Milan Hladík

LINEÁRNÍ ALGEBRA

(NEJEN)

PRO INFORMATIKY

3. listopadu 2014

Co?

Právě čtete učební text k přednáškám Lineární algebra I a II pro první ročník studia informatiky na Matematicko-fyzikální fakultě Univerzity Karlovy v Praze. Nicméně věřím, že může dobře posloužit i na jiných školách.

Proč?

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.

Jak?

Text poskytuje poměrně ucelený výklad na sebe navazujících témat základní lineární algebry. Několik složitých důkazů z didaktických důvodů vynecháváme – konkrétně důkaz Věty 4.29 o velikosti konečných těles, Věty 10.34 o Jordanově normální formě, Perronovy Věty 10.48 a Věty 13.11 o SVD rozkladu.

Formát textu je tradiční se členěním do definic, vět, důkazů apod. Navzdory jiným moderním trendům mi připadá tento styl přehlednější a srozumitelnější. Snažil jsem, nicméně, obohatit text vysvětlujícími komentáři a ilustrativními obrázky.

Jistým specifikem testu je něco, co nazývám „nahlédnutí pod pokličku“ jiných oborů. Bez detailů, na které není prostor a mnohdy ani matematické zázemí, ukazujeme netriviální aplikace a souvislosti s jinými matematickými obory. Toto se týká mj. aplikací o diskrétní a rychlé Fourierově transformaci (Sekce 3.6), samoopravných kódech (Příklad 4.35), Stewartově–Goughově platformě v robotice (Sekce 7.2), vyhledávači od Google (Příklad 10.56), určování struktury bílkovin (Příklad 11.20), kuželoseček (Sekce 12.2) či komprese dat (Sekce 13.5).

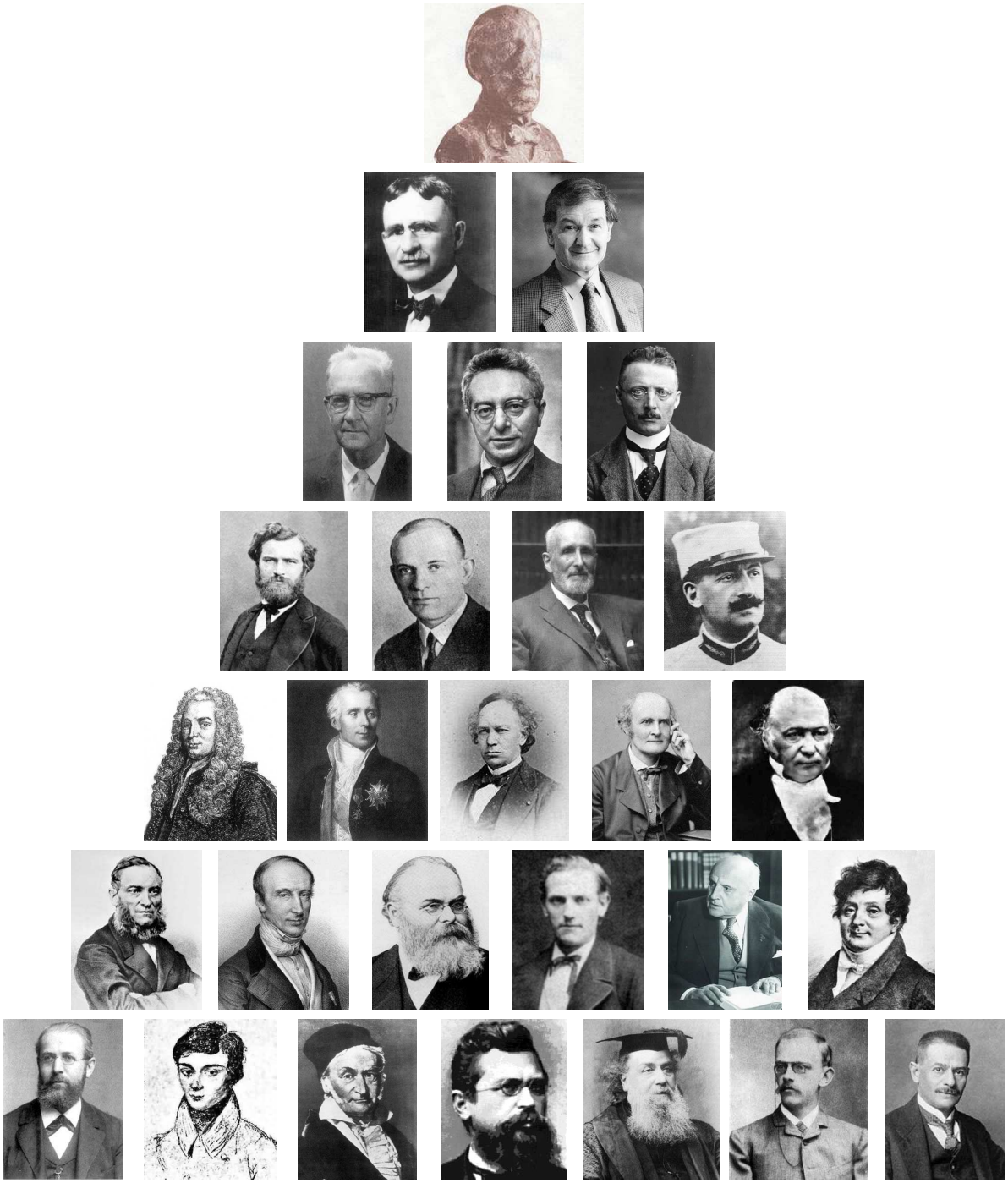
Některé partie a věty dále nerozvíjíme a v případě nutnosti je lze při výkladu vynechat. Jedná se například o sekci o jednoznačnosti RREF (Sekce 3.4), o dodatcích k soustavám rovnic (Sekce 3.5), o prostoru lineárních zobrazení (Sekce 6.3), o afinních prostorech (Kapitola 7), o teorii nezáporných matic (Sekce 10.6), o výpočtu vlastních čísel (Sekce 10.7) a o maticových rozkladech (Kapitola 13). Z vět je možno přeskočit například Shermanovu–Morrisonovu formuli (Věta 3.34), Besselova nerovnost a Parsevalovu rovnost (Věta 8.22), Gramovu matici (Věta 8.32), ortogonální matici a lineární zobrazení (Věty 8.46 a 8.47), nebo Courantovu–Fischerovu formuli (Věta 10.47).

Poděkování

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 mj. studentům: Jan Tomášek, Jakub Suchý, Martin Polák, Tomáš Novella, Tomáš Musil, Petr Babička, Antonín Tomeček a Jiří Pavlovský. Za podnětné připomínky děkuji kolegům Jaroslavu Horáčkovi, Jiřímu Šejnohovi a zejména Jiřímu Matouškovi.

Chyby?

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



„Pokud jsem dohlédl dále než jiní, bylo to proto, že jsem stál na ramenech obrů.“
[Isaac Newton, 1675]

Obsah

Kapitola 1

Úvod

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

1.1 Pojmy a značení

Nejprve je nutné zavést některé standardní značení, které se v matematice používá.

Číselné obory

Připomeňme základní číselné obory:

- $\mathbb{N}$ ... množina přirozených čísel,
- $\mathbb{Z}$ ... množina celých čísel,
- $\mathbb{Q}$ ... množina racionálních čísel,
- $\mathbb{R}$ ... množina reálných čísel.

Suma

Symbol sumy „$\sum$“ reprezentuje součet všech instancí výrazu za sumou pro všechny přípustné hodnoty indexu (resp. indexů) pod sumou. Konkrétně:

$$\sum_{i=1}^{n} a_i \quad \text{je zkratka za} \quad a_1 + \ldots + a_n,$$
$$\sum_{1\leq i\leq 8 \text{ a liché}} a_i \quad \text{je zkratka za} \quad a_1 + a_3 + a_5 + a_7,$$
$$\sum_{i,j\in\{1,2\}} a_{ij} \quad \text{je zkratka za} \quad a_{11} + a_{12} + a_{21} + a_{22}.$$

Součet přes prázdnou množinu definujeme jako 0.

Produkt

Analogicky symbol „$\prod$“ se používá pro součin, tedy např.

$$\prod_{i=1}^{n} a_i \quad \text{je zkratka za} \quad a_1 \cdot a_2 \cdot \ldots \cdot a_n.$$

Kvantifikátory

Symbol „$\forall$“ je zkratka pro sousloví „pro všechna“, a symbol „$\exists$“ znamená „existuje“. Např.

$$\forall x \in \mathbb{R} : x + 1 \leq e^x$$

se čte

pro všechna reálná čísla x platí nerovnost $x + 1 \leq e^x$.

Podobně,

$$\forall x, y \in \mathbb{R}, x < y, \exists z \in \mathbb{Q} : x < z < y$$

můžeme číst

pro jakékoliv dvě různá reálná čísla existuje racionální číslo ležící mezi nimi.

Modulo

Modulo, zapisované výrazem „$a \bmod n$“, udává zbytek při dělení celého čísla a přirozeným číslem n. Například,

$$17 \bmod 7 = 3,$$
$$-17 \bmod 7 = 4.$$

Body a vektory

Pojem bod se v základním kurzu z lineární algebry moc nepoužívá. Bod, jakožto jako n-tice reálných čísel $(v_1, \ldots, v_n)$, se algebraicky chová stejně jako aritmetický vektor (Definice 2.3). Oba pojmy se interpretují různě až z geometrického hlediska, kdy nenulovému vektoru odpovídá určitý směr (mimochodem, slovo „vektor“, stejně jako „vehikl“, pochází z latinského *vehere*, tedy „vézt“).

Zobrazení

Zobrazení f z množiny $\mathcal{A}$ do množiny $\mathcal{B}$ se značí $f\colon \mathcal{A} \to \mathcal{B}$. Pro každé $a \in \mathcal{A}$ je tedy $f(a)$ definováno a náleží do $\mathcal{B}$. Některé důležité typy zobrazení, se kterými budeme pracovat, jsou následující:

- Zobrazení $f\colon \mathcal{A} \to \mathcal{B}$ je *prosté*, pokud pro každé $a_1, a_2 \in \mathcal{A}$, $a_1 \neq a_2$, je $f(a_1) \neq f(a_2)$. Prosté zobrazení tedy nezobrazí dva různé prky z množiny $\mathcal{A}$ na jeden prvek množiny $\mathcal{B}$.
- Zobrazení $f\colon \mathcal{A} \to \mathcal{B}$ je „*na*“, pokud pro každé $b \in \mathcal{B}$ existuje $a \in \mathcal{A}$ takové, že $f(a) = b$. Jinými slovy, zobrazení f pokryje celou množinu $\mathcal{B}$.
- Zobrazení $f\colon \mathcal{A} \to \mathcal{B}$ je *vzájemně jednoznačné (bijekce)*, pokud je prosté a „na“.
- Je-li $f\colon \mathcal{A} \to \mathcal{B}$ vzájemně jednoznačné, pak *inverzní zobrazení* k f je zobrazení $f^{-1}\colon \mathcal{B} \to \mathcal{A}$ definované $f^{-1}(b) = a$ pokud $f(a) = b$. Vzájemná jednoznačnost zobrazení f zajistí, že inverzní zobrazení f^{-1} je dobře definované v každém bodě množiny $\mathcal{B}$ a je také vzájemně jednoznačné (ověřte!).
- Jsou-li $f\colon \mathcal{A} \to \mathcal{B}$, $g\colon \mathcal{B} \to \mathcal{C}$, pak *složené zobrazení* f a g je zobrazení $g \circ f\colon \mathcal{A} \to \mathcal{C}$ definované předpisem $(g \circ f)(a) = g(f(a))$. Složením vzájemně jednoznačných zobrazení dostaneme vzájemně jednoznačné zobrazení (ověřte!).

1.2 Reprezentace čísel

V počítači se standardně reprezentují čísla v tzv. tvaru s pohyblivou řádovou čárkou

$$m \times b^t,$$

kde b je daný základ vyjadřující, jakou číselnou soustavu používáme; většinou je $b = 2$. Hodnota matisy m a exponentu t pak určují konkrétní hodnotu reprezentovaného čísla. Navic vyjádření normujeme tak, aby mantisa m splňovala podmínku $1 \leq m < b$. Protože pro mantisu a exponent bývá na počítači omezená velikost zápisu, můžeme reprezentovat pouze konečně mnoho reálných čísel. Ty ostatní pak alespoň chceme vyjádřit nejbližším reprezentovatelným číslem. Tím přirozeně dochází ke ztrátě informace.

Například, číslo $1/3$ se v dekadickém zápisu při přesnosti na čtyři plané cifry reprezentuje jako 3.333×10^{-1}, čili odpovídá číslu 0.3333. Takovéto zaokrouhlovací chyby se pak mohou dále akumulovat při vyhodnocování aritmetických operací. Například, součet čísel $1/3$ a $1/3$ vede na součet reprezentací 0.3333 a 0.3333 s výsledkem 0.6666. Nicméně, nejbližší reprezentovatelné číslo ke skutečnému součtu $1/3+1/3 = 2/3$ je 0.6667.

Vliv zaokrouhlovacích chyb a omezené reprezentace čísel proto musíme vzít v úvahu při návrhu algoritmů. Podrobněji se touto problematikou zabývá obor *numerická analýza*, ale i my se numerického hlediska dotkneme např. v Sekci 3.5.1 a Sekci 13.5.

1.3 Komplexní čísla

Komplexní číslo z zavádíme jako výraz $a + bi$, kde $a, b \in \mathbb{R}$ a imaginární jednotka i splňuje $i^2 = -1$. Zde a je *reálná část* komplexního čísla z a značí se $\mathsf{Re}(z)$, a b je *imaginární část* komplexního čísla z a značí se $\mathsf{Im}(z)$. Díky vlastnosti imaginární jednotky definujeme základní operace sčítání a násobení pro dvě komplexní čísla $z_1 = a + bi$, $z_2 = c + di$ takto:

$$\begin{aligned} z_1 + z_2 &= (a + c) + (b + d)i, \\ z_1 z_2 &= (ac - bd) + (cb + ad)i. \end{aligned}$$

Podobně pro odečítání. Pro $z_2 \neq 0$ pak vychází podíl

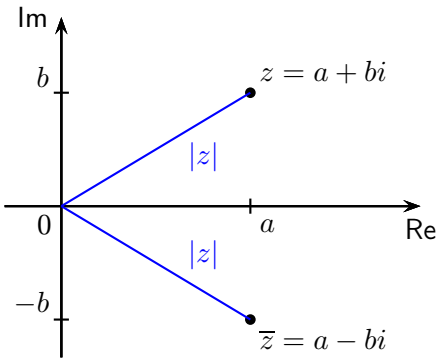
$$\frac{z_1}{z_2} = \frac{a + bi}{c + di} = \frac{a + bi}{c + di} \cdot \frac{c - di}{c - di} = \frac{ac + bd}{c^2 + d^2} + \frac{cb - ad}{c^2 + d^2} i.$$

Komplexní čísla mají také geometrickou interpretaci. Číslo $a + bi$ si lze představit jako bod (a, b) v rovině. Tato rovina se nazývá komplexní rovina (též Gaussova rovina).

Pro komplexní číslo $z = a + bi$ pak zavádíme následující operace:

$$\begin{aligned} \text{komplexně sdružené číslo:} \quad & \overline{z} := a - bi, \\ \text{absolutní hodnota:} \quad & |z| := \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}. \end{aligned}$$

Absolutní hodnota čísla $z = a + bi$ vlastně určuje eukleidovskou vzdálenost bodu (a, b) od počátku. Poznamenejme, že obecně $|z|^2 \neq z^2$.



Je jednoduchým cvičením ukázat, že komplexně sdružená čísla splňují vlastnosti:

$$\begin{aligned} \overline{z_1 + z_2} &= \overline{z_1} + \overline{z_1}, \\ \overline{z_1 \cdot z_2} &= \overline{z_1} \cdot \overline{z_1}. \end{aligned}$$

1.4 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 $n \geq m$. 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 $s(x)$ představuje zbytek. Například, dělíme-li polynom $p(x) = x^3$ polynomem $q(x) = x^2 - x$, dostaneme polynom $r(x) = x + 1$ a zbytek $s(x) = x$, tedy
$$p(x) = (x + 1)q(x) + x.$$

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, byť komplexní, vždy existuje.

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

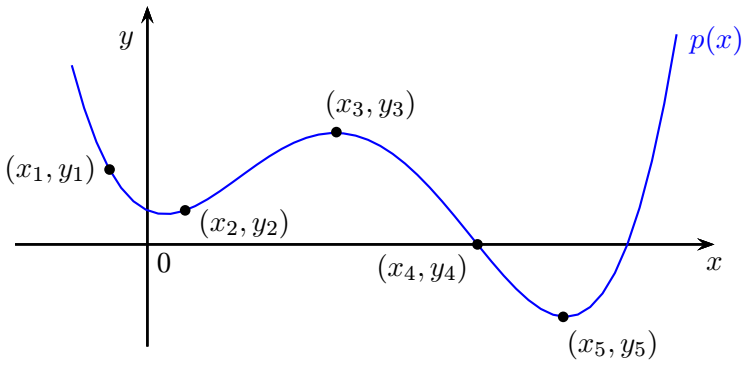
Důkaz. Důkazů existuje celá řada a žádný není zcela elementární. Myšlenkově snadno uchopitelný je důkaz autorů Melane & Birkhof a základní idea je následující. Uvažujme obraz kružnice v komplexní rovině se středem v počátku a poloměrem r při zobrazení $x \mapsto p(x)$. Je-li r hodně blízko nuly, je obrazem 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 $x_{1,2} = \frac{1}{2a_2}(-a_1 \pm \sqrt{a_1^2 - 4a_2 a_0})$. 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 o jednoznačnosti a minimalitě stupně prokládaného polynomu v Sekci 3.6.



Věta 1.2 (Lagrangeův interpolační polynom)**.** *Danými 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 $j \neq k$. □

1.5 Optimalizace

Buď $f\colon \mathbb{R}^n \to \mathbb{R}$ reálná funkce, která přiřazuje každému bodu $x = (x_1, \ldots, x_n)$ reálné číslo $f(x)$. Buď $M \subset \mathbb{R}^n$ množina bodů. Pak úloha *optimalizace* je

$$\min f(x) \text{ za podmínky } x \in M. \tag{1.1}$$

Chceme tedy najít minimální hodnotu funkce $f(x)$ na množině M. Jinými slovy, hledáme takový bod $x \in M$, že $f(x) \leq f(y)$ pro všechna $y \in M$.

Příklad 1.3. Uvažujme funkci $f(x_1, x_2) = x_1 - x_2$ a množinu bodů M v rovině zadanou omezeními

$$x_1 + 2x_2 \leq 4,\ x_1 \geq 0,\ x_2 \geq 0.$$

Množina M představuje trojúhelník s vrcholy $(0, 0)$, $(4, 0)$ a $(0, 2)$. Minimální hodnota funkce se nabyde v bodě $(0, 2)$, což je hledané optimální řešení optimalizační úlohy (1.1). □

Kapitola 2

Soustavy lineárních 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 soustavy rovnic často objeví jako jeho podproblém.

Příklad 2.1 ([Meyer, 2000])**.** Nejstarší zaznamenaná úloha na soustavy rovnic z čínské knihy 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 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 sloupcový *vektor* je matice typu $n \times 1$

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

a řádkový vektor je matice typu $1 \times n$

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

Standardně, pokud není řečeno jinak, uvažujeme vektory sloupcové. 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: $A_{*j} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix}$.

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 $x \in \mathbb{R}^n$ 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

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

Svislá čára v rozšířené matice soustavy symbolizuje rovnost mezi levou a pravou stranou soustavy, Z formálního hlediska sice není nutné ji zobrazovat, ale pomáhá mnemotechnicky chápat význam této matice.

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

Kupříkladu, soustava z Příkladu 2.1 by se maticově zapsala jako

$$\left(\begin{array}{ccc|c} 3 & 2 & 1 & 39 \\ 2 & 3 & 1 & 34 \\ 1 & 2 & 3 & 26 \end{array}\right).$$

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

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

Za obecných předpokladů ($a_{11} \neq 0$ nebo $a_{12} \neq 0$) popisuje první rovnice přímku v rovině $\mathbb{R}^2$, a stejně tak druhá rovnice popisuje nějakou přímku. Řešení soustavy leží tedy v průniku obou přímek. Podobně pro $n = 3$, každá rovnice s aspoň jedním nenulovým koeficientem popisuje rovinu v prostoru $\mathbb{R}^3$ a řešení představuje průnik těchto rovin. Obecně pro libovolné n, rovnice určují tzv. nadroviny (srov. Kapitola 7) a řešení soustavy hledáme v jejich průniku.

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

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

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

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

Důkaz. Ponecháváme za cvičení. □

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).

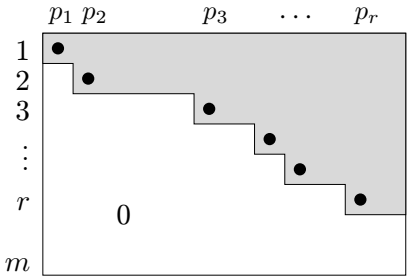
Definice 2.10 (Odstupňovaný tvar matice)**.** Matice $A \in \mathbb{R}^{m\times n}$ je v řádkově odstupňovaném tvaru, pokud existuje r takové, že platí

- 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 $(1, p_1)$, $(2, p_2)$, …, (r, p_r) se nazývají *pivoty*, sloupce p_1, p_2, …, p_r se nazývají *bázické* a ostatní sloupce *nebázické* (význam bude zřejmý později).



Schematické znázornění odstupňovaného tvaru. Pivoty jsou pozice černých teček.

Definice 2.11. *Hodností* matice A rozumíme počet nenulových řádků po převodu do odstupňovaného tvaru a značíme $\operatorname{rank}(A)$.

Hodnost matice je tedy rovna počtu pivotů (tj. číslu r) po převedení do odstupňovaného tvaru. I když odstupňovaný tvar není jednoznačný, pozice pivotů jednoznačné jsou (ukážeme si později ve Větě 3.36). Proto je pojem hodnosti[1)] dobře definován, i když to v tuto chvíli ještě není zřejmé.

Každou matici lze převést elementárními řádkovými úpravami do odstupňovaného tvaru. Například následující algoritmus převádí matici do odstupňovaného tvaru; důkaz správnosti se udělá matematickou indukcí podle počtu sloupců a rozborem. Pochopitelně, existují i různé varianty.

Algoritmus 2.12 (REF(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: $j \coloneqq \min\{\ell;\, l \geq j,\ a_{k\ell} \neq 0$ pro nějaké $k \geq i\}$, //přeskočíme nulové podsloupečky
4: urči k takové, že $a_{kj} \neq 0$, $k \geq i$ a vyměň řádky A_{i*} a A_{k*},
//nyní je na pozici pivota hodnota $a_{ij} \neq 0$
5: pro všechna $k > i$ polož $A_{k*} \coloneqq A_{k*} - \frac{a_{kj}}{a_{ij}} A_{i*}$, //2. elementární úprava

[1)] Pojem hodnosti zavedl německý matematik Ferdinand Georg Frobenius, ale podobný koncept už byl používán dříve např. anglickým matematikem Sylvestrem.

6: polož $i \coloneqq i+1$, $j \coloneqq j+1$, 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 a_{kj} s maximální absolutní hodnotou, tzv. *parciální pivotizace*, protože má lepší numerické vlastnosti při řešení soustav rovnic na počítačích. V kroku 5: zkráceně popisujeme druhou elementární úpravu, kdy od k-tého řádku odečítáme $\frac{a_{kj}}{a_{ij}}$-násobek i-tého řádku.

Důkaz správnosti algoritmu uvádět nebudeme, ale povšimneme si alespoň, že v kroku 5: vynulujeme všechny prvky pod pivotem (i,j). Pro každé $k > i$ je hodnota a_{kj} po úpravě rovna j-tému prvku řádku $A_{k*} \coloneqq A_{k*} - \frac{a_{kj}}{a_{ij}} A_{i*}$, a ten má hodnotu $a_{kj} - \frac{a_{kj}}{a_{ij}} a_{ij} = 0$.

Příklad 2.13. Ukázka převodu matice na odstupňovaný tvar, zakroužkované hodnoty ukazují aktuální pivoty:

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

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

Teď už máme vše připraveno na Gaussovu eliminaci pro řešení soustav rovnic.

Algoritmus 2.14 (Gaussova eliminace[2])**.** Buď dána soustava rovnic $(A \mid b)$. Převeď ji na odstupňovaný tvar $(A' \mid b')$. Rozlišme tři situace:

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

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. $\operatorname{rank}(A) = \operatorname{rank}(A \mid b)$, neboli $\operatorname{rank}(A') = \operatorname{rank}(A' \mid b')$).

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*: Postupně pro $k = n, n-1, \ldots, 1$ v tomto pořadí dosaď

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

Důkaz. Soustava v odstupňovaném tvaru má rovnicovou podobu

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

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

(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[3)], které popíšeme parametricky. Jako *bázické proměnné* označme ty, které odpovídají bázickým sloupcům, tj. x_{p_1}, x_{p_2}, ...,x_{p_r}, a jako *nebázické proměnné* ty zbývající. Potom nebázické proměnné budou parametry, které mohou nabývat libovolných reálných hodnot a pomocí nichž dopočítáme bázické proměnné opět zpětnou substitucí: Postupně pro $k=r,r-1,\ldots,1$ v tomto pořadí dosaď

$$x_{p_k} := \frac{b'_{p_k}-\sum_{j=p_k+1}^{n} a'_{kj}x_j}{a'_{kp_k}}.$$

Příklad 2.15. Vyřešme Gaussovou eliminací následující soustavu. Nejprve převedeme rozšířenou matici soustavy na odstupňovaný tvar

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

Zpětná substituce:

1. $x_4=1$
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 (zapsáno v řádku)

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

Tato řešení můžeme vyjádřit ekvivalentně ve tvaru

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

jehož význam vyplyne v následující kapitole. Z tohoto vyjádření rovněž vyplyne, 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 Gaussova–Jordanova eliminace

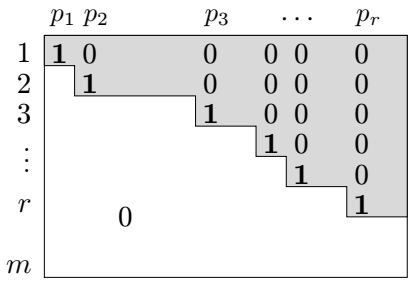
Druhý algoritmus, který si uvedeme, je Gaussova–Jordanova eliminace. Namísto odstupňovaného tvaru používá ještě specifičtější redukovaný odstupňovaný tvar, v angličtině „reduced row echelon form“ (RREF).

Definice 2.16 (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

- $a_{1p_1}=a_{2p_2}=\ldots=a_{rp_r}=1$,
- pro každé $i=1,\ldots,r$ je $a_{1p_i}=a_{2p_i}=\ldots=a_{i-1,p_i}=0$.

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

Schematické znázornění redukovaného odstupňovaného tvaru. Narozdíl od REF jsou pivoty 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 2.17 (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: $j \coloneqq \min\{l;\ l \geq j,\ a_{kl} \neq 0 \text{ pro nějaké } k \geq i\}$, //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 2.18. Ukázka převodu matice na redukovaný odstupňovaný tvar, zakroužkované hodnoty ukazují aktuální pivoty:

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

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

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

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

□

Gaussova–Jordanova eliminace pak funguje následujícím způsobem.

Algoritmus 2.19 (Gaussova–Jordanova eliminace[4])**.** 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.

(B1) Poslední sloupec je nebázický a $r = n$. Potom existuje jediné řešení, a to $(x_1, \ldots, x_n) = (b'_1, \ldots, b'_n)$.

[4] Wilhelm Jordan, z r. 1887.

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 zde přímo určují řešení. □

(B2) Poslední sloupec je nebázický a $r < n$. Potom existuje nekonečně mnoho řešení, které popíšeme parametricky. Označme 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 libovolných reálných hodnot a pomocí nich dopočítáme bázické proměnné opět zpětnou substitucí (zde lze i dopřednou): Postupně pro $k = r, r-1, \ldots, 1$ v tomto pořadí dosaď

$$x_{p_k} \coloneqq b'_{p_k} - \sum_{j \in N,\ j > p_k} a'_{kj} x_j.$$

Poznámka 2.20 (Frobeniova věta)**.** Při odvozování Gaussovy a Gaussovy-Jordanovy eliminace jsme jako důsledek dostali důležitou větu lineární algebry nazývanou Frobeniova věta,[5)] která charakterizuje řešitelnost soustav rovnic pomocí hodností matice a rozšířené matice soustavy:

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

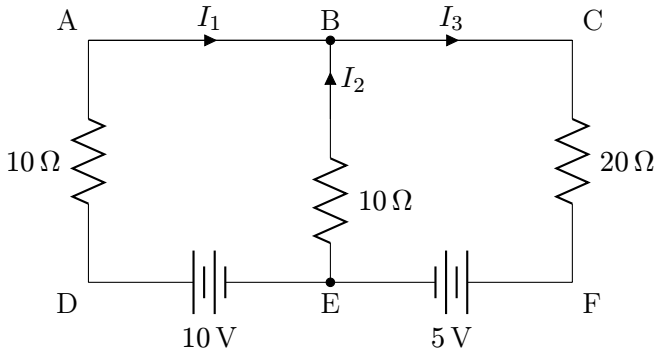
Později, v kapitole věnované vektorovým prostorům k tomu získáme ještě jiný náhled.

Poznámka 2.21 (Gaussova versus Gaussova-Jordanova eliminace)**.** Čtenář se může ptát, proč jsme uváděli dvě poměrně podobné metody na řešení soustav rovnic. Gaussova eliminace má výhodu v tom, že je ca o 50% rychlejší než ta druhá, na druhou stranu Gaussovu-Jordanovu eliminaci (či spíše RREF tvar) budeme potřebovat při invertování matic (sekce 3.3).

2.4 Aplikace

Soustavy lineárních rovnic se v praktických problémech objevují velice často, zejména jako podúloha většího problému. Uvedeme jednu aplikaci, vedoucí přímo na soustavu rovnic. Další jsou zmíněné například v Sekci 3.6.

Příklad 2.22. Uvažujme elektrický obvod jak je vyznačený na obrázku



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

Chceme-li určit hodnoty elektrických proudů I_1, I_2, I_3, využijeme fyzikálních zákonů:

1. *Ohmův zákon:* Napětí je rovno součinu proudu a odporu: $U = IR$,
2. *Kirchhoffův zákon o proudu:* Součet proudů vstupujících do uzlu se rovná součtu proudů z uzlu vystupujících.
3. *Kirchhoffův zákon o napětí:* Součet napětí ve smyčce je roven nule.

Konkrétně, Kirchhoffův zákon o proudu dává rovnici $I_1 + I_2 - I_3 = 0$. Kirchhoffův zákon o napětí (spolu s Ohmovým zákonem) pro smyčku DABE dává rovnici $10I_1 - 10I_2 = 10$, a pro smyčku EBCF dává $10I_2 + 20I_3 = 5$. (Smyčku DABCFE již uvažovat nemusíme, neboť vyplývá z předchozích dvou.) Tím dostáváme soustavu rovnic

$$\left(\begin{array}{ccc|c} 1 & 1 & -1 & 0 \\ 10 & -10 & 0 & 10 \\ 0 & 10 & 20 & 5 \end{array}\right).$$

□

Vyřešením máme $I_1 = 0.7A$, $I_2 = -0.3A$, $I_3 = 0.4A$.

Problémy

2.1. Jaké maximální absolutní hodnoty mohou nabývat složky řešení soustavy $(A \mid b)$ pokud nenulové prvky matice $A \in \mathbb{R}^{n\times n}$ jsou omezeny $q^{-1} \leq |a_{ij}| \leq q$ pro nějaké dané q?

2.2. Určete maximální počet aritmetických operací Gaussovy a Gauss-Jordanovy eliminace (tj. kolikrát sčítáme / odčítáme, a násobíme / dělíme reálná čísla) pro soustavu $n \times n$.

Kapitola 3

Matice

Matice jsme zavedli v minulé kapitole ke kompaktnímu zápisu soustav lineárních rovnic a popisu metod na jejich řešení. Matice však mají mnohem širší využití a proto se na ně v této kapitole podíváme podrobněji.

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 $i = 1, \ldots, m$, $j = 1, \ldots, n$.

Definice 3.2 (Součet)**.** Buď $A, B \in \mathbb{R}^{m\times n}$. Pak $A+B$ je matice typu $m\times n$ s prvky $(A+B)_{ij} = A_{ij}+B_{ij}$, $i = 1, \ldots, m$, $j = 1, \ldots, n$.

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 $(\alpha A)_{ij} = \alpha A_{ij}$, $i = 1, \ldots, m$, $j = 1, \ldots, n$.

Příklad 3.4 (Součet a násobek matic)**.**

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 6 & 8 \\ 10 & 12 \end{pmatrix}, \quad 5 \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 10 \\ 15 & 20 \end{pmatrix}. \qquad \square$$

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

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

Věta 3.5 (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. $\square$

Nyní zavedeme násobení matic; to je definováno na první pohled trochu neobvykle, jeho význam vyplyne později v Sekci 6.1.

Definice 3.6 (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 3.7 (Mnemotechnika násobení matic)**.** Buď

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

Mnemotechnická pomůcka pro násobení matic AB, prvek na pozici (i, j) spočítáme jako skalární součin i-tého řádku matice A a j-tého sloupce matice B:

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

□

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 3.8 (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 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

$$((AB)C)_{ij} = \sum_{k=1}^{r} (AB)_{ik}C_{kj} = \sum_{k=1}^{r} \left(\sum_{\ell=1}^{p} A_{i\ell}B_{\ell k} \right) C_{kj} = \sum_{k=1}^{r} \sum_{\ell=1}^{p} A_{i\ell}B_{\ell k}C_{kj},$$

$$(A(BC))_{ij} = \sum_{\ell=1}^{p} A_{i\ell}(BC)_{\ell j} = \sum_{\ell=1}^{p} A_{i\ell} \left(\sum_{k=1}^{r} B_{\ell k}C_{kj} \right) = \sum_{\ell=1}^{p} \sum_{k=1}^{r} A_{i\ell}B_{\ell k}C_{kj}.$$

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

Poznámka 3.9. Součin matic obecně není komutativní, pro mnoho matic je $AB \neq BA$. Navíc, může se stát, že součin AB má smysl, a přitom násobit matice v pořadí BA nelze. Najděte takové příklady!

Definice 3.10 (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 3.11. 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 3.12 (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. Pro ilustraci dokážeme jen vlastnost (1).

(1) Buď $A \in \mathbb{R}^{m \times n}$. Pak A^T má rozměr $n \times n$ a $(A^T)^T$ má tedy rozměr $m \times n$, shodný s A. Porovnáním odpovídajících si prvků $((A^T)^T)_{ij} = (A^T)_{ji} = A_{ij}$ konstatujeme rovnost, tudíž $(A^T)^T = A$. □

Definice 3.13 (Symetrická matice)**.** Matice $A \in \mathbb{R}^{n \times n}$ je *symetrická*, pokud $A = A^T$.

Symetrická matice je tedy vizuálně symetrická dle hlavní diagonály. Příkladem symetrických matic jsou jednotková matice I_n, čtvercová nulová matice 0_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.

  Příkladem diagonální matice je I_n nebo 0_n. Diagonální matici s diagonálními prvky $v_1, \ldots, v_n$ značíme $\mathrm{diag}(v)$.

- *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.*

  Příkladem horní trojúhelníkové matice je jakákoli matice v REF tvaru, protože pivoty musí být na nebo nad diagonálou. Obráceně to ovšem neplatí, horní trojúhelníková matice není automaticky v REF.

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

$$xy^T = \begin{pmatrix} x_1 y_1 & x_1 y_2 & \ldots & x_1 y_n \\ \vdots & \vdots & & \vdots \\ x_n y_1 & x_n y_2 & \ldots & x_n y_n \end{pmatrix}.$$

Například $e_i e_j^T$ je matice s jedničkou na pozici (i, j) a jinde s nulami. Standardní eukleidovskou normu 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 zmíníme 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 3.14. *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 3.15. Soustavu lineárních rovnic (2.1) můžeme maticově zapsat také takto: $Ax = b$, kde $x = (x_1, \ldots, x_n)^T$ je vektor proměnných, $b \in \mathbb{R}^m$ vektor pravých stran a $A \in \mathbb{R}^{m\times n}$ matice soustavy.

Poznámka 3.16 (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 3.17 (Rychlé násobení matic)**.** Jestliže 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, Coppersmithův–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

Regulární matice představují jeden z nejdůležitějších typů matic a budou nás provázet celou knihou.

Definice 3.18 (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*.

Soustava $Ax = 0$ s nulovou pravou stranou se nazývá *homogenní*. Evidentně, nulový vektor je vždy jejím řešením. Pro A regulární ale žádné jiné řešení existovat nesmí. 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_n.

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

(1) A je regulární,
(2) $RREF(A) = I$,
(3) $\operatorname{rank}(A) = n$.

Důkaz. Plyne z rozboru Gaussovy–Jordanovy eliminace. □

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

Věta 3.20. *Buď $A \in \mathbb{R}^{n\times n}$. Pak následující jsou 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 Gaussovy–Jordanovy eliminace a Věty 3.19. □

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

Věta 3.21. *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 $y \coloneqq Bx$. Pak soustava lze přepsat na $Ay = 0$ a z regularity A je $y = 0$, neboli $Bx = 0$. Z regularity B je $x = 0$. □

Věta 3.22. *Je-li aspoň jedna z matic $A, B \in \mathbb{R}^{n\times n}$ singulární, pak AB je také singulární.*

Důkaz. Uvažme dva případy. Je-li B singulární, pak $Bx = 0$ pro nějaké $x \neq 0$. Z toho ale plyne $(AB)x = A(Bx) = A0 = 0$, tedy i AB je singulární.

Nyní předpokládejme, že B je regulární, tedy A je singulární a existuje $y \neq 0$ takové, že $Ay = 0$. Z regularity B dostáváme, že existuje $x \neq 0$ tak, že $Bx = y$. Celkem dostáváme $(AB)x = A(Bx) = Ay = 0$, tedy AB je singulární. □

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 se dá vyjádřit jako EA pro nějakou matici E. Jak najít tuto matici? Pomůže nám uvědomíme-li si, že aplikací dané úpravy na jednotkovou matici I_n 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

$$E_{ij}(\alpha) = I + \alpha e_i e_j^T = \begin{matrix} \\ \\ \\ i \\ \\ \\ \end{matrix} \begin{matrix} \begin{matrix} 1 & 0 & \dots & \dots & 0 \end{matrix} \\ \begin{matrix} & \ddots & \ddots & & \vdots \end{matrix} \\ \begin{matrix} & & 1 & \ddots & \vdots \end{matrix} \\ \begin{matrix} & \alpha & & \ddots & 0 \end{matrix} \\ \begin{matrix} & & & & 1 \end{matrix} \\ \begin{matrix} \\ j \end{matrix} \end{matrix}.$$

3. Výměna i-tého a j-tého řádku jde reprezentovat vynásobením zleva maticí

$$E_{ij} = I + (e_j - e_i)(e_i - e_j)^T = \begin{array}{c} \\ i \\ \\ j \\ \\ \end{array} \begin{array}{c} \begin{array}{cc} i & j \end{array} \\ \begin{pmatrix} 0 & 1 \\ \\ 1 & 0 \end{pmatrix} \end{array}.$$

Snadno se ukáže, že matice elementárních operací jsou regulární. Získali jsme je totiž aplikací elementární úpravy na jednotkovou matici, tudíž inverzní úpravou převedeme matici zpět na jednotkovou.

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

Věta 3.23. *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 $E_1, E_2, \ldots, E_k$. Pak $RREF(A) = E_k \ldots E_2 E_1 A = QA$, kde $Q = E_k \ldots E_2 E_1$. Protože matice $E_1, E_2, \ldots, E_k$ jsou regulární, i jejich součin Q je regulární. □

Věta 3.24. *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 $E_1, \ldots, E_k$ elementárních úprav tak, že $A = E_k \ldots E_2 E_1 I_n = E_k \ldots E_2 E_1$. □

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

Například, matice inverzní k I_n je opět I_n. Inverzní matice k nulové 0_n evidentně neexistuje. Které matice tedy mají inverzi? Ukážeme, že pouze a jen ty regulární.

Věta 3.26 (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 $j = 1, \ldots, n$, označme je x_j, $j = 1, \ldots, n$. Vytvořme matici A^{-1} tak, aby její sloupce byly vektory $x_1, \ldots, x_n$, to jest, $A^{-1} = (x_1|x_2|\ldots|x_n)$. Ukážeme, že tato matice je hledaná inverze. Rovnost $AA^{-1} = I$ ukážeme po sloupcích. Buď $j \in \{1, \ldots, n\}$, 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 $j \in \{1, \ldots, n\}$, 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 3.29) si ukážeme lepší metodu.

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

Věta 3.27. *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 3.28 (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.

„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 3.27 je i $(A^T)^T = A$ regulární.

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

Věta 3.29 (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 3.23 existuje regulární matice Q taková, že $(I_n \,|\, B) = Q(A \,|\, I_n)$, neboli po roztržení 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 3.30. 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 3.31 (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 3.27.

(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 3.32 (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 3.33. 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, pro určitou třídu matic můžeme inverzi součtu matic vyjádřit explicitně. 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 3.34 (Shermanova–Morrisonova formule[1])**.** *Buď $A \in \mathbb{R}^{n\times n}$ regulární a $b, c \in \mathbb{R}^n$. Pokud $c^TA^{-1}b = -1$, tak $A + bc^T$ je singulární, jinak*

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

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

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

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

[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.

3.4 Jednoznačnost RREF

V této sekci ukážeme, že RREF tvar matice je jednoznačný. Sekci je možno při výkladu přeskočit, na zde uvedené výsledky již dále nenavazujeme.

Abychom dokázali jednoznačnost RREF tvaru, zformulujeme nejprve pomocné tvrzení.

Lemma 3.35. *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 matice 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 nich 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 b matice B bázický nebo ne. Jestliže 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 je nebázický, použijeme předchozí úvahy symetricky na vztah $B = Q^{-1}A$ a dostaneme, že b je také nebázický, což je spor. □

Věta 3.36 (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 3.23 existují regulární matice Q_1, Q_2 takové, že $Q_1 A = A_1$, $Q_2 A = A_2$. Přenásobením první rovnice zleva Q_1^{-1} a druhé Q_2^{-1} 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 3.35 dostáváme $A_1 = A_2$, což je spor. □

Poznámka 3.37. Předchozí věta je důležitá mj. z toho důvodu, že ospravedlňuje definici hodnosti matice jako počet pivotů RREF tvaru matice (viz Definice 2.11). Nyní je tedy pojem hodnosti dobře definován. Korektnost definice hodnosti vyplyne rovněž z teorie maticových prostorů (Věta 5.48).

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

3.5 Ještě k soustavám rovnic

3.5.1 Numerická stabilita při řešení soustav

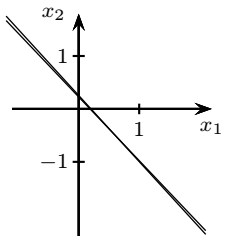
Na závěr kapitol věnovaných soustavám rovnic a maticím zmíníme, jak je to s numerickým řešením soustav lineárních rovnic (srov. Sekce 1.2). Přestože Gaussova eliminace představuje teoreticky kvalitní nástroj na řešení soustav, při numerickém řešení na počítačích dochází k zaokrouhlovacím chybám a vypočtený 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 3.38. 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 3.39. 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 $b = H_n e$ a $e = (1, \ldots, 1)^T$. Řešení soustavy je evidentně $x = e$, 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, což odpovídá přesnosti $\approx 10^{-16}$, v roce 2009 ukázaly následující složky numericky spočítaného řešení:

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

Tedy již při $n \approx 14$ mají numerické chyby enormní vliv na přesnost řešení. □

Příklad 3.40 (Parciální pivotizace)**.** Nyní 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 $(\frac{1000}{2001}, -\frac{2000}{2001})^T$. □

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 matice A a matici L můžeme získat z elementárních úprav. Pokud z elementárních úprav používáme pouze přičtení násobku řádku k nějakému pod ním (tedy bez prohazování řádků), tak matice $E_{ij}(\alpha)$ takovýchto úprav jsou dolní trojúhelníkové a jejich inverze $E_{ij}(\alpha)^{-1} = E_{ij}(-\alpha)$ taky. Tudíž nám dají dohromady hledanou matici L. Základní algoritmus tedy 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 3.41. Upravme matici A tak, že namísto nul pod diagonálou budeme zapisovat koeficienty $-\alpha$ z elementárních úprav s maticí $E_{ij}(\alpha)$, pro zdůraznění jsou zakroužkovány:

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

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 LU rozklad neexistuje pro každou matici (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. V zásadě umožňuje matici A předzpracovat tak, aby další výpočty na ní byly pak jednodušší.

