Polynomy

Polynom je možno definovat dvěma způsoby:

- jako reálnou nebo komplexní funkci, jejichž hodnoty jsou dány jistým vzorcem,
- jako ten vzorec samotný.

a) algebra-all, 1, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) Viz p. d. 4/2010

První způsob zavedení polynomu

Definice 1: *Polynom* je komplexní funkce $p : \mathbf{C} \to \mathbf{C}$, pro kterou existují komplexní čísla $a_0, a_1, \ldots, a_n$ taková, že

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

pro všechna $x \in \mathbf{C}$.

Čísla $a_0, a_1, \ldots, a_n$ nazýváme *koeficienty polynomu*.

Dále zavádíme pojmy:

Rovnost polynomů jako rovnost funkcí:
$p = q$, když $p(x) = q(x)$ pro všechna $x \in \mathbf{C}$.

Součet polynomů, násobek polynomu jako součet a násobek funkcí:
$p+q$ je funkce, pro kterou $(p+q)(x) = p(x)+q(x)$ pro všechna $x \in \mathbf{C}$,

αp je funkce, pro kterou $(\alpha p)(x) = \alpha \cdot p(x)$ pro všechna $x \in \mathbf{C}$.

Druhý způsob zavedení polynomu

Definice 2: *Polynom* je vzorec tvaru

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

kde $a_0, a_1, \ldots, a_n$ jsou komplexní čísla a x je formální proměnná.

Čísla $a_0, a_1, \ldots, a_n$ nazýváme *koeficienty polynomu*.

Hodnota polynomu $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ v bodě $\alpha \in \mathbf{C}$ je komplexní číslo, které dostaneme dosazením čísla α za proměnou x do uvedeného vzorce.

Dále zavádíme pojmy:

Rovnost polynomů: Dva polynomy se rovnají, pokud současně platí

- koeficienty se stejnými indexy se rovnají,
- má-li jeden polynom koeficient, který druhý polynom nemá, pak tento koeficient je nulový.

Součet polynomů, násobek polynomu: jako součet příslušných vzorců a násobek vzorce konstantou. Přesněji:

Má-li polynom p koeficienty $a_0, a_1, \ldots, a_m$ a má-li polynom q koeficienty $b_0, b_1, \ldots, b_n$ a je $m \le n$, pak polynom $p + q$ má koeficienty

$$a_0 + b_0, a_1 + b_1, \ldots, a_m + b_m, b_{m+1}, \ldots b_n.$$

Dále polynom αp má koeficienty $\alpha a_0, \alpha a_1, \ldots, \alpha a_m$.

Výsledky operací jsou tedy popsány pomocí svých koeficientů *algoritmicky*. Na vstupu do algoritmu jsou koeficienty polynomů, které sčítáme resp. násobíme. S proměnnou x algoritmy nepracují.

Součin polynomů

Součin dvou polynomů p a q, které mají koeficienty $a_0, a_1, \ldots, a_m$ a $b_0, b_1, \ldots, b_n$, je polynom, který má koeficienty $c_0, c_1, \ldots, c_{m+n}$ takové, že

$$c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0,$$

přičemž v tomto vzorci klademe $a_i = 0$ pro $i > m$ a $b_i = 0$ pro $i > n$.

Jak jsme na to přišli?

$$\begin{aligned}(a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m) \cdot (b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n) = \\ = (a_0 b_0) + (a_0 b_1 + a_1 b_0)x + \\ + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots + \\ + (a_0 b_{m+n} + a_1 b_{m+n-1} + \cdots + a_m b_n + \cdots + a_{m+n} b_0)x^{m+n}.\end{aligned}$$

Vztah mezi funkcí a koeficienty

Jaký je vztah mezi prvním a druhým způsobem pojetí polynomu?

Tj. mezi polynomem jako *funkcí* a polynomem jako *vzorcem* charakterizovaným svými *koeficienty*?

Tvrzení:

- Polynom daný koeficienty jednoznačně určuje funkci podle definice 1.
- Polynom jako funkce má své koeficienty určeny jednoznačně (až na „přebývající“ nulové koeficienty).

První část tvrzení je zřejmá. Vzorec určuje funkci.

Druhá část tvrzení není zcela zřejmá. K jejímu důkazu použijeme pomocnou větu:

Věta: nulová funkce je polynom, který musí mít všechny koeficienty nulové.

Důkaz: Nechť $p(x) = a_n x^n + \ldots + a_1 x + a_0 = 0$ pro všechna $x \in \mathbf{C}$, Koeficient a_0 musí být nulový (stačí dostadit $x = 0$). Takže platí $p(x) = x\,(a_n x^{n-1} + \ldots + a_1) = x\,q(x) = 0$. Polynom q je nulový pro všechna $x \in \mathbf{C} \setminus \{0\}$. Protože q je funkce spojitá, je také $q(0) = 0$. Dosazením $x = 0$ dostáváme $a_1 = 0$ a postup můžeme opakovat. Dostaneme $a_2 = 0, \ldots, a_n = 0$.

Vraťme se k tvrzení: Polynom jako funkce má své koeficienty určeny jednoznačně.

Důkaz: Ať polynom p (jako funkce) má koeficienty $a_0, a_1, \ldots, a_n$ a také ať má koeficienty $b_0, b_1, \ldots, b_n$ (koeficienty doplníme nulami, kdyby původně měl být počet koeficientů různý). Funkce $p - p$ je nulová a má zřejmě koeficienty $a_0 - b_0, a_1 - b_1, \ldots, a_n - b_n$. Podle předchozí věty musejí být tyto koeficienty nulové, takže musí být $a_i = b_i$ pro všechna i. Nemůže se tedy stát, aby měl jeden polynom (jako funkce) dvě sady různých koeficientů.

