 6.3 (Příklady lineárních zobrazení v rovině)**.**



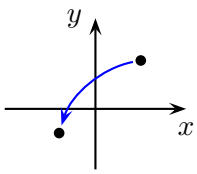
Škálování: $(x, y) \mapsto (\alpha x, \alpha y)$



Projekce do osy x: $(x, y) \mapsto (x, 0)$



Překlopení dle osy y: $(x, y) \mapsto (-x, y)$



Obecný tvar lineárního zobrazení:
$(x, y) \mapsto (a_{11}x + a_{12}y, a_{21}x + a_{22}y)$ □

Tvrzení 6.4 (Vlastnosti lineárních zobrazení)**.** *Buď $f : U \mapsto V$ lineární zobrazení. Pak*

1. $f(\sum_{i=1}^{n} \alpha_i x_i) = \sum_{i=1}^{n} \alpha_i f(x_i)$ *pro každé* $\alpha_i \in \mathbb{T},\ x_i \in U,\ i = 1, \ldots, n$,

2. $f(o) = o$.

Důkaz.
(1) Definice lineárního zobrazení máme $f(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 f(x_1) + \alpha_2 f(x_2)$ a zbytek dostaneme rozšířením matematickou indukcí pro libovolné přirozené n.
(2) $f(o) = f(0 \cdot o) = 0 \cdot f(o) = o$. □

Ke každému lineárnímu zobrazení se vztahují dva důležité vektorové prostory, obraz a jádro (též nazývané nulátor).

Definice 6.5 (Obraz a jádro)**.** Buď $f : U \mapsto V$ lineární zobrazení. Pak definujeme

- obraz $f(U) \coloneqq \{f(x);\, x \in U\}$,
- jádro $\mathrm{Ker}\,(f) \coloneqq \{x \in U;\, f(x) = o\}$.

Snadno nahlédneme, že obraz představuje podprostor prostoru V a jádro podprostor prostoru U. Následující větu tak uvádíme bez důkazu.

Věta 6.6. *Buď $f : U \mapsto V$ lineární zobrazení. Pak:*
(1) $f(U) \trianglelefteq V$,
(2) $\mathrm{Ker}\,(f) \trianglelefteq U$,
(3) pro každé $x_1, \ldots, x_n \in U$: $f(\mathrm{span}(x_1, \ldots, x_n)) = \mathrm{span}(f(x_1), \ldots, f(x_n))$.

Jádro matice a lineárního zobrazení spolu úzce souvisí. Pokud zadefinujeme f předpisem $f(x) = Ax$, potom $\mathrm{Ker}\,(A) = \mathrm{Ker}\,(f)$.

Příklad 6.7 (Příklady lineárních zobrazení)**.** V Příkladu 6.3:

- překlopení: obraz $f(\mathbb{R}^2) = \mathbb{R}^2$, jádro $\mathrm{Ker}\,(f) = \{o\}$,
- projekce do osy x: obraz $f(\mathbb{R}^2) = \text{osa } x$, jádro $\mathrm{Ker}\,(f) = \text{osa } y$. □

Připomeňme, že zobrazení $F : U \mapsto V$ je prosté pokud $f(x) = f(y)$ nastane jenom pro $x = y$.

Věta 6.8 (Prosté lineární zobrazení)**.** *Buď $f : U \mapsto V$ lineární zobrazení. Pak následující je ekvivalentní:*
(1) f je prosté,
(2) $\mathrm{Ker}\,(f) = \{o\}$,
(3) obraz libovolné lineárně nezávislé množiny je lineárně nezávislá množina.

Důkaz. Dokážeme implikace (1) ⇒ (2) ⇒ (3) ⇒ (1).

- Implikace „(1) ⇒ (2)“. Protože $f(o) = o$, tak $o \in \mathrm{Ker}\,(f)$. Ale vzhledem k tomu, že f je prosté zobrazení, tak jádro už jiný prvek neobsahuje.
- Implikace „(2) ⇒ (3)“. Buďte $x_1 \ldots, x_n \in U$ lineárně nezávislé a nechť $\sum_{i=1}^n \alpha_i f(x_i) = o$. Pak $f\big(\sum_{i=1}^n \alpha_i x_i\big) = o$, čili $\sum_{i=1}^n \alpha_i x_i$ náleží do jádra $\mathrm{Ker}\,(f) = \{o\}$. Tudíž musí $\sum_{i=1}^n \alpha_i x_i = o$ a z lineární nezávislosti vektorů máme $\alpha_i = 0\ \forall i$.
- Implikace „(3) ⇒ (1)“. Sporem předpokládejme, že existují dva různé vektory $x, y \in U$ takové, že $f(x) = f(y)$. Potom $o = f(x) - f(y) = f(x - y)$. Vektor o představuje lineárně závislou množinu vektorů, tedy $x - y$ musí být podle předpokladu (2) také lineárně závislá množina, a tudíž $x - y = o$, neboli $x = y$. To je spor. □

U vektorových prostorů víme, že je každý (konečně generovaný) prostor jednoznačně určený nějakou bází. Analogie platí i u lineárních zobrazení, každé lineární zobrazení je jednoznačně určeno tím, kam se zobrazí vektory z báze.

Věta 6.9 (Lineární zobrazení a jednoznačnost vzhledem k obrazům báze)**.** *Buďte U, V prostory nad $\mathbb{T}$ a $x_1, \ldots, x_n$ báze U. Pak pro libovolné vektory $y_1, \ldots, y_n \in V$ existuje právě jedno lineární zobrazení takové, že $f(x_i) = y_i$, $i = 1, \ldots, n$.*

Důkaz. „Existence“. Buď $x \in U$ libovolné, tedy $x = \sum_{i=1}^{n} \alpha_i x_i$ pro nějaké skaláry $\alpha_1, \ldots, \alpha_n \in \mathbb{T}$. Pak zadefinujeme obraz x jako $f(x) = \sum_{i=1}^{n} \alpha_i y_i$, protože lineární zobrazení musí splňovat

$$f(x) = f\left(\sum_{i=1}^{n} \alpha_i x_i\right) = \sum_{i=1}^{n} \alpha_i f(x_i) = \sum_{i=1}^{n} \alpha_i y_i.$$

To, že takto definované zobrazení je lineární, se ověří už snadno.

„Jednoznačnost.“ Mějme dvě různá lineární zobrazení f a g splňující $f(x_i) = g(x_i) = y_i$ pro všechna $i = 1, \ldots, n$. Pak pro libovolné $x \in U$ je

$$f(x) = f\left(\sum_{i=1}^{n} \alpha_i x_i\right) = \sum_{i=1}^{n} \alpha_i f(x_i) = \sum_{i=1}^{n} \alpha_i y_i = \sum_{i=1}^{n} \alpha_i g(x_i) = g\left(\sum_{i=1}^{n} \alpha_i x_i\right) = g(x).$$

Tedy $f(x) = g(x)\ \forall x \in U$, což je ve sporu s tím, že jsou to různá zobrazení. □

6.1 Maticová reprezentace lineárního zobrazení

Každé lineární zobrazení jde reprezentovat maticově. Protože vektory mohou být všelijaké podivné objekty, je nutno je popisovat v řeči souřadnic. Potom s nimi můžeme operovat jako s aritmetickými vektory, což je mnohem pohodlnější.

Definice 6.10 (Matice lineárního zobrazení)**.** Buď $f : U \mapsto V$ lineární zobrazení, $B_1 = \{x_1, \ldots, x_n\}$ báze prostoru U nad $\mathbb{T}$, a $B_2 = \{y_1, \ldots, y_m\}$ báze prostoru V nad $\mathbb{T}$. Nechť $f(x_j) = \sum_{i=1}^{m} a_{ij} y_i$. Potom matice $A \in \mathbb{T}^{m \times n}$ s prvky a_{ij}, $i = 1, \ldots, m$, $j = 1, \ldots, n$ se nazývá *matice lineárního zobrazení* f a značí se: $A = {}_{B_2}[f]_{B_1}$.

Jinými slovy, matice lineárního zobrazení tak, že její j-tý sloupec je tvořen souřadnicemi obrazu vektoru x_j vzhledem k bázi B_2, to jest $A_{*j} = [f(x_j)]_{B_2}$. K čemu je matice lineárního zobrazení užitečná říká následující věta.

Věta 6.11 (Maticová reprezentace lineárního zobrazení)**.** *Buď $f : U \mapsto V$ lineární zobrazení, $B_1 = \{x_1, \ldots, x_n\}$ báze prostoru U, a $B_2 = \{y_1, \ldots, y_m\}$ báze prostoru V. Pak pro každé $x \in U$ je*

$$[f(x)]_{B_2} = {}_{B_2}[f]_{B_1}\ [x]_{B_1}.$$

Důkaz. Buď $x \in U$, tedy $x = \sum_{i=1}^{n} \alpha_i x_i$, neboli $[x]_{B_1} = (\alpha_1, \ldots, \alpha_n)$. Pak

$$f(x) = f\left(\sum_{j=1}^{n} \alpha_j x_j\right) = \sum_{j=1}^{n} \alpha_j f(x_j) = \sum_{j=1}^{n} \alpha_j \left(\sum_{i=1}^{m} a_{ij} y_i\right) = \sum_{j=1}^{n} \sum_{i=1}^{m} \alpha_j a_{ij} y_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_j a_{ij}\right) y_i.$$

Tedy výraz $\sum_{j=1}^{n} \alpha_j a_{ij}$ representuje i-tou souřadnici vektoru $[f(x)]_{B_2}$, ale jeho hodnota je $\sum_{j=1}^{n} \alpha_j a_{ij} = (A[x]_{B_1})_i$, což je i-tá složka vektoru ${}_{B_2}[f]_{B_1}\ [x]_{B_1}$. □

Matice lineárního zobrazení tedy převádí souřadnice vektoru vzhledem k dané bázi na souřadnice jeho obrazu. Plně tak popisuje lineární zobrazení a navíc obraz libovolného vektoru můžeme vyjádřit jednoduchým způsobem jako násobení maticí.

V následujícím bude *kan* značit kanonickou bázi, tj. skládající se z jednotkových vektorů.

Důsledek 6.12. *Každé lineární zobrazení $f : \mathbb{R}^n \mapsto \mathbb{R}^m$ se dá vyjádřit jako $f(x) = Ax$ pro nějakou matici $A \in \mathbb{R}^{m \times n}$.*

Důkaz.

$$f(x) = [f(x)]_{\text{kan}} = {}_{\text{kan}}[f]_{\text{kan}}\ [x]_{\text{kan}} = {}_{\text{kan}}[f]_{\text{kan}}\, x$$

Tedy $f(x) = Ax$, kde $A = {}_{\text{kan}}[f]_{\text{kan}}$. □

Mějme lineární zobrazení $f : U \mapsto V$ a báze B_1, B_2 prostorů. Víme, že matice $A = {}_{B_2}[f]_{B_1}$ splňuje vlastnost

$$[f(x)]_{B_2} = A\,[x]_{B_1} \quad \forall x \in U. \tag{6.1}$$

Ukážeme, že žádná jiná matice tuto vlastnost nemá.

Věta 6.13 (Jednoznačnost matice lineárního zobrazení)**.** *Buď $f : U \mapsto V$ lineární zobrazení, B_1 báze prostoru U, a B_2 báze prostoru V. Pak jediná matice A splňující (6.1) je $A = {}_{B_2}[f]_{B_1}$.*

Důkaz. Nechť báze B_1 se stává z vektorů $x_1, \ldots, x_n$. Pro spor předpokládejme, že lineární zobrazení f má dvě maticové reprezentace (6.1) pomocí matic $A \neq A'$. Tudíž existuje vektor $s \in \mathbb{T}^n$ takový, že $As \neq A's$; takový vektor lze volit např. jako jednotkový s jedničkou na takové pozici, ve kterém sloupci se matice A, A' liší. Definujme vektor $x \coloneqq \sum_{i=1}^{n} s_i x_i$. Pak $[f(x)]_{B_2} = As \neq A's = [f(x)]_{B_2}$, což je spor s jednoznačností souřadnic (Věta 5.20). □

Speciálním případem zobrazení je identita, jeho matici pak nazýváme *maticí přechodu*, protože nám umožňuje přecházet od jednoho souřadného systému k jinému.

Definice 6.14 (Matice přechodu)**.** Buď V vektorový prostor a B_1, B_2 dvě jeho báze. Pak *maticí přechodu* od B_1 k B_2 nazveme matici ${}_{B_2}[id]_{B_1}$.

Matice přechodu má pak podle maticové reprezentace tento význam; buď $x \in U$, pak

$$[x]_{B_2} = {}_{B_2}[id]_{B_1}\,[x]_{B_1},$$

tedy prostým maticovým násobením získáváme souřadnice vzhledem k jiné bázi.

Příklad 6.15. Najděte matici přechodu v $\mathbb{R}^3$ od báze

$$B_1 : ((1,1,-1)^T, (3,-2,0)^T, (2,-1,1)^T)$$

k bázi

$$B_2 : ((8,-4,1)^T, (-8,5,-2)^T, (3,-2,1)^T).$$

Řešení: spočítáme

$$[(1,1,-1)^T]_{B_2} = (2,3,3)^T, \quad [(3,-2,0)^T]_{B_2} = (-1,-4,-7)^T, \quad [(2,-1,1)^T]_{B_2} = (1,3,6)^T.$$

Tedy

$${}_{B_2}[id]_{B_1} = \begin{pmatrix} 2 & -1 & 1 \\ 3 & -4 & 3 \\ 3 & -7 & 6 \end{pmatrix}.$$

Víme-li např., že souřadnice vektoru $(4,-1,-1)^T$ vzhledem k bázi B_1 jsou $(1,1,0)^T$, pak souřadnice vzhledem k B_2 získáme

$$[(4,-1,-1)^T]_{B_2} = {}_{B_2}[id]_{B_1}\,[(4,-1,-1)^T]_{B_1} = {}_{B_2}[id]_{B_1}\,(1,1,0)^T = (1,-1,-4)^T.$$

Důležitou roli v teorii lineárních zobrazení hraje jejich vzájemné skládání. Lineární zobrazení skládáme stejné jako jakékoliv jiná zobrazení.

Definice 6.16 (Složené zobrazení)**.** Buďte $f : U \mapsto V$ a $g : V \mapsto W$ zobrazení. Pak *složené zobrazení* $g \circ f$ je definované

$$(g \circ f)(x) \coloneqq g(f(x)), \quad x \in U$$

Tvrzení 6.17 (Složené lineární zobrazení)**.** *Buďte $f : U \mapsto V$ a $g : V \mapsto W$ lineární zobrazení. Pak složené zobrazení $g \circ f$ je zase lineární zobrazení.*

Důkaz. Podle definice ověříme pro $x, y \in U$ a $\alpha \in \mathbb{T}$:

$$(g \circ f)(x+y) = g(f(x+y)) = g(f(x)+f(y)) = g(f(x)) + g(f(y)) = (g \circ f)(x) + (g \circ f)(y),$$
$$(g \circ f)(\alpha x) = g(f(\alpha x)) = g(\alpha f(x)) = \alpha g(f(x)) = \alpha (g \circ f)(x).$$ □

Věta 6.18 (Matice složeného lineárního zobrazení)**.** *Buďte $f : U \mapsto V$ a $g : V \mapsto W$ lineární zobrazení, buď B_1 báze U, B_2 báze V a B_3 báze W. Pak*

$$_{B_3}[g \circ f]_{B_1} = {}_{B_3}[g]_{B_2} \; {}_{B_2}[f]_{B_1}.$$

Důkaz. Pro každé $x \in U$ je

$$[(g \circ f)(x)]_{B_3} = [g(f(x))]_{B_3} = {}_{B_3}[g]_{B_2} \, [f(x)]_{B_2} = {}_{B_3}[g]_{B_2} \; {}_{B_2}[f]_{B_1} \, [x]_{B_1}.$$

Díky jednoznačnosti matice lineárního zobrazení (Věta 6.13) je ${}_{B_3}[g]_{B_2} \; {}_{B_2}[f]_{B_1}$ hledaná matice složeného zobrazení. □

Vidíme, že skládání zobrazení se v maticové reprezentaci projeví jako součin příslušných matic. To není náhoda, neboť zakladatelé teorie matic, jako např. A. Cayley, definovali (kolem roku 1855) násobení matic právě tak, aby mělo požadované vlastnosti pro skládání zobrazení. Takže i když význam násobení matic daleko přesáhl původní myšlenky, jeho kořeny je třeba hledat zde.

Příklad 6.19 (Skládání otočení a součtové vzorce pro sin a cos)**.** Otočení v rovině o úhel α proti směru hodinových ručiček má matici vzhledem ke kanonické bázi

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

Podobně otočení o úhel β. Matici otočení o úhel $\alpha+\beta$ můžeme získat přímo nebo složením otočení o α a pak o β. Porovnáním získáme součtové vzorce pro sin a cos:

$$\begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} = \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$
$$= \begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\sin\alpha\cos\beta - \sin\beta\cos\alpha \\ \cos\alpha\sin\beta + \cos\beta\sin\alpha & -\sin\alpha\sin\beta + \cos\alpha\cos\beta \end{pmatrix}.$$ □

Příklad 6.20. Nechť máme dánu matici lineárního zobrazení f vzhledem k bázím B_1, B_2, tj. ${}_{B_2}[f]_{B_1}$. Chceme určit matici vzhledem k bázím B_3, B_4, tj. ${}_{B_4}[f]_{B_3}$.

Řešení:

$$_{B_4}[f]_{B_3} = {}_{B_4}[id]_{B_2} \; {}_{B_2}[f]_{B_1} \; {}_{B_1}[id]_{B_3}.$$

Tedy veškerou práci vykonají matice přechodu mezi bázemi. □

Věta o matici složeného zobrazení má řadu pěkných důsledků týkajících se většinou isomorfismů.

6.2 Isomorfismus

Definice 6.21 (Isomorfismus)**.** *Isomorfismus* mezi prostory U, V je vzájemně jednoznačné lineární zobrazení $f : U \mapsto V$. Pokud mezi prostory U, V existuje isomorfismus, pak říkáme, že U, V jsou *isomorfní.*

Příklad 6.22. Příkladem isomorfismu je třeba škálování, překlápění v $\mathbb{R}^2$ (Příklad 6.3) nebo otáčení (Příklad 6.19). Příkladem neisomorfního zobrazení je projekce (Příklad 6.3).

Isomorfismus najdeme i mezi některými nekonečně generovanými prostory, například mezi prostorem polynomů $\mathcal{P}$ a prostorem reálných posloupností s konečně mnoha nenulovými prvky. Isomorfismem je pak třeba zobrazení $a_n x^n + \cdots + a_1 x + a_0 \mapsto (a_0, a_1, \ldots, a_n, 0, \ldots)$. □

Tvrzení 6.23 (Vlastnosti isomorfismu)**.**

(1) Je-li $f : U \mapsto V$ isomorfismus, pak $f^{-1} : V \mapsto U$ existuje a je to také isomorfismus.

(2) Jsou-li $f : U \mapsto V$ a $g : V \mapsto W$ isomorfismy, pak $g \circ f : U \mapsto W$ je také isomorfismus.

Důkaz.
(1) Zobrazení f je bijekce, tedy f^{-1} existuje a je to také bijekce. Zbývá dokázat linearitu. Buď $v_1, v_2 \in V$ a nechť $f^{-1}(v_1) = u_1$ a $f^{-1}(v_2) = u_2$. Pak $f(u_1+u_2) = f(u_1)+f(u_2) = v_1+v_2$, tedy $f^{-1}(v_1+v_2) = u_1+u_2 = f^{-1}(v_1)+f^{-1}(v_2)$. Podobně pro násobky: Nechť $v \in V$ a $f^{-1}(v) = u$, pak $f(\alpha u) = \alpha f(u) = \alpha v$, tedy $f^{-1}(\alpha v) = \alpha u = \alpha f^{-1}(v)$.
(2) Snadné. □

Nyní přichází na řadu slíbené důsledky věty o matici složeného lineárního zobrazení.

Důsledek 6.24. *Buď $f : U \mapsto V$ isomorfismus, B_1 báze U a B_2 báze V. Pak*

$$ {}_{B_1}[f^{-1}]_{B_2} \;=\; {}_{B_2}[f]_{B_1}^{-1}\,. $$

Důkaz. Protože $f^{-1} \circ f = id$, dostáváme

$$ {}_{B_1}[f^{-1}]_{B_2}\ {}_{B_2}[f]_{B_1} \;=\; {}_{B_1}[f^{-1} \circ f]_{B_1} \;=\; {}_{B_1}[id]_{B_1} \;= I. $$

Podobně

$$ {}_{B_2}[f]_{B_1}\ {}_{B_1}[f^{-1}]_{B_2} \;=\; {}_{B_2}[f \circ f^{-1}]_{B_2} \;=\; {}_{B_2}[id]_{B_2} \;= I. $$

Tedy matice ${}_{B_2}[f]_{B_1}$ a ${}_{B_1}[f^{-1}]_{B_2}$ jsou navzájem inverzní.

Poznamenejme, že jsme museli ukázat i druhou rovnost, protože dopředu nevíme, že matice zobrazení je čtvercová. Obdélníkové matice se sice můžou vynásobit na jednotkovou matici, ale ne v obou pořadích. Jsou-li $P \in \mathbb{R}^{m\times n}$, $Q \in \mathbb{R}^{n\times m}$ a $m > n$, potom podle Vět 5.40 a 5.42 je $\mathrm{rank}(PQ) \le \mathrm{rank}(Q) \le n$, ale $\mathrm{rank}(I_m) = m$. Proto nenastane $PQ = I_m$. □

Matice isomorfismu má inverzní, tedy musí být regulární. Dále, speciálně pro matici přechodu mezi bázemi B_1 a B_2, dostáváme

$$ {}_{B_1}[id]_{B_2} \;=\; {}_{B_2}[id]_{B_1}^{-1}\,. $$

Matice isomorfismu má tedy pěkné vlastnosti.

Nyní se obraťme od matic zpět k prostorům mezi nimiž existuje isomorfismus. Schyluje se k důležitým výsledkům, které vytváří spojitost mezi dimenzí a isomorfismem prostorů.

Věta 6.25. *Jsou-li vektorové prostory U, V konečně generované a isomorfní, pak* $\dim U = \dim V$.

Důkaz. Buď B_1 báze U a B_2 báze V. Pak matice zobrazení ${}_{B_2}[f]_{B_1}$ je podle Důsledku 6.24 regulární a tudíž čtvercová. Počet sloupců matice je velikost B_1 a počet řádků velikost B_2, z čehož dostáváme shodu dimenzí. □

Tvrzení 6.26. *Buď V vektorový prostor nad tělesem T dimenze n a bází B. Pak zobrazení $x \mapsto [x]_B$ je isomorfismus mezi prostory V a $\mathbb{T}^n$ nad $\mathbb{T}$.*

Důkaz. Nechť báze B se skládá z vektorů $v_1, \ldots, v_n$. Snadno se nahlédne, že zobrazení $x \mapsto [x]_B$ je to lineární zobrazení, že je na a prosté: Prostota plyne to díky jednoznačnosti souřadnic, Věta 5.20. Dále, zobrazení je „na“, protože každá n-tice $(\alpha_1, \ldots, \alpha_n) \in \mathbb{T}^n$ představuje souřadnice nějakého vektoru, konkrétně vektoru $\sum_{i=1}^n \alpha_i v_i$. Linearitu zobrazení dokážeme takto. Buďte $u, v \in V$ a nechť $u = \sum_{i=1}^n \alpha_i v_i$ a $v = \sum_{i=1}^n \beta_i v_i$, potom $u + v = \sum_{i=1}^n (\alpha_i + \beta_i) v_i$. Tedy

$$ [u]_B + [v]_B = (\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n) = [u + v]_B. $$

Podobně, pro každé $\alpha \in \mathbb{T}$ je $\alpha[u]_B = \alpha(\alpha_1, \ldots, \alpha_n) = (\alpha\alpha_1, \ldots, \alpha\alpha_n) = [\alpha u]_B$. □

Věta 6.27 (Isomorfismus n-dimenzionálních prostorů)**.** *Všechny n-dimenzionální vektorové prostory nad tělesem $\mathbb{T}$ jsou navzájem isomorfní.*

Důkaz. Podle Tvrzení 6.26 jsou všechny n-dimenzionální vektorové prostory nad tělesem $\mathbb{T}$ isomorfní s $\mathbb{T}^n$ nad $\mathbb{T}$, a tím pádem i navzájem mezi sebou, neboť složením isomorfismů je zase isomorfismus. □

Věta říká, že všechny n-dimenzionální prostory nad stejným tělesem jsou navzájem isomorfní. To znamená, že jsou z lineárněalgebraického pohledu stejné, přestože každý má svá specifika, zvláštní operace atp. Z hlediska lineárních prostorů se ale chovají stejně. Tudíž při hledání dimenze, ověřování lineární nezávislosti atp. stačí přejít isomorfismem do prostoru T^n nad $\mathbb{T}$, kde se pracuje mnohem lépe.

Příklad 6.28 (Příklady isomorfismů)**.**

- $\mathcal{P}^n$ a $\mathbb{R}^{n+1}$, vhodný isomorfismus je např. $a_n x^n + \cdots + a_1 x + a_0 \mapsto (a_n, \ldots, a_1, a_0)$;
- $\mathbb{R}^{m\times n}$ a $\mathbb{R}^{mn}$, vhodný isomorfismus je např. $A \mapsto (a_{11}, \ldots, a_{1n}, a_{21}, \ldots, a_{2n}, \ldots, a_{m1}, \ldots, a_{mn})$. □

Pro lineární zobrazení $f : \mathbb{R}^n \mapsto \mathbb{R}^m$ definované předpisem $f(x) = Ax$ platí $\mathrm{Ker}\,(f) = \mathrm{Ker}\,(A)$ a $f(\mathbb{R}^n) = \mathcal{S}(A)$. Pro lineární zobrazení mezi jinými prostory tato vlastnost pochopitelně neplatí, ale dá se ukázat aspoň shoda dimenzí.

Věta 6.29 (O dimenzi jádra a obrazu)**.** *Buď $f : U \mapsto V$ lineární zobrazení, U, V prostory nad $\mathbb{T}$, $\dim U = n$, $\dim V = m$, B_1 báze U a B_2 báze V. Označme $A = {}_{B_2}[f]_{B_1}$. Pak:*

(1) $\dim \mathrm{Ker}\,(f) = \dim \mathrm{Ker}\,(A)$,

(2) $\dim f(U) = \dim \mathcal{S}(A) = \mathrm{rank}(A)$.

Důkaz. (1) Podle Věty 6.25 stačí sestrojit isomorfismus mezi prostory $\mathrm{Ker}\,(f)$ a $\mathrm{Ker}\,(A)$. Isomorfismem může být např. zobrazení $x \in \mathrm{Ker}\,(f) \mapsto [x]_{B_1}$. Z Tvrzení 6.26 víme, že je lineární a prosté. Zbývá ukázat, že $[x]_{B_1} \in \mathrm{Ker}\,(A)$ a že zobrazení je „na“. Buď $x \in \mathrm{Ker}\,(f)$, pak $o = [f(x)]_{B_2} = {}_{B_2}[f]_{B_1}\,[x]_{B_1}$, tedy $[x]_{B_1}$ náleží do jádra A. A naopak, pro každé $[x]_{B_1} \in \mathrm{Ker}\,(A)$ je $f(x) = o$.

(2) Opět sestrojíme isomorfismus, nyní mezi $f(U)$ a $\mathcal{S}(A)$, a to takto $y \in f(U) \mapsto [y]_{B_2}$. A opět, zobrazení je lineární a prosté. Dále, pro $y \in f(U)$ existuje $x \in U$ takové, že $f(x) = y$. Nyní $[y]_{B_2} = [f(x)]_{B_2} = {}_{B_2}[f]_{B_1}\,[x]_{B_1}$, tedy $[y]_{B_2}$ náleží do sloupcového prostoru $\mathcal{S}(A)$. A naopak, pro každé $a \in \mathcal{S}(A)$ najdeme $x \in U$ tak, že $[x]_{B_1} = a$, a pak $y := f(x) \in f(U)$ splňuje $[y]_{B_2} \in \mathcal{S}(A)$. □

Důsledek 6.30. *Buď $f : U \mapsto V$ lineární zobrazení, pak* $\dim U = \dim \mathrm{Ker}\,(f) + \dim f(U)$.

Důkaz. Podle Věty 5.45 platí pro matici A typu $m \times n$ rovnost $n = \dim \mathrm{Ker}\,(A) + \mathrm{rank}\,(A)$. Speciálně, pro $A = {}_{B_2}[f]_{B_1}$ dostáváme hledanou identitu, neboť $n = \dim U$, $\dim \mathrm{Ker}\,(f) = \dim \mathrm{Ker}\,(A)$ a $\dim f(U) = \mathrm{rank}(A)$. □

6.3 Prostor lineárních zobrazení

Není těžké nahlédnout, že lineární zobrazení z prostoru U nad $\mathbb{T}$ dimenze n do prostoru V nad $\mathbb{T}$ dimenze m tvoří vektorový prostor. Navíc, protože každé lineární zobrazení je jednoznačně určeno maticí vzhledem k daným bázím, je tento prostor isomorfní s $\mathbb{T}^{m\times n}$ a má tedy dimenzi mn. Nejzajímavější je případ když $V = \mathbb{T}$.

Definice 6.31. Buď V vektorový prostor nad $\mathbb{T}$. Pak *lineární funkcionál* (nebo též lineární forma) je libovolné lineární zobrazení z V do $\mathbb{T}$. *Duální prostor*, značený V^*, je vektorový prostor všech lineárních funkcionálů.

Je-li $\dim V = n$, pak také $\dim V^* = n$. Je-li $v_1, \ldots, v_n$ báze V, pak duální prostor má např. bázi $f_1, \ldots, f_n$, kde f_i je určeno obrazy báze $f_i(v_i) = 1$ a $f_i(v_j) = 1$ pro $i \neq j$.

Pro konečně generovaný prostor je tedy V isomorfní s duálním prostorem V^*, s duálem k duálnímu prostoru V^{**} atd. Pro nekonečně generované prostory už to pravda být nemusí. Nicméně vždy existuje kanonické vnoření V do V^{**}. Pokud navíc platí, že V a V^{**} jsou isomorfní, tak V má určité pěkné vlastnosti. Podrobnosti odkrývá obor zvaný funkcionální analýza.

Kapitola 7

Afinní prostory

Toto je velmi letmý úvod do afinních prostorů.

Vektorové prostory a podprostory jsou omezeny tím, že musí obsahovat nulový vektor. Motivací pro afinní prostory je takové zobecnění, abychom se vyhnuli této restrikci a přiblížili se reálným situacím. Afinním podprostorem v $\mathbb{R}^3$ tak může být jakákoli přímka či rovina, ne jenom ta procházející počátkem.

7.1 Základní pojmy

Definice 7.1 (Afinní prostor)**.** Buď V vektorový prostor nad $\mathbb{T}$. Pak *afinním prostorem* je jakákoli množina $M \subseteq V$ tvaru

$$M = U + a = \{v + a;\, v \in U\},$$

kde $a \in U$ a U je podprostor V.

Afinní prostor (používá se i pojem afinní podprostor či afinní množina se stejným významem) je tedy jakýkoli podprostor U „posunutý“ nějakým vektorem a. Representant a není jednoznačný, můžeme si volit libovolný vektor z M. Naopak, podprostor U je u každého afinního prostoru určený jednoznačně.