Příklad 3.42. 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 3.41

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

Krok 2.

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

Krok 3.

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

Řešením soustavy $Ax = b$ je tedy vektor $x = (5, -8, -1)^T$. □

Podívejme se nyní na to, co se stane, když při Gaussově eliminaci musíme někde prohodit dva řádky. Nechť matice A je upravena na tvar $E_\ell \dots E_1 A$ pomocí ℓ elementárních úprav přičtení násobku řádku k nějakému pod ním, a nechť nyní potřebuje prohodit řádky i, j, což je reprezentováno elementární maticí E_{ij}, $i < j$. Dále, nechť předposlední úprava s maticí E_ℓ je tvaru $E_{p,q}(\alpha)$. Uvědomme si, že z charakteru Gaussovy eliminace je $q < i$.

Jsou-li indexové množiny $\{i, j\}$ a $\{p, q\}$ disjunktní, pak $E_{ij}E_{p,q}(\alpha) = E_{p,q}(\alpha)E_{ij}$. V opačném případě je $p \in \{i, j\}$. Pro $p = i$ dostaneme $E_{ij}E_{p,q}(\alpha) = E_{j,q}(\alpha)E_{ij}$ a pro $p = j$ analogicky $E_{ij}E_{p,q}(\alpha) = E_{i,q}(\alpha)E_{ij}$. Tudíž můžeme souhrnně psát $E_{ij}E_\ell = E'_\ell E_{ij}$, kde E'_ℓ je matice elementární úpravy přičtení násobku řádku k nějakému pod ním. Podobně můžeme pokračovat dál, a nakonec přepíšeme $E_{ij}E_\ell \dots E_1 A = E'_\ell \dots E'_1 E_{ij} A$, kde $E'_\ell, \dots, E'_1$ jsou matice elementární úpravy přičtení násobku řádku k řádku pod ním.

Tento postup lze aplikovat pokaždé, když musíme vyměnit dva řádky. Takže po upravení na odstupňovaný tvar U máme $E'_k \dots E'_1 E_{i_1 j_1} \dots E_{i_r j_r} A = U$, kde $E'_k, \dots, E'_1$ jsou matice elementární úpravy přičtení násobku řádku k řádku pod ním a $E_{i_1 j_1}, \dots, E_{i_r j_r}$ jsou matice úpravy prohození dvou řádků. Po úpravě dostaneme $PA = LU$, kde $L = (E'_k \dots E'_1)^{-1}$ je hledaná dolní dolní trojúhelníková matice s jedničkami na diagonále a $P = E_{i_1 j_1} \cdots E_{i_r j_r}$ je takzvaná *permutační matice*, neboť způsobuje permutaci řádků matice A.

Důsledek 3.43. *Každá matice $A \in \mathbb{R}^{n\times n}$ jde rozložit na tvar $PA = LU$, kde $P \in \mathbb{R}^{n\times n}$ je permutační matice, $L \in \mathbb{R}^{n\times n}$ je dolní trojúhelníková matice s jedničkami na diagonále a $U \in \mathbb{R}^{n\times n}$ horní trojúhelníková matice.*

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 Gaussova–Seidelova metoda, ukážeme si ji na konkrétním příkladu.

Příklad 3.44. Uvažujme soustavu

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

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 prvních šesti iterací:

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

Vidíme, že již po několika iteracích máme aproximaci skutečného řešení $(2, -1, 6)^T$. □

3.6 Aplikace

Příklad 3.45 (Leontiefův model ekonomiky)**.** Leontiefův[2)] vstupně-výstupní model ekonomiky popisuje vztahy mezi různými odvětvími ekonomiky.

Uvažujme ekonomiku s n sektory (např. zemědělství, průmysl, dopravu, atp.). Sektor i vyrábí jednu komoditu o množství x_i. Předpokládejme, že výroba jednotky j-té komodity potřebuje a_{ij} jednotek i-té komodity. Označme d_i výsledný požadavek na výrobu sektoru i. Nyní nás model vypadá

$$x_i = a_{i1}x_1 + \ldots + a_{in}x_n + d_i, \quad i = 1, \ldots, n.$$

V maticové formě

$$x = Ax + d.$$

Problém tedy vede na řešení soustavy lineárních rovnic, kde $x = (x_1, \ldots, x_n)^T$ je vektor neznámých a $A \in \mathbb{R}^n$, $d \in \mathbb{R}^n$ jsou dány. Řešení má explicitní vyjádření $x = (I_n - A)^{-1}d$ a za mírných předpokladů na matici A se dá (s pokročilými znalostmi maticové teorie) ukázat, že řešení je nezáporné, což odpovídá našemu očekávání.

Leontief model aplikoval na ekonomiku USA ve 40. letech 20. století. Ekonomiku rozdělil na 500 sektorů, což v tehdejší době to byla příliš velká soustava na vyřešení, a tak zredukoval model na 42 sektorů. Z praktických důvodů ukážeme zjednodušený model se třemi sektory zemědělství, zpracovatelský průmysl a služby. Reálná data z roku 1947 jsou

$$x = Ax + d = \begin{pmatrix} 0.4102 & 0.0301 & 0.0257 \\ 0.0624 & 0.3783 & 0.1050 \\ 0.1236 & 0.1588 & 0.1919 \end{pmatrix} x + \begin{pmatrix} 39.24 \\ 60.02 \\ 130.65 \end{pmatrix},$$

kde hodnoty složek x a d jsou v mld. \$. Výsledné řešení je $x = (82.4, 138.85, 201.57)^T$, tedy celková produkce v zemědělství musí být 82.4 mld. \$, ve zpracovatelském průmyslu 138.85 mld. \$ a ve službách 201.57 mld. \$. □

Příklad 3.46 (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 $p(x) = a_n x^n + \ldots + a_1 x + a_0$. Dosadíme-li dané body, dostáváme soustavu rovnic

$$\begin{aligned} a_n x_0^n + \ldots + a_1 x_0 + a_0 &= y_0, \\ a_n x_1^n + \ldots + a_1 x_1 + a_0 &= y_1, \\ &\vdots \\ a_n x_n^n + \ldots + a_1 x_n + a_0 &= y_n. \end{aligned}$$

Rovnic je $n+1$ a proměnných také, jsou to koeficienty $a_n, \ldots, a_0$. Máme tedy soustavu rovnic se čtvercovou maticí, nazývanou Vandermondova[3)]. 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 ukážeme dole, 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 od každého sloupce kromě posledního odečteme x_n-násobek sloupce těsně napravo a pak pro $i = 1, \ldots, n$ vydělíme i-tý řádek

[2)] Wassily Leontief (1906–1999) byl rusko-americký ekonom. Jeho model ekonomiky pochází z 30. let 20. století, a byl za něj roku 1973 oceněn Nobelovou cenou za ekonomii.

[3)] Francouzský matematik Alexandre–Théophile Vandermonde (1735–1796) byl i jedním ze zakladatelů matematické teorie uzlů.

číslem $x_{i-1} - x_n$. Až na poslední řádek a sloupec dostaneme Vandermondovu matici menšího řádu, kterou upravujeme rekursivně dále.

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

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

□

Příklad 3.47 (Diskrétní a rychlá Fourierova transformace)**.** Nyní máme v zásadě dvě možné reprezentace polynomu $p(x)$, první je základní tvar $p(x) = a_n x^n + \ldots + a_1 x + a_0$ a druhá je seznamem funkčních hodnot v $n+1$ různých bodech. Mezi těmito reprezentacemi můžeme snadno přecházet. Z první na druhou 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 vynásobit 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 spočítáme funkční hodnoty ve vhodných bodech, vynásobíme 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. □

Problémy

3.1. Buď $A \in \mathbb{R}^{n\times n}$, $b \in \mathbb{R}^n$. Navrhněte co nejefektivnější způsob výpočtu $A^k b$ v závislosti na k, n, měříme-li efektivitu počtem aritmetických operací s čísly (pro jednoduchost počítejte jen součiny čísel).

3.2. Dokažte, že soustava $Ax = b$ má řešení právě tehdy když $A^T y = 0,\ b^T y = 1$ nemá řešení.

3.3. Na řešení soustavy rovnic $Ax = b$ s regulární maticí se můžeme dívat jako na funkci $(A \mid b) \mapsto x = A^{-1}b$, která vstupním hodnotám, reprezentovaným prvky matice A a vektoru b, přiřadí řešení soustavy. Znáte-li derivace, spočítejte derivaci této funkce podle a_{ij}.

3.4. *(Souboj o regularitu)* René a Simona hrají hru s maticí řádu $n \geq 2$. René přiřadí nějakému políčku libovolné reálné číslo, pak Simona přiřadí jinému políčku číslo atd. dokud se nezaplní celá matice. René vyhraje, pokud je výsledná matice regulární, a Simona vyhraje, pokud je singulární. Má někdo vítěznou strategii? A jaká bude situace, když začne Simona?

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 aj.) čísel s operacemi sčítání 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. Příkladem situace kdy to nelze je polynom $x^5 - 2x - 1$.

Grupy mají však mnohem širší použití. Díky jejich obecnosti a abstraktnosti je můžeme najít v různých oborech: fyzika (Lieovy grupy), architektura (Friezovy grupy), geometrie a molekulární chemie (symetrické grupy) aj.

Definice 4.1 (Grupa)**.** Buď $\circ\colon G^2 \to G$ binární operace na množině G. Pak *grupa* 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).

Abelova (komutativní) grupa 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. Příklady grup:

- Dobře známé $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.
- Grupy matic $(\mathbb{R}^{m\times n}, +)$.
- Množina $\mathbb{Z}_n \coloneqq \{0, 1, \ldots, n-1\}$ 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 (Sekce 4.2),
- Regulární matice s násobením (tzv. maticová grupa).

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* $a = b$ *(tzv. krácení),*

(2) neutrální prvek e je určen jednoznačně,

(3) pro každé $a \in G$ je jeho inverzní prvek určen jednoznačně,

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

(5) $(a^{-1})^{-1} = a$,

(6) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Důkaz. Ukážeme jen několik vlastností.

(1)

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

(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 $a \circ x = b$ 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)**.** *Podgrupa* grupy $(G, \circ)$ je grupa $(H, \diamond)$ taková, že $H \subseteq G$ a pro všechna $a, b \in H$ platí $a \circ b = a \diamond b$. Značení: $(H, \diamond) \leq (G, \circ)$.

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 $f\colon X \to Y$ je zobrazení, které je prosté (žádné dva různé prvky se nezobrazí na jeden) a „na“ (pokryje celou množinu Y).

Definice 4.6 (Permutace)**.** *Permutace* na konečné množině X je vzájemně jednoznačné zobrazení $p\colon X \to X$.

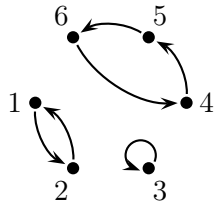
Většinou budeme uvažovat $X = \{1, \ldots, n\}$. Množina všech permutací na množině $\{1, \ldots, n\}$ se pak značí S_n.

Zadání permutace:

- Tabulkou

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

- Grafem



- Rozložením na cykly

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

kde v závorce uvádíme seznam prvků v jednom cyklu. Tedy $(a_1, \ldots, a_k)$ znamená, že a_1 se zobrazí na a_2, a_2 se zobrazí na a_3, atd. až a_{k-1} se zobrazí na a_k. Z definice je patrné, že každou permutaci lze rozložit na disjunktní cykly.

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 permutace* 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 rozdělují permutace na *sudé* (ty, co mají znaménko 1) a na *liché* (ty se znaménkem -1).

Věta 4.13 (O znaménku složení permutace a transpozice)**.** *Buď $p \in S_n$ a buď $t = (i,j)$ 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

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

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 $(-1)^r$. $\square$

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. Tedy $p \circ q$ lze složit z $r_1 + r_2$ transpozic. Pak $\operatorname{sgn}(p \circ q) = (-1)^{r_1+r_2} = (-1)^{r_1}(-1)^{r_2} = \operatorname{sgn}(p) \operatorname{sgn}(q)$. $\square$

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. $\square$

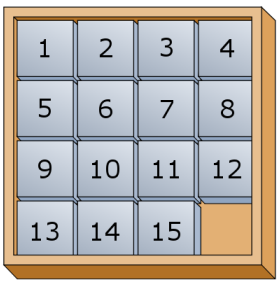
Poznámka 4.18. Kromě počtu cyklů a počtu transpozic jde znaménko permutace p zavést také např. pomocí počtu inverzí. Inverzí zde rozumíme uspořádanou dvojici (i, j) takovou, že $i < j$ a $p(i) > p(j)$. Označíme-li počet inverzí permutace p jako $I(p)$, pak platí $\operatorname{sgn}(p) = (-1)^{I(p)}$.

Poznámka 4.19. Vraťme se zpět ke grupám. Množina permutací S_n s operací skládání $\circ$ tvoří nekomutativní grupu $(S_n, \circ)$, tzv. *symetrickou grupu*. Ta hraje důležitou roli v algebře, protože se dá ukázat, že každá grupa je isomorfní nějaké symetrické grupě či její podgrupě (tzv. Cayleyova reprezentace, dokonce platí i zobecnění na nekonečné grupy). Podobnou roli hrají maticové grupy, protože každá konečná grupa je isomorfní nějaké maticové podgrupě (lineární reprezentace) s tím, že těleso, nad kterým s maticemi pracujeme, si můžeme dopředu zvolit.

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

Loydova patnáctka

Symetrické grupy a znaménko permutace se využijí také při analýze hlavolamů jako je Loydova patnáctka nebo Rubikova kostka. Rubikova kostka vyžaduje trochu hlubší rozbor, proto nahlédneme pod pokličku pouze Loydova patnáctky.



Obrázek 4.1: Loydova patnáctka. Cílový stav. [zdroj: Wikipedia]

Loydova patnáctka je hra, která sestává z pole 4×4 a kachlíky očíslovanými 1 až 15. Jedno pole je prázdné a přesouváním sousedních kachlíků na prázdné pole měníme rozložení kachlíků. Cílem je dospět pomocí těchto přesunů k vzestupnému uspořádání kachlíků tak, jak je uvedeno na obrázku.

Otázka zní, které počáteční konfigurace jsou řešitelné a které ne. Jestliže očíslujeme 1 až 16 jednotlivá políčka, pak konfigurace kachlíků odpovídá nějaké permutaci $p \in S_{16}$ a přesun kachlíku odpovídá složení p s transpozicí. Označíme-li (r, s) pozici prázdného pole, pak hodnota $h = (-1)^{r+s} \operatorname{sgn}(p)$ zůstává po celou hru stejná, protože každý posun kachlíku změní o jedničku buď r nebo s, ale zároveň posun kachlíku odpovídá složení p s odpovídající transpozicí, čili i $\operatorname{sgn}(p)$ změní znaménko.

Cílová konfigurace má hodnotu $h = 1$, tedy počáteční konfigurace s $h = -1$ řešitelné být nemohou. Detailnější analýza [Výborný a Zahradník, 2002] ukáže, že všechny počáteční konfigurace s $h = 1$ už řešitelné jsou.

4.3 Tělesa

Algebraická tělesa 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)**.** *Těleso* 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. □

Příklad 4.22 (Kvaterniony)**.** Oblíbeným příkladem těles jsou *kvaterniony*. Jedná se o zobecnění komplexních čísel přidáním dalších dvou imaginárních jednotek j a k, jejichž druhá mocnina je -1. Zatímco sčítání se definuje přirozeně, násobení je trochu komplikovanější a neplatí už pro něj komutativita. Kvaterniony pak tudíž tvoří nekomutativní těleso. Pomocí kvaternionů se dobře popisují rotace ve třírozměrném prostoru a našly využití i ve fyzikální kvantové teorii. □

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

(1) $0a = 0$,

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

(3) $-a = (-1)a$.

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 $1b = 0$.

(3) $0 = 0a = (1 - 1)a = 1a + (-1)a = a + (-1)a$, tedy $-a = (-1)a$. □

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 $\mathbb{Z}_3$ jsou tělesy, ale $\mathbb{Z}_4$ už není, neboť prvek 2 nemá inverzi 2^{-1}. Tento výsledek můžeme zobecnit.

Lemma 4.24. *Buď p prvočíslo a buď $0 \neq a \in \mathbb{Z}_p$. 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 4.25. *$\mathbb{Z}_n$ 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 4.23 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 4.24. 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 4.26. 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 4.27 (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

·	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 $\mathbb{Z}_5$

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

□

Poznámka 4.28 (Jak najít inverzi)**.** Přirozená otázka při počítání nad tělesem $\mathbb{Z}_p$ zní, jak najít inverzní prvek k $x \in \mathbb{Z}_p \setminus \{0\}$. Pro malé hodnoty p mohu zkusit postupně $1, 2, \ldots, p-1$ dokud nenarazím na inverzní prvek k x. Pokud p je hodně velké prvočíslo, tento postup už není efektivní a postupuje se tzv. *rozšířeným Eukleidovým algoritmem*, který najde $a, b \in \mathbb{Z}$ taková, že $ax + bp = 1$, z čehož vidíme, že hledanou inverzí x^{-1} je prvek a (resp. jeho zbytek po dělení p).

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

Věta 4.29 (O velikosti konečných těles)**.** *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).

Další zajímavá vlastnost je, že každé konečné těleso velikosti p^n je isomorfní s $\mathrm{GF}(p^n)$, to znamená, že taková tělesa jsou v zásadě stejná až na jiné označení prvků.

Příklad 4.30 (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 4.31 (Charakteristika tělesa)**.** *Charakteristika tělesa* $\mathbb{T}$ je nejmenší n takové, že $\underbrace{1+1+\ldots+1}_{n} = 0$. Pokud takové n neexistuje pak ji definujeme jako 0.

Věta 4.32. *Charakteristika tělesa je buď nula nebo prvočíslo.*

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

Příklad 4.33. Jestliže 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 $a - p = p - b$, je tedy stejně „vzdálené“ od a jako od b. (Viz důkaz Věty 7.3 či Příklad 12.7.)

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 4.34 (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 4.24 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 $1 = a \cdots a$. □

4.4 Aplikace

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

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

[2] Malá Fermatova věta byla formulována francouzským právníkem a amatérským matematikem Pierre de Fermatem r. 1640. Pro srovnání, 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.

Příklad 4.35 (Samoopravné kódy – Hammingův kód $(7,4,3)$)**.** Uvažujme problém přenosu dat, která jsou tvořena posloupností nul a jedniček. Zatímco úlohou šifrování je transformovat data tak, aby je nikdo nepovolaný nepřečetl, úlohou kódování je zlepšit jejich přenosové vlastnosti. Tím myslíme zejména umět detekovat a opravit chyby, které při přenosu přirozeně vznikají.

Kódování vesměs funguje tak, že odesílatel rozdělí binární posloupnost na úseky o délce k. Každý úsek pak určitou metodou přetransformuje na úsek délky k', který pak odešle. Příjemce dat pak transformuje každý úsek na původní hodnoty. Podle zvolené metody je pak schopen detekovat nebo i rovnou opravit určitý počet chyb, které v úseku vznikly.

Jednoduchý příklad. Pokud kódujeme tak, že zdvojíme každý bit, tedy např. úsek $v = 010$ zakódujeme na $v' = 001100$, tak jsme schopni detekovat maximálně jednu chybu v každém úseku. Nicméně, neumíme data opravit. Pokud budeme kódovat tak, že každý bit ztrojíme, tedy např. úsek $v = 010$ zakódujeme na $v' = 000111000$, tak už jsme schopni nejen detekovat, ale i opravit jednu chybu. Pokud příjemce dostane úsek 000111010, ví, že původní úsek byl 000111000, anebo došlo aspoň ke dvěma přenosovým chybám. Tento způsob kódování je značně neefektivní, ukážeme si šikovnější způsob.

Hammingův kód $(7,4,3)$ spočívá v rozdělení přenosových dat na úseky o čtyřech bitech, které zakódujeme na sedm bitů. Tento kód umí detekovat a opravit jednu přenosovou chybu. Kódování a dekódování jde elegantně reprezentovat maticovým násobením. Úsek čtyř bitů si představíme jako aritmetický vektor a nad tělesem $\mathbb{Z}_2$. Kódování probíhá vynásobením vektoru a takzvanou 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 obdrží úsek reprezentovaný vektorem b. Bity původních dat jsou na pozicích b_3, b_5, b_6, b_7, ostatní bity b_1, b_2, b_4 jsou kontrolní. K detekci a opravě chyb používá příjemce detekční matici $D \in \mathbb{Z}_2^{3\times 7}$. Pokud $Db = 0$, nedošlo k žádné chybě v přenosu (nebo nastaly více než dvě chyby). V opačném případě nastala přenosová chyba a chybný bit je na pozici Db, bereme-li tento vektor jako binární zápis přirozeného čísla.

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

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

Jak to, že chybný bit najdeme tak snadno? Protože vektor $Db = (1,1,0)^T$ je obsažen v matici D v šestém sloupečku, stačí změnit šestý bit vektoru b a už bude platit rovnost $Db = 0$. Všimněme si, že matice D obsahuje ve sloupcích všechny nenulové vektory, tedy všechny možné výsledky součinu Db jsou pokryty. Navíc sloupce matice D vyjadřují v binárním zápisu čísla 1 až 7, proto určíme index pokaženého bitu pomocí dvojkového vyjádření vektoru Db.

To, jak se obecně sestavují matice H, D, je však na pokročilou přednášku šifrování. Nicméně ještě několik podrobností k matici D zmíníme v Příkladu 5.53. □

Problémy

4.1. Buď G konečná grupa a H její podgrupa. Dokažte, že velikost G je dělitelná velikostí H. Při důkazu možná využijete následující mezikroky:

(a) označme $aH := \{ah;\ h \in H\}$,

(b) pro každé $a, b \in G$ platí buď $aH = bH$, anebo $aH \cap bH = \emptyset$,

(c) pro každé $a \in G$ platí, že velikost aH je stejná jako velikost H.

4.2. Pro permutaci $p \in S_n$ definujme matici $P \in \mathbb{R}^n$ tak, že $P_{ij} = 1$ pokud $p(i) = j$ a nula jinak. Ukažte, že tato definice je ekvivalentní definici permutační matice ze Sekce 3.5.2. Dále zjistěte, jak vypadá

permutační matice inverzní permutace a permutační matice složení dvou permutací.

4.3. Spočítejte průměrný počet cyklů v n-prvkové permutaci.

4.4. Určete pravděpodobnost, že náhodně zvolená permutace $p \in S_n$ má cyklus obsahující prvek 1 dlouhý přesně k.

Kapitola 5

Vektorové prostory

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

Vektorové prostory byly zavedeny „zapomenutým“ německým učitelem, lingvistou a 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 $+\colon V^2 \to V$, a násobení vektoru skalárem $\cdot\colon T \times V \to V$ 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 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 $\mathbb{R}^n$ nad $\mathbb{Q}$, opět s analogicky definovanými operacemi.
- 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:

$$\begin{aligned}(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0) + (b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0)\\ = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \ldots + (a_1 + b_1)x + (a_0 + b_0)\end{aligned}$$

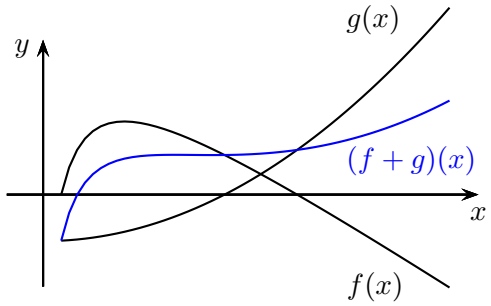
  - Násobení skalárem $\alpha \in \mathbb{R}$:

$$\begin{aligned}\alpha(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0)\\ = (\alpha a_n)x^n + (\alpha a_{n-1})x^{n-1} + \ldots + (\alpha a_1)x + (\alpha a_0)\end{aligned}$$

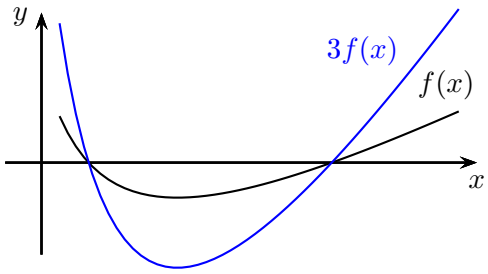
– Nulový vektor: 0
– Opačný vektor:

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

- Prostor všech reálných funkcí $f\colon \mathbb{R} \to \mathbb{R}$, značíme $\mathcal{F}$. Funkce $f, g\colon \mathbb{R} \to \mathbb{R}$ sčítáme tak, že sečteme příslušné funkční hodnoty, tedy $(f+g)(x) = f(x) + g(x)$. Podobně funkci $f\colon \mathbb{R} \to \mathbb{R}$ násobíme skalárem $\alpha \in \mathbb{R}$ tak, že vynásobíme všechny funkční hodnoty, tj. $(\alpha f)(x) = \alpha f(x)$.



Součet vektorů.



Vynásobení vektoru skalárem.

- Prostor všech spojitých funkcí $f\colon \mathbb{R} \to \mathbb{R}$, značíme $\mathcal{C}$. Prostor všech spojitých funkcí $f\colon [a,b] \to \mathbb{R}$ na intervalu $[a,b]$ pak značíme $\mathcal{C}_{[a,b]}$. Operace jsou definovány analogicky jako pro $\mathcal{F}$.

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 tvoří vektorový prostor nad $\mathbb{T}$ 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 $u, v \in U$ platí $u + v \in U$, a pro každé $\alpha \in \mathbb{T}$ a $u \in U$ platí $\alpha u \in U$.

Příklad 5.5. Příklady vektorových podprostorů:

- Dva triviální podprostory prostoru V jsou: V a $\{o\}$.
- Libovolná přímka v rovině procházející počátkem je podprostorem $\mathbb{R}^2$ nad $\mathbb{R}$, jiná ne.
- $\mathcal{P}^n \Subset \mathcal{P} \Subset \mathcal{C} \Subset \mathcal{F}$.
- 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-li $U \subseteq V$, pak $U \Subset V$. □

Nyní 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 $\operatorname{span}(W) = \bigcap_{U:W\subseteq U\leqslant V} U$.

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*, jestliže 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* vektorů $v_1, \ldots, v_n$ rozumíme výraz typu $\sum_{i=1}^n \alpha_i v_i = \alpha_1 v_1 + \ldots + \alpha_n v_n$, 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.

Pomocí lineárních kombinací (vždy uvažujeme pouze konečné!) můžeme vygenerovat celý lineární obal konečné množiny vektorů.

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 „$\supseteq$“. Lineární obal $\operatorname{span}\{v_1, \ldots, v_n\}$ 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 lineárních kombinací

$$M \coloneqq \{\textstyle\sum_{i=1}^n \alpha_i v_i;\ \alpha_1, \ldots, \alpha_n \in \mathbb{T}\}$$

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 množině M 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 $u = \sum_{i=1}^n \beta_i v_i$, $u' = \sum_{i=1}^n \beta'_i v_i$ z množiny M. 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 M. □

Překvapivě můžeme pomocí (konečných) lineárních kombinací vygenerovat lineární obal i nekonečné množiny vektorů.

Věta 5.12. *Buď V vektorový prostor nad $\mathbb{T}$ a buď $M \subseteq V$. Pak* $\operatorname{span}(M)$ *je tvořen všemi lineárními kombinacemi všech konečně mnoha vektorů z M.*

Důkaz. Analogický důkazu Věty 5.11, necháváme na cvičení. □

Příklad 5.13 (Trochu jiný pohled na soustavu rovnic $Ax = b$)**.** Výraz Ax je vlastně lineární kombinace sloupců matice A, takže řešit soustavu $Ax = b$ znamená hledat lineární kombinaci sloupců, která se rovná b. Řešení tedy existuje právě tehdy, když b náleží do podprostoru generovaného sloupci matice A. □

5.3 Lineární nezávislost

Konečně generovaný prostor typicky může být generován různými množinami vektorů. Motivací pro tuto podkapitolu je snaha najít množinu generátorů, která bude minimální co do počtu i co do inkluze. To pak povede i k pojmům jako báze, souřadnice a dimenze.

Definice 5.14 (Lineární nezávislost)**.** Buď V vektorový prostor nad $\mathbb{T}$ a mějme vektory $v_1, \ldots, v_n \in V$. 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 $\sum_{i=1}^{n} \alpha_i v_i = o$.

Pojem lineární nezávislosti zobecníme i na nekonečné množiny vektorů, nicméně s nekonečny bývá trochu potíž (např. co by se myslelo nekonečnou lineární kombinací?), proto se to definuje takto:

Definice 5.15 (Lineární nezávislost nekonečné množiny)**.** Buď V vektorový prostor nad $\mathbb{T}$ a $M \subseteq V$ nekonečná množina vektorů. Pak M je *lineárně nezávislá*, pokud každá konečná podmnožina M je lineárně nezávislá. V opačném případě je M *lineárně závislá*.

Příklad 5.16. 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 5.17. Jak zjistit zda dané aritmetické vektory, např. $(1, 3, 2)$, $(2, 5, 3)$, $(2, 3, 1)$ jsou lineárně závislé či nezávislé? Podle definice hledejme, kdy lineární kombinace vektorů dá nulový vektor:

$$\alpha(1, 3, 2) + \beta(2, 5, 3) + \gamma(2, 3, 1) = (0, 0, 0).$$

Toto vyjádříme ekvivalentně jako soustavu rovnic s neznámými α, β, γ, kdy první rovnice odpovídá rovnosti vektorů v první složce, a podobně pro další dvě:

$$\begin{aligned} 1\alpha + 2\beta + 2\gamma &= 0, \\ 3\alpha + 5\beta + 3\gamma &= 0, \\ 2\alpha + 3\beta + 1\gamma &= 0. \end{aligned}$$

Soustavu vyřešíme upravením matice soustavy na odstupňovaný tvar

$$\left(\begin{array}{ccc|c} 1 & 2 & 2 & 0 \\ 3 & 5 & 3 & 0 \\ 2 & 3 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & -4 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Soustava má nekonečně mnoho řešení a určitě najdeme nějaké nenulové, např. $\alpha = 4$, $\beta = -3$, $\gamma = 1$. To znamená, že dané vektory jsou lineárně závislé. (Ještě jiné postupy uvedeme později v Sekci 5.6.) □

Příklad 5.18. Definice lineární nezávislosti trochu připomíná definici regularity (Definice 3.18). Není to náhoda, sloupce regulární matice (a potažmo i řádky) představují další příklad lineárně nezávislých vektorů. □

Věta 5.19. *Buď V vektorový prostor nad $\mathbb{T}$, a mějme $v_1, \dots, v_n \in V$. Pak vektory $v_1 \dots, v_n$ jsou lineárně závislé právě tehdy, když existuje $k \in \{1, \dots, n\}$ takové, že $v_k = \sum_{i \neq k} \alpha_i v_i$ pro nějaké $\alpha_1, \dots, \alpha_n \in \mathbb{T}$, to jest $v_k \in \operatorname{span}\{v_1, \dots, v_{k-1}, v_{k+1}, \dots, v_n\}$.*

Důkaz. Implikace „⇒“. Jsou-li vektory $v_1, \dots, v_n$ lineárně závislé, pak existuje jejich netriviální lineární kombinace rovna nule, tj. $\sum_{i=1}^{n} \beta_i v_i = o$ pro $\beta_1, \dots, \beta_n \in \mathbb{T}$ a $\beta_k \neq 0$ pro nějaké $k \in \{1, \dots, n\}$. Vyjádříme 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 $1 \neq 0$. □

Důsledkem je ještě jiná charakterizace lineární závislosti.

Důsledek 5.20. *Buď V vektorový prostor nad $\mathbb{T}$, a mějme $v_1, \dots, v_n \in V$. Pak vektory $v_1 \dots, v_n$ jsou lineárně závislé právě tehdy, když existuje $k \in \{1, \dots, n\}$ takové, že*

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

Důkaz. Implikace „⇒“. Jsou-li vektory $v_1, \dots, v_n$ lineárně závislé, pak podle Věty 5.19 existuje $k \in \{1, \dots, n\}$ takové, že $v_k = \sum_{i \neq k} \alpha_i v_i$ pro nějaké $\alpha_1, \dots, \alpha_n \in \mathbb{T}$. Inkluze $\supseteq$ v (5.2) je splněna triviálně, zaměříme se na tu opačnou. Libovolný vektor $u \in \operatorname{span}\{v_1, \dots, v_n\}$ 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 $u \in \operatorname{span}\{v_1, \dots, v_{k-1}, v_{k+1}, \dots, v_n\}$ a máme dokázanou inkluzi „$\subseteq$“ v (5.2)

Implikace „⇐“. Pokud platí rovnost (5.2), tak

$$v_k \in \operatorname{span}\{v_1, \dots, v_n\} = \operatorname{span}\{v_1, \dots, v_{k-1}, v_{k+1}, \dots, v_n\}$$

a podle Věty 5.19 jsou vektory $v_1, \dots, v_n$ 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. Tudíž mezi nimi je nějaký nadbytečný. U lineárně nezávislého systému je tomu naopak: Odebráním libovolného z nich se jejich lineární obal ostře zmenší, není mezi nimi tedy žádný nadbytečný.

5.4 Báze

Definice 5.21 (Báze)**.** Buď V vektorový prostor nad $\mathbb{T}$. Pak *bází* rozumíme jakýkoli lineárně nezávislý systém generátorů V.

V definici pod pojmem systém rozumíme uspořádanou množinu, časem uvidíme, proč je uspořádání důležité (pro souřadnice atp.).

Příklad 5.22. 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 $e_1, \dots, e_n$, říká se jí *kanonická* a značí se kan.
- V $\mathcal{P}^n$ je bází např. $1, x, x^2, \dots, x^n$. 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 pro různé aproximace, např. ve výpočetní geometrii pro aproximaci křivek procházejících danými body (tzv. Bézierovy křivky). □
- V $\mathcal{P}$ je bází např. nekonečný ale spočetný systém polynomů $1, x, x^2, \dots$

- V prostoru $\mathcal{C}_{[a,b]}$ také musí existovat báze, ale není jednoduché žádnou explicitně vyjádřit.

Věta 5.23. *Nechť $v_1, \dots, v_n$ je báze prostoru V. Pak pro každý vektor $u \in V$ existují jednoznačně určené koeficienty $\alpha_1, \dots, \alpha_n \in \mathbb{T}$ takové, že $u = \sum_{i=1}^n \alpha_i v_i$.*

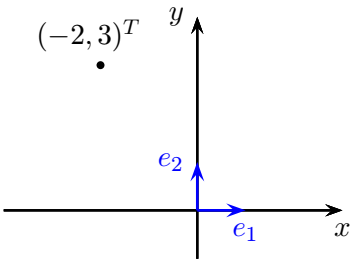
Důkaz. Vektory $v_1, \dots, v_n$ tvoří bázi V, tedy každé $u \in V$ se dá vyjádřit jako $u = \sum_{i=1}^n \alpha_i v_i$ pro vhodné skaláry. Jednoznačnost ukážeme sporem. Nechť existuje i jiné vyjádření $u = \sum_{i=1}^n \beta_i v_i$. Potom $\sum_{i=1}^n \alpha_i v_i - \sum_{i=1}^n \beta_i v_i = u - u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

Díky zmíněné jednoznačnosti můžeme zavést pojem souřadnice.

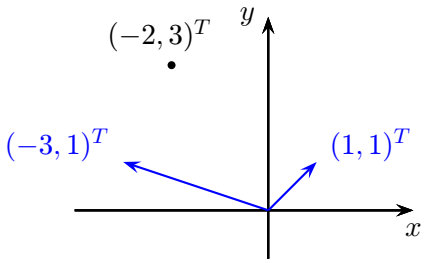
Definice 5.24 (Souřadnice)**.** Nechť $B = \{v_1, \dots, v_n\}$ je báze prostoru V a nechť vektor $u \in V$ má vyjádření $u = \sum_{i=1}^n \alpha_i v_i$. Pak *souřadnicemi* vektoru $u \in V$ vzhledem k bázi B rozumíme koeficienty $\alpha_1, \dots, \alpha_n$ a vektor souřadnic značíme $[u]_B \coloneqq (\alpha_1, \dots, \alpha_n)^T$.

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



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



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

Příklad 5.26. Pro každé $v \in \mathbb{R}^n$ je $[v]_{\text{kan}} = v$. □

Příklad 5.27. Uvažujme bázi $B = \{1, x, x^2\}$ prostoru $\mathcal{P}^2$. Pak $[3x^2 - 5]_B = (-5, 0, 3)$. □

Příklad 5.28.

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

Věta 5.29 (O existenci báze)**.** *Každý vektorový prostor má bázi.*

Důkaz. Důkaz provedeme pouze pro konečně generovaný prostor V. Pro ty ostatní je důkaz složitější a je potřeba určité poznatky z teorie množin (tzv. Zornovo lemma).

Buď $v_1, \dots, v_n$ systém generátorů V. Jsou-li lineárně nezávislé, tak už tvoří bázi. Jinak podle Důsledku 5.20 existuje index k tak, že

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

Tedy odstraněním v_k bude systém vektorů stále generovat V. Je-li nyní systém vektorů lineárně nezávislý, tvoří bázi. Jinak postup opakujeme dokud nenajdeme bázi. Postup je konečný, protože máme konečnou množinu generátorů, tudíž bázi najít musíme. □

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

Věta 5.30 (Steinitzova věta o výměně[1])**.** *Buď V vektorový prostor, buď $x_1, \dots, x_m$ lineárně nezávislý systém ve V, a nechť $y_1, \dots, y_n$ je systém generátorů V. Pak platí*

(1) $m \leq n$,

(2) existují navzájem různé indexy $k_1, \dots, k_{n-m}$ tak, že $x_1, \dots, x_m, y_{k_1}, \dots, y_{k_{n-m}}$ tvoří systém generátorů 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 $x_1, \dots, x_{m-1}$. Ty jsou lineárně nezávislé, a podle indukčního předpokladu je $m-1 \leq n$ a existují navzájem různé indexy $l_1, \dots, l_{n-m+1}$ takové, že $x_1, \dots, x_{m-1}, y_{l_1}, \dots, y_{l_{n-m+1}}$ generují V. Kdyby $m - 1 = n$, pak vektory $x_1, \dots, x_{m-1}$ jsou generátory prostoru V, a dostáváme $x_m \in V = \operatorname{span}\{x_1, \dots, x_{m-1}\}$, což je spor s lineární nezávislostí $x_1, \dots, x_m$. 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 $\beta_1 = \ldots = \beta_{n-m+1} = 0$, pak dostáváme spor s lineární nezávislostí $x_1, \dots, x_m$. Proto existuje k takové, že $\beta_k \neq 0$. Idea zbytku důkazu je vyměnit y_{l_k} za x_m. Z rovnosti 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 $x_1, \dots, x_m, y_{l_1}, \dots, y_{l_{k-1}}, y_{l_{k+1}}, \dots, y_{l_{n-m+1}}$ generují V. Vezměme libovolný vektor $x \in V$. Pro vhodné koeficienty γ_i, δ_j ho můžeme vyjádřit 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 5.31. *Všechny báze konečně generovaného vektorového prostoru V jsou stejně velké.*

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

Tvrzení se dá zobecnit na nekonečně generované prostory s tím, že všechny báze mají stejnou mohutnost.

5.5 Dimenze

Každý konečně generovaný prostor má bázi (Věta 5.29) a všechny báze jsou stejně velké (Důsledek 5.31), což ospravedlňuje zavedení dimenze prostoru jako velikosti (libovolné) báze.

Definice 5.32 (Dimenze)**.** *Dimenze* konečně generovaného vektorového prostoru V je velikost nějaké jeho báze a dimenze nekonečně generovaného prostoru je ∞. Značíme ji $\dim V$.

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

Příklad 5.33. Příklady dimenzí:

- $\dim \mathbb{R}^n = n$, $\dim \mathbb{R}^{m\times n} = mn$, $\dim \{o\} = 0$, $\dim \mathcal{P}^n = n+1$,
- reálné prostory $\mathcal{P}$, $\mathcal{F}$, a prostor $\mathbb{R}$ nad $\mathbb{Q}$ nejsou konečně generované, mají dimenzi ∞ (viz Problém 5.1.). □

Věta 5.34 (Vztah počtu prvků systému k dimenzi)**.** *Buď V konečně generovaný vektorový prostor. 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 5.30 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 systém generátorů 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 5.30 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 5.20). Podle Steinitzovy věty by pak ale platilo $d \le n-1$, což vede ke sporu. □

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

Věta 5.35 (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 5.30 existují indexy $k_1, \dots, k_{d-m}$ takové, že $x_1, \dots, x_m, z_{k_1}, \dots, z_{k_{d-m}}$ jsou generátory V. Jejich počet je d, tedy podle věty 5.34 je to báze V. □

Věta 5.36 (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 0, a shora omezená, protože pro každý lineárně nezávislý systém $x_1, \dots, x_m$ ve W (a tím i ve V) podle Věty 5.34 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 5.34 tvořit bázi V, a proto $W = V$. □

Příklad 5.37. Najděme všechny podprostory $\mathbb{R}^2$:

- dimenze 2: to je pouze $\mathbb{R}^2$ (z Věty 5.36),
- 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 lineární obal sjednocení, tomu se říká spojení podprostorů a má následující ekvivalentní předpis.

Definice 5.38 (Spojení podprostorů)**.** Buďte U, V podprostory vektorového prostoru W. Pak *spojení podprostorů U, V* je definováno jako $U + V \coloneqq \{u + v;\ u \in U, v \in V\}$.

Věta 5.39 (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 5.40.

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

Věta 5.41 (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 prostoru W, tedy má konečnou bázi $z_1, \ldots, z_p$. Podle Věty 5.35 ji můžeme rozšířit na bázi U tvaru $z_1, \ldots, z_p, x_1 \ldots, x_m$. Podobně ji můžeme rozšířit na bázi V tvaru $z_1, \ldots, z_p, y_1 \ldots, y_n$. 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.

„Generujícnost.“ 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 lineárně nezávislých vektorů, která dá nulový vektor, je triviální, proto $\delta_i = 0$ pro všechna i a $\gamma_k = 0$ pro všechna 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 $\alpha_i = 0$ pro všechna i a $\beta_j = 0$ pro všechna j. □

Poznámka 5.42 (Direktní součet podprostorů)**.** Je-li $U \cap V = \{o\}$, pak spojení podprostorů $W = U + V$ se nazývá *direktní součet* podprostorů U, V a značí se $W = U \oplus V$. 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 jsou např. $\mathbb{R}^2 = \operatorname{span}\{e_1\} \oplus \operatorname{span}\{e_2\}$, $\mathbb{R}^2 = \operatorname{span}\{(1,2)^T\} \oplus \operatorname{span}\{(3,4)^T\}$ nebo $\mathbb{R}^3 = \operatorname{span}\{e_1\} \oplus \operatorname{span}\{e_2\} \oplus \operatorname{span}\{e_3\}$ direktními součty, ale $\mathbb{R}^2 = \operatorname{span}\{(1,2)^T\} \oplus \operatorname{span}\{(3,4)^T\} \oplus \operatorname{span}\{(5,6)^T\}$ 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.

Definice 5.43 (Maticové prostory)**.** Buď $A \in \mathbb{T}^{m \times n}$. Pak definujeme

(1) sloupcový prostor $\mathcal{S}(A) \coloneqq \operatorname{span}\{A_{*1}, \ldots, A_{*n}\}$,

(2) řádkový prostor $\mathcal{R}(A) \coloneqq \mathcal{S}(A^T)$,

(3) jádro $\mathrm{Ker}\,(A) \coloneqq \{x \in \mathbb{T}^n;\ Ax = o\}$.