Stupeň polynomu

Definice: polynom se všemi koeficienty nulovými se nazývá *nulový polynom*.

Stupeň polynomu p s koeficienty $a_0, a_1, \ldots, a_n$ je největší index i takový, že $a_i \neq 0$. Stupeň nulového polynomu definujeme hodnotou -1.

Stupeň polynomu p značíme $\operatorname{St} p$

Pozorování: Pro nenulové polynomy p a q platí:

$$\operatorname{St}(p+q) \leq \max(\operatorname{St} p, \operatorname{St} q), \qquad \operatorname{St}(p \cdot q) = \operatorname{St} p + \operatorname{St} q$$

Dělení polynomu polynomem se zbytkem

Věta: Pro polynomy p a q (polynom q nenulový) existují polynomy r a z takové, že

- $p = r \cdot q + z$, (neboli $p/q = r + z/q$),
- $\operatorname{St} z < \operatorname{St} q$.

Polynomu r říkáme *částečný podíl* a polynomu z říkáme *zbytek* při dělení polynomu p polynomem q.

Platnost věty je zaručena existencí algoritmu, který pro každé p, q vytvoří r a z uvedených vlastností.

Algoritmus (příklad):

$$\begin{aligned}
&(2x^5 - 3x^4 + 3x^3 - x^2 - 6x + 8) : (x^2 - 2x + 4) = 2x^3 + x^2 - 3x - 11 \\
&\underline{-(2x^5 - 4x^4 + 8x^3)} \\
&\qquad x^4 - 5x^3 - x^2 - 6x + 8 \\
&\qquad \underline{-(x^4 - 2x^3 + 4x^2)} \\
&\qquad\quad -3x^3 - 5x^2 - 6x + 8 \\
&\qquad\quad \underline{-(-3x^3 + 6x^2 - 12x)} \\
&\qquad\qquad -11x^2 + 6x + 8 \\
&\qquad\qquad \underline{-(-11x^2 + 22x - 44)} \\
&\qquad\qquad\quad -16x + 52
\end{aligned}$$

Algoritmus (náčrt):

$$\begin{aligned}
&p && : \; q \;=\; c_k x^k + c_{k-1}x^{k-1} + \ldots + c_0 \\
&\underline{-c_k x^k \cdot q} \\
&p - c_k x^k \cdot q \\
&\quad \underline{-c_{k-1}x^{k-1} \cdot q} \\
&\quad p - c_k x^k \cdot q - c_{k-1}x^{k-1} \cdot q \\
&\qquad \underline{\qquad\qquad \ldots} \\
&\qquad p - (c_k x^k + c_{k-1}x^{k-1} + \ldots + c_0) \cdot q = p - r\,q = z
\end{aligned}$$

Algoritmus:

- vždy skončí po konečně mnoha krocích,
- vyprodukuje polynomy r a z, které mají vlastnosti podle věty.

(rozmyslete si, proč)

Jednoznačnost částečného podílu a zbytku

Polynomy r a z s vlastnomstmi podle předchozí věty jsou určeny výchozími polynomy p a q jednoznačně.

Důkaz: Ať kromě r a z ještě polynomy r_1 a z_1 mají uvedené vlastnosti, tj.

$$p = r \cdot q + z = r_1 \cdot q + z_1, \qquad \operatorname{St} z < \operatorname{St} q, \quad \operatorname{St} z_1 < \operatorname{St} q.$$

Po odečtení první rovnosti je $(r - r_1)\,q = z_1 - z$. Stupeň na pravé straně je menší než q, takže na levé straně musí být q násobeno nulou. Tj. $r = r_1$. Z toho také plyne, že $z = z_1$.

Hornerovo schéma =

= algoritmus na efektivní vyhodnocení polynomu v daném bodě.

$$\begin{aligned}
p(\alpha) &= a_n\alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_2\alpha^2 + a_1\alpha + a_0 = \\
&= ((\cdots((a_n\alpha + a_{n-1})\,\alpha + a_{n-2})\,\alpha + \cdots + a_2)\,\alpha + a_1)\,\alpha + a_0.
\end{aligned}$$

Mezivýpočty (závorky) mohou zůstávat v registru procesoru.

Odhadněte počet násobení a sčítání při vyhodnocení polynomu stupně n v bodě

a) přímo pomocí vzorce z definice polynomu

b) podle Hornerova schématu

Tři řádky Hornerova schématu

Při psaní mezivýpočtů na papír můžeme použít třířádkové schéma:

$$\begin{array}{rccccccc}
 & a_n & a_{n-1} & a_{n-2} & \ldots & a_2 & a_1 & a_0 \\
\alpha: & & \alpha b_{n-1} & \alpha b_{n-2} & \ldots & \alpha b_2 & \alpha b_1 & \alpha b_0 \\
\hline
 & b_{n-1} & b_{n-2} & b_{n-3} & \ldots & b_1 & b_0 & p(\alpha)
\end{array}$$

kde $b_{n-1} = a_n$, $b_{k-1} = a_k + \alpha b_k$ pro $k = n-1, n-2, \ldots, 3, 2, 1$.

Vyplatí se to, protože platí následující tvrzení ...

Tvrzení: třetí řádek Hornerova schématu obsahuje koeficienty b_i, což jsou koeficienty polynomu r, pro který platí:

$$p(x) = r(x)\,(x - \alpha) + p(\alpha)$$

tedy: r je částečný podíl polynomu p polynomem $(x - \alpha)$.