Nad tělesem reálných čísel můžeme charakterizovat afinní prostory i jinak.

Věta 7.2 (Charakterizace afinního prostoru)**.** *Buď V vektorový prostor nad tělesem $\mathbb{T}$ charakteristiky různé od 2, a buď $\emptyset \neq M \subseteq V$. Pak M je afinní, tj. je tvaru $M = V + a$ právě tehdy když pro každé $x, y \in M$ a $\alpha \in \mathbb{T}$ je $\alpha x + (1 - \alpha)y \in M$.*

Poznámka. Ještě před důkazem poznamenejme, že výraz $\alpha x + (1 - \alpha)y$ se nazývá *afinní kombinace* a afinní množina ve V musí být tedy uzavřená na afinní kombinace. Jinými slovy, s každými dvěma body musí obsahovat i přímku, která jimi prochází, protože afinní kombinaci lze přepsat $\alpha x + (1 - \alpha)y = y + \alpha(x - y)$, což je parametrický popis přímky s bodem y a směrnicí $x - y$.

Důkaz. Implikace „$\Rightarrow$“. Buď $x, y \in M$, tedy jsou tvaru $x = u + a$, $y = v + a$, kde $u, v \in U$. Potom $\alpha x + (1 - \alpha)y = \alpha(u + a) + (1 - \alpha)(v + a) = \alpha u + (1 - \alpha)v + a \in U + a = M$.

Implikace „$\Leftarrow$“. Ukážeme, že stačí zvolit $a \in M$ libovolně pevně a $U \coloneqq M - M = \{x - y;\, x, y \in M\}$. Tedy ukážeme, že $M = (M - M) + a$.

„$\subseteq$“: Buď $x \in M$, pak $x = x - a + a \in (M - M) + a = U + a$.

„$\supseteq$“: Buď $x - y + a \in (M - M) + a$. Protože $a, x, y \in M$ dostáváme, že afinní kombinace $\frac{1}{2}a + \frac{1}{2}x \in M$ a také $2\left(\frac{1}{2}a + \frac{1}{2}x\right) + (1 - 2)y = x - y + a \in M$. □

Nad tělesem charakteristiky 2 tato charakterizace obecně nefunguje. Stačí si vzít za příklad prostor $\mathbb{Z}_2^n$ nad $\mathbb{Z}_2$, v němž je každá množina vektorů uzavřená na afinní kombinace.

Příklad 7.3. Množina řešení soustavy rovnic $Ax = b$ je prázdná nebo afinní. Navíc tuto množinu řešení můžeme vyjádřit ve tvaru $\mathrm{Ker}\,(A) + x_0$, kde x_0 je jedno libovolné řešení soustavy.

Důkaz. Pokud x_1 je řešením, pak lze psát $x_1 = x_1 - x_0 + x_0$. Stačí ukázat, že $x_1 - x_0 \in \mathrm{Ker}\,(A)$. Dosazením $A(x_1 - x_0) = Ax_1 - Ax_0 = b - b = 0$. Tedy $x_1 \in \mathrm{Ker}\,(A) + x_0$. Naopak, je-li $x_2 \in \mathrm{Ker}\,(A)$, pak $x_2 + x_0$ je řešením soustavy, neboť $A(x_2 + x_0) = Ax_2 + Ax_0 = 0 + b = b$.

Poznámka. Platí i obrácená implikace, tedy každý afinní prostor lze popsat pomocí soustavy rovnic (v souřadnicích), viz Bican [2009]. □

Poznámka 7.4. Shrňme stručně několik pojmů a vlastností okolo afinních prostorů:

- Průnik afinních prostorů je zase afinní prostor nebo prázdná množina.
- *Dimenze* afinního prostoru $M = U + a$ je definována jako $\dim(M) := \dim(U)$. Tedy přirozeně dimenze přímky v $\mathbb{R}^n$ je jedna a roviny dva.

  To nám také umožňuje definovat *přímku* p v libovolném vektorovém prostoru W nad $\mathbb{T}$ jakožto afinní množinu dimenze jedna. Jinými slovy, $p = \operatorname{span}(v) + a$, kde $a, v \in U$ a $v \neq o$. Odsud dostáváme i známý parametrický popis přímky $p = \{\alpha v + a;\ \alpha \in \mathbb{T}\}$.

  Nadrovinou v prostoru dimenze n rozumíme pak libovolný afinní podprostor dimenze $n-1$. Tedy např. v $\mathbb{R}^2$ jsou to přímky, v $\mathbb{R}^3$ roviny, atd.
- Čemu odpovídala lineární nezávislost u vektorových prostorů, tomu odpovídá afinní nezávislost u afinních prostorů. Jedná se o formalizaci toho, co známe pod pojmem „Mějme body v obecné poloze.“ Tedy definujeme, že $x_0, x_1, \ldots, x_n$ jsou *afinně nezávislé* pokud $x_1 - x_0, \ldots, x_n - x_0$ jsou lineárně nezávislé.
- Buď $M = U + a$ afinní prostor a $v_1, \ldots, v_n$ báze U. Pak každé $x \in M$ se dá jednoznačně zapsat ve tvaru $x = a + \sum_{i=1}^{n} \alpha_i v_i$. Tedy $a, v_1, \ldots, v_n$ lze považovat za *souřadný systém* a vektor $(\alpha_1, \ldots, \alpha_n)$ za příslušné *souřadnice*.

  K přechodu mezi souřadnými systémy pak můžeme použít naši známou matici přechodu přesně jak jsme zvyklí. V případě, že měníme i vektor a, s drobnou úpravou.
- Vztah afinních prostorů. Afinní prostory $U+a$ a $W+b$ jsou *rovnoběžné* pokud $U \Subset W$ nebo $W \Subset U$; *různoběžné* pokud nejsou rovnoběžné a mají neprázdný průnik; a *mimoběžné* pokud pokud nejsou rovnoběžné a mají prázdný průnik.
- Buď $f : U \mapsto V$ lineární zobrazení. Potom *afinní zobrazení* (jednoduššího typu) má tvar $F(u) = f(u) + a$, kde $a \in V$. Jednoduchým příkladem afinního zobrazení je posunutí, tedy zobrazení $f : V \mapsto V$ s popisem $f(x) = x + a$, kde $a \in V$ je pevné.

  Afinní zobrazení nemusí zobrazovat o na o, je to posunuté o aditivní člen a. Snadno se nahlédne, že obraz prostoru při afinním zobrazení je afinní prostor, a že složením dvou afinních zobrazení dostaneme opět afinní zobrazení.

7.2 Aplikace

Fraktály

Příklad 7.5 (Afinní zobrazení a fraktály [Gareth, 2001, sekce 4.4])**.** Pomocí čtyř afinních zobrazení dokážeme v rovině vykreslit složitý fraktál. Začněme v počátku a s danými pravděpodobnostmi uvažujme přechod podle příslušného afinního zobrazení.

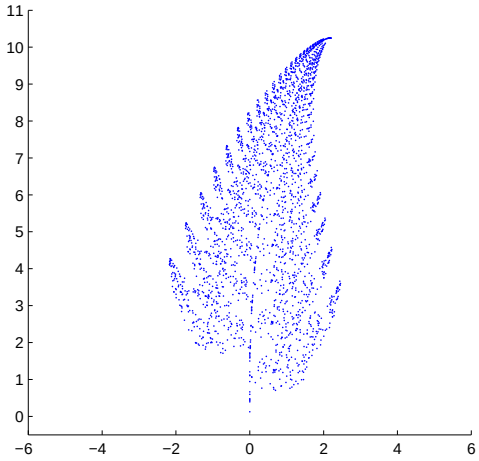
$$T_1(x,y) = \begin{pmatrix} 0.86 & 0.03 \\ -0.03 & 0.86 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 1.5 \end{pmatrix} \quad \text{s pravděpodobností } 0.83$$

$$T_2(x,y) = \begin{pmatrix} 0.2 & -0.25 \\ 0.21 & 0.23 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 1.5 \end{pmatrix} \quad \text{s pravděpodobností } 0.08$$

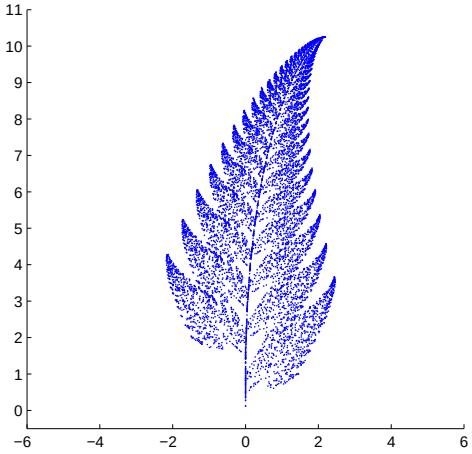
$$T_3(x,y) = \begin{pmatrix} -0.15 & 0.27 \\ 0.25 & 0.26 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 0.45 \end{pmatrix} \quad \text{s pravděpodobností } 0.08$$

$$T_4(x,y) = \begin{pmatrix} 0 & 0 \\ 0 & 0.17 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \text{s pravděpodobností } 0.01$$

Navštívené body nám postupně vykreslí fraktál ve tvaru listu kapradiny.



2500 iterací.



10000 iterací. □

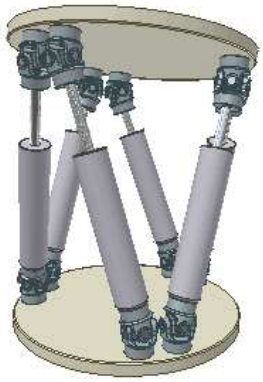
Stewart–Goughova platforma v robotice

Stewart–Goughova platforma je tzv. paralelní manipulátor v oboru kinematické robotiky. Pevná základna je připevněna několika (většinou šesti) pohyblivými rameny k mobilní plošině. Tyto platformy se využívají jako manu[ulátory, v simulacích (např. letů), nebo třeba v biomechanice kloubů k ověřování implantátů mimo lidské tělo.

Základna i mobilní plošina mají své vlastní souřadné systémy, mezi kterými můžeme přecházet pomocí afinního zobrazení. Např., jsou-li $x = (x_1, x_2, x_3)$ souřadnice bodu v systému plošiny, pak souřadnice vůči základně získáme jako $x' = Px + c$, kde P matice reprezentující naklonění a c je nějaký pevný vektor reprezentující posun. Navíc se dá ukázat, že matice P závisí pouze na třech parametrech, protože systém plošiny vzhledem k základně je pouze natočený a není nijak deformovaný (natáhnutý, zkosený atp.).

Označme $x^{(1)}, \ldots, x^{(6)}$ koncové body ramen u základny a $y^{(1)}, \ldots, y^{(6)}$ koncové body na plošině. Ty druhé převedeme výše zmíněnou transformací do soustavy základny: $y'^{(1)}, \ldots, y'^{(6)}$. Nyní jednoduše můžeme spočítat délku ramen jako vzdálenosti bodů $x^{(i)}$ a $y'^{(i)}$ pro $i = 1, \ldots, 6$.

Typicky ale problém stojí opačně: délky ramen známe, protože ty ovládáme, a je potřeba spočítat pozici plošiny, tj. koncových bodů. Jiným problémem pak je třeba zjistit všechny pozice nebo omezit hranice, ve kterých se může plošina nacházet. To už jsou úlohy nad rámec úvodního kurzu lineární algebry.



Obrázek 7.1: Stewart–Goughova platforma. [zdroj: Wikipedia]

Kapitola 8

Skalární součin

Vektorové prostory byly definovány velice obecně, takže pokryjí velkou třídu problémů. Na druhou stanu, pokud přidáme další požadavky co mají prostory splňovat, tak nám to umožní odvodit hlubší výsledky. Konkrétně, skalární součin nám dá možnost přirozeně zavést pojem kolmosti, velikost a vzdálenost vektorů (a tím i limity) atd.

8.1 Skalární součin a norma

Skalární součin (stejně jako grupu, vektorové prostory aj.) zavádíme obecně pomocí seznamu vlastností, které má splňovat. Kvůli vlastnosti 1. zavádíme skalární součin pouze nad tělesy $\mathbb{R}$ a $\mathbb{C}$. Připomeňme, že komplexně sdružené číslo k $a + bi \in \mathbb{C}$ je definované jako $\overline{a + bi} = a - bi$.

Definice 8.1 (Skalární součin nad $\mathbb{R}$)**.** Buď V vektorový prostor nad $\mathbb{R}$. Pak *skalárním součinem* je binární operace $\langle \cdot, \cdot \rangle : V^2 \mapsto \mathbb{R}$, splňující:

1. $\langle x, x \rangle \geq 0 \ \forall x \in V$, a rovnost nastane pouze pro $x = 0$,
2. $\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle \ \forall x, y, z \in V$,
3. $\langle \alpha x, y \rangle = \alpha \langle x, y \rangle \ \forall x, y \in V, \forall \alpha \in \mathbb{R}$,
4. $\langle x, y \rangle = \langle y, x \rangle \ \forall x, y \in V$.

Definice 8.2 (Skalární součin nad $\mathbb{C}$)**.** Buď V vektorový prostor nad $\mathbb{C}$. Pak *skalárním součinem* je binární operace $\langle \cdot, \cdot \rangle : V^2 \mapsto \mathbb{C}$, splňující:

1. $\langle x, x \rangle \geq 0 \ \forall x \in V$, a rovnost nastane pouze pro $x = 0$,
2. $\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle \ \forall x, y, z \in V$,
3. $\langle \alpha x, y \rangle = \alpha \langle x, y \rangle \ \forall x, y \in V, \forall \alpha \in \mathbb{C}$,
4. $\langle x, y \rangle = \overline{\langle y, x \rangle} \ \forall x, y \in V$.

Čtvrtá vlastnost u komplexního skalárního součinu zařídí, že $\langle x, x \rangle = \overline{\langle x, x \rangle} \in \mathbb{R}$, tedy $\langle x, x \rangle$ je vždy reálné číslo a lze porovnávat s nulou u první vlastnosti.

Vlastnosti 2.–3. říkají, že skalární součin je lineární funkcí v první složce. Jak je to s druhou?

$$\langle x, y + z \rangle = \overline{\langle y + z, x \rangle} = \overline{\langle y, x \rangle} + \overline{\langle z, x \rangle} = \langle x, y \rangle + \langle x, z \rangle,$$
$$\langle x, \alpha y \rangle = \overline{\langle \alpha y, x \rangle} = \overline{\alpha} \overline{\langle y, x \rangle} = \overline{\alpha} \langle x, y \rangle.$$

Pokud dosadíme $\alpha = 0$, dostáváme $\langle o, x \rangle = \langle x, o \rangle = 0$.

Příklad 8.3 (Příklady skalárních součinů)**.**

- V $\mathbb{R}^n$: standardní skalární součin $\langle x, y \rangle = x^T y = \sum_{i=1}^{n} x_i y_i$.
- V $\mathbb{C}^n$: standardní skalární součin $\langle x, y \rangle = x^T \overline{y} = \sum_{i=1}^{n} x_i \overline{y}_i$.

- V $\mathbb{R}^{m\times n}$: standardní skalární součin $\langle A, B\rangle = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}b_{ij}$.
- V $\mathcal{C}_{[a,b]}$, prostoru spojitých funkcí na intervalu $[a,b]$: standardní skalární součin $\langle f, g\rangle = \int_a^b f(x)g(x)dx$.

Výše zmíněné skalární součiny jsou pouze příklady možných zavedení součinů na daných prostorech; jako skalární součin mohou fungovat i jiné operace.

Poznamenejme, že existují prostory, kde skalární součin zavést nelze! □

Nadále uvažujme vektorový prostor V nad $\mathbb{R}$ či $\mathbb{C}$ se skalárním součinem. Nejprve si ukážeme, že skalární součin umožňuje zavést normu, neboli velikost vektoru.

Definice 8.4 (Norma indukovaná skalárním součinem)**.** *Norma indukovaná skalárním součinem* je definovaná $\|x\| \coloneqq \sqrt{\langle x, x\rangle}$, $x \in V$.

Norma je dobře definovaná díky první vlastnosti z definice skalárního součinu, a je to vždy nezáporná hodnota.

Pro standardní skalární součin v $\mathbb{R}^n$ dostáváme známou eukleidovskou normu $\|x\| = \sqrt{\sum_{i=1}^{n} x_i^2}$.

Geometrická interpretace standardního skalárního součinu v $\mathbb{R}^n$ je $\langle x, y\rangle = \|x\|\cdot\|y\|\cos\phi$, kde ϕ je úhel mezi vektory x, y. Speciálně, x, y jsou kolmě právě tehdy když $\langle x, y\rangle = 0$. V jiných prostorech takováto geometrie chybí, proto kolmost zavedeme právě pomocí vztahu $\langle x, y\rangle = 0$.

Definice 8.5 (Kolmost)**.** Vektory x, y jsou *kolmé* pokud $\langle x, y\rangle = 0$. Značení: $x \perp y$.

Příklad 8.6 (Příklady kolmých vektorů pro standardní skalární součiny)**.**

- V $\mathbb{R}^3$: $(1,2,3) \perp (1,1,-1)$.
- V $\mathcal{C}_{[-\pi,\pi]}$: $\sin x \perp \cos x \perp 1$. □

Věta 8.7 (Pythagorova)**.** *Pokud x, y jsou kolmé, tak $\|x+y\|^2 = \|x\|^2 + \|y\|^2$.*

Důkaz. $\|x+y\|^2 = \langle x+y, x+y\rangle = \langle x, x\rangle + \underbrace{\langle x, y\rangle}_{=0} + \underbrace{\langle y, x\rangle}_{=0} + \langle y, y\rangle = \langle x, x\rangle + \langle y, y\rangle = \|x\|^2 + \|y\|^2$. □

Poznamenejme, že nad $\mathbb{R}$ platí i opačná implikace, ale nad $\mathbb{C}$ obecně nikoli.

Věta 8.8 (Cauchy–Schwarzova nerovnost[1])**.** *Pro každé $x, y \in V$ platí $|\langle x, y\rangle| \le \|x\|\cdot\|y\|$.*

Důkaz. Dokážeme si jen reálnou verzi, která má elegantní důkaz. Uvažujme reálnou funkci $f(t) = \langle x+ty, x+ty\rangle \ge 0$ proměnné $t \in \mathbb{R}$. Pak

$$f(t) = \langle x, x\rangle + t\langle x, y\rangle + t\langle y, x\rangle + t^2\langle y, y\rangle = \langle x, x\rangle + 2t\langle x, y\rangle + t^2\langle y, y\rangle.$$

Jedná se o kvadratickou funkci, která je všude nezáporná, nemůže mít tedy dva různé kořeny. Proto je příslušný diskriminant nekladný:

$$4\langle x, y\rangle^2 - 4\langle x, x\rangle\langle y, y\rangle \le 0.$$

Z toho dostáváme $\langle x, y\rangle^2 \le \langle x, x\rangle\langle y, y\rangle$, odmocněním $|\langle x, y\rangle| \le \|x\|\cdot\|y\|$. □

Cauchy–Schwarzova nerovnost je užitečná pro odvozování dalších výsledků na obecné bázi, nebo i pro konkrétní algebraické výrazy. Např. pro standardní skalární součin v $\mathbb{R}^n$ dostaneme nerovnost

$$\left(\sum_{i=1}^{n} x_i y_i\right)^2 \le \left(\sum_{i=1}^{n} x_i^2\right)\left(\sum_{i=1}^{n} y_i^2\right).$$

Teoretické použití je např. k odvození trojúhelníkové nerovnosti. Další využití viz např. [Krisl, 2008].

Důsledek 8.9 (Trojúhelníková nerovnost)**.** *Pro každé $x, y \in V$ platí $\|x+y\| \le \|x\| + \|y\|$.*

[1] Nerovnost se také někdy nazývá jen Schwarzova, nebo Cauchy–Bunjakovského, popř. Cauchy–Schwarz–Bunjakovského. Augustin-Louis Cauchy ji dokázal r. 1821 pro prostor $\mathbb{R}^n$ a později ji nezávisle na sobě zobecnili Hermann Amandus Schwarz (1880) a Viktor Jakovlevič Bunjakovskij (1859).

Důkaz. Nejprve připomeňme, že pro každé komplexní číslo $z = a + bi$ platí: $z + \overline{z} = 2a = 2\,\mathsf{Re}(z)$, a dále $a \leq |z|$. Nyní můžeme odvodit:

$$\begin{aligned}\|x+y\|^2 &= \langle x+y, x+y\rangle = \langle x,x\rangle + \langle y,y\rangle + \langle x,y\rangle + \langle y,x\rangle \\ &= \langle x,x\rangle + \langle y,y\rangle + 2\,\mathsf{Re}(\langle x,y\rangle) \leq \langle x,x\rangle + \langle y,y\rangle + 2\,|\langle x,y\rangle| \\ &\leq \|x\|^2 + \|y\|^2 + 2\,\|x\|\cdot\|y\| = (\|x\| + \|y\|)^2,\end{aligned}$$

kde poslední nerovnost plyne z Cauchy–Schwarzovy věty. Tedy máme $\|x+y\|^2 \leq (\|x\| + \|y\|)^2$ a odmocněním získáme hledaný vztah. □

Norma indukovaná skalárním součinem je jen jedním typem normy, pojem normy je ale definován obecněji. My budeme vesměs pracovat s normou indukovanou skalárním součinem, takže následující odstavec je pouze malou odbočkou.

Definice 8.10 (Norma)**.** Buď V vektorový prostor nad $\mathbb{R}$ nebo $\mathbb{C}$. Pak *norma* je zobrazení $\|\cdot\| : V \mapsto \mathbb{R}$, splňující:

1. $\|x\| \geq 0\ \forall x \in V$, a rovnost nastane pouze pro $x = 0$,
2. $\|\alpha x\| = |\alpha| \cdot \|x\|\ \forall x, \in V$, $\forall \alpha \in \mathbb{R}$ resp. $\forall \alpha \in \mathbb{C}$,
3. $\|x+y\| \leq \|x\| + \|y\|$.

Tvrzení 8.11. *Norma indukovaná skalárním součinem je normou.*

Důkaz. Vlastnost 1. je splněna díky definici normy indukované skalárním součinem. Vlastnost 3. je ukázána v Důsledku 8.9. Zbývá vlastnost 2.:

$$\|\alpha x\| = \sqrt{\langle \alpha x, \alpha x\rangle} = \sqrt{\alpha\overline{\alpha}\langle x,x\rangle} = \sqrt{\alpha\overline{\alpha}}\sqrt{\langle x,x\rangle} = |\alpha|\cdot\|x\|.$$ □

Příklad 8.12 (Příklady norem v $\mathbb{R}^n$)**.**

- p-norma: $\|x\|_p = \left(\sum_{i=1}^n |x_i|^p\right)^{\frac{1}{p}}$, kde $p = 1, 2, \ldots$.
- speciálně pro $p = 2$: eukleidovská norma $\|x\|_2 = \sqrt{\sum_{i=1}^n x_i^2}$, což je norma indukovaná standardním skalárním součinem,
- speciálně pro $p = 1$: součtová norma $\|x\|_1 = \sum_{i=1}^n |x_i|$; nazývá se Manhattanská norma, protože odpovídá reálným vzdálenostem při procházení pravoúhlé sítě ulic v městě,
- speciálně pro $p = \infty$ (limitním přechodem): maximová (Čebyševova) norma $\|x\|_\infty = \max_{i=1,\ldots,n} |x_i|$.

Součtová a maximová norma nejsou indukované žádným skalárním součinem. □

Norma umožňuje zavést vzdálenost mezi vektory x, y jako $\|x-y\|$. A pokud máme vzdálenost, můžeme zavést limity, etc.

8.2 Ortonormální báze, Gram–Schmidtova ortogonalizace

Definice 8.13 (Ortogonální a ortonormální systém)**.** Systém vektorů $z_1, \ldots, z_n$ je *ortogonální* pokud $\langle z_i, z_j\rangle = 0\ \forall i \neq j$. Systém vektorů $z_1, \ldots, z_n$ je *ortonormální* pokud je ortogonální a $\|z_i\| = 1\ \forall i = 1, \ldots, n$.

Je-li systém $z_1, \ldots, z_n$ ortonormální, pak je také ortogonální. Naopak to obecně neplatí, ale není problém ortogonální systém zortonormalizovat. Jsou-li $z_1, \ldots, z_n$ nenulové a ortogonální, pak $\frac{1}{\|z_1\|}z_1, \ldots, \frac{1}{\|z_n\|}z_n$ je ortonormální. Důkaz: $\|\frac{1}{\|z_i\|}z_i\| = \frac{1}{\|z_i\|}\|z_i\| = 1$.

Věta 8.14. *Je-li systém vektorů $z_1, \ldots, z_n$ ortonormální, pak je lineárně nezávislý.*

Důkaz. Uvažujme lineární kombinaci $\sum_{i=1}^n \alpha_i z_i = o$. Pak $\forall k$ platí:

$$0 = \langle o, z_k\rangle = \Big\langle \sum_{i=1}^n \alpha_i z_i, z_k \Big\rangle = \sum_{i=1}^n \alpha_i \langle z_i, z_k\rangle = \alpha_k \langle z_k, z_k\rangle = \alpha_k. \qquad \square$$

Následující věta říká jak jednoduše spočítat souřadnice vůči bázi, která je ortonormální.

Věta 8.15 (Fourierovy koeficienty)**.** *Buď $z_1, \dots, z_n$ ortonormální báze prostoru V. Pak $\forall x \in V$ platí $x = \sum_{i=1}^n \langle x, z_i\rangle z_i$.*

Důkaz. Víme, že $x = \sum_{i=1}^n \alpha_i z_i$ jednoznačně (Věta 5.20). Nyní $\forall k$ platí:

$$\langle x, z_k\rangle = \Big\langle \sum_{i=1}^n \alpha_i z_i, z_k \Big\rangle = \sum_{i=1}^n \alpha_i \langle z_i, z_k\rangle = \alpha_k \langle z_k, z_k\rangle = \alpha_k. \qquad \square$$

Vyjádření $x = \sum_{i=1}^n \langle x, z_i\rangle z_i$ se nazývá *Fourierův rozvoj*, a skaláry $\langle x, z_i\rangle$, $i = 1, \dots, n$ se nazývají *Fourierovy koeficienty.*

Příklad 8.16 (Ortonormální báze)**.**

- V $\mathbb{R}^n$ např. kanonická báze $e_1, \dots, e_n$.
- V $\mathcal{C}_{[-\pi,\pi]}$ existuje spočetná ortonormální báze $z_1, z_2, \dots$ sestávající z

$$\frac{1}{\sqrt{2\pi}},\ \frac{1}{\sqrt{\pi}}\cos x,\ \frac{1}{\sqrt{\pi}}\sin x,\ \frac{1}{\sqrt{\pi}}\cos 2x,\ \frac{1}{\sqrt{\pi}}\sin 2x,\ \frac{1}{\sqrt{\pi}}\cos 3x, \frac{1}{\sqrt{\pi}}\sin 3x,\ \dots$$

A tedy každou funkci $f \in \mathcal{C}_{[-\pi,\pi]}$ lze vyjádřit $f(x) = \sum_{i=1}^\infty \langle f, z_i\rangle z_i$. Poznámka: zde trochu zjednodušujeme a odbýváme pojem nekonečného součtu, ale pro intuitivní pochopení to snad postačuje.

Vyjádření několika prvních členů $f(x) \approx \sum_{i=1}^k \langle f, z_i\rangle z_i$ dává dobrou aproximaci funkce $f(x)$, což se používá hojně v teorii zpracování signálů (např. zvuku).

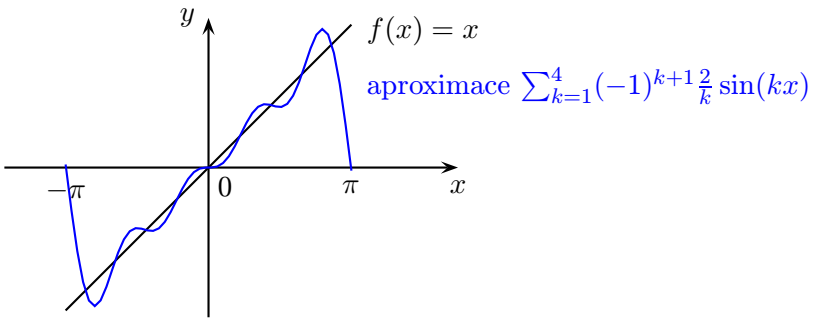
Konkrétně, spočítejme Fourierův rozvoj funkce $f(x) = x$ na $\langle -\pi, \pi\rangle$

$$x = a_0 + \sum_{k=1}^\infty (a_k \sin(kx) + b_k \cos(kx)),$$

kde

$$\begin{aligned} a_0 &= \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)\cdot 1\ dx = \frac{1}{2\pi}\int_{-\pi}^{\pi} x\ dx = 0,\\ a_k &= \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin(kx)\ dx = \frac{1}{\pi}\int_{-\pi}^{\pi} x\sin(kx)\ dx = (-1)^{k+1}\frac{2}{k},\\ b_k &= \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos(kx)\ dx = \frac{1}{\pi}\int_{-\pi}^{\pi} x\cos(kx)\ dx = 0. \end{aligned}$$

Tedy $x = \sum_{k=1}^\infty (-1)^{k+1}\frac{2}{k}\sin(kx)$.



$\square$

Jak sestrojit ortonormální bázi nějakého prostoru? Následující procedura, Gram–Schmidtova ortogonalizační metoda, začne s libovolnou bází a postupným nakolmováním vektorů vytvoří bázi, která je ortonormální. Nakolmování v kroku 2 funguje tak, že od vektoru x_k odečtu jeho projekci do prostoru generovaného vektory $x_1, \dots, x_{k-1}$; tak bude kolmý na všechny předchozí. O projekci více v Sekci 8.3.

Algoritmus 8.17 (Gram–Schmidtova ortogonalizace[2])**.** Buď $x_1, \dots, x_n$ lineárně nezávislý systém v V.

1: **for** $k \coloneqq 1$ **to** n **do**

2: $\quad y_k \coloneqq x_k - \sum_{j=1}^{k-1} \langle x_k, z_j \rangle z_j,$ //vypočítáme kolmici

3: $\quad z_k \coloneqq \frac{1}{\|y_k\|} y_k$ //normalizujeme délku na 1

4: **end for**

Výstup: $z_1, \dots, z_n$ ortonormální báze prostoru $\operatorname{span}\{x_1, \dots, x_n\}$.

Důkaz. (Správnost Gram–Schmidtovy ortogonalizace.) Matematickou indukcí podle n. Pro $n = 1$ je $y_1 = x_1$ a $z_1 = \frac{1}{\|x_k\|} x_k$ je dobře definované a $\operatorname{span}\{x_1\} = \operatorname{span}\{z_1\}$.

Indukční krok $n \leftarrow n-1$. Předpokládejme, že $z_1, \dots, z_{n-1}$ je ortonormální báze $\operatorname{span}\{x_1, \dots, x_{n-1}\}$. Kdyby $y_n = o$, tak $x_n = \sum_{j=1}^{n-1} \langle x_k, z_j \rangle z_j$ a $x_n \in \operatorname{span}\{z_1, \dots, z_{n-1}\} = \operatorname{span}\{x_1, \dots, x_{n-1}\}$, což by byl spor s lineární nezávislostí $x_1, \dots, x_n$. Proto $y_n \neq o$ a $z_n = \frac{1}{\|y_n\|} y_n$ je dobře definovaný a má jednotkovou normu.