Sloupcový prostor je tedy prostor generovaný sloupci matice A, a je to podprostor $\mathbb{T}^m$. Podobně, řádkový prostor je prostor generovaný řádky matice A, a je to podprostor $\mathbb{T}^n$. Jádro pak je tvořeno všemi řešeními soustavy $Ax = o$ a ponecháváme na rozmyšlení, že je také jedná o podprostor $\mathbb{T}^n$.

Příklad 5.44. Uvažme matici

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Pak její sloupcový prostor $\mathcal{S}(A) = \mathbb{R}^2$, její řádkový prostor $\mathcal{S}(A) = \mathrm{span}\{(1,1,1)^T, (0,1,0)^T\}$, a její jádro $\mathrm{Ker}\,(A) = \{(1,0,-1)^T\}$. □

Díky Větě 5.11 můžeme maticové prostory ekvivalentně charakterizovat pomocí lineárních kombinací, což vede na následující tvrzení.

Tvrzení 5.45. *Buď $A \in \mathbb{T}^{m\times n}$. Pak*

(1) $\mathcal{S}(A) = \{Ax;\ x \in \mathbb{T}^n\}$,

(2) $\mathcal{R}(A) = \{A^T y;\ y \in \mathbb{T}^m\}$.

Důkaz. Necháváme za cvičení. □

Maticově můžeme reprezentovat libovolný podprostor V prostoru $\mathbb{T}^n$. Stačí vzít nějaké jeho generátory $v_1, \ldots, v_m$ a sestavit matici $A \in \mathbb{T}^{m\times n}$, 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 $\mathbb{T}^{n\times m}$. Pokud tedy dokážeme dobře manipulovat s maticovými prostory, umožní nám to zacházet i s podprostory $\mathbb{T}^n$. Jak 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).

Věta 5.46 (Prostory a násobení maticí zleva)**.** *Buď $A \in \mathbb{T}^{m\times n}$, $Q \in \mathbb{T}^{p\times m}$. Pak*

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

(2) Pokud $A_{*k} = \sum_{j\neq k} \alpha_j A_{*j}$ *pro nějaké* $k \in \{1, \ldots, n\}$ *a nějaká* $\alpha_j \in \mathbb{T}$, $j \neq k$, *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 $y \in \mathbb{T}^p$ takové, že $x = (QA)^T y = A^T Q^T y = A^T (Q^T y) \in \mathcal{R}(A)$.

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

Věta říká, že řádkové prostory jsou porovnatelné přímo – po pronásobení libovolnou maticí zleva dostaneme podprostor. Sloupcové prostory z principu porovnávat nelze, protože jsou to podprostory různých prostorů ($\mathbb{T}^m$ a $\mathbb{T}^p$). Nicméně, mezi sloupci se zachovává jakási lineárně závislostní vazba: Je-li i-tý sloupec matice A závislý na ostatních, potom i-tý sloupec matice QA je závislý na ostatních se stejnou lineární kombinací (pozor, lineární nezávislost se nemusí zachovávat).

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

Věta 5.47 (Prostory a násobení regulární maticí zleva)**.** *Buď $Q \in \mathbb{T}^{m\times m}$ regulární a $A \in \mathbb{T}^{m\times n}$. Pak*

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

(2) Rovnost $A_{*k} = \sum_{j\neq k} \alpha_j A_{*j}$ *platí právě tehdy, když* $(QA)_{*k} = \sum_{j\neq k} \alpha_j (QA)_{*j}$, *kde* $k \in \{1, \ldots, n\}$ *a* $\alpha_j \in \mathbb{T}$, $j \neq k$.

Důkaz.

(1) Podle Věty 5.46 je $\mathcal{R}(QA) \subseteq \mathcal{R}(A)$. Aplikujeme-li Větu 5.46 na matici (QA) násobenou zleva Q^{-1}, dostaneme $\mathcal{R}(Q^{-1}QA) \subseteq \mathcal{R}(QA)$, tedy $\mathcal{R}(A) \subseteq \mathcal{R}(QA)$. Dohromady máme $\mathcal{R}(QA) = \mathcal{R}(A)$.

(2) Implikaci zleva doprava dostaneme z Věty 5.46. Obrácenou implikaci dostaneme z Věty 5.46 aplikované na matici (QA) násobenou zleva Q^{-1}. □

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

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

Věta 5.48 (Maticové prostory a RREF)**.** *Buď $A \in \mathbb{T}^{m\times n}$ a A^R její RREF tvar s pivoty na pozicích $(1,p_1),\dots,(r,p_r)$. Pak*

(1) nenulové řádky A^R, tedy vektory $A^R_{1*},\dots,A^R_{r*}$, tvoří bázi $\mathcal{R}(A)$,

(2) sloupce $A_{*p_1},\dots,A_{*p_r}$ tvoří bázi $\mathcal{S}(A)$,

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

Důkaz. Víme z Věty 3.23, že $A^R = QA$ pro nějakou regulární matici Q.

(1) Podle Věty 5.47 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 $A^R_{*p_1},\dots,A^R_{*p_r}$ 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 5.47, která zaručí, že i $A_{*p_1},\dots,A_{*p_r}$ 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 5.48 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 5.49. *Pro každou matici $A \in \mathbb{T}^{m\times n}$ platí $\operatorname{rank}(A) = \operatorname{rank}(A^T)$.*

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 tady dvě teorie a společně produkují zajímavé výsledky.

Věta 5.48 rovněž nabízí ekvivalentní charakterizaci hodnosti matice jako dimenzi řádkového nebo sloupcového prostoru. Tím potvrzuje korektnost definice hodnosti z Definice 2.11, alternativně k Větě 3.36 o jednoznačnosti RREF tvaru matice.

Věta 5.48 dále dává návod, jak zjistit určité charakteristiky prostorů pomocí RREF tvaru matice. Stačí dát aritmetické vektory do matice, převést do RREF tvaru a z něj pak vyčíst danou informaci. Jestliže vektory nejsou z aritmetického prostoru $\mathbb{T}^n$, pak je potřeba na to jít oklikou, pomocí tzv. isomorfismu (Sekce 6.2).

Příklad 5.50. Uvažujme prostor

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

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 $\dim(V) = 3$ a báze V je například $(1,2,3,4,5)^T$, $(1,1,1,1,1)^T$, $(2,1,1,0,0)^T$. Třetí z generátorů je závislý na ostatních, konkrétně je roven dvojnásobku prvního minus druhý (koeficienty vidíme ve třetím sloupci matice v RREF tvaru).

Nyní dejme generující vektory do 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 5.51 (O dimenzi jádra a hodnosti matice)**.** *Pro každou matici $A \in \mathbb{T}^{m\times n}$ platí*

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

Důkaz. Buď $\dim \operatorname{Ker}(A) = k$ a nechť vektory $v_1, \ldots, v_k$ tvoří bázi $\operatorname{Ker}(A)$. Rozšiřme ji na bázi $\mathbb{T}^n$ doplněním o vektory $v_{k+1}, \ldots, v_n$. Stačí ukázat, že vektory $Av_{k+1}, \ldots, Av_n$ tvoří bázi $\mathcal{S}(A)$, protože pak $\operatorname{rank}(A) = \dim \mathcal{S}(A) = n - k$ a rovnost z věty je splněna.

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

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

„Lineární nezávislost.“ Buď $\sum_{i=k+1}^n \alpha_i A v_i = o$. Pak $A\big(\sum_{i=k+1}^n \alpha_i v_i\big) = o$, čili $\sum_{i=k+1}^n \alpha_i v_i$ patří do jádra matice A. Proto $\sum_{i=k+1}^n \alpha_i v_i = \sum_{i=1}^k \beta_i v_i$ pro nějaké skaláry $\beta_1, \ldots, \beta_k$. Přepsáním rovnice dostáváme $\sum_{i=k+1}^n \alpha_i v_i + \sum_{i=1}^k (-\beta_i) v_i = o$ a vzhledem k lineární nezávislosti $v_1, \ldots, v_n$ je $\alpha_{k+1} = \ldots = \alpha_n = \beta_1 = \ldots = \beta_k = 0$. □

Příklad 5.52. 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 $\dim \operatorname{Ker}(A) = 4 - 2 = 2$. Prostor $\operatorname{Ker}(A)$ 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

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

Tudíž vektory $(6,-4,1,0)$, $(4,-3,0,1)$ tvoří bázi $\operatorname{Ker}(A)$. Vektory získané tímto postupem představují vždy bázi $\operatorname{Ker}(A)$, protože jsou to generátory jádra a je jich stejný počet jako je $\dim \operatorname{Ker}(A)$, tedy $n - \operatorname{rank}(A)$ (srov. Věta 5.34). □

Další vlastnosti maticových prostorů ukážeme v Důsledku 8.35.

5.7 Aplikace

Příklad 5.53 (Ještě ke kódování)**.** Navažme na Příklad 4.35 o Hammingově kódu $(7,4,3)$. Ke kódování jsme používali generující matici H rozměru 7×4 jednoduše tak, že vstupní úsek a délky 4 se zakóduje na úsek $b := Ha$ délky 7. Všechny zakódované úseky tak představují sloupcový prostor matice H. Protože H má lineárně nezávislé sloupce, jedná se o podprostor dimenze 4 v prostoru $\mathbb{Z}_2^7$.

Detekce chyb přijatého úseku b probíhá pomocí detekční matice D rozměru 3×7. Pokud $Db = o$, nenastala chyba (nebo nastaly alespoň dvě). Po detekční matici tedy chceme, aby (pouze) vektory ze sloupcového prostoru matice H zobrazovala na nulový vektor. Tudíž musí $\mathcal{S}(H) = \mathrm{Ker}\,(D)$. Nyní již vidíme, proč má matice D dané rozměry – aby její jádro byl čtyř-dimenzionální podprostor, musí mít podle Věty 5.51 hodnost 3, a proto 3 lineárně nezávislé řádky postačují.

Příklad 5.54 (Rozpoznávání obličejů [Turk and Pentland, 1991])**.** Detekce a rozpoznávání obličejů z digitálního obrazu je moderní úloha počítačové grafiky. Je to příliš složitá úloha, abychom mohli vysvětlit všechny detaily úspěšných algoritmů, ale zkusíme objasnit jejich podstatu z hlediska vektorových prostorů.

Digitální obraz reprezentujeme jako matici $A \in \mathbb{R}^{m\times n}$, kde a_{ij} udává barvu pixelu na pozici i, j. Množinu obrázků s obličeji si můžeme s jistou mírou zjednodušení představit jako podprostor prostoru všech obrázků $\mathbb{R}^{m\times n}$. Báze tohoto podprostoru jsou tzv. *eigenfaces*, čili určité základní typy nebo rysy obličejů, ze kterých skládáme ostatní obličeje.

Pokud chceme rozhodnout, zda obrázek odpovídá obličeji, tak spočítáme, zda odpovídající vektor leží v podprostoru obličejů nebo v jejich blízkosti. Podobně postupujeme, pokud chceme rozpoznat zda daný obrázek odpovídá nějakému známému obličeji: Ve vektorovém prostoru $\mathbb{R}^{m\times n}$ zjistíme, který z vektorů odpovídajících známým tvářím je nejblíže vektoru našeho obrázku.

Několikrát jsme použili pojem „vzdálenost“ vektorů. Eukleidovskou vzdálenost čtenář patrně zná, podrobněji a obecněji však tento termín rozebíráme v Kapitole 8. □

Problémy

5.1. Ukažte, že prostor reálných polynomů $\mathcal{P}$, prostor reálných funkcí $\mathcal{F}$ a prostor $\mathbb{R}$ nad $\mathbb{Q}$ nejsou konečně generované.

5.2. Dokažte, že hodnost matice $A \in \mathbb{T}^{m\times n}$ je rovna velikosti největší regulární podmatice (podmatice vznikne odstraněním určitého počtu, i nulového, řádků a sloupců).

5.3. Pro matice $A \in \mathbb{R}^{m\times n}$, $B \in \mathbb{R}^{n\times p}$ zdůvodněte následující odhady pro hodnost jejich součinu

$$\mathrm{rank}(A) + \mathrm{rank}(B) - n \leq \mathrm{rank}(AB) \leq \min\{\mathrm{rank}(A), \mathrm{rank}(B)\}.$$

Kapitola 6

Lineární zobrazení

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

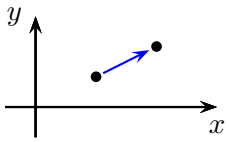
- $f(x+y) = f(x) + f(y)$,
- $f(\alpha x) = \alpha f(x)$.

Lineární zobrazení se též nazývá *homomorfismus*. Pro toho, 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*.[1)]

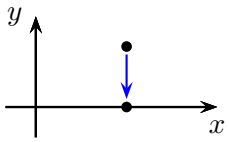
Příklad 6.2 (Příklady lineárních zobrazení)**.**

- $f\colon U \to V$ definované $f(x) = o$,
- identita je zobrazení $id\colon U \to U$ definované $id(x) = x$,
- $f\colon \mathbb{R}^n \to \mathbb{R}^m$ definované $f(x) = Ax$, kde $A \in \mathbb{R}^{m\times n}$ je pevná matice,
- derivace z prostoru reálných diferencovatelných funkcí do prostoru reálných funkcí $\mathcal{F}$.
- zobrazení $V \to \mathbb{T}^n$, které vektoru $x \in V$ přiřadí vektor souřadnic vzhledem k dané bázi B, tedy $x \mapsto [x]_B \in \mathbb{T}^n$, kde $n = \dim V < \infty$. □

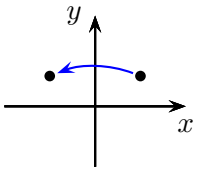
Příklad 6.3 (Příklady lineárních zobrazení v rovině)**.**



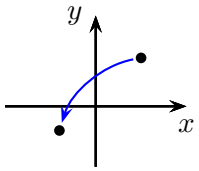
Škálování: $(x, y) \mapsto (\alpha x, \alpha y)$



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



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



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

[1)] V teorii kategorií mají pojmy jako monomorfismus a další ještě trochu obecnější význam.

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

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

(2) $f(o) = o$.

Důkaz.

(1) Z 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 $f\colon U \to V$ lineární zobrazení. Pak definujeme

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

Příklad 6.6 (Obraz a jádro)**.** V Příkladu 6.3:

- překlopení má obraz $f(\mathbb{R}^2) = \mathbb{R}^2$, a jádro $\operatorname{Ker}(f) = \{o\}$,
- projekce na osu x má obraz $f(\mathbb{R}^2) =$ osa x, a jádro $\operatorname{Ker}(f) =$ osa y. □

Snadno nahlédneme, že obraz představuje podprostor prostoru V a jádro podprostor prostoru U.

Tvrzení 6.7. *Buď $f\colon U \to V$ lineární zobrazení. Pak:*

(1) $f(U) \trianglelefteq V$,

(2) $\operatorname{Ker}(f) \trianglelefteq U$,

(3) pro každé $x_1, \dots, x_n \in U : f(\operatorname{span}(x_1, \dots, x_n)) = \operatorname{span}(f(x_1), \dots, f(x_n))$.

Důkaz. Pro ilustraci dokážeme jen první tvrzení, zbytek necháme za cvičení.

(1) Stačí ověřit, že $f(U)$ obsahuje nulový vektor a je uzavřený na součty a násobky vektorů. Protože $f(o) = o$, máme $o \in V$. Pokud $v_1, v_2 \in f(U)$, tak existují $u_1, u_2 \in U$ takové, že $f(u_1) = v_1$ a $f(u_2) = v_2$. Potom $f(u_1 + u_2) = f(u_1) + f(u_2) = v_1 + v_2$, tudíž i $v_1 + v_2 \in f(U)$. Konečně pokud $v \in V$, tak existuje $u \in U : f(u) = v$. Pak pro libovolné $\alpha \in \mathbb{T}$ je $f(\alpha u) = \alpha f(u) = \alpha v \in f(U)$, z čehož je $\alpha v \in f(U)$. □

Jádro matice a jádro lineárního zobrazení spolu úzce souvisí. Definujeme-li f předpisem $f(x) = Ax$, potom $\operatorname{Ker}(A) = \operatorname{Ker}(f)$.

Připomeňme, že zobrazení $f\colon U \to V$ je prosté, pokud $f(x) = f(y)$ nastane jenom pro $x = y$. Následující věta charakterizuje, kdy je lineární zobrazení prosté. Za cvičení aplikujte podmínky na lineární zobrazení z Příkladu 6.3.

Věta 6.8 (Prosté lineární zobrazení)**.** *Buď $f\colon U \to V$ lineární zobrazení. Pak následující jsou ekvivalentní:*

(1) f je prosté,

(2) $\operatorname{Ker}(f) = \{o\}$,

(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 $o \in \operatorname{Ker}(f)$. Ale vzhledem k tomu, že f je prosté zobrazení, tak jádro už jiný prvek neobsahuje.
- Implikace „(2) ⇒ (3)“. Buďte $x_1, \dots, x_n \in U$ 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 $\operatorname{Ker}(f) = \{o\}$. Tudíž musí $\sum_{i=1}^n \alpha_i x_i = o$ a z lineární nezávislosti vektorů máme $\alpha_i = 0$ pro všechna 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 (3) také lineárně závislá množina, a tudíž $x - y = o$, neboli $x = y$. To je spor. □

U vektorových prostorů víme, že je každý (konečně generovaný) podprostor 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. Pak $x = \sum_{i=1}^{n} \alpha_i x_i$ pro nějaké skaláry $\alpha_1, \ldots, \alpha_n \in \mathbb{T}$. Definujme 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 často pohodlnější.

Definice 6.10 (Matice lineárního zobrazení)**.** Buď $f\colon U \to V$ 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 ${}_{B_2}[f]_{B_1}$.

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

Příklad 6.11 (Matice lineárního zobrazení)**.** Uvažujme lineární zobrazení $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ s předpisem $f(x) = Ax$, kde

$$A = \begin{pmatrix} 1 & 2 \\ 3 & -4 \end{pmatrix}.$$

Zvolme báze $B_1 = \{(1,2)^T, (2,1)^T\}$, $B_2 = \{(1,-1)^T, (0,1)^T\}$ a najděme matici zobrazení f vzhledem k bázím B_1, B_2.

Obraz prvního vektoru báze B_1 je $f(1,2) = (5,-5)^T$, a jeho souřadnice vzhledem k bázi B_2 jsou $[f(1,2)]_{B_2} = (5,0)^T$. Podobně, obraz druhého vektoru báze B_1 je $f(2,1) = (4,2)^T$, a jeho souřadnice vzhledem k bázi B_2 jsou $[f(2,1)]_{B_2} = (4,6)^T$. Tudíž

$${}_{B_2}[f]_{B_1} = \begin{pmatrix} 5 & 4 \\ 0 & 6 \end{pmatrix}.$$ □

K čemu je matice lineárního zobrazení užitečná říká následující věta.

Věta 6.12 (Maticová reprezentace lineárního zobrazení)**.** *Buď $f\colon U \to V$ lineární zobrazení, $B_1 = \{x_1, \dots, x_n\}$ báze prostoru U, a $B_2 = \{y_1, \dots, y_m\}$ báze prostoru V. Pak pro každé $x \in U$ je*

$$[f(x)]_{B_2} = {}_{B_2}[f]_{B_1}\,[x]_{B_1}. \tag{6.1}$$

Důkaz. Označme $A \coloneqq {}_{B_2}[f]_{B_1}$. Buď $x \in U$, tedy $x = \sum_{i=1}^{n} \alpha_i x_i$, neboli $[x]_{B_1} = (\alpha_1, \dots, \alpha_n)^T$. Pak

$$\begin{aligned} f(x) &= f\Big(\sum_{j=1}^{n} \alpha_j x_j\Big) = \sum_{j=1}^{n} \alpha_j f(x_j) = \sum_{j=1}^{n} \alpha_j \Big(\sum_{i=1}^{m} a_{ij} y_i\Big) \\ &= \sum_{j=1}^{n}\sum_{i=1}^{m} \alpha_j a_{ij} y_i = \sum_{i=1}^{m} \Big(\sum_{j=1}^{n} \alpha_j a_{ij}\Big) y_i. \end{aligned}$$

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.

Připomeňme, že symbol kan značí kanonickou bázi, tj. tu skládající se z jednotkových vektorů.

Důsledek 6.13. *Každé lineární zobrazení $f\colon \mathbb{R}^n \to \mathbb{R}^m$ 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 $f\colon U \to V$ a báze B_1, B_2 prostorů. Víme, že matice $A = {}_{B_2}[f]_{B_1}$ splňuje

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

Ukážeme, že žádná jiná matice tuto vlastnost nemá.

Věta 6.14 (Jednoznačnost matice lineárního zobrazení)**.** *Buď $f\colon U \to V$ 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 sestává z vektorů $x_1, \dots, x_n$. 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 5.23). □

Poznámka 6.15. Nejen že každé linerní zobrazení jde representovat maticově, ale i naopak každá matice představuje matici nějakého lineárního zobrazení. Buďte B_1, B_2 báze prostorů U, V dimenzí n, m a mějme $A \in \mathbb{T}^{m\times n}$. Pak existuje jediné lineární zobrazení $f\colon U \to V$ takové, že $A = {}_{B_2}[f]_{B_1}$; ve sloupcích matice A vyčteme souřadnice obrazů vektorů báze B_1, což plně určuje zobrazení f dle Věty 6.9.

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

Definice 6.16 (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 6.17. 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

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

Důležitou roli v teorii lineárních zobrazení hraje jejich vzájemné skládání. Připomeňme, že pro zobrazení $f\colon U \to V$ a $g\colon V \to W$ je složené zobrazení $g \circ f$ je definované předpisem $(g \circ f)(x) \coloneqq g(f(x))$, $x \in U$.

Tvrzení 6.18 (Složené lineární zobrazení)**.** *Buďte $f\colon U \to V$, $g\colon V \to W$ lineární zobrazení. Pak složené zobrazení $g \circ f$ je zase lineární zobrazení.*

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

$$\begin{aligned} (g \circ f)(x+y) &= g(f(x+y)) = g(f(x)+f(y)) \\ &= g(f(x)) + g(f(y)) = (g \circ f)(x) + (g \circ f)(y), \\ (g \circ f)(\alpha x) &= g(f(\alpha x)) = g(\alpha f(x)) = \alpha g(f(x)) = \alpha (g \circ f)(x). \end{aligned}$$ $\square$

Věta 6.19 (Matice složeného lineárního zobrazení)**.** *Buďte $f\colon U \to V$ a $g\colon V \to W$ 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 6.14) je ${}_{B_3}[g]_{B_2}\ {}_{B_2}[f]_{B_1}$ hledaná matice složeného zobrazení. $\square$

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

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

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:

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

Příklad 6.21 (Otočení v $\mathbb{R}^n$)**.** Matici otočení z předchozího příkladu jednoduše zobecníme na matici otočení o úhel α v rovině os x_i, x_j. Schematicky (prázdné místo odpovídá nulám):

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

S touto maticí se setkáme ještě později v Příkladu 8.44. □

Příklad 6.22. Nechť máme dánu matici lineárního zobrazení f vzhledem k bázím B_1, B_2, tj. ${}_{B_2}[f]_{B_1}$. Jak určit matici vzhledem k bázím B_3, B_4, tj. ${}_{B_4}[f]_{B_3}$? Podle věty o matici složeného zobrazení aplikované na $f = id \circ f \circ id$ a příslušné báze máme

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

Tedy veškerou práci vykonají matice přechodu mezi bázemi. □

Příklad 6.23 (Mnemotechnika počítání matic přechodu)**.** Pro počítání matice přechodu v $\mathbb{R}^n$ od báze B_1 do báze B_2, tj. ${}_{B_2}[id]_{B_1}$, lze použít následující mnemotechniku:

$$(B_2 \mid B_1) \overset{RREF}{\sim} (I_n \mid {}_{B_2}[id]_{B_1})\,.$$

První matice ve sloupcích obsahuje bázi B_2 a pak bázi B_1, což jou vlastně matice ${}_{\text{kan}}[id]_{B_2}$ a ${}_{\text{kan}}[id]_{B_1}$. Převedením na RREF tvar dostaneme napravo hledanou matici přechodu. Důvod pramení ze vztahu ${}_{B_2}[id]_{B_1} = {}_{\text{kan}}[id]_{B_2}^{-1}\ {}_{\text{kan}}[id]_{B_1}$.

Konkrétně, pro Příklad 6.17, dostaneme

$$\left(\begin{array}{ccc|ccc} 8 & -8 & 3 & 1 & 3 & 2 \\ -4 & 5 & -2 & 1 & -2 & -1 \\ 1 & -2 & 1 & -1 & 0 & 1 \end{array}\right) \overset{RREF}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & -1 & 1 \\ 0 & 1 & 0 & 3 & -4 & 3 \\ 0 & 0 & 1 & 3 & -7 & 6 \end{array}\right).$$ □

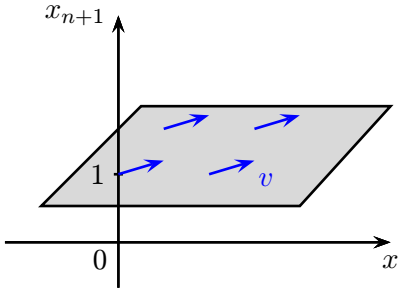
Příklad 6.24 (Posunutí jako lineární zobrazení?)**.** Buď $v \in \mathbb{R}^n$ pevné a uvažujme zobrazení $f\colon \mathbb{R}^n \to \mathbb{R}^n$ dané předpisem $f(x) = x + v$. Toto zobrazení není lineární! Nicméně můžeme ho jako lineární simulovat. Vnoříme se do prostoru o jednu dimenzi většího tak, aby pro určité lineární zobrazení $g\colon \mathbb{R}^{n+1} \to \mathbb{R}^{n+1}$ platilo

$$g(x_1, \ldots, x_n, 1) = (x_1 + v_1, \ldots, x_n + v_n, 1).$$

Dodefinujeme g pro ostatní body tak, aby tvořilo lineární zobrazení

$$g(x_1, \ldots, x_n, x_{n+1}) = (x_1 + v_1 x_{n+1}, \ldots, x_n + v_n x_{n+1}, x_{n+1}).$$

Ilustrace vnoření:



Matice zobrazení:

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & v_1 \\ 0 & 1 & \ldots & 0 & v_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \ldots & 1 & v_n \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

□

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

6.2 Isomorfismus

Definice 6.25 (Isomorfismus)**.** *Isomorfismus* mezi prostory U, V je vzájemně jednoznačné lineární zobrazení $f\colon U \to V$. Pokud mezi prostory U, V existuje isomorfismus, pak říkáme, že U, V jsou *isomorfní.*

Příklad 6.26. Příkladem isomorfismu je třeba škálování, překlápění v $\mathbb{R}^2$ (Příklad 6.3) nebo otáčení (Příklad 6.20). Příkladem lineárního zobrazení, které není isomorfismem, 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 $a_n x^n + \ldots + a_1 x + a_0 \mapsto (a_0, a_1, \ldots, a_n, 0, \ldots)$. □

Tvrzení 6.27 (Vlastnosti isomorfismu)**.**

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

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

(3) Je-li $f\colon U \to V$ isomorfismus, pak libovolná báze prostoru U se zobrazuje na bázi prostoru V.

(4) Je-li $f\colon U \to V$ isomorfismus, pak $\dim U = \dim V$.

Důkaz.

(1) Zobrazení f je vzájemně jednoznačné, tedy f^{-1} existuje a je také vzájemně jednoznačné. 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.

(3) Buď $x_1, \ldots, x_n$ báze U. Protože f je prosté, dle Věty 6.8(3) jsou $f(x_1), \ldots, f(x_n)$ lineárně nezávislé. Protože f je na, generují vektory $f(x_1), \ldots, f(x_n)$ dle Věty 6.7(3) prostor $f(U) = V$. Tedy $f(x_1), \ldots, f(x_n)$ tvoří bázi V.

(4) Plyne z předchozího bodu. □

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

Důsledek 6.28. *Buď $f\colon U \to V$ 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

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

Jelikož ${}_{B_2}[f]_{B_1}$ je podle Věty 6.27(4) čtvercová, je ${}_{B_1}[f^{-1}]_{B_2}$ její inverzní matice. □

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

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

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. Již víme z Věty 6.27(4), že isomorfní prostory mají stejnou dimenzi. Platí to i naopak?

Tvrzení 6.29. *Buď V vektorový prostor nad tělesem $\mathbb{T}$ dimenze n s bází B. Pak zobrazení $x \mapsto [x]_B$ je isomorfismus mezi prostory V a $\mathbb{T}^n$ nad $\mathbb{T}$.*

Důkaz. Nechť báze B sestává 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 z jednoznačnosti souřadnic, Věta 5.23. 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

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

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

Věta 6.30 (Isomorfismus n-dimenzionálních prostorů)**.** *Všechny n-dimenzionální vektorové prostory nad tělesem $\mathbb{T}$ jsou navzájem isomorfní.*

Důkaz. Podle Tvrzení 6.29 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 složení 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 $\mathbb{T}^n$ nad $\mathbb{T}$, kde se pracuje mnohem lépe.

Příklad 6.31 (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 $f\colon \mathbb{R}^n \to \mathbb{R}^m$ definované předpisem $f(x) = Ax$ platí $\operatorname{Ker}(f) = \operatorname{Ker}(A)$ 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 6.32 (O dimenzi jádra a obrazu)**.** *Buď $f\colon U \to V$ lineární zobrazení, U, V prostory nad $\mathbb{T}$,* $\dim U = n$, $\dim V = m$, *B_1 báze prostoru U a B_2 báze prostoru V. Označme $A = {}_{B_2}[f]_{B_1}$. Pak:*

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

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

Důkaz. (1) Podle Věty 6.27(4) stačí sestrojit isomorfismus mezi prostory $\operatorname{Ker}(f)$ a $\operatorname{Ker}(A)$. Isomorfismem může být např. zobrazení $x \in \operatorname{Ker}(f) \mapsto [x]_{B_1}$. Z Tvrzení 6.29 víme, že je lineární a prosté. Zbývá ukázat, že $[x]_{B_1} \in \operatorname{Ker}(A)$ a že zobrazení je „na“. Buď $x \in \operatorname{Ker}(f)$, pak

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

tedy $[x]_{B_1}$ náleží do jádra matice A. A naopak, pro každé $[x]_{B_1} \in \operatorname{Ker}(A)$ 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 $y \coloneqq f(x) \in f(U)$ splňuje $[y]_{B_2} \in \mathcal{S}(A)$. □

Poznámka 6.33. Důkaz Věty 6.32 je konstruktivní – říká nejen jak spočítat dimenzi jádra a obrazu f, ale také jak najít jejich báze. Je-li $x_1, \ldots, x_k$ báze $\operatorname{Ker}(A)$, pak tyto vektory tvoří souřadnice (vzhledem k bázi B_1) báze $\operatorname{Ker}(f)$. Podobně, je-li $y_1, \ldots, y_r$ báze $\mathcal{S}(A)$, pak tyto vektory představují souřadnice báze $f(U)$ vzhledem k B_2.

Důsledek 6.34. *Buď $f\colon U \to V$ lineární zobrazení, pak* $\dim U = \dim \operatorname{Ker}(f) + \dim f(U)$.

Důkaz. Podle Věty 5.51 platí pro matici A typu $m \times n$ rovnost $n = \dim \operatorname{Ker}(A) + \operatorname{rank}(A)$. Speciálně, pro $A = {}_{B_2}[f]_{B_1}$ dostáváme hledanou identitu, neboť $n = \dim U$, $\dim \operatorname{Ker}(f) = \dim \operatorname{Ker}(A)$ a $\dim f(U) = \operatorname{rank}(A)$. □

Příklad 6.35. Mějme lineární zobrazení $f\colon \mathbb{R}^3 \to \mathcal{P}^2$ dané

$${}_{B_2}[f]_{B_1} = A = \begin{pmatrix} 1 & 1 & 1 \\ 3 & 2 & 0 \\ 0 & 1 & 3 \end{pmatrix},$$

kde

$$B_1 = \{(1,2,1)^T,\ (0,1,1)^T,\ (1,2,4)^T\},$$
$$B_2 = \{x^2 - 2x + 3,\ x - 1,\ 2x^2 + x\}.$$

- Jelikož $\operatorname{rank}(A) = 2$, dostáváme ihned $\dim \operatorname{Ker}(f) = 3 - \operatorname{rank}(A) = 1$ a $\dim f(\mathbb{R}^3) = \operatorname{rank}(A) = 2$.
- Báze $\operatorname{Ker}(A)$ je $(2,-3,1)^T$, tedy báze $\operatorname{Ker}(f)$ je

$$2(1,2,1)^T - 3(0,1,1)^T + 1(1,2,4)^T = (3,3,3)^T.$$

- Báze $\mathcal{S}(A)$ je $(1,3,0)^T$, $(1,2,1)^T$, tedy báze $f(\mathbb{R}^3)$ je

$$1(x^2 - 2x + 3) + 3(x - 1) + 0(2x^2 + x) = x^2 + x,$$
$$1(x^2 - 2x + 3) + 2(x - 1) + 1(2x^2 + x) = 3x^2 + x + 1.$$ □

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 $V = \mathbb{T}$.

Definice 6.36. 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 $f_i(v_j) = 0$ pro $i \neq j$. Tato báze se nazývá duální k bázi $v_1, \ldots, v_n$.

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 obecně není. Nicméně vždy existuje kanonické vnoření V do V^{**}. Pokud navíc platí, že V a V^{**} jsou isomorfní, tak V má určité pěkné vlastnosti.

Další podrobnosti odkrývá obor zvaný funkcionální analýza. I když se matematika za tím může zdát hodně náročná, pomáhá řešit tak složité problémy jako je nalezení rovnovážné pozice membrány vychýlené nějakou překážkou, problémy ve zpracování a analýze signálů či obrázků, ve strojovém učení, nemluvě o fyzikálních problémech (třeba kvantové mechaniky) a mnoha jiných.

Problémy

6.1. Uvažujme lineární zobrazení $x \mapsto Dx$, kde $D \in \mathbb{R}^{n\times n}$ je regulární. Buď $A \in \mathbb{R}^{m\times n}$ a $b \in \mathbb{R}^m$.

(a) Co je obrazem množiny $\{x \in \mathbb{R}^n;\ Ax = b\}$?

(b) Co se zobrazí na množinu $\{x \in \mathbb{R}^n;\ Ax = b\}$?

Jak se změní předchozí výsledky když D nebude regulární?

6.2. Dokažte, že lineární zobrazení $f\colon U \to V$ je

(a) prosté právě tehdy, když existuje lineární zobrazení $g\colon V \to U$ takové, že $g \circ f = id$ (na U).

(b) „na“ právě tehdy, když existuje lineární zobrazení $g\colon V \to U$ takové, že $f \circ g = id$ (na V).

Kapitola 7

Afinní podprostory

Toto je velmi letmý úvod do afinních podprostorů. Podrobněji o afinních prostorech pojednává například Bican [2009].

Vektorové prostory a podprostory jsou omezeny tím, že musí obsahovat nulový vektor. Motivací pro afinní podprostory 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

Afinní podprostor je možno definovat axiomaticky podobně jako vektorový prostor, ale pro naše účely se omezíme na speciální typ.

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

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

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

Afinní podprostor (používá se i pojem afinní prostor či afinní množina se stejným významem) je tedy jakýkoli podprostor U „posunutý“ nějakým vektorem a.

Protože $o \in U$, je $a \in M$. Tento representant a není jednoznačný, můžeme zvolit libovolný vektor z M. Naopak, U je u každého afinního podprostoru určený jednoznačně (Problém 7.1.).

Příklad 7.2. Buď V vektorový prostor. Každý jeho vektorový podprostor U je zároveň jeho afinním podprostorem, neboť lze volit $a = o$, čímž $U = U + o$ je tvaru afinního podprostoru.

Dále, pro každý vektor $a \in V$ je množina $\{a\}$ jednoprvkový afinní podprostor ve V. Ten dostaneme volbou $U \coloneqq \{o\}$, protože potom $U + a = \{a\}$. □

Nad tělesem reálných čísel můžeme afinní podprostory charakterizovat i jinak.

Věta 7.3 (Charakterizace afinního podprostoru)**.** *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 $\alpha \in \mathbb{T}$ platí $\alpha x + (1 - \alpha)y \in M$.*

Poznámka. Ještě před důkazem poznamenejme, že výraz $\alpha x + (1 - \alpha)y$ se nazývá *afinní kombinace* a afinní podprostor ve V musí být tedy uzavřený 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 „⇒“. 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 „⇐“. Ukážeme, že stačí zvolit $a \in M$ libovolně pevně a $U \coloneqq M - M = \{x - y;\, x, y \in M\}$. Tedy ukážeme, že $M = (M - M) + a$.

„⊆“: 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 vzít za příklad prostor $\mathbb{Z}_2^n$ nad $\mathbb{Z}_2$, v němž je každá množina vektorů uzavřená na afinní kombinace.

Věta 7.4. *Množina řešení soustavy rovnic $Ax = b$ je prázdná nebo afinní. Je-li neprázdná, můžeme tuto množinu řešení 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 podprostor lze popsat pomocí soustavy rovnic (v souřadnicích), viz Bican [2009].

Příklad 7.5. Věta 7.4 dává následující geometrický pohled na soustavy rovnic při perturbaci pravé strany. Nechť $Ax = b$ je řešitelná, tedy popisuje afinní podprostor $\mathrm{Ker}\,(A) + x_0$. Změníme-li pravou stranu soustavy b na b', pak buďto soustava přestane mít řešení (což se nestává často), nebo se afinní podprostor posune na $\mathrm{Ker}\,(A) + x_0'$, kde x_0' je jedno vybrané řešení. Typicky se tedy množina řešení při změně pravé strany pouze posouvá nějakým směrem. □

Dimenze afinního podprostoru

Definice 7.6 (Dimenze afinního podprostoru)**.** *Dimenze* afinního podprostoru $M = U + a$ je definována jako $\dim(M) \coloneqq \dim(U)$.

Protože každý vektorový podprostor prostoru V je zároveň jeho afinním podprostorem, definice tedy zobecňuje pojem dimenze, zavedený pro vektorové prostory. Definice přirozeně zavádí dimenzi bodu jako nula, dimenzi přímky v $\mathbb{R}^n$ jako jedna a dimenzi roviny jako dva.

Také umožňuje definovat *přímku* p v libovolném vektorovém prostoru W nad $\mathbb{T}$ jakožto afinní množinu dimenze jedna. Jinými slovy, $p = \mathrm{span}(v) + a$, 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.

Příklad 7.7. Množina $\{e^x + \alpha \sin x;\ \alpha \in \mathbb{R}\}$ je přímka v prostoru funkcí $\mathcal{F}$. □

Příklad 7.8. Pro jakékoli $a \in \mathbb{R}^n \setminus \{o\}$ a $b \in \mathbb{R}$ je množina popsaná rovnicí $a^T x = b$ nadrovinou v $\mathbb{R}^n$. □

Afinní nezávislost

Definice 7.9 (Afinní nezávislost)**.** Vektory $x_0, x_1, \ldots, x_n$ vektorového prostoru jsou *afinně nezávislé*, pokud $x_1 - x_0, \ldots, x_n - x_0$ jsou lineárně nezávislé.

Afinní nezávislost u afinních podprostorů odpovídá tomu, čemu odpovídala lineární nezávislost u vektorových prostorů. Navíc umožňuje jednoduše formalizovat to, co známe pod pojmem „Mějme body v obecné poloze“: Množina bodů $x_1, \ldots, x_m \in \mathbb{R}^n$ je v obecné poloze, když každá její podmnožina velikosti nanejvýš $n + 1$ je afinně nezávislá. Tedy například v rovině $\mathbb{R}^2$ jsou dané body v obecné poloze pokud žádné tři neleží na společné přímce.

Příklad 7.10. Vektory $(1,1)^T, (2,2)^T, (1,2)^T \in \mathbb{R}^2$ jsou sice lineárně závislé, ale afinně nezávislé. □

Souřadnice v afinním podprostoru

Buď $M = U + a$ afinní podprostor a $B = \{v_1, \dots, v_n\}$ báze U. Pak každé $x \in M$ se dá jednoznačně zapsat ve tvaru $x = a + \sum_{i=1}^{n} \alpha_i v_i$. Tedy $S = \{a, v_1, \dots, v_n\}$ lze považovat za *souřadný systém* a vektor $[x]_S \coloneqq [x - a]_B = (\alpha_1, \dots, \alpha_n)^T$ za příslušné *souřadnice*.

K přechodu mezi souřadnými systémy pak můžeme použít naši známou matici přechodu přesně tak, jak jsme zvyklí. V případě, že měníme i vektor a, objeví se i konstantní aditivní člen.

Tvrzení 7.11. *Buď $M = U + a$ afinní podprostor a $B = \{v_1, \dots, v_n\}$, $B' = \{v'_1, \dots, v'_n\}$ dvě báze U.*

(1) Pro souřadné systémy $S = \{a, v_1, \dots, v_n\}$ a $S' = \{a, v'_1, \dots, v'_n\}$ máme

$$[x]_{S'} = {}_{B'}[id]_B \, [x]_S, \quad \forall x \in U + a.$$

(2) Pro souřadné systémy $S = \{a, v_1, \dots, v_n\}$ a $S' = \{a', v'_1, \dots, v'_n\}$ máme

$$[x]_{S'} = [a - a']_{B'} + {}_{B'}[id]_B \, [x]_S, \quad \forall x \in U + a.$$

Důkaz.

(1) Nechť $x \in U + a$ je tvaru $x = u + a$. Pak

$$[x]_{S'} = [u]_{B'} = {}_{B'}[id]_B \, [u]_B = {}_{B'}[id]_B \, [x]_S.$$

(2) Nechť $x \in U + a$ je tvaru $x = u + a$, tj. $x = (a - a') + u + a'$. Pak

$$[x]_{S'} = [(a - a') + u]_{B'} = [(a - a')]_{B'} + [u]_{B'} = [(a - a')]_{B'} + {}_{B'}[id]_B \, [x]_S. \qquad \square$$

Vztah afinních podprostorů

Afinní podprostory $U + a$ a $W + b$ jsou *rovnoběžné*, pokud $U \Subset W$ nebo $W \Subset U$; *různoběžné*, pokud nejsou rovnoběžné a mají neprázdný průnik; a *mimoběžné*, pokud nejsou rovnoběžné a mají prázdný průnik.

Příklad 7.12. Buď v libovolný vektor vektorového prostoru V. Pak afinní podprostor $\{v\}$ je rovnoběžný s každým afinním podprostorem V. Stejnou vlastnost má i celý prostor V. $\square$

Afinní zobrazení

Buď $f \colon U \to V$ lineární zobrazení a mějme pevné vektory $a \in U$, $b \in V$. Potom *afinní zobrazení* má tvar $F(u + a) = f(u) + b$. Jednoduchým příkladem afinního zobrazení je posunutí, tedy zobrazení $f \colon V \to V$ s popisem $f(x) = x + b$, kde $b \in V$ je pevné.

Afinní zobrazení nemusí zobrazovat o na o, protože jsou obrazy posunuté o aditivní člen b.

Příklad 7.13. Buď $U + a$ afinní podprostor dimenze k v prostoru V, a buď S souřadný systém v $U + a$. Pak zobrazení $f(v) = [v]_S$ je afinní zobrazení zobrazující isomorfně $U + a$ na $\mathbb{T}^k$. $\square$

Snadno se nahlédne následující pozorování, necháme je čtenáři na rozmyšlení.

Tvrzení 7.14.

(1) Obraz afinního podprostoru při afinním zobrazení je afinní podprostor.

(2) Složením dvou afinních zobrazení dostaneme opět afinní zobrazení.