Důkaz: je třeba využít rekurentních vztahů

$$b_{n-1} = a_n, \quad b_{k-1} = a_k + \alpha b_k$$

a propočítat výraz $r(x)\,(x - \alpha) + p(\alpha)$.

K čemu to je: nemusíme pro výpočet částečného podílu polynomu polynomem stupně prvního používat algoritmus ze slídu [12].

Kořen polynomu

Definice: *Kořen polynomu p* je takové číslo $\alpha \in \mathbf{C}$, pro které je $p(\alpha) = 0$.

Jinými slovy: kořen je číslo, ve kterém má polynom nulovou hodnotu.

Definice: *Kořenový činitel polynomu p* je polynom tvaru $x-\alpha$, kde α je kořen polynomu p.

Pozorování: Polynom je dělitelný svým kořenovým činitelem.

Důkaz: Částečný podíl polynomu p kořenovým činitelem $(x-\alpha)$ musí mít stupeň zbytku menší než 1, takže zbytek je konstanta z. Takže

$$p(x) = r(x)\cdot(x-\alpha)+z.$$

Po dosazení $x=\alpha$ dostáváme $0 = p(\alpha) = r(\alpha)\cdot 0 + z$, takže $z=0$.

Základní věta algebry

Věta: Každý polynom stupně aspoň prvního má v $\mathbf{C}$ kořen.

Poznámka: Polynom stupně nula je nenulová konstanta, tj. nemá kořen.

Pozorování: Třebaže má polynom stupně aspoň prvního reálné koeficienty, nemusí mít žádný reálný kořen. Například polynom x^2+1. Základní věta algebry praví, že polynom má *komplexní*, kořen.

Důkaz základní věty algebry: neuvádíme.

Rozklad polynomu na kořenové činitele

Nechť p je polynom stupně aspoň prvního. Pak má kořen α_1 a je dělitelný kořenovým činitelem $x-\alpha_1$, tedy $p = (x-\alpha_1)\cdot p_1(x)$. Polynom p_1 má stupeň o jeden menší, než stupeň p.

Nechť p_1 je polynom stupně aspoň prvního. Pak má kořen α_2 a je dělitelný činitelem $x-\alpha_2$, tedy $p = (x-\alpha_1)\cdot p_1(x) = (x-\alpha_1)(x-\alpha_2)\cdot p_2(x)$. Polynom p_2 má stupeň o dva menší, než stupeň p.

Opakovaným postupem této úvahy dostáváme

$$p = (x-\alpha_1)\cdot p_1(x) = (x-\alpha_1)\cdot(x-\alpha_2)\cdots(x-\alpha_n)\cdot K,$$

kde $K = p_n$ je polynom stupně nultého (nenulová konstanta).

Tomuto vzorci se říká *rozklad polynomu p na kořenové činitele*.

Násobnost kořene

Pozorování: Všechna čísla α_i v předchozím vzorci (v rozkladu na kořenové činitele) jsou kořeny polynomu p.

Pozorování: Počet kořenových činitelů v předchozím vzorci je roven stupni polynomu.

Definice: *Násobnost* kořene α je počet výskytů čísla α v kořenových činitelích v rozkladu na kořenové činitele.

Pozorování: Každý polynom má tolik kořenů, kolik je jeho stupeň. Každý kořen ovšem započítáme tolikrát, kolik činí jeho násobnost.

Pozorování: Konstanta K v rozkladu na kořenové činitele je rovna koeficientu a_n.

Nalézt rozklad na kořenové činitele

není algebraicky pro obecný polynom p možné.

Při hledání rozkladu je totiž potřeba najít všechny kořeny polynomu p na základě znalosti jeho koeficientů. Vzorce existují pro polynomy stupně 1, 2, 3, 4 a dále pro některé speciální polynomy.

Příklad: Pro polynom stupně 2 vzorce pro kořeny jistě znáte:

$$\alpha_1 = \frac{-a_1+\sqrt{a_1^2-4a_2a_0}}{2a_2}, \qquad \alpha_2 = \frac{-a_1-\sqrt{a_1^2-4a_2a_0}}{2a_2}$$

Pro polynomy stupně pátého a vyššího algebraické vzorce *neexistují*. Pomocí teorie grup Niels Abel a Évartiste Galois dokázali, že tyto vzorce skutečně neexistují (tj. je dokázáno, že vzorce ani v budoucnu nikdo objeví).

To není ve sporu se základní větou algebry, která říká, že kořen existuje (zdůvodněte proč).

Speciální případ: kořeny jsou celá čísla

Jsou-li koeficienty polynomu celočíselné, pak je možno vyzkoušet, zda nepůjde nalézt kořen mezi děliteli koeficientu a_0. Těch je konečně mnoho. Pokud mezi nimi kořen nenalezneme, nemáme sice rozklad, ale máme aspoň jistotu, že polynom nemá další celočíselné kořeny. Platí totiž:

Věta: Je-li α celočíselný kořen polynomu p s celočíselnými koeficienty, pak α dělí koeficient a_0.

Důkaz: V rovnosti $0 = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$ (která plyne z toho, že α je kořen) odečteme z obou stran a_0 a ze zbytku vytkneme α. Dostáváme $a_0 = -\alpha\cdot(a_n\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1) = \alpha\cdot c$, kde c je celé číslo. Takže α dělí a_0.