Nyní dokážeme, že $z_1, \dots, z_n$ ortonormální systém. Z indukčního předpokladu je $z_1, \dots, z_{n-1}$ ortonormální systém a proto $\langle z_i, z_j \rangle$ je 0 pro $i \neq j$ a 1 pro $i = j$. Stačí ukázat, že z_n je kolmé na ostatní:

$$\begin{aligned} \langle z_n, z_i \rangle &= \frac{1}{\|y_n\|} \langle y_n, z_i \rangle = \frac{1}{\|y_n\|} \Big\langle x_n - \sum_{j=1}^{n-1} \langle x_n, z_j \rangle z_j, z_i \Big\rangle \\ &= \frac{1}{\|y_n\|} \langle x_n, z_i \rangle - \frac{1}{\|y_n\|} \sum_{j=1}^{n-1} \langle x_n, z_j \rangle \langle z_j, z_i \rangle = \frac{1}{\|y_n\|} \langle x_n, z_i \rangle - \frac{1}{\|y_n\|} \langle x_n, z_i \rangle = 0. \end{aligned}$$

Zbývá ověřit $\operatorname{span}\{z_1, \dots, z_n\} = \operatorname{span}\{x_1, \dots, x_n\}$. Z algoritmu je vidět, že $z_n \in \operatorname{span}\{z_1, \dots, z_{n-1}, x_n\} \subseteq \operatorname{span}\{x_1, \dots, x_n\}$, a tedy $\operatorname{span}\{z_1, \dots, z_n\} \subseteq \operatorname{span}\{x_1, \dots, x_n\}$. Protože oba prostory mají stejnou dimenzi, nastane rovnost (Věta 5.32). □

Gram–Schmidtova ortogonalizace má tu přednost, že je použitelná v každém prostoru se skalárním součinem. Na druhou stranu, pro standardní skalární součin v $\mathbb{R}^n$ existují jiné metody, které mají lepší numerické vlastnosti.

Důsledek 8.18 (Existence ortonormální báze)**.** *Každý konečně generovaný prostor (se skalárním součinem) má ortonormální bázi.*

Důkaz. Víme (Věta 5.25), že každý konečně generovaný prostor má bázi, a tu můžeme Gram–Schmidtovou metodou zortogonalizovat. □

Důsledek 8.19 (Rozšíření ortonormálního systému na ortonormální bázi)**.** *Každý ortonormální systém vektorů v konečně generovaném prostoru lze rozšířit na ortonormální bázi.*

Důkaz. Víme (Věta 5.31), že každý ortonormální systém vektorů $z_1, \dots, z_m$ lze rozšířit na bázi $z_1, \dots, z_m$, $x_{m+1}, \dots, x_n$, a tu můžeme Gram–Schmidtovou metodou zortogonalizovat na $z_1, \dots, z_m, z_{m+1}, \dots, z_n$. Povšimněme si, že ortogonalizací se prvních m vektorů nezmění (nebo lze metodu aplikovat až od $k = m+1$ do $k = n$). □

[2] Metoda pochází od dánského finančního matematika Jørgen Pedersen Grama z r. 1883, explicitní vzorec publikoval r. 1907 německý matematik Erhard Schmidt. Jak už to bývá, nezávisle na nich a dříve objevili postup i P.S. Laplace (1816) nebo A.L. Cauchy (1836).

8.3 Ortogonální doplněk a projekce

Definice 8.20 (Ortogonální doplněk)**.** Buď V vektorový prostor a $M \subseteq V$. Pak *ortogonálním doplňkem* M je $M^\perp := \{x \in V;\ \langle x, y\rangle = 0\ \forall y \in M\}$.

Věta 8.21 (Vlastnosti ortogonálního doplňku množiny)**.** *Buď V vektorový prostor a $M, N \subseteq V$. Pak*

(1) $M^\perp$ je podprostor V,

(2) je-li $M \subseteq N$ pak $M^\perp \supseteq N^\perp$,

(3) $M^\perp = \operatorname{span}(M)^\perp$.

Důkaz.

(1) Ověříme vlastnosti podprostoru: $o \in M^\perp$ triviálně. Nyní buďte $x_1, x_2 \in M^\perp$. Pak $\langle x_1, y\rangle = \langle x_2, y\rangle = 0\ \forall y \in M$, tedy i $\langle x_1 + x_2, y\rangle = \langle x_1, y\rangle + \langle x_2, y\rangle = 0$. Nakonec, buď $x \in M^\perp$, tedy $\langle x, y\rangle = 0$ $\forall y \in M$. Pak pro každý skalár α je $\langle \alpha x, y\rangle = \alpha\langle x, y\rangle = 0$.

(2) Buď $x \in N^\perp$, tedy $\langle x, y\rangle = 0\ \forall y \in N$. Tím spíš $\langle x, y\rangle = 0\ \forall y \in M \subseteq N$, a proto $x \in M^\perp$.

(3) $M \subseteq \operatorname{span}(M)$, tedy dle předchozího je $M^\perp \supseteq \operatorname{span}(M)^\perp$. Druhou inkluzi ukážeme takto: buď $x \in M^\perp$ tedy $\langle x, y\rangle = 0\ \forall y \in M$. Speciálně, $\langle x, y_i\rangle = 0$, kde $y_1, \dots, y_n \in M$ je báze $\operatorname{span}(M)$. Pak pro libovolné $y = \sum_{i=1}^n \alpha_i y_i \in \operatorname{span}(M)$ jest $\langle x, y\rangle = \langle x, \sum_{i=1}^n \alpha_i y_i\rangle = \sum_{i=1}^n \alpha_i \langle x, y_i\rangle = 0$. □

Věta 8.22 (Vlastnosti ortogonálního doplňku podprostoru)**.** *Buď V vektorový prostor a $U \Subset V$. Pak*

(1) Buď $z_1, \dots, z_m$ ortonormální báze U, a $z_1, \dots, z_m, z_{m+1}, \dots, z_n$ její rozšíření na ortonormální bázi V. Pak $z_{m+1}, \dots, z_n$ je ortonormální báze $U^\perp$.

(2) $\dim V = \dim U + \dim U^\perp$,

(3) $V = U + U^\perp$,

(4) $(U^\perp)^\perp = U$,

(5) $U \cap U^\perp = \{o\}$.

Důkaz.

(1) $z_{m+1}, \dots, z_n$ je ortonormální systém v V, stačí dokázat $\operatorname{span}\{z_{m+1}, \dots, z_n\} = U^\perp$.

Inkluze „$\supseteq$“. Každý $x \in V$ má Fourierův rozvoj $x = \sum_{i=1}^n \langle x, z_i\rangle z_i$. Je-li $x \in M^\perp$, pak $\langle x, z_i\rangle = 0$, $i = 1, \dots, m$, a tudíž $x = \sum_{i=m+1}^n \langle x, z_i\rangle z_i \in \operatorname{span}\{z_{m+1}, \dots, z_n\}$.

Inkluze „$\subseteq$“. Buď $x \in \operatorname{span}\{z_{m+1}, \dots, z_n\}$, pak $x = \sum_{i=m+1}^n \langle x, z_i\rangle z_i = \sum_{i=1}^m 0 z_i + \sum_{i=m+1}^n \langle x, z_i\rangle z_i$. Z jednoznačnosti souřadnic dostáváme $\langle x, z_i\rangle = 0$, $i = 1, \dots, m$, a tím $x \in M^\perp$.

(2) Z první vlastnosti máme $\dim V = n$, $\dim U = m$, $\dim U^\perp = n - m$.

(3) Z první vlastnosti máme $x = \underbrace{\sum_{i=1}^m \langle x, z_i\rangle z_i}_{\in U} + \underbrace{\sum_{i=m+1}^n \langle x, z_i\rangle z_i}_{\in U^\perp} \in U + U^\perp$.

(4) Z první vlastnosti je $z_{m+1}, \dots, z_n$ ortonormální báze $U^\perp$, tedy $z_1, \dots, z_m$ je ortonormální báze $(U^\perp)^\perp$.

(5) Z předchozího a podle Věty 5.37 o dimenzi spojení a průniku je $\dim(U \cap U^\perp) = \dim V - \dim U - \dim U^\perp = 0$. □

Další z pěkných vlastností ortonormálních systémů je, že nám umožňují jednoduše spočítat projekci x_U vektoru x do podprostoru U, což je vektor z U nejbližší k x. Následující věta opravňuje k zavedení projekce jakožto zobrazení $V \mapsto U$ definované $x \mapsto x_U$.

Věta 8.23 (O ortogonální projekci)**.** *Buď V vektorový prostor a $U \Subset V$. Pak pro každé $x \in V$ existuje jediné $x_U \in U$ takové, že*

$$\|x - x_U\| = \min_{y \in U} \|x - y\|.$$

Navíc, je-li $z_1, \dots, z_m$ ortonormální báze U, pak

$$x_U = \sum_{i=1}^m \langle x, z_i\rangle z_i.$$

Důkaz. Buď $z_1, \ldots, z_m, z_{m+1}, \ldots, z_n$ rozšíření na ortonormální bázi V. Zadefinujme $x_U \coloneqq \sum_{i=1}^{m} \langle x, z_i \rangle z_i$ a ukážeme, že je to hledaný vektor. Nyní $x - x_U = \sum_{i=1}^{n} \langle x, z_i \rangle z_i - \sum_{i=1}^{m} \langle x, z_i \rangle z_i = \sum_{i=m+1}^{n} \langle x, z_i \rangle z_i \in U^\perp$. Buď $y \in U$ libovolné. Protože $x_U - y \in U$, můžeme použít Pythagorovu větu, která dává

$$\|(x - x_U) + (x_U - y)\|^2 = \|x - x_U\|^2 + \|x_U - y\|^2 \geq \|x - x_U\|^2,$$

neboli $\|x - y\| \geq \|x - x_U\|$, což dokazuje minimalitu. Abychom dokázali jednoznačnost, uvědomíme si, že rovnost nastane pouze když $\|x_U - y\|^2 = 0$, čili když $x_U = y$. □

8.4 Ortogonální doplněk a projekce v $\mathbb{R}^n$

Z minulé sekce víme jak počítat ortogonální doplněk a projekci pro libovolný vektorový prostor se skalárním součinem, a to pomocí ortonormální báze. Nyní si ukážeme, že v $\mathbb{R}^n$ pro standardní skalární součin tyto transformace lze vyjádřit explicitně a přímo bez počítání ortonormální báze.

Následující věta říká, jak spočítat ortogonální doplněk libovolného podprostoru $\mathbb{R}^n$ známe-li jeho bázi nebo konečný systém generátorů (představují řádky matice A).

Věta 8.24 (Ortogonální doplněk v $\mathbb{R}^n$)**.** *Buď $A \in \mathbb{R}^{m \times n}$. Pak $\mathcal{R}(A)^\perp = \operatorname{Ker}(A)$.*

Důkaz. Z vlastností ortogonálního doplňku (Věta 8.21(3)) víme $\mathcal{R}(A)^\perp = \{A_{1*}, \ldots, A_{m*}\}^\perp$. Tedy $x \in \mathcal{R}(A)^\perp$ právě tehdy když x je kolmé na řádky matice A, neboli $A_{i*}x = 0$ pro všechna $i = 1, \ldots, m$. Ekvivalentně, $Ax = o$, to jest $x \in \operatorname{Ker}(A)$. □

Charakterizace ortogonálního doplňku má i teoretické důsledky, např. vztah matice A a matice A^TA. Pozor, pro sloupcové prostory analogie neplatí!

Důsledek 8.25. *Buď $A \in \mathbb{R}^{m \times n}$. Pak*

(1) $\operatorname{Ker}(A^TA) = \operatorname{Ker}(A)$,

(2) $\mathcal{R}(A^TA) = \mathcal{R}(A)$,

(3) $\operatorname{rank}(A^TA) = \operatorname{rank}(A)$.

Důkaz.

(1) Je-li $x \in \operatorname{Ker}(A)$, pak $Ax = o$, a tedy také $A^TAx = A^To = o$, čímž $x \in \operatorname{Ker}(A^TA)$. Naopak, je-li $x \in \operatorname{Ker}(A^TA)$, pak $A^TAx = o$. Pronásobením x^T dostaneme $x^TA^TAx = o$, neboli $\|Ax\|^2 = o$. Z vlastnosti normy musí $Ax = o$ a tudíž $x \in \operatorname{Ker}(A)$.

(2) $\mathcal{R}(A^TA) = \operatorname{Ker}(A^TA)^\perp = \operatorname{Ker}(A)^\perp = \mathcal{R}(A)$.

(3) Triviálně z předchozího bodu. □

Nyní se podívejme na projekci.

Věta 8.26 (Ortogonální projekce v $\mathbb{R}^n$)**.** *Buď $A \in \mathbb{R}^{m \times n}$ hodnosti n. Pak projekce vektoru $x \in \mathbb{R}^m$ do sloupcového prostoru $\mathcal{S}(A)$ je $x' = A(A^TA)^{-1}A^Tx$.*

Důkaz. Nejprve si uvědomíme, že x' je dobře definované. Matice A^TA má dimenzi n (Důsledek 8.25(3)), tedy je regulární a má inverzi. Dále, $x' \in \mathcal{S}(A)$, neboť $x' = Ay$ pro $y = (A^TA)^{-1}A^Tx$.

Nyní ukážeme, že $x - x' \in \mathcal{S}(A)^\perp$. Protože $\mathcal{S}(A)^\perp = \mathcal{R}(A^T)^\perp = \operatorname{Ker}(A^T)$, stačí ověřit

$$A^T(x - x') = A^T(x - A(A^TA)^{-1}A^Tx) = A^Tx - A^TA(A^TA)^{-1}A^Tx = A^Tx - A^Tx = o.$$

Speciálně, $(x - x') \perp (x' - Ay)$ pro každé $y \in \mathbb{R}^n$.

Analogicky jako v důkazu Věty 8.23 využijeme Pythagorovy věty:

$$\|x - Ay\|^2 = \|(x - x') + (x' - Ay)\|^2 = \|x - x'\|^2 + \|x' - Ay\|^2 \geq \|x - x'\|^2,$$

tedy $\|x - Ay\| \geq \|x - x'\|$ pro libovolné $y \in \mathbb{R}^n$ a proto je x' hledaná projekce. □

Poznamenejme, že projekce je lineární zobrazení a podle věty je $P \coloneqq A(A^TA)^{-1}A^T$ jeho matice (vzhledem ke kanonické bázi). Navíc tato matice má pozoruhodné vlastnosti. Např. je symetrická, $P^2 = P$ a regulární pouze tehdy když $m = n$.

8.4.1 Metoda nejmenších čtverců

Věta o projekci má široké použití nejenom v geometrii. Uvažujme soustavu $Ax = b$, která nemá řešení (typicky když $m \gg n$). V tom případě bychom chtěli nějakou dobrou aproximaci, tj. takový vektor x, že levá a pravá strana jsou si co nejblíže. Formálně,

$$\min_{x\in\mathbb{R}^n} \|Ax - b\|$$

Tento přístup se studuje pro různé normy, ale pro eukleidovskou dostáváme

$$\min_{x\in\mathbb{R}^n} \|Ax - b\|_2$$

což je ekvivalentní s

$$\min_{x\in\mathbb{R}^n} \|Ax - b\|_2^2 = \min_{x\in\mathbb{R}^n} \sum_{j=1}^{n} (A_{*j}x_j - b_j)^2.$$

Odtud název *metoda nejmenších čtverců*. S využitím věty o projekci najdeme řešení snadno.

Věta 8.27 (Metoda nejmenších čtverců)**.** *Buď $A \in \mathbb{R}^{m\times n}$ hodnosti n. Pak přibližné řešení soustavy $Ax = b$ metodou nejmenších čtverců je $x = (A^TA)^{-1}A^Tb$, a je jednoznačné.*

Důkaz. Projekce vektoru b do podprostoru $\mathcal{S}(A)$ je $A(A^TA)^{-1}A^Tb = Ax$. Jednoznačnost plyne z lineární nezávislosti sloupců A. Pokud $Ax = Ay$, pak $A(x - y) = o$ a tedy $x = y$. □

V praxi se nepočítá $x = (A^TA)^{-1}A^Tb$, ale efektivněji jako řešení soustavy

$$A^TAx = A^Tb.$$

Tato soustava se nazývá *soustava normálních rovnic* a vznikne z původní soustavy přenásobením A^T.

Metoda nejmenších čtverců má uplatnění v řadě oborů, zejména ve statistice.[3)]

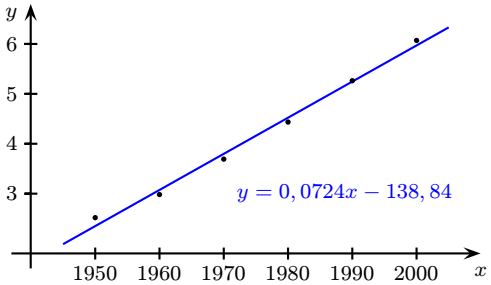
Příklad 8.28 (Lineární regrese: vývoj světové populace)**.** Data vývoje světové populace:

rok	1950	1960	1970	1980	1990	2000
populace (mld.)	2,519	2,982	3,692	4,435	5,263	6,070

Chceme najít lineární závislost velikosti populace (odtud „lineární regrese“) na čase. Tj. prokládáme přímkou $y = px + q$:

$$\begin{aligned} 2,519 &= p \cdot 1950 + q \\ &\vdots \\ 6,070 &= p \cdot 2000 + q \end{aligned}$$

Řešení metodou nejmenších čtverců: $p = 0,0724,\ q = -138,84$. Grafické znázornění závislosti a zdrojový kód pro Matlab / Octave:




```
A = [1950 1960 1970
     1980 1990 2000;
     1 1 1 1 1 1 ]';
b = [2.519 2.982 3.692
     4.435 5.263 6.070]';
x = inv(A'*A)*A'*b,
x'*[2009; 1]
```

Výslednou závislost lze využít pro predikce na další rok. Odhad pro rok 2010: 6,6943 mld., skutečnost: 6,853 mld. □

[3)] Metoda nejmenších čtverců byla vyvinuta Gaussem kolem roku 1801 pro astronomická pozorování. Tehdy se objevil asteroid Ceres, aby v zápětí zase zmizel. Gauss metodou popsal jeho dráhu a předpověděl kdy se znovu objeví.

8.5 Ortogonální matice

I v této sekci uvažujeme standardní skalární součin v $\mathbb{R}^n$.

Definice 8.29 (Ortogonální a unitární matice)**.** Matice $Q \in \mathbb{R}^{n\times n}$ je *ortogonální* pokud $Q^TQ = I$. Matice $Q \in \mathbb{C}^{n\times n}$ je *unitární* pokud $\overline{Q}^TQ = I$.

Pojem unitární matice je zobecnění ortogonálních matic pro komplexní čísla. Nadále ale budeme vesměs pracovat jen s ortogonálními maticemi.

Věta 8.30 (Charakterizace ortogonálních matic)**.** *Buď $Q \in \mathbb{R}^{n\times n}$. Pak následující je ekvivalentní:*

(1) Q je ortogonální,
(2) Q je regulární a $Q^{-1} = Q^T$,
(3) $QQ^T = I$,
(4) Q^T je ortogonální,
(5) Q^{-1} existuje a je ortogonální,
(6) sloupce Q tvoří ortonormální bázi $\mathbb{R}^n$,
(7) řádky Q tvoří ortonormální bázi $\mathbb{R}^n$.

Důkaz. Stručně. (1)–(5): Je-li Q ortogonální, pak $Q^TQ = I$ a tedy $Q^{-1} = Q^T$. Dle vlastnosti inverze máme i $QQ^T = I$, neboli $(Q^T)^TQ^T = I$, tedy Q^T je ortogonální.

(6): Z rovnosti $Q^TQ = I$ dostáváme porovnáním prvků na pozici i, j, že $\langle Q_{*i}, Q_{*j}\rangle = 1$ pokud $i = j$, a $\langle Q_{*i}, Q_{*j}\rangle = 0$ pokud $i \neq j$. Tedy sloupce Q tvoří ortonormální systém. Analogicky naopak. □

Vzhledem k vlastnosti (6) by se spíš slušelo říkat „ortonormální matice“, ale termín ortogonální matice je už zažitý.

Věta 8.31 (Součin ortogonálních matic)**.** *Jsou-li $Q_1, Q_2 \in \mathbb{R}^{n\times n}$ ortogonální, pak Q_1Q_2 je ortogonální.*

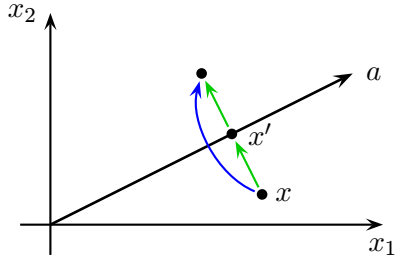
Důkaz. $(Q_1Q_2)^TQ_1Q_2 = Q_2^TQ_1^TQ_1Q_2 = Q_2^TQ_2 = I_n$. □

Příklad 8.32 (Příklady ortogonálních matic)**.**

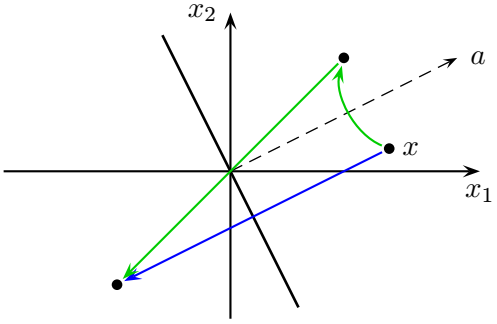
- Např. $\pm I_n$,
- *Householderova matice*: $H(a) \coloneqq I_n - \frac{2}{a^Ta}aa^T$, kde $o \neq a \in \mathbb{R}^n$. Její geometrický význam je následující. Uvažme lineární zobrazení otočení bodu x dle přímky se směrnicí a o 180°. Pomocí Věty 8.26 o projekci dostáváme

$$x + 2(x' - x) = 2x' - x = 2a(a^Ta)^{-1}a^Tx - x = \left(2\frac{aa^T}{a^Ta} - I\right)x.$$

Tedy matice otočení je $\frac{2}{a^Ta}aa^T - I$. Uvažujme nyní zrcadlení dle nadroviny s normálou a. To můžeme reprezentovat jako otočení o 180° dle a, a pak překlopení dle počátku. Tedy matice tohoto zobrazení je $I - 2\frac{aa^T}{a^Ta} = H(a)$.



Otočení kolem přímky a o 180°.



Zrcadlení dle nadroviny s normálou a.

Householderova matice je nejenom ortogonální, ale každá ortogonální matice řádu n lze rozložit jako součin nanejvýš n vhodných Householderových matic.

- *Givensova matice*[4]: Pro $n = 2$ je to matice otočení o úhel α proti směru hodinových ručiček

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

Je to tedy matice tvaru $\left(\begin{smallmatrix} c & -s \\ s & c \end{smallmatrix}\right)$, kde $c^2 + s^2 = 1$. Obecně pro dimenzi n je to matice reprezentující otočení o úhel α v rovině os x_i, x_j, tedy schematicky

$$G_{i,j}(c,s) = \begin{pmatrix} I & & & & \\ & c & & -s & \\ & & I & & \\ & s & & c & \\ & & & & I \end{pmatrix}$$

Také z Givensových matic lze složit každou ortogonální matici, ale je jich potřeba až $\binom{n}{2}$. □

Dole jsou uvedeny základní vlastnosti ortogonálních matic. Díváme-li se na Q jako na matici příslušného lineárního zobrazení $x \mapsto Qx$, pak vlastnost (1) říká, že v při tomto zobrazení se zachovávají úhly, a vlastnost (2) zase říká, že se zachovávají délky. Vlastnost (3) je zase ceněná v numerické matematice, protože Q a Q^{-1} mají omezené velikosti složek. Nejdůležitější vlastností pro numerické počítání je (2), protože při násobení s ortogonální maticí prvky (a tedy i zaokrouhlovací chyby) nemají tendenci se zvětšovat.

Věta 8.33 (Vlastnosti ortogonálních matic)**.** *Buď $Q \in \mathbb{R}^{n\times n}$ ortogonální. Pak*

(1) $\langle Qx, Qy\rangle = \langle x, y\rangle$ pro každé $x, y \in \mathbb{R}^n$,

(2) $\|Qx\| = \|x\|$ pro každé $x \in \mathbb{R}^n$,

(3) $|Q_{ij}| \le 1$ a $|Q^{-1}_{ij}| \le 1$ pro každé $i, j = 1, \ldots, n$,

(4) $\begin{pmatrix} 1 & o^T \\ o & Q \end{pmatrix}$ je ortogonální matice.

Důkaz.

(1) $\langle Qx, Qy\rangle = (Qx)^T Qy = x^T Q^T Qy = x^T Iy = x^T y = \langle x, y\rangle$.

(2) $\|Qx\| = \sqrt{\langle Qx, Qx\rangle} = \sqrt{\langle x, x\rangle} = \|x\|$.

(3) Vzhledem k vlastnosti (6) z Věty 8.30 je $\|Q_{*j}\| = 1$ pro každé $j = 1, \ldots, n$. Tedy $1 = \|Q_{*j}\|^2 = \sum_{i=1}^n q_{ij}^2$, z čehož $|q_{ij}| \le 1$. Matice Q^{-1} je ortogonální, takže pro ni tvrzení platí také.

(4) Z definice $\begin{pmatrix} 1 & o^T \\ o & Q \end{pmatrix}^T \begin{pmatrix} 1 & o^T \\ o & Q \end{pmatrix} = \begin{pmatrix} 1 & o^T \\ o & Q^T Q \end{pmatrix} = I_{n+1}$. □

[4] James Wallace Givens, Jr., americký matematik.

Kapitola 9

Determinanty

Determinanty byly vyvinuty pro účely řešení soustavy lineárních rovnic a dávají explicitní vzorec na jejich řešení (viz Věta 9.13), ale ukázalo se, že determinant sám o sobě je důležitá charakteristika čtvercové matice. [1)]

Definice 9.1 (Determinant)**.** Buď $A \in \mathbb{R}^{n\times n}$. Pak *determinant* matice A je číslo

$$\det(A) = \sum_{p\in S_n} \operatorname{sgn}(p) \prod_{i=1}^{n} a_{i,p(i)} = \sum_{p\in S_n} \operatorname{sgn}(p)\, a_{1,p(1)} \dots a_{n,p(n)}.$$

Značení: $\det(A)$ nebo $|A|$.

Determinanty se stejným způsobem zavedou i pro matice $A \in \mathbb{T}^{n\times n}$ s libovolným tělesem $\mathbb{T}$. S drobnou výjimkou (viz poznámka k Důsledku 9.5) zůstává veškerá teorie v platnosti.

Počítat determinanty z definice je značně neefektivní, protože vyžaduje zpracovat $n!$ sčítanců. Ukážeme si rychlejší způsob, např. pomocí REF tvaru matice.

Příklad 9.2 (Příklady determinantů)**.**

- Matice řádu 2:

$$\det\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{21}a_{12};$$

- Matice řádu 3:

$$\det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{31}a_{22}a_{13} - a_{11}a_{32}a_{23} - a_{21}a_{12}a_{33};$$

- $\det(I_n) = 1$;
- Obecněji, determinant trojúhelníkové matice je součin diagonálních prvků. □

Věta 9.3 (Determinant transpozice)**.** *Buď $A \in \mathbb{R}^{n\times n}$. Pak $\det(A^T) = \det(A)$.*

Důkaz.

$$\begin{aligned}\det(A^T) &= \sum_{p\in S_n} \operatorname{sgn}(p) \prod_{i=1}^{n} A^T_{i,p(i)} = \sum_{p\in S_n} \operatorname{sgn}(p) \prod_{i=1}^{n} a_{p(i),i} = \sum_{p\in S_n} \operatorname{sgn}(p^{-1}) \prod_{i=1}^{n} a_{i,p^{-1}(i)} \\ &= \sum_{p^{-1}\in S_n} \operatorname{sgn}(p^{-1}) \prod_{i=1}^{n} a_{i,p^{-1}(i)} = \sum_{q\in S_n} \operatorname{sgn}(q) \prod_{i=1}^{n} a_{i,q(i)} = \det(A).\end{aligned}$$

□

[1)] Za autora determinantu se považuje Gottfried Wilhelm Leibniz, ale nezávisle na něm jej objevil japonský matematik Seki Kōwa stejného roku 1683.

Pro determinanty obecně $\det(A+B) \neq \det(A)+\det(B)$, ani není znám jednoduchý vzoreček na determinant součtu matic. Výjimkou je následující speciální případ řádkové linearity. Vzhledem k Větě 9.3 je determinant nejen řádkově, ale i sloupcově lineární.

Věta 9.4 (Řádková linearita determinantu)**.** *Buď $A \in \mathbb{R}^{n\times n}$ a $b \in \mathbb{R}^n$. Pak pro libovolné $i = 1,\dots,n$ platí:*

$$\det(A + e_i b^T) = \det(A) + \det(A + e_i(b^T - A_{i*})).$$

Jinými slovy,

$$\det\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{i1}+b_1 & \dots & a_{in}+b_n \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} = \det\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{i1} & \dots & a_{in} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} + \det\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ b_1 & \dots & b_n \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}.$$

Důkaz.

$$\begin{aligned}\det(A + e_i b^T) &= \sum_{p\in S_n} \operatorname{sgn}(p)\, a_{1,p(1)} \dots (a_{i,p(i)} + b_{p(i)}) \dots a_{n,p(n)} \\ &= \sum_{p\in S_n} \operatorname{sgn}(p)\, a_{1,p(1)} \dots a_{i,p(i)} \dots a_{n,p(n)} + \sum_{p\in S_n} \operatorname{sgn}(p)\, a_{1,p(1)} \dots b_{p(i)} \dots a_{n,p(n)} \\ &= \det(A) + \det(A + e_i(b^T - A_{i*}))\end{aligned}$$

□

9.1 Determinant a elementární úpravy

Protože bychom chtěli počítat determinanty pomocí Gaussovy eliminace, je nutné se nejprve podívat na to, jak elementární řádkové úpravy ovlivňují hodnotu determinantu. Nechť matice A' vznikne z A nějakou elementární úpravou.