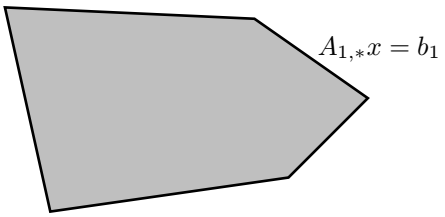
(3) Buď $f \colon U \to V$ lineární zobrazení a $v \in V$. Pak úplný vzor vektoru v

$$f^{-1}(v) \coloneqq \{u \in U;\, f(u) = v\}$$

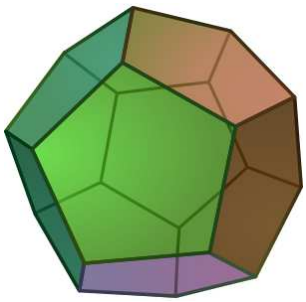
je afinní podprostor v U.

Poznámka 7.15 (Rovnice ano, ale nerovnice?)**.** V minulých kapitolách jsme studovali jsme soustavy lineárních rovnic $Ax = b$, tudíž je přirozená otázka zabývat se i soustavou nerovnic $Ax \leq b$. Nerovnost mezi vektory znamená nerovnost v každé složce, tedy $(Ax)_i \leq b_i$ pro všechna i. Dále, omezíme se jen na těleso $\mathbb{R}$, kde máme definováno uspořádání.

Zatímco jedna rovnice vytyčuje v prostoru nadrovinu a soustava rovnic pak nějaký afinní podprostor, tak jedna nerovnice vymezuje v prostoru poloprostor a soustava nerovnic pak tudíž průnik poloprostorů, což je *konvexní polyedr (mnohostěn)*.



Příklad v $\mathbb{R}^2$.



Příklad v $\mathbb{R}^3$.

Konvexními polyedry se více zabývá např. obor *lineární programování*. Ten zkoumá nejen konvexní polyedry, ale také nad nimi řeší optimalizační úlohy typu

$$\min c^T x \text{ za podmínek } Ax \leq b,$$

kde $c \in \mathbb{R}^n$, $A \in \mathbb{R}^{m \times n}$ a $b \in \mathbb{R}^m$ jsou dané a $x \in \mathbb{R}^n$ je vektor proměnných.

7.2 Aplikace

Fraktály

Fraktál je soběpodobný geometrický útvar na první pohled složitého tvaru. Ukážeme si na příkladu, že i poměrně složitý fraktál může mít jednoduchý popis pomocí afinních zobrazení.

Příklad 7.16 (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.

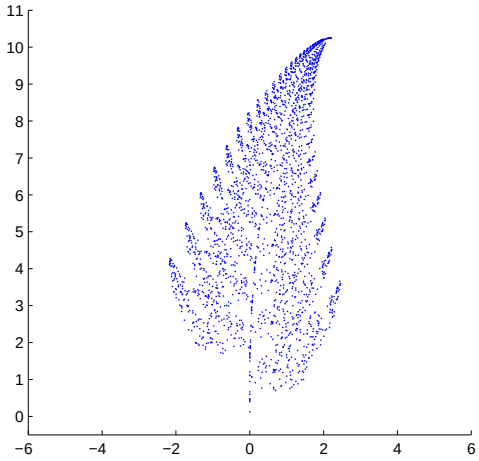
$$T_1(x,y) = \begin{pmatrix} 0.86 & 0.03 \\ -0.03 & 0.86 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 1.5 \end{pmatrix} \quad \text{s pravděpodobností } 0.83$$

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

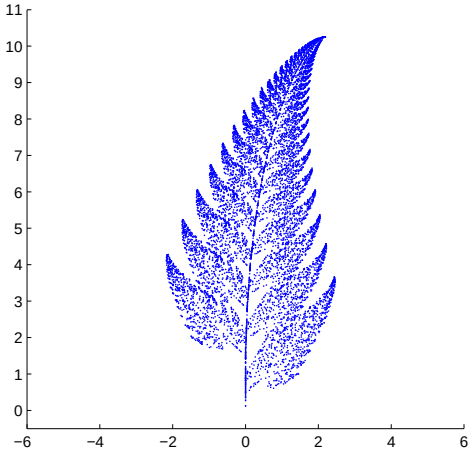
$$T_3(x,y) = \begin{pmatrix} -0.15 & 0.27 \\ 0.25 & 0.26 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 0.45 \end{pmatrix} \quad \text{s pravděpodobností } 0.08$$

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

Navštívené body postupně vykreslí fraktál ve tvaru listu kapradiny.



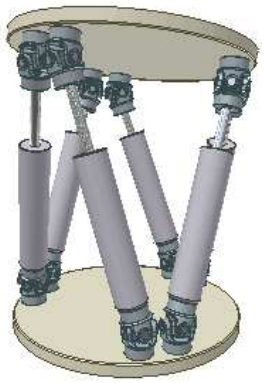
2500 iterací.



10000 iterací. □

Stewartova–Goughova platforma v robotice

Stewartova–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 manipulátory, v simulacích (např. letů), nebo třeba v biomechanice kloubů k ověřování implantátů mimo lidské tělo.



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

Základna i mobilní plošina mají své vlastní souřadné systémy, mezi kterými můžeme přecházet pomocí afinního zobrazení. Např., jsou-li $x = (x_1, x_2, x_3)^T$ 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. Pochopitelně, P a c nejsou pevné, ale závisí na míře natažení pohyblivých ramen. 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.).

Uvažujme problém určení délek pohyblivých ramen. Označme $x^{(1)}, \ldots, x^{(6)}$ koncové body ramen u základny v souřadném systému základny a $y^{(1)}, \ldots, y^{(6)}$ koncové body na plošině v souřadném systému plošiny. Ty druhé převedeme výše zmíněnou transformací do souřadného systému základny: $y'^{(1)} = Px^{(1)} + c, \ldots, y'^{(6)} = Px^{(6)} + c$. Nyní můžeme jednoduše spočítat délku ramen jako vzdálenosti bodů $x^{(i)}$ a $y'^{(i)}$ pro $i = 1, \ldots, 6$.

Typicky ale problém zní 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.

Problémy

7.1. Buď $M = U + a$ afinní podprostor. Dokažte, že prostor U je dán jednoznačně.

7.2. Ukažte, že průnik afinních podprostorů je zase afinní podprostor nebo prázdná množina.

7.3. Buďte afinní podprostory $U + a$ a $W + b$ rovnoběžné. Ukažte, že pak jsou disjunktní právě tehdy, když $a - b \notin U \cup W$.

7.4. (Analogie vět o isomorfismu vektorových prostorů.) Ukažte, že afinní prostory $U + a$, $W + b$ mají stejnou dimenzi právě tehdy, když existuje prosté afinní zobrazení $U + a$ na $W + b$.

Kapitola 8

Skalární součin

Vektorové prostory byly definovány velice obecně, takže pokryjí velkou třídu problémů. Na druhou stanu, jestliže přidáme další požadavky na to co mají prostory splňovat, tak budeme moci odvodit hlubší výsledky. Konkrétně, skalární součin dává 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.

Definice 8.1 (Skalární součin nad $\mathbb{R}$)**.** Buď V vektorový prostor nad $\mathbb{R}$. Pak *skalární součin* je binární operace $\langle\cdot,\cdot\rangle\colon V^2 \to \mathbb{R}$, 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) $\langle x, y\rangle = \langle y, x\rangle\ \forall x, y \in V$.

Zobecnění na těleso komplexních čísel je následující. Připomeňme ještě, že komplexně sdružené číslo k $a + bi \in \mathbb{C}$ je definované jako $\overline{a + bi} = a - bi$.

Definice 8.2 (Skalární součin nad $\mathbb{C}$)**.** Buď V vektorový prostor nad $\mathbb{C}$. Pak *skalární součin* je binární operace $\langle\cdot,\cdot\rangle\colon V^2 \to \mathbb{C}$, 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) $\langle x, y\rangle = \overline{\langle y, x\rangle}\ \forall x, y \in V$.

Kvůli vlastnosti (1), kde je potřeba uspořádání, zavádíme skalární součin pouze nad tělesy $\mathbb{R}$ a $\mathbb{C}$.

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 jej porovnávat s nulou u první vlastnosti.

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

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

Ve druhé složce tedy komplexní skalární součin není lineární (je pouze tzv. seskvilineární).

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

Příklad 8.3 (Příklady standardních 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. Později, ve Větě 11.17, popíšeme všechny skalární součiny v prostoru $\mathbb{R}^n$.

□

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

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

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 $\langle x, y\rangle = \|x\| \cdot \|y\| \cos(\varphi)$, kde φ je úhel mezi vektory x, y. Speciálně, x, y jsou kolmé 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 $x, y \in V$ 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 $x, y \in V$ 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 (Problém 8.2.).

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

Důkaz. (Reálná verze) Nejprve ukážeme reálnou verzi, protože má elegantní důkaz. Pro $y = o$ platí nerovnost triviálně, tak předpokládejme $y \neq o$. Uvažujme reálnou funkci $f(t) = \langle x + ty, x + ty\rangle \geq 0$ 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:

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

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

Důkaz. (Komplexní verze) Je-li $\langle x, y\rangle = 0$, pak tvrzení platí triviálně. Budeme tedy předpokládat, že $\langle x, y\rangle \neq 0$, a zavedeme vektor

$$z \coloneqq \frac{\langle y, y\rangle}{\langle x, y\rangle} x - y.$$

[1] Nerovnost se také někdy nazývá jen Schwarzova, nebo Cauchyho–Bunjakovského, popř. Cauchyho–Schwarzova–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).

Potom platí

$$\langle z, y\rangle = \Big\langle \frac{\langle y,y\rangle}{\langle x,y\rangle}x - y, y\Big\rangle = \frac{\langle y,y\rangle}{\langle x,y\rangle}\langle x,y\rangle - \langle y,y\rangle = 0.$$

Vektory z, y jsou tudíž na sebe kolmé a podle Pythagorovy věty

$$\|z+y\|^2 = \|z\|^2 + \|y\|^2,$$

neboli

$$\frac{\langle y,y\rangle^2}{|\langle x,y\rangle|^2}\|x\|^2 = \|z\|^2 + \|y\|^2 \geq \|y\|^2.$$

Zkrácením $\|y\|^2$ a vynásobením $|\langle x,y\rangle|^2$ dostaneme hledanou nerovnost $\|x\|^2\|y\|^2 \geq |\langle x,y\rangle|^2$ v druhých mocninách. □

Občas se Cauchyho–Schwarzova nerovnost uvádí v ekvivalentní podobě

$$|\langle x,y\rangle|^2 \leq \langle x,x\rangle\langle y,y\rangle.$$

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

$$\Big(\sum_{i=1}^n x_i y_i\Big)^2 \leq \Big(\sum_{i=1}^n x_i^2\Big)\Big(\sum_{i=1}^n y_i^2\Big).$$

Další využití viz např. [Krisl, 2008]. My použijeme Cauchyho–Schwarzovu nerovnost hned v následujícím k odvození trojúhelníkové nerovnosti.

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

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 Cauchyho–Schwarzovy nerovnosti. 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 je pouze malou odbočkou.

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

(1) $\|x\| \geq 0$ pro všechna $x \in V$, a rovnost nastane pouze pro $x = 0$,

(2) $\|\alpha x\| = |\alpha| \cdot \|x\|$ pro všechna $x \in V$, a pro všechna $\alpha \in \mathbb{R}$ resp. $\alpha \in \mathbb{C}$,

(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 $\|x\|_\infty = \max_{i=1,\ldots,n} |x_i|$. □

Poznámka 8.13 (Rovnoběžníkové pravidlo)**.** Pro normu indukovanou skalárním součinem platí tzv. *rovnoběžníkové pravidlo:*

$$\|x - y\|^2 + \|x + y\|^2 = 2\|x\|^2 + 2\|y\|^2.$$

Důkaz. $\|x - y\|^2 + \|x + y\|^2 = \langle x - y, x - y\rangle + \langle x + y, x + y\rangle = 2\langle x, x\rangle + 2\langle y, y\rangle = 2\|x\|^2 + 2\|y\|^2$. □

Díky tomu snadno nahlédneme, že součtová a maximová norma nejsou indukované žádným skalárním součinem. Např. pro $x = (1, 0)$ a $y = (0, 1)$ nesplňují rovnoběžníkové pravidlo.

Norma umožňuje zavést vzdálenost (neboli metriku) mezi vektory x, y jako $\|x - y\|$. A pokud máme vzdálenost, můžeme zavést limity, etc. Čtenáře by již nemělo překvapit, že i metriku lze zavést axiomaticky. Navíc k definici metriky nepotřebujeme ani vektorový prostor, stačí libovolná množina.

Poznámka 8.14 (Metrika)**.** Metriku na množině M definujeme jako je zobrazení $d\colon M^2 \to \mathbb{R}$, splňující:

(1) $d(x, y) \geq 0$ pro všechna $x, y \in M$, a rovnost nastane pouze pro $x = y$,

(2) $d(x, y) = d(y, x)$ pro všechna $x, y \in M$,

(3) $d(x, z) \leq d(x, y) + d(y, z)$ pro všechna $x, y, z \in M$.

Každá norma určuje metriku předpisem $d(x, y) \coloneqq \|x - y\|$. Na druhou stranu to ale obecně neplatí. Existují prostory s metrikou, která není indukována žádnou normou, např. diskrétní metrika $d(x, y) \coloneqq \lceil \|x - y\|_2 \rceil$, nebo diskrétní metrika definovaná $d(x, y) \coloneqq 1$ pro $x \neq y$ a $d(x, y) \coloneqq 0$ pro $x = y$.

8.2 Ortonormální báze, Gramova–Schmidtova ortogonalizace

Každý vektorový prostor má bázi. U prostoru se skalárním součinem je přirozené se ptát, zda existuje báze složená z navzájem kolmých vektorů. V této sekci ukážeme, že je to pravda, že taková báze má řadu pozoruhodných vlastností a také odvodíme algoritmus na její nalezení.

Definice 8.15 (Ortogonální a ortonormální systém)**.** Systém vektorů $z_1, \ldots, z_n$ je *ortogonální*, pokud $\langle z_i, z_j\rangle = 0$ pro všechna $i \neq j$. Systém vektorů $z_1, \ldots, z_n$ je *ortonormální*, pokud je ortogonální a $\|z_i\| = 1$ pro všechna $i = 1, \ldots, n$.

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: $\|\frac{1}{\|z_i\|}z_i\| = \frac{1}{\|z_i\|}\|z_i\| = 1$.

Příklad 8.16. V $\mathbb{R}^n$ je ortonormálním systémem například kanonická báze $e_1, \ldots, e_n$. □

Věta 8.17. *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 pro každé $k = 1, \ldots, n$ platí:

$$0 = \langle o, z_k\rangle = \left\langle \sum_{i=1}^n \alpha_i z_i, z_k \right\rangle = \sum_{i=1}^n \alpha_i \langle z_i, z_k\rangle = \alpha_k \langle z_k, z_k\rangle = \alpha_k.$$ □

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

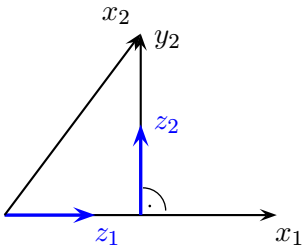
Věta 8.18 (Fourierovy koeficienty)**.** *Buď $z_1, \ldots, z_n$ ortonormální báze prostoru V. Pak pro každé $x \in V$ platí $x = \sum_{i=1}^n \langle x, z_i\rangle z_i$.*

Důkaz. Víme, že $x = \sum_{i=1}^{n} \alpha_i z_i$ a souřadnice $\alpha_1, \dots, \alpha_n$ jsou jednoznačné (Věta 5.23). Nyní pro každé $k = 1, \dots, n$ platí:

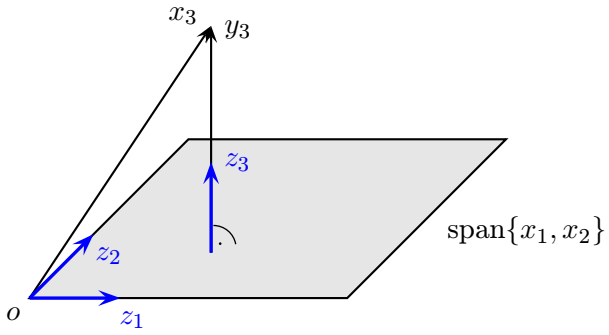
$$\langle x, z_k \rangle = \Big\langle \sum_{i=1}^{n} \alpha_i z_i, z_k \Big\rangle = \sum_{i=1}^{n} \alpha_i \langle z_i, z_k \rangle = \alpha_k \langle z_k, z_k \rangle = \alpha_k. \qquad \square$$

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*[2)].

Jak sestrojit ortonormální bázi nějakého prostoru? Následující procedura, Gramova–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 budeme pojednávat více v Sekci 8.3.



Nakolmení druhého vektoru.



Nakolmení třetího vektoru.

Algoritmus 8.19 (Gramova–Schmidtova ortogonalizace[3)])**.** Buďte $x_1, \dots, x_n \in V$ lineárně nezávislé.

1: **for** $k := 1$ **to** n **do**

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

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

4: **end for**

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

Důkaz. (Správnost Gramovy–Schmidtovy ortogonalizace.) Matematickou indukcí podle n dokážeme, že $z_1, \dots, z_n$ ortonormální báze prostoru $\mathrm{span}\{x_1, \dots, x_n\}$. Pro $n = 1$ je $y_1 = x_1 \neq o$ a $z_1 = \frac{1}{\|x_k\|} x_k$ je dobře definované a $\mathrm{span}\{x_1\} = \mathrm{span}\{z_1\}$.

Indukční krok $n \leftarrow n - 1$. Předpokládejme, že $z_1, \dots, z_{n-1}$ je ortonormální báze $\mathrm{span}\{x_1, \dots, x_{n-1}\}$. Kdyby $y_n = o$, tak $x_n = \sum_{j=1}^{n-1} \langle x_n, z_j \rangle z_j$ a $x_n \in \mathrm{span}\{z_1, \dots, z_{n-1}\} = \mathrm{span}\{x_1, \dots, x_{n-1}\}$, 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 $z_1, \dots, z_n$ je ortonormální systém. Z indukčního předpokladu je $z_1, \dots, z_{n-1}$ ortonormální systém a proto $\langle z_i, z_j \rangle$ je rovno 0 pro $i \neq j$ a rovno 1 pro $i = j$. Stačí ukázat, že z_n je kolmé na

[2)] Jean Baptiste Joseph Fourier (1768–1830), francouzský matematik a fyzik. Rozvoj použil pro řešení problému vedení tepla v pevných látkách kolem r. 1807.

[3)] 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 také P.S. Laplace (1816) nebo A.L. Cauchy (1836).

ostatní z_i, $i < n$:

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

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 5.36). □

Gramova–Schmidtova ortogonalizace má tu přednost, že je použitelná v každém prostoru se skalárním součinem. Při standardním skalárním součinu v $\mathbb{R}^n$ můžeme ortogonalizaci vyjádřit maticově (viz Poznámka 13.7), ale na druhou stranu v tomto případě existují i jiné metody, které mají lepší numerické vlastnosti; srov. Sekce 13.3.

Důsledek 8.20 (Existence ortonormální báze)**.** *Každý konečně generovaný prostor (se skalárním součinem) má ortonormální bázi.*

Důkaz. Víme (Věta 5.29), že každý konečně generovaný prostor má bázi, a tu můžeme Gramovou–Schmidtovou metodou zortogonalizovat. □

Poznamenejme, že pro nekonečně generované prostory tvrzení věty neplatí – existují prostory se skalárním součinem, které nemají ortonormální bázi; viz Bečvář [2005].

Důsledek 8.21 (Rozšíření ortonormálního systému na ortonormální bázi)**.** *Každý ortonormální systém vektorů v konečně generovaném prostoru lze rozšířit na ortonormální bázi.*

Důkaz. Víme (Věta 5.35), 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 Gramovou–Schmidtovou metodou zortogonalizovat na $z_1, \dots, z_m, z_{m+1}, \dots, z_n$. Povšimněme si, že ortogonalizací se prvních m vektorů nezmění. □

Další užitečný vztah je Besselova nerovnost a Parsevalova rovnost.

Věta 8.22. *Buď $z_1, \dots, z_n$ ortonormální systém ve V a buď $x \in V$. Pak platí:*

(1) Besselova nerovnost: $\|x\|^2 \geq \sum_{j=1}^n |\langle x, z_j\rangle|^2$,

(2) Parsevalova rovnost: $\|x\|^2 = \sum_{j=1}^n |\langle x, z_j\rangle|^2$ právě tehdy, když $x \in \operatorname{span}\{z_1, \dots, z_n\}$.

Důkaz.

(1) Vyplývá z úpravy

$$0 \leq \Big\langle x - \sum_{j=1}^n \langle x, z_j\rangle z_j, x - \sum_{j=1}^n \langle x, z_j\rangle z_j\Big\rangle =$$
$$= \langle x, x\rangle - \sum_{j=1}^n \overline{\langle x, z_j\rangle}\langle x, z_j\rangle - \sum_{j=1}^n \langle x, z_j\rangle\langle z_j, x\rangle + \sum_{j=1}^n \langle x, z_j\rangle\overline{\langle x, z_j\rangle} =$$
$$= \|x\|^2 - \sum_{j=1}^n |\langle x, z_j\rangle|^2.$$

(2) Vyplývá z předchozího, neboť rovnost nastane právě tehdy, když $x = \sum_{j=1}^n \langle x, z_j\rangle z_j$. □

Parsevalova rovnost ukazuje, že pro vektory blízké počátku musí i jejich souřadnice být dostatečně malé. Dále, rovnost se dá zobecnit i pro nekonečně generované prostory jako je $\mathcal{C}_{[-\pi,\pi]}$, což mj. znamená, že Fourierovy koeficienty v nekonečném rozvoji musí konvergovat k nule.

Parsevalova rovnost také jinými slovy říká, že v jakémkoli konečně generovaném prostoru V se norma libovolného $x \in V$ dá vyjádřit jako standardní eukleidovská norma jeho vektoru souřadnic: $\|x\| = \sqrt{[x]_B^T [x]_B}$, kde B je ortonormální báze V. Jak ukážeme dole, tato vlastnost analogicky platí i pro skalární součin: $\langle x, y\rangle = [x]_B^T [y]_B$ pro reálný a $\langle x, y\rangle = [x]_B^T \overline{[y]}_B$ pro komplexní prostor.

Tvrzení 8.23. *Buď $z_1, \dots, z_n$ ortonormální báze V a buď $x, y \in V$. Pak $\langle x, y\rangle = \sum_{j=1}^n \langle x, z_j\rangle \overline{\langle y, z_j\rangle}$.*

Důkaz. $\langle x, y\rangle = \langle \sum_{j=1}^n \langle x, z_j\rangle z_j, y\rangle = \sum_{j=1}^n \langle x, z_j\rangle \langle z_j, y\rangle = \sum_{j=1}^n \langle x, z_j\rangle \overline{\langle y, z_j\rangle}$. □

8.3 Ortogonální doplněk a projekce

Ortogonální doplněk je užitečný pojem s názornou geometrickou interpretací. Ortogonální projekce je pak navíc ohromně důležitý nátroj, jehož použití v mnoha různých oborech překonává jeho základní geometrický význam.

Definice 8.24 (Ortogonální doplněk)**.** Buď V vektorový prostor a $M \subseteq V$. Pak *ortogonální doplněk* množiny M je $M^\perp \coloneqq \{x \in V;\ \langle x, y\rangle = 0\ \forall y \in M\}$.

Příklad 8.25. Ortogonální doplněk k vektoru $(2, 5)^T$ je přímka $\operatorname{span}\{(5, -2)^T\}$.

Věta 8.26 (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 $\langle x, y\rangle = \langle x, \sum_{i=1}^n \alpha_i y_i\rangle = \sum_{i=1}^n \overline{\alpha}_i \langle x, y_i\rangle = 0$. □

Věta 8.27 (Vlastnosti ortogonálního doplňku podprostoru)**.** *Buď V vektorový prostor a $U \Subset V$. Potom platí:*

(1) Je-li $z_1, \dots, z_m$ 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 $x \in U^\perp$, 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 $x \in U^\perp$.

(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 $z_{m+1}, \ldots, z_n$ ortonormální báze $U^\perp$, tedy $z_1, \ldots, z_m$ je ortonormální báze $(U^\perp)^\perp$.

(5) Z předchozího a podle Věty 5.41 o dimenzi spojení a průniku je $\dim(U \cap U^\perp) = \dim V - \dim U - \dim U^\perp = 0$. □

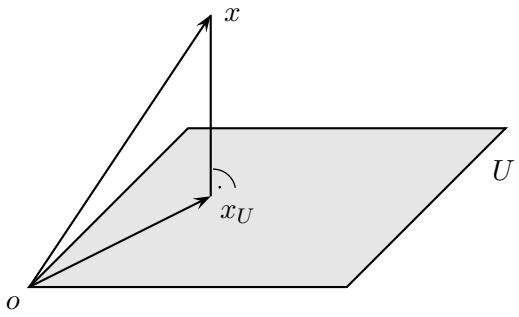
Další z pěkných vlastností ortonormálních systémů je, že umožňují jednoduše spočítat projekci x_U vektoru x do podprostoru U, což je vektor z U nejbližší k x. Následující věta opravňuje k zavedení projekce jakožto zobrazení $V \to U$ definované $x \mapsto x_U$.

Věta 8.28 (O ortogonální projekci)**.** *Buď V vektorový prostor a $U \leqslant V$. 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 $z_1, \ldots, z_m$ 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 $x_U := \sum_{i=1}^{m} \langle x, z_i\rangle z_i \in U$ 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

$$\|x - y\|^2 = \|(x - x_U) + (x_U - y)\|^2 = \|x - x_U\|^2 + \|x_U - y\|^2 \geq \|x - x_U\|^2,$$

neboli $\|x - y\| \geq \|x - x_U\|$, což dokazuje minimalitu. Abychom dokázali jednoznačnost, uvědomíme si, že rovnost nastane pouze tehdy, když $\|x_U - y\|^2 = 0$, čili když $x_U = y$. □

Poznámka 8.29. Vzhledem k vlastnostem (3) a (5) Věty 8.27 se dá prostor V vyjádřit jako direktní součet podprostorů U a $U^\perp$ (Poznámka 5.42). To mj. znamená, že každý vektor $v \in V$ má jednoznačné vyjádření $v = u + u'$, kde $u \in U$ a $u' \in U^\perp$. Podle Věty 8.28 je navíc vektor u projekcí vektoru v do U, a vektor u' projekcí v do $U^\perp$.

Příklad 8.30 (Legendreovy polynomy)**.** Uvažujme prostor polynomů $\mathcal{P}^n$. Jaký pro něj zavést skalární součin? První nápad je využít isomorfismu s $\mathbb{R}^{n+1}$ a pro polynomy $p(x) = a_n x^n + \ldots + a_0$, $q(x) = b_n x^n + \ldots + b_0$ zavést skalární součin jako

$$\langle p, q\rangle = \sum_{i=1}^{n} a_i b_i$$

a vektory $1, x, x^2, \ldots, x^n$ pak budou tvořit ortonormální systém. To je sice v pořádku, ale není to jediný možný způsob. Pokud si uvědomíme, že $\mathcal{P}^n$ je podprostorem prostoru spojitých funkcí $\mathcal{C}_{[a,b]}$, tak můžeme

na $\mathcal{P}^n$ použít standardní skalární součin prostoru $\mathcal{C}_{[a,b]}$. Pokud zortogonalizujeme Gramovou–Schmidtovou metodou vektory $1, x, x^2, \dots$ speciálně na $\mathcal{C}_{[-1,1]}$, pak dostaneme tzv. *Legendreovy polynomy*

$$p_0(x) = 1,\ p_1(x) = x,\ p_2(x) = \frac{1}{2}(3x^2-1),\ p_3(x) = \frac{1}{5}(5x^3-3x),\ \dots$$

Technické detaily výpočtu přeskočíme. Ani explicitní vyjádření není příliš jednoduché, neboť n-tý člen má tvar

$$p_n(x) = 2^{-n}\sum_{k=0}^{n}\binom{n}{k}^2 (x-1)^{n-k}(x+1)^k.$$

Tyto polynomy jsou na sebe kolmé, ale z důvodu určitých aplikací jsou znormovány tak, že n-tý má normu $2/(2n+1)$.

Legendreovy polynomy můžeme použít třeba k aproximaci funkce polynomem, srov. metodu v Sekci 3.6. Pokud funkci f chceme aproximovat polynomem n-tého stupně, tak spočítáme projekci f do podprostoru $\mathcal{P}^n$ v tomto skalárním součinu. Projekci spočítáme podle Věty 8.28 a za ortonormální bázi $\mathcal{P}^n$ použijeme Legendreovy polynomy. Výsledná projekce má třeba tu vlastnost, že ze všech polynomů stupně n je nejblíže k f v normě indukované daným skalárním součinem, což zhruba odpovídá snaze minimalizovat plochu mezi f a polynomem. Historicky byly Legendreovy polynomy poprvé použity ve fyzice k vyjádření určitých operátorů a řešení diferenciálních rovnic. □

Příklad 8.31 (Ortonormální systém v prostoru funkcí)**.** V $\mathcal{C}_{[-\pi,\pi]}$ existuje spočetný ortonormální systém $z_1, z_2, \dots$ sestávající z

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

I když to není báze v pravém slova smyslu, každou funkci $f \in \mathcal{C}_{[-\pi,\pi]}$ lze vyjádřit jako nekonečnou řadu $f(x) = \sum_{i=1}^{\infty}\langle f, z_i\rangle z_i$. Poznámka: zde trochu zjednodušujeme a odbýváme pojem nekonečného součtu, ale pro intuitivní pochopení to snad postačuje.

Vyjádření několika prvních členů $f(x) \approx \sum_{i=1}^{k}\langle f, z_i\rangle z_i$, což je vlastně projekce do prostoru $\operatorname{span}\{z_1,\dots,z_k\}$ dimenze k, dává dobrou aproximaci funkce $f(x)$. Takovéto aproximace se používá hojně v teorii zpracování signálů (např. zvuku).

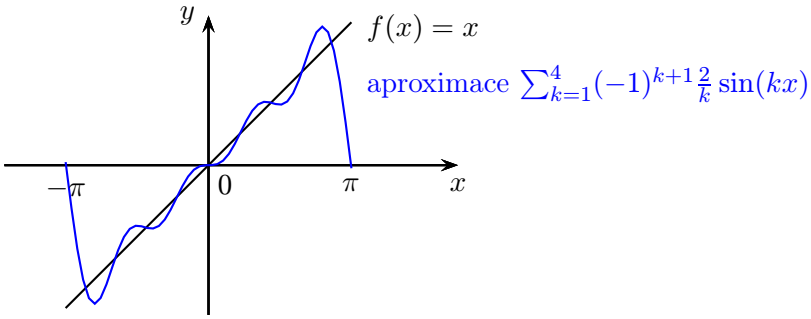
Konkrétně, spočítejme Fourierův rozvoj funkce $f(x) = x$ na intervalu $[-\pi,\pi]$

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

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



□

Je možné spočítat projekci bez nutnosti mít ortonormální bázi podprostoru? Ano, pomocí řešení soustavy s tzv. Gramovou maticí.

Věta 8.32 (Gramova matice)**.** *Buď V reálný vektorový prostor a $U \Subset V$. Nechť U má bázi $B = \{w_1, \dots, w_m\}$. Označme jako Gramovu matici $G \in \mathbb{R}^{m\times m}$ matici s prvky $G_{ij} = \langle w_i, w_j\rangle$. Pak G je regulární a vektor souřadnic s projekce x_U libovolného vektoru $x \in V$ do podprostoru U je řešením soustavy*

$$Gs = (\langle w_1, x\rangle, \dots, \langle w_m, x\rangle)^T. \tag{8.1}$$

Důkaz. Pro důkaz regularity G buď $s \in \mathbb{R}^m$ řešení soustavy $Gs = o$. Pak i-tý řádek soustavy rovnic má tvar $\langle w_i, \sum_{j=1}^m s_j w_j\rangle = 0$, čili $\sum_{j=1}^m s_j w_j \in U^\perp \cap U = \{o\}$. Z lineární nezávislosti $w_1, \dots, w_m$ nutně $s = o$.

Víme, že x_U existuje a je jednoznačná a lze psát ve tvaru $x_U = \sum_{j=1}^m \alpha_j w_j$ pro vhodné skaláry α_j. Protože $x - x_U \in U^\perp$, dostáváme speciálně $\langle w_i, x - x_U\rangle = 0$, pro všechna $i = 1, \dots, m$. Dosazením za x_U získáme $\langle w_i, x - \sum_{j=1}^m \alpha_j w_j\rangle = 0$, neboli

$$\sum_{j=1}^m \alpha_j \langle w_i, w_j\rangle = \langle w_i, x\rangle, \quad i = 1, \dots, m.$$

Tedy $s \coloneqq [x_U]_B = (\alpha_1, \dots, \alpha_m)^T$ řeší soustavu (8.1). Z regularity G pak existuje pouze jediné řešení soustavy a odpovídá dané projekci. □

8.4 Ortogonální doplněk a projekce v $\mathbb{R}^n$

Z minulé sekce víme, jak počítat ortogonální doplněk a projekci pro libovolný konečně generovaný vektorový prostor se skalárním součinem, a to pomocí ortonormální báze. Nyní 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 8.33 (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 8.26(3)) víme $\mathcal{R}(A)^\perp = \{A_{1*}, \dots, A_{m*}\}^\perp$. Tedy $x \in \mathcal{R}(A)^\perp$ právě tehdy, když x je kolmé na řádky matice A, neboli $A_{i*}x = 0$ pro všechna $i = 1, \dots, m$. Ekvivalentně, $Ax = o$, to jest $x \in \operatorname{Ker}(A)$. □

Příklad 8.34. Buď V prostor generovaný vektory $(1, 2, 3)^T$ a $(1, -1, 0)^T$. Chceme-li určit $V^\perp$, tak sestavíme matici

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & -1 & 0 \end{pmatrix},$$

protože $V = \mathcal{R}(A)$. Nyní již stačí nalézt bázi $V^\perp = \operatorname{Ker}(A)$, kterou tvoří např. vektor $(1, 1, -1)^T$. □

Charakterizace ortogonálního doplňku má i teoretické důsledky, např. vztah matice A a matice A^TA. Pozor, pro sloupcové prostory analogie neplatí!

Důsledek 8.35. *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, pro kterou odvodíme explicitní vzorec.

Věta 8.36 (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 8.35(3)), tedy je regulární a má inverzi. Dále, $x' \in \mathcal{S}(A)$, neboť $x' = Az$ pro $z = (A^TA)^{-1}A^Tx$.

Nyní ukážeme, že $x - x' \in \mathcal{S}(A)^\perp$. Protože $\mathcal{S}(A)^\perp = \mathcal{R}(A^T)^\perp = \mathrm{Ker}\,(A^T)$, 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 8.28 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 $m = n$.

Věta 8.37 (Ortogonální projekce do doplňku)**.** *Buď $P \in \mathbb{R}^{n\times n}$ matice projekce do podprostoru $V \leqslant \mathbb{R}^n$. Pak $I - P$ je maticí projekce do $V^\perp$.*

Důkaz. Podle Věty 8.27 lze každý vektor $x \in \mathbb{R}^n$ jednoznačně rozložit na součet $x = y + z$, kde $y \in V$ a $z \in V^\perp$. Z pohledu Věty 8.28 je y projekce x do V a z projekce x do $V^\perp$. Tedy $z = x - y = x - Px = (I - P)x$. □

8.5 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 vzhledem k monotonii druhé mocniny 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 8.38 (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. Hledáme vlastně projekci vektoru b do podprostoru $\mathcal{S}(A)$, což je vektor $A(A^TA)^{-1}A^Tb$. Protože tento vektor chceme vyjádřit ve tvaru Ax, hodnota $x \coloneqq (A^TA)^{-1}A^Tb$ vyhovuje. 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*. Zajímavé je, že tuto soustavu dostaneme z původní soustavy $Ax = b$ pouhým přenásobením A^T. Navíc soustava normálních rovnic popisuje přibližná řešení metodou nejmenších čtverců i když není splněn předpoklad na plnou sloupcovou hodnost matice A.

Věta 8.39 (Množina řešení metodou nejmenších čtverců)**.** *Buď $A \in \mathbb{R}^{m\times n}$. Pak množina přibližných řešení soustavy $Ax = b$ metodou nejmenších čtverců je rovna množině řešení soustavy normálních rovnic.*

Poznámka. Později ve Větě 13.25 ukážeme, že soustava normálních rovnic je vždy řešitelná.

Důkaz. Podobně jako v důkazu Věty 8.38 hledáme projekci vektoru b do podprostoru $\mathcal{S}(A)$, což je vektor tvaru Ax, $x \in \mathbb{R}^n$. Protože rozdíl projektovaného vektoru a jeho projekce musí být kolmý na podprostor, do kterého projektujeme, je nutně $Ax-b \in \mathcal{S}(A)^\perp = \mathrm{Ker}\,(A^T)$. Tudíž $A^T(Ax-b) = 0$, z čehož $A^TAx = A^Tb$.

Naopak, Je-li $x \in \mathbb{R}^n$ řešením $A^TAx = A^Tb$, tak $A^T(Ax-b) = 0$ a proto $Ax-b \in \mathcal{S}(A)^\perp$. Pro libovolné $y \in \mathbb{R}^n$ pak podle Pythagorovy věty máme

$$\|Ay-b\|^2 = \|A(y-x)+(Ax-b)\|^2 = \|A(y-x))\|^2 + \|Ax-b\|^2 \geq \|Ax-b\|^2,$$

tudíž x je přibližným řešením metodou nejmenších čtverců. □

Metoda nejmenších čtverců[4)] má uplatnění v řadě oborů, zejména ve statistice při lineární regresi. Ta studuje chování a odhaduje budoucí vývoj různých veličin, např. globální teploty, HDP, ceny akcií či ropy v čase. Setkáme se s ní ale skoro ve všech vědních oborech. Např. ve fyzice tzv. Hookeův zákon říká, že natažení materiálu je přímo úměrné působící síle. Chceme-li odhadnout konstantu úměrnosti, provedeme velké množství pozorování a z nich vypočítáme hodnotu metodou nejmenších čtverců.

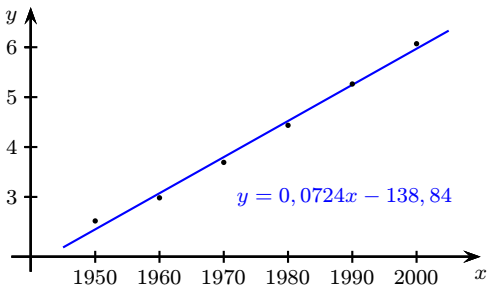
Příklad 8.40 (Lineární regrese: vývoj světové populace)**.** Data vývoje světové populace jsou následující:

rok	1950	1960	1970	1980	1990	2000
populace (mld.)	2,519	2,982	3,692	4,435	5,263	6,070

Chceme najít závislost velikosti populace na čase. Předpokládejme, že závislost je lineární. (To není vůbec samozřejmé, třeba Fibonacciho zjednodušený model růstu populace králíků byl exponenciální.) Obrázek dole, ilustrující data, v zásadě lineární závislost naznačuje. Lineární vztah popíšeme přímkou $y = px + q$, kde x je čas a y velikost populace. Neznámé parametry p, q vypočítáme. Po dosazení dat do rovnic by parametry p, q měly splňovat podmínky

$$2,519 = p \cdot 1950 + q$$
$$\vdots$$
$$6,070 = p \cdot 2000 + q$$

Přesné řešení neexistuje ale řešení metodou nejmenších čtverců je $p = 0,0724$, $q = -138,84$. 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 je 6,6943 mld. obyvatel, ve skutečnost jich bylo 6,853 mld. Ovšem pozor, má smysl vytvářet pouze krátkodobé odhady – v roce 1900 určitě nebyla velikost populace záporná. □

[4)] Metoda nejmenších čtverců byla vyvinuta Gaussem kolem roku 1801 pro astronomická pozorování. Tehdy se objevil asteroid Ceres, aby vzápětí zase zmizel. Gauss metodou popsal jeho dráhu a předpověděl kdy se znovu objeví.

8.6 Ortogonální matice

Uvažujme lineární zobrazení v prostoru $\mathbb{R}^n$. Jaké toto zobrazení (potažmo jeho matice) musí být, aby nijak nedeformovalo geometrické objekty? Otočení kolem počátku či překlopení podle osy jsou příklady takových zobrazení, ale chtěli bychom je analyzovat podrobně. Ukážeme, že tato vlastnost souvisí s tzv. ortogonálními maticemi. Ty ale mají dalekosáhlejší význam. Protože mají dobré numerické vlastnosti (viz Sekce 1.2 a 3.5.1), setkáváme se s nimi často v nejrůznějších numerických algoritmech.

I v této sekci uvažujeme standardní skalární součin v $\mathbb{R}^n$.

Definice 8.41 (Ortogonální a unitární matice)**.** Matice $Q \in \mathbb{R}^{n\times n}$ je *ortogonální*, pokud $Q^TQ = I_n$. Matice $Q \in \mathbb{C}^{n\times n}$ je *unitární*, pokud $\overline{Q}^TQ = I_n$.

Pojem unitární matice je zobecnění ortogonálních matic pro komplexní čísla. Nadále ale budeme vesměs pracovat jen s ortogonálními maticemi.

Věta 8.42 (Charakterizace ortogonálních matic)**.** *Buď $Q \in \mathbb{R}^{n\times n}$. Pak následující jsou ekvivalentní:*

(1) Q je ortogonální,

(2) Q je regulární a $Q^{-1} = Q^T$,

(3) $QQ^T = I_n$,

(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 $Q^{-1} = Q^T$; podobně naopak. 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.

Tvrzení 8.43 (Součin ortogonálních matic)**.** *Jsou-li $Q_1, Q_2 \in \mathbb{R}^{n\times n}$ ortogonální, pak Q_1Q_2 je ortogonální.*

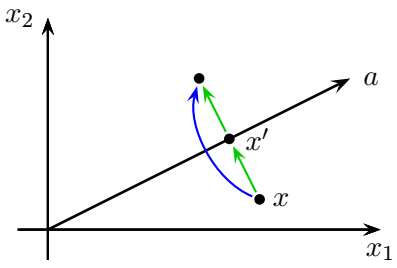
Důkaz. $(Q_1Q_2)^TQ_1Q_2 = Q_2^TQ_1^TQ_1Q_2 = Q_2^TQ_2 = I_n$. □

Příklad 8.44 (Příklady ortogonálních matic)**.**

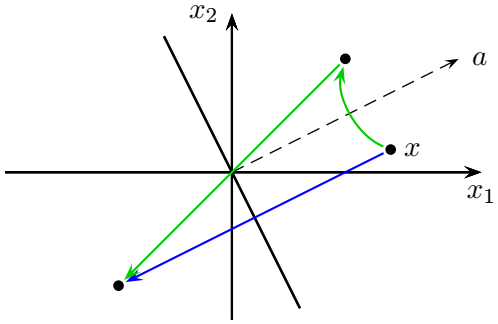
- Jednotková matice I_n, nebo k ní opačná $-I_n$.
- *Householderova matice*: $H(a) \coloneqq I_n - \frac{2}{a^Ta}aa^T$, kde $o \neq a \in \mathbb{R}^n$. Její geometrický význam je následující. Uvažme lineární zobrazení otočení bodu x dle přímky se směrnicí a o 180°. Pomocí Věty 8.36 o projekci dostáváme, že se zobrazí na vektor

$$x + 2(x' - x) = 2x' - x = 2a(a^Ta)^{-1}a^Tx - x = \left(2\frac{aa^T}{a^Ta} - I\right)x.$$

  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.

Navíc se dá ukázat, že každou ortogonální matici řádu n lze rozložit jako součin nanejvýš n vhodných Householderových matic.

- *Givensova matice*[5]: 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 $c^2 + s^2 = 1$ a každá takováto matice odpovídá nějaké matici otočení. 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 $\binom{n}{2}$ a případně navíc jedna diagonální matice s ± 1 na diagonále. □

Věta 8.45 (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 8.42 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 $\begin{pmatrix} 1 & o^T \\ o & Q \end{pmatrix}^T \begin{pmatrix} 1 & o^T \\ o & Q \end{pmatrix} = \begin{pmatrix} 1 & o^T \\ o & Q^TQ \end{pmatrix} = I_{n+1}$. □

Díváme-li se na Q jako na matici příslušného lineárního zobrazení $x \mapsto Qx$, pak vlastnost (1) Věty 8.45 říká, že při tomto zobrazení se zachovávají úhly, a vlastnost (2) zase říká, že se zachovávají délky. Tvrzení platí i naopak: matice zobrazení zachovávající skalární součin musí být nutně ortogonální (srov. Věta 8.46). 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.