Příklad

Rozložíme $p(x) = x^5 - 12x^4 + 48x^3 - 62x^2 - 33x + 90$. Má-li být kořenem celé číslo, může to být jedině dělitel devadesátky, tedy čísla $1, 2, 3, 5, 6, \ldots, 90, -1, -2, -3, \ldots, -90$. Těchto konečně mnoho čísel můžeme zkusit dosadit do polynomu. Vychází např. $p(2) = 0$, takže 2 je kořen. Další kořeny stačí hledat v polynomu $p_1(x) = p(x)/(x-2)$. Koeficienty tohoto polynomu najdeme ve třetím řádku Hornerova schématu. Je $p_1(x) = x^4 - 10x^3 + 28x^2 - 6x - 45$. Tento polynom má kořen 3 a $p_2(x) = p(x)/((x-2)(x-3)) = x^3 - 7x^2 + 7x + 15$. Trojka je znovu kořen polynomu p_2 a $p_3(x) = p(x)/((x-2)(x-3)^2) = x^2 - 4x - 5$. Tento kvadratický polynom má kořeny 5 a -1. Rozklad daného polynomu je: $p(x) = (x-2)(x-3)^2(x-5)(x+1)$.

Jiný příklad: rozklad polynomu $x^5-12x^4+48x^3-62x^2-33x+91$ nelze algebraicky nalézt. Dělitele 91 jsou $1, 7, 13, 91, -1, -7, -13, -91$. Můžeme zjistit, že žádné z těchto čísel není kořen, takže polynom nemá celočíselné kořeny.

Komplexně sdružené kořeny

Polynomy s reálnými koeficienty ne vždy mají jen reálné kořeny. Komplexní kořeny se ovšem v takovém případě vyskytují v párech:

Tvrzení: Je-li $\alpha \in \mathbf{C}$ kořen polynomu p s reálnými koeficienty, pak $\overline{\alpha}$ (komplexně sdružené číslo k číslu α) je také kořen polynomu p, dokonce stejné násobnosti.

Proč je $\overline{\alpha}$ kořen? Platí

$$\begin{aligned} p(\overline{\alpha}) &= a_0 + a_1\overline{\alpha} + a_2\overline{\alpha}^2 + \cdots + a_n\overline{\alpha}^n = \\ &= \overline{a_0} + \overline{a_1}\ \overline{\alpha} + \overline{a_2}\ \overline{\alpha^2} + \cdots + \overline{a_n}\ \overline{\alpha^n} = \\ &= \overline{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n} = \overline{p(\alpha)} = \overline{0} = 0. \end{aligned}$$

Proč mají α a $\overline{\alpha}$ stejnou násobnost? Součin $(x-\alpha)\cdot(x-\overline{\alpha})$ je polynom s reálnými koeficienty (propočítejte si to).

Reálný rozklad

Dvojici kořenových činitelů $(x-\alpha)$ a $(x-\overline{\alpha})$ můžeme roznásobit a dostáváme kvadratický polynom s reálnými koeficienty

$$(x-\alpha)\cdot(x-\overline{\alpha}) = x^2+\beta x+\gamma.$$

Nahradíme-li všechny takové páry kořenových činitelů jejich součiny, dostáváme v případě polynomu s reálnými koeficienty:

- součin kořenových činitelů s reálnými kořeny násobený
- součinem kvadratických polynomů, které nemají reálné kořeny.

Reálný rozklad má obecně tvar

$$p(x) = c\cdot(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)(x^2+\beta_1x+\gamma_1)\cdots(x^2+\beta_mx+\gamma_m)$$

Reálný rozklad s násobnostmi

Zapíšeme-li v reálném rozkladu vícenásobné kořenové činitele pomocí mocnin a stejně tak opakované kvadratické polynomy pomocí mocnin, dostáváme rozklad:

$$p(x) = c\,(x-\alpha_1)^{u_1}\cdots(x-\alpha_k)^{u_k}\cdot(x^2+\beta_1x+\gamma_1)^{v_1}\cdots(x^2+\beta_mx+\gamma_m)^{v_m}$$

Takový rozklad se často používá,

- aby se výpočet obešel bez použití komplexních čísel a
- aby explicitně počítal s možností výskytu vícenásobných kořenů

(např. integrál racionální lomené funkce).

Parciální zlomky

Věta: Nechť $\mathrm{St}\,p < \mathrm{St}\,q$ a α je k násobným kořenem polynomu q. Označme $q = (x-\alpha)^k\cdot q_1$. Pak existuje $a\in\mathbf{C}$ a polynom p_1 takový, že $\mathrm{St}\,p_1 < \mathrm{St}\,q-1$ a

$$\frac{p(x)}{q(x)} = \frac{a}{(x-\alpha)^k}+\frac{p_1(x)}{(x-\alpha)^{k-1}q_1(x)} \quad \forall\, x\in\mathbf{C} \text{ takové, že } q(x)\neq 0$$

Důkaz: Protože α je k-násobným kořenem q, platí $q_1(\alpha)\neq 0$. Dokazovaná rovnost je ekvivalentní s $p(x) = a\cdot q_1(x)+p_1(x)\cdot(x-\alpha)$. Po dosazení $\alpha\to x$ je $p(\alpha) = a\cdot q_1(\alpha)$, tj. $a = p(\alpha)/q_1(\alpha)$. Polynom $p(x)-a\cdot q_1(x)$ má stupeň nejvýše roven $\max(\mathrm{St}\,p,\mathrm{St}\,q_1)$ a má kořen α. Dělení jeho kořenovým činitelem vychází tedy beze zbytku a výsledkem dělení je polynom p_1. Jeho stupeň je tedy aspoň o jedničku menší než $\max(\mathrm{St}\,p,\mathrm{St}\,q_1)$ a je tedy menší než $\mathrm{St}\,q-1$.