1. Vynásobení i-tého řádku číslem $\alpha \in \mathbb{R}$: $\det(A') = \alpha \det(A)$.

   Důkaz.

   $$\begin{aligned}\det(A') &= \sum_{p\in S_n} \operatorname{sgn}(p)\, a'_{1,p(1)} \dots a'_{i,p(i)} \dots a'_{n,p(n)} = \sum_{p\in S_n} \operatorname{sgn}(p)\, a_{1,p(1)} \dots (\alpha a_{i,p(i)}) \dots a_{n,p(n)} \\ &= \alpha \sum_{p\in S_n} \operatorname{sgn}(p)\, a_{1,p(1)} \dots a_{i,p(i)} \dots a_{n,p(n)} = \alpha \det(A).\end{aligned}$$

   □

2. Výměna i-tého a j-tého řádku: $\det(A') = -\det(A)$.

   Důkaz. Označme transpozici $t = (i,j)$, pak

   $$\det(A') = \sum_{p\in S_n} \operatorname{sgn}(p)\, a'_{1,p(1)} \dots a'_{i,p(i)} \dots a'_{j,p(j)} \dots a'_{n,p(n)},$$

   kde $a'_{1,p(1)} = a_{1,p(1)} = a_{1,p\circ t(1)}$, $a'_{i,p(i)} = a_{j,p(i)} = a_{j,p\circ t(j)}$, atd. Tedy

   $$\begin{aligned}\det(A') &= \sum_{p\in S_n} \operatorname{sgn}(p)\, a_{1,p\circ t(1)} \dots a_{j,p\circ t(j)} \dots a_{i,p\circ t(i)} \dots a_{n,p\circ t(n)} = \sum_{p\in S_n} \operatorname{sgn}(p) \prod_{i=1}^{n} a_{i,p\circ t(i)} \\ &= -\sum_{p\circ t\in S_n} \operatorname{sgn}(p\circ t) \prod_{i=1}^{n} a_{i,p\circ t(i)} = -\sum_{q\in S_n} \operatorname{sgn}(q) \prod_{i=1}^{n} a_{i,q(i)} = -\det(A).\end{aligned}$$

   □

Důsledek 9.5. *Pokud má matice $A \in \mathbb{R}^{n\times n}$ dva stejné řádky, pak* $\det(A) = 0$.

Důkaz. Prohozením těchto dvou řádků dostaneme $\det(A) = -\det(A)$, a tedy $\det(A) = 0$. □

Poznamenejme, že toto tvrzení platí nad jakýmkoli tělesem, ale pro tělesa charakteristiky 2 se musí použít jiný důkaz, protože např. v $\mathbb{Z}_2$ je $-1 = 1$.

3. Přičtení α-násobku j-tého řádku k i-tému, přičemž $i \neq j$: $\det(A') = \det(A)$.

Důkaz. Z řádkové linearity determinantu, Důsledku 9.5 a první elementární úpravy dostáváme

$$\det(A') = \det\begin{pmatrix} A_{1*} \\ \vdots \\ A_{j*} + \alpha A_{i*} \\ \vdots \\ A_{n*} \end{pmatrix} = \det(A) + \det\begin{pmatrix} A_{1*} \\ \vdots \\ \alpha A_{i*} \\ \vdots \\ A_{n*} \end{pmatrix} = \det(A) + \alpha 0 = \det(A). \qquad \square$$

Výše zmíněná pozorování mají několik důsledků: Pro libovolnou matici $A \in \mathbb{R}^{n\times n}$ je $\det(\alpha A) = \alpha^n \det(A)$. Dále, obsahuje-li A nulový řádek nebo sloupec, tak $\det(A) = 0$.

Hlavní význam vlivu elementárních úprav na determinant je, že determinanty můžeme počítat pomocí Gaussovy eliminace:

Algoritmus 9.6 (Výpočet determinantu pomocí REF)**.** Převeď matici A do REF tvaru a pamatuj si případné změny determinantu v koeficientu c; pak $\det(A)$ je roven součinu c a diagonálních prvků matice $REF(A)$.

9.2 Další vlastnosti determinantu

Věta 9.7 (Kriterium regularity)**.** *Matice $A \in \mathbb{R}^{n\times n}$ je regulární právě tehdy když* $\det(A) \neq 0$.

Důkaz. Převedeme matici A elementárními úpravami na REF, ty mohou měnit hodnotu determinantu, ale nikoli jeho (ne)nulovost. Pak A je regulární právě tehdy když $REF(A)$ má na diagonále nenulová čísla. □

Poznámka 9.8 (Míra regularity)**.** Věta 9.7 umožňuje zavést jakousi míru regularity. Čím je $\det(A)$ blíže k 0, tím je matice A blíž k nějaké singulární matici. Např. Hilbertova matice H_n (viz Příklad 3.37), která je špatně podmíněná protože je „skoro“ singulární. Skutečně, jak ukazuje tabulka, determinant matice je velmi blízko nule.

n	$\det(H_n)$
4	$\approx 10^{-7}$
6	$\approx 10^{-18}$
8	$\approx 10^{-33}$
10	$\approx 10^{-53}$

Tato míra není ale ideální (lepší je např. pomocí vlastních nebo singulárních čísel, viz Sekce 13.5), protože je hodně citlivá ke škálování. Vezměme si např. matici $0.1I_n$, pro níž $\det(0.1I_n) = 10^{-n}$. Přestože 10^{-n} může být libovolně malé číslo, samotná matice má k singulární poměrně daleko.

Věta 9.9 (Multiplikativnost determinantu)**.** *Pro každé $A, B \in \mathbb{R}^{n\times n}$ platí* $\det(AB) = \det(A)\det(B)$.

Důkaz. (A). Nejprve uvažujme speciální případ, když A je elementární matice:

1. $A = E_i(\alpha)$, pak $\det(AB) = \alpha\det(B)$ a $\det(A)\det(B) = \alpha\det(B)$, tedy rovnost platí.
2. $A = E_{ij}$, pak $\det(AB) = -\det(B)$ a $\det(A)\det(B) = -1\det(B)$, tedy rovnost také platí.

3. $A = E_{ij}(\alpha)$, pak $\det(AB) = \det(B)$ a $\det(A)\det(B) = 1\det(B)$, takže i zde rovnost platí.

(B). Nyní uvažme obecný případ. Pokud A je singulární, pak i AB je singulární a rovnost platí, neboť obě strany jsou nulové. Pokud A je regulární, pak jde rozložit na součin elementárních matic $A = E_1 \dots E_k$. Nyní postupujme matematickou indukcí, případ $k = 1$ máme vyřešený v bodě (A), takže se věnujme indukčnímu kroku. Podle indukčního předpokladu a z bodu (A) dostáváme

$$\begin{aligned}\det(AB) &= \det(E_1(E_2 \dots E_k B)) = \det(E_1)\det((E_2 \dots E_k)B) \\ &= \det(E_1)\det(E_2 \dots E_k)\det(B) = \det(E_1 E_2 \dots E_k)\det(B) = \det(A)\det(B).\end{aligned}$$ □

Důsledek 9.10. *Buď $A \in \mathbb{R}^{n\times n}$ regulární, pak $\det(A^{-1}) = \det(A)^{-1}$.*

Důkaz. $1 = \det(I_n) = \det(AA^{-1}) = \det(A)\det(A^{-1})$. □

Nyní si ukážeme rekurentní vzoreček na výpočet determinantu. Podobně jako pro řádek můžeme rozvíjet podle libovolného sloupce.

Věta 9.11 (Laplaceův rozvoj podle i-tého řádku)**.** *Buď $A \in \mathbb{R}^{n\times n}$. Pak pro každé $i = 1, \dots, n$ platí*

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A^{ij}),$$

kde A^{ij} je matice vzniklá z A vyškrtnutím i-tého řádku a j-tého sloupce.

Důkaz. (A). Nejprve uvažujme případ $A_{i*} = e_j^T$, tj. i-tý řádek matice A je jednotkový vektor. Postupným vyměňováním řádků $(i, i+1)$, $(i+1, i+2)$, $\dots$ $(n-1, n)$ převedeme jednotkový vektor do posledního řádku. Podobně postupujeme pro sloupce a j-tý sloupec převedeme na poslední. Výslednou matici označme

$$A' := \left(\begin{array}{ccc|c} & A^{ij} & & \\ & & & \\ \hline 0 & \dots & 0 & 1 \end{array}\right)$$

a znaménko determinantu se změní koeficientem $(-1)^{(n-i)+(n-j)} = (-1)^{i+j}$. Nyní máme

$$\begin{aligned}\det(A) &= (-1)^{i+j}\det(A') = (-1)^{i+j} \sum_{p\in S_n} \operatorname{sgn}(p) \prod_{i=1}^{n} a'_{i,p(i)} \\ &= (-1)^{i+j} \sum_{p;\, p(n)=n} \operatorname{sgn}(p) \prod_{i=1}^{n-1} a'_{i,p(i)} = (-1)^{i+j}\det(A^{ij}).\end{aligned}$$

(B). Nyní uvažme obecný případ. Z řádkové linearity determinantu a z předchozího dostáváme

$$\begin{aligned}\det(A) &= \det\begin{pmatrix} \dots & & & \\ a_{i1} & 0 & \dots & 0 \\ \dots & & & \end{pmatrix} + \dots + \det\begin{pmatrix} \dots & & & \\ 0 & \dots & 0 & a_{in} \\ \dots & & & \end{pmatrix} \\ &= a_{i1}(-1)^{i+1}\det(A^{i1}) + \dots + a_{in}(-1)^{i+n}\det(A^{in}).\end{aligned}$$ □

Příklad 9.12 (Laplaceův rozvoj podle 4. řádku)**.**

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 1 & 2 \\ 2 & 5 & 5 & 5 \\ 0 & 2 & -4 & -4 \end{vmatrix} = (-1)^{4+1} \cdot 0 \cdot \begin{vmatrix} 2 & 3 & 4 \\ 2 & 1 & 2 \\ 5 & 5 & 5 \end{vmatrix} + (-1)^{4+2} \cdot 2 \cdot \begin{vmatrix} 1 & 3 & 4 \\ 1 & 1 & 2 \\ 2 & 5 & 5 \end{vmatrix}$$
$$+ (-1)^{4+3} \cdot (-4) \cdot \begin{vmatrix} 1 & 2 & 4 \\ 1 & 2 & 2 \\ 2 & 5 & 5 \end{vmatrix} + (-1)^{4+4} \cdot (-4) \cdot \begin{vmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \\ 2 & 5 & 5 \end{vmatrix}$$
$$= 0 + 2 \cdot 4 + 4 \cdot 2 - 4 \cdot 2 = 8$$

□

Následující věta dává explicitní vzoreček na řešení soustavy s regulární maticí[2)]. Matice $A+(b-A_{*i})e_i^T$ ve výrazu představuje matici A, ve které nahradíme i-tý sloupec vektorem b.

Věta 9.13 (Cramerovo pravidlo)**.** *Buď $A \in \mathbb{R}^{n\times n}$ regulární a $b \in \mathbb{R}^n$. Pak řešení soustavy $Ax = b$ je tvaru*

$$x_i = \frac{\det(A + (b - A_{*i})e_i^T)}{\det(A)}, \quad i = 1, \ldots, n.$$

Důkaz. Buď x řešení soustavy $Ax = b$; díky regularitě A řešení existuje a je jednoznačné. Rovnost rozepíšeme $\sum_{j=1}^n A_{*j}x_j = b$. Ze sloupcové linearity determinantu dostaneme

$$\det(A + (b - A_{*j})e_i^T) = \det(A_{*1}|\ldots|b|\ldots|A_{*n}) = \det(A_{*1}|\ldots|\textstyle\sum_{j=1}^n A_{*j}x_j|\ldots|A_{*n})$$
$$= \sum_{j=1}^n \det(A_{*1}|\ldots|A_{*j}|\ldots|A_{*n})x_j = \det(A_{*1}|\ldots|A_{*i}|\ldots|A_{*n})x_i = \det(A)x_i.$$

Nyní stačí obě strany podělit číslem $\det(A) \neq 0$. □

Cramerovo pravidlo z roku 1750 je pojmenováno po švýcarském matematikovi G. Cramerovi. Ve své době to byl populární nástroj na řešení soustav lineárních rovnic, dnes má význam spíše teoretický. Mimo jiné nám ukazuje a dává:

- explicitní vyjádření řešení soustavy lineárních rovnic,
- spojitost řešení vzhledem k prvkům A a b,
- odhad velikosti popisu řešení z velikosti popisu vstupních hodnot.

Příklad 9.14 (Cramerovo pravidlo)**.** Řešení soustavy rovnic

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 1 & 2 & 1 & 3 \\ 2 & 5 & 5 & 4 \end{array}\right)$$

spočítáme:

$$x_1 = \frac{\begin{vmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 4 & 5 & 5 \end{vmatrix}}{\begin{vmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \\ 2 & 5 & 5 \end{vmatrix}} = \frac{4}{2} = 2, \; x_2 = \frac{\begin{vmatrix} 1 & 1 & 3 \\ 1 & 3 & 1 \\ 2 & 4 & 5 \end{vmatrix}}{\begin{vmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \\ 2 & 5 & 5 \end{vmatrix}} = \frac{2}{2} = 1, \; x_3 = \frac{\begin{vmatrix} 1 & 2 & 1 \\ 1 & 2 & 3 \\ 2 & 5 & 4 \end{vmatrix}}{\begin{vmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \\ 2 & 5 & 5 \end{vmatrix}} = \frac{-2}{2} = -1,$$

□

[2)] Gabriel Cramer, švýcarský matematik, pravidlo z r. 1750, i když bylo známo už dříve.

9.3 Adjungovaná matice

Adjungovaná matice[3)] úzce souvisí s determinanty a maticovou inverzí. Využijeme ji při odvozování Cayley–Hamiltonovy věty (Věta 10.15), ale čtenář se s ní může potkat např. v kryptografii nebo při odvozování vzorečku pro derivaci determinantu.

Definice 9.15 (Adjungovaná matice)**.** Buď $A \in \mathbb{R}^{n\times n}$ a $n \geq 2$. Pak *adjungovaná matice* $\operatorname{adj}(A) \in \mathbb{R}^{n\times n}$ má složky

$$\operatorname{adj}(A)_{ij} = (-1)^{i+j} \det(A^{ji}), \quad i,j = 1,\ldots,n$$

kde opět A^{ji} značí matici vzniklou z A vyškrtnutím j-tého řádku a i-tého sloupce.

Věta 9.16 (O adjungované matici)**.** *Pro každou matici $A \in \mathbb{R}^{n\times n}$ platí $A\operatorname{adj}(A) = \det(A) I_n$.*

Důkaz. Odvodíme

$$\begin{aligned}(A\operatorname{adj}(A))_{ij} &= \sum_{k=1}^{n} A_{ik} \operatorname{adj}(A)_{kj} = \sum_{k=1}^{n} A_{ik}(-1)^{k+j} \det(A^{jk}) \\ &= \begin{cases} \det(A) & \text{pokud } i = j \text{(rozvoj } \det(A) \text{ podle } i\text{-tého řádku)}, \\ 0 & \text{pokud } i \neq j \text{ (determinant matice kde } j\text{-tý řádek nahradíme } i\text{-tým)}. \end{cases}\end{aligned}$$

□

Pro regulární matici A je $\det(A) \neq 0$ a vydělením $\det(A)$ dostaneme explicitní vzoreček pro inverzní matici A^{-1}.

Důsledek 9.17. *Je-li $A \in \mathbb{R}^{n\times n}$ regulární, pak $A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A)$.*

Příklad 9.18 (Adjungovaná matice)**.** Buď

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \\ 2 & 5 & 5 \end{pmatrix}.$$

Pak:

$$\operatorname{adj}(A)_{12} = (-1)^{1+2} \begin{vmatrix} 2 & 3 \\ 5 & 5 \end{vmatrix} = 5, \ \ldots$$

Celkem:

$$\operatorname{adj}(A) = \begin{pmatrix} 5 & 5 & -4 \\ -3 & -1 & 2 \\ 1 & -1 & 0 \end{pmatrix}.$$

Tedy:

$$A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A) = \frac{1}{2} \begin{pmatrix} 5 & 5 & -4 \\ -3 & -1 & 2 \\ 1 & -1 & 0 \end{pmatrix}.$$

□

9.4 Aplikace determinantu

Determinant se používá např. v teorii grafů pro vyjádření počtu koster grafu [Matoušek and Nešetřil, 2009]. Věta o adjungované matici zase dává následující charakterizaci celočíselnosti inverzní matice.

Tvrzení 9.19. *Buď $A \in \mathbb{Z}^{n\times n}$. Pak A^{-1} má celočíselné hodnoty právě tehdy když* $\det(A) = \pm 1$.

Důkaz. Implikace „⇒“. Víme $1 = \det(A)\det(A^{-1})$. Jsou-li matice A, A^{-1} celočíselné, pak i jejich determinanty jsou celočíselné a tudíž musejí být rovny ± 1.

Implikace „⇐“. Víme $A^{-1}_{ij} = \frac{1}{\det(A)}(-1)^{i+j}\det(A^{ji})$. To je celočíselná hodnota pokud $\det(A) = \pm 1$ a $\det(A^{ji})$ je celé číslo. □

[3)] V angličtině *adjugate* nebo *adjoint*.

9.4.1 Geometrická interpretace determinantu

Determinant má pěkný geometrický význam. Uvažujeme-li lineární zobrazení $x \mapsto Ax$, pak geometrická tělesa mění v tomto zobrazení svůj objem s koeficientem $|\det(A)|$. Ukažme si nejprve speciální případ rovnoběžnostěnu. *Rovnoběžnostěn* s lineárně nezávislými hranami $h_1, \dots, h_m$ definujeme jako množinu $\{x \in \mathbb{R}^n;\, x = \sum_{i=1}^m \alpha_i h_i,\ o \le \alpha_i \le 1\}$.

Věta 9.20 (Objem rovnoběžnostěnu)**.** *Buď $A \in \mathbb{R}^{m\times n}$ a uvažujme rovnoběžnostěn s hranami danými řádky matice A. Pak jeho objem je $\sqrt{\det(AA^T)}$. Speciálně, pro $m = n$ je objem $|\det(A)|$.*

Důkaz. (Podrobná idea.) Důkaz provedeme matematickou indukcí podle m. Pro $m = 1$ je to zřejmé, postupme k indukčnímu kroku. Označme

$$A = \begin{pmatrix} a_1^T \\ \vdots \\ a_m^T \end{pmatrix}, \quad D = \begin{pmatrix} a_1^T \\ \vdots \\ a_{m-1}^T \end{pmatrix}.$$

Rozložme $a_m = b_m + c_m$, kde $c_m \in \mathcal{R}(D)$ a $b_m \in \mathcal{R}(D)^\perp$ (tedy c_m je projekce a_m do $\mathcal{R}(D)$). Označme

$$A' = \begin{pmatrix} a_1^T \\ \vdots \\ a_{m-1}^T \\ b_m^T \end{pmatrix}.$$

Od A' k A lze přejít pomocí elementárních řádkových úprav, neboť k poslednímu řádku stačí přičíst c_m, což je lineární kombinace $a_1, \dots, a_{m-1}$. Tedy existují elementární matice $E_1, \dots, E_k$ tak, že $A = E_1 \dots E_k A'$; navíc jejich determinant je 1 protože jen přičítají násobek řádku k jinému. Nyní

$$\begin{aligned} \det(AA^T) &= \det(E_1 \dots E_k A' A'^T E_k^T \dots E_1^T) \\ &= \det(E_k) \dots \det(E_1) \det(A'A'^T) \det(E_k^T) \dots (E_1^T) = \det(A'A'^T). \end{aligned}$$

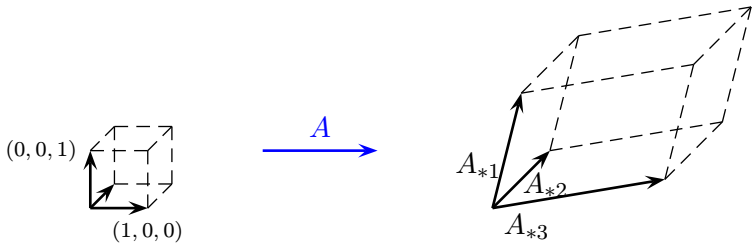
Dále,

$$A'A'^T = \begin{pmatrix} D \\ b_m^T \end{pmatrix} \begin{pmatrix} D^T & b_m \end{pmatrix} = \begin{pmatrix} DD^T & Db_m \\ b_m^T D^T & b_m^T b_m \end{pmatrix} = \begin{pmatrix} DD^T & o^T \\ o & b_m^T b_m \end{pmatrix}$$

Tedy $\det(A'A'^T) = b_m^T b_m \det(DD^T)$ a odmocněním $\sqrt{\det(A'A'^T)} = \|b_m\| \sqrt{\det(DD^T)}$. To odpovídá intuitivní představě objemu jako velikosti výšky krát obsah základny. □

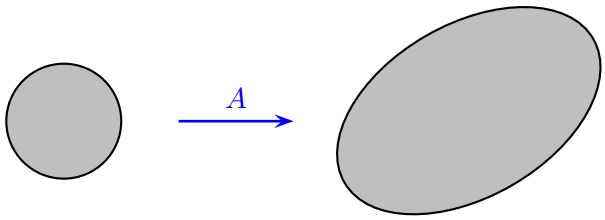
Buď $A \in \mathbb{R}^{n\times n}$. Jak jsme již zmínili, objem geometrických těles se při zobrazení $x \mapsto Ax$ mění s koeficientem $|\det(A)|$. Krychle o hraně 1 se zobrazí na rovnoběžnostěn o hranách, které odpovídají sloupcům matice A, a jeho objem je proto $|\det(A^T)| = |\det(A)|$. Tuto vlastnost můžeme zobecnit na ostatní „rozumná“ geometrická tělesa, protože každé lze aproximovat krychličkami, a jejich obraz je tedy aproximován rovnoběžnostěny a změna objemu je přibližně $|\det(A)|$. Postupným zjemňováním aproximace dostaneme limitním přechodem výsledný poměr.

Příklad 9.21 (Geometrická interpretace determinantu)**.** Obraz jednotkové krychle při zobrazení $x \mapsto Ax$:



objem $= 1$ objem $= \det(A)$

Obraz geometrického tělesa krychle při zobrazení $x \mapsto Ax$:



objem $= V$ objem $= \det(A) \cdot V$

□

Kapitola 10

Vlastní čísla

Vlastní čísla (dříve též nazývaná „charakteristická čísla“), podobně jako determinant, charakterizují jistým způsobem matici. Na rozdíl od determinantu, jejich význam je ještě dalekosáhlejší.

Definice 10.1 (Vlastní čísla a vlastní vektory)**.** Buď $A \in \mathbb{R}^{n\times n}$. Pak $\lambda \in \mathbb{C}$ je *vlastní číslo* matice A a $x \in \mathbb{C}^n$ jemu příslušný *vlastní vektor* pokud $Ax = \lambda x$, $x \neq o$.

Poznamenejme, že $x \neq o$ je nezbytná podmínka, protože pro $x = o$ by rovnost byla triviálně splněna pro každé $\lambda \in \mathbb{C}$. Na druhou stranu, $\lambda = 0$ klidně může nastat.

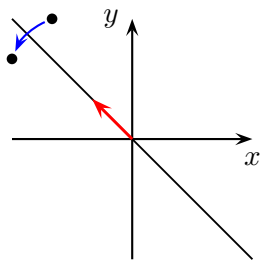
Povšimněme si dále, že vlastní vektory nejsou určeny jednoznačně – každý jeho nenulový násobek je také vlastním vektorem. Někdy se proto vlastní vektor normuje tak, aby $\|x\| = 1$.

Přirozeně, vlastní čísla a vektory lze stejně definovat nad jakýmkoli jiným tělesem. My zůstaneme u $\mathbb{R}$ resp. $\mathbb{C}$. Jak uvidíme později, komplexním číslům se nevyhneme i když matice A je reálná.

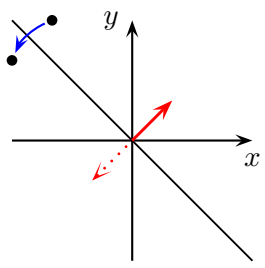
Vlastní čísla se dají zavést i obecněji. Buď V vektorový prostor a $f : V \mapsto V$. Pak λ je vlastní číslo a $x \neq o$ příslušný vlastní vektor pokud platí $f(x) = \lambda x$. My se však vesměs budeme zabývat vlastními čísly matic.

Příklad 10.2 (Geometrická interpretace vlastních čísel a vektorů)**.** Vlastní vektor reprezentuje invariantní směr při zobrazení $x \mapsto Ax$, a vlastní číslo škálování v tomto směru.

- Překlopení dle přímky $y = -x$, matice zobrazení $A = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$:

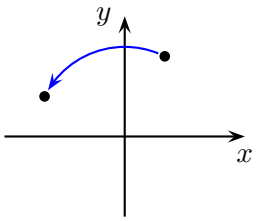


vlastní číslo 1, vlastní vektor $(-1, 1)^T$,



vlastní číslo-1, vlastní vektor $(1, 1)^T$,

- Rotace o úhel 90°, matice zobrazení $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$:



žádná reálná vlastní čísla.

□

Věta 10.3 (Charakterizace vlastních čísel a vektorů). *Buď $A \in \mathbb{R}^{n\times n}$. Pak*

(1) $\lambda \in \mathbb{C}$ je vlastním číslem A právě tehdy když $\det(A - \lambda I_n) = 0$,

(2) $x \in \mathbb{C}^n$ je vlastním vektorem příslušným k vlastnímu číslu $\lambda \in \mathbb{C}$ právě tehdy když $o \neq x \in$ $\operatorname{Ker}(A - \lambda I_n)$.

Důkaz.

(1) $\lambda \in \mathbb{C}$ je vlastním číslem A právě tehdy když $Ax = \lambda I_n x$, $x \neq o$, neboli $(A - \lambda I_n)x = o$, $x \neq o$, což je ekvivalentní singularitě matice $A - \lambda I_n$, a to zase $\det(A - \lambda I_n) = 0$.

(2) Analogicky, $x \in \mathbb{C}^n$ je vlastním vektorem k $\lambda \in \mathbb{C}$ právě tehdy když $(A - \lambda I_n)x = o$, $x \neq o$, tedy x je v jádru matice $A - \lambda I_n$. □

Důsledkem věty je, že k danému vlastnímu číslu λ přísluší $\dim \operatorname{Ker}(A - \lambda I_n) = n - \operatorname{rank}(A - \lambda I_n)$ lineárně nezávislých vlastních vektorů.

Věta 10.4 (Vlastnosti vlastních čísel). *Nechť $A \in \mathbb{R}^{n\times n}$ má vlastní čísla $\lambda_1, \ldots, \lambda_n$ a jim odpovídající vlastní vektory $x_1 \ldots, x_n$. Pak:*

(1) A je regulární právě tehdy když 0 není její vlastní číslo,

(2) je-li A regulární, pak A^{-1} má vlastní čísla $\lambda_1^{-1}, \ldots, \lambda_n^{-1}$ a vlastní vektory $x_1 \ldots, x_n$,

(3) A^2 má vlastní čísla $\lambda_1^2, \ldots, \lambda_n^2$ a vlastní vektory $x_1 \ldots, x_n$,

(4) αA má vlastní čísla $\alpha\lambda_1, \ldots, \alpha\lambda_n$ a vlastní vektory $x_1 \ldots, x_n$,

(5) A^T má vlastní čísla $\lambda_1, \ldots, \lambda_n$, ale vlastní vektory obecně jiné.

Důkaz. Dokážeme první dvě tvrzení, ostatní necháme čtenáři na rozmyšlení.

(1) A má vlastní číslo 0 právě tehdy když $0 = \det(A - 0I_n) = \det(A)$, neboli když A je singulární.

(2) Pro každé $i = 1, \ldots, n$ je $Ax_i = \lambda_i x_i$. Přenásobením A^{-1} dostaneme $x_i = \lambda_i A^{-1} x_i$ a vydělením $\lambda_i \neq 0$ pak $A^{-1}x_i = \lambda_i^{-1} x_i$. □

10.1 Charakteristický polynom

Definice 10.5 (Charakteristický polynom). *Charakteristickým polynomem* matice $A \in \mathbb{R}^{n\times n}$ vzhledem k proměnné λ je $p_A(\lambda) = \det(A - \lambda I_n)$.

Z definice determinantu je patrno, že charakteristický polynom se dá vyjádřit ve tvaru

$$p_A(\lambda) = \det(A - \lambda I_n) = (-1)^n \lambda^n + a_{n-1}\lambda^{n-1} + \ldots a_1\lambda + a_0.$$

Tedy je to skutečně polynom a má stupeň n. Podle základní věty algebry má tento polynom n komplexních kořenů (včetně násobností), označme je $\lambda_1, \ldots, \lambda_n$. Pak

$$p_A(\lambda) = (-1)^n(\lambda - \lambda_1)\ldots(\lambda - \lambda_n).$$

Vidíme tedy, že kořeny $p_A(\lambda)$ odpovídají vlastním číslům matice A, a vlastních čísel je n (včetně násobností).

Definice 10.6 (Spektrum a spektrální poloměr). Nechť $A \in \mathbb{R}^{n\times n}$ má vlastní čísla $\lambda_1, \ldots, \lambda_n$. Pak *spektrum* matice A je množina jejích vlastních čísel a *spektrální poloměr* je $\rho(A) = \max_{i=1,\ldots,n} |\lambda_i|$.

Počítat vlastní čísla jako kořeny charakteristického polynomu není příliš efektivní. Navíc, pro kořeny polynomu neexistuje žádný vzoreček ani konečný postup a počítají se iterativními metodami. Totéž platí i o vlastních číslech (srov. Věta 10.13). Zde nepomůže ani jindy tak oblíbená a všestranná Gaussova eliminace. Nicméně, pro speciální matice, vlastní čísla můžeme určit snadno.

Příklad 10.7.

- Nechť $A \in \mathbb{R}^{n\times n}$ je trojúhelníková matice. Pak její vlastní čísla jsou prvky na diagonále, neboť $\det(A - \lambda I_n) = (a_{11} - \lambda)\dots(a_{nn} - \lambda)$.
- Speciálně, I_n má vlastní číslo 1, které je n-násobné.
- Speciálně, O_n má vlastní číslo 0, které je n-násobné. □

Příklad 10.8. Mějme matici $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ z Příkladu 10.2. Pak

$$p_A(\lambda) = \det(A - \lambda I_n) = \det \begin{pmatrix} -\lambda & -1 \\ 1 & -\lambda \end{pmatrix} = \lambda^2 + 1.$$

Kořeny polynomu, a tedy vlastními čísly matice A jsou $\pm i$. □

Věta 10.9 (Součin a součet vlastních čísel)**.** *Buď $A \in \mathbb{R}^{n\times n}$ s vlastními čísly $\lambda_1, \dots, \lambda_n$. Pak*

(1) $\det(A) = \lambda_1 \dots \lambda_n$,

(2) $a_{11} + \dots + a_{nn} = \lambda_1 + \dots + \lambda_n$.

Důkaz.

(1) Víme, že $\det(A - \lambda I_n) = (-1)^n(\lambda - \lambda_1)\dots(\lambda - \lambda_n)$. Dosazením $\lambda = 0$ dostáváme $\det(A) = (-1)^n(-\lambda_1)\dots(-\lambda_n) = \lambda_1 \dots \lambda_n$.

(2) Porovnejme koeficienty u λ^{n-1} různých vyjádření charakteristického polynomu. V rozvoji $\det(A - \lambda I_n)$ dostáváme, že koeficient vznikne pouze ze součinu $(a_{11} - \lambda)\dots(a_{nn} - \lambda)$, a to $(-1)^{n-1}(a_{11} + \dots + a_{nn})$. Koeficient u λ^{n-1} v rozvoji $(-1)^n(\lambda - \lambda_1)\dots(\lambda - \lambda_n)$ je očividně $(-1)^n(-\lambda_1 - \dots - \lambda_n)$. Porovnáním tedy $(-1)^{n-1}(a_{11} + \dots + a_{nn}) = (-1)^n(-\lambda_1 - \dots - \lambda_n)$. □

Poznamenejme, že porovnáním koeficientů u jiných členů charakteristického polynomu dostaneme další vztahy mezi prvky matice A a vlastními čísly, ale již trochu komplikovanější.