Na závěr ukažme některá zobecnění výše zmíněných vlastností na libovolný skalární součin a libovolné lineární zobrazení.

[5] James Wallace Givens (1910–1993), Jr., americký matematik.

Věta 8.46 (Ortogonální matice a lineární zobrazení)**.** *Buďte U, V prostory nad $\mathbb{R}$ s libovolným skalárním součinem a $f\colon U \to V$ lineární zobrazení. Nechť B_1 resp. B_2 je ortonormální báze U resp. V. Pak matice zobrazení ${}_{B_2}[f]_{B_1}$ je ortogonální právě tehdy, když $\langle f(x), f(y)\rangle = \langle x, y\rangle$ pro každé $x, y \in U$.*

Důkaz. Podle Tvrzení 8.23 a vlastnosti matice zobrazení je

$$\begin{aligned}\langle x, y\rangle &= [x]_{B_1}^T [y]_{B_1},\\ \langle f(x), f(y)\rangle &= [f(x)]_{B_2}^T [f(y)]_{B_2} = \left({}_{B_2}[f]_{B_1}\,[x]_{B_1}\right)^T {}_{B_2}[f]_{B_1}\,[y]_{B_1}\\ &= [x]_{B_1}^T\, {}_{B_2}[f]_{B_1}^T\, {}_{B_2}[f]_{B_1}\,[y]_{B_1}.\end{aligned}$$

Tudíž, je-li ${}_{B_2}[f]_{B_1}$ ortogonální, pak $\langle f(x), f(y)\rangle = \langle x, y\rangle$. Naopak, pokud $\langle f(x), f(y)\rangle = \langle x, y\rangle$ platí pro každé $x, y \in U$, platí rovnost speciálně pro vektory jejichž souřadnice jsou jednotkové vektory. Dosadíme-li za x konkrétně i-tý vektor báze B_1 a za y pak j-tý vektor báze B_2, máme $[x]_{B_1} = e_i$, $[y]_{B_2} = e_j$ a proto

$$\begin{aligned}(I_n)_{ij} = e_i^T e_j = [x]_{B_1}^T [y]_{B_1} = \langle x, y\rangle = \langle f(x), f(y)\rangle = [x]_{B_1}^T\, {}_{B_2}[f]_{B_1}^T\, {}_{B_2}[f]_{B_1}\,[y]_{B_1}\\ = e_i^T\, {}_{B_2}[f]_{B_1}^T\, {}_{B_2}[f]_{B_1}\, e_j = \left({}_{B_2}[f]_{B_1}^T\, {}_{B_2}[f]_{B_1}\right)_{ij}.\end{aligned}$$

Tímto po složkách dostáváme rovnost $I_n = {}_{B_2}[f]_{B_1}^T\, {}_{B_2}[f]_{B_1}$. □

Věta 8.47 (Ortogonální matice a matice přechodu)**.** *Buď V prostor nad $\mathbb{R}$ s libovolným skalárním součinem a B_1, B_2 dvě jeho báze. Jakékoli dvě z následujících vlastností implikují tu třetí:*

(1) B_1 je ortonormální báze,

(2) B_2 je ortonormální báze,

(3) ${}_{B_2}[id]_{B_1}$ je ortogonální matice.

Důkaz.

Implikace „$(1), (2) \Rightarrow (3)$“. Plyne z Věty 8.46, neboť identita zachovává skalární součin.

Implikace „$(2), (3) \Rightarrow (1)$“. Buď $B_1 = \{x_1, \ldots, x_n\}$. Z definice pak sloupce ${}_{B_2}[id]_{B_1}$ tvoří vektory $[x_i]_{B_2}$, které jsou (díky ortogonalitě matice přechodu) ortonormální při standardním skalárním součinu v $\mathbb{R}^n$. Podle Tvrzení 8.23 pak $\langle x_i, x_j\rangle = [x_i]_{B_2}^T [x_j]_{B_2}$, což je 0 pro $i = j$ a 1 jinak.

Implikace „$(3), (1) \Rightarrow (2)$“. Platí z předchozího ze symetrie, neboť ${}_{B_1}[id]_{B_2} = {}_{B_2}[id]_{B_1}^{-1}$. □

Problémy

8.1. *Stopa* matice $A \in \mathbb{R}^{n\times n}$ je číslo $\operatorname{trace}(A) = \sum_{i=1}^n a_{ii}$. Ukažte, že $\langle A, B\rangle \coloneqq \operatorname{trace}(A^T B)$ je skalární součin na prostoru matic $\mathbb{R}^{m\times n}$.

8.2. Dokažte, že následující tvrzení platí pro reálný vektorový prostor, ale pro komplexní už obecně ne: Vektory $x, y \in V$ jsou kolmé právě tehdy, když $\|x + y\|^2 = \|x\|^2 + \|y\|^2$.

8.3. Rozhodněte, pro které vektory se Cauchy–Schwarzova nerovnost nabyde jako rovnost a pro které jako ostrá nerovnost.

8.4. Porovnejte velikost (normu) vektoru $x \in V$ s velikostí jeho projekce do podprostoru $U \trianglelefteqslant V$.

8.5. Určete vzdálenost $c \in \mathbb{R}^n$ od

(a) nadroviny $a^T x = b$, kde $o \neq a \in \mathbb{R}^n$ a $b \in \mathbb{R}$.

(b) přímky $p = b + \operatorname{span}\{a\}$, $a \neq o$.

8.6. Ukažte, že projekce vektoru x do podprostoru U se dá vyjádřit jako jednoznačný bod v průniku podprostoru U a afinního podprostoru $U^\perp + x$.

8.7. Buď P matice projekce do $U \trianglelefteqslant \mathbb{R}^n$. Dokažte, že $\operatorname{rank}(P) = \operatorname{trace}(P)$.

8.8. Odvoďte vzoreček pro projekci do $\operatorname{Ker}(A)$, má-li matice $A \in \mathbb{R}^{m\times n}$ hodnost m.

8.9. Odvoďte vzorečky pro ortogonální projekci v $\mathbb{R}^n$ (Věta 8.36) a pro metodu nejmenších čtverců (Věta 8.38) pomocí Gramovy matice (Věta 8.32).

8.10. Může být součet ortogonálních matic zase ortogonální matice?

8.11. Buďte U, V prostory nad $\mathbb{R}$ se skalárním součinem a $f\colon U \to V$ zobrazení zachovávající skalární součin, tj. $\langle f(x), f(y)\rangle = \langle x, y\rangle$ pro všechna $x, y \in U$. Ukažte, že f je lineární a prosté.

Kapitola 9

Determinanty

Determinanty byly vyvinuty pro účely řešení čtvercové soustavy lineárních rovnic a dávají explicitní vzorec pro jejich řešení (viz Větu 9.13). Za autora determinantu se považuje Gottfried Wilhelm Leibniz a nezávisle na něm jej objevil stejného roku 1683 japonský matematik Seki Kōwa. Jejich přístup (v trochu jiné podobě než uvádíme v definici) upadl trochu v zapomnění a determinanty se staly populární pro řešení soustav rovnic až tak v letech 1750–1900, pak je vystřídaly jiné metody. Nicméně se ukázalo, že determinant sám o sobě je důležitá charakteristika čtvercové matice s řadou uplatnění. Samotný pojem „determinant“ pochází od Gausse (*Disquisitiones arithmeticae*, 1801), i když jej používal v trochu jiném smyslu.

Připomeňme, že S_n značí množinu všech permutací na $\{1, \dots, n\}$, viz Sekci 4.2.

Definice 9.1 (Determinant)**.** Buď $A \in \mathbb{T}^{n\times n}$. 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 $|A|$.

Co vlastně říká vzoreček z definice determinantu? Každý sčítanec má tvar $\operatorname{sgn}(p)a_{1,p(1)} \dots a_{n,p(n)}$, což odpovídá tomu, že v matici A vybereme n prvků tak, že z každého řádku a sloupce máme právě jeden. Tyto prvky pak mezi sebou vynásobíme a ještě sčítanci přiřadíme kladné či záporné znaménko podle toho, jaké bylo znaménko permutace, která tyto prvky určovala.

Příklad 9.2 (Příklady determinantů)**.** Matice řádu 2 má determinant

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{21}a_{12}.$$

Matice řádu 3 má determinant

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{cases} a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} \\ -a_{31}a_{22}a_{13} - a_{11}a_{32}a_{23} - a_{21}a_{12}a_{33}. \end{cases}$$

Počítat determinanty z definice pro větší matice je obecně značně neefektivní, protože vyžaduje zpracovat $n!$ sčítanců. Výpočet je jednoduší jen pro speciální matice. Například, determinant trojúhelníkové matice je součin diagonálních prvků, protože v definici determinantu je jediný potenciálně nenulový člen sumy pro permutaci $p = id$, která odpovídá výběru diagonálních prvků. Speciálně, $\det(I_n) = 1$. □

Věta 9.3 (Determinant transpozice)**.** *Buď $A \in \mathbb{T}^{n\times n}$. Pak* $\det(A^T) = \det(A)$.

Důkaz.

$$\det(A^T) = \sum_{p\in S_n} \operatorname{sgn}(p) \prod_{i=1}^{n} A^T_{i,p(i)} = \sum_{p\in S_n} \operatorname{sgn}(p) \prod_{i=1}^{n} a_{p(i),i} = \sum_{p\in S_n} \operatorname{sgn}(p^{-1}) \prod_{i=1}^{n} a_{i,p^{-1}(i)}$$

$$= \sum_{p^{-1}\in S_n} \operatorname{sgn}(p^{-1}) \prod_{i=1}^{n} a_{i,p^{-1}(i)} = \sum_{q\in S_n} \operatorname{sgn}(q) \prod_{i=1}^{n} a_{i,q(i)} = \det(A).$$ □

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.

Věta 9.4 (Řádková linearita determinantu)**.** *Buď $A \in \mathbb{T}^{n\times n}$ a $b \in \mathbb{T}^n$. 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.

$$\begin{aligned}\det(A + e_i b^T) &= \sum_{p\in S_n} \operatorname{sgn}(p) a_{1,p(1)} \dots (a_{i,p(i)} + b_{p(i)}) \dots a_{n,p(n)} \\ &= \sum_{p\in S_n} \operatorname{sgn}(p) a_{1,p(1)} \dots a_{i,p(i)} \dots a_{n,p(n)} + \sum_{p\in S_n} \operatorname{sgn}(p) a_{1,p(1)} \dots b_{p(i)} \dots a_{n,p(n)} \\ &= \det(A) + \det(A + e_i(b^T - A_{i*}))\end{aligned}$$

□

Vzhledem k Větě 9.3 je determinant nejen řádkově, ale i sloupcově lineární.

9.1 Determinant a elementární úpravy

Naším plánem je k výpočtu determinantu využít Gaussovu eliminaci. K tomu musíme nejprve umět spočítat determinant matice v odstupňovaném tvaru, a vědět, jak hodnotu determinantu ovlivňují elementární řádkové úpravy. Na první otázku je jednoduchá odpověď, protože matice v odstupňovaném tvaru je zároveň horní trojúhelníková, a tudíž je její determinant roven součinu diagonálních prvků. Druhou otázku zodpovíme rozborem jednotlivých elementárních úprav. Nechť matice A' vznikne z A nějakou elementární úpravou:

1. Vynásobení i-tého řádku číslem $\alpha \in \mathbb{T}$: $\det(A') = \alpha \det(A)$.

   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 $A \in \mathbb{T}^{n\times n}$ 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 $-1 = 1$.

Důkaz č. 2. Definujme transpozici $t := (i, j)$, kde i, j jsou indexy stejných řádků. Nechť S'_n je množina sudých permutací z S_n. Pak S_n lze disjunktně rozložit na sjednocení S'_n a $\{p \circ t;\ p \in S'_n\}$. Tudíž

$$\begin{aligned}\det(A) &= \sum_{p\in S'_n} \operatorname{sgn}(p) \prod_{i=1}^{n} a_{i,p(i)} + \sum_{p\in S'_n} \operatorname{sgn}(p\circ t) \prod_{i=1}^{n} a_{i,p\circ t(i)} \\ &= \sum_{p\in S'_n} \operatorname{sgn}(p) \prod_{i=1}^{n} a_{i,p(i)} - \sum_{p\in S'_n} \operatorname{sgn}(p) \prod_{i=1}^{n} a_{i,p(i)} = 0.\end{aligned}$$ □

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

$$\det(A') = \det\begin{pmatrix} A_{1*} \\ \vdots \\ A_{i*} + \alpha A_{j*} \\ \vdots \\ A_{n*} \end{pmatrix} = \det(A) + \det\begin{pmatrix} A_{1*} \\ \vdots \\ \alpha A_{j*} \\ \vdots \\ A_{n*} \end{pmatrix} = \det(A) + \alpha 0 = \det(A).$$ □

Výše zmíněná pozorování mají několik důsledků: Pro libovolnou matici $A \in \mathbb{T}^{n\times n}$ 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 odstupňovaného tvaru A' a pamatuj si případné změny determinantu v koeficientu c; pak $\det(A)$ je roven součinu c^{-1} a diagonálních prvků matice A'.

9.2 Další vlastnosti determinantu

Věta 9.7 (Kriterium regularity)**.** *Matice $A \in \mathbb{T}^{n\times n}$ je regulární právě tehdy, když* $\det(A) \neq 0$.

Důkaz. Převedeme matici A elementárními úpravami na odstupňovaný tvar A', ty mohou měnit hodnotu determinantu, ale nikoli jeho (ne)nulovost. Pak A je regulární právě tehdy, když 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. Příkladem je Hilbertova matice H_n (viz Příklad 3.39), 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. Uvažujme 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 $A, B \in \mathbb{T}^{n\times n}$ platí* $\det(AB) = \det(A)\det(B)$.

Důkaz. (A). Nejprve uvažujme speciální případ, když A je matice elementární úpravy:

1. $A = E_i(\alpha)$, vynásobení i-tého řádku číslem α. Pak $\det(AB) = \alpha\det(B)$ a $\det(A)\det(B) = \alpha\det(B)$.
2. $A = E_{ij}$, prohození i-tého a j-tého řádku. Pak $\det(AB) = -\det(B)$ a $\det(A)\det(B) = -1\det(B)$.
3. $A = E_{ij}(\alpha)$, přičtení α-násobku j-tého řádku k i-tému. Pak $\det(AB) = \det(B)$ a $\det(A)\det(B) = 1\det(B)$.

Tedy rovnost platí ve všech případech.

(B). Nyní uvažme obecný případ. Je-li A singulární, pak i AB je singulární (Věta 3.22) a tedy podle Věty 9.7 je $\det(AB) = 0 = 0\det(B) = \det(A)\det(B)$. Je-li A 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

$$\begin{aligned}\det(AB) &= \det(E_1(E_2 \dots E_k B)) = \det(E_1)\det((E_2 \dots E_k)B)\\ &= \det(E_1)\det(E_2 \dots E_k)\det(B) = \det(E_1E_2 \dots E_k)\det(B)\\ &= \det(A)\det(B).\end{aligned}$$

□

Důsledek 9.10. *Buď $A \in \mathbb{T}^{n\times n}$ regulární, pak* $\det(A^{-1}) = \det(A)^{-1}$.

Důkaz. $1 = \det(I_n) = \det(AA^{-1}) = \det(A)\det(A^{-1})$. □

Nyní ukážeme rekurentní vzoreček na výpočet determinantu.

Věta 9.11 (Laplaceův rozvoj podle i-tého řádku)**.** *Buď $A \in \mathbb{T}^{n\times n}$, $n \geq 2$. 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.

Poznámka. Podobně jako podle řádku můžeme rozvíjet podle libovolného sloupce.

Důkaz. (A). Nejprve uvažujme případ $A_{i*} = e_j^T$, tj. i-tý řádek matice A je jednotkový vektor. Postupným vyměňováním řádků $(i, i+1)$, $(i+1, i+2)$, …, $(n-1, n)$ 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)**.**

$$\begin{aligned}\begin{vmatrix}1&2&3&4\\1&2&1&2\\2&5&5&5\\0&2&-4&-4\end{vmatrix} &= (-1)^{4+1}\cdot 0\cdot\begin{vmatrix}2&3&4\\2&1&2\\5&5&5\end{vmatrix} + (-1)^{4+2}\cdot 2\cdot\begin{vmatrix}1&3&4\\1&1&2\\2&5&5\end{vmatrix}\\ &\quad + (-1)^{4+3}\cdot(-4)\cdot\begin{vmatrix}1&2&4\\1&2&2\\2&5&5\end{vmatrix} + (-1)^{4+4}\cdot(-4)\cdot\begin{vmatrix}1&2&3\\1&2&1\\2&5&5\end{vmatrix}\\ &= 0 + 2\cdot 4 + 4\cdot 2 - 4\cdot 2 = 8\end{aligned}$$

□

Následující věta dává explicitní vzoreček na řešení soustavy s regulární maticí. 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 $A \in \mathbb{T}^{n\times n}$ regulární, $b \in \mathbb{T}^n$. Pak řešení soustavy $Ax = b$ je dáno vzorcem*

$$x_i = \frac{\det(A + (b - A_{*i})e_i^T)}{\det(A)}, \quad i = 1, \dots, n.$$

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

$$\begin{aligned}\det(A + (b - A_{*i})e_i^T) &= \det(A_{*1}|\dots|b|\dots|A_{*n}) = \det(A_{*1}|\dots|\textstyle\sum_{j=1}^n A_{*j}x_j|\dots|A_{*n})\\ &= \sum_{j=1}^{n}\det(A_{*1}|\dots|A_{*j}|\dots|A_{*n})x_j\\ &= \det(A_{*1}|\dots|A_{*i}|\dots|A_{*n})x_i = \det(A)x_i.\end{aligned}$$

Nyní stačí obě strany podělit číslem $\det(A) \neq 0$. □

Cramerovo pravidlo z roku 1750 (i když bylo známo už dříve) je pojmenováno po švýcarském matematikovi Gabrielu Cramerovi. Ve své době to byl populární nástroj na řešení soustav lineárních rovnic, dnes má význam spíše teoretický. Mimo jiné ukazuje a dává:

- Explicitní vyjádření řešení soustavy lineárních rovnic.
- Spojitost řešení vzhledem k prvkům matice A a vektoru b.

  Formálně, zobrazení $(A, b) \mapsto A^{-1}b$ je spojité na definičním oboru regulárních matic A. To je snadné nahlédnout, protože podle Cramerova pravidla počítáme jednotlivé složky řešení pouze pomocí aritmetických operací.

- Odhad velikosti popisu řešení z velikosti popisu vstupních hodnot.

  Potřebujeme-li k zápisu vstupních hodnot soustavy $Ax = b$ (tj., k zápisu a_{ij}, b_j) celkem K bitů, tak její řešení má zápis pomocí polynomiálně mnoha bitů vzhledem ke K. To dá trochu více práce nahlédnout, ale je to důležité pozorování, protože nám zaručuje omezenou velikost zápisu řešení.

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 po složkách

$$x_1 = \frac{\begin{vmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 4 & 5 & 5 \end{vmatrix}}{\begin{vmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \\ 2 & 5 & 5 \end{vmatrix}} = \frac{4}{2} = 2,\ x_2 = \frac{\begin{vmatrix} 1 & 1 & 3 \\ 1 & 3 & 1 \\ 2 & 4 & 5 \end{vmatrix}}{\begin{vmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \\ 2 & 5 & 5 \end{vmatrix}} = \frac{2}{2} = 1,\ x_3 = \frac{\begin{vmatrix} 1 & 2 & 1 \\ 1 & 2 & 3 \\ 2 & 5 & 4 \end{vmatrix}}{\begin{vmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \\ 2 & 5 & 5 \end{vmatrix}} = \frac{-2}{2} = -1,$$

□

9.3 Adjungovaná matice

Adjungovaná matice[1)] úzce souvisí s determinanty a maticovou inverzí. Využijeme ji při odvozování Cayleyho–Hamiltonovy věty (Věta 10.17), ale čtenář se s ní může potkat např. v kryptografii nebo při odvozování vzorečku pro derivaci determinantu.

Definice 9.15 (Adjungovaná matice)**.** Buď $A \in \mathbb{T}^{n\times n}$ a $n \geq 2$. Pak *adjungovaná matice* $\operatorname{adj}(A) \in \mathbb{T}^{n\times n}$ má složky

$$\operatorname{adj}(A)_{ij} = (-1)^{i+j} \det(A^{ji}), \quad i, j = 1, \ldots, n$$

kde A^{ji} opět značí matici vzniklou z A vyškrtnutím j-tého řádku a i-tého sloupce.

Věta 9.16 (O adjungované matici)**.** *Pro každou matici $A \in \mathbb{T}^{n\times n}$ platí $A \operatorname{adj}(A) = \det(A) I_n$.*

Důkaz. Odvodíme

$$(A \operatorname{adj}(A))_{ij} = \sum_{k=1}^{n} A_{ik} \operatorname{adj}(A)_{kj} = \sum_{k=1}^{n} A_{ik} (-1)^{k+j} \det(A^{jk}) = \begin{cases} \det(A), & \text{pro } i = j, \\ 0, & \text{pro } i \neq j. \end{cases}$$

Zdůvodnění je, že pro $i = j$ se jedná o rozvoj $\det(A)$ podle i-tého řádku. Pro $i \neq j$ se zase jedná o determinant matice A, kde ale j-tý řádek nahradíme i-tým. □

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 $A \in \mathbb{T}^{n\times n}$ 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:

$$\operatorname{adj}(A)_{12} = (-1)^{1+2} \begin{vmatrix} 2 & 3 \\ 5 & 5 \end{vmatrix} = 5,\ \ldots$$

[1)] V angličtině *adjugate*, popř. *adjoint*.

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

Determinant se používá např. v teorii grafů pro vyjádření počtu koster grafu [Matoušek a 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, jestliže $\det(A) = \pm 1$ a $\det(A^{ji})$ je celé číslo. □

Další ukázka použití determinantu je v polynomech. Determinant z následující věty se nazývá *rezultant* a používá se například k řešení nelineárních rovnic.

Věta 9.20. *Polynomy $p(x) = a_n x^n + \ldots + a_1 x + a_0$, $q(x) = b_m x^m + \ldots + b_1 x + b_0$ mají společný kořen právě tehdy, když*

$$\begin{vmatrix} a_n & a_{n-1} & \ldots & a_0 & & & \\ & a_n & a_{n-1} & \ldots & a_0 & & \\ & & \ddots & & & \ddots & \\ & & & a_n & a_{n-1} & \ldots & a_0 \\ b_m & b_{m-1} & \ldots & b_1 & b_0 & & \\ & \ddots & & & & \ddots & \\ & & b_m & b_{m-1} & \ldots & b_1 & b_0 \end{vmatrix} = 0.$$

Důkaz. Polynomy $p(x)$, $q(x)$ mají společný kořen právě tehdy, když existují polynomy $r(x)$, $s(x)$ stupňů nanejvýš $m-1, n-1$ takové, že $r(x)p(x) + s(x)q(x) = 0$. Pokud si neznámé polynomy vyjádříme jako $r(x) = c_{m-1}x^{m-1} + \ldots + c_1 x + c_0$, $s(x) = d_{n-1}x^{n-1} + \ldots + d_1 x + d_0$, tak rovnost $r(x)p(x) + s(x)q(x) = 0$ můžeme přepsat jako homogenní soustavu $m+n$ rovnic s $m+n$ neznámými $c_{m-1}, \ldots, c_0, d_{n-1}, \ldots, d_0$. Nenulové řešení existuje právě tehdy, když je matice singulární, neboli její determinant nulový. Ve větě je pak determinant transponované matice. □

Geometrická interpretace determinantu

Determinant má pěkný geometrický význam. Uvažujeme-li lineární zobrazení $x \mapsto Ax$ s maticí $A \in \mathbb{R}^{n\times n}$, pak geometrická tělesa mění v tomto zobrazení svůj objem s koeficientem $|\det(A)|$. Uvažujeme nejprve speciální případ rovnoběžnostěnu. *Rovnoběžnostěn* s lineárně nezávislými hranami $a_1, \ldots, a_m$ definujeme jako množinu $\{x \in \mathbb{R}^n;\ x = \sum_{i=1}^m \alpha_i a_i,\ 0 \le \alpha_i \le 1\}$.

Věta 9.21 (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 $|\det(A)|$.*

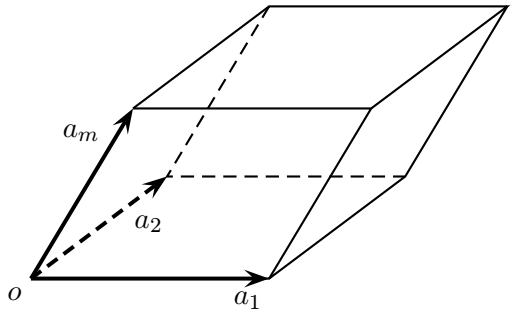
Poznámka. Svou roli hraje nejen velikost determinantu A, ale také jeho znaménko; to souvisí s pořadím hran rovnoběžnostěnu jako řádků matice A. Speciálně, pro $A \in \mathbb{R}^{3\times 3}$ je $\det(A) > 0$ pokud řádky A tvoří pravotočivou posloupnost vektorů (tzv. pravidlo palce), a $\det(A) < 0$ pokud tvoří levotočivou posloupnost.

Důkaz. Důkaz provedeme matematickou indukcí podle m. Pro $m = 1$ je to zřejmé, postupme k indukčnímu kroku. Označme i-tý řádek matice A jako a_i a definujme matici

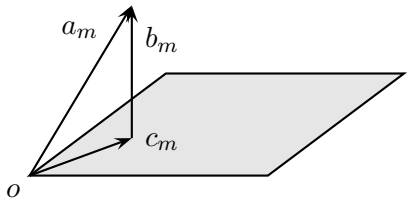
$$D \coloneqq \begin{pmatrix} a_1^T \\ \vdots \\ a_{m-1}^T \end{pmatrix},$$

která vznikne z A odstraněním posledního řádku. Rozložme $a_m = b_m + c_m$, kde $c_m \in \mathcal{R}(D)$ a $b_m \in \mathcal{R}(D)^\perp$ podle Poznámky 8.29. Označme

$$A' \coloneqq \begin{pmatrix} a_1^T \\ \vdots \\ a_{m-1}^T \\ b_m^T \end{pmatrix}.$$



Rovnoběžnostěn $a_1, a_2, \ldots, a_m$.



Plocha základny: $\sqrt{\det(DD^T)}$, výška: $\|b_m\|$.

Od A' k A lze přejít pomocí elementárních řádkových úprav, neboť k poslednímu řádku stačí přičíst c_m, což je lineární kombinace $a_1, \ldots, a_{m-1}$. Tedy existují elementární matice $E_1, \ldots, E_k$ tak, že $A = E_1 \ldots E_k A'$; navíc jejich determinant je 1 protože jen přičítají násobek řádku k jinému. Nyní

$$\begin{aligned} \det(AA^T) &= \det(E_1 \ldots E_k A' A'^T E_k^T \ldots E_1^T) \\ &= \det(E_k) \ldots \det(E_1) \det(A'A'^T) \det(E_k^T) \ldots \det(E_1^T) = \det(A'A'^T). \end{aligned}$$

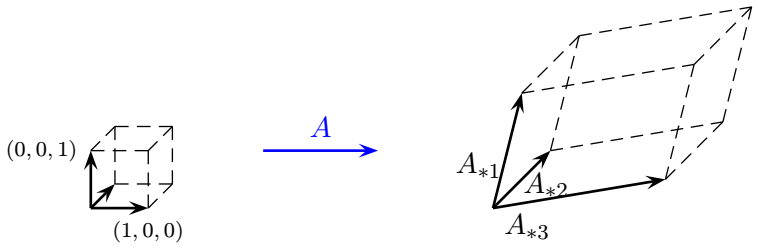
Dále,

$$A'A'^T = \begin{pmatrix} D \\ b_m^T \end{pmatrix} \begin{pmatrix} D^T & b_m \end{pmatrix} = \begin{pmatrix} DD^T & Db_m \\ b_m^T D^T & b_m^T b_m \end{pmatrix} = \begin{pmatrix} DD^T & o \\ o^T & b_m^T b_m \end{pmatrix}$$

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. □

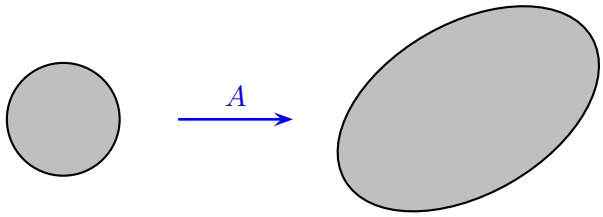
Buď $A \in \mathbb{R}^{n \times n}$. Jak jsme již zmínili, objem geometrických těles se při zobrazení $x \mapsto Ax$ mění s koeficientem $|\det(A)|$. Krychle o hraně 1 se zobrazí na rovnoběžnostěn o hranách, které odpovídají sloupcům matice A, a jeho objem je proto $|\det(A^T)| = |\det(A)|$. Tuto vlastnost 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 9.22 (Geometrická interpretace determinantu)**.** Obraz jednotkové krychle při zobrazení $x \mapsto Ax$:



objem $= 1$ objem $= \det(A)$

Obraz geometrického tělesa při zobrazení $x \mapsto Ax$:



objem $= V$ objem $= \det(A) \cdot V$ □

Determinanty se používají při řešení ještě mnoha dalších geometrických problémů [Berger, 1987; Dattorro, 2011]. Zmiňme úlohu, která souvisí s objemem rovnoběžnostěnu, o určení objemu mnohostěnu s $n+1$ vrcholy v $\mathbb{R}^n$. Bez újmy na obecnosti nechť je jeden vrchol a_0 v počátku a ostatní mají pozice $a_1, \ldots, a_n \in \mathbb{R}^n$. Definujme matici $A \in \mathbb{R}^{n\times n}$ tak, že její sloupce jsou vektory $a_1, \ldots, a_n$. Pak objem mnohostěnu je $\frac{1}{n!}|\det(A)|$, čili tvoří jen část rovnoběžnostěnu danou faktorem $1 : n!$.

Předchozí způsob výpočtu objemu mnohostěnu předpokládal, že známe pozice jednotlivých vrcholů v prostoru $\mathbb{R}^n$. V některých případech (např. molekulární biologie) jsou ale známy pouze vzdálenosti $d_{ij} = \|a_i - a_j\|$ mezi jednotlivými vrcholy, tj. délky hran mnohostěnu. V tomto případě spočítáme objem pomocí tzv. Cayleyho–Mengerova determinantu jako

$$\frac{(-1)^{n-1}}{2^n (n!)^2} \begin{vmatrix} 0 & 1 & 1 & 1 & \ldots & 1 \\ 1 & 0 & d_{01}^2 & d_{02}^2 & \ldots & d_{0n}^2 \\ 1 & d_{10}^2 & 0 & d_{12}^2 & \ldots & d_{1n}^2 \\ 1 & d_{20}^2 & d_{21}^2 & 0 & \ldots & d_{2n}^2 \\ \vdots & \vdots & \vdots & \ddots & & \vdots \\ 1 & d_{n0}^2 & d_{n1}^2 & d_{2n}^2 & \ldots & 0 \end{vmatrix}.$$

Problémy

9.1. Dokažte multiplikativnost determinantu přímo ze sloupcové linearity determinantu.

9.2. Dokažte, že v každém kroku Gaussovy–Jordanovy eliminace se každý nenulový prvek matice dá vyjádřit buď jako determinant, nebo podíl dvou determinantů podmatic původní matice.

9.3. Pomocí Cramerova pravidla odvoďte vzorec pro inverzní matici a porovnejte jej s adjungovanou maticí.

9.4. Pomocí věty o adjungované matici odvoďte Cramerovo pravidlo.

9.5. Rozhodněte, zda $\operatorname{adj}(AB) = \operatorname{adj}(BA)$ pro libovolné matice $A, B \in \mathbb{R}^{n\times n}$.

9.6. Uvažujme determinant jako funkci $\mathbb{R}^{n\times n} \to \mathbb{R}$. Určete parciální derivaci $\det(A)$ podle a_{ij} a sestavte matici parciálních derivací.

Kapitola 10

Vlastní čísla

Vlastní čísla (dříve též nazývaná „charakteristická čísla“), podobně jako determinant, představují určitou charakteristiku matice. Narozdíl od determinantu je jejich význam ještě dalekosáhlejší.

Definice 10.1 (Vlastní čísla a vlastní vektory)**.** Buď $A \in \mathbb{C}^{n\times n}$. 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.

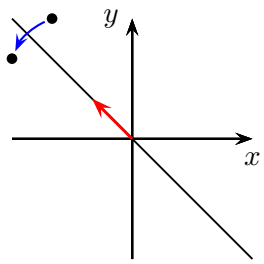
Povšimněme si dále, že vlastní vektor při daném vlastním čísle není určen jednoznačně – každý jeho nenulový násobek je také vlastním vektorem. Někdy se proto vlastní vektor normuje tak, aby $\|x\| = 1$.

Přirozeně, vlastní čísla a vektory lze definovat stejně 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.

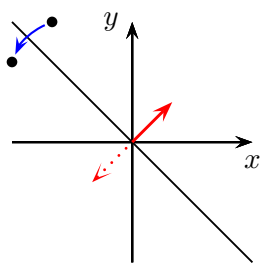
Vlastní čísla se dají zavést i obecněji. Buď V vektorový prostor a $f\colon V \to V$ lineární zobrazení. Pak λ je vlastní číslo a $x \neq o$ příslušný vlastní vektor, pokud platí $f(x) = \lambda x$. My se však vesměs budeme zabývat vlastními čísly matic, protože vzhledem k maticové reprezentaci lineárních zobrazení můžeme úlohu hledání vlastních čísel a vektorů lineárních zobrazení redukovat na matice.

Příklad 10.2 (Geometrická interpretace vlastních čísel a vektorů)**.** Vlastní vektor reprezentuje invariantní směr při zobrazení $x \mapsto Ax$, tedy směr, který se zobrazí opět na ten samý směr. Jinými slovy, je-li v vlastní vektor, pak přímka $\operatorname{span}\{v\}$ se zobrazí do sebe sama. Vlastní číslo pak představuje škálování v tomto invariantním směru.

- Překlopení dle přímky $y = -x$, matice zobrazení $A = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$:

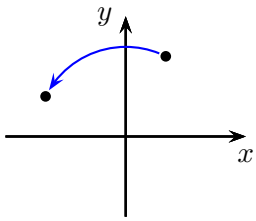


vlastní číslo 1, vlastní vektor $(-1, 1)^T$,



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 $A \in \mathbb{C}^{n\times n}$. 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.

10.1 Charakteristický polynom

Definice 10.4 (Charakteristický polynom)**.** *Charakteristický polynom* matice $A \in \mathbb{C}^{n\times n}$ vzhledem k proměnné λ je $p_A(\lambda) = \det(A - \lambda I_n)$.

Z definice determinantu je patrné, 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. Snadno nahlédneme, že $a_{n-1} = (-1)^{n-1}(a_{11} + \cdots + a_{nn})$ a po dosazení $\lambda = 0$ získáme $a_0 = \det(A)$.

Podle základní věty algebry (Věta 1.1) 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).

Věta 10.5. *Vlastní čísla matice $A \in \mathbb{C}^{n\times n}$ jsou právě kořeny jejího charakteristického polynomu $p_A(\lambda)$, a je jich n včetně násobností.*

Definice 10.6 (Algebraická a geometrická násobnost vlastního čísla)**.** Buď $\lambda \in \mathbb{C}$ vlastní číslo matice $A \in \mathbb{C}^{n\times n}$. *Algebraická násobnost* λ je rovna násobnosti λ jakožto kořene $p_A(\lambda)$. *Geometrická násobnost* λ je rovna $n - \operatorname{rank}(A - \lambda I_n)$, tj. počtu lineárně nezávislých vlastních vektorů, které odpovídají λ.

Algebraická násobnost je vždy větší nebo rovna geometrické násobnosti, což vyplyne v Sekci 10.4. Nadále budeme pojem násobnost používat pro algebraickou násobnost.

Definice 10.7 (Spektrum a spektrální poloměr)**.** Nechť $A \in \mathbb{C}^{n\times n}$ má vlastní čísla $\lambda_1, \ldots, \lambda_n$. Pak *spektrum* matice A je množina jejích vlastních čísel $\{\lambda_1, \ldots, \lambda_n\}$ a *spektrální poloměr* je $\rho(A) = \max_{i=1,\ldots,n} |\lambda_i|$.

Počítat vlastní čísla jako kořeny charakteristického polynomu není příliš efektivní. Navíc, jak víme ze Sekce 1.4, pro kořeny polynomu neexistuje žádný vzoreček ani konečný postup a počítají se iterativními metodami. Totéž platí i o vlastních číslech (uvidíme ve Větě 10.15). Zde nepomůže ani jindy tak oblíbená a všestranná Gaussova eliminace. Nicméně pro některé speciální matice můžeme vlastní čísla určit snadno.

Příklad 10.8 (Vlastní čísla trojúhelníkové matice)**.**

- Nechť $A \in \mathbb{C}^{n\times n}$ 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. Množina příslušných vlastních vektorů je $\mathbb{R}^n\backslash\{o\}$.
- Speciálně, 0_n má vlastní číslo 0, které je n-násobné. Množina příslušných vlastních vektorů je $\mathbb{R}^n\backslash\{o\}$.
- Speciálně, matice $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ má vlastní číslo 1, které je dvojnásobné (algebraicky). Odpovídající vlastní vektor je až na násobek pouze $(1,0)^T$, proto je geometrická násobnost vlastního čísla 1 pouze jedna. □

Příklad 10.9. 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 $\pm i$. Vlastní vektor příslušný i je $(1,-i)^T$ a vlastní vektor příslušný $-i$ je $(1,i)^T$. □

Pro následující připomeňme, že $\mathrm{trace}(A)$ značí stopu matice A, čili součet diagonálních prvků A.

Věta 10.10 (Součin a součet vlastních čísel)**.** *Buď $A \in \mathbb{C}^{n\times n}$ s vlastními čísly $\lambda_1, \dots, \lambda_n$. Pak*

(1) $\det(A) = \lambda_1 \dots \lambda_n$,

(2) $\mathrm{trace}(A) = \lambda_1 + \dots + \lambda_n$.

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 má hodnotu $(-1)^{n-1}(a_{11} + \dots + a_{nn})$. 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.

Věta 10.11 (Vlastnosti vlastních čísel)**.** *Nechť $A \in \mathbb{C}^{n\times n}$ má vlastní čísla $\lambda_1, \dots, \lambda_n$ a jim odpovídající vlastní vektory $x_1, \dots, x_n$. Pak:*

(1) A je regulární právě tehdy, když 0 není její vlastní číslo,

(2) je-li A regulární, pak A^{-1} má vlastní čísla $\lambda_1^{-1}, \dots, \lambda_n^{-1}$ a vlastní vektory $x_1 \dots, x_n$,

(3) A^2 má vlastní čísla $\lambda_1^2, \dots, \lambda_n^2$ a vlastní vektory $x_1 \dots, x_n$,

(4) αA má vlastní čísla $\alpha\lambda_1, \dots, \alpha\lambda_n$ a vlastní vektory $x_1 \dots, x_n$,

(5) $A + \alpha I_n$ má vlastní čísla $\lambda_1 + \alpha, \dots, \lambda_n + \alpha$ a vlastní vektory $x_1 \dots, x_n$,

(6) A^T má vlastní čísla $\lambda_1, \dots, \lambda_n$, 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.

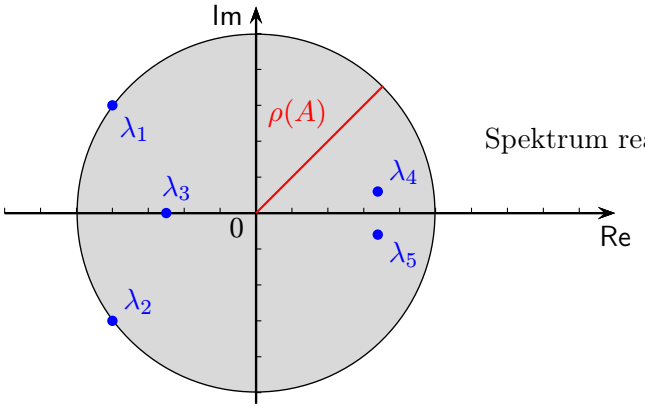
(2) Pro každé $i = 1, \dots, n$ je $Ax_i = \lambda_i x_i$. Přenásobením A^{-1} dostaneme $x_i = \lambda_i A^{-1}x_i$ a vydělením $\lambda_i \neq 0$ pak $A^{-1}x_i = \lambda_i^{-1}x_i$. □

V následující větě je důležité, že matice A je reálná, pro komplexní už tvrzení neplatí.

Věta 10.12. *Je-li $\lambda \in \mathbb{C}$ vlastní číslo matice $A \in \mathbb{R}^{n\times n}$, pak i komplexně sdružené $\overline{\lambda}$ je vlastním číslem A.*

Důkaz. Víme, že λ je kořenem $p_A(\lambda) = (-1)^n\lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda + a_0 = 0$. Komplexním sdružením obou stran rovnosti máme $(-1)^n\overline{\lambda}^n + a_{n-1}\overline{\lambda}^{n-1} + \ldots + a_1\overline{\lambda} + a_0 = 0$, tedy i $\overline{\lambda}$ je kořenem $p_A(\lambda)$. □

Příklad 10.13. Spektrum reálné matice je tedy množina symetrická podle reálné osy. Komplexní matice můžou mít za spektrum jakýchkoli n komplexních čísel.



Spektrum reálné matice A

□

Nyní ukážeme, že výpočet kořenů polynomu lze převést na úlohu hledání vlastních čísel určité matice.

Definice 10.14 (Matice společnice[1])**.** Buď $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$. Pak *matice společnice* polynomu $p(x)$ je čtvercová matice řádu n definovaná

$$C(p) \coloneqq \begin{pmatrix} 0 & \ldots & \ldots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & -a_{n-1} \end{pmatrix}.$$

Věta 10.15 (O matici společnici)**.** *Platí* $p_{C(p)}(\lambda) = (-1)^n p(\lambda)$*, tedy vlastní čísla* $C(p)$ *odpovídají kořenům polynomu* $p(\lambda)$*.*

Důkaz. Upravme

$$p_{C(p)}(\lambda) = \det(C(p) - \lambda I_n) = \det \begin{pmatrix} -\lambda & \ldots & \ldots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & -a_2 \\ \vdots & \ddots & \ddots & -\lambda & \vdots \\ 0 & \ldots & 0 & 1 & -a_{n-1} - \lambda \end{pmatrix}.$$

Přičtením λ-násobku posledního řádku k předposlednímu, pak λ-násobku předposledního řádku k předpředposlednímu, atd. dostaneme

$$p_{C(p)}(\lambda) = \det \begin{pmatrix} 0 & \ldots & \ldots & 0 & -p(\lambda) \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} - a_{n-1}\lambda - \lambda^2 \\ 0 & \ldots & 0 & 1 & -a_{n-1} - \lambda \end{pmatrix}.$$

Laplaceovým rozvojem podle prvního řádku pak $p_{C(p)}(\lambda) = (-1)^{n+1}(-p(\lambda))\det(I_{n-1}) = (-1)^n p(\lambda)$. □

[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 pracovníci jiných škol.

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). Zajímavostí je, že např. Matlab počítá charakteristický polynom $p_A(\lambda)$ matice A tak, že najde vlastní čísla $\lambda_1, \ldots, \lambda_n$ a pak roznásobí dvojčleny ve výrazu $p_A(\lambda) = (-1)^n(\lambda - \lambda_1)\ldots(\lambda - \lambda_n)$.

10.2 Cayleyho–Hamiltonova věta

Stručně řečeno, Cayleyho–Hamiltonova věta[2)] říká, že každá čtvercová matice je kořenem svého charakteristického polynomu.