Rozklad na parciální zlomky

je důsledek předchozí věty:

$$\frac{p(x)}{q(x)} = \frac{a_k}{(x-\alpha)^k}+\frac{a_{k-1}}{(x-\alpha)^{k-1}}+\cdots+\frac{a_1}{(x-\alpha)}+\frac{p_2(x)}{q_1(x)} = \\ = \sum_{i=1}^{k_1}\frac{a_{i,k_1}}{(x-\alpha_1)^i}+\sum_{i=1}^{k_2}\frac{a_{i,k_2}}{(x-\alpha_2)^i}+\cdots+\sum_{i=1}^{k_u}\frac{a_{i,k_u}}{(x-\alpha_r)^i}$$

Reálný rozklad na parciální zlomky:

$$\frac{p(x)}{q(x)} = \sum_{i=1}^{k_1}\frac{a_{i,k_1}}{(x-\alpha_1)^i}+\sum_{i=1}^{k_2}\frac{a_{i,k_2}}{(x-\alpha_2)^i}+\cdots+\sum_{i=1}^{k_u}\frac{a_{i,k_u}}{(x-\alpha_r)^i}+ \\ +\sum_{i=1}^{m_1}\frac{b_{i,m_1}x+c_{i,m_1}}{(x^2+\beta_1x+\gamma_1)^i}+\sum_{i=1}^{m_2}\frac{b_{i,m_2}x+c_{i,m_2}}{(x^2+\beta_2x+\gamma_2)^i}+\cdots+\sum_{i=1}^{m_v}\frac{b_{i,m_v}x+c_{i,m_v}}{(x^2+\beta_sx+\gamma_s)^i}$$

Polynom nad tělesem

Číselné obory $\mathbf{Q}$, $\mathbf{R}$ a $\mathbf{C}$ jsou příklady takzvaných *těles* (o tom promluvíme podrobněji později). Těleso zde značím písmenem T.

Pokud polynom má koeficienty jen z T a definiční obor je také z T (tj. za formální proměnnou x dosazujeme jen čísla z T), pak hovoříme o *polynomu nad tělesem* T.

Definice: Polynom p nad tělesem T je *ireducibilní v* T, pokud jej není možné rozložit na součin polynomů r, s nad T stupně aspoň prvního. Takže nemůže platit $p = r\cdot s$.

Pokud je možné polynom výše zmíněným způsobem rozložit, říkáme mu *reducibilní v* T.

Příklad: Polynom x^2+1 je ireducibilní v $\mathbf{R}$.

Příklad: Polynom x^2+1 je reducibilní v $\mathbf{C}$, protože

$$x^2+1 = (x+i)\cdot(x-i).$$

Příklad: V $\mathbf{C}$ jsou ireducibilní pouze polynomy stupně nejvýše prvního. To zaručuje základní věta algebry.

Příklad: Polynom x^2-2 je ireducibilní v $\mathbf{Q}$, ale je reducibilní v $\mathbf{R}$ i $\mathbf{C}$, protože $x^2-2 = (x-\sqrt{2})\cdot(x+\sqrt{2})$ a to jsou polynomy stupně aspoň prvního nad $\mathbf{R}$ i nad $\mathbf{C}$, ale ne nad $\mathbf{Q}$.

Příklad: Rozklad na kořenové činitele je rozklad na součin ireducibilních polynomů v $\mathbf{C}$.

Příklad: Reálný rozklad je rozklad na součin ireducibilních polynomů v $\mathbf{R}$.

Lineární prostor

- je množina L jakýchkoli objektů s operacemi + a ·
- objekty lze sčítat mezi sebou, součet je také objekt z množiny L
- objekt lze násobit konstantou, násobek je také objekt z L
- operace sčítání a násobení splňují tzv. axiomy linearity

a) algebra-all, 2, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) Viz p. d. 4/2010

Příklady

- Funkce
- Polynomy
- Uspořádané n-tice čísel
- Orientovné úsečky
- Nekonečné posloupnosti
- Reálná čísla samotná
- Komplexní čísla
- …

Definice lineárního prostoru

Lineárním prostorem nazýváme každou neprázdnou množinu L, na které je definováno sčítání $+ : L \times L \to L$ a násobení reálným číslem $\cdot : \mathbf{R} \times L \to L$ a tyto operace splňují pro každé $\vec{x} \in L, \vec{y} \in L, \vec{z} \in L, \alpha \in \mathbf{R}, \beta \in \mathbf{R}$ vlastnosti:

(1) $\vec{x} + \vec{y} = \vec{y} + \vec{x}$
(2) $(\vec{x} + \vec{y}) + \vec{z} = \vec{x} + (\vec{y} + \vec{z})$
(3) $\alpha \cdot (\beta \cdot \vec{x}) = (\alpha\beta) \cdot \vec{x}$
(4) $\alpha \cdot (\vec{x} + \vec{y}) = \alpha \cdot \vec{x} + \alpha \cdot \vec{y}$
(5) $(\alpha + \beta) \cdot \vec{x} = \alpha \cdot \vec{x} + \beta \cdot \vec{x}$
(6) $1 \cdot \vec{x} = \vec{x}$
(7) existuje $\vec{o} \in L$, že pro každé $\vec{x} \in L$ je $0 \cdot \vec{x} = \vec{o}$

Prvky lineárního prostoru nazýváme *vektory*. Reálnému číslu v kontextu násobení $\cdot : \mathbf{R} \times L \to L$ říkáme *skalár*. Prvku $\vec{o} \in L$ z vlastnosti (7) říkáme *nulový prvek* nebo *nulový vektor*.