V následující větě je důležité, že matice A je reálná, pro komplexní už tvrzení neplatí.

Věta 10.10. *Buď $A \in \mathbb{R}^{n\times n}$. Je-li $\lambda \in \mathbb{C}$ vlastní číslo A, pak i $\overline{\lambda}$ je vlastním číslem A.*

Důkaz. Víme, že λ je kořenem $p_A(\lambda) = (-1)^n\lambda^n + a_{n-1}\lambda^{n-1} + \dots a_1\lambda + a_0 = 0$. Komplexním sdružením obou stran rovnosti máme $(-1)^n\overline{\lambda}^n + a_{n-1}\overline{\lambda}^{n-1} + \dots a_1\overline{\lambda} + a_0 = 0$, tedy i $\overline{\lambda}$ je kořenem $p_A(\lambda)$. □

Příklad 10.11. Spektrum reálné matice je tedy množina symetrická podle reálné osy. Komplexní matice můžou mít za spektrum jakýchkoli n komplexních čísel. □

Nyní si ukážeme, že výpočet kořenů polynomu lze převést na úlohu hledání vlastních čísel určité matice.

Definice 10.12 (Matice společnice[1])**.** Buď $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$. Pak *matice společnice* polynomu $p(x)$ je čtvercová matice řádu n definovaná

$$C(p) \coloneqq \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}.$$

[1] V angličtině *companion matrix*. V češtině se používají různé termíny, např. doprovodná matice polynomu, matice přidružená polynomu atd. Pojem *matice společnice* začal používat nezávisle autor a někteří lidé z FJFI ČVUT.

Věta 10.13 (O matici společnici)**.** *Platí $p_{C(p)}(\lambda) = (-1)^n p(\lambda)$, tedy vlastní čísla $C(p)$ odpovídají kořenům polynomu $p(\lambda)$.*

Důkaz. Upravme

$$p_{C(p)}(\lambda) = \det(C(p) - \lambda I_n) = \det \begin{pmatrix} -\lambda & \dots & \dots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & -a_2 \\ \vdots & \ddots & \ddots & -\lambda & \vdots \\ 0 & \dots & 0 & 1 & -a_{n-1} - \lambda \end{pmatrix}.$$

Přičtením λ-násobku posledního řádku k předposlednímu, pak λ-násobku předposledního řádku k předpředposlednímu, atd. dostaneme

$$p_{C(p)}(\lambda) = \det \begin{pmatrix} 0 & \dots & \dots & 0 & -p(\lambda) \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} - a_{n-1}\lambda - \lambda^2 \\ 0 & \dots & 0 & 1 & -a_{n-1} - \lambda \end{pmatrix}.$$

Laplaceovým rozvojem podle prvního řádku pak $p_{C(p)}(\lambda) = (-1)^{n+1}(-p(\lambda)) \det(I_{n-1}) = (-1)^n p(\lambda)$. □

Věta má mj. za důsledek, že úloha hledání kořenů reálných polynomů a vlastních čísel matic jsou na sebe navzájem převoditelné. To znamená, že vlastní čísla obecně můžeme počítat pouze numericky, žádný konečný postup neexistuje (praktické numerické metody jsou ale efektivní). Zatímco vlastní čísla se přes kořeny charakteristického polynomu v praxi nepočítají, opačný postup použitelný je (i když se využívají spíš specializované metody).

10.2 Cayley–Hamiltonova věta

Stručně řečeno, Cayley–Hamiltonova věta[2)] říká, že každá čtvercová matice je kořenem svého charakteristického polynomu.

Příklad 10.14. Příklad polynomiální matice resp. maticového polynomu:

$$\begin{pmatrix} \lambda^2 - \lambda & 2\lambda - 3 \\ 7 & 5\lambda^2 - 4 \end{pmatrix} = \lambda^2 \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} + \lambda \begin{pmatrix} -1 & 2 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & -3 \\ 7 & -4 \end{pmatrix}.$$ □

Věta 10.15 (Cayley–Hamiltonova)**.** *Buď $A \in \mathbb{R}^{n\times n}$ a $p_A(\lambda) = (-1)^n\lambda^n + a_{n-1}\lambda^{n-1} + \dots a_1\lambda + a_0$. Pak*

$$(-1)^n A^n + a_{n-1}A^{n-1} + \dots a_1 A + a_0 I_n = 0.$$

Důkaz. Víme, že pro adjungované matice platí $(A - \lambda I_n)\operatorname{adj}(A - \lambda I_n) = \det(A - \lambda I_n) I_n$. Každý prvek $\operatorname{adj}(A - \lambda I_n)$ je polynom stupně nanejvýš $n-1$ proměnné λ, takže se dá vyjádřit ve tvaru $\operatorname{adj}(A - \lambda I_n) = \lambda^{n-1}B_{n-1} + \dots + \lambda B_1 + B_0$ pro určité $B_{n-1}, \dots, B_0 \in \mathbb{R}^{n\times n}$. Dosazením máme

$$(A - \lambda I_n)(\lambda^{n-1}B_{n-1} + \dots + \lambda B_1 + B_0) = \det(A - \lambda I_n) I_n = ((-1)^n\lambda^n + a_{n-1}\lambda^{n-1} + \dots a_1\lambda + a_0) I_n.$$

Roznásobením

$$-B_{n-1}\lambda^n + (AB_{n-1} - B_{n-2})\lambda^{n-1} + \dots + (AB_1 - B_0)\lambda + AB_0 = (-1)^n\lambda^n I_n + a_{n-1}\lambda^{n-1} I_n + \dots a_1\lambda I_n + a_0 I_n.$$

[2)] Arthur Cayley objevil danou identitu r. 1858, William Rowan Hamilton nezávisle na něm r. 1853, oba pouze pro dimenzi 3. Zobecnění pro vyšší řády provedl až Ferdinand Georg Frobenius r. 1878.

Porovnáním koeficientů

$$\begin{aligned} -B_{n-1} &= (-1)^n I_n, \\ AB_j - B_{j-1} &= a_j I_n, \quad j = 1, \dots, n-1, \\ AB_0 &= a_0 I_n, \end{aligned}$$

Vynásobme první rovnici A^n, další A^j a poslední $A^0 = I_n$. Sečtením pak získáme

$$\begin{aligned} &-A^n B_{n-1} + (A^n B_{n-1} - A^{n-1} B_{n-2}) + \ldots + (A^2 B_1 - AB_0) + AB_0 = \\ &= 0 = (-1)^n A^n + a_{n-1} A^{n-1} + \ldots a_1 A + a_0 I_n \end{aligned}$$ □

Důsledek 10.16. *Buď $A \in \mathbb{R}^{n\times n}$. Pak:*

(1) Pro každé $k \in \mathbb{N}$ je $A^k \in \operatorname{span}\{I_n, A, \dots, A^{n-1}\}$, tedy A^k je lineární kombinací $I_n, A, \dots, A^{n-1}$.

(2) je-li A regulární, pak $A^{-1} \in \operatorname{span}\{I_n, A, \dots, A^{n-1}\}$.

Důkaz.

(1) Stačí uvažovat $k \geq n$. Při dělení polynomu λ^k polynomem $p_A(\lambda)$ se zbytkem tak vlastně polynom λ^k rozložíme $\lambda^k = r(\lambda)\, p_A(\lambda) + s(\lambda)$, kde $r(\lambda)$ je polynom stupně $k-n$ a $s(\lambda) = b_{n-1}\lambda^{n-1} + \ldots + b_1\lambda + b_0$ je zbytek. Pak

$$A^k = r(A)\, p_A(A) + s(A) = s(A) = b_{n-1} A^{n-1} + \ldots + b_1 A + b_0 I_n.$$

(2) Víme $p_A(A) = (-1)^n A^n + a_{n-1} A^{n-1} + \ldots a_1 A + a_0 I_n = 0$ a $a_0 \neq 0$ z regularity A. Tedy

$$I = -\frac{(-1)^n}{a_0} A^n - \frac{a_{n-1}}{a_0} A^{n-1} - \ldots - \frac{a_1}{a_0} A = A \left(-\frac{(-1)^n}{a_0} A^{n-1} - \frac{a_{n-1}}{a_0} A^{n-2} - \ldots - \frac{a_1}{a_0} I_n \right).$$

Tudíž vynásobením A^{-1}

$$A^{-1} = -\frac{(-1)^n}{a_0} A^{n-1} - \frac{a_{n-1}}{a_0} A^{n-2} - \ldots - \frac{a_1}{a_0} I_n.$$ □

Podle tohoto důsledku lze velkou mocninu A^k matice A spočítat efektivněji tak, že si najdeme příslušné koeficienty charakteristického polynomu a vyjádříme A^k jako lineární kombinaci $I_n, A, \dots, A^{n-1}$.

Podobně můžeme vyjádřit i A^{-1}, a tím pádem vyjádřit řešení soustavy $Ax = b$ s regulární maticí jako $A^{-1}b = \frac{1}{a_0}(-(-1)^n A^{n-1} b - \ldots - a_1 b)$. Podobný přístup se občas používá pro řešení velmi rozměrných soustav rovnic (tzv. Krylovova metoda), ale tam se uvažuje trochu jiný polynom nižšího stupně.

10.3 Diagonalizovatelnost

Motivací pro diagonalizovatelnost je snaha převést danou matici vhodnými úpravami, které nemění spektrum, na diagonální matice a z nich vyčteme vlastní čísla snadno z diagonály. Těmi „vhodnými úpravami" určitě nebude Gaussova eliminace, protože ta obecně spektrum mění. Je tedy třeba hledat jiné transformace matice.

Jiný pohled je geometrický: víme, že vlastní vektor představuje invariantní směr při zobrazení $x \mapsto Ax$. Nyní si představme, že A představuje matici nějakého lineárního zobrazení $f : V \mapsto V$ vhledem k bázi B. Buď $S = {}_{B'}[id]_B$ matice přechodu od B k jiné bázi B'. Pak $SAS^{-1} = {}_{B'}[f]_{B'}$ je matice zobrazení f vzhledem k nové bázi B'. Nyní diagonalizovatelnost můžeme chápat jako hledání vhodné báze B', aby příslušná matice byla diagonální, a tak jednoduše popisovala chování zobrazení.

Definice 10.17 (Podobnost)**.** Matice $A, B \in \mathbb{R}^{n\times n}$ jsou *podobné* pokud existuje regulární $S \in \mathbb{R}^{n\times n}$ tak, že $A = SBS^{-1}$.

Definice 10.18 (Diagonalizovatelnost)**.** Matice $A \in \mathbb{R}^{n\times n}$ je *diagonalizovatelná* pokud je podobná nějaké diagonální matici.

Příklad 10.19. Ukažte, že podobnost jako binární relace je reflexivní, symetrická a tranzitivní. Tedy jedná se o relaci ekvivalenci. □

Věta 10.20 (Vlastní čísla podobných matic)**.** *Podobné matice mají stejná vlastní čísla.*

Důkaz. Buď $A = SBS^{-1}$. Pak

$$\begin{aligned} p_A(\lambda) &= \det(A - \lambda I_n) = \det(SBS^{-1} - \lambda S I_n S^{-1}) = \det(S(B - \lambda I_n)S^{-1}) \\ &= \det(S)\det(B - \lambda I_n)\det(S^{-1}) = \det(B - \lambda I_n) = p_B(\lambda). \end{aligned}$$

Obě matice mají stejné charakteristické polynomy, tedy i vlastní čísla. □

Uvědomme si, že věta neříká nic o vlastních vektorech. Ale vlastní čísla se podobnostní transformací nemění, tedy pokud matici A diagonalizujeme, tak na diagonále najdeme její vlastní čísla.

Příklad 10.21. Ne každá matice je diagonalizovatelná, např.

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Její vlastní číslo (dvojnásobné) je 0. Pokud by A byla diagonalizovatelná, pak by byla podobná nulové matici, tedy $A = S0S^{-1} = 0$, což je spor. □

Věta 10.22 (Charakterizace diagonalizovatelnosti)**.** *Matice $A \in \mathbb{R}^{n\times n}$ je diagonalizovatelná právě tehdy když má n lineárně nezávislých vlastních vektorů.*

Důkaz. Implikace „⇒“. Je-li A diagonalizovatelná, pak $A = S\Lambda S^{-1}$, kde S je regulární a Λ diagonální. Rovnost přepíšeme $AS = S\Lambda$ a porovnáním j-tých sloupců dostaneme

$$AS_{*j} = (AS)_{*j} = (S\Lambda)_{*j} = S\Lambda_{*j} = S\Lambda_{jj}e_j = \Lambda_{jj}S_{*j}.$$

Tedy Λ_{jj} a S_{*j} příslušný vlastní vektor. Sloupce S jsou lineárně nezávislé.

Implikace „⇐“. Analogicky opačným směrem. Nechť A má vlastní čísla $\lambda_1, \ldots, \lambda_n$ a jim přísluší lineárně nezávislé vlastní vektory $x_1, \ldots, x_n$. Sestavme regulární matici $S \coloneqq (x_1 \mid \cdots \mid x_n)$ a diagonální $\Lambda \coloneqq \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$. Pak

$$(AS)_{*j} = Ax_j = \lambda_j x_j = \Lambda_{jj}S_{*j} = S\Lambda_{jj}e_j = S\Lambda_{*j} = (S\Lambda)_{*j}.$$

Tedy $AS = S\Lambda$, z čehož $A = S\Lambda S^{-1}$. □

Důkaz věty byl konstruktivní, tedy dává návod jak diagonalizovat matici ze znalosti vlastních čísel, a naopak ze znalosti diagonalizace jak najít vlastní vektory (jsou to sloupce matice S).

Příklad 10.23 (Geometrická interpretace diagonalizace)**.** Buď

$$A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}.$$

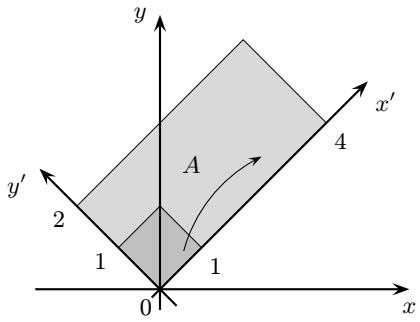
Vlastní čísla a vlastní vektory:

$$\lambda_1 = 4,\ x_1 = (1,1)^T, \quad \lambda_2 = 2,\ x_2 = (-1,1)^T.$$

Diagonalizace:

$$A = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Geometrická interpretace: v souřadném systému vlastních vektorů je matice zobrazení diagonální a zobrazení představuje jen škálování na osách.



□

Nyní si ukážeme, že různým vlastním číslům odpovídají lineárně nezávislé vlastní vektory.

Věta 10.24 (Vlastní vektory různých vlastních čísel)**.** *Nechť $\lambda_1, \ldots, \lambda_k$ jsou navzájem různá vlastní čísla (ne nutně všechna) matice $A \in \mathbb{R}^{n\times n}$. Pak odpovídající vlastní vektory $x_1, \ldots, x_k$ jsou lineárně nezávislé.*

Důkaz. Matematickou indukcí podle k. Pro $k = 1$ zřejmé, neboť vlastní vektor je nenulový.

Indukční krok $k \leftarrow k - 1$. Uvažme lineární kombinaci

$$\alpha_1 x_1 + \ldots + \alpha_k x_k = o. \tag{10.1}$$

Pak přenásobením maticí A:

$$A(\alpha_1 x_1 + \ldots + \alpha_k x_k) = \alpha_1 A x_1 + \ldots + \alpha_k A x_k = \alpha_1 \lambda_1 x_1 + \ldots + \alpha_k \lambda_k x_k = o. \tag{10.2}$$

Odečtením λ_k-násobku (10.1) od (10.2) dostaneme

$$\alpha_1(\lambda_1 - \lambda_k)x_1 + \ldots + \alpha_{k-1}(\lambda_{k-1} - \lambda_k)x_{k-1} = o.$$

Z indukčního předpokladu jsou $x_1, \ldots, x_{k-1}$ lineárně nezávislé, tedy $\alpha_1 = \ldots = \alpha_{k-1} = 0$. Dosazením do (10.1) máme $\alpha_k x_k = o$, neboli $\alpha_k = 0$. □

Důsledek 10.25. *Pokud matice $A \in \mathbb{R}^{n\times n}$ má n navzájem různých vlastních čísel, pak je diagonalizovatelná.*

Příklad 10.26 (Mocnina matice)**.** Buď $A = S\Lambda S^{-1}$ diagonalizace matice $A \in \mathbb{R}^{n\times n}$. Pak $A^2 = S\Lambda S^{-1}S\Lambda S^{-1} = S\Lambda^2 S^{-1}$. Obecněji:

$$A^k = S\Lambda^k S^{-1} = S \begin{pmatrix} \lambda_1^k & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n^k \end{pmatrix} S^{-1}.$$

Můžeme studovat i asymptotické chování. Zjednodušeně:

$$\lim_{k\to\infty} A^k = S \begin{pmatrix} \lim_{k\to\infty} \lambda_1^k & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lim_{k\to\infty} \lambda_n^k \end{pmatrix} S^{-1} = \begin{cases} 0 & \text{pokud } \rho(A) < 1, \\ \text{diverguje} & \text{pokud } \rho(A) > 1, \\ \text{konverguje / diverguje} & \text{pokud } \rho(A) = 1. \end{cases}$$

Případ $\rho(A) = 1$ se nedá obecně rozhodnout. Pro $A = I_n$ matice konverguje k I_n, pro $A = -I_n$ matice osciluje mezi I_n a $-I_n$. □

10.4 Jordanova normální forma

Víme, že ne všechny matice jsou diagonalizovatelné. Nicméně, každá matice lze podobnostní transformací převést na poměrně jednoduchý tvar, nazývaný Jordanova normální forma.[3)]

[3)] Autorem je francouzský matematik Marie Ennemond Camille Jordan. Spolutvůrcem Gauss–Jordanovy eliminace je někdo jiný, německý geodet Wilhelm Jordan.

Definice 10.27 (Jordanova buňka)**.** Buď $\lambda \in \mathbb{C}$, $k \in \mathbb{N}$. *Jordanova buňka* $J_k(\lambda)$ je čtvercová matice řádu k definovaná

$$J_k(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \dots & \dots & 0 & \lambda \end{pmatrix}$$

Jordanova buňka má vlastní číslo λ, které je k-násobné, a přísluší mu pouze jeden vlastní vektor (matice $J_k(\lambda) - \lambda I_k$ má hodnost $k-1$).

Definice 10.28 (Jordanova normální forma)**.** Matice $J \in \mathbb{C}^{n\times n}$ je v *Jordanově normální formě* pokud je v blokově diagonálním tvaru

$$J = \begin{pmatrix} J_{k_1}(\lambda_1) & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & J_{k_m}(\lambda_m) \end{pmatrix}$$

a na diagonále jsou Jordanovy buňky $J_{k_1}(\lambda_1), \dots, J_{k_m}(\lambda_m)$.

Hodnoty λ_i a k_i nemusí být navzájem různé. Stejně tak nějaká Jordanova buňka se může vyskytovat vícekrát.

Věta 10.29 (O Jordanově normální formě)**.** *Každá matice $A \in \mathbb{C}^{n\times n}$ je podobná matici v Jordanově normální formě. Tato matice je až na pořadí buněk určena jednoznačně.*

Důkaz. Viz např. [Bečvář, 2005; Bican, 2009]. □

Příklad 10.30. Matice

$$A = \begin{pmatrix} 5 & -2 & 2 & -2 & 0 \\ 0 & 6 & -1 & 3 & 2 \\ 2 & 2 & 7 & -2 & -2 \\ 2 & 3 & 1 & 2 & -4 \\ -2 & -2 & -2 & 6 & 11 \end{pmatrix}$$

má Jordanovu normální formu

$$\begin{pmatrix} 5 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 7 & 0 & 0 \\ 0 & 0 & 0 & 7 & 1 \\ 0 & 0 & 0 & 0 & 7 \end{pmatrix}.$$

□

Poznámka 10.31 (Velikosti a počet buněk)**.** Počet buněk $J_k(\lambda)$ matice $A \in \mathbb{C}^{n\times n}$ ve výsledné Jordanově normální formě je roven

$$\operatorname{rank}\left((A-\lambda I_n)^{k-1}\right) - 2\operatorname{rank}\left((A-\lambda I_n)^{k}\right) + \operatorname{rank}\left((A-\lambda I_n)^{k+1}\right).$$

Ke konstrukci Jordanovy normální formy tedy nestačí jen znalost vlastních čísel a/nebo vlastních vektorů, ale ještě další informace o výše zmíněných hodnostech matic.

Víme, že počet (lineárně nezávislých) vlastních vektorů, které odpovídají vlastnímu číslu λ, je roven dimenzi $\operatorname{Ker}(A-\lambda I_n)$, tedy číslu $n-\operatorname{rank}(A-\lambda I_n)$. Tato hodnota se podobnostní transformací nemění (je-li $SAS^{-1} = J$, pak $\operatorname{rank}(A-\lambda I_n) = \operatorname{rank}(S(A-\lambda I_n)S^{-1}) = \operatorname{rank}(SAS^{-1} - \lambda I_n) = \operatorname{rank}(J-\lambda I_n)$), proto dostáváme: Počet všech Jordanových buněk odpovídajících λ je roven počtu vlastních vektorů pro λ. A dále, jako důsledek, násobnost každého vlastního čísla λ je vždy větší nebo rovna počtu vlastních vektorů, které mu přísluší.

Příklad 10.32 (Aplikace Jordanovy normální formy)**.**

- Umožňuje zobecnit základní reálné funkce na maticové funkce, tedy zavést např. $\cos(A)$, e^A, ... Je-li $A = SJS^{-1}$, pak reálnou funkci $f : \mathbb{R} \mapsto \mathbb{R}$ zobecníme na $f : \mathbb{R}^{n\times n} \mapsto \mathbb{R}^{n\times n}$ předpisem $f(A) \coloneqq Sf(J)S^{-1}$, kde

$$f(J) \coloneqq \begin{pmatrix} f(J_{k_1}(\lambda_1)) & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & f(J_{k_m}(\lambda_m)) \end{pmatrix}.$$

  Chybí tedy ještě zavést obraz Jordanových buněk $J_{k_i}(\lambda_i)$. Pro $k_i = 1$ je to triviální, jde o matici řádu 1. Pro $k_i > 1$ je předpis složitější [Meyer, 2000]:

$$f(J_{k_i}(\lambda_i)) \coloneqq \begin{pmatrix} f(\lambda_i) & f'(\lambda_i) & \dots & \frac{f^{(k_i-1)}(\lambda_i)}{(k_i-1)!} \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & f'(\lambda_i) \\ 0 & \dots & 0 & f(\lambda_i) \end{pmatrix}.$$

- Již jsme v Příkladu 10.26 zmínili využití diagonalizace pro počítání mocniny matice. Pomocí Jordanovy normální formy můžeme tvrzení zobecnit pro libovolné $A \in \mathbb{C}^{n\times n}$: Buď $A = SJS^{-1}$, pak

$$A^k = SJ^kS^{-1} = S \begin{pmatrix} J_{k_1}(\lambda_1)^k & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & J_{k_m}(\lambda_m)^k \end{pmatrix} S^{-1}.$$

  Asymptoticky:

$$\lim_{k\to\infty} A^k = \begin{cases} 0 & \text{pokud } \rho(A) < 1, \\ \text{diverguje} & \text{pokud } \rho(A) > 1, \\ \text{konverguje / diverguje} & \text{pokud } \rho(A) = 1. \end{cases}$$

□

Příklad 10.33 (Soustava lineárních diferenciálních rovnic)**.** Homogenní soustava lineárních diferenciálních rovnic 1. řádu s konstantními koeficienty:

$$u(t)' = Au(t),$$

kde $u : \mathbb{R} \mapsto \mathbb{R}^n$ je neznámá funkce a $u(t_0) = u_0$ počáteční podmínka. Hledáme řešení ve tvaru $u(t)_i = v_i e^{\lambda t}$, kde v_i, λ jsou neznámé. Dosazením:

$$\lambda e^{\lambda t} v = e^{\lambda t} Av, \quad \text{neboli} \quad \lambda v = Av.$$

Vede na výpočet vlastních čísel $\lambda_1, \dots, \lambda_n$ a vektorů $x_1, \dots, x_n$. Řešení je $u(t) = \sum_{i=1}^n \alpha_i e^{\lambda_i t} x_i$, kde $\alpha_i \in \mathbb{R}$ (získá se z poč. podm.).

Uvažme konkrétní příklad:

$$u_1' = 7u_1 - 4u_2$$
$$u_2' = 5u_1 - 2u_2$$

Matice $\begin{pmatrix} 7 & -4 \\ 5 & -2 \end{pmatrix}$ má vlastní čísla 2 a 3, jim odpovídají vlastní vektory $(4, 5)^T$ a $(1, 1)^T$. Řešení úlohy jsou tvaru

$$\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = a \cdot e^{2t} \begin{pmatrix} 4 \\ 5 \end{pmatrix} + b \cdot e^{3t} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad a, b \in \mathbb{R}.$$

□

10.5 Symetrické matice

Reálné symetrické matice mají řadu pozoruhodných vlastností týkající se vlastních čísel. Jejich vlastní čísla jsou reálná, a jsou vždy diagonalizovatelné.

Nejprve se podívejme na zobecnění transpozice a symetrických matic pro komplexní matice.

Definice 10.34 (Hermitovská matice a transpozice)**.** *Hermitovská transpozice* matice $A \in \mathbb{C}^{n\times n}$ je matice $A^* \coloneqq \overline{A}^T$. Matice $A \in \mathbb{C}^{n\times n}$ se nazývá *hermitovská* pokud $A^* = A$.

Pomocí hermitovské transpozice můžeme unitární matice (rozšiřující pojem ortogonální matice pro komplexní matice, viz Definice 8.29) definovat jako matice $Q \in \mathbb{C}^{n\times n}$ splňující $Q^*Q = I_n$.

Příklad 10.35. Z matic

$$\begin{pmatrix} 2 & i \\ i & 5 \end{pmatrix}, \quad \begin{pmatrix} 2 & i \\ -i & 5 \end{pmatrix}$$

je první symetrická, ale ne hermitovská, a druhá je hermitovská, ale ne symetrická. Pro reálné matice oba pojmy splývají. □

Věta 10.36 (Vlastní čísla symetrických matic)**.** *Vlastní čísla reálných symetrických (resp. komplexních hermitovských) jsou reálná.*

Důkaz. Buď $A \in \mathbb{C}^{n\times n}$, $\lambda \in \mathbb{C}$ libovolné vlastní číslo a $x \in \mathbb{C}^n$ příslušný vlastní vektor jednotkové velikosti, tj. $\|x\|_2 = 1$. Pak $Ax = \lambda x$, přenásobením x^* máme $x^*Ax = \lambda x^*x = \lambda$. Hermitovskou transpozicí obou stran dostaneme

$$\lambda = x^*Ax = x^*A^*x = (x^*Ax)^* = \lambda^*.$$

Tedy $\lambda = \lambda^*$ a proto $\lambda \in \mathbb{R}$. □

Poznamenejme, že komplexní symetrické matice mohou mít ryze komplexní vlastní čísla.

Následující věta říká, že symetrické matice jsou diagonalizovatelné[4)]. Navíc také, že lze vybrat n vlastních vektorů, které jsou na sebe navzájem kolmé (jsou to sloupce Q).

Věta 10.37 (Spektrální rozklad symetrických matic)**.** *Pro každou symetrickou matici $A \in \mathbb{R}^{n\times n}$ existuje ortogonální $Q \in \mathbb{R}^{n\times n}$ a diagonální $\Lambda \in \mathbb{R}^{n\times n}$ tak, že $A = Q\Lambda Q^T$.*

Důkaz. Matematickou indukcí podle n. Případ $n = 1$ je triviální: $\Lambda = A$, $Q = 1$.

Indukční krok $n \leftarrow n-1$. Buď λ vlastní číslo A a x odpovídající vlastní vektor normovaný $\|x\|_2 = 1$. Doplňme x, jakožto ortonormální systém (Důsledek 8.19), na ortogonální matici $S \coloneqq (x \mid \cdots)$. Upravme matici $S^T(A - \lambda I_n)S = S^T(o \mid \cdots) = (o \mid \cdots)$. Protože tato matice je symetrická, máme

$$S^T(A - \lambda I_n)S = \begin{pmatrix} 0 & o^T \\ o & A' \end{pmatrix},$$

kde A' je nějaká symetrická matice řádu $n-1$. Podle indukčního předpokladu má spektrální rozklad $A' = Q'\Lambda'Q'^T$, kde Λ' je diagonální a Q' ortogonální. Matice a rovnost rozšíříme o jeden řád takto:

$$\begin{pmatrix} 0 & o^T \\ o & A' \end{pmatrix} = \begin{pmatrix} 1 & o^T \\ o & Q' \end{pmatrix} \begin{pmatrix} 0 & o^T \\ o & \Lambda' \end{pmatrix} \begin{pmatrix} 1 & o^T \\ o & Q'^T \end{pmatrix}.$$

Označme

$$R \coloneqq \begin{pmatrix} 1 & o^T \\ o & Q' \end{pmatrix}, \quad \Lambda'' \coloneqq \begin{pmatrix} 0 & o^T \\ o & \Lambda' \end{pmatrix}.$$

Matice R je ortogonální (Věta 8.33(4)), matice Λ'' diagonální. Nyní můžeme psát

$$S^T(A - \lambda I_n)S = R\Lambda''R^T,$$

[4)] A.L. Cauchy, r. 1829.

z čehož

$$A = SR\Lambda'' R^T S^T + \lambda I_n = SR\Lambda'' R^T S^T + \lambda SRR^T S^T = SR(\Lambda'' + \lambda I_n)R^T S^T.$$

Nyní máme hledaný rozklad $A = Q\Lambda Q^T$, kde $Q := SR$ je ortogonální matice a $\Lambda := \Lambda'' + \lambda I_n$ je diagonální. □

Podobně můžeme spektrálně rozložit hermitovské matice $A = Q\Lambda Q^*$, kde Q je unitární matice.

Jedním z pěkných důsledků je následující, byť trochu teoretický, vzoreček na výpočet největšího a nejmenšího vlastního čísla[5)].

Věta 10.38 (Courant–Fischer)**.** *Nechť $\lambda_1 \geq \cdots \geq \lambda_n$ jsou vlastní čísla symetrické matice $A \in \mathbb{R}^{n\times n}$. Pak*

$$\lambda_1 = \max_{x:\|x\|_2=1} x^T Ax, \quad \lambda_n = \min_{x:\|x\|_2=1} x^T Ax.$$

Důkaz. Pouze pro λ_1, druhá část je analogická.

Nerovnost „$\leq$“: Buď x_1 vlastní vektor příslušný k λ_1 normovaný $\|x_1\|_2 = 1$. Pak $Ax_1 = \lambda_1 x_1$. Přenásobením x_1^T zleva dostaneme

$$\lambda_1 = \lambda_1 x_1^T x_1 = x_1^T AX_1 \leq \max_{x:\|x\|_2=1} x^T Ax.$$

Nerovnost „$\geq$“: Buď $x \in \mathbb{R}^n$ libovolný vektor takový, že $\|x\|_2 = 1$. Označme $y := Q^T x$, pak $\|y\|_2 = 1$ (Věta 8.33(2)). S využitím spektrálního rozkladu $A = Q\Lambda Q^T$ dostaneme:

$$x^T Ax = x^T Q\Lambda Q^T x = y^T \Lambda y = \sum_{i=1}^n \lambda_i y_i^2 \leq \sum_{i=1}^n \lambda_1 y_i^2 = \lambda_1 \|y\|_2^2 = \lambda_1.$$ □

10.6 Teorie nezáporných matic

Perron–Frobeniova teorie nezáporných matic[6)] je pokročilá teorie kolem vlastních čísel nezáporných matic. Uvedeme si jen základní výsledek bez důkazu.