Příklad 10.16. Abychom lépe porozuměli následující větě, uvádíme příklad polynomiální matice a maticového polynomu

$$\begin{pmatrix} \lambda^2 - \lambda & 2\lambda - 3 \\ 7 & 5\lambda^2 - 4 \end{pmatrix} = \lambda^2 \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} + \lambda \begin{pmatrix} -1 & 2 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & -3 \\ 7 & -4 \end{pmatrix}.$$

Jsou to dva zápisy stejné matice s parametrem λ, a můžeme jednoduše převést jeden zápis na druhý. V různých situacích bývá užitečný jeden či druhý tvar. □

Věta 10.17 (Cayleyho–Hamiltonova)**.** *Buď $A \in \mathbb{C}^{n\times n}$ a $p_A(\lambda) = (-1)^n\lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda + a_0$. Pak*

$$(-1)^n A^n + a_{n-1}A^{n-1} + \ldots + a_1 A + a_0 I_n = 0.$$

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 $\operatorname{adj}(A - \lambda I_n) = \lambda^{n-1}B_{n-1} + \ldots + \lambda B_1 + B_0$ pro určité $B_{n-1}, \ldots, B_0 \in \mathbb{C}^{n\times n}$. Dosazením máme

$$\begin{aligned}(A - \lambda I_n)(\lambda^{n-1}B_{n-1} + \ldots + \lambda B_1 + B_0) &= \det(A - \lambda I_n)I_n \\ &= ((-1)^n\lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda + a_0)I_n.\end{aligned}$$

Roznásobením

$$\begin{aligned}-B_{n-1}\lambda^n + (AB_{n-1} - B_{n-2})\lambda^{n-1} + \ldots + (AB_1 - B_0)\lambda + AB_0 \\ = (-1)^n\lambda^n I_n + a_{n-1}\lambda^{n-1}I_n + \ldots + a_1\lambda I_n + a_0 I_n.\end{aligned}$$

Porovnáním koeficientů

$$\begin{aligned}-B_{n-1} &= (-1)^n I_n, \\ AB_j - B_{j-1} &= a_j I_n, \quad j = 1, \ldots, n-1, \\ AB_0 &= a_0 I_n.\end{aligned}$$

Vynásobme první rovnici A^n, další A^j a poslední $A^0 = I_n$. Sečtením pak získáme

$$\begin{aligned}&-A^nB_{n-1} + (A^nB_{n-1} - A^{n-1}B_{n-2}) + \ldots + (A^2B_1 - AB_0) + AB_0 = \\ &= 0 = (-1)^n A^n + a_{n-1}A^{n-1} + \ldots + a_1 A + a_0 I_n\end{aligned}$$

□

Přestože Cayleyho–Hamiltonova věta může působit jenom jako matematická zajímavost, má netriviální důsledky.

Důsledek 10.18. *Buď $A \in \mathbb{C}^{n\times n}$. Pak:*

(1) Pro každé $k \in \mathbb{N}$ je $A^k \in \operatorname{span}\{I_n, A, \ldots, A^{n-1}\}$, tedy A^k je lineární kombinací $I_n, A, \ldots, A^{n-1}$.

[2)] Arthur Cayley objevil tuto identitu r. 1858, William Rowan Hamilton nezávisle na něm r. 1853, oba pouze pro řád 3. Na vyšší řády ji zobecnil až Ferdinand Georg Frobenius r. 1878.

(2) je-li A regulární, pak $A^{-1} \in \operatorname{span}\{I_n, A, \ldots, A^{n-1}\}$.

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

$$\begin{aligned} I &= -\frac{(-1)^n}{a_0}A^n - \frac{a_{n-1}}{a_0}A^{n-1} - \ldots - \frac{a_1}{a_0}A \\ &= A\left(-\frac{(-1)^n}{a_0}A^{n-1} - \frac{a_{n-1}}{a_0}A^{n-2} - \ldots - \frac{a_1}{a_0}I_n\right). \end{aligned}$$

Tudíž vynásobením A^{-1} dostáváme

$$A^{-1} = -\frac{(-1)^n}{a_0}A^{n-1} - \frac{a_{n-1}}{a_0}A^{n-2} - \ldots - \frac{a_1}{a_0}I_n. \qquad \square$$

Podle tohoto důsledku lze velkou mocninu A^k matice A spočítat alternativně tak, že najdeme příslušné koeficienty charakteristického polynomu a vyjádříme A^k jako lineární kombinaci $I_n, A, \ldots, A^{n-1}$.

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

Při řešení soustav lineárních rovnic pomocí Gaussovy–Jordanovy eliminace jsme používali elementární řádkové úpravy. Ty nemění množinu řešení a upraví matici soustavy na tvar, ze kterého snadno vyčteme řešení. Je přirozené hledat analogické, spektrum neměnící, úpravy i na problém počítání vlastních čísel. Elementární řádkové úpravy použít nelze, protože ty mění spektrum. Vhodnou transformací je tzv. *podobnost*, protože ta spektrum nemění. A pokud se nám podaří touto transformací převést matici na diagonální tvar, máme vyhráno – na diagonále jsou hledaná vlastní čísla.

Definice 10.19 (Podobnost)**.** Matice $A, B \in \mathbb{C}^{n\times n}$ jsou *podobné*, pokud existuje regulární $S \in \mathbb{C}^{n\times n}$ tak, že $A = SBS^{-1}$.

Podobnost jde ekvivalentně definovat vztahem $AS = SB$ pro nějakou regulární matici S. Tímto přepisem můžeme i najít matici S, skrze kterou jsou A, B podobné (více viz Bečvář [2005]).

Příklad 10.20. Matice

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{a} \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

jsou si podobné skrze matici $S = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

Věta 10.21 (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. $\square$

Příklad 10.22. Ukažte, že podobnost jako binární relace je reflexivní, symetrická a tranzitivní. Tedy jedná se o relaci ekvivalenci. □

Uvědomme si, že věta neříká nic o vlastních vektorech, ty se měnit mohou. Vlastní čísla se ale podobnostní transformací nemění, tedy jestliže matici A převedeme podobnostní transformací na diagonální či obecněji trojúhelníkovou, tak na diagonále najdeme její vlastní čísla.

Definice 10.23 (Diagonalizovatelnost)**.** Matice $A \in \mathbb{C}^{n\times n}$ je *diagonalizovatelná*, pokud je podobná nějaké diagonální matici.

Příklad 10.24. Ne každá matice je diagonalizovatelná, např.

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

není. 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 10.25 (Charakterizace diagonalizovatelnosti)**.** *Matice $A \in \mathbb{C}^{n\times n}$ 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

$$AS_{*j} = (AS)_{*j} = (S\Lambda)_{*j} = S\Lambda_{*j} = S\Lambda_{jj}e_j = \Lambda_{jj}S_{*j},$$

což můžeme názorně zapsat jako

$$AS = A\begin{pmatrix} | & & | \\ S_{*1} & \dots & S_{*n} \\ | & & | \end{pmatrix} = \begin{pmatrix} | & & | \\ (\Lambda_{11}S_{*1}) & \dots & (\Lambda_{nn}S_{*n}) \\ | & & | \end{pmatrix} = S\Lambda.$$

Tedy Λ_{jj} je vlastní číslo a S_{*j} je příslušný vlastní vektor. Sloupce S jsou lineárně nezávislé díky regularitě matice.

Implikace „⇐“. Analogicky opačným směrem. Nechť A má vlastní čísla $\lambda_1, \dots, \lambda_n$ a jim přísluší lineárně nezávislé vlastní vektory $x_1, \dots, x_n$. Sestavme regulární matici $S \coloneqq (x_1 \mid \cdots \mid x_n)$ a diagonální $\Lambda \coloneqq \operatorname{diag}(\lambda_1, \dots, \lambda_n)$. Pak

$$(AS)_{*j} = AS_{*j} = Ax_j = \lambda_j x_j = \Lambda_{jj}S_{*j} = S(\Lambda_{jj}e_j) = S\Lambda_{*j} = (S\Lambda)_{*j}.$$

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 vlastních vektorů. Podobně i naopak ze znalosti diagonalizačního rozkladu $A = S\Lambda S^{-1}$ snadno určíme vlastní vektory (jsou to sloupce matice S v pořadí odpovídajícím vlastním číslům na diagonále Λ).

Jiný pohled na diagonalizaci je geometrický: víme, že vlastní vektor představuje invariantní směr při zobrazení $x \mapsto Ax$. Nyní si představme, že A představuje matici nějakého lineárního zobrazení $f\colon \mathbb{C}^{n\times n} \to \mathbb{C}^{n\times n}$ vzhledem 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.

Příklad 10.26 (Geometrická interpretace diagonalizace)**.** Buď

$$A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}.$$

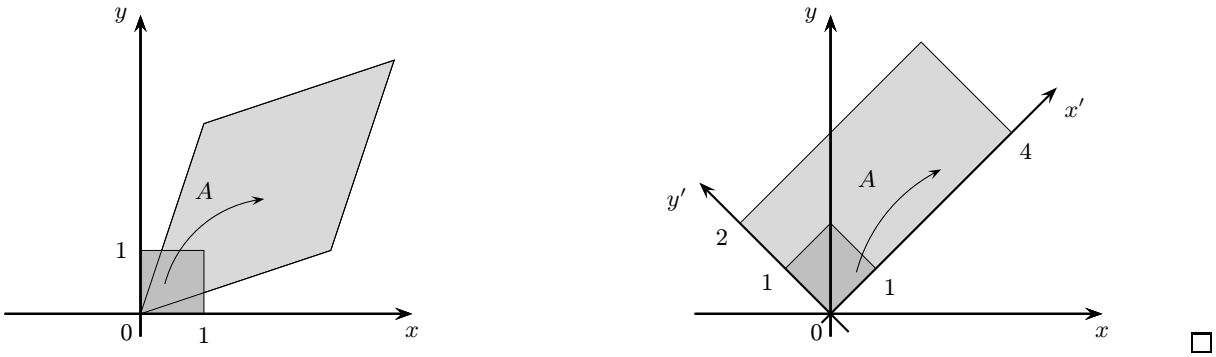
Vlastní čísla a vlastní vektory:

$$\lambda_1 = 4,\ x_1 = (1,1)^T, \quad \lambda_2 = 2,\ x_2 = (-1,1)^T.$$

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. Na obrázku dole je znázorněný jednotkový čtverec a jeho obraz při zobrazení $x \mapsto Ax$. Nalevo je situace, kdy pracujeme v souřadném systému kanonické báze, a napravo v souřadném systému báze z vlastních vektorů.



□

Nyní ukážeme, že různým vlastním číslům odpovídají lineárně nezávislé vlastní vektory.

Věta 10.27 (Vlastní vektory různých vlastních čísel)**.** *Nechť $\lambda_1, \ldots, \lambda_k$ jsou navzájem různá vlastní čísla (ne nutně všechna) matice $A \in \mathbb{C}^{n\times n}$. 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 dostaneme

$$A(\alpha_1 x_1 + \ldots + \alpha_k x_k) = \alpha_1 A x_1 + \ldots + \alpha_k A x_k = \alpha_1 \lambda_1 x_1 + \ldots + \alpha_k \lambda_k x_k = o. \tag{10.2}$$

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 10.28. *Pokud matice $A \in \mathbb{C}^{n\times n}$ má n navzájem různých vlastních čísel, pak je diagonalizovatelná.*

Nyní předvedeme několik teoretických i praktických aplikací diagonalizace.

Příklad 10.29 (Mocnina matice)**.** Buď $A = S\Lambda S^{-1}$ diagonalizace matice $A \in \mathbb{C}^{n\times n}$. 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 $-I_n$. □

Věta 10.30. *Buď $A, B \in \mathbb{C}^{n\times n}$. Pak AB i BA mají stejná vlastní čísla včetně násobností.*

Důkaz. Matice

$$\begin{pmatrix} AB & 0 \\ B & 0 \end{pmatrix} \quad \text{resp.} \quad \begin{pmatrix} 0 & 0 \\ B & BA \end{pmatrix}$$

jsou blokově trojúhelníkové, proto mají stejná vlastní čísla jako AB resp. BA, plus navíc n-násobné vlastní číslo 0. Nyní stačí ukázat shodu spekter obou blokových matic. Tyto matice jsou podobné skrze matici $S = \left(\begin{smallmatrix} I & A \\ 0 & I \end{smallmatrix}\right)$, neboť

$$\begin{pmatrix} AB & 0 \\ B & 0 \end{pmatrix}\begin{pmatrix} I & A \\ 0 & I \end{pmatrix} = \begin{pmatrix} AB & ABA \\ B & BA \end{pmatrix} = \begin{pmatrix} I & A \\ 0 & I \end{pmatrix}\begin{pmatrix} 0 & 0 \\ B & BA \end{pmatrix}$$ □

Předchozí věta platí i pro obdélníkové matice $A, B^T \in \mathbb{R}^{m\times n}$, ale znění platí pouze pro nenulová vlastní čísla; násobnost nulových vlastních čísel může být (a typicky je) odlišná.

Příklad 10.31 (Rekurentní vzorečky a Fibonacci)**.** Uvažujme posloupnost $a_1, a_2, \ldots$ zadanou rekurentním vztahem

$$a_n = pa_{n-1} + qa_{n-2},$$

kde a_1, a_2 jsou dané první hodnoty posloupnosti a p, q konstanty. Ukážeme, jak „rozbít“ rekurzi a vyjádřit explicitně n-tý prvek posloupnosti. Uvedený postup funguje i na složitější rekurze, kdy a_n závisí na více než dvou předchozích členech.

Rekurenci vyjádříme maticově

$$\begin{pmatrix} a_n \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} p & q \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_{n-1} \\ a_{n-2} \end{pmatrix}.$$

Označíme-li

$$x_n \coloneqq \begin{pmatrix} a_n \\ a_{n-1} \end{pmatrix}, \quad A = \begin{pmatrix} p & q \\ 1 & 0 \end{pmatrix},$$

pak rekurence má tvar

$$x_n = Ax_{n-1} = A^2x_{n-2} = \ldots = A^{n-2}x_2.$$

Potřebujeme tedy určit vyšší mocninu matice A. K tomu poslouží postup z Příkladu 10.29. Diagonalizujeme $A = S\Lambda S^{-1}$, a pak $x_n = S\Lambda^{n-2}S^{-1}x_2$. A jsme hotovi, explicitní vyjádření a_n je skryto v první složce vektoru $x_n = S\Lambda^{n-2}S^{-1}x_2$.

Ukažme si postup konkrétně pro Fibonacciho posloupnost, která je daná rekurencí $a_n = a_{n-1} + a_{n-2}$ a prvními členy $a_1 = a_2 = 1$. Označme $\varphi \coloneqq \frac{1}{2}(1 + \sqrt{5})$ hodnotu zlatého řezu. Nyní

$$x_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = S\Lambda S^{-1},$$

kde

$$S = \begin{pmatrix} -1 & \varphi \\ \varphi & 1 \end{pmatrix}, \quad S^{-1} = \frac{\sqrt{5}}{5}\begin{pmatrix} 1-\varphi & 1 \\ 1 & \varphi - 1 \end{pmatrix}, \quad \Lambda = \begin{pmatrix} 1-\varphi & 0 \\ 0 & \varphi \end{pmatrix}.$$

Tudíž

$$a_n = S_{1*}\Lambda^{n-2}S^{-1}x_2 = \frac{5-3\sqrt{5}}{10}(1-\varphi)^{n-2} + \frac{5+3\sqrt{5}}{10}\varphi^{n-2},$$

což se dá snadno přepsat do běžněji používaného tvaru

$$a_n = -\frac{\sqrt{5}}{5}(1-\varphi)^n + \frac{\sqrt{5}}{5}\varphi^n.$$ □

10.4 Jordanova normální forma

Víme, že ne všechny matice jsou diagonalizovatelné. Nicméně každou matici lze podobnostní transformací převést na poměrně jednoduchý tvar, nazývaný Jordanova normální forma.[3)]

[3)] Autorem je francouzský matematik Marie Ennemond Camille Jordan. Spolutvůrcem Gaussovy–Jordanovy eliminace je však někdo jiný, německý geodet Wilhelm Jordan.

Definice 10.32 (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, protože matice $J_k(\lambda) - \lambda I_k$ má hodnost $k-1$.

Definice 10.33 (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 10.34 (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. Úplný důkaz viz např. [Bečvář, 2005; Bican, 2009; Horn and Johnson, 1985]. Zde řekneme alespoň pár myšlenek z důkazu a konstrukce Jordanovy normální formy.

Bez újmu na obecnost buď $\lambda = 0$ vlastní číslo A, jinak použijeme transformaci $A - \lambda I_n$. Uvažujme podprostory $\mathbb{C}^n$:

$$\operatorname{Ker}(A) \subsetneqq \operatorname{Ker}(A^2) \subsetneqq \dots \subsetneqq \operatorname{Ker}(A^p) = \operatorname{Ker}(A^{p+1}) = \dots$$

Buď $v \in \operatorname{Ker}(A^p) \setminus \operatorname{Ker}(A^{p-1})$, a uvažujme bázi B tvořenou vektory $v, Av, \dots, A^{p-1}v$. Na podprostoru generovaném těmito vektory pak lineární zobrazení $x \mapsto Ax$ má matici vůči bázi B rovnou Jordanově buňce $J_p(0)$.

Podobně dostaneme i ostatní Jordanovy buňky, jen postup trochu zobecníme. Namísto vektoru v vezmeme systém vektorů $v_1, \dots, v_\ell$ o velikosti $\dim \operatorname{Ker}(A^p) - \dim \operatorname{Ker}(A^{p-1})$, který doplňuje nějakou bázi $\operatorname{Ker}(A^{p-1})$ na bázi $\operatorname{Ker}(A^p)$. Každý z těchto vektorů je zdrojem řetízku vektorů $v_i, Av_i, \dots, A^{p-1}v_i$, který odpovídá Jordanově buňce $J_p(0)$; těchto buněk je tedy ℓ. Pokud $\ell' := \dim \operatorname{Ker}(A^{p-1}) - \dim \operatorname{Ker}(A^{p-2}) - \ell > 0$, tak musíme vektory $Av_1, \dots, Av_\ell$ doplnit o nové vektory $v_{\ell+1}, \dots, v_{\ell+\ell'}$, aby opět doplňovaly nějakou bázi $\operatorname{Ker}(A^{p-2})$ na bázi $\operatorname{Ker}(A^{p-1})$. Tyto nové vektory se stanou základem řetízků $v_j, Av_j, \dots, A^{p-2}v_j$, které odpovídají ℓ' Jordanovým buňkám typu $J_{p-1}(0)$. Tento postup opakujeme až do dimenze 1. □

Příklad 10.35. 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

$$\begin{pmatrix} 5 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 7 & 0 & 0 \\ 0 & 0 & 0 & 7 & 1 \\ 0 & 0 & 0 & 0 & 7 \end{pmatrix}.$$

□

Jordanova normální forma je nestabilní v tom smyslu, že i nepatrná změna v původní matici způsobí skokovou změnu Jordanovy formy – není to tedy spojitá funkce vzhledem k prvkům matice A. To je také důvod, proč třeba výpočetní systém Maple odmítl zařadit výpočet Jordanovy formy do své knihovny.

Jak spočítat Jordanovu normální formu pro danou matici? Kromě vlastních čísel potřebujeme vědět ještě něco navíc. 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, neboť je-li $A = SJS^{-1}$, pak $\operatorname{rank}(A-\lambda I_n) = \operatorname{rank}(SJS^{-1}-\lambda SI_nS^{-1}) = \operatorname{rank}(S(J-\lambda I_n)S^{-1}) = \operatorname{rank}(J-\lambda I_n)$. Vzhledem k tomu, že každé Jordanově buňce odpovídá jeden vlastní vektor, tak jsme právě odvodili:

Tvrzení 10.36. *Počet všech Jordanových buněk odpovídajících λ je roven počtu vlastních vektorů pro λ.*

Jako důsledek dále dostáváme, že (algebraická) násobnost každého vlastního čísla λ je vždy větší nebo rovna počtu vlastních vektorů, které mu přísluší (tedy geometrické násobnosti).

Důsledek 10.37. *Násobnost vlastního čísla je větší nebo rovna počtu vlastních vektorů, které mu přísluší.*

Nicméně ani tyto znalosti ještě nemusí stačit k určení Jordanovy normální formy. Obecně potřebujeme znát ještě nějakou informaci navíc, např. jak to dělá následující vzoreček.

Poznámka 10.38 (Velikosti a počet buněk)**.** Počet buněk $J_k(\lambda)$ matice $A \in \mathbb{C}^{n\times n}$ ve výsledné Jordanově normální formě je roven

$$\operatorname{rank}\left((A-\lambda I_n)^{k-1}\right) - 2\operatorname{rank}\left((A-\lambda I_n)^{k}\right) + \operatorname{rank}\left((A-\lambda I_n)^{k+1}\right).$$

Důkaz viz např. Horn and Johnson [1985]; Meyer [2000]. Vzoreček je možno též odvodit z myšlenky důkazy Věty 10.34 o Jordanově normální formě.

V následujících příkladech ukážeme několik aplikací Jordanovy normální formy.

Příklad 10.39 (Mocnění matice)**.** Již v Příkladu 10.29 jsme 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

$$A^k = SJ^kS^{-1} = S\begin{pmatrix} J_{k_1}(\lambda_1)^k & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & J_{k_m}(\lambda_m)^k \end{pmatrix} S^{-1}.$$

Zde je třeba si trochu rozmyslet, jak se chovají mocniny Jordanových buněk $J_{k_i}(\lambda_i)^k$, $i = 1,\dots,m$. Asymptoticky pak dostaneme stejně jako pro diagonalizovatelné matice:

$$\lim_{k\to\infty} A^k = \begin{cases} 0, & \text{pokud } \rho(A) < 1, \\ \text{diverguje}, & \text{pokud } \rho(A) > 1, \\ \text{konverguje / diverguje}, & \text{pokud } \rho(A) = 1. \end{cases}$$

Příklad 10.40 (Maticová funkce)**.** Položme si otázku: Jak zavést maticovou funkci jako např. $\cos(A)$, e^A, atp.? Pro reálnou funkci $f\colon \mathbb{R}\to\mathbb{R}$ a matici $A \in \mathbb{R}^{n\times n}$ zavést $f(A)$ tak, že aplikujeme funkci na každou složku matice zvlášť,

$$f(A) = \begin{pmatrix} f(a_{11}) & \dots & f(a_{1n}) \\ \vdots & & \vdots \\ f(a_{n1}) & \dots & f(a_{nn}) \end{pmatrix}, \tag{10.3}$$

je sice možné, ale moc pěkných vlastností to mít nebude. Zkusme jiný přístup. Předpokládejme, že funkce $f\colon \mathbb{R}\to\mathbb{R}$ se dá vyjádřit nekonečným rozvojem $f(x) = \sum_{i=0}^{\infty} a_i x^i$; reálné analytické funkce jako např.

$\sin(x)$, $\exp(x)$ aj. tento předpoklad splňují. Pak je tedy přirozené zavést $f(A) = \sum_{i=0}^{\infty} a_i A^i$. Mocnit matice již umíme, proto je-li $A = SJS^{-1}$, tak

$$f(A) = \sum_{i=0}^{\infty} a_i S J^i S^{-1} = S f(J) S^{-1}.$$

Dále snadno nahlédneme, že

$$f(J) \coloneqq \begin{pmatrix} f(J_{k_1}(\lambda_1)) & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & f(J_{k_m}(\lambda_m)) \end{pmatrix}.$$

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]:

$$f(J_{k_i}(\lambda_i)) \coloneqq \begin{pmatrix} f(\lambda_i) & f'(\lambda_i) & \dots & \frac{f^{(k_i-1)}(\lambda_i)}{(k_i-1)!} \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & f'(\lambda_i) \\ 0 & \dots & 0 & f(\lambda_i) \end{pmatrix}.$$

Například funkce $f(x) = x^2$ má maticové rozšíření $f(A) = A^2$, jedná se tedy o klasické maticové mocnění. Na druhou stranu, předpis (10.3) by naznačoval mocnit jednotlivé prvky matice zvlášť, což není to, co bychom chtěli. □

Příklad 10.41 (Soustava lineárních diferenciálních rovnic)**.** Uvažme tzv. soustavu lineárních diferenciálních rovnic:

$$u(t)' = Au(t) \tag{10.4}$$

kde $A \in \mathbb{R}^{n\times n}$. Cílem je nalézt neznámou funkci $u\colon \mathbb{R} \to \mathbb{R}^n$ splňující tuto soustavu pro určitou počáteční podmínku tvaru $u(t_0) = u_0$. Pro případ $n = 1$ je řešením diferenciální rovnice $u(t)' = au(t)$ funkce $u(t) = v \cdot e^{at}$, kde $v \in \mathbb{R}^n$ je libovolné (volí se tak, aby byla splněna počáteční podmínka). To nás motivuje (ale je za tím hlubší teorie) hledat řešení obecného případu ve tvaru

$$u(t) = (u_1(t), \dots, u_n(t)) = (v_1 e^{\lambda t}, \dots, v_n e^{\lambda t}) = e^{\lambda t} v,$$

kde v_i, λ jsou neznámé, $i = 1, \dots, n$. Dosazením $u(t) \coloneqq e^{\lambda t} v$ do (10.4) dostaneme

$$\lambda e^{\lambda t} v = e^{\lambda t} A v, \quad \text{neboli} \quad \lambda v = Av.$$

To je přímo úloha výpočtu vlastních čísel a vektorů. Nechť matice A má vlastní čísla $\lambda_1, \dots, \lambda_n$ a vlastní vektory $x_1, \dots, x_n$. Pak řešení (10.4) je $u(t) = \sum_{i=1}^{n} \alpha_i e^{\lambda_i t} x_i$, kde $\alpha_i \in \mathbb{R}$ se získá z počátečních podmínek.

Uvažme konkrétní příklad:

$$u_1'(t) = 7u_1(t) - 4u_2(t)$$
$$u_2'(t) = 5u_1(t) - 2u_2(t)$$

Matice $A = \begin{pmatrix} 7 & -4 \\ 5 & -2 \end{pmatrix}$ má vlastní čísla 2 a 3, jim odpovídají vlastní vektory $(4,5)^T$ a $(1,1)^T$. Řešení úlohy jsou tvaru

$$\begin{pmatrix} u_1(t) \\ u_2(t) \end{pmatrix} = \alpha_1 e^{2t} \begin{pmatrix} 4 \\ 5 \end{pmatrix} + \alpha_2 e^{3t} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \alpha_1, \alpha_2 \in \mathbb{R}.$$

Pro řešení lineárních diferenciálních rovnic je tedy znalost vlastních čísel a vlastních vektorů důležitá. Jordanova normální forma se použije, pokud matice A není diagonalizovatelná a deficience počtu vlastních vektorů se projeví tím, že ve vyjádření $u(t)$ nebudou α_i již skaláry, ale polynomy proměnné t stupňů odpovídajících násobnostem λ_i. □

10.5 Symetrické matice

Reálné symetrické matice mají řadu pozoruhodných vlastností týkající se vlastních čísel. Jsou vždy diagonalizovatelné a jejich vlastní čísla jsou reálná.

Nejprve se podívejme na zobecnění transpozice a symetrických matic pro komplexní matice.

Definice 10.42 (Hermitovská matice a transpozice)**.** *Hermitovská transpozice*[4] 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 $A^* = A$.

Hermitovská transpozice má podobné vlastnosti jako klasická transpozice, např. $(A^*)^* = A$, $(\alpha A)^* = \overline{\alpha}A^*$, $(A+B)^* = A^* + B^*$, $(AB)^* = B^*A^*$.

Pomocí hermitovské transpozice můžeme unitární matice (rozšiřující pojem ortogonální matice pro komplexní matice, viz Definice 8.41) definovat jako matice $Q \in \mathbb{C}^{n\times n}$ splňující $Q^*Q = I_n$.

Příklad 10.43. Z matic

$$\begin{pmatrix} 2 & 1+i \\ 1+i & 5 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1+i \\ 1-i & 5 \end{pmatrix}$$

je první symetrická, ale ne hermitovská, a druhá je hermitovská, ale ne symetrická. Pro reálné matice oba pojmy splývají. □

Věta 10.44 (Vlastní čísla symetrických matic)**.** *Vlastní čísla reálných symetrických (resp. komplexních hermitovských) jsou reálná.*

Důkaz. Buď $A \in \mathbb{C}^{n\times n}$ a buď $\lambda \in \mathbb{C}$ její 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 $x^*Ax = \lambda x^*x = \lambda$. Nyní

$$\lambda = x^*Ax = x^*A^*x = (x^*Ax)^* = \lambda^*.$$

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[5]. Navíc jsou diagonalizovatelné specifickým způsobem: z vlastních vektorů lze vybrat ortonormální systém, tedy matice podobnosti je ortogonální.

Věta 10.45 (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 8.21), na ortogonální matici $S \coloneqq (x \mid \cdots)$. Protože $(A - \lambda I_n)x = o$, máme $(A - \lambda I_n)S = (o \mid \cdots)$, a tudíž $S^T(A - \lambda I_n)S = S^T(o \mid \cdots) = (o \mid \cdots)$. A jelikož je tato matice 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:

$$\begin{pmatrix} 0 & o^T \\ o & A' \end{pmatrix} = \begin{pmatrix} 1 & o^T \\ o & Q' \end{pmatrix} \begin{pmatrix} 0 & o^T \\ o & \Lambda' \end{pmatrix} \begin{pmatrix} 1 & o^T \\ o & Q'^T \end{pmatrix},$$

což snadno můžeme ověřit pronásobením. Označme

$$R \coloneqq \begin{pmatrix} 1 & o^T \\ o & Q' \end{pmatrix}, \quad \Lambda'' \coloneqq \begin{pmatrix} 0 & o^T \\ o & \Lambda' \end{pmatrix}.$$

[4] Charles Hermite (1822–1901) byl francouzský matematik. Dokázal mj., že e je transcendentní, to jest není kořenem žádné polynomu s racionálními koeficienty.

[5] A.L. Cauchy, r. 1829.

Matice R je ortogonální (Věta 8.45(4)), matice Λ'' diagonální. Nyní můžeme psát

$$S^T(A - \lambda I_n)S = R\Lambda'' R^T,$$

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 $Q \coloneqq SR$ je ortogonální matice a $\Lambda \coloneqq \Lambda'' + \lambda I_n$ je diagonální. □

Podobně můžeme spektrálně rozložit hermitovské matice $A = Q\Lambda Q^*$, kde Q je unitární matice.

Poznámka 10.46 (Jiná forma spektrálního rozkladu)**.** Nechť symetrická $A \in \mathbb{R}^{n\times n}$ má vlastní čísla $\lambda_1, \ldots, \lambda_n$ a odpovídající ortonormální vlastní vektory $x_1, \ldots, x_n$. Tedy ve spektrálním rozkladu $A = Q\Lambda Q^T$ je $\Lambda_{ii} = \lambda_i$ a $Q_{*i} = x_i$. Upravme

$$A = Q\Lambda Q^T = Q\left(\sum_{i=1}^n \lambda_i e_i e_i^T\right)Q^T = \sum_{i=1}^n \lambda_i Q e_i e_i^T Q^T = \sum_{i=1}^n \lambda_i Q_{*i} Q_{*i}^T = \sum_{i=1}^n \lambda_i x_i x_i^T.$$

Tvar $A = \sum_{i=1}^n \lambda_i x_i x_i^T$ je tak alternativní vyjádření spektrálního rozkladu, ve kterém matici A rozepisujeme na součet n matic hodnosti 0 nebo 1.

Jedním z pěkných důsledků je následující, byť trochu teoretický, vzoreček na výpočet největšího a nejmenšího vlastního čísla[6)]. Říká, že největší resp. nejmenší vlastní číslo se dá vyjádřit jako největší resp. nejmenší hodnota kvadratické funkce $f(x) = x^T Ax$ na jednotkové sféře.

Věta 10.47 (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 $y \coloneqq Q^T x$, pak $\|y\|_2 = 1$ (Věta 8.45(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

Perronova–Frobeniova teorie nezáporných matic[7)] je pokročilá teorie kolem vlastních čísel nezáporných matic. Uvedeme jen základní výsledek bez důkazu.

Věta 10.48 (Perronova)**.**

(1) Buď $A \in \mathbb{R}^{n\times n}$ nezáporná matice (tj. $a_{ij} \geq 0$ pro všechna i, j). Pak největší (v absolutní hodnotě) vlastní číslo je reálné nezáporné a příslušný vlastní vektor je nezáporný (ve všech složkách).

[6)] 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.

[7)] Základní věta je od německého matematika Oskara Perrona z r. 1907, a byla rozšířena Ferdinandem Georgem Frobeniem r. 1912.

(2) Buď $A \in \mathbb{R}^{n\times n}$ kladná matice (tj. $a_{ij} > 0$ pro všechna 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 10.49 (Markovovy řetězce)**.** Jedním z využití mocnin matice (Příklad 10.39) a trochu i teorie nezáporných matic jsou Markovovy řetězce.[8)] Ilustrujeme si je na konkrétním příkladu:

Migrace obyvatel USA město–předměstí–venkov probíhá každoročně 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. obyvatel ve městě, 142 mil. na předměstí a 60 mil. na venkově. Jak se bude situace vyvíjet v čase? Označme

$$A \coloneqq \begin{pmatrix} 0.96 & 0.01 & 0.015 \\ 0.03 & 0.98 & 0.005 \\ 0.01 & 0.01 & 0.98 \end{pmatrix}, \quad x_0 = (58, 142, 60)^T.$$

V nultém roce je rozmístění obyvatel dáno vektorem x_0 a v prvním roce vektorem Ax_0, protože Ax_0 má v první složce výsledný počet obyvatel ve městě po jednoroční migraci a podobně v druhé a třetí složce pro předměstí a venkov. Vývoj v čase probíhá tedy takto: x_0, Ax_0, A^2x_0, A^3x_0, …,$A^\infty x_0$. Diagonalizací spočítáme

$$A = Q \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0.95 & 0 \\ 0 & 0 & 0.97 \end{pmatrix} Q^{-1}.$$

z čehož

$$\lim_{k\to\infty} A^k = Q \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} Q^{-1} = Q_{*1} Q_{1*}^{-1} = \begin{pmatrix} 0.23 & 0.23 & 0.23 \\ 0.43 & 0.43 & 0.43 \\ 0.33 & 0.33 & 0.33 \end{pmatrix}.$$

Tedy (bez ohledu na počáteční stav x_0) se rozložení obyvatelstva ustálí na hodnotách: 23% ve městě, 43% předměstí, 33% venkov.

Tento příklad ilustruje ještě jednu věc. Má-li vlastní číslo 1 násobnost jedna a ostatní vlastní čísla jsou v absolutní hodnotě menší (což nastane např. pokud A je kladná), tak $A^\infty = Q_{*1} Q_{1*}^{-1}$, kde Q_{*1} je vlastní vektor A k číslu 1, a $Q_{1*}^{-1} = (1, \ldots, 1)^T$ je vlastní vektor A^T k číslu 1. Tudíž sloupce A^∞ budou opět stejné, a výsledné rozložení odpovídá složkám vlastního vektoru Q_{*1} (ty jsou kladné, podle Perronovy věty). Takže v tomto případě stačí jen spočítat kladný vektor z $\operatorname{Ker}(A - I_n)$, což odpovídá intuici, že ustálené rozložení representované vektorem v má splňovat $Av = v$. □

10.7 Výpočet vlastních čísel

Jak jsme již zmínili (poznámky k Větě 10.15), vlastní čísla se počítají veskrze numerickými iteračními metodami, a hledat je jako kořeny charakteristického polynomu není efektivní postup. V této sekci 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[9)] (viz [Meyer, 2000]).

[8)] Andrej Andrejevič Markov (1856–1922), ruský matematik. Tvrdí se, že první aplikací Markovových řetězců byla analýza distribuce samohlásek a souhlásek v Puškinově Evženu Oněginovi, kdy vytvořil model předpokládající, že pravděpodobnost výskytu samohlásky či souhlásky na dané pozici závisí jen na posledním předchozím znaku, ale na žádném z předešlých už nikoli. Tato jednoduchá Markovova vlastnost se pak stala základem Markovových řetězců. Více o této lingvistické aplikaci se dočtete např. v *Učiteli matematiky*, 1–2(77–78), roč. 19, 2010–2011.

[9)] Algoritmus pochází z r. 1950 od maďarského matematika Cornelia Lanczose.

Nejprve uvedeme jednoduchý odhad pro vlastní čísla, tzv. Gerschgorinovy disky[10].

Věta 10.50 (Gerschgorinovy disky)**.** *Každé vlastní číslo λ matice $A \in \mathbb{C}^{n\times n}$ leží v kruhu o středu a_{ii} a poloměru $\sum_{j\neq i} |a_{ij}|$ pro nějaké $i \in \{1,\dots,n\}$.*

Důkaz. Buď λ vlastní číslo a x odpovídající vlastní vektor, tedy $Ax = \lambda x$. Nechť i-tá složka x má největší absolutní hodnostu, tj. $|x_i| = \max_{k=1,\dots,n} |x_k|$. Protože i-tá rovnice má tvar $\sum_{j=1}^{n} a_{ij}x_j = \lambda x_i$, vydělením $x_i \neq 0$ dostáváme

$$\lambda = a_{ii} + \sum_{j\neq i} a_{ij}\frac{x_j}{x_i}$$

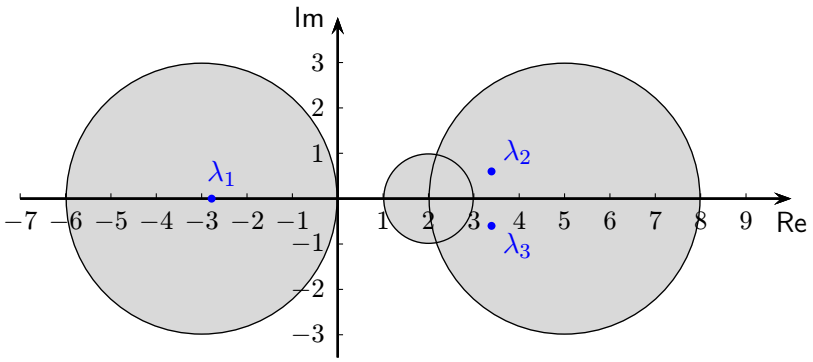
a tím pádem

$$|\lambda - a_{ii}| = \Big|\sum_{j\neq i} a_{ij}\frac{x_j}{x_i}\Big| \leq \sum_{j\neq i} |a_{ij}|\frac{|x_j|}{|x_i|} \leq \sum_{j\neq i} |a_{ij}|. \qquad \square$$

Příklad 10.51. Mějme

$$A = \begin{pmatrix} 2 & 1 & 0 \\ -2 & 5 & 1 \\ -1 & -2 & -3 \end{pmatrix}.$$

Vlastní čísla matice A 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. $\square$

Věta dává jednoduchý odhad na velikost vlastních čísel (existují i vylepšení, např. Cassiniho ovály aj.). 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[11] pro regularitu matice $A \in \mathbb{C}^{n\times n}$: $|a_{ii}| > \sum_{j\neq i} |a_{ij}|\ \forall i = 1,\dots,n$. V tomto případě totiž disky neobsahují počátek a proto nula není vlastním číslem A. Matice s touto vlastností se nazývají *diagonálně dominantní*.

Nyní ukážeme jednoduchou metodu na výpočet dominantního vlastního čísla.[12] Přes svou jednoduchost se stala základem některých numerických metod jako je např. inverzní mocninná metoda[13], nebo metoda Rayleighova podílu[14] pro symetrické matice.

[10] 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).

[11] Tzv. Lévyho–Desplanquesova věta.

[12] Mocninou metodu, anglicky *power method*, představil americký matematik a fyzik Richard Edler von Mises r. 1929.

[13] Autorem je německý matematik Helmut Wielandt, z r. 1944, anglicky *inverse iteration*.

[14] Autorem anglický fyzik John William Strutt, lord Rayleigh, nositel Nobelovy ceny za fyziku (1904), anglicky *Rayleigh quotient iteration*.

Algoritmus 10.52 (Mocninná metoda)**.** Buď $A \in \mathbb{C}^{n\times n}$.