Jednoduché vlastnosti

Pro nulový prvek $\vec{o}$ lineárního prostoru L platí vlastnosti:

(1) $\vec{x} + \vec{o} = \vec{x} \qquad \forall\, \vec{x} \in L,$
(2) $\alpha \cdot \vec{o} = \vec{o} \qquad \forall\, \alpha \in \mathbf{R},$
(3) Nechť $\vec{x} \in L$. Je-li $\alpha \cdot \vec{x} = \vec{o}$ a $\alpha \neq 0$, pak $\vec{x} = \vec{o}$.

Co není lineárním prostorem

- Kvůli operacím: $(a,b) + (c,d) = (a+d, c+b)$, ...
- Kvůli množině: množina nenulových funkcí, ...

Konečné lineární prostory (nad R)

Jednobodový prostor (tzv. *triviální*, obsahuje jen nulový vektor)

ALE: Neexistuje konečný lineární prostor s aspoň dvěma vektory.

Neobvyklý lineární prostor

- Množina: $\mathbf{R}^+$, operace: $\oplus : \mathbf{R}^+ \times \mathbf{R}^+ \to \mathbf{R}^+$, $\odot : \mathbf{R} \times \mathbf{R}^+ \to \mathbf{R}^+$

$$x \oplus y = x \cdot y, \quad \alpha \odot x = x^\alpha$$

Lineární podprostor

je podmnožina M lineárního prostoru L, která je sama se stejnými operacemi lineárním prostorem. Vlastnosti (1) až (7) jsou zaručeny, protože tytéž operace „pracují“ v L. Nemusí být ale splněna uzavřenost operací, tedy:

Definice: Nechť L je lineární prostor s operacemi „+“ a „$\cdot$“. Neprázdnou množinu $M \subseteq L$ nazýváme *lineárním podprostorem prostoru* L, pokud pro všechna $\vec{x} \in M, \vec{y} \in M$ a $\alpha \in \mathbf{R}$ platí:

(1) $\vec{x} + \vec{y} \in M,$
(2) $\alpha \cdot \vec{x} \in M.$

Příklady lineárních podprostorů

- Polynomy v lineárním prostoru funkcí
- Polynomy nejvýše druhého stupně v lineárním prostoru polynomů
- Podmnožiny z $\mathbf{R}^3$:

$M = \{(x,y,z);\ x + 2y = 0,\ z \text{ libovolné}\}$ ANO,
$N = \{(x,y,z);\ 2x + y - z = 0\}$ ANO,
$S = \{(x,y,z);\ 2x + y - z = 3\}$ NE.

- Orientované úsečky ve společné rovině procházející bodem O,
- Orientované úsečky ve společné přímce procházející bodem O.

Průnik a sjednocení podprostorů

- Průnik podprostorů stejného lin. prostoru je vždy podprostor,
- sjednocení podprostorů stejného lin. prostoru nemusí být podprostor.

Lineární (ne)závislost

Skupiny, resp. množiny, vektorů mohou být *lineárně závislé* nebo *lineárně nezávislé*...

a) algebra-all, 3, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) Viz p. d. 4/2010

Odečítání vektorů, asociativita

Místo, abychom psali zdlouhavě: $\overrightarrow{x} + (-1) \cdot \overrightarrow{y}$, píšeme stručněji $\overrightarrow{x} - \overrightarrow{y}$.

Vektoru $-\overrightarrow{y} = (-1) \cdot \overrightarrow{y}$ říkáme *opačný vektor k vektoru* $\overrightarrow{y}$.

Pozorování: $\overrightarrow{x} - \overrightarrow{x} = \overrightarrow{o}$, protože
$\overrightarrow{x} - \overrightarrow{x} = 1 \cdot \overrightarrow{x} + (-1)\overrightarrow{x} = (1 + (-1)) \cdot \overrightarrow{x} = 0 \cdot \overrightarrow{x} = \overrightarrow{o}$.

Další zkrácení zápisu: Protože $(\overrightarrow{x}+\overrightarrow{y})+\overrightarrow{z} = \overrightarrow{x}+(\overrightarrow{y}+\overrightarrow{z})$, tj. nezáleží na pořadí provádění operací, budeme nadále závorky vynechávat a psát jen $\overrightarrow{x} + \overrightarrow{y} + \overrightarrow{z}$.

Lineární kombinace

Vče, co s vektory můžeme dělat je:

- násobit je konstantou
- sčítat je mezi sebou, neboli:
- tvořit lineární kombinace.

Definice: *Linární kombinace* vektorů $\overrightarrow{x}_1, \overrightarrow{x}_2, \dots, \overrightarrow{x}_n$ je vektor:

$$\alpha_1 \cdot \overrightarrow{x}_1 + \alpha_2 \cdot \overrightarrow{x}_2 + \cdots + \alpha_n \cdot \overrightarrow{x}_n$$

Reálná čísla $\alpha_1, \alpha_2, \dots, \alpha_n$ se nazývají *koeficienty lineární kombinace*.

Triviální lineární kombinace

Definice: Má-li lineární kombinace všechny koeficienty nulové, říkáme ji *triviální*. Triviální lineární kombinace vypadá takto:

$$0\overrightarrow{x}_1 + 0\overrightarrow{x}_2 + \cdots + 0\overrightarrow{x}_n$$

Má-li lineární kombinace aspoň jeden koeficient nenulový, říkáme ji *netriviální*.