Věta 10.39 (Perronova)**.**

(1) Buď $A \in \mathbb{R}^{n\times n}$ nezáporná matice (tj. $a_{ij} \geq 0\ \forall i,j$). Pak největší (v absolutní hodnotě) vlastní číslo je reálné nezáporné a příslušný vlastní vektor je nezáporný (ve všech složkách).

(2) Buď $A \in \mathbb{R}^{n\times n}$ kladná matice (tj. $a_{ij} > 0\ \forall i,j$). Pak největší (v absolutní hodnotě) vlastní číslo je reálné kladné, je jediné, a příslušný vlastní vektor je kladný (ve všech složkách). Navíc žádnému jinému vlastnímu číslu neodpovídá nezáporný vlastní vektor.

Důkaz. Viz např. [Meyer, 2000]. □

Příklad 10.40 (Markovovy řetězce)**.** Jedním z využití mocnin matice (Příklad 10.32) a trochu i teorie nezáporných matic jsou Markovovy řetězce. Ilustrujeme si je na konkrétním příkladu:

Migrace obyvatel USA město–předměstí–venkov probíhá podle vzorce:

z města:	96% zůstane, 3% do předměstí, 1% na venkov,
z předměstí:	1% do města, 98% zůstane, 1% na venkov,
z venkova:	1.5% do města, 0.5% do předměstí, 98% zůstane.

Počáteční stav: 58 mil. ve městě, 142 mil. předměstí, 60 mil. venkov. Jak se bude situace vyvíjet v čase? Označme

$$A := \begin{pmatrix} 0.96 & 0.01 & 0.015 \\ 0.03 & 0.98 & 0.005 \\ 0.01 & 0.01 & 0.98 \end{pmatrix}, \quad x_0 = (58, 142, 60)^T.$$

[5)] Ernst Fischer odvodil vzorec r. 1905, Richard Courant ho zobecnil pro nekonečně rozměrné operátory r. 1920. Jejich vzorec zahrnuje i mezilehlá vlastní čísla $\lambda_2, \ldots, \lambda_{n-1}$, ale pro ně je to trochu komplikovanější. Tato jednodušší verze se také někdy nazývá Rayleigh-Ritzova věta.

[6)] Základní věta je od německého matematika Oskara Perrona z r. 1907, a byla rozšířena Ferdinandem Georgem Frobeniem r. 1912.

Vývoj v čase: Ax_0, A^2x_0, A^3x_0, $\ldots$,$A^\infty x_0$. Diagonalizací spočítáme

$$A = Q\begin{pmatrix}1 & 0 & 0\\ 0 & 0.95 & 0\\ 0 & 0 & 0.97\end{pmatrix}Q^{-1} \quad \Rightarrow \quad A^\infty = \begin{pmatrix}0.23 & 0.23 & 0.23\\ 0.43 & 0.43 & 0.43\\ 0.33 & 0.33 & 0.33\end{pmatrix}.$$

Tedy (bez ohledu na počáteční stav x_0) bude se rozložení obyvatelstva ustálí na hodnotách: 23% ve městě, 43% předměstí, 33% venkov. □

10.7 Výpočet vlastních čísel

Jak jsme již zmínili (poznámky k Větě 10.13), vlastní čísla se počítají veskrze numerickými iteračními metodami, a hledat je jako kořeny charakteristického polynomu není efektivní postup. V této sekci si ukážeme jednoduchý odhad na vlastní čísla, a jednoduchou metodu na výpočet největšího vlastního čísla. Další metodu, populární QR algoritmus, probereme v Sekci 13.3. Pro velmi přesný výpočet vlastních čísel symetrických (zvláště tzv. positivně definitních) matic se používá také Jacobiho metoda (viz např. [Rohn, 2004]) a pro velké řídké symetrické matice např. Lanczosova metoda[7] (viz [Meyer, 2000]).

Nejprve uvedeme jednoduchý odhad pro vlastní čísla, tzv. Gerschgorinovy disky[8].

Věta 10.41 (Gerschgorinovy disky)**.** *Každé vlastní číslo λ matice $A \in \mathbb{C}^{n\times n}$ leží v nějakém kruhu o středu a_{ii} a poloměru $\sum_{j\neq i}|a_{ij}|$, $i \in \{1,\ldots,n\}$.*

Důkaz. Buď $Ax = \lambda x$ a vezměme $i := \arg\max_{k=1,\ldots,n}|x_k|$. Pak i-tá rovnice má tvar $\sum_{j=1}^n a_{ij}x_j = \lambda x_i$. Vydělením $x_i \neq 0$ dostáváme

$$\lambda = a_{ii} + \sum_{j\neq i} a_{ij}\frac{x_j}{x_i}$$

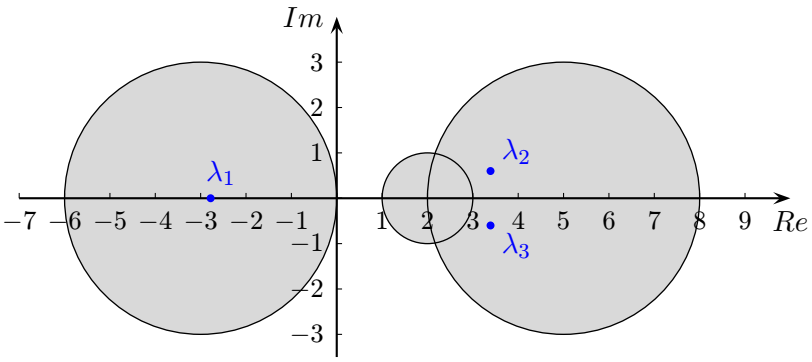
a tím pádem

$$|\lambda - a_{ii}| = \Big|\sum_{j\neq i} a_{ij}\frac{x_j}{x_i}\Big| \leq \sum_{j\neq i}|a_{ij}|\frac{|x_j|}{|x_i|} \leq \sum_{j\neq i}|a_{ij}|. \qquad \square$$

Příklad 10.42. Mějme

$$A = \begin{pmatrix}2 & 1 & 0\\ -2 & 5 & 1\\ -1 & -2 & -3\end{pmatrix}, \quad \text{vlastní čísla: } -2.78,\ 3.39 \pm 0.6\,i$$

Vlastní čísla matice jsou $\lambda_1 = -2.78$, $\lambda_2 = 3.39 + 0.6\,i$, $\lambda_3 = 3.39 - 0.6\,i$.



Vidíme, že ne každý kruh obsahuje nějaké vlastní číslo. Nicméně platí [Meyer, 2000] , že v každé komponentě souvislosti je tolik vlastních čísel, z kolika kruhů daná komponenta vznikla. □

[7] Algoritmus pochází z r. 1950 od maďarského matematika Cornelia Lanczose.

[8] Pochází z r. 1931, a autorem je běloruský matematik Semyon Aranovich Gerschgorin. Nicméně tvrzení bylo známo už dříve: L. Lévy (1881), H. Minkowski (1900), J. Hadamard (1903).

Věta dává jednoduchý odhad na velikost vlastních čísel (existují i vylepšení, např. Cassiniho ovály atp.). V některých aplikacích může takovýto odhad postačovat, ale většinou se používá jako kriterium pro zastavení výpočtu iteračních metod. Např. Jacobiho metoda spočívá na postupném zmenšování nediagonálních prvků symetrické matice, takže matice konverguje k diagonální matici. Gerschgorinovy disky pak dávají horní mez na přesnost vypočtených vlastních čísel.

Gerschgorinovy disky dávají také následující postačující podmínku[9] pro regularitu matice $A \in \mathbb{R}^{n\times n}$: $|a_{ii}| > \sum_{j\neq i} |a_{ij}|\ \forall i = 1, \ldots, n$. V tomto případě totiž disky neobsahují počátek a proto nula není vlastním číslem A. Matice s touto vlastností se nazývají *diagonálně dominantní*.

Nyní si ukážeme jednoduchou metodu na výpočet dominantního vlastního čísla[10] Přes svou jednoduchost se stala základem některých numerických metod tohoto typu, např. inverzní mocninná metoda[11], nebo metoda Rayleighova podílu[12] pro symetrické matice.

Algoritmus 10.43 (Mocninná metoda)**.** Buď $A \in \mathbb{R}^{n\times n}$.

1: Zvol $o \neq x_0 \in \mathbb{R}^n$, $i \coloneqq 1$,
2: **while not** konec **do**
3: $\quad y_i \coloneqq Ax_{i-1}$,
4: $\quad x_i \coloneqq \frac{1}{\|y_i\|} y_i$,
5: $\quad i \coloneqq i + 1$,
6: **end while**

Výstup: $\lambda_1 \coloneqq x_{i-1}^T y_i$, $v_1 \coloneqq x_i$.

Příklad 10.44. Mějme

$$A = \begin{pmatrix} 2 & 4 & 2 \\ 4 & 2 & 2 \\ 2 & 2 & -1 \end{pmatrix}, \quad x_0 = (1, 0, 1)^T.$$

Postup výpočtu a zdrojový kód pro Matlab / Octave:

i	x_i	$x_{i-1}^T y_i$
0	$(1.00, 0.00, 1.00)^T$	2.5
1	$(0.67, 1.00, 0.17)^T$	6.32
2	$(1.00, 0.88, 0.56)^T$	6.94
3	$(0.97, 1.00, 0.47)^T$	6.99
4	$(1.00, 1.00, 0.50)^T$	7

```
A=[2 4 2; 4 2 2; 2 2 -1];
x=[1;0;1];
for i=1:5
  y=A*x;
  x=y/norm(y);
  x/max(abs(x)),
  (y'*x),
end
```

□

Metodu ukončíme ve chvíli, když se hodnota $x_{i-1}^T y_i$ ustálí. Metoda může být pomalá, špatně se odhaduje chyba a míra konvergence a navíc velmi záleží na počáteční volbě x_0. Na druhou stranu, je robustní (zaokrouhlovací chyby nemají velký vliv) a snadno aplikovatelné na velké řídké matice. Ne vždy metoda konverguje, ale za určitých předpokladů se to dá zajistit.

Věta 10.45 (Konvergence mocninné metody)**.** *Buď $A \in \mathbb{R}^{n\times n}$ s vlastními čísly $|\lambda_1| > |\lambda_2| \geq \ldots \geq |\lambda_n|$ a odpovídajícími lineárně nezávislými vektory $v_1, \ldots, v_n$ velikosti 1. Nechť x_0 má nenulovou složku ve směru v_1. Pak x_i konverguje k v_1 a $x_{i-1}^T y_i$ konverguje k λ_1.*

Důkaz. Nechť $x_0 = \sum_{j=1}^n \alpha_j v_j$, kde $\alpha_1 \neq 0$ podle předpokladu. Pak $x_i = \frac{1}{\|A^i x_0\|} A^i x_0$ a

$$A^i x_0 = A^i \Big(\sum_{j=1}^n \alpha_j v_j \Big) = \sum_{j=1}^n \alpha_j A^i v_j = \sum_{j=1}^n \alpha_j \lambda_j^i v_j = \lambda_1^i \Big(\alpha_1 v_1 + \sum_{j\neq 1} \alpha_j \Big(\frac{\lambda_j}{\lambda_1} \Big)^i v_j \Big).$$

[9] Tzv. Lévy–Desplanquesova věta.

[10] Mocninou metodu, anglicky *power method*, představil americký matematik a fyzik Richard Edler von Mises r. 1929.

[11] Autorem je německý matematik Helmut Wielandt, z r. 1944, anglicky *inverse iteration*.

[12] Autorem anglický fyzik John William Strutt, lord Rayleigh, nositel Nobelovy ceny za fyziku (1904), anglicky *Rayleigh quotient iteration*.

Protože vektory x_i postupně normujeme, násobek λ_1^i nás nemusí zajímat. Zbylý vektor postupně konverguje k $\alpha_1 v_1$, protože $\left|\frac{\lambda_j}{\lambda_1}\right| < 1$.

Nyní předpokládejme, že x_i již dobře aproximuje vlastní vektor v_1. Pak $x_{i-1}^T y_i = x_{i-1}^T A x_{i-1} = x_{i-1}^T \lambda_1 x_{i-1} = \lambda_1 \|x_{i-1}\|^2 = \lambda_1$. □

Z důkazu věty vidíme, že rychlost konvergence výrazně závisí na poměru $\left|\frac{\lambda_2}{\lambda_1}\right|$. Poznamenejme, že vzhledem k tomu, že λ_1 je dominantní vlastní číslo, tak musí být reálné a v_1 rovněž tak (Věta 10.10).

Mocninná metoda počítá jen dominantní vlastní číslo a vektor. Následující technika ale umožňuje jednoduchou transformací vynulovat jedno vlastní číslo, a tak rekurzivně dopočítat mocninnou metodou i zbylá vlastní čísla. Pro jednoduchost uvádíme verzi pro symetrické matice.

Věta 10.46 (O deflaci dominantního vlastního čísla)**.** *Buď $A \in \mathbb{R}^{n\times n}$ symetrická, $\lambda_1, \ldots, \lambda_n$ její vlastní čísla a $v_1, \ldots, v_n$ odpovídající ortonormální vlastní vektory. Pak matice $A - \lambda_1 v_1 v_1^T$ má vlastní čísla $0, \lambda_2, \ldots, \lambda_n$ a vlastní vektory $v_1, \ldots, v_n$.*

Důkaz. Počítejme $(A - \lambda_1 v_1 v_1^T)v_1 = Av_1 - \lambda_1 v_1 v_1^T v_1 = \lambda_1 v_1 - \lambda_1 v_1 = o$, tedy 0 je vlastní číslo k v_1. Buď $i \in \{2, \ldots, n\}$, pak $(A - \lambda_1 v_1 v_1^T)v_i = Av_i - \lambda_1 v_1 v_1^T v_i = \lambda_i v_i - o = \lambda_i v_i$, tedy λ_i je vlastní číslo k v_i. □

Příklad 10.47 (Vyhledávač Google™ a PageRank[13])**.** Uvažujme webovou síť:

$$\begin{aligned} &N \text{ webových stránek,} \\ &a_{ij} = \begin{cases} 1 & j\text{-tá stránka odkazuje na } i\text{-tou} \\ 0 & \text{jinak} \end{cases}, \\ &b_j = \text{počet odkazů z } j\text{-té stránky,} \\ &x_i = \text{důležitost } i\text{-té stránky.} \end{aligned}$$

Důležitost i-té stránky stanovíme tak, aby byla úměrná součtu důležitosti stránek na ni odkazujících. Řešíme tedy $x_i = \sum_{j=1}^n \frac{a_{ij}}{b_j} x_j$, $i = 1, \ldots, N$. Maticově $A'x = x$, kde $a'_{ij} \coloneqq \frac{a_{ij}}{b_j}$. Tedy x je vlastní vektor k vlastnímu číslu 1. Vlastní číslo 1 je dominantní, což snadno nahlédneme z Gerschgorinových disků pro matici A'^T (součet sloupců matice A' je roven 1). Podle Perronovy Věty 10.39 je vlastní vektor x nezáporný. Ten pak normujeme a složky zaokrouhlíme, aby měly hodnoty v rozmezí $0, 1, 2, \ldots, 10$.

Matice A' je obrovská $\approx 10^{10}$, a zároveň řídká (Většina hodnot jsou nuly). Proto se na výpočet x hodí mocninná metoda, stačí ≈ 100 iterací. Prakticky se ještě matice A' trochu upravuje, aby byla stochastická, aperiodická a ireducibilní (vadilo by např. když z nějaké stránky není odkaz na žádnou jinou), více viz [Langville and Meyer, 2006; Tůma, 2003].

Příklady Page ranku (k roku 2010):

`www.google.com`	10
`www.cuni.cz`	8
`www.mff.cuni.cz`	7
`kam.mff.cuni.cz`	6
`kam.mff.cuni.cz/~hladik`	4

□

[13] Z r. 1997, autory jsou Sergey Brin a Larry Page.

Kapitola 11

Positivně (semi-)definitní matice

Definice 11.1 (Positivně (semi-)definitní matice)**.** Buď $A \in \mathbb{R}^{n\times n}$ symetrická. Pak A je *positivně semi-definitní* pokud $x^TAx \geq 0\ \forall x \in \mathbb{R}^n$, a A je *positivně definitní* pokud $x^TAx > 0\ \forall x \neq o$.

Zřejmě, pokud A je positivně definitní, pak je i positivně semidefinitní.

Definice dává smysl i pro nesymetrické matice, ale ty můžeme snadno zesymetrizovat $\frac{1}{2}(A + A^T)$, neboť

$$x^T\frac{1}{2}(A + A^T)x = \frac{1}{2}x^TAx + \frac{1}{2}x^TA^Tx = \frac{1}{2}x^TAx + (\frac{1}{2}x^TAx)^T = x^TAx.$$

Tedy pro testování podmínky lze použít symetrickou matici $\frac{1}{2}(A + A^T)$. Omezení na symetrické matice je tudíž bez újmy na obecnosti. Důvod, proč se omezujeme na symetrické matice, je, že řada testovacích podmínek funguje pouze pro symetrické matice.

Příklad 11.2. Příkladem positivně semidefinitní matice je 0_n. Příkladem positivně definitní matice je I_n, neboť $x^TAx = x^TI_nx = x^Tx = \|x\|_2^2 > 0\ \forall x \neq o$. □

Věta 11.3 (Vlastnosti positivně definitních matic)**.**

(1) Jsou-li $A, B \in \mathbb{R}^{n\times n}$ positivně definitní, pak i $A + B$ je positivně definitní,

(2) Je-li $A \in \mathbb{R}^{n\times n}$ positivně definitní a $\alpha > 0$, pak i αA je positivně definitní,

(3) Je-li $A \in \mathbb{R}^{n\times n}$ positivně definitní, pak i A^{-1} je positivně definitní.

Důkaz. První dvě vlastnosti jsou triviální, ukážeme si tu třetí.

Nejprve ukážeme regularitu matice A. Buď x řešení $Ax = o$. Pak $x^TAx = x^To = 0$. Z předpokladu musí $x = o$.

Nyní ukážeme positivní definitnost. Sporem nechť $x \neq o$ tak, že $x^TA^{-1}x \leq 0$. Pak

$$x^TA^{-1}x = x^TA^{-1}AA^{-1}x = y^TAy \leq 0,$$

kde $y = Ax \neq o$. To je spor, neboť A je positivně definitní. □

Analogie věty platí i pro positivně semidefinitní matice. Část (1) platí beze změny, část (2) platí pro všechna $\alpha \geq 0$, ale část (3) už neplatí.

Věta 11.4 (Charakterizace positivní definitnosti)**.** *Buď $A \in \mathbb{R}^{n\times n}$ symetrická. Pak následující podmínky jsou ekvivalentní:*

(1) A je positivně definitní,

(2) vlastní čísla A jsou kladná,

(3) existuje $U \in \mathbb{R}^{m\times n}$ hodnosti n taková, že $A = U^TU$.

Důkaz. Implikace (1) ⇒ (2): Sporem nechť existuje vlastní číslo $\lambda \leq 0$, a x je příslušný vlastní vektor s normou 1. Pak $Ax = \lambda x$ implikuje $x^TAx = \lambda x^Tx = \lambda \leq 0$. To je spor s positivní definitností A.

Implikace (2) ⇒ (3): Protože A je symetrická, má spektrální rozklad $A = Q\Lambda Q^T$, kde Λ je diagonální matice s prvky $\lambda_1, \ldots, \lambda_n > 0$. Definujme matici Λ' jako diagonální s prvky $\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_n} > 0$. Pak

hledaná matice je $U = \Lambda' Q^T$, neboť $U^T U = Q\Lambda'\Lambda' Q^T = Q\Lambda'^2 Q^T = Q\Lambda Q^T = A$. Uvědomme si, že U má hodnost n a je tudíž regulární, neboť je součinem dvou regulárních matic.

Implikace (3) $\Rightarrow$ (1): Sporem nechť $x^T Ax \leq 0$ pro nějaké $x \neq o$. Pak $0 \geq x^T Ax = x^T U^T Ux = (Ux)^T Ux = \langle Ux, Ux\rangle = \|Ux\|_2^2$. Tedy musí $Ux = o$, ale sloupce U jsou lineárně nezávislé, a tak $x = o$, spor. □

Pro positivní semidefinitnost máme následující charakterizaci. Důkaz již neuvádíme, je analogický.

Věta 11.5 (Charakterizace positivní semidefinitnosti)**.** *Buď $A \in \mathbb{R}^{n\times n}$ symetrická. Pak následující podmínky jsou ekvivalentní:*

(1) A je positivně semidefinitní,

(2) vlastní čísla A jsou nezáporná,

(3) existuje $U \in \mathbb{R}^{m\times n}$ taková, že $A = U^T U$.

11.1 Metody na testování positivní definitnosti

Nyní se zaměříme na konkrétní metody pro testování positivní definitnosti. Řada z nich vychází z následujícího rekurentního vztahu. Povšimněme si, že pro testování positivní semidefinitnosti uzpůsobit nelze.

Věta 11.6 (Rekurentní vzoreček na testování positivní definitnosti)**.** *Symetrická matice $A = \left(\begin{smallmatrix} \alpha & a^T \\ a & \tilde{A} \end{smallmatrix}\right)$, kde $\alpha \in \mathbb{R}$, $a \in \mathbb{R}^{n-1}$, $\tilde{A} \in \mathbb{R}^{(n-1)\times(n-1)}$ je positivně definitní právě tehdy když $\alpha > 0$ a $\tilde{A} - \frac{1}{\alpha} aa^T$ je positivně definitní.*

Důkaz. Implikace „⇒“. Buď A positivně definitní. Pak $x^T Ax > 0$ pro všechny $x \neq o$, tedy speciálně pro $x = e_1$ dostáváme $\alpha = e_1^T Ae_1 > 0$. Dále, buď $\tilde{x} \in \mathbb{R}^{n-1}$, $\tilde{x} \neq o$. Pak

$$\tilde{x}^T\big(\tilde{A} - \tfrac{1}{\alpha} aa^T\big)\tilde{x} = \tilde{x}\tilde{A}\tilde{x} - \tfrac{1}{\alpha}(a^T\tilde{x})^2 = \begin{pmatrix} -\frac{1}{\alpha}a^T\tilde{x} & \tilde{x}^T \end{pmatrix} \begin{pmatrix} \alpha & a^T \\ a & \tilde{A} \end{pmatrix} \begin{pmatrix} -\frac{1}{\alpha}a^T\tilde{x} \\ \tilde{x} \end{pmatrix} > 0.$$

Implikace „⇐“. Buď $x = \left(\begin{smallmatrix} \beta \\ \tilde{x} \end{smallmatrix}\right) \in \mathbb{R}^n$. Pak

$$x^T Ax = \begin{pmatrix} \beta & \tilde{x}^T \end{pmatrix} \begin{pmatrix} \alpha & a^T \\ a & \tilde{A} \end{pmatrix} \begin{pmatrix} \beta \\ \tilde{x} \end{pmatrix} = \alpha\beta^2 + 2\beta a^T\tilde{x} + \tilde{x}\tilde{A}\tilde{x} = \tilde{x}^T\big(\tilde{A} - \tfrac{1}{\alpha}aa^T\big)\tilde{x} + \big(\sqrt{\alpha}\beta + \tfrac{1}{\sqrt{\alpha}}a^T\tilde{x}\big)^2 \geq 0.$$

Rovnost nastane pouze když $\tilde{x} = o$ a druhý čtverec je nulový, tj. $\beta = 0$. □

Přestože rekurentní vzoreček je pro testování positivní definitnosti použitelný, větší roli hraje následující Choleského rozklad[1)].

Věta 11.7 (Choleského rozklad)**.** *Pro každou positivně definitní matici $A \in \mathbb{R}^{n\times n}$ existuje jediná dolní trojúhelníková matice $L \in \mathbb{R}^{n\times n}$ s kladnou diagonálou tak, že $A = LL^T$.*

Důkaz. Matematickou indukcí podle n. Pro $n = 1$ máme $A = (a_{11})$ a $L = (\sqrt{a_{11}})$.

Indukční krok $n \leftarrow n-1$. Mějme $A = \left(\begin{smallmatrix} \alpha & a^T \\ a & \tilde{A} \end{smallmatrix}\right)$. Podle Věty 11.6 je $\alpha > 0$ a $\tilde{A} - \frac{1}{\alpha}aa^T$ je positivně definitní. Tedy dle indukčního předpokladu existuje dolní trojúhelníková matice $\tilde{L} \in \mathbb{R}^{(n-1)\times(n-1)}$ s kladnou diagonálou tak, že $\tilde{A} - \frac{1}{\alpha}aa^T = \tilde{L}\tilde{L}^T$. Potom $L = \left(\begin{smallmatrix} \sqrt{\alpha} & o^T \\ \frac{1}{\sqrt{\alpha}}a & \tilde{L} \end{smallmatrix}\right)$, neboť

$$LL^T = \begin{pmatrix} \sqrt{\alpha} & o^T \\ \frac{1}{\sqrt{\alpha}}a & \tilde{L} \end{pmatrix} \begin{pmatrix} \sqrt{\alpha} & \frac{1}{\sqrt{\alpha}}a^T \\ o & \tilde{L} \end{pmatrix} = \begin{pmatrix} \alpha & a^T \\ a & \frac{1}{\alpha}aa^T + \tilde{L}\tilde{L}^T \end{pmatrix} = A.$$

[1)] André-Louis Cholesky, francouzský důstojník ukrajinského původu, metodu z r. 1910 vyvinul pro účely triangularizace a vytvoření přesnějších map (v podstatě pro řešení soustavy normálních rovnic v metodě nejmenších čtverců), ale publikována byla až po jeho smrti roku 1924.

Pro důkaz jednoznačnosti mějme jiný rozklad $A = L'L'^T$, kde $L' = \begin{pmatrix} \beta & o^T \\ b & \tilde{L}' \end{pmatrix}$. Pak

$$\begin{pmatrix} \alpha & a^T \\ a & \tilde{A} \end{pmatrix} = A = L'L'^T = \begin{pmatrix} \beta^2 & \beta b^T \\ \beta b & bb^T + \tilde{L}'\tilde{L}'^T \end{pmatrix}.$$

Porovnáním matic dostaneme: $\beta = \sqrt{\alpha}$, $b = \frac{1}{\alpha}a$ a $\tilde{A} = bb^T + \tilde{L}'\tilde{L}'^T$, neboli $\tilde{L}'\tilde{L}'^T = \tilde{A} - \frac{1}{\alpha}aa^T$. Jenže podle indukčního předpokladu je $\tilde{A} - \frac{1}{\alpha}aa^T = \tilde{L}\tilde{L}^T$ jednoznačné, tedy $\tilde{L}' = \tilde{L}$, a tudíž i $L' = L$. □

Choleského rozklad existuje i pro positivně semidefinitní matice, ale není už jednoznačný.

Věta byla spíše existenčního charakteru, nicméně sestrojit Choleského rozklad je vcelku jednoduché. Základní idea je postupně porovnávat shora prvky v prvním sloupci matice $A = LL^T$, pak ve druhém atd. Výsledný postup je popsán dole. Pokud A je positivně definitní, algoritmus najde rozklad, a pokud A není, tak to algoritmus ohlásí.

Algoritmus 11.8 (Choleského rozklad)**.** Buď $A \in \mathbb{R}^{n\times n}$ symetrická.

1: $L \coloneqq 0_n$,
2: **for** $k \coloneqq 1$ **to** n **do**
3: **if** $a_{kk} - \sum_{j=1}^{k-1} l_{kj}^2 \leq 0$ **then return** „A není positivně definitní“,
4: $l_{kk} \coloneqq \sqrt{a_{kk} - \sum_{j=1}^{k-1} l_{kj}^2}$,
5: **for** $i \coloneqq k+1$ **to** n **do**
6: $l_{ik} \coloneqq \frac{1}{l_{kk}} \left(a_{ik} - \sum_{j=1}^{k-1} l_{ij}l_{kj} \right)$,
7: **end for**
8: **end for**
9: **return** $A = LL^T$.

Příklad 11.9. Choleského rozklad matice A:

$$\begin{array}{c|c} & L^T \\ \hline L & A \end{array} \quad \equiv \quad \begin{array}{ccc|ccc} & & & 2 & -1 & 2 \\ & & & 0 & 3 & 1 \\ & & & 0 & 0 & 1 \\ \hline 2 & 0 & 0 & 4 & -2 & 4 \\ -1 & 3 & 0 & -2 & 10 & 1 \\ 2 & 1 & 1 & 4 & 1 & 6 \end{array}$$

□

Příklad 11.10. Použití Choleského rozkladu pro řešení soustavy $Ax = b$ s positivně definitní maticí A. Pokud máme rozklad $A = LL^T$, pak soustava má tvar $L(L^T x) = b$. Nejprve vyřešíme soustavu $Ly = b$, potom $L^T x = y$ a její řešení je to hledané. Postup:

1. Najdi Choleského rozklad $A = LL^T$,
2. Najdi řešení y^* soustavy $Ly = b$ pomocí dopředné substituce,
3. Najdi řešení x^* soustavy $L^T x = y^*$ pomocí zpětné substituce.

Tento postup je řádově o 50% rychlejší než řešení Gaussovou eliminací. □

Rekurentní vzoreček má ještě další důsledky:

Věta 11.11 (Gaussova eliminace a positivní definitnost)**.** *Symetrická matice $A \in \mathbb{R}^{n\times n}$ je positivně definitní právě tehdy když ji Gaussova eliminace převede do odstupňovaného tvaru s kladnou diagonálou za použití pouze elementární úpravy přičtení násobku řádku k jinému, který je pod ním.*

Důkaz. Mějme $A = \begin{pmatrix} \alpha & a^T \\ a & \tilde{A} \end{pmatrix}$ positivně definitní. První krok Gaussovy eliminace převede matici na tvar $\begin{pmatrix} \alpha & a^T \\ o & \tilde{A} - \frac{1}{\alpha} a a^T \end{pmatrix}$. Podle Věty 11.6 je $\alpha > 0$ a $\tilde{A} - \frac{1}{\alpha} a a^T$ je zase positivně definitní, takže můžeme pokračovat induktivně dál. □

Věta 11.12 (Sylvestrovo[2] kriterium positivní definitnosti)**.** *Symetrická matice $A \in \mathbb{R}^{n \times n}$ je positivně definitní právě tehdy když determinanty všech hlavních vedoucích matic $A_1, \ldots, A_n$ jsou kladné, přičemž A_i je levá horní podmatice A velikosti i (tj. vznikne z A odstraněním posledních $n - i$ řádků a sloupců).*

Důkaz. Implikace „⇒“. Buď $A \in \mathbb{R}^{n \times n}$ positivně definitní. Pak pro každé $i = 1, \ldots, n$ je A_i positivně definitní, neboť pokud $x^T A_i X \leq 0$, tak $(x^T\, o^T) A \begin{pmatrix} x \\ o \end{pmatrix} = x^T A_i X \leq 0$. Tedy A_i má kladná vlastní čísla a její determinant je také kladný (je roven součinu vlastních čísel).