1: Zvol $o \neq x_0 \in \mathbb{C}^n$, $i \coloneqq 1$,
2: **while not** splněna ukončovací podmínka **do**
3: $\quad y_i \coloneqq Ax_{i-1}$,
4: $\quad x_i \coloneqq \frac{1}{\|y_i\|_2} y_i$,
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 10.53. 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	$\frac{1}{\|x_i\|_\infty} x_i$	$x_{i-1}^T y_i$
0	$(1.00, 0.00, 1.00)^T$	–
1	$(0.67, 1.00, 0.17)^T$	5
2	$(1.00, 0.88, 0.56)^T$	6.32
3	$(0.97, 1.00, 0.47)^T$	6.94
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=1:4
  y=A*x;
  (y'*x),
  x=y/norm(y);
  x/max(abs(x)),
end
```

□

Metodu ukončíme ve chvíli, když se hodnota $x_{i-1}^T y_i$ resp. vektor x_i ustálí; potom $x_i \approx x_{i-1}$ je odhad vlastního vektoru a $x_{i-1}^T y_i = x_{i-1}^T A x_{i-1} \approx x_{i-1}^T \lambda x_{i-1} \approx \lambda$ odhad odpovídajícího vlastního čísla. 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 aplikovatelná na velké řídké matice. Ne vždy konverguje, ale za určitých předpokladů se to dá zajistit.

Věta 10.54 (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 (až na znaménko) k vlastnímu vektoru v_1 a $x_{i-1}^T y_i$ konverguje k vlastnímu číslu 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

$$A^i x_0 = A^i \Big(\sum_{j=1}^n \alpha_j v_j \Big) = \sum_{j=1}^n \alpha_j A^i v_j = \sum_{j=1}^n \alpha_j \lambda_j^i v_j = \lambda_1^i \Big(\alpha_1 v_1 + \sum_{j\neq 1} \alpha_j \Big(\frac{\lambda_j}{\lambda_1}\Big)^i v_j \Big).$$

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 $x_{i-1}^T y_i = x_{i-1}^T A x_{i-1} = x_{i-1}^T \lambda_1 x_{i-1} = \lambda_1 \|x_{i-1}\|_2^2 = \lambda_1$. □

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 10.12).

Mocninná metoda počítá jen dominantní vlastní číslo a vektor. Následující technika ale umožňuje jednoduchou transformací vynulovat jedno vlastní číslo, např. to dominantní, a pak můžeme rekurzivně dopočítat mocninnou metodou i zbylá vlastní čísla. Pro jednoduchost uvádíme verzi pro symetrické matice.

Věta 10.55 (O deflaci 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. Podle Poznámky 10.46 lze psát $A = \sum_{i=1}^{n} \lambda_i v_i v_i^T$. Pak $A - \lambda_1 v_1 v_1^T = 0 v_1 v_1^T + \sum_{i=2}^{n} \lambda_i v_i v_i^T$, což je spektrální rozklad matice $A - \lambda_1 v_1 v_1^T$. □

Příklad 10.56 (Vyhledávač Google™ a PageRank[15]). Uvažujme webovou síť s těmito parametry:

$$\begin{aligned} &N \text{ webových stránek,} \\ &a_{ij} = \begin{cases} 1 & j\text{-tá stránka odkazuje na } i\text{-tou,} \\ 0 & \text{jinak,} \end{cases} \\ &b_j = \text{počet odkazů z } j\text{-té stránky,} \\ &x_i = \text{důležitost } i\text{-té stránky.} \end{aligned}$$

Cílem je stanovit důležitosti $x_1, \ldots, x_N$ jednotlivých stránek. Základní myšlenka autorů googlovského PageRanku spočívá ve stanovení důležitosti i-té stránky 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 $a'_{ij} := \frac{a_{ij}}{b_j}$. Tedy x je vlastní vektor matice A příslušný 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, tedy všechny Gerschgorinovy disky mají nejpravější konec v bodě 1). Podle Perronovy Věty 10.48 je vlastní vektor x nezáporný. Ten pak normujeme a složky zaokrouhlíme, aby měly hodnoty v rozmezí $0, 1, 2, \ldots, 10$.

V praxi je matice A' obrovská, řádově $\approx 10^{10}$, 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 tzv. stochastická, aperiodická a ireducibilní (vadilo by např. pokud by z nějaké stránky nebyl odkaz na žádnou jinou), více viz [Langville and Meyer, 2006; Tůma, 2003].

Na matici A' se můžeme dívat i z pohledu Markovových řetězců (Příklad 10.49). Pokud budeme symbolicky procházet po webové síti a se stejnou pravděpodobností se na každé stránce rozhodneme, kam pokračovat, tak A' odpovídá přechodové matici a hledaný vektor x rovnovážnému stavu.

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

□

Problémy

10.1. Buď $A \in \mathbb{R}^{n \times n}$ singulární. Dokažte, že existuje posloupnost regulárních matic A_i, $i = 1, \ldots,$ konvergující po složkách k A. (Množina regulárních matic je tzv. *hustá* v $\mathbb{R}^{n \times n}$)

10.2. Dokažte přímo Cayleyho–Hamiltonovu Větu 10.17 pro diagonalizovatelné matice.

10.3. Ukažte, že každá matice $A \in \mathbb{R}^{n \times n}$ má invariantní podprostor dimenze 1 nebo 2.

10.4. Dokažte následující odhad pro hodnost druhé mocniny matice $A \in \mathbb{R}^{n \times n}$

$$\operatorname{rank}(A) - \tfrac{n}{2} \leq \operatorname{rank}(A^2) \leq \operatorname{rank}(A).$$

10.5. Domyslete detaily důkazu Věty 10.34 o Jordanově normální formě:

(a) Ukažte, že pro každou matici $A \in \mathbb{C}^{n \times n}$ existuje $p \in \mathbb{N}$ takové, že

$$\operatorname{Ker}(A) \subsetneqq \operatorname{Ker}(A^2) \subsetneqq \cdots \subsetneqq \operatorname{Ker}(A^p) = \operatorname{Ker}(A^{p+1}) = \ldots$$

(b) Buď $v \in \operatorname{Ker}(A^p) \setminus \operatorname{Ker}(A^{p-1})$. Ukažte, že vektory $v, Av, \ldots, A^{p-1}v$ jsou lineárně nezávislé.

(c) Dokažte vzoreček z Poznámky 10.38 o velikostech a počtu Jordanových buněk.

[15] 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 semidefinitní*, pokud $x^TAx \geq 0$ pro všechna $x \in \mathbb{R}^n$, a A je *positivně definitní*, pokud $x^TAx > 0$ pro všechna $x \neq o$.

Zřejmě, je-li A positivně definitní, pak je i positivně semidefinitní.

Kromě positivně (semi-)definitních matic lze zavést i negativně (semi-)definitní matice pomocí obrácené nerovnosti. Zabývat se jimi nebudeme, protože A je negativně (semi-)definitní právě tehdy, když $-A$ je positivně (semi-)definitní, čili vše se redukuje na základní případ.

Poznámka 11.2. Definice dává smysl i pro nesymetrické matice, ale ty můžeme snadno zesymetrizovat úpravou $\frac{1}{2}(A + A^T)$, neboť

$$x^T\tfrac{1}{2}(A + A^T)x = \tfrac{1}{2}x^TAx + \tfrac{1}{2}x^TA^Tx = \tfrac{1}{2}x^TAx + \left(\tfrac{1}{2}x^TAx\right)^T = x^TAx.$$

Tedy pro testování podmínky lze ekvivalentně 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 11.3. Příkladem positivně semidefinitní matice je 0_n. Příkladem positivně definitní matice je I_n, neboť $x^TAx = x^TI_nx = x^Tx = \|x\|_2^2 > 0$ pro všechna $x \neq o$. □

Poznámka 11.4 (Nutná podmínka pro positivní (semi-)definitnost)**.** Buď $A \in \mathbb{R}^{n\times n}$ symetrická matice. Aby byla positivně semidefinitní, musí podle definice $x^TAx \geq 0$ pro všechna $x \in \mathbb{R}^n$. Postupným dosazením $x = e_i$, $i = 1, \ldots, n$, dostaneme $x^TAx = e_i^TAe_i = a_{ii} \geq 0$. Tím pádem, positivně semidefinitní matice musí mít nezápornou diagonálu a positivně definitní matice dokonce kladnou.

Poznámka 11.5. Matice $A = (a) \in \mathbb{R}^{1\times 1}$ je positivně semidefinitní právě tehdy, když $a \geq 0$, a positivně definitní právě tehdy, když $a > 0$. Tím pádem se můžeme dívat na positivní semidefinitnost jako na zobecnění pojmu nezápornosti z čísel na matice. Proto se také positivní semidefinitnost matice $A \in \mathbb{R}^{n\times n}$ značívá $A \succeq 0$ (narozdíl od $A \geq 0$, což se používá pro nezápornost v každé složce).

Věta 11.6 (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, dokážeme pouze tu třetí.

Nejprve ověříme 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 $y = A^{-1}x \neq o$. 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 obecně neplatí.

Součinem positivně definitních matic se zabýváme v Příkladu 12.16.

Následující věta dává důležitou charakterizaci positivně definitních matic jednak pomocí vlastních čísel a jednak pomocí tvaru U^TU; s tímto výrazem jsme se skrytě setkali už např. v metodě nejmenších čtverců (Sekce 8.5) nebo obecně při explicitním vyjádření ortogonální projekce v $\mathbb{R}^n$ (Věta 8.36).

Věta 11.7 (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 matice $U \in \mathbb{R}^{m\times n}$ hodnosti n taková, že $A = U^TU$.

Důkaz. Implikace (1) $\Rightarrow$ (2): Sporem nechť existuje vlastní číslo $\lambda \leq 0$, a x je příslušný vlastní vektor s eukleidovskou normou 1. Pak $Ax = \lambda x$ implikuje $x^TAx = \lambda x^Tx = \lambda \leq 0$. To je spor s positivní definitností A.

Implikace (2) $\Rightarrow$ (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 $U^TU = Q\Lambda'\Lambda'Q^T = Q\Lambda'^2Q^T = Q\Lambda Q^T = A$. Uvědomme si, že U má hodnost n a je tudíž regulární, neboť je součinem dvou regulárních matic.

Implikace (3) $\Rightarrow$ (1): Sporem nechť $x^TAx \leq 0$ pro nějaké $x \neq o$. Pak $0 \geq x^TAx = x^TU^TUx = (Ux)^TUx = \langle Ux, Ux\rangle = \|Ux\|_2^2$. 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 11.8 (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 matice $U \in \mathbb{R}^{m\times n}$ taková, že $A = U^TU$.

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 použít ani jednoduše přizpůsobit nelze.

Věta 11.9 (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 $x^TAx > 0$ pro všechny $x \neq o$, tedy speciálně pro $x = e_1$ dostáváme $\alpha = e_1^TAe_1 > 0$. Dále, buď $\tilde{x} \in \mathbb{R}^{n-1}$, $\tilde{x} \neq o$. Pak

$$\tilde{x}^T\big(\tilde{A} - \tfrac{1}{\alpha}aa^T\big)\tilde{x} = \tilde{x}^T\tilde{A}\tilde{x} - \tfrac{1}{\alpha}(a^T\tilde{x})^2 = \begin{pmatrix} -\frac{1}{\alpha}a^T\tilde{x} & \tilde{x}^T \end{pmatrix}\begin{pmatrix} \alpha & a^T \\ a & \tilde{A} \end{pmatrix}\begin{pmatrix} -\frac{1}{\alpha}a^T\tilde{x} \\ \tilde{x} \end{pmatrix} > 0.$$

Implikace „⇐“. Buď $x = \left(\begin{smallmatrix} \beta \\ \tilde{x} \end{smallmatrix}\right) \in \mathbb{R}^n$. Pak

$$\begin{aligned} x^TAx &= \begin{pmatrix} \beta & \tilde{x}^T \end{pmatrix}\begin{pmatrix} \alpha & a^T \\ a & \tilde{A} \end{pmatrix}\begin{pmatrix} \beta \\ \tilde{x} \end{pmatrix} = \alpha\beta^2 + 2\beta a^T\tilde{x} + \tilde{x}^T\tilde{A}\tilde{x} \\ &= \tilde{x}^T\big(\tilde{A} - \tfrac{1}{\alpha}aa^T\big)\tilde{x} + \big(\sqrt{\alpha}\beta + \tfrac{1}{\sqrt{\alpha}}a^T\tilde{x}\big)^2 \geq 0. \end{aligned}$$

Rovnost nastane pouze tehdy, 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 11.10 (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 taková, 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 $A = \begin{pmatrix} \alpha & a^T \\ a & \tilde{A} \end{pmatrix}$. Podle Věty 11.9 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 $L = \begin{pmatrix} \sqrt{\alpha} & o^T \\ \frac{1}{\sqrt{\alpha}}a & \tilde{L} \end{pmatrix}$, neboť

$$LL^T = \begin{pmatrix} \sqrt{\alpha} & o^T \\ \frac{1}{\sqrt{\alpha}}a & \tilde{L} \end{pmatrix} \begin{pmatrix} \sqrt{\alpha} & \frac{1}{\sqrt{\alpha}}a^T \\ o & \tilde{L}^T \end{pmatrix} = \begin{pmatrix} \alpha & a^T \\ a & \frac{1}{\alpha}aa^T + \tilde{L}\tilde{L}^T \end{pmatrix} = A.$$

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: $\beta = \sqrt{\alpha}$, $b = \frac{1}{\sqrt{\alpha}}a$ 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. Odvození a výsledný postup jsou popsány níže. Jestliže A je positivně definitní, algoritmus najde rozklad, a pokud A není, tak to algoritmus ohlásí.

Algoritmus 11.11 (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** $A = LL^T$.

[1)] André-Louis Cholesky, francouzský důstojník (pravděpodobně polského 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.

Odvození Choleského rozkladu. Předpokládejme, že máme spočítaný první až $(k-1)$-ní sloupec matice L. Ze vztahu $A = LL^T$ odvodíme

$$a_{kk} = \sum_{j=1}^{n} L_{kj}(L^T)_{jk} = \sum_{j=1}^{n} l_{kj}^2.$$

Jediná neznámá v tomto vztahu je hodnota l_{kk}, a pokud ji z rovnice vyjádříme, dostaneme výraz z kroku 4:.

Nyní předpokládejme, že z matice L máme navíc určeny hodnoty prvních $i-1$ prvků sloupce k. Ze vztahu $A = LL^T$ odvodíme

$$a_{ik} = \sum_{j=1}^{n} L_{ij}(L^T)_{jk} = \sum_{j=1}^{n} l_{ij}l_{kj}.$$

V tomto výrazu je jediná neznámá hodnota l_{ik} a jejím vyjádřením dostaneme vzorec z kroku 6:. □

Příklad 11.12. Choleského rozklad matice A:

$$\begin{array}{c|c} & L^T \\ \hline L & A \end{array} \quad \equiv \quad \begin{array}{c|c} & \begin{pmatrix} 2 & -1 & 2 \\ 0 & 3 & 1 \\ 0 & 0 & 1 \end{pmatrix} \\ \hline \begin{pmatrix} 2 & 0 & 0 \\ -1 & 3 & 0 \\ 2 & 1 & 1 \end{pmatrix} & \begin{pmatrix} 4 & -2 & 4 \\ -2 & 10 & 1 \\ 4 & 1 & 6 \end{pmatrix} \end{array}$$

□

Příklad 11.13. Použití Choleského rozkladu pro řešení soustavy $Ax = b$ s positivně definitní maticí A. Pokud máme rozklad $A = LL^T$, pak soustava má tvar $L(L^Tx) = b$. Nejprve vyřešíme soustavu $Ly = b$, potom $L^Tx = y$ 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 $L^Tx = y^*$ pomocí zpětné substituce.

Tento postup je řádově o 50% rychlejší než řešení Gaussovou eliminací.

Choleského rozklad můžeme použít i k invertování positivně definitních matic, protože $A^{-1} = (LL^T)^{-1} = (L^{-1})^TL^{-1}$ a inverze k dolní trojúhelníkové matici L se najde snadno. □

Rekurentní vzoreček má ještě další důsledky, které vyjadřují, jak testovat positivní definitnost pomocí Gaussovy–Jordanovy eliminace a pomocí determinantů.

Věta 11.14 (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 $A = \left(\begin{smallmatrix} \alpha & a^T \\ a & \tilde{A} \end{smallmatrix}\right)$ positivně definitní. První krok Gaussovy eliminace převede matici na tvar $\left(\begin{smallmatrix} \alpha & a^T \\ o & \tilde{A} - \frac{1}{\alpha}aa^T \end{smallmatrix}\right)$. Podle Věty 11.9 je $\alpha > 0$ a $\tilde{A} - \frac{1}{\alpha}aa^T$ je zase positivně definitní, takže můžeme pokračovat induktivně dál. □

Věta 11.15 (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 $x^TA_ix \le 0$ pro jisté $x \neq o$, tak $(x^T\, o^T)A\left(\begin{smallmatrix} x \\ o \end{smallmatrix}\right) = x^TA_ix \le 0$. 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 $\det(A_i) \le 0$. Podle Věty 11.14 je tedy A positivně definitní. □

[2)] James Joseph Sylvester, anglický matematik, spoluzakladatel teorie matic. Jako první použil pojem „matice“ v práci z r. 1850. Kriterium je z r. 1852.

Z nezápornosti determinantů všech hlavních vedoucích matic ještě positivní semidefinitnost nevyplývá (najděte takový příklad!). Analogie Sylvestrovy podmínky pro positivně semidefinitností matice je následující, uvádíme ji bez důkazu.

Věta 11.16 (Sylvestrovo kriterium positivní semidefinitnosti)**.** *Symetrická matice $A \in \mathbb{R}^{n\times n}$ je positivně semidefinitní právě tehdy, když determinanty všech hlavních matic jsou nezáporné, přičemž hlavní matice je matice, která vznikne z A odstraněním určitého počtu (i nulového) řádků a sloupců s týmiž indexy.*

Důkaz. Viz Meyer [2000]. □

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 ukážeme později v Sekci 12.2 (Důsledek 12.13).

Přestože jsme uvedli několik metod na testování positivní definitnosti, některé jsou si dost podobné. Důkaz Věty 11.14 ukazuje, že rekurentní vzoreček a Gaussova eliminace fungují v podstatě stejně. A pokud počítáme determinanty Gaussovou eliminací, tak i Sylvestrovo pravidlo je varianta prvních dvou. Naproti tomu Choleského rozklad je metoda principiálně odlišná.

11.2 Aplikace

Věta 11.17 (Skalární součin a positivní definitnost)**.** *Operace $\langle x, y\rangle$ je skalárním součinem v $\mathbb{R}^n$ právě tehdy, když má tvar $\langle x, y\rangle = x^T Ay$ pro nějakou positivně definitní matici $A \in \mathbb{R}^{n\times n}$.*

Důkaz. Implikace „⇒“. Definujme matici $A \in \mathbb{R}^{n\times n}$ předpisem $a_{ij} = \langle e_i, e_j\rangle$. Ta je zjevně symetrická. Pak

$$\langle x, y\rangle = \Big\langle \sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} y_j e_j \Big\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j a_{ij} = x^T Ay.$$

Matice A je positivně definitní, neboť $\langle x, x\rangle = x^T Ax \geq 0$ a nulové jen pro $x = o$.

Implikace „⇐“. Nechť A je positivně definitní. Pak $\langle x, y\rangle = x^T Ay$ tvoří skalární součin: $\langle x, x\rangle = x^T Ax \geq 0$ a nulové jen pro $x = o$, je lineární v první složce a je symetrický neboť

$$\langle x, y\rangle = x^T Ay = (x^T Ay)^T = y^T A^T x = y^T Ax = \langle y, x\rangle.$$ □

Víme, že skalární součin indukuje normu (Definice 8.4). Norma indukovaná výše zmíněným skalárním součinem je $\|x\| = \sqrt{x^T Ax}$. V této normě je jednotková koule elipsoid (viz Příklad 12.17). 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 11.18 (Odmocnina z matice)**.** *Pro každou positivně semidefinitní matici $A \in \mathbb{R}^{n\times n}$ existuje positivně semidefinitní matice $B \in \mathbb{R}^{n\times n}$ taková, 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 $B^2 = Q\Lambda' Q^T Q\Lambda' Q^T = Q\Lambda'^2 Q^T = Q\Lambda Q^T = A$. □

Zde je zajímavé porovnat odmocninu z matice s maticovými funkcemi z Příkladu 10.40. Odmocninu lze vyjádřit nekonečným rozvojem pouze v malém okolí daného kladného čísla, nicméně tam, kde existuje, se budou obě definice shodovat.

Poznámka 11.19. 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].

Positivně definitní matice hrají v optimalizaci ještě jednu důležitou roli. Semidefinitní program je taková optimalizační úloha, při níž hledáme minimum lineární funkce za podmínky na positivní semidefinitnost matice, jejíž prvky jsou lineární funkcí proměnných [Gärtner and Matoušek, 2012]. Formálně, jedná se o úlohu

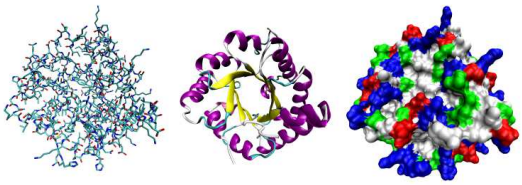
$$\min c^T x \text{ za podmínky } A_0 + \sum_{i=1}^{m} A_i x_i \text{ je positivně definitní,}$$

kde $c \in \mathbb{R}^n$, $A_0, A_1, \ldots, A_m \in \mathbb{R}^{n\times n}$ jsou dány a $x = (x_1, \ldots, x_n)^T$ je vektor proměnných. Semidefinitními programy dokážeme nejen modelovat větší třídu úloh než lineárními programy (Poznámka 7.15), ale stále jsou řešitelné efektivně za rozumný čas. Umožnily mj. velký pokrok na poli kombinatorické optimalizace, protože řada výpočetně složitých problémů se dá rychle a těsně aproximovat právě pomocí vhodných semidefinitních programů.

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.

Na závěr této sekce ukážeme ještě aplikaci z chemie.

Příklad 11.20 (Určování struktury bílkovin)**.** Jedna ze základních úloh modelování bílkovin je určení trojrozměrné struktury bílkovin. Typický postup je určení matice vzdáleností jednotlivých atomů pomocí jaderné magnetické rezonance a pak odvození struktury.



Struktura bílkoviny. [zdroj: Wikipedia]

Buď $X \in \mathbb{R}^{n\times 3}$ matice pozic jednotlivých atomů, to jest, řádek X_{i*} udává souřadnice i-tého atomu v prostoru. Maticí $D \in \mathbb{R}^{n\times n}$ si označíme vzdálenosti jednotlivých atomů, tedy $d_{ij} =$ vzdálenost i-tého a j-tého atomu. Jestliže známe X, tak D spočítáme následujícím způsobem. Posuneme souřadný systém, aby n-tý atom byl v počátku, tj. $X_{n*} = (0, 0, 0)$ a z matice X odstraníme poslední řádek, který je nyní redundantní. Označme pomocnou matici $D^* := XX^T$ a souřadnice libovolných dvou atomů $u := X_{i*}$, $v := X_{j*}$. Vztah matic D a D^* je tento:

$$d_{ij}^2 = \|u - v\|^2 = \langle u - v, u - v\rangle = \langle u, u\rangle + \langle v, v\rangle - 2\langle u, v\rangle = d_{ii}^* + d_{jj}^* - 2d_{ij}^*. \tag{11.1}$$

Náš problém stojí typicky naopak: ze znalosti naměřených vzdáleností D potřebujeme určit X, čímž získáme představu, kde v prostoru se jaký atom nachází a tím pádem jaká je struktura bílkoviny. Ze vztahu (11.1) odvodíme

$$d_{ij}^* = \frac{1}{2}(d_{ii}^* + d_{jj}^* - d_{ij}^2) = \frac{1}{2}(d_{in}^2 + d_{jn}^2 - d_{ij}^2).$$

Tímto předpisem z matice D spočítáme matici D^*. Protože D^* je symetrická a positivně definitní, ze spektrálního rozkladu $D^* = Q\Lambda Q^T$ sestrojíme hledanou matici $X = Q \cdot \operatorname{diag}\left(\sqrt{\lambda_1}, \sqrt{\lambda_2}, \sqrt{\lambda_3}\right)$. Pak totiž máme $D = XX^T$.

Poznamenejme, že X se dá někdy spočítat i za částečné informace vzdáleností (matice D není známa celá), ale tato úloha může být výpočetně složitá (tzv. NP-úplný problém).

Jiný problém z tohoto oboru je tzv. *Prokrustův problém*,[3)] v němž porovnáváme dvě struktury bílkovin jak moc jsou podobné. Označme matice dvou struktur X, Y. Lineární zobrazení s ortogonální maticí Q zachovává úhly a vzdálenosti (Věta 8.26), tudíž YQ odpovídá té samé struktuře, jako Y, pouze nějakým

[3)] Prokrustes nebyl matematik, ale řecká mytologická postava, lupič z Attiky, který pocestným usekával končetiny nebo jim je natahoval, aby se přesně vešli na jeho lože. Jeho život ukončil až Theseus.

způsobem otočené či zrcadlené. Chceme-li určit podobnost obou struktur, hledáme takovou ortogonální matici $Q \in \mathbb{R}^{3\times 3}$, aby matice X a YQ byly „co nejbližší“. Matematická formulace vede na optimalizační úlohu minimalizovat hodnotu maticové normy $\|X - YQ\|$ na množině ortogonálních matic Q. Tato úloha trochu připomíná metodu nejmenších čtverců. □

Problémy

11.1. Porovnejte počet aritmetických operací (nejhorší případ) následujících metod na testování positivní definitnosti matice $A \in \mathbb{R}^{n\times n}$: rekurentní vzoreček, Choleského rozklad, Gaussova eliminace a Sylvestrovo kriterium. Která metoda vychází nejlépe?

11.2. Ukažte, že každá symetrická matice se dá zapsat jako rozdíl dvou positivně definitních matic.

11.3. Buď $A \in \mathbb{R}^{n\times n}$ positivně definitní. Ukažte, že $A_{ii}(A^{-1})_{ii} \geq 1$ pro všechna $i = 1, \ldots, n$.

11.4. Buďte $A, B \in \mathbb{R}^{n\times n}$ symetrické a nechť všechna vlastní čísla A jsou větší než vlastní čísla B. Dokažte, že $A - B$ je positivně definitní.

Kapitola 12

Kvadratické formy

Přestože se lineární algebra zabývá převážně lineárními záležitostmi, i kvadratické modely zde mají své opodstatnění. V zásadě jsme se s nimi setkali již u eukleidovské normy (str. 76) a positivní definitnosti (Definice 11.1). V této kapitole probereme kvadratické formy podrobněji. Ukážeme souvislosti s positivní (semi-)definitností, znaménky vlastních čísel a popisem určitých geometrických objektů.

12.1 Bilineární a kvadratické formy

Definice 12.1 (Bilineární a kvadratická forma)**.** Buď V vektorový prostor nad $\mathbb{T}$. *Bilineární forma* je zobrazení $b\colon V^2 \to \mathbb{T}$, které je lineární v první i druhé složce, tj.

$$\begin{aligned} b(\alpha u + \beta v, w) &= \alpha b(u,w) + \beta b(v,w), \quad \forall \alpha,\beta \in \mathbb{T},\ \forall u,v,w \in V, \\ b(w, \alpha u + \beta v) &= \alpha b(w,u) + \beta b(w,v), \quad \forall \alpha,\beta \in \mathbb{T},\ \forall u,v,w \in V. \end{aligned}$$

Bilineární forma se nazývá *symetrická*, pokud $b(u,v) = b(v,u)$ pro všechna $u, v \in V$. Zobrazení $f\colon V \to \mathbb{T}$ je *kvadratická forma*, pokud se dá vyjádřit $f(u) = b(u,u)$ pro nějakou symetrickou bilineární formu b.

Příklad 12.2.

- Každý reálný skalární součin je bilineární formou.
- Buď $V = \mathbb{R}^2$. Pak
$$b(x,y) = x_1y_1 + 2x_1y_2 + 4x_2y_1 + 10x_2y_2$$
je příkladem bilineární formy,
$$b'(x,y) = x_1y_1 + 3x_1y_2 + 3x_2y_1 + 10x_2y_2$$
je příkladem symetrické 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 této kapitole se budeme převážně zabývat kvadratickými formami, i když bilineární formy jsou také zajímavé, např. právě vztahem se skalárním součinem.

V analogii s teorií lineárních zobrazení, i bilineární formy jsou jednoznačně určeny obrazy bází a dají se vyjádřit maticově. Čtenáři proto doporučujeme porovnat pojmy a výsledky této sekce se Sekcí 6.1 a uvědomit si jistou paralelu.

Definice 12.3 (Matice bilineární a kvadratické formy)**.** Buď $b\colon V^2 \to \mathbb{T}$ bilineární forma a $B = \{w_1, \dots, w_n\}$ báze prostoru V. Pak definujme matici $A \in \mathbb{T}^{n\times n}$ bilineární formy vzhledem k bázi B předpisem $a_{ij} = b(w_i, w_j)$. Matice kvadratické formy $f\colon V \to \mathbb{T}$ je definována jako matice libovolné symetrické bilineární formy indukující f.

Pomocí matic forem můžeme elegantně vyjádřit jejich funkční hodnoty explicitním předpisem.

Věta 12.4 (Maticové vyjádření forem)**.** *Buď B báze vektorového prostoru V a buď b bilineární forma na V. Pak A je matice formy b vzhledem k bázi B právě tehdy, když pro každé $u, v \in V$ platí*

$$b(u,v) = [u]_B^T A [v]_B. \tag{12.1}$$

Dále, je-li b symetrická forma, pak odpovídající kvadratická forma f pro každé $u \in V$ splňuje

$$f(u) = [u]_B^T A [u]_B.$$

Důkaz. Označme $x \coloneqq [u]_B$, $y \coloneqq [v]_B$, a nechť B se skládá z vektorů $w_1, \dots, w_n$. Je-li A je matice formy b, tak

$$b(u,v) = b\Big(\sum_{i=1}^n x_i w_i, \sum_{j=1}^n y_j w_j\Big) = \sum_{i=1}^n \sum_{j=1}^n x_i y_j b(w_i, w_j) = \sum_{i=1}^n \sum_{j=1}^n x_i y_j a_{ij} = x^T A y.$$

Naopak, pokud platí (12.1) pro každé $u, v \in V$, tak dosazením $u \coloneqq w_i$, $v \coloneqq w_j$ dostaneme $b(w_i, w_j) = [w_i]_B^T A [w_j]_B = e_i^T A e_j = a_{ij}$ pro všechna $i, j = 1, \dots, n$.

Konečně, $f(u) = b(u,u) = x^T A x$. □

Každá bilineární forma je jednoznačně určená obrazy všech dvojic bázických vektorů.

Důsledek 12.5. *Buď $B = \{w_1, \dots, w_n\}$ báze vektorového prostoru V nad $\mathbb{T}$ a buď $A \in \mathbb{T}^{n \times n}$. Pak existuje jediná bilineární forma $b\colon V^2 \to \mathbb{T}$ taková, že $b(w_i, w_j) = a_{ij}$ pro všechna $i, j = 1, \dots, n$.*

Důkaz. „Existence.“ Stačí ověřit, že zobrazení $b\colon V^2 \to \mathbb{T}$ dané předpisem $b(u,v) = [u]_B^T A [v]_B$ splňuje podmínky bilineární formy.

„Jednoznačnost.“ Z (12.1) plyne, že pro každé $u, v \in V$ je $b(u,v) = [u]_B^T A [v]_B$, tedy obrazy jsou jednoznačně dány. □

Ve vektorovém prostoru $\mathbb{R}^n$ mají bilineární formy speciální tvar.

Důsledek 12.6. *Každá bilineární forma na $\mathbb{R}^n$ se dá vyjádřit ve tvaru*

$$b(x,y) = x^T A y$$

pro určitou matici $A \in \mathbb{R}^{n \times n}$, a každá kvadratická forma na $\mathbb{R}^n$ se dá vyjádřit ve tvaru

$$f(x) = x^T A x$$

pro určitou symetrickou matici $A \in \mathbb{R}^{n \times n}$.

Důkaz. Stačí vzít A jako matici formy vzhledem ke kanonické bázi. □

Příklad 12.7. Uvažme bilineární formu na $\mathbb{R}^2$

$$b(x,y) = x_1 y_1 + 2 x_1 y_2 + 4 x_2 y_1 + 10 x_2 y_2.$$

Matice b vzhledem ke kanonické bázi je $A = \begin{pmatrix} 1 & 2 \\ 4 & 10 \end{pmatrix}$, což snadno nahlédneme i z vyjádření

$$b(x,y) = x^T A y = \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 4 & 10 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

Tato bilineární forma není symetrická, narozdíl od bilineární formy

$$b'(x,y) = x_1 y_1 + 3 x_1 y_2 + 3 x_2 y_1 + 10 x_2 y_2.$$

Matice b' vzhledem ke kanonické bázi je $A' = \begin{pmatrix} 1 & 3 \\ 3 & 10 \end{pmatrix}$, tedy $b'(x,y) = x^T A' y$. Odpovídající kvadratická forma splňuje

$$f'(x) = b'(x,x) = x^T A' x = \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 3 & 10 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

□

Poznámka 12.8. Mohli bychom si klást otázku, proč kvadratickou formu definujeme pouze pomocí symetrických bilineárních forem. Vždyť nic nám nebrání zavést $f(u) = b(u,u)$ i pro nesymetrickou bilineární formu b. Důvod je podobný jaký jsme uvedli u positivně definitních matic, viz Poznámka 11.2. Můžeme zavést bilineární formu $b_s(u,v) \coloneqq \frac{1}{2}\big(b(u,v) + b(v,u)\big)$, která již bude symetrická. Navíc, jak se snadno nahlédne, obě formy b, b_s indukují stejnou kvadratickou formu f. Zde ovšem těleso $\mathbb{T}$ nesmí mít charakteristiku 2, jinak by zlomek nedával smysl.

Matice forem závisí na volbě báze. Jak se změní matice, když přejdeme k jiné bázi?

Věta 12.9 (Matice kvadratické formy při změně báze)**.** *Buď $A \in \mathbb{T}^{n\times n}$ matice kvadratické formy f 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 bázi B' je S^TAS, a odpovídá stejné symetrické bilineární formě.*

Důkaz. Buď $u, v \in V$ a b symetrická bilineární forma indukující f. Pak

$$b(u,v) = [u]_B^T A[v]_B = ({}_B[id]_{B'}\,[u]_{B'})^T A({}_B[id]_{B'}\,[v]_{B'}) = [u]_{B'}^T S^T AS[v]_{B'}.$$

Podle Věty 12.4 je S^TAS je matice formy b, a tím i f, vzhledem k bázi B'. □

Různou volbou báze V dosahujeme různé maticové representace. Naším cílem bude najít takovou bázi, vůči níž je matice co nejjednodušší, tedy diagonální.

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 – každou matici lze diagonalizovat.

12.2 Sylvestrův zákon setrvačnosti

V této sekci nadále uvažujeme reálný prostor $\mathbb{R}^n$ nad $\mathbb{R}$. Z definice je patrné, že matice kvadratické formy je symetrická. Tato vlastnost budeme velmi potřebovat.

Věta 12.10 (Sylvestrův zákon setrvačnosti[1])**.** *Buď $f(x) = x^TAx$ kvadratická forma. Pak existuje báze, vůči níž má f diagonální matici s prvky $1, -1, 0$. Navíc, tato matice je až na pořadí prvků jednoznačná.*

Důkaz. „Existence“.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 $\Lambda'_{ii} = 1$ jinak.

„Jednoznačnost“. Sporem předpokládejme, že máme dvě různé diagonalizace D, D' pro bázi B : $w_1, \ldots, w_n$ a bázi B' : $w'_1, \ldots, w'_n$. Buď $u \in \mathbb{R}^n$ libovolné a nechť má souřadnice $y = [u]_B$, $z = [u]_{B'}$. Pak

$$f(u) = y^TDy = y_1^2 + \ldots + y_p^2 - x_{p+1}^2 - \ldots - y_q^2 + 0x_{q+1}^2 + \ldots + 0y_n^2,$$
$$f(u) = z^TD'z = z_1^2 + \ldots + z_s^2 - z_{s+1}^2 - \ldots - z_t^2 + 0z_{t+1}^2 + \ldots + 0z_n^2.$$

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 $u = \sum_{i=1}^p y_i w_i = \sum_{j=s+1}^n z_j w'_j$, z čehož dostáváme

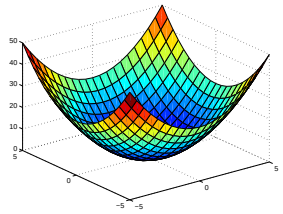
$$f(u) = \begin{cases} y_1^2 + \ldots + y_p^2 > 0, \\ -z_{s+1}^2 - \ldots - z_t^2 \leq 0. \end{cases}$$

To je spor. □

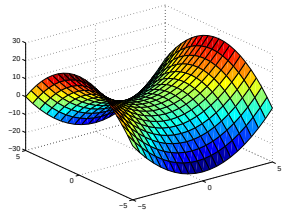
[1] Anglicky *Sylvester's law of inertia*, z r. 1852.

Poznamenejme, že báze, vůči níž matice kvadratické formy je diagonální, se nazývá *polární báze*. Tedy báze z Věty 12.10 je polární (ne naopak!). Dá se také ukázat, že polární báze existuje nejen pro reálné prostory, ale i pro prostory nad libovolným tělesem charakteristiky různé od 2.

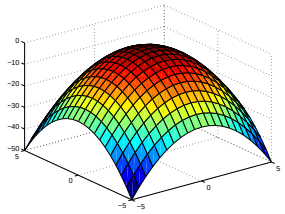
Příklad 12.11 (Kvadratické formy v $\mathbb{R}^2$)**.** Podle Sylvestrova zákona, kvadratické formy v $\mathbb{R}^2$ mají v podstatě jeden z následujících tvarů v souřadném systému vhodné báze.



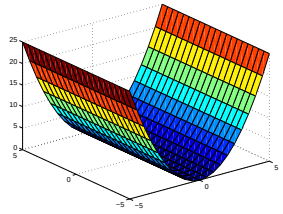
$x_1^2 + x_2^2$



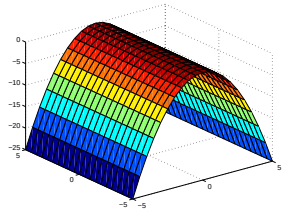
$x_1^2 - x_2^2$



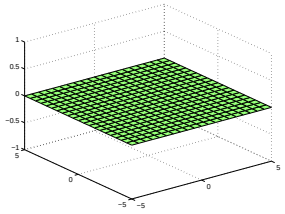
$-x_1^2 - x_2^2$



x_1^2



$-x_1^2$



0 □

Význam Sylvestrova zákona nespočívá ani tak v existenci diagonalizace, jako spíš v její jednoznačnosti (odtud název „jednoznačnost“). Tato jednoznačnost opravňuje k zavedení pojmu *signatura* jako trojice (p, q, z), kde p je počet jedniček, q počet minus jedniček a z počet nul ve výsledné diagonální matici. Navíc má řadu důsledků týkající se mj. positivní (semi-)definitnosti a vlastních čísel.

Důsledek 12.12. *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. □

Diagonalizací matice A tedy nenajdeme vlastní čísla, ale určíme kolik jich je kladných a kolik záporných. Pokud tento postup 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 12.13. *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 12.12 a vztahu mezi positivní (semi-)definitností a vlastními čísly (Věta 11.7). □

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 řádková 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.

Algoritmus 12.14 (Diagonalizace matice kvadratické formy)**.** Buď $A \in \mathbb{R}^{n\times n}$ symetrická. Aplikováním elementárních řádkových úprav a odpovídajících sloupcových úprav převeď matici na diagonální tvar.

Příklad 12.15. 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. □

Příklad 12.16. Ukažte, že součin positivně definitních matic $A, B \in \mathbb{R}^{n\times n}$ nemusí být positivně definitní matice, a to ve smyslu původní definice, nejen že AB není nutně symetrická.

Zajímavé ale je, že AB, přestože ne nutně symetrická, má stále kladná vlastní čísla. Snadno je to vidět z vyjádření $AB = \sqrt{A}\sqrt{A}B$. Vynásobením $\sqrt{A}^{-1}$ zleva a $\sqrt{A}$ zprava dostaneme podobnou matici $\sqrt{A}B\sqrt{A}$, která ze setrvačnosti má stejnou signaturu jako B, což znamená kladná vlastní čísla. □

Kuželosečky a kvadriky

Pomocí kvadratických forem lze popisovat geometrické útvary zvané *kvadriky*. To jsou (stručně řečeno, podrobněji viz např. [Bican, 2009]) množiny popsané rovnicí $x^TAx + b^Tx + c = 0$. 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 12.17 (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.

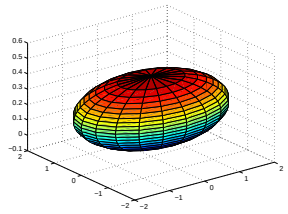
Nyní uvažme rovnici $x^TAx = 1$, kde $A \in \mathbb{R}^{n\times n}$ je positivně definitní a $x = (x_1, \dots, x_n)^T$ je vektor proměnných. Nahlédneme, že rovnice popisuje elipsoid v prostoru $\mathbb{R}^n$. Buď $A = Q\Lambda Q^T$ spektrální rozklad. Při substituci $y \coloneqq Q^Tx$ dostaneme

$$1 = x^TAx = x^TQ\Lambda Q^Tx = y^T\Lambda y = \sum_{i=1}^{n} \lambda_i y_i^2 = \sum_{i=1}^{n} \frac{1}{\left(\lambda_i^{-1/2}\right)^2} y_i^2.$$

Dostáváme tedy popis elipsoidu se středem v počátku, poloosy jsou ve směru souřadnic a mají délky $\frac{1}{\sqrt{\lambda_1}}, \dots, \frac{1}{\sqrt{\lambda_n}}$. Nicméně, tento popis je v prostoru po transformaci $y = Q^Tx$. Vrátíme zpět transformací $x = Qy$. Protože Q je ortogonální matice, dostaneme stejný elipsoid se středem v počátku, jen nějak pootočený. Protože kanonická báze $e_1, \dots, e_n$ se zobrazí na sloupce matice Q (což jsou vlastní vektory matice A), tak poloosy původního elipsoidu budou ve směrech vlastních vektorů A.

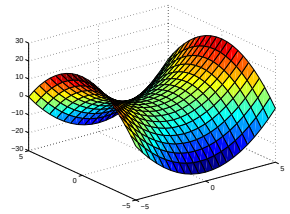
Je-li A symetrická, ale ne positivně definitní, analýza bude stejná. Jenom nedostaneme elipsoid, ale jiný geometrický útvar (hyperboloid aj.)

Příklad 12.18 (Některé kvadriky v $\mathbb{R}^3$)**.**



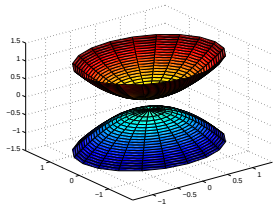
$$\frac{x_1^2}{a^2}+\frac{x_2^2}{b^2}+\frac{x_3^2}{c^2}=1$$

elipsoid



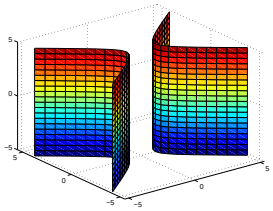
$$\frac{x_1^2}{a^2}-\frac{x_2^2}{b^2}-x_3=0$$

hyperbolický paraboloid



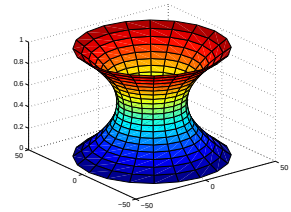
$$-\frac{x_1^2}{a^2}-\frac{x_2^2}{b^2}+\frac{x_3^2}{c^2}=1$$

dvojdílný hyperboloid



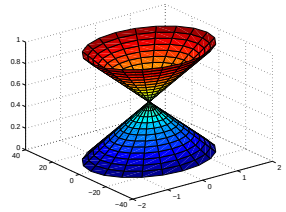
$$\frac{x_1^2}{a^2}-\frac{x_2^2}{b^2}=1$$

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 □

Problémy

12.1. Diskutujte jednoznačnost matice kvadratické formy, a jednoznačnost kvadratické formy ze znalosti obrazu nějaké báze.

12.2. Ukažte, že bilineární formy na prostoru V tvoří vektorový prostor a určete jeho dimenzi.

12.3. Ukažte, že kvadratické formy na prostoru V tvoří vektorový prostor a určete jeho dimenzi.

12.4. Buď V vektorový prostor nad tělesem $\mathbb{T}$ charakteristiky různé od 2. Ukažte, že každá symetrická bilineární forma $b\colon V^2 \to \mathbb{T}$ je určena hodnotami $b(v,v)$, $v \in V$. To v důsledku znamená, že ze znalosti kvadratické formy jsme schopni zrekonstruovat jednoznačnou symetrickou bilineární formu, která ji indukuje.