Pozorování: Triviální lineární kombinace je rovna nulovému vektoru.

Plyne to z axiomu (7) a z tvrzení, že $\overrightarrow{x} + \overrightarrow{o} = \overrightarrow{x}$.

Lineární závislost, lineární nezávislost

Definice: Skupina vektorů $\overrightarrow{x}_1, \overrightarrow{x}_2, \dots, \overrightarrow{x}_n$ je *lineárně závislá*, pokud existuje jejich netriviální lineární kombinace rovna nulovému vektoru.

Skupina vektorů $\overrightarrow{x}_1, \overrightarrow{x}_2, \dots, \overrightarrow{x}_n$ je *lineárně nezávislá*, pokud neexistuje jejich netriviální lineární kombinace rovna nulovému vektoru, tedy pokud jedině jejich triviální lineární kombinace je rovna nulovému vektoru, neboli pokud z rovnosti

$$\alpha_1 \cdot \overrightarrow{x}_1 + \alpha_2 \cdot \overrightarrow{x}_2 + \cdots + \alpha_n \cdot \overrightarrow{x}_n = \overrightarrow{o}$$

nutně plyne $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

Příklady

- v $\mathbf{R}^3$ jsou vektory $(1,2,3),(5,7,8),(3,3,2)$ lineárně závislé
- v $\mathbf{R}^3$ jsou vektory $(1,2,3),(4,7,8),(3,4,2)$ lineárně nezávislé.
- v prostoru reálných funkcí jsou vektory $\sin(x), \cos(x), e^x$ lineárně nezávislé.
- v prostoru reálných funkcí jsou vektory $\sin^2 x, \cos^2 x, 3$ lineárně závislé.
- v prostoru polynomů jsou vektory $x^2 + x + 1, x + 2, x^2 - 1$ lienárně závislé.

Všechny příklady si ověřte podle definice.

Jiný pohled na lineární závislost

Tvrzení: Vektory $\overrightarrow{x}_1, \overrightarrow{x}_2, \dots, \overrightarrow{x}_n$ jsou lineárně závislé právě když existuje aspoň jeden z nich, který je lineární kombinací ostatních.

Důkaz. 1. nechť jsou lin. závislé. Pak existuje jejich netriviální lin. kombinace rovna nulovému vektoru, tj. aspoň jeden koeficient je nenulový, vydělením tímto koeficientem a přenosem vektoru na druhou stranu rovnosti zjišťujeme, že vektor je lineární kombinací ostatních.

2. nechť existuje jeden vektor, který je lineární kombinací ostatních. Přeneseme jej na druhou stranu rovnosti (odečteme jej) a máme netriviální lineární kombinaci rovnou nulovému vektoru.

Procvičování pochopení definice

- Lineární (ne)závislost není podmíněna pořadím vektorů ve skupině.
- Skupina vektorů, v níž se některý vektor opakuje, je lineárně závislá.
- Skupina vektorů obsahující nulový vektor je lineárně závislá.
- Skupina dvou vektorů je lineárně závislá právě když jeden je násobkem druhého.
- Přidáním vektoru do lineárně závislé skupiny se její závislost nezmění.
- Odebráním vektoru z lineárně nezávislé skupiny se její nezávislost nezmění.

Závislost orientovaných úseček

- Dvě orientované úsečky jsou lineárně závislé právě když leží ve společné přímce.
- Tři orientované úsečky jsou lineárně závislé právě když leží ve společné rovině.
- Čtyři orientované úsečky jsou závislé vždy.

Závislost nekonečných množin vektorů

Pravidlo: V algebře pracujeme jen s konečnými lineárními kombinacemi, tj. sčítanců je vždy konečně mnoho.

- Nekonečná množina M vektorů je *lineárně závislá*, pokud existuje jejich konečná lineárně závislá podmnožina, tj. existují vektory $\overrightarrow{x}_1, \overrightarrow{x}_2, \ldots, \overrightarrow{x}_n$ z množiny M tak, že jsou lineárně závislé.
- Nekonečná množina M vektorů je *lineárně nezávislá*, pokud každá její konečná podmnožina je lineárně nezávislá, jinými slovy neexistuje lineárně závislá konečná podmnožina. Ještě jinak: neexistuje žádný vektor z M, který by se rovnal konečné lineární kombinaci ostatních vektorů.

Příklad nekonečné lin. nezávislé množiny

Množina polynomů $\{1, x, x^2, x^3, x^4, \ldots\}$ je lineárně nezávislá.

Lineární obal

Definice: Lineární obal vektorů $\overrightarrow{x}_1, \overrightarrow{x}_2, \ldots, \overrightarrow{x}_n$ je množina včech jejich lineárních kombinací, tedy

$$\{\alpha_1 \overrightarrow{x}_1 + \alpha_2 \overrightarrow{x}_2 + \cdots + \alpha_n \overrightarrow{x}_n;\ \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbf{R}\}$$

Lineární obal vektorů $\overrightarrow{x}_1, \overrightarrow{x}_2, \ldots, \overrightarrow{x}_n$ značíme $\langle \overrightarrow{x}_1, \overrightarrow{x}_2, \ldots, \overrightarrow{x}_n \rangle$.

Lineární obal (konečné nebo nekonečné) množiny vektorů M je množina všech konečných lineárních kombinací vektorů z množiny M. Lineární obal množiny M značíme $\langle M \rangle$.

Pozorování: $M \subseteq \langle M \rangle$.