Implikace „⇐“. Během Gaussovy eliminace matice A jsou všechny pivoty kladné, neboť pokud je i-tý pivot první nekladný, pak $\det(A_i) \leq 0$. Podle Věty 11.11 je tedy A positivně definitní. □

Analogie Sylvestrovy podmínky pro positivně semidefinitností matice je následující, uvádíme ji bez důkazu.

Věta 11.13 (Sylvestrovo kriterium positivní semidefinitnosti)**.** *Symetrická m $A \in \mathbb{R}^{n \times n}$ je positivně semidefinitní právě tehdy když determinanty všech hlavních matic jsou nezáporné, přičemž hlavní matice je matice, která vznikne z A odstraněním několika řádků a sloupců s týmiž indexy.*

Zatímco Sylvestrovo kriterium positivní definitnosti vyžaduje počítání n determinantů, pro positivní semidefinitnost počet vzroste na $2^n - 1$, a proto není moc použitelnou metodou. Lepší způsob si ukážeme později v Sekci 12.2 (Důsledek 12.9).

Přestože jsme si uvedli několik metod na testování positivní definitnosti, některé jsou si dost podobné. Důkaz Věty 11.11 ukazuje, že rekurentní vzoreček a Gaussova eliminace v podstatě fungují stejně. A pokud počítáme determinanty Gaussovou eliminací, tak i Sylvestrovo pravidlo je varianta prvních dvou. Naproti tomu, Choleského rozklad je z principu odlišná metoda.

11.2 Aplikace

Věta 11.14 (Skalární součin a positivní definitnost)**.** *Operace $\langle x, y \rangle$ je skalárním součinem v $\mathbb{R}^n$ právě tehdy když má tvar $\langle x, y \rangle = x^T A y$ pro nějakou positivně definitní matici $A \in \mathbb{R}^{n \times n}$.*

Důkaz. Implikace „⇒“. Definujme matici $A \in \mathbb{R}^{n \times n}$ předpisem $a_{ij} = \langle e_i, e_j \rangle$, je zjevně symetrická. Pak

$$\langle x, y \rangle = \Big\langle \sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} y_j e_j \Big\rangle = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_j a_{ij} = x^T A y.$$

Matice A je positivně definitní, neboť $\langle x, x \rangle = x^T A x \geq 0$ a nulové jen pro $x = o$.

Implikace „⇐“. Nechť A je positivně definitní. Pak $\langle x, y \rangle = x^T A y$ tvoří skalární součin: $\langle x, x \rangle = x^T A x \geq 0$ a nulové jen pro $x = o$, je lineární v první složce a je symetrický neboť

$$\langle x, y \rangle = x^T A y = (x^T A y)^T = y^T A^T x = y^T A x = \langle y, x \rangle.$$ □

Víme, že skalární součin indukuje normu (Definice 8.4). Norma indukovaná výše zmíněným skalárním součinem je $\|x\| = \sqrt{x^T A x}$.

Pro $A = I_n$ dostáváme standardní skalární součin v $\mathbb{R}^n$ a eukleidovskou normu.

Další aplikací je odmocnina z matice. Pro positivně semidefinitní matice můžeme zavést $\sqrt{A}$.

Věta 11.15 (Odmocnina z matice)**.** *Pro každou positivně semidefinitní matici $A \in \mathbb{R}^{n \times n}$ existuje positivně semidefinitní matice $B \in \mathbb{R}^{n \times n}$ tak, že $B^2 = A$.*

Důkaz. Nechť A má spektrální rozklad $A = Q \Lambda Q^T$, kde $\Lambda = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, $\lambda_1, \ldots, \lambda_n \geq 0$. Definujme $\Lambda' = \operatorname{diag}(\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_n})$ a $B = Q \Lambda' Q^T$. Pak $B^2 = Q \Lambda' Q^T Q \Lambda' Q^T = Q \Lambda'^2 Q^T = Q \Lambda Q^T = A$. □

[2] James Joseph Sylvester, anglický matematik, spoluzakladatel teorie matic. Kriterium je z r. 1852.

Poznámka 11.16. Positivní (semi-)definitnost je důležitá i v optimalizaci při určování minima funkce. Matice, která zde vystupuje, je tzv. hessián, matice druhých parciálních derivací. Za předpokladu, že jsme v bodě x^* s nulovým gradientem, pak positivní definitnost dává postačující podmínku pro to aby x^* bylo lokální minimum, a naopak positivní semidefinitnost dává nutnou podmínku.

Hessián se podobně používá i při určování konvexity funkce. Positivní definitnost na nějaké otevřené konvexní množině implikuje konvexitu funkce f. Více např. viz [Rohn, 1997].

Výskyt positivně (semi-)definitních matic je ještě širší. Například ve statistice se setkáváme s tzv. kovarianční a korelační maticí. Obě dávají jistou informaci o závislosti mezi n náhodnými veličinami a, ne náhodou, jsou vždy positivně semidefinitní.

Kapitola 12

Kvadratické formy

12.1 Bilineární a kvadratické formy

Definice 12.1 (Bilineární a kvadratické forma)**.** Buď V vektorový prostor nad $\mathbb{T}$. *Bilineární forma* je zobrazení $b : V^2 \mapsto \mathbb{T}$, které je lineární v první i druhé složce, tj.

$$b(\alpha u + \beta v, w) = \alpha b(u, w) + \beta b(v, w), \quad \forall \alpha, \beta \in \mathbb{T},\ \forall u, v, w \in V,$$
$$b(w, \alpha u + \beta v) = \alpha b(w, u) + \beta b(w, v), \quad \forall \alpha, \beta \in \mathbb{T},\ \forall u, v, w \in V.$$

Zobrazení $f : V \mapsto \mathbb{T}$ je *kvadratická forma* pokud se dá vyjádřit $f(u) = b(u, u)$ pro nějakou bilineární formu b.

Příklad 12.2.

- Každý reálný skalární součin je bilineární formou.
- Buď $V = \mathbb{R}^2$, $b(x, y) = x_1y_1 + 2x_1y_2 + 4x_2y_1 + 10x_2y_2$ je příkladem bilineární formy a $f(x) = b(x, x) = x_1^2 + 6x_1x_2 + 10x_2^2$ odpovídající kvadratické formy.
- $b(o, v) = b(v, o) = 0$, $f(o) = 0$. □

V analogii s teorií lineárních zobrazení, i bilineární formy jsou jednoznačně určeny obrazy bází a dají se vyjádřit maticově.

Věta 12.3 (Maticové vyjádření forem)**.** *Buď $B : w_1, \ldots, w_n$ báze V, buď b bilineární a f odpovídající kvadratická forma. Definujme matici $A \in \mathbb{T}^{n\times n}$ předpisem $a_{ij} = b(w_i, w_j)$. Pak pro každé $u, v \in V$ platí*

$$b(u, v) = [u]_B^T A [v]_B, \quad f(u) = [u]_B^T A [u]_B.$$

Důkaz. Označme $x \coloneqq [u]_B$, $y \coloneqq [v]_B$. Pak

$$b(u, v) = b\Big(\sum_{i=1}^n x_i w_i, \sum_{j=1}^n y_j w_j\Big) = \sum_{i=1}^n \sum_{j=1}^n x_i y_j b(w_i, w_j) = \sum_{i=1}^n \sum_{j=1}^n x_i y_j a_{ij} = x^T A y.$$

Dále, $f(u) = b(u, u) = x^T A x$. □

Příklad 12.4. Uvažme kvadratickou formu

$$f(x) = x_1^2 + 6x_1x_2 + 10x_2^2 = x^T \begin{pmatrix} 1 & 3 \\ 3 & 10 \end{pmatrix} x = x^T \begin{pmatrix} 1 & 4 \\ 2 & 10 \end{pmatrix} x.$$

Maticové vyjádření tedy není jednoznačné. Nicméně, pro reálný vektorový prostor můžeme vždy předpokládat, že matice kvadratické formy je symetrická, neboť $x^T A x = x^T \frac{A + A^T}{2} x$. Tuto úvahu lze zobecnit i na prostory nad jinými tělesy, ale nesmí mít charakteristiku 2. Např.

$$f(x) = x_1^2 + x_1x_2 + x_2^2 = x^T \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} x$$

nelze nad $\mathbb{Z}_2$ representovat symetrickou maticí. □

Matice forem závisí na volbě báze. Jak se změní matice když přejdeme k jiné bázi?

Věta 12.5 (Matice kvadratické formy při změně báze)**.** *Buď $A \in \mathbb{T}^{n\times n}$ matice kvadratické formy vzhledem k bázi B prostoru V. Buď B' jiná báze a $S = {}_B[id]_{B'}$ matice přechodu od B' k B. Pak matice f vzhledem k B' je S^TAS.*

Důkaz. Buď $u, v \in V$ a b bilineární forma indukující f. Pak

$$b(u,v) = [u]_B^T A[v]_B = ({}_B[id]_{B'}\,[u]_{B'})^T A({}_B[id]_{B'}\,[v]_{B'})$$

Speciálně pro $u = w_i$, $v = w_j$, kde $w_1, \ldots, w_n$ je báze B', tak dostáváme $b(w_i, w_j) = (S^TAS)_{ij}$. Tedy S^TAS je matice forem b, f. □

Různou volbou báze V dosahujeme různé maticové representace. Naším cílem bude najít takovou bázi, vůči níž je matice co nejjednodušší, tedy diagonální. Nadále budeme uvažovat pouze reálné vektorové prostory.

Zde je jistá paralela z diagonalizací pro vlastní čísla, kde jsme transformovali matici pomocí podobnosti. Nyní transformujeme matici úpravou S^TAS, kde S je regulární. Místo podobnosti nyní máme tzv. *kongruenci*. Jak uvidíme, u kvadratických forem je situace jednodušší – každá matice lze diagonalizovat.

12.2 Sylvestrův zákon setrvačnosti

Věta 12.6 (Sylvestrův zákon setrvačnosti[1])**.** *Pro každou kvadratickou formu f existuje báze, vůči níž má f diagonální matici s prvky $1, -1, 0$. Navíc, tato matice je až na pořadí prvků jednoznačná.*

Důkaz. „Existence“. Nechť A je matice formy f. Protože A je symetrická, tak má spektrální rozklad $A = Q\Lambda Q^T$, kde $\Lambda = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$. Tedy $\Lambda = Q^TAQ$ je diagonalizace formy. Abychom docílili na diagonále ± 1, tak provedeme ještě úpravu $\Lambda' Q^TAQ\Lambda'$, kde Λ' je diagonální matice s prvky $\Lambda'_{ii} = |\lambda_i|^{-\frac{1}{2}}$ pokud $\lambda_i \neq 0$ a $\Lambda'_{ii} = 0$ jinak.

„Jednoznačnost“. Sporem předpokládejme, že máme dvě různé diagonalizace D, D' pro bázi B : $w_1, \ldots, w_n$ a $B' : w'_1, \ldots, w'_n$. Buď $u \in V$ libovolné a nechť má souřadnice $x = [u]_B$, $y = [u]_{B'}$. Pak

$$f(u) = x^TDx = x_1^2 + \ldots + x_p^2 - x_{p+1}^2 - \ldots - x_q^2 + 0x_{q+1}^2 + \ldots + 0x_n^2,$$
$$f(u) = y^TD'y = y_1^2 + \ldots + y_s^2 - y_{s+1}^2 - \ldots - y_t^2 + 0y_{t+1}^2 + \ldots + 0y_n^2.$$

Platí $q = t$, neboť $D = S^TD'S$ pro nějakou regulární S, a proto D, D' mají stejnou hodnost. Chceme ukázat, že nutně $p = s$. Bez újmy na obecnosti předpokládejme $p > s$. Definujme prostory $P = \operatorname{span}(w_1, \ldots, w_p)$ a $R = \operatorname{span}(w'_{s+1}, \ldots, w'_n)$. Pak

$$\dim P \cap R = \dim P + \dim R - \dim(P+R) \geq p + (n-s) - n = p - s \geq 1.$$

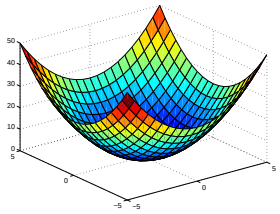
Tedy existuje nenulový $u \in P \cap R$ a pro něj máme $u = \sum_{i=1}^{p} x_i w_i = \sum_{j=s+1}^{n} y_j w'_j$, z čehož dostáváme

$$\begin{aligned} f(u) &= x_1^2 + \ldots + x_p^2 > 0, \\ &= -y_{s+1}^2 - \ldots - y_t^2 \leq 0. \end{aligned}$$

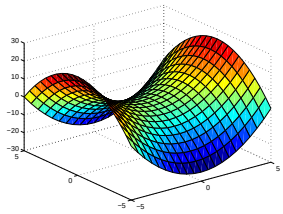
To je spor. □

Příklad 12.7 (Kvadratické formy v $\mathbb{R}^2$)**.** Podle Sylvestrova zákona, kvadratické formy v $\mathbb{R}^2$ mají v podstatě jeden z následujících tvarů v souřadném systému vhodné báze.

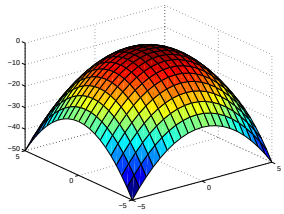
[1] Anglicky *Sylvester's law of inertia*, z r. 1852.



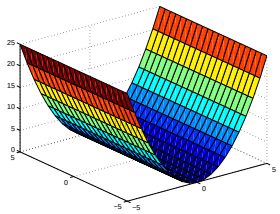
$x_1^2 + x_2^2$



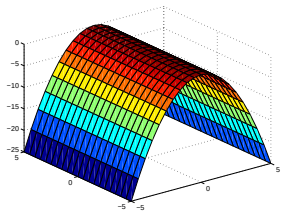
$x_1^2 - x_2^2$



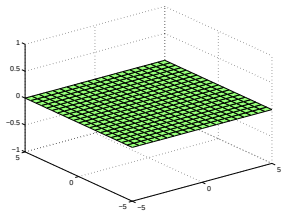
$-x_1^2 - x_2^2$



x_1^2



$-x_1^2$



0 □

Sylvestrův zákon opravňuje k zavedení pojmu *signatura* jako počet $1, -1, 0$ ve výsledné diagonální matici. Navíc má řadu důsledků týkající se mj. positivní (semi-)definitnosti a vlastních čísel.

Důsledek 12.8. *Buď $A \in \mathbb{R}^{n\times n}$ symetrická a S^TAS převedení na diagonální tvar. Pak počet jedniček resp. minus jedniček resp. nul na diagonále odpovídá počtu kladných resp. záporných resp nulových vlastních čísel.*

Důkaz. Stačí uvažovat kvadratickou formu $f(x) = x^TAx$, která má matici A. Z důkazu věty je patrné, že jednu diagonalizaci získáme ze spektrálního rozkladu. Ze setrvačnosti pak musí počty vždy souhlasit. □

Pokud důsledek aplikujeme na matici $A - \alpha I_n$ tak zjistíme, kolik vlastních čísel matice A je větších / menších / rovno číslu α. Takto lze postupným půlením intervalu omezovat potenciální rozsah vlastních čísel a limitně konvergovat k jejich hodnotám. Tento postup se kdysi používal pro výpočet vlastních čísel, ale nyní je již překonaný (mj. to není moc stabilní metoda).

Důsledek 12.9. *Buď $A \in \mathbb{R}^{n\times n}$ symetrická a S^TAS převedení na diagonální tvar. Pak*

(1) A je positivně definitní právě tehdy když S^TAS má kladnou diagonálu,

(2) A je positivně semidefinitní právě tehdy když S^TAS má nezápornou diagonálu.

Důkaz. Z Důsledku 12.8 a vztahu mezi positivní (semi-)definitností a vlastními čísly (Věta 11.4). □

Sylvestrův zákon tedy dává návod jak jednou metodou rozhodnout o positivní definitnosti resp. positivní semidefinitnosti v jednom.

Zbývá otázka jak matice kvadratických forem převést na diagonální tvar. Důkaz věty o Sylvestrově zákonu sice dává návod (přes spektrální rozklad), ale můžeme jednoduše adaptovat elementární maticové úpravy. Co se stane, když symetrickou matici A převedeme na E^TAE, kde E^T je matice elementární řádkové úpravy? Provede se řádkový úprava a na sloupce i analogická sloupcová úprava. Budeme na matici tedy aplikovat řádkové úpravy a odpovídající sloupcové úpravy. Tím budeme nulovat prvky pod i nad diagonálou, až matici převedeme na diagonální tvar.

Příklad 12.10. Diagonalizujme matici

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 5 & -3 \\ -1 & -3 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & -1 \\ 0 & 1 & -1 \\ -1 & -3 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ -1 & -1 & 2 \end{pmatrix} \sim$$
$$\sim \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Matice A má dvě kladná vlastní čísla a jedno nulové, je tedy positivně semidefinitní. □

Kuželosečky a kvadriky

Pomocí kvadratických forem lze popisovat geometrické útvary zvané *kvadriky*. To jsou (stručně řečeno, podrobněji viz např. [Bican, 2009]) množiny popsané rovnicí $x^T Ax + b^T x + c = 0$. Speciálním případem jsou *kuželosečky*, což jsou kvadriky v $\mathbb{R}^2$. Pomocí různých charakteristik, jako jsou vlastní čísla apod., můžeme pak snadno kvadriky klasifikovat.

Příklad 12.11 (Elipsoidy)**.** Rovnice $\frac{1}{a^2}x_1^2 + \frac{1}{b^2}x_2^2 = 1$ popisuje elipsu se středem v počátku, poloosy jsou ve směru souřadných os a mají délky a resp. b. Podobně pro vyšší dimenze.

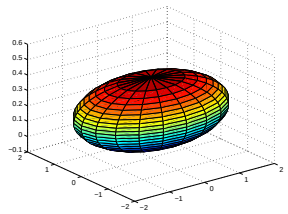
Nyní uvažme rovnici $x^T Ax = 1$, kde $A \in \mathbb{R}^{n\times n}$ je positivně definitní. Buď $A = Q\Lambda Q^T$ spektrální rozklad. Při substituci $y \coloneqq Q^T x$ dostaneme

$$1 = x^T Ax = x^T Q\Lambda Q^T x = y^T \Lambda y = \sum_{i=1}^{n} \lambda_i y_i^2 = \sum_{i=1}^{n} \frac{1}{\left(\lambda_i^{-1/2}\right)^2} y_i^2.$$

Dostáváme tedy popis elipsoidu se středem v počátky, poloosy jsou ve směru souřadnic a mají délky $\frac{1}{\sqrt{\lambda_1}}, \ldots, \frac{1}{\sqrt{\lambda_n}}$. Nicméně, tento popis je v prostoru po transformaci $y = Q^T x$. Vrátíme zpět transformací $x = Qy$. Protože Q je ortogonální matice, dostaneme stejný elipsoid se středem v počátku, jen nějak pootočený. Protože kanonická báze $e_1, \ldots, e_n$ se zobrazí na sloupce matice Q (což jsou vlastní vektory matice A), tak poloosy původního elipsoidu budou ve směrech vlastních vektorů A.

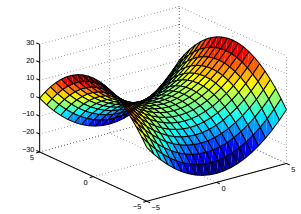
Pokud A je symetrická, ale ne positivně definitní, analýza bude stejná. Jenom nedostaneme elipsoid, ale jiný geometrický útvar (hyperboloid aj.)

Příklad 12.12 (Některé kvadriky v $\mathbb{R}^3$)**.**



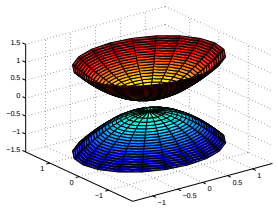
$\frac{x_1^2}{a^2} + \frac{x_2^2}{b^2} + \frac{x_3^2}{c^2} = 1$

elipsoid



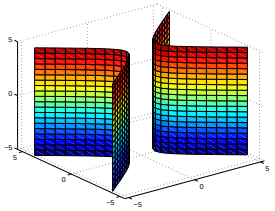
$\frac{x_1^2}{a^2} - \frac{x_2^2}{b^2} - x_3 = 0$

hyperbolický paraboloid



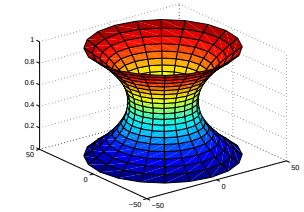
$-\frac{x_1^2}{a^2} - \frac{x_2^2}{b^2} + \frac{x_3^2}{c^2} = 1$

dvojdílný hyperboloid



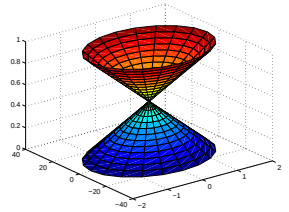
$\frac{x_1^2}{a^2} - \frac{x_2^2}{b^2} = 1$

hyperbolická válcová plocha



$\frac{x_1^2}{a^2} + \frac{x_2^2}{b^2} - \frac{x_3^2}{c^2} = 1$

jednodílný hyperboloid



$\frac{x_1^2}{a^2} + \frac{x_2^2}{b^2} - \frac{x_3^2}{c^2} = 0$

kuželová plocha □

Kapitola 13

Maticové rozklady

Maticové rozklady byly zařazeny do *Top 10* algoritmů 20. století. S několika rozklady jsme se už potkali (Choleského rozklad, spektrální rozklad, ...), ale QR rozklad (bude o něm řeč později) se v seznamu objevuje skrytě ještě jednou, protože je základem QR algoritmu. Jeho důležitost je tedy patrná.

Top 10 algoritmy 20. století podle [Dongarra and Sullivan, 2000; Cipra, 2000] jsou:

1. Metoda Monte Carlo (1946, J. von Neumann, S. Ulam, and N. Metropolis)
2. Simplexová metoda pro lineární programování (1946, G. Dantzig)
3. Iterační metody Krylovových podprostorů (1950, M. Hestenes, E. Stiefel, C. Lanczos)
4. Dekompozice matic (1951, A. Householder)
5. Překladač Fortranu (1957, J. Backus)
6. QR algoritmus pro výpočet vlastních čísel, (1961, J. Francis)
7. Quicksort (1962, A. Hoare)
8. Rychlá Fourierova transformace (1965, J. Cooley, J. Tukey)
9. Integer relation detection algorithm (1977, H. Ferguson, R. Forcade)
10. Fast multipole algorithm (1987, L. Greengard, V. Rokhlin)

13.1 Householderova transformace

Připomeňme (Příklad 8.32), že Householderova matice je definována jako $H(x) \coloneqq I_n - \frac{2}{x^T x} x x^T$, kde $o \neq x \in \mathbb{R}^n$. Tato matice je ortogonální a symetrická. A jak si ukážeme, může nahradit elementární matice při výpočtu odstupňovaného tvaru matice. Tento postup se nazývá Householderova transformace.[1)]

Věta 13.1 (Householderova transformace)**.** *Pro každé $x, y \in \mathbb{R}^n$, $x \neq y$, $\|x\|_2 = \|y\|_2$ platí $y = H(x-y)x$.*

Důkaz. Počítejme

$$\begin{aligned} H(x-y)x &= \left(I_n - \frac{2}{(x-y)^T(x-y)}(x-y)(x-y)^T\right)x = x - \frac{2(x-y)^T x}{(x-y)^T(x-y)}(x-y) \\ &= x - \frac{2\|x\|_2^2 - 2y^T x}{(x-y)^T(x-y)}(x-y) = x - \frac{\|x\|_2^2 + \|y\|_2^2 - 2y^T x}{\|x-y\|_2^2}(x-y) = x - (x-y) = y. \end{aligned}$$ □

Householderova matice tedy převádí jeden vybraný vektor na jiný se stejnou normou. Speciálně lze převést na vhodný násobek jednotkového vektoru:

Důsledek 13.2. *Buď $x \in \mathbb{R}^n$ a definujme*

$$H \coloneqq \begin{cases} H(x - \|x\|_2 e_1) & \text{pokud } x \neq \|x\|_2 e_1, \\ I_n & \text{jinak.} \end{cases}$$

Potom $Hx = \|x\|_2 e_1$.

[1)] Alston Scott Householder, americký numerický matematik, transformace je z r. 1958.

Důkaz. Případ $x = \|x\|_2 e_1$ je jasný. Jinak použijeme větu, vektory $x, \|x\|_2 e_1$ mají stejnou normu. □

Mějme matici $A \in \mathbb{R}^{m\times n}$ a H sestrojíme podle prvního sloupce A. Vynásobením HA tak vynulujeme prvky v prvním sloupci A až na první z nich. Rekurzivním voláním transformace pak převedeme matici do odstupňovaného tvaru. Tento postup je tedy alternativou k elementárním řádkovým úpravám. Máme tu však ještě něco navíc, a to tzv. QR rozklad.

Podobně lze použít i Givensova matice, ale ta nuluje pouze jeden prvek (stejně jako elementární matice), takže ji musíme použít vícekrát.

13.2 QR rozklad

Věta 13.3 (QR rozklad)**.** *Pro každou matici $A \in \mathbb{R}^{m\times n}$ existuje ortogonální $Q \in \mathbb{R}^{m\times m}$ a horní trojúhelníková matice $R \in \mathbb{R}^{m\times n}$ s nezápornou diagonálou tak, že $A = QR$.*

Důkaz. Matematickou indukcí podle n, tj. počtu sloupců. Je-li $n = 1$, pak $A = a \in \mathbb{R}^m$ a pro matici H sestrojenou podle Důsledku 13.2 platí $Ha = \|a\|_2 e_1$. Stačí položit $Q \coloneqq H^T$ a $R \coloneqq \|a\|_2 e_1$.

Indukční krok $n \leftarrow n-1$. Aplikací Důsledku 13.2 na první sloupec matice A dostaneme $HA_{*1} = \|A_{*1}\|_2 e_1$. Tedy HA je tvaru

$$HA = \begin{pmatrix} \alpha & b^T \\ o & B \end{pmatrix},$$

kde $B \in \mathbb{R}^{(m-1)\times(n-1)}$ a $\alpha = \|A_{*1}\|_2 \geq 0$. Podle indukčního předpokladu existuje rozklad $B = Q'R'$, kde $Q' \in \mathbb{R}^{(m-1)\times(m-1)}$ je ortogonální a $R' \in \mathbb{R}^{(m-1)\times(n-1)}$ horní trojúhelníková s nezápornou diagonálou. Upravme

$$\begin{pmatrix} 1 & o^T \\ o & Q'^T \end{pmatrix} HA = \begin{pmatrix} 1 & o^T \\ o & Q'^T \end{pmatrix} \begin{pmatrix} \alpha & b^T \\ o & B \end{pmatrix} = \begin{pmatrix} \alpha & b^T \\ o & R' \end{pmatrix}.$$

Označme

$$Q \coloneqq H^T \begin{pmatrix} 1 & o^T \\ o & Q' \end{pmatrix}, \quad R \coloneqq \begin{pmatrix} \alpha & b^T \\ o & R' \end{pmatrix}.$$

Matice Q je ortogonální a R horní trojúhelníková s nezápornou diagonálou. Nyní rovnice má tvar $Q^T A = R$, neboli $A = QR$ je hledaný rozklad. □

Věta dává i návod na konstrukci QR rozkladu. Poznamenejme, že v průběhu algoritmu platí invariant: $A = QR$ a Q je ortogonální. Podstata tedy spočívá v tom, že postupně R přeměníme na horní trojúhelníkovou matici. Symbol $R(j : m, j)$ značí vektor $(r_{jj}, \ldots, r_{mj})^T$.

Algoritmus 13.4 (QR rozklad)**.** Buď $A \in \mathbb{R}^{m\times n}$.

1: $Q \coloneqq I_m$, $R \coloneqq A$,
2: **for** $j \coloneqq 1$ **to** $\min(m, n)$ **do**
3: $\quad x \coloneqq R(j : m, j)$,
4: $\quad$ **if** $x \neq \|x\|_2 e_1$ **then**
5: $\quad\quad x \coloneqq x - \|x\|_2 e_1$,
6: $\quad\quad H(x) \coloneqq I_{m-j+1} - \frac{2}{x^T x} x x^T$,
7: $\quad\quad H \coloneqq \begin{pmatrix} I_{j-1} & 0 \\ 0 & H(x) \end{pmatrix}$,
8: $\quad\quad R \coloneqq HR$, $Q \coloneqq QH$,
9: $\quad$ **end if**
10: **end for**

Výstup: $A = QR$.

Příklad 13.5 (QR rozklad)**.** Buď

$$A = \begin{pmatrix} 0 & -20 & -14 \\ 3 & 27 & -4 \\ 4 & 11 & -2 \end{pmatrix}.$$

První iterace:

$$x = A_{*1} - \|A_{*1}\|e_1 = (-5, 3, 4)^T,$$
$$Q_1 = I_3 - 2\frac{xx^T}{x^Tx} = \frac{1}{25}\begin{pmatrix} 0 & 15 & 20 \\ 15 & 16 & -12 \\ 20 & -12 & 9 \end{pmatrix}, \quad Q_1A = \begin{pmatrix} 5 & 25 & -4 \\ 0 & 0 & -10 \\ 0 & -25 & -10 \end{pmatrix}.$$

Druhá iterace:

$$x = (0, -25)^T - 25e_1 = (-25, -25)^T,$$
$$Q_2 = I_2 - 2\frac{xx^T}{x^Tx} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \quad Q_1\begin{pmatrix} 0 & -10 \\ -25 & -10 \end{pmatrix} = \begin{pmatrix} 25 & 10 \\ 0 & 10 \end{pmatrix}.$$

Výsledek:

$$Q = Q_1\begin{pmatrix} 1 & 0 \\ 0 & Q_2 \end{pmatrix} = \frac{1}{25}\begin{pmatrix} 0 & -20 & -15 \\ 15 & 12 & -16 \\ 20 & -9 & 12 \end{pmatrix}, \quad R = \begin{pmatrix} 5 & 25 & -4 \\ 0 & 25 & 10 \\ 0 & 0 & 10 \end{pmatrix}.$$

□

QR rozklad je jednoznačný jen za určitých předpokladů. Např. pro nulovou matici $A = 0$ je $R = 0$ a Q libovolná ortogonální matice, tedy jednoznačnost tu není.

Věta 13.6 (Jednoznačnost QR rozkladu)**.** *Pro regulární matici $A \in \mathbb{R}^{n\times n}$ je QR rozklad jednoznačný a R má na diagonále kladné hodnoty.*

Důkaz. Ze vztahu $A = QR$ plyne, že R je regulární, a tudíž musí mít nenulovou, a proto kladnou, diagonálu.