12.5. Platí Sylvestrův zákon setrvačnosti na komplexním prostoru?

12.6. Vyjádřete kvadratickou formu $f(x) = x^T A x$ s positivně definitní maticí $A \in \mathbb{R}^{n\times n}$ jako součet čtverců lineárních forem. (*Poznámka.* Platí dokonce, že každý nezáporný polynom se dá vyjádřit jako zlomek, kde čitatel i jmenovatel jsou ve tvaru součtu čtverců.)

12.7. Buď $f\colon V \to \mathbb{R}$ kvadratická forma a $h\colon V \to V$ isomorfismus.

(a) Ukažte, že $f \circ h$ je kvadratická forma ns V.

(b) Ukažte, že obě kvadratické formy f, $f \circ h$ mají stejnou signaturu.

12.8. Buď f kvadratická forma na reálném prostoru V a buď (p,q,z) její signatura. Ukažte, že v prostoru V existuje podprostor dimenze $z+\min(p,q)$, na kterém je kvadratická forma f nulová, a větší takový podprostor neexistuje.

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, a N. Metropolis)

   Pomocí simulací s náhodnými čísly spočítáme přibližná řešení problémů, které jsou velmi těžké na to spočítat jejich řešení přesně.

2. *Simplexová metoda pro lineární programování* (1946, G. Dantzig)

   Metoda na výpočet optimalizačních úloh s lineárním kriteriem i omezeními, tj. v jakém bodu polyedru se nabyde nejmenší hodnota lineární funkce (viz Sekce 1.5 a Poznámka 7.15).

3. *Iterační metody Krylovových podprostorů* (1950, M. Hestenes, E. Stiefel, C. Lanczos)

   Metody na řešení velkých a řídkých soustav lineárních rovnic.

4. *Dekompozice matic* (1951, A. Householder)

   Maticové rozklady jako je např. Choleského rozklad, LU rozklad, QR rozklad, spektrální rozklad, Schurova triangularizace nebo SVD rozklad.

5. *Překladač Fortranu* (1957, J. Backus)

   Informatikům netřeba představovat překladač programovacího jazyka Fortran, který jako jeden z prvních umožnil náročné numerické výpočty.

6. *QR algoritmus*, (1961, J. Francis)

   Algoritmus pro výpočet vlastních čísel.

7. *Quicksort* (1962, A. Hoare)

   Algoritmus na třídění.

8. *Rychlá Fourierova transformace* (1965, J. Cooley, J. Tukey)

   Pro rychlé násobení polynomů a čísel, zpracování signálu a mnoho dalších věcí.

9. *Algoritmus „Integer relation detection“* (1977, H. Ferguson, R. Forcade)

   Zobecnění Euklidova algoritmu postupného dělení na problém: Dáno n reálných čísel $x_1, \ldots, x_n$, existuje netriviální celočíselná kombinace $a_1x_1 + \ldots + a_nx_n = 0$?

10. *Metoda více pólů – „Fast multipole algorithm“* (1987, L. Greengard, V. Rokhlin)

    Simulace v problému výpočtu sil dalekého dosahu v úloze n těles. Seskupuje zdroje ležící u sebe a pracuje s nimi jako s jediným.

V této kapitole budeme uvažovat standardní skalární součin v $\mathbb{R}^n$ eukleidovskou normu (pokud není explicitně řečeno jinak).

13.1 Householderova transformace

Připomeňme (Příklad 8.44), 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 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 x na jiný y se stejnou normou tím, že vynásobíme vektor x zleva vhodnou Householderovou maticí. Speciálně lze převést každý vektor 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 $Hx = \|x\|_2 e_1$.

Důkaz. Případ $x = \|x\|_2 e_1$ je jasný. Jinak použijeme Větu 13.1, 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, o němž hovoříme podrobněji v následující sekci.

Podobně lze použít i Givensova matice, ale ta nuluje pouze jeden prvek (stejně jako elementární matice), takže ji musíme použít vícekrát (Problém 13.1.).

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

$$\begin{pmatrix} 1 & o^T \\ o & Q'^T \end{pmatrix} HA = \begin{pmatrix} 1 & o^T \\ o & Q'^T \end{pmatrix} \begin{pmatrix} \alpha & b^T \\ o & B \end{pmatrix} = \begin{pmatrix} \alpha & b^T \\ o & R' \end{pmatrix}.$$

[1)] Alston Scott Householder (1904–1993), americký numerický matematik, transformace je z r. 1958. Byl spoluzakladatelem numerické matematiky a prý nikdy necestoval letadlem, neboť si byl vědom, kde všude při výpočtech konstrukce mohlo dojít k chybě.

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:

$$x = A_{*1} - \|A_{*1}\| e_1 = (-5, 3, 4)^T,$$
$$Q_1 = I_3 - 2\frac{x x^T}{x^T x} = \frac{1}{25} \begin{pmatrix} 0 & 15 & 20 \\ 15 & 16 & -12 \\ 20 & -12 & 9 \end{pmatrix}, \quad Q_1 A = \begin{pmatrix} 5 & 25 & -4 \\ 0 & 0 & -10 \\ 0 & -25 & -10 \end{pmatrix}.$$

Druhá iterace:

$$x = (0, -25)^T - 25 e_1 = (-25, -25)^T,$$
$$Q_2 = I_2 - 2\frac{x x^T}{x^T x} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \quad Q_1 \begin{pmatrix} 0 & -10 \\ -25 & -10 \end{pmatrix} = \begin{pmatrix} 25 & 10 \\ 0 & 10 \end{pmatrix}.$$

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 $U_{*1} = (u_{11}, 0, \dots, 0)^T$, 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.

Poznámka 13.7 (QR rozklad pomocí Gramovy–Schmidtovy ortogonalizace)**.** QR rozklad matice $A \in \mathbb{R}^{m\times n}$ lze sestrojit i pomocí Gramovy–Schmidtovy ortogonalizace. Prakticky se to sice nedělá, protože právě použití ortogonálních matic je Householderova transformace numericky lepší, ale pro pochopení vztahu obou metod je to užitečné.

Základní myšlenka je následující: Zatímco Householderovými transformacemi (tj., sekvencí ortogonálních matic) upravujeme matici A na horní trojúhelníkovou, Gramova–Schmidtova ortogonalizace funguje přesně naopak – pomocí sekvence vhodných horních trojúhelníkových matic upravíme A na matici s ortonormálními sloupci.

Konkrétně popíšeme Gramovu–Schmidtovu ortogonalizaci takto. Mějme matici $A \in \mathbb{R}^{m\times n}$, jejíž sloupce chceme zortonormalizovat. Budeme postupovat podle Algoritmu 8.19 s tím, že vektory $x_1, \dots, x_n$ jsou sloupce matice A a v průběhu výpočtu budeme sloupce matice A nahrazovat vektory y_k a z_k. Krok 2: algorimu má tvar

$$y_k \coloneqq x_k - \sum_{j=1}^{k-1} \langle x_k, z_j\rangle z_j.$$

Tuto operaci vyjádříme maticově tak, že matici A vynásobíme zprava maticí

$$\begin{pmatrix} 1 & & & \alpha_1 & \\ & \ddots & & \vdots & \\ & & 1 & \alpha_{k-1} & \\ & & & 1 & \\ & & & & 1 \end{pmatrix},$$

kde $\alpha_j = -\langle x_k, z_j\rangle$, $j = 1, \dots, k-1$. Podobně krok 3:, který má tvar

$$z_k \coloneqq \frac{1}{\|y_k\|} y_k,$$

vyjádříme vynásobením matice A zprava diagonální maticí s prvky $1, \dots, 1, \frac{1}{\|y_k\|}, 1, \dots, 1$ na diagonále. Protože obě matice, kterými jsme násobili A zprava, jsou horní trojúhelníkové, můžeme celou ortogonalizaci vyjádřit jako

$$AR_1 \dots R_\ell = Q,$$

kde $R_1, \dots, R_\ell$ jsou horní trojúhelníkové matice a Q má ortonormální sloupce. Hledaný QR nyní dostaneme tak, že vyjádříme $A = QR$, kde $R \coloneqq (R_1 \dots R_\ell)^{-1}$ je rovněž horní trojúhelníková matice.

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 8.45(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 $Rx = Q^T b$. 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 Gramově–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 5.47), že $\mathcal{S}(A) = \mathcal{S}(\tilde{Q})$. Tedy ortonormální bázi $\mathcal{S}(A)$ tvoří sloupce $\tilde{Q}$.

Vzhledem k vlastnostem ortogonálních matic pak $\tilde{Q}'$ tvoří ortonormální bázi $\mathrm{Ker}\,(A^T)$, protože $\mathrm{Ker}\,(A^T)$ je ortogonální doplněk k $\mathcal{S}(A)$. Z QR rozkladu matice A resp. A^T tedy dokážeme vyčíst ortonormální bázi všech základních maticových prostorů – řádkového, sloupcového a jádra.

QR rozklad a rozšíření na ortonormální bázi

Několikrát jsme použili vlastnost, že ortonormální systém vektorů jde rozšířit na ortonormální bázi. Zaměříme se na speciální případ jak rozšířit vektor jednotkové velikosti na ortonormální bázi. Tento případ se objevil např. v důkazu Věty 10.45 o spektrálním rozkladu symetrických matic.

Buď $a \in \mathbb{R}^n$, $\|a\| = 1$, a buď $a = Qr$ jeho QR rozklad. Aby byl vektor r, bráno jako matice s jedním sloupcem, v horním trojúhelníkovém tvaru s nezápornou diagonálou, musí mít tvar $r = (\alpha, 0, \ldots, 0)^T$ pro nějaké $\alpha \geq 0$. Protože $\|a\| = 1$ a Q je ortogonální, musí $\|r\| = 1$. Tudíž $r = e_1$, z čehož $a = Q_{*1}$. Vektor a tak leží v prvním sloupci Q a ostatní sloupce představují jeho rozšíření na ortonormální bázi.

QR rozklad a projekce do podprostoru

Nechť $A \in \mathbb{R}^{m\times n}$ má lineárně nezávislé sloupce. Víme (Věta 8.36), 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 $A = \tilde{Q}\tilde{R}$:

$$\begin{aligned}A(A^TA)^{-1}A^T &= \tilde{Q}\tilde{R}(\tilde{R}^T\tilde{Q}^T\tilde{Q}\tilde{R})^{-1}\tilde{R}^T\tilde{Q}^T = \tilde{Q}\tilde{R}(\tilde{R}^T\tilde{R})^{-1}\tilde{R}^T\tilde{Q}^T\\ &= \tilde{Q}\tilde{R}\tilde{R}^{-1}(\tilde{R}^T)^{-1}\tilde{R}^T\tilde{Q}^T = \tilde{Q}\tilde{Q}^T.\end{aligned}$$

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 8.5) 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 13.8 (QR algoritmus)**.** Buď $A \in \mathbb{R}^{n\times n}$.

1: $A_0 \coloneqq A$, $i \coloneqq 0$,

2: **while not** splněna ukončovací podmínka **do**

3: sestroj QR rozklad matice A_i, tj. $A_i = QR$,

4: $A_{i+1} \coloneqq RQ$,

5: $i \coloneqq i + 1$,

6: **end while**

Výstup: A_i.

Tvrzení 13.9. *Matice $A_0, A_1, \ldots$ jsou si navzájem podobné.*

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 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 13.10. 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 10.50 o Gerschgorinových discích. □

[2)] Autory jsou anglický informatik John G.F. Francis a ruská matematička Vera Nikolaevna Kublanovskaya, kteří jej vyvinuli nezávisle r. 1961.

13.4 SVD rozklad

Stejně jako QR rozklad je SVD rozklad[3)] jednou ze základních technik v numerických výpočtech.

Věta 13.11 (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 $A = U\Sigma V^T$.*

Ideu důkazu uvádíme za Algoritmem 13.14, 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 13.12 (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. Nechť $A = U\Sigma V^T$ je SVD rozklad A. Pak

$$A^TA = V\Sigma^TU^TU\Sigma V^T = V\Sigma^T\Sigma V^T = V\operatorname{diag}(\sigma_1^2,\ldots,\sigma_q^2,0,\ldots,0)V^T,$$

což je spektrální rozklad positivně definitní matice A^TA. Tudíž $\lambda_i = \sigma_i^2$. □

Příklad 13.13. 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 matice A^TA. Podobně, matice U je ortogonální maticí ze spektrálního rozkladu AA^T:

$$AA^T = U\Sigma V^TV\Sigma^TU^T = U\Sigma\Sigma^TU^T = U\operatorname{diag}(\sigma_1^2,\ldots,\sigma_q^2,0,\ldots,0)U^T.$$

Bohužel, spektrální rozklady matic A^TA a AA^T nemůžeme použít ke konstrukci SVD rozkladu, protože nejsou jednoznačné. Použít můžeme jen jeden a druhý dopočítat trochu jinak.

Algoritmus 13.14 (SVD rozklad)**.** Buď $A \in \mathbb{R}^{m\times n}$.

1: Sestroj $V\Lambda V^T$ spektrální rozklad matice A^TA;
2: $r \coloneqq \operatorname{rank}(A)$;
3: $\sigma_i \coloneqq \sqrt{\lambda_i}$, $i = 1,\ldots,r$;
4: $S \coloneqq \operatorname{diag}(\sigma_1,\ldots,\sigma_r)$;
5: V_1 je matice tvořená prvními r sloupci V;
6: $U_1 \coloneqq AV_1S^{-1}$;
7: doplň U_1 na ortogonální matici $U = (U_1 \mid U_2)$;

Výstup: $A = U\Sigma V^T$ je SVD rozklad A.

Důkaz. Z Věty 13.12 víme, že $\sigma_1,\ldots,\sigma_r$ 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 odříznutím posledních $n-r$ řádků a sloupců dostaneme matici $\operatorname{diag}(\lambda_1,\ldots,\lambda_r) = V_1^TA^TAV_1$. Nyní je vidět, že U_1 má ortonormální sloupce, neboť

$$U_1^TU_1 = (S^{-1})^TV_1^TA^TAV_1S^{-1} = (S^{-1})^T\operatorname{diag}(\lambda_1,\ldots,\lambda_r)S^{-1} = (S^{-1})^TS^2S^{-1} = I_r.$$

Zbývá ukázat, že $A = U\Sigma V^T$, neboli $\Sigma = U^TAV$. Rozložme $V = (V_1 \mid V_2)$. Odříznutím prvních r řádků a sloupců v matici $\Lambda = V^TA^TAV$ dostaneme $0 = V_2^TA^TAV_2$, z čehož $AV_2 = 0$ (Důsledek 8.35). Nyní s využitím rovnosti $AV_1 = U_1S$ máme

$$U^TAV = U^TA(V_1 \mid V_2) = (U^TU_1S \mid U^TAV_2) = \begin{pmatrix} S & 0 \\ 0 & 0 \end{pmatrix} = \Sigma.$$ □

[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.

Příklad 13.15 (SVD rozklad)**.** Mějme

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 0 \\ 0 & -2 \end{pmatrix}.$$

Spektrální rozklad matice $A^T A$:

$$A^T A = \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{pmatrix} \begin{pmatrix} 6 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{pmatrix} \equiv V \Lambda V^T.$$

Určení S:

$$S = \begin{pmatrix} \sqrt{6} & 0 \\ 0 & 2 \end{pmatrix}.$$

Určení U_1 (v tomto příkladu máme $V_1 = V$):

$$U_1 = A V_1 S^{-1} = \begin{pmatrix} \frac{\sqrt{3}}{3} & 0 \\ \frac{\sqrt{3}}{3} & \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{3}}{3} & \frac{\sqrt{2}}{2} \end{pmatrix}.$$

Doplnění U_1 ortogonální matici U:

$$U = \begin{pmatrix} \frac{\sqrt{3}}{3} & 0 & -\frac{\sqrt{6}}{3} \\ \frac{\sqrt{3}}{3} & \frac{\sqrt{2}}{2} & \frac{\sqrt{6}}{6} \\ -\frac{\sqrt{3}}{3} & \frac{\sqrt{2}}{2} & -\frac{\sqrt{6}}{6} \end{pmatrix}.$$

Výsledný SVD rozklad:

$$A = \begin{pmatrix} \frac{\sqrt{3}}{3} & 0 & -\frac{\sqrt{6}}{3} \\ \frac{\sqrt{3}}{3} & \frac{\sqrt{2}}{2} & \frac{\sqrt{6}}{6} \\ -\frac{\sqrt{3}}{3} & \frac{\sqrt{2}}{2} & -\frac{\sqrt{6}}{6} \end{pmatrix} \begin{pmatrix} \sqrt{6} & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{pmatrix} \equiv U \Sigma V^T. \qquad \square$$

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 $S \coloneqq \operatorname{diag}(\sigma_1, \ldots, \sigma_r)$. Pak

$$A = U\Sigma V^T = \begin{pmatrix} U_1 & U_2 \end{pmatrix} \begin{pmatrix} S & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} V_1^T \\ V_2^T \end{pmatrix} = U_1 S V_1^T.$$

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 13.14.

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 13.16. *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_1 tvoří ortonormální bázi prostoru $\mathcal{R}(A)$.

(3) Sloupce V_2 tvoří ortonormální bázi prostoru $\operatorname{Ker}(A)$.

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 $\operatorname{rank}(A) = \operatorname{rank}(U_1)$, máme rovnost $\mathcal{S}(A) = \mathcal{S}(U_1)$.

(2) Plyne z předchozího díky $\mathcal{R}(A) = \mathcal{S}(A^T)$.

(3) 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 $\mathcal{S}(A^T) = \mathcal{R}(A) = \operatorname{Ker}(A)^\perp$. Proto sloupce V_2, které doplňují sloupce V_1 na ortonormální bázi $\mathbb{R}^n$, představují ortonormální bázi $\operatorname{Ker}(A)$. □

SVD a projekce do podprostoru

Pomocí SVD rozkladu můžeme snadno vyjádřit matici projekce do sloupcového (a řádkového) prostoru dané matice. Dokonce k tomu nepotřebujeme předpoklad na lineární nezávislost sloupců matice, což bylo potřeba ve Větě 8.36.

Věta 13.17. *Nechť $A = U\Sigma V^T$ je SVD rozklad matice $A \in \mathbb{R}^{m\times n}$. Pak matice projekce do*

(1) sloupcového prostoru $\mathcal{S}(A)$ je $U_1 U_1^T$,

(2) řádkového prostoru $\mathcal{R}(A)$ je $V_1 V_1^T$,

Důkaz.

(1) Z Věty 13.16 je $\mathcal{S}(A) = \mathcal{S}(U_1)$. Sloupce U_1 jsou lineárně nezávislé, a proto matice projekce má dle Věty 8.36 tvar $U_1(U_1^T U_1)^{-1} U_1^T = U_1 (I_r)^{-1} U_1^T = U_1 U_1^T$.

(2) Plyne z předchozího díky $\mathcal{R}(A) = \mathcal{S}(A^T)$. □

Podobným způsobem lze odvodit i vzoreček pro přibližné řešení soustavy $Ax = b$ metodou nejmenších čtverců. Nicméně, později ve Větě 13.25 ukážeme silnější výsledek.

SVD a geometrie lineárního zobrazení

Buď $A \in \mathbb{R}^{n\times n}$ 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, zobrazení s maticí V^T zobrazí kouli na sebe sama, Σ ji zdeformuje na elipsoid a U ji otočí/převrátí. Tedy výsledkem bude elipsoid 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. Je-li hodnota rovna 1, elipsoid bude mít tvar koule, a naopak čím větší bude hodnota, tím protáhlejší bude elipsoid. Význam této hodnoty 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 (viz Sekce 1.2).

Empirické pravidlo říká, že je-li 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 rovné 1, a proto se v numerické matematice často používají. Naproti tomu např. Hilbertovy matice z Příkladu 3.39 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. Jestliže ponecháme k největších singulárních čísel a ostatní vynulujeme $\sigma_{k+1} \coloneqq 0, \ldots, \sigma_r \coloneqq 0$, 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 (viz Sekce 13.7) je ze všech matic hodnosti k právě A' nejblíže matici A. Low-rank aproximaci využijeme v následujícím:

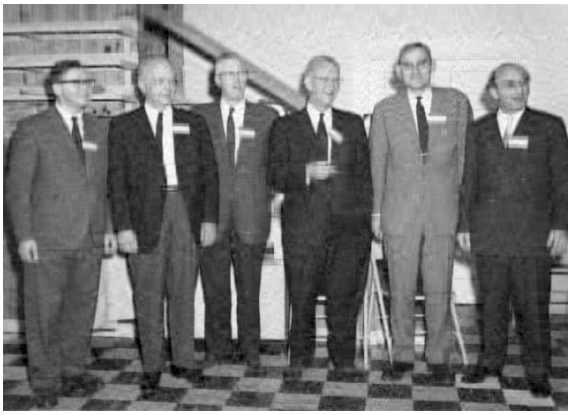
SVD a komprese dat

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 potřebujeme 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.

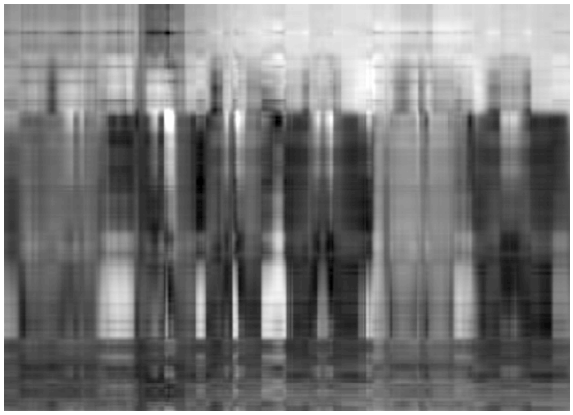
Příklad 13.18. Zmíněný postup ilustrujeme na kompresi obrázku. Předpokládáme, že matice $A \in \mathbb{R}^{m\times n}$ reprezentuje obrázek, ve kterém pixel na pozici (i, j) má barvu s číslem a_{ij}. Následující obrázky ilustrují komprimaci pro různou volbu k. Pro $k = 480$ máme originální obrázek, pro 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, a 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 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, viz Sekce 13.7) 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	$\approx 10^{-18}$

13.6 Pseudoinverzní matice

Je přirozenou snahou zobecnit pojem inverze matice i na singulární nebo obdélníkové matice. Takové zobecněné inverzi se říká *pseudoinverze* a existuje několik druhů. Nejčastější je tzv. Mooreova–Penroseova pseudoinverze[4)], která spočívá na SVD rozkladu.

Definice 13.19 (Mooreova–Penroseova pseudoinverze)**.** Buď $A \in \mathbb{R}^{m\times n}$ matice s redukovaným SVD rozkladem $A = U_1 S V_1^T$. Je-li $A \neq 0$, pak její *pseudoinverze* je $A^\dagger = V_1 S^{-1} U_1^T \in \mathbb{R}^{n\times m}$. Pro $A = 0$ definujeme pseudoinverzi předpisem $A^\dagger = A^T$.

Příklad 13.20. Pseudoinverze nenulového vektoru $a \in \mathbb{R}^n$ je $a^\dagger = \frac{1}{a^T a} a^T$, speciálně např. $(1,1,1,1)^\dagger = \frac{1}{4}(1,1,1,1)^T$. □

Věta 13.21 (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) $A^\dagger = A^\dagger A A^\dagger$,
(6) $AA^\dagger$ je symetrická,
(7) $A^\dagger A$ je symetrická,
(8) má-li A lineárně nezávislé sloupce, pak $A^\dagger = (A^T A)^{-1} A^T$,
(9) má-li A lineárně nezávislé řádky, pak $A^\dagger = A^T (AA^T)^{-1}$.

Důkaz. Vlastnosti se dokážou jednoduše z definice. Pro ilustraci ukážeme jen dvě vlastnosti, zbytek necháváme čtenáři.

[4)] Nezávisle ji objevili americký matematik Eliakim Hastings Moore r. 1920 a anglický fyzik, slavný popularizátor, Roger Penrose r. 1955.

(4) Z definice $AA^\dagger A = U_1 S V_1^T V_1 S^{-1} U_1^T U_1 S V_1^T = U_1 S S^{-1} S V_1^T = U_1 S V_1^T = A$.

(8) Z předpokladu je V_1 čtvercová, tedy ortogonální. Pak

$$(A^T A)^{-1} = (V_1 S U_1^T U_1 S V_1^T)^{-1} = (V_1 S^2 V_1^T)^{-1} = V_1 S^{-2} V_1^T,$$

z čehož $(A^T A)^{-1} A^T = V_1 S^{-2} V_1^T V_1 S U_1^T = V_1 S^{-1} U_1^T = A^\dagger$. □

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 $(AB)^\dagger \neq B^\dagger A^\dagger$.

Pomocí pseudoinverze elegantně vyjádříme matice projekce do maticových prostorů.

Věta 13.22. *Buď $A \in \mathbb{R}^{m\times n}$. Pak matice projekce do*

(1) sloupcového prostoru $\mathcal{S}(A)$ je $AA^\dagger$,

(2) řádkového prostoru $\mathcal{R}(A)$ je $A^\dagger A$,

(3) jádra $\operatorname{Ker}(A)$ je $I_n - A^\dagger A$.

Důkaz.

(1) S použitím redukovaného SVD rozkladu $A = U_1 S V_1^T$ upravme

$$AA^\dagger = U_1 S V_1^T V_1 S^{-1} U_1^T = U_1 U_1^T.$$

Podle Věty 13.17 je to hledaná matice projekce $U_1 U_1^T$.

(2) Analogicky jako v předchozím je $A^\dagger A = V_1 V_1^T$, což je matice projekce do $\mathcal{R}(A)$.

(3) Plyne z Věty 8.37 a vlastnosti $\operatorname{Ker}(A) = \mathcal{R}(A)^\perp$ (Věta 8.33). □

Zajímavá je interpretace pseudoinverze z hlediska lineárních zobrazení.

Věta 13.23 (Pseudoinverzní matice a lineární zobrazení)**.** *Uvažujme lineární zobrazení $f(x) = Ax$, kde $A \in \mathbb{R}^{m\times n}$.*

(1) Pokud definiční obor $f(x)$ omezíme pouze na prostor $\mathcal{R}(A)$, tak dostaneme isomorfismus mezi $\mathcal{R}(A)$ a $f(\mathbb{R}^n)$.

(2) Inverzní zobrazení k tomuto isomorfismu má tvar $y \mapsto A^\dagger y$.

Důkaz.

(1) Zobrazení s omezeným definičním oborem je „na“, protože podle Důsledku 8.35(2) je

$$f(\mathbb{R}^n) = \mathcal{S}(A) = \mathcal{R}(A^T) = \mathcal{R}(AA^T) = \mathcal{S}(AA^T) = \{Ay;\, y \in \mathcal{R}(A)\} = f(\mathcal{R}(A)).$$

Jelikož prostory $f(\mathbb{R}^n)$ a $\mathcal{R}(A)$ mají stejnou dimenzi (Věta 5.51), musí být zobrazení isomorfismem.

(2) Podle Věty 13.22(2) se každý vektor $x \in \mathcal{R}(A)$ při zobrazení $x \mapsto A^\dagger A x$ zobrazí na $A^\dagger A x = x$. Tudíž $A^\dagger$ je matice inverzního zobrazení k zobrazení $x \mapsto Ax$. □

Nejvýznačnější vlastnost pseudoinverze spočívá v popisu množiny řešení řešitelných soustav a množiny přibližných řešení metodou nejmenších čtverců neřešitelných soustav. V obou případech je $A^\dagger b$ v jistém smyslu význačné řešení.

Věta 13.24 (Pseudoinverzní matice a řešení soustav rovnic)**.** *Buď $A \in \mathbb{R}^{m\times n}$, $b \in \mathbb{R}^m$ a X množina řešení soustavy $Ax = b$. Je-li $X \neq \emptyset$, pak*

$$X = A^\dagger b + \mathcal{S}(I_n - A^\dagger A).$$

Navíc, ze všech vektorů z množiny X má $A^\dagger b$ nejmenší eukleidovskou normu, a je to jediné řešení s touto vlastností.

Důkaz. „$\subseteq$“ Buď $x \in X$, tj. $Ax = b$. Potom $AA^\dagger b = AA^\dagger Ax = Ax = b$, tedy $A^\dagger b \in X$. Podle Věty 7.4 je $X = x_0 + \mathrm{Ker}\,(A)$, kde x_0 je libovolné řešení. Podle Věty 13.22(3) je $\mathrm{Ker}\,(A) = \mathcal{S}(I_n - A^\dagger A)$ a za x_0 můžeme volit $A^\dagger b$.

„$\supseteq$“ Buď $x = A^\dagger b + (I - A^\dagger A)y$ pro nějaké $y \in \mathbb{R}^n$. Pak

$$Ax = AA^\dagger b + (A - AA^\dagger A)y = b + 0y = b.$$

„Norma.“ Nejprve ukážeme, že $A^\dagger b \in \mathcal{S}(I_n - A^\dagger A)^\perp = \mathcal{R}(I_n - A^\dagger A)^\perp = \mathrm{Ker}\,(I_n - A^\dagger A)$:

$$(I_n - A^\dagger A)A^\dagger b = A^\dagger b - A^\dagger AA^\dagger b = 0.$$

Nyní podle Pythagorovy Věty 8.7 pro každé $y \in \mathbb{R}^n$ platí

$$\|A^\dagger b + (I_n - A^\dagger A)y\|_2^2 = \|A^\dagger b\|_2^2 + \|(I_n - A^\dagger A)y\|_2^2 \geq \|A^\dagger b\|_2^2.$$

Tedy $A^\dagger b$ nejmenší eukleidovskou normu. Každý jiný vektor z X má normu větší, protože $(I_n - A^\dagger A)y \neq 0$ implikuje $\|(I_n - A^\dagger A)y\|_2 > 0$. □

Věta 13.25 (Pseudoinverzní matice a metoda nejmenších čtverců)**.** *Buď $A \in \mathbb{R}^{m\times n}$, $b \in \mathbb{R}^m$ a X množina přibližných řešení soustavy $Ax = b$ metodou nejmenších čtverců. Pak*

$$X = A^\dagger b + \mathcal{S}(I_n - A^\dagger A).$$

Navíc, ze všech vektorů z množiny X má $A^\dagger b$ nejmenší eukleidovskou normu, a je to jediné řešení s touto vlastností.

Důkaz. Množina přibližných řešení soustavy $Ax = b$ metodou nejmenších čtverců je popsána soustavou $A^TAx = A^Tb$, viz Věta 8.39. Dosazením $x := A^\dagger b$ dostaneme

$$A^TA(A^\dagger b) = A^T(AA^\dagger)^Tb = (AA^\dagger A)^Tb = A^Tb,$$

tudíž $A^\dagger b \in X$. Protože $X \neq \emptyset$, podle Věty 13.24 máme

$$X = (A^TA)^\dagger(A^Tb) + \mathcal{S}(I_n - (A^TA)^\dagger(A^TA)).$$

Jelikož $(A^TA)^\dagger A^T = A^\dagger$ a $(A^TA)^\dagger(A^TA) = A^\dagger A$, má množina X požadovaný popis a $A^\dagger b$ požadovanou vlastnost. □

13.7 Maticová norma

Nyní se vrátíme zpět k normám a podíváme se na to, jak zavést normu pro matice. Přestože normy jsme probírali v Sekci 8.1, důležitou maticovou normu představuje největší singulární číslo matice, proto zařazujeme tuto část k SVD rozkladu.

V zásadě, matice z $\mathbb{R}^{m\times n}$ tvoří vektorový prostor, proto na matice můžeme pohlížet jako na vektory. Nicméně, pro maticovou normu se uvažuje ještě jedna vlastnost navíc, proto máme speciální definici.

Definice 13.26 (Norma matice)**.** Třída zobrazení $\|\cdot\|\colon \mathbb{R}^{m\times n} \to \mathbb{R}$ je reálná *maticová norma*, pokud je to norma pro libovolné m, n a navíc splňuje:

$$\|AB\| \leq \|A\| \cdot \|B\| \quad \text{pro všechna } A \in \mathbb{R}^{m\times p},\ B \in \mathbb{R}^{p\times n}.$$

Příklady maticových norem:

- *Frobeniova norma*: $\|A\|_F := \sqrt{\sum_{i=1}^m \sum_{j=1}^n a_{ij}^2}$.

  Je to vlastně eukleidovská norma vektoru tvořeného všemi prvky matice A.

- *Maticová p-norma*: $\|A\|_p = \max_{x:\|x\|_p=1} \|Ax\|_p$.

  V této definici používáme vektorovou p-normu. Výslednou normu si můžeme představit takto: Zobrazíme jednotkovou kouli (v p-normě, tedy vektory splňující $\|x\|_p = 1$) lineárním zobrazením $x \mapsto Ax$ a v obrazu vybereme vektor s největší normou. Pro různé hodnoty p dostáváme různé maticové normy. Ty nejdůležitější shrnuje následující věta.

Věta 13.27 (Maticové p-normy)**.** *Buď $A \in \mathbb{R}^{m\times n}$. Pak maticové p-normy pro $p \in \{1, 2, \infty\}$ mají tvar*

(1) $\|A\|_2 = \sigma_1(A)$ *(největší singulární číslo),*

(2) $\|A\|_1 = \max_{j=1,\dots,n} \sum_{i=1}^{m} |a_{ij}|$,

(3) $\|A\|_\infty = \max_{i=1,\dots,m} \sum_{j=1}^{n} |a_{ij}| = \|A^T\|_1$.

Důkaz.

(1) Jak jsme již zmínili, $\|A\|_2$ je velikost největšího bodu elipsy, vzniklé obrazem jednotkové koule při zobrazení $x \mapsto Ax$. Ze Sekce 13.5 (SVD a geometrie lineárního zobrazení) víme, že tato hodnota je $\sigma_1(A)$.

(2) Označme $c \coloneqq \max_{j=1,\dots,n} \sum_{i=1}^{m} |a_{ij}|$. Připomeňme, že $\|x\|_1 = \sum_{k=1}^{n} |x_k|$. Pro jakékoli x takové, že $\|x\|_1 = 1$, platí

$$\|Ax\|_1 = \sum_{i=1}^{m} \left| \sum_{j=1}^{n} a_{ij}x_j \right| \le \sum_{i=1}^{m}\sum_{j=1}^{n} |a_{ij}||x_j| = \sum_{j=1}^{n} |x_j| \left(\sum_{i=1}^{m} |a_{ij}| \right) \le \sum_{j=1}^{n} |x_j| c = c.$$

Zároveň se nabyde rovnost $\|Ax\|_1 = c$ vhodnou volbou jednotkového vektoru $x = e_i$. Proto dostáváme $\max_{x:\|x\|_1=1} \|Ax\|_1 = c$.

(3) Označme $c \coloneqq \max_{i=1,\dots,m} \sum_{j=1}^{n} |a_{ij}|$. Připomeňme, že $\|x\|_\infty = \max_{k=1,\dots,n} |x_k|$. Pro jakékoli x takové, že $\|x\|_\infty = 1$, platí

$$\|Ax\|_\infty = \max_{i=1,\dots,m} \left| \sum_{j=1}^{n} a_{ij}x_j \right| \le \max_{i=1,\dots,m} \sum_{j=1}^{n} |a_{ij}||x_j| \le \max_{i=1,\dots,m} \sum_{j=1}^{n} |a_{ij}| = c.$$

Zároveň se nabyde rovnost $\|Ax\|_\infty = c$ vhodnou volbou vektoru $x \in \{\pm 1\}^n$. Proto dostáváme $\max_{x:\|x\|_\infty=1} \|Ax\|_\infty = c$. □

Poznámka 13.28. Mějme vektor $v \in \mathbb{R}^n$ a libovolné p. Nyní výraz $\|v\|_p$ může označovat jak vektorovou, tak maticovou p-normu. To však nevadí, protože obě dávají stejnou hodnotu:

$$\|v\|_p = \max_{x\in\mathbb{R}:\|x\|=1} \|vx\|_p = \max_{x\in\{\pm 1\}} \|vx\|_p = \| \pm v\|_p = \|v\|_p.$$

Začali jsme s maticovou normou a ukázali, že se rovná vektorové.

Víme z Věty 8.45, že přenásobení vektoru ortogonální maticí nemění jeho eukleidovskou normu. Nyní tvrzení zobecníme pro maticovou 2-normu.

Tvrzení 13.29. *Buď $A \in \mathbb{R}^{m\times n}$ a buďte $Q \in \mathbb{R}^{m\times m}$, $R \in \mathbb{R}^{n\times n}$ ortogonální. Pak $\|QAR\|_2 = \|A\|_2$.*

Důkaz.

$$\begin{aligned}\|QAR\|_2 &= \max_{x:\|x\|_2=1} \|QARx\|_2 = \max_{x:\|x\|_2=1} \|ARx\|_2 \\ &= \max_{y:\|R^Ty\|_2=1} \|Ay\|_2 = \max_{y:\|y\|_2=1} \|Ay\|_2 = \|A\|_2.\end{aligned}$$

□

Maticové normy se objevují v různých souvislostech. Nejprve ukažme, že dávají odhad na velikost vlastních čísel.

Věta 13.30 (Odhad spektrálního poloměru pomocí normy)**.** *Buď $A \in \mathbb{R}^{n\times n}$. Pak pro každou maticovou normu $\rho(A) \le \|A\|$.*

Důkaz. Buď $\lambda \in \mathbb{C}$ libovolné vlastní číslo a x odpovídající vlastní vektor matice A. Pak $Ax = \lambda x$, tedy

$$|\lambda| \cdot \|x\| = \|\lambda x\| = \|Ax\| \leq \|A\| \cdot \|x\|.$$

Vydělením $\|x\| \neq 0$ dostáváme $|\lambda| \leq \|A\|$. □

Další velmi zajímavá vlastnost singulárních čísel je, že σ_i udává v 2-normě vzdálenost matice k nejbližší matici hodnosti nanejvýš $i-1$. V důkazu následující věty je schované i to, jak tuto matici sestrojit – ne náhodou je to matice z low-rank aproximace (Sekce 13.5). Speciálně, nejmenší singulární číslo σ_n matice $A \in \mathbb{R}^{n\times n}$ udává vzdálenost k nejbližší singulární matici, srov. Sekce 13.5 (SVD a míra regularity).

Věta 13.31 (Interpretace singulárních čísel)**.** *Buď $A \in \mathbb{R}^{m\times n}$ se singulárními čísly $\sigma_1, \ldots, \sigma_r$. Pak $\sigma_i = \min\{\|A-B\|_2;\ B \in \mathbb{R}^{m\times n}, \operatorname{rank}(B) \leq i-1\}$ pro každé $i = 1, \ldots, r$.*

Důkaz. Nerovnost „$\geq$“. Nechť $A = U\Sigma V^T$ je SVD rozklad matice A. Definujme matici předpisem $B \coloneqq U\operatorname{diag}(\sigma_1, \ldots, \sigma_{i-1}, 0, \ldots, 0)V^T$. Pak

$$\|A-B\|_2 = \|U\operatorname{diag}(0, \ldots, 0, \sigma_i, \ldots, \sigma_n)V^T\|_2 = \|\operatorname{diag}(0, \ldots, 0, \sigma_i, \ldots, \sigma_n)\|_2 = \sigma_i.$$

Nerovnost „$\leq$“. Buď $B \in \mathbb{R}^{n\times n}$ libovolná matice hodnosti nanejvýš $i-1$ a ukážeme, že $\|A-B\|_2 \geq \sigma_i$. Nechť V_1 sestává z prvních i sloupců matice V. Buď $o \neq z \in \operatorname{Ker}(B) \cap \mathcal{S}(V_1)$, to jest $Bz = o$, a navíc normujeme z tak, aby $\|z\|_2 = 1$. Takový vektor existuje, protože $\dim \operatorname{Ker}(B) \geq n-i+1$ a $\dim \mathcal{S}(V_1) = i$. Pak

$$\|A-B\|_2^2 = \max_{x:\|x\|_2=1} \|(A-B)x\|_2^2 \geq \|(A-B)z\|_2^2 = \|Az\|_2^2 = \|U\Sigma V^T z\|_2^2.$$

Protože $z \in \mathcal{S}(V_1)$, lze psát $z = Vy$ pro nějaký vektor $y = (y_1, \ldots, y_i, 0, \ldots, 0)^T$, přičemž $\|y\|_2 = \|V^T z\|_2 = \|z\|_2 = 1$. Nyní

$$\|U\Sigma V^T z\|_2^2 = \|U\Sigma V^T V y\|_2^2 = \|\Sigma y\|_2^2 = \sum_{j=1}^{i} \sigma_j^2 y_j^2 \geq \sum_{j=1}^{i} \sigma_i^2 y_j^2 = \sigma_i^2 \|y\|_2^2 = \sigma_i^2.$$ □

Problémy

13.1. Navrhněte metodu na QR rozklad za použití Givensových matic.

13.2. Za použití QR rozkladu popište všechna řešení soustavy $Ax = b$, kde A má lineárně nezávislé řádky.

13.3. Ukažte, že Frobeniova a p-norma jsou skutečně maticovými normami.

Značení

$U + V$	spojení podprostorů, $U + V = \{u + v;\, u \in U, v \in V\}$, str. 52
$U + a$	součet množiny vektorů a vektoru, $U + a = \{v + a;\, v \in U\}$, str. 69
$[v]_B$	souřadnice vektoru v vzhledem k bázi B, str. 50
$\exists$	existenční kvantifikátor („existuje“), str. 8
$\forall$	univerzální kvantifikátor („pro všechna“), str. 8
${}_{B_2}[f]_{B_1}$	matice lineárního zobrazení f vzhledem k bázi B_1, B_2, str. 61
$\|A\|$	norma matice A, str. 145
$\|x\|$	norma vektoru x, str. 77
$\|x\|_2$	eukleidovská norma, $\|x\|_2 = \sqrt{\sum_{i=1}^{n} x_i^2}$, str. 78
$\|x\|_p$	p-norma vektoru x, str. 78
$\Subset$	podprostor, str. 46
$\prod$	produkt (součin), str. 7
$g \circ f$	složené zobrazení, $(g \circ f)(x) = g(f(x))$, str. 8
$\langle x, y \rangle$	skalární součin vektorů x, y, str. 75
$\sum$	suma (součet), str. 7
$H(a)$	Householderova matice vytvořená z a, str. 87
$M^\perp$	ortogonální doplněk množiny M, str. 81
$\mathrm{adj}\,(A)$	adjungovaná matice k A, str. 96
A_{i*}	i-tý řádek matice A, str. 14
A_{*j}	j-tý sloupec matice A, str. 14
$A^\dagger$	pseudoinverze matice A, str. 143
A^*	Hermitovská transpozice matice, $A^* = \overline{A}^T$, str. 113
A^T	transpozice matice, str. 22
$\mathbb{C}$	množina komplexních čísel, str. 9
$C(p)$	matice společnice polynomu $p(x)$, str. 104
$\det(A)$	determinant matice A, str. 91
$\mathrm{diag}(v)$	diagonální matice s diagonálními prvky $v_1, \ldots, v_n$, str. 23
$\dim V$	dimenze prostoru V, str. 51
e_i	jednotkový vektor, str. 22
$E_i(\alpha)$	elementární matice pro vynásobení i-tého řádku číslem $\alpha \neq 0$, str. 25
E_{ij}	elementární matice pro prohození dvou řádků i, j, str. 25
$E_{ij}(\alpha)$	elementární matice pro přičtení α-násobku j-tého řádku k i-tému, str. 25
$f(U)$	obraz množiny U při zobrazení f, str. 60
$\mathsf{Im}(z)$	imaginární část komplexního čísla z, str. 9
I_n, I	jednotková matice, str. 22
$J_k(\lambda)$	Jordanova buňka, str. 110
kan	kanonická báze, str. 49

$\mathrm{Ker}\,(A)$	jádro matice A, str. 54
$\mathrm{Ker}\,(f)$	jádro zobrazení f, str. 60
$\mathbb{N}$	množina přirozených čísel
$p_A(\lambda)$	charakteristický polynom matice A, str. 102
$\mathcal{P}^n$	prostor reálných polynomů proměnné x stupně nanejvýš n, str. 45
$\mathbb{Q}$	množina racionálních čísel
$\mathbb{R}$	množina reálných čísel
$\mathrm{rank}(A)$	hodnost matice A, str. 15
$\mathsf{Re}(z)$	reálná část komplexního čísla z, str. 9
REF	odstupňovaný tvar matice, str. 15
$\rho(A)$	spektrální poloměr matice A, str. 102
RREF	redukovaný odstupňovaný tvar matice, str. 17
$\mathcal{R}(A)$	řádkový prostor matice A, str. 53
$\mathcal{S}(A)$	sloupcový prostor matice A, str. 53
$\mathrm{sgn}(p)$	znaménko permutace p, str. 37
S_n	množina všech permutací na $\{1, \ldots, n\}$, str. 36
$\mathrm{span}(W)$	lineární obal množiny vektorů W, str. 47
$\mathbb{T}$	nějaké těleso, str. 39
$\mathrm{trace}(A)$	stopa matice, $\mathrm{trace}(A) = \sum_{i=1}^{n} a_{ii}$, str. 89
$\overline{z}$	komplexně sdružené číslo, str. 9
$\mathbb{Z}$	množina celých čísel
$\mathbb{Z}_n$	množina $\{0, 1, \ldots, n-1\}$, str. 39

Literatura

J. Bečvář. *Lineární algebra.* Matfyzpress, Praha, třetí vydání, 2005.

M. Berger. *Geometry I.* Springer, Berlin, 1987.

L. Bican. *Lineární algebra a geometrie.* Academia, Praha, druhé vydání, 2009.

B. A. Cipra. The best of the 20th century: Editors name top 10 algorithms. *SIAM News*, 33:1–2, 2000.

J. Dattorro. *Convex Optimization & Euclidean Distance Geometry.* Meboo Publishing, USA, 2011.

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.

B. Gärtner and J. Matoušek. *Approximation Algorithms and Semidefinite Programming.* Springer, Berlin Heidelberg, 2012.

R. A. Horn and C. R. Johnson. *Matrix analysis.* Cambridge University Press, Cambridge, 1985.

T. Krisl. Cauchyova–Schwarzova nerovnost. Diplomová práce, Masarykova Univerzita, Přírodovědecká fakulta, Ústav matematiky a statistiky, Brno, 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 a J. Nešetřil. *Kapitoly z diskrétní matematiky.* Karolinum, Praha, čtvrté vydání, 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), 1997.
`http://kam.mff.cuni.cz/~hladik/doc/Rohn-LP_NLP-1997.pdf`

J. Rohn. *Lineární algebra a optimalizace.* Karolinum, Praha, 2004. 1st edition.

G. Strang. *Linear algebra and its applications.* Thomson, USA, 3rd edition, 1988.

J. Tůma. Texty k přednášce Lineární algebra, 2003.
`http://www.karlin.mff.cuni.cz/~tuma/NNlinalg.htm`

M. Turk and A. Pentland. Eigenfaces for recognition. *J. Cognitive Neuroscience*, 3(1):71–86, 1991.
`http:/www.face-rec.org/algorithms/PCA/jcn.pdf`.

K. Výborný a M. Zahradník. *Používáme lineární algebru.* Karolinum, Praha, první vydání, 2002.
`http://matematika.cuni.cz/zahradnik-plas.html`