Geometrická představa lineárního obalu

Předpokládejme vektory z množiny orientovaných úseček se společným počátkem O.

- Lineární obal jednoho nenulového vektoru je množina všech vektorů ležících ve společné přímce.
- Lineární obal dvou lineárně nezávislých vektorů je množina všech vektorů ležících ve společné rovině.
- Lineární obal tří lineárně nezávislých vektorů je množina všech orientovaných úseček.
- Lineární obal (libovolně mnoha) vektorů ležících ve společné rovině je množina všech vektorů ležících v této rovině.

Obal obalu

Věta: $\langle\langle M \rangle\rangle = \langle M \rangle$, neboli:
lineární obal lineárního obalu už není větší než původní lineární obal.

Důkaz: Lineární kombinace lineárních kombinací vektorů z M je po využití distributivního zákona rovna přímo lineární kombinaci vektorů z M (rozepište si to).

Obal je podprostor

(1) Je-li P lineárním obalem nějaké množiny M, je P lineární podprostor.

(2) P je lineární podprostor právě tehdy, když $\langle P \rangle = P$.

(3) Lineární obal množiny M je nejmenší lineární podprostor obsahující M.

Důkazy: (1) Součet prvků z obalu zůstává v obalu a α-násobek také. Protože lineární kombinace lin. kombinací je přímo lin. kombinace.

(2) Je-li P lineární podprostor, pak všechny lineární kombinace prvků z P zůstávají v P, takže $\langle P \rangle = P$. Obráceně: viz (1), stačí zvolit $M = P$.

(3) Nechť $P = \langle M \rangle$ a Q je podprostor obsahující M, tedy $M \subseteq Q$. Je $P = \langle M \rangle \subseteq \langle Q \rangle = Q$, takže je P nejmenší.

Rozšíření lineárně nezávislé množiny

Věta: Je-li N lineárně nezávislá množina vektorů a $z \notin \langle N \rangle$, pak $N \cup \{\overrightarrow{z}\}$ je lineárně nezávislá.

Důkaz: Sporem. Nechť $N \cup \{\overrightarrow{z}\}$ je lineárně závislá. Pak existuje konečně mnoho $\overrightarrow{x}_1, \overrightarrow{x}_2, \ldots, \overrightarrow{x}_n \in N$ tak, že

$$\alpha_1 \overrightarrow{x}_1 + \alpha_2 \overrightarrow{x}_2 + \cdots + \alpha_n \overrightarrow{x}_n + \alpha_{n+1} \overrightarrow{z} = \overrightarrow{o},$$

a přitom aspoň jedno α_i je nenulové. Kdyby byla $\alpha_{n+1} = 0$, máme netriviální lin. kombinaci vektorů nezávislé množiny N rovnu nulovému vektoru a to není možné. Takže musí $\alpha_{n+1} \neq 0$. Po vydělení α_{n+1} a převedení $\overrightarrow{z}$ na druhou stranu rovnosti je $\overrightarrow{z}$ lineární kombinací vektorů z N, což je ve sporu s tím, že $z \notin \langle N \rangle$.

Redukce lin. nezávislé množiny

Věta: Množina N je lineárně nezávislá právě tehdy, když každá její vlastní podmnožina má menší obal.

Důkaz: Nechť N je nezávislá. Nechť $N' \subset N$. Vektor $\overrightarrow{z} \in N \setminus N'$ není lin. kombinací prvků z N', protože jinak by N byla závislá. Nemůže tedy $\langle N\rangle = \langle N'\rangle$, protože v takovém případě je $\overrightarrow{z} \in \langle N'\rangle$.

Nechť N je závislá. Existuje jeden vektor $\overrightarrow{z}$, který je lin. kombinací ostatních. Jeho odebráním vzniká N', která má stejný lin. obal.

Báze

- Každý lineární (pod)prostor má svou bázi
- Vzhledem ke zvolené bázi určujeme souřadnice vektorů...

a) algebra-all, 4, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) Viz p. d. 4/2010

Definice báze

Definice: Množina vektorů B je *báze* lineárního prostoru L, pokud

(1) B je lineárně nezávislá,
(2) $\langle B\rangle = L$.

Podobně definujeme bázi lineárního podprostoru $P \subseteq L$.

Příklady bází

- $\{(1,2,3),\ (4,7,8),\ (3,4,2)\}$ je báze $\mathbf{R}^3$.
- $\{(1,0,0),\ (0,1,0),\ (0,0,1)\}$ je také báze $\mathbf{R}^3$.
- $\{(1,0,0,\ldots,0),\ (0,1,0,\ldots,0),\ \ldots,\ (0,0,0,\ldots,1)\}$ je báze $\mathbf{R}^n$.
- libovolné tři lineárně nezávislé orientované úsečky tvoří bázi lineárního prostoru všech orientovaných úseček.
- libovolné dvě lineárně nezávislé orientované úsečky v rovině tvoří bázi lineárního podprostoru orientovaných úseček ležících v této rovině.
- Množina $\{1, x, x^2, x^3, \ldots\}$ tvoří bázi lin. prostoru všech polynomů.

Pozorování: Jeden lineární (pod)prostor má více bází, všechny mají společnou vlastnost: mají stejný počet prvků. (To dokážeme za chvíli.)

Existence báze

Věta:

- Každý netriviální lineární prostor má bázi.
- Každá lineárně nezávislá množina se dá doplnit na bázi.
- V každé množině, pro kterou $\langle M\rangle = L$, se dá najít podmnožina, která tvoří bázi L.

Důkaz