Jednoznačnost ukážeme sporem. Nechť A má dva různé rozklady $A = Q_1R_1 = Q_2R_2$. Pak $Q_2^TQ_1 = R_2R_1^{-1}$, a tuto matici označíme jako U. Zřejmě U je ortogonální (je to součin ortogonálních matic Q_2^T a Q_1) a horní trojúhelníková (je to součin horních trojúhelníkových matic R_2 a R_1^{-1}). Speciálně, první sloupec U má tvar $U_{*1} = (u_{11}, 0, \ldots, 0)^T$, kde $u_{11} > 0$. Aby měl jednotkovou velikost, musí $u_{11} = 1$ a proto $U_{*1} = e_1$. Druhý sloupec je kolmý na první, proto $u_{21} = 0$, a aby měl jednotkovou velikost, musí $u_{22} = 1$. Tedy $U_{*2} = e_2$. Atd. pokračujeme dále až dostaneme $U = I_n$, z čehož $Q_1 = Q_2$ a $R_1 = R_2$. To je spor. □

Věta se dá zobecnit i na případ $A \in \mathbb{R}^{m\times n}$ s lineárně nezávislými sloupci. Pak matice R a prvních n sloupců Q je jednoznačně určeno, a diagonála R je kladná.

13.3 Aplikace QR rozkladu

QR rozklad se dá použít na řešení mnoha úloh, se kterými jsme se doposud setkali. Jeho hlavní výhodou je, že pracuje s ortogonální maticí Q. Protože ortogonální matice zachovávají normu (Věta 8.33(2)), tak se zaokrouhlovací chyby příliš nezvětšují. To je důvod, proč se ortogonální matice hojně využívají v numerických metodách.

QR rozklad a soustavy rovnic

Uvažujme soustavu lineárních rovnic $Ax = b$, kde $A \in \mathbb{R}^{n\times n}$ je regulární. Řešení vypočítáme následujícím způsobem: Vypočítej QR rozklad $A = QR$. Pak soustava má tvar $QRx = b$, neboli $Rx = Q^Tb$. Protože R je horní trojúhelníková matice, řešení dostaneme snadno zpětnou substitucí.

Oproti Gaussově eliminaci je tento způsob přibližně dvakrát pomalejší, na druhou stranu je numericky stabilnější a přesnější.

QR rozklad a ortogonalizace

Pro následující si nejprve zavedeme tzv. *redukovaný QR rozklad*. Nechť $A \in \mathbb{R}^{m\times n}$ má lineárně nezávislé sloupce. Pak QR rozklad rozepíšeme blokově

$$A = QR = \begin{pmatrix}\tilde{Q} & \tilde{Q}'\end{pmatrix}\begin{pmatrix}\tilde{R}\\ 0\end{pmatrix} = \tilde{Q}\tilde{R},$$

kde $\tilde{Q} \in \mathbb{R}^{m\times n}$ tvoří prvních n sloupců matice Q a $\tilde{R}$ prvních n řádků R. Matice $\tilde{R}$ je regulární.

Nyní se podívejme, jak QR rozklad aplikovat k nalezení ortonormální báze daného prostoru; je to tedy alternativa ke Gram–Schmidtově ortogonalizaci v $\mathbb{R}^m$. Nechť $A \in \mathbb{R}^{m\times n}$ má lineárně nezávislé sloupce a chceme sestrojit ortonormální bázi sloupcového prostoru $\mathcal{S}(A)$. Z rovnosti $A = \tilde{Q}\tilde{R}$ a regularity $\tilde{R}$ vyplývá (Věta 5.41), že $\mathcal{S}(A) = \mathcal{S}(\tilde{Q})$. Tedy ortonormální bázi $\mathcal{S}(A)$ tvoří sloupce $\tilde{Q}$.

QR rozklad a projekce do podprostoru

Nechť $A \in \mathbb{R}^{m\times n}$ má lineárně nezávislé sloupce. Víme (Věta 8.26), že projekce vektoru $x \in \mathbb{R}^m$ do sloupcového prostoru $\mathcal{S}(A)$ je $x' = A(A^TA)^{-1}A^Tx$. Výraz můžeme zjednodušit s použitím redukovaného QR rozkladu $A = \tilde{Q}\tilde{R}$:

$$A(A^TA)^{-1}A^T = \tilde{Q}\tilde{R}(\tilde{R}^T\tilde{Q}^T\tilde{Q}\tilde{R})^{-1}\tilde{R}^T\tilde{Q}^T = \tilde{Q}\tilde{R}(\tilde{R}^T\tilde{R})^{-1}\tilde{R}^T\tilde{Q}^T = \tilde{Q}\tilde{R}\tilde{R}^{-1}(\tilde{R}^T)^{-1}\tilde{R}^T\tilde{Q}^T = \tilde{Q}\tilde{Q}^T.$$

Matice projekce je tedy $\tilde{Q}\tilde{Q}^T$ a x se projektuje na $x' = \tilde{Q}\tilde{Q}^Tx$.

QR rozklad a metoda nejmenších čtverců

Metoda nejmenších čtverců (Sekce 8.4.1) spočívá v přibližném řešení přeurčené soustavy rovnic $Ax = b$, kde $A \in \mathbb{R}^{m\times n}$, $m > n$. Nechť A má hodnost n, pak přibližné řešení metodou nejmenších čtverců je

$$x = (A^TA)^{-1}A^Tb = (\tilde{R}^T\tilde{Q}^T\tilde{Q}\tilde{R})^{-1}\tilde{R}^T\tilde{Q}^Tb = \tilde{R}^{-1}(\tilde{R}^T)^{-1}\tilde{R}^T\tilde{Q}^Tb = \tilde{R}^{-1}\tilde{Q}^Tb.$$

Jinými slovy, x získáme jako řešení regulární soustavy $\tilde{R}x = \tilde{Q}^Tb$, a to zpětnou substitucí. Povšimněme si analogie s řešením regulární soustavy $Ax = b$, které vedlo na $Rx = Q^Tb$; nyní máme oříznutou soustavu $\tilde{R}x = \tilde{Q}^Tb$.

QR algoritmus

QR algoritmus[2)] je metoda na výpočet vlastních čísel matice $A \in \mathbb{R}^{n\times n}$, která se stala základem soudobých efektivních metod.

Algoritmus 13.7 (QR algoritmus)**.** Buď $A \in \mathbb{R}^{n\times n}$.

1: $A_0 := A$, $i := 0$,
2: **while not** konec **do**
3: sestroj QR rozklad matice A_i, tj. $A_i = QR$,
4: $A_{i+1} := RQ$,
5: $i := i + 1$,
6: **end while**

Výstup: A_i.

Tvrzení 13.8. *Matice $A_0, A_1, \ldots$ jsou si navzájem podobné.*

[2)] Autory jsou anglický informatik John G.F. Francis a ruská matematička Vera Nikolaevna Kublanovskaya, kteří jej vyvinuli nezávisle r. 1961.

Důkaz. $A_{i+1} = RQ = I_n RQ = Q^T QRQ = Q^T A_i Q$. □

Matice A_i na výstupu je podobná s A, a má tím pádem i stejná vlastní čísla. Jak je zjistíme? Algoritmus vesměs konverguje (případy kdy nekonverguje jsou řídké, skoro umělé; dlouho nebyl znám případ kdy by nekonvergoval) k blokově diagonální horní trojúhelníkové matici s bloky o velikosti 1 a 2. Bloky o velikosti 1 jsou vlastní čísla, a z bloků o velikosti 2 jednoduše dopočítáme dvojice komplexně sdružených vlastních čísel.

Příklad 13.9. Iterace QR algoritmu pro danou matici:

$$A = \begin{pmatrix} 2 & 4 & 2 \\ 4 & 2 & 2 \\ 2 & 2 & -1 \end{pmatrix} \to \begin{pmatrix} 6.1667 & -2.4623 & 0.8616 \\ -2.4623 & -1.2576 & -0.2598 \\ 0.8616 & -0.2598 & -1.9091 \end{pmatrix}$$
$$\to \begin{pmatrix} 6.9257 & 0.7725 & 0.2586 \\ 0.7725 & -1.9331 & 0.0224 \\ 0.2586 & 0.0224 & -1.9925 \end{pmatrix} \to \begin{pmatrix} 6.9939 & -0.2225 & 0.0742 \\ -0.2225 & -1.9945 & -0.0018 \\ 0.0742 & -0.0018 & -1.9994 \end{pmatrix}$$
$$\to \begin{pmatrix} 6.9995 & 0.0636 & 0.0212 \\ 0.0636 & -1.9996 & 0.0001 \\ 0.0212 & 0.0001 & -1.9999 \end{pmatrix} \to \begin{pmatrix} 7 & -0.0182 & 0.0061 \\ -0.0182 & -2 & -10^{-5} \\ 0.0061 & -10^{-5} & -2 \end{pmatrix}$$

```
A=[2 4 2;
   4 2 2;
   2 2 -1];
for i=1:5
  [Q,R]=qr(A);
  A=R*Q,
end
```

Symetrická matice konverguje k diagonální. Přesnost vypočítaných vlastních čísel určuje Věta 10.41 o Gerschgorinových discích. □

13.4 SVD rozklad

Stejně jako QR rozklad je SVD rozklad[3)] jednou ze základních technik v numerických výpočtech.

Věta 13.10 (SVD rozklad)**.** *Buď $A \in \mathbb{R}^{m\times n}$, $q \coloneqq \min\{m,n\}$. Pak existuje diagonální matice $\Sigma \in \mathbb{R}^{m\times n}$ s prvky $\sigma_{11} \geq \ldots \geq \sigma_{qq} \geq 0$ a ortogonální matice $U \in \mathbb{R}^{m\times m}$, $V \in \mathbb{R}^{n\times n}$ tak, že $A = U\Sigma V^T$.*

Důkaz uvádíme za Algoritmem 13.13, který konstruuje SVD rozklad. Kladným číslům na diagonále $\sigma_{11}, \ldots, \sigma_{rr}$ říkáme *singulární čísla* matice A a značíme je obvykle $\sigma_1, \ldots, \sigma_r$. Zjevně $r = \operatorname{rank}(A)$.

Věta 13.11 (Vztah singulárních a vlastních čísel)**.** *Buď $A \in \mathbb{R}^{m\times n}$, $r = \operatorname{rank}(A)$, a nechť A^TA má vlastní čísla $\lambda_1 \geq \ldots \geq \lambda_n$. Pak singulární čísla A jsou $\sigma_i = \sqrt{\lambda_i}$, $i = 1, \ldots, r$.*

Důkaz. Buď $A = U\Sigma V^T$ SVD rozklad A. Pak

$$A^TA = V\Sigma^T U^T U\Sigma V^T = V\Sigma^T\Sigma V^T = V \operatorname{diag}(\sigma_1^2, \ldots, \sigma_q^2, 0, \ldots, 0)V^T,$$

což je spektrální rozklad positivně definitní matice A^TA. Tudíž $\lambda_i = \sigma_i^2$. □

Příklad 13.12. Buď $Q \in \mathbb{R}^{n\times n}$ ortogonální. Pak $Q^TQ = I_n$ má vlastní čísla samé jedničky. Tedy ortogonální matice Q má singulární čísla také samé jedničky. □

Důkaz věty prozradil navíc, že matice V je ortogonální maticí ze spektrálního rozkladu A^TA. Podobně, matice U je ortogonální maticí ze spektrálního rozkladu AA^T:

$$AA^T = U\Sigma V^T V\Sigma^T U^T = U\Sigma\Sigma^T U^T = U \operatorname{diag}(\sigma_1^2, \ldots, \sigma_q^2, 0, \ldots, 0)U^T.$$

Bohužel, spektrální rozklady A^TA a AA^T nemůžeme použít ke konstrukci SVD rozkladu, protože nejsou jednoznačné. Použít můžeme jen jeden a druhý dopočítat trochu jinak.

Algoritmus 13.13 (SVD rozklad)**.** Buď $A \in \mathbb{R}^{m\times n}$.

[3)] Zkratka za *Singular value decomposition*, rozklad na singulární čísla. Byl objeven r. 1873 nezávisle řadou autorů jako byli např. Ital Eugenio Beltrami, francouz Marie E. Camille Jordan, Angličan James Sylvester, Němec Erhard Schmidt nebo Švýcar Hermann Weyl.

1: Sestroj $V\Lambda V^T$ spektrální rozklad A^TA;

2: $r \coloneqq \operatorname{rank}(A)$;

3: $\sigma_i \coloneqq \sqrt{\lambda_i}$, $i = 1, \dots, r$;

4: $S \coloneqq \operatorname{diag}(\sigma_1, \dots, \sigma_r)$;

5: V_1 je matice tvořená prvními r sloupci V;

6: $U_1 \coloneqq AV_1S^{-1}$;

7: doplň U_r na ortogonální matici $U = (U_1 \mid U_2)$;

Výstup: $A = U\Sigma V^T$ je SVD rozklad A.

Důkaz. Z věty 13.11 víme, že $\sigma_1, \dots, \sigma_r$ jsou hledaná singulární čísla a zjevně V je ortogonální. Musíme dokázat, že U_1 má ortonormální sloupce a $A = U\Sigma V^T$.

Z rovnosti $A^TA = V\Lambda V^T$ odvodíme $\Lambda = V^TA^TAV$ a oříznutím posledních $n - s$ řádků a sloupců $\operatorname{diag}(\lambda_1, \dots, \lambda_r) = V_1^TA^TAV_1$. Nyní je vidět, že U_1 má ortonormální sloupce, neboť

$$U_1^TU_1 = (S^{-1})^TV_1^TA^TAV_1S^{-1} = (S^{-1})^T \operatorname{diag}(\lambda_1, \dots, \lambda_r)S^{-1} = (S^{-1})^TS^2S^{-1} = I_r.$$

Zbývá ukázat, že $A = U\Sigma V^T$, neboli $\Sigma = U^TAV$. Rozložme $V = (V_1 \mid V_2)$. Oříznutím prvních r řádků a sloupců v $\Lambda = V^TA^TAV$ dostaneme $0 = V_2^TA^TAV_2$, z čehož $AV_2 = 0$ (Důsledek 8.25). Nyní

$$U^TAV = U^TA(V_1 \mid V_2) = (U^TU_1S \mid U^TAV_2) = \begin{pmatrix} S & 0 \\ 0 & 0 \end{pmatrix}. \qquad \square$$

Příklad 13.14. Mějme

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 0 \\ 0 & -2 \end{pmatrix}.$$

SVD rozklad:

$$A = \begin{pmatrix} \frac{\sqrt{3}}{3} & 0 & -\frac{\sqrt{6}}{3} \\ \frac{\sqrt{3}}{3} & \frac{\sqrt{2}}{2} & \frac{\sqrt{6}}{6} \\ -\frac{\sqrt{3}}{3} & \frac{\sqrt{2}}{2} & -\frac{\sqrt{6}}{6} \end{pmatrix} \begin{pmatrix} \sqrt{6} & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{pmatrix}$$

Spektrální rozklady:

$$AA^T = \begin{pmatrix} \frac{\sqrt{3}}{3} & 0 & -\frac{\sqrt{6}}{3} \\ \frac{\sqrt{3}}{3} & \frac{\sqrt{2}}{2} & \frac{\sqrt{6}}{6} \\ -\frac{\sqrt{3}}{3} & \frac{\sqrt{2}}{2} & -\frac{\sqrt{6}}{6} \end{pmatrix} \begin{pmatrix} 6 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{\sqrt{3}}{3} & \frac{\sqrt{3}}{3} & -\frac{\sqrt{3}}{3} \\ 0 & \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{6}}{3} & \frac{\sqrt{6}}{6} & -\frac{\sqrt{6}}{6} \end{pmatrix},$$

$$A^TA = \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{pmatrix} \begin{pmatrix} 6 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{pmatrix}. \qquad \square$$

Podobně jako u QR rozkladu, tak i pro SVD rozklad existuje redukovaná verze, tzv. *redukovaný* (nebo též *tenký*) SVD rozklad. Buď $A = U\Sigma V^T$ hodnosti r. Rozložme $U = (U_1 \mid U_2)$, $V = (V_1 \mid V_2)$ na prvních r sloupců a zbytek, a dále $S \coloneqq \operatorname{diag}(\sigma_1, \dots, \sigma_r)$. Pak

$$A = U\Sigma V^T = \begin{pmatrix} U_1 & U_1 \end{pmatrix} \begin{pmatrix} S & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} V_1^T \\ V_2^T \end{pmatrix} = U_1SV_1^T.$$

Redukovaný SVD používá jen část informace z SVD rozkladu, ale tu podstatnou, ze které můžeme plný SVD rozklad zrekonstruovat (doplněním U, V na ortogonální matice). Redukovaný SVD jsme trochu používali už v důkazu Algoritmu 13.13.

13.5 Aplikace SVD rozkladu

SVD a ortogonalizace

SVD rozklad lze použít k nalezení ortonormální báze (nejen) sloupcového prostoru $\mathcal{S}(A)$. Na rozdíl od dosavadních přístupů nemusíme předpokládat lineární nezávislost sloupců matice A.

Věta 13.15. *Nechť $A = U\Sigma V^T$ je SVD rozklad matice $A \in \mathbb{R}^{m\times n}$. Pak*

(1) Sloupce U_1 tvoří ortonormální bázi prostoru $\mathcal{S}(A)$.

(2) Sloupce V_2 tvoří ortonormální bázi prostoru $\mathrm{Ker}\,(A)$.

Důkaz.

(1) Redukovaný SVD rozklad je $A = U_1 S V_1^T$. Přenásobením V_1 zprava dostaneme $AV_1 = U_1 S$. Nyní, $\mathcal{S}(A) \ni \mathcal{S}(AV_1) = \mathcal{S}(U_1 S) = \mathcal{S}(U_1)$. Protože $\mathrm{rank}(A) = \mathrm{rank}(U_1)$ máme rovnost $\mathcal{S}(A) = \mathcal{S}(U_1)$.

(2) Z transpozice $A^T = V_1 S U_1^T$ dostáváme redukovaný SVD rozklad matice A^T. Tedy sloupce V_1 tvoří ortonormální bázi prostoru $\mathcal{S}(A^T) = \mathcal{R}(A) = \mathrm{Ker}\,(A)^\perp$. Proto sloupce V_2, které doplňují sloupce V_1 na ortonormální bázi $\mathbb{R}^n$, představují ortonormální bázi $\mathrm{Ker}\,(A)$. □

SVD a projekce do podprostoru

Nechť $A \in \mathbb{R}^{m\times n}$ má lineárně nezávislé sloupce. Projekce vektoru $x \in \mathbb{R}^m$ do sloupcového prostoru $\mathcal{S}(A)$ je $x' = A(A^TA)^{-1}A^Tx$. Výraz zjednodušíme s použitím redukovaného SVD rozkladu $A = U_1 S V_1^T$. Protože $\mathrm{rank}(A) = n$, tak $V_1 = V \in \mathbb{R}^{n\times n}$ je čtvercová matice. Pak

$$\begin{aligned} A(A^TA)^{-1}A^T &= U_1 S V^T (V S U_1^T U_1 S V^T)^{-1} V S U_1^T = U_1 S V^T (V S^2 V^T)^{-1} V S U_1^T \\ &= U_1 S V^T V S^{-2} V^T V S U_1^T = U_1 U_1^T. \end{aligned}$$

Matice projekce je tedy $U_1U_1^T$ a x se projektuje na $x' = U_1U_1^Tx$.

Podobným způsobem odvodíme i vzoreček pro přibližné řešení soustavy $Ax = b$, kde $A \in \mathbb{R}^{m\times n}$, $m > n$, $\mathrm{rank}(A) = n$, metodou nejmenších čtverců:

$$x = (A^TA)^{-1}A^Tb = (VSU_1^TU_1SV^T)^{-1}VSU_1^Tb = VS^{-1}U_1^Tb.$$

SVD a pseudoinverze

SVD rozklad umožňuje také zobecnit pojem inverze matice i na singulární nebo obdélníkové matice. Takové zobecněné inverzi se říká *pseudoinverze* a existuje několik druhů. Nejčastější je tzv. Moore–Penroseova pseudoinverze.[4)].

Definice 13.16 (Moore–Penroseova pseudoinverze)**.** Buď $A \in \mathbb{R}^{m\times n}$ matice s redukovaným SVD rozkladem $A = U_1 S V_1^T$. Pak Její *pseudoinverze* je $A^\dagger = V_1 S^{-1} U_1^T \in \mathbb{R}^{n\times m}$.

Příklad 13.17. $0_{m,n}^\dagger = 0_{n,m}$, pro vektory $a^\dagger = \frac{1}{a^Ta}a^T$, speciálně např. $(1,1,1,1)^\dagger = \frac{1}{4}(1,1,1,1)^T$. □

Věta 13.18 (Vlastnosti pseudoinverze)**.** *Buď $A \in \mathbb{R}^{m\times n}$, pak*

(1) Je-li A regulární, tak $A^{-1} = A^\dagger$,

(2) $(A^\dagger)^\dagger = A$,

(3) $(A^T)^\dagger = (A^\dagger)^T$,

(4) $A = AA^\dagger A$,

(5) $A^\dagger = A^\dagger AA^\dagger$,

(6) $AA^\dagger$ je symetrická,

(7) $A^\dagger A$ je symetrická.

[4)] Nezávisle ji objevili americký matematik Eliakim Hastings Moore r. 1920 a anglický fyzik, slavný popularizátor, Roger Penrose r. 1955

Důkaz. Vlastnosti se dokážou jednoduše z definice. Pro ilustraci si ukážeme jen vlastnost (4), zbytek necháváme čtenáři.

(4) Z definice $AA^\dagger A = U_1 S V_1^T V_1 S^{-1} U_1^T U_1 S V_1^T = U_1 S S^{-1} S V_1^T = U_1 S V_1^T = A$. □

První vlastnost říká, že se skutečně jedná o zobecnění klasické inverze. Vlastnosti (4)–(7) jsou zajímavé v tom, že dávají alternativní definici pseudoinverze; ta se totiž ekvivalentně dá definovat jako matice, která splňuje podmínky (4)–(7), a taková matice kupodivu existuje vždy právě jedna.

Poznamenejme, že některé vlastnosti, u kterých bychom očekávali že platí, tak obecně platit nemusí. Např. obecně $AA^\dagger \neq A^\dagger A$ a $(AB)^\dagger \neq B^\dagger A^\dagger$.

SVD a geometrie lineárního zobrazení

Mějme $A \in \mathbb{R}^{n\times n}$ regulární a studujme obraz jednotkové koule při zobrazení $x \mapsto Ax$. Z SVD rozkladu $A = U\Sigma V^T$ plyne, že lineární zobrazení lze rozložit na složení tří základních zobrazení: ortogonální zobrazení s maticí V^T, škálování podle Σ a ortogonální zobrazení s U. Konkrétně, V^T kouli zobrazí na sebe sama, Σ ji zdeformuje na elipsu a U ji otočí/převrátí. Tedy výsledkem bude elipsa se středem v počátku, poloosy jsou ve směrech sloupců U a délky mají $\sigma_1, \ldots, \sigma_n$.

Hodnota $\frac{\sigma_1}{\sigma_n} \geq 1$ se nazývá *míra deformace* a kvantitativně udává jak moc zobrazení deformuje geometrické útvary. Význam je ale nejenom geometrický. V numerické matematice se podíl $\frac{\sigma_1}{\sigma_n}$ nazývá číslo podmíněnosti a čím je větší, tím hůře podmíněná je matice A ve smyslu, že vykazuje špatné numerické vlastnosti – zaokrouhlování v počítačové aritmetice s pohyblivou řádkovou čárkou způsobuje chyby.

Empirické pravidlo říká, že pokud je číslo podmíněnosti řádově 10^k, pak při výpočtech s maticí (inverze, řešení soustav, atp.) ztrácíme přesnost o k desetinných míst. Ortogonální matice mají číslo podmíněnosti 1, a proto se v numerické matematice často používají. Naproti tomu např. Hilbertovy matice z Příkladu 3.37 mají číslo podmíněnosti velmi vysoké:

n	číslo podmíněnosti H_n
3	≈ 500
5	$\approx 10^5$
10	$\approx 10^{13}$
15	$\approx 10^{17}$

SVD a numerický rank

Hodnost matice A je rovna počtu (kladných) singulárních čísel. Nicméně, pro výpočetní účely se hodně malé kladné číslo považuje za praktickou nulu. Buď $\varepsilon > 0$, pak *numerický rank* matice A je $\max\{s;\ \sigma_s > \varepsilon\}$, tedy počet singulárních čísel větších než ε, ostatní se berou za nulová. Např. Matlab / Octave bere $\varepsilon := \max\{m, n\} \cdot \sigma_1 \cdot eps$, kde $eps \approx 2 \cdot 10^{-16}$ je přesnost počítačové aritmetiky.

SVD a low-rank aproximace

Buď $A \in \mathbb{R}^{m\times n}$ a $A = U\Sigma V^T$ její SVD rozklad. Pokud ponecháme k největších singulárních čísel a ostatní vynulujeme $\sigma_{k+1} := 0, \ldots \sigma_r := 0$, tak dostaneme matici

$$A' = U \operatorname{diag}(\sigma_1, \ldots, \sigma_k, 0, \ldots, 0) V^T$$

hodnosti k, která dobře aproximuje A. Navíc tato aproximace je v jistém smyslu nejlepší možná. To jest, v určité normě je ze všech matic hodnosti k právě A' nejblíže matici A. Low-rank aproximaci využijeme v následujícím:

SVD a komprese dat

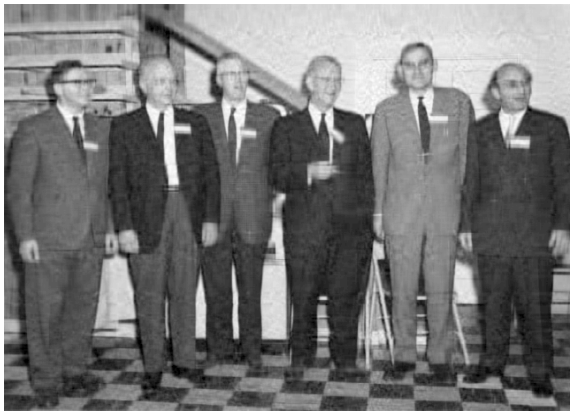
Předpokládejme, že matice $A \in \mathbb{R}^{m\times n}$ reprezentuje data, které chceme zkomprimovat. Pokud $\operatorname{rank}(A) = r$, tak pro redukovaný SVD rozklad $A = U_1 S V_1^T$ si potřebuje zapamatovat $mr + r + nr = (m + n + 1)r$ hodnot. Při low-rank aproximaci $A \approx U \operatorname{diag}(\sigma_1, \ldots, \sigma_k, 0, \ldots, 0) V^T$ si stačí pamatovat jen $(m + n + 1)k$.

Tedy kompresní poměr je $k : r$. Čím menší k, tím menší objem dat si stačí pamatovat. Ale na druhou stranu, menší k značí horší aproximaci.

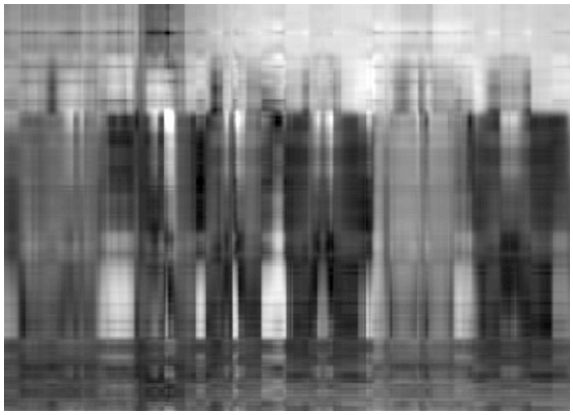
Příklad 13.19. Ilustrujeme si zmíněný postup na kompresi obrázku. Předpokládáme, že matice $A \in \mathbb{R}^{m\times n}$ reprezentuje obrázek, ve kterém pixel na pozici (i, j) má barvu s číslem a_{ij}. Následující obrázky ilustrují komprimaci pro různou volbu k. Pro $k = 480$ máme originální obrázek, pro 150 asi třetinovou kompresi bez znatelné újmy na kvalitě obrázku, při $k = 50$ už dochází k zrnění a při $k = 5$ je obrázek značně rozmazán (ale na to, že máme zhruba 1% původního objemu dat, je výsledek stále slušný).

originál ($k = 480$)

$k = 150$



$k = 50$



$k = 5$

Obrázek představuje foto z konference o numerické algebře v Gatlinburgu z r. 1964, a zaznamenává největší numerické matematiky své doby, zleva: James H. Wilkinson, Wallace Givens, George Forsythe, Alston Householder, Peter Henrici, and Fritz Bauer. Obrázek se skládá z 480×640 pixelů, SVD rozklad trval cca 5 sec (11.5.2010). Zdrojový kód pro Matlab / Octave:

```
load gatlin,
[X,S,Y] = svd(X);
figure(2), clf,
k = 150;
Xk = X(:,1:k)*S(1:k,1:k)*Y(:,1:k)';
image(Xk),
colormap(map),
axis equal, axis off,
```

□

SVD a míra regularity

Jak jsme si uvedli v Poznámce 9.8, determinant se jako míra regularity moc nehodí. Zato singulární čísla jsou pro to jako stvořená. buď $A \in \mathbb{R}^{n\times n}$. Pak σ_n udává vzdálenost (v jisté normě) k nejbližší

singulární matici, podrobněji viz [Rohn, 2004]. Takže je to v souladu s tím, co bychom si pod takovou mírou představovali. Ortogonální matice mají míru 1, naproti tomu Hilberovy matice mají malou míru regularity, tj. jsou téměř singulární:

n	$\sigma_n(H_n)$
3	≈ 0.0027
5	$\approx 10^{-6}$
10	$\approx 10^{-13}$
15	$\approx 10^{-18}$

Literatura

J. Bečvář. *Lineární algebra*. Matfyzpress, Praha, 3rd edition, 2005.

L. Bican. *Lineární algebra a geometrie*. Academia, Praha, 2nd edition, 2009.

B. A. Cipra. The best of the 20th century: Editors name top 10 algorithms. *SIAM News*, 33:1–2, 2000.

J. Dongarra and F. Sullivan. Guest editors' introduction: The top 10 algorithms. *Computing in Science and Engineering*, 2:22–23, 2000.

W. Gareth. *Linear Algebra with Applications*. Jones and Bartlett Publishers, Boston, 4th edition, 2001.

T. Krisl. Cauchyova–Schwarzova nerovnost. Master's thesis, Masaryk University, Faculty of Science, Department of Mathematics and Statistics, Brno, Czech Republic, May 2008. `http://www.is.muni.cz/th/106635/prif_m/diplomka.pdf`.

A. N. Langville and C. D. Meyer. *Google's PageRank and beyond. The science of search engine rankings*. Princeton University Press, Princeton, 2006.

J. Matoušek. Informace k přednáškám a cvičením, 2010. `http://kam.mff.cuni.cz/~matousek/vyuka.html`.

J. Matoušek and J. Nešetřil. *Kapitoly z diskrétní matematiky*. Karolinum, Praha, 4th edition, 2009.

C. D. Meyer. *Matrix analysis and applied linear algebra (incl. CD-ROM and solutions manual)*. SIAM, Philadelphia, PA, 2000. `http://www.matrixanalysis.com/DownloadChapters.html`.

J. Rohn. Lineární a nelineární programování (Učební text). `http://uivtx.cs.cas.cz/~rohn/ucebnitexty/linnelinprog.pdf`, 1997.

J. Rohn. *Lineární algebra a optimalizace*. Karolinum, Praha, 2004. 1st edition, na slidech na `http://uivtx.cs.cas.cz/~rohn/publist/laslidesrev.ps`.

G. Strang. *Linear algebra and its applications*. Thomson, USA, 3rd edition, 1988.

J. Tůma. Texty k přednášce Lineární algebra. `http://www.karlin.mff.cuni.cz/~tuma/NNlinalg.htm`, 2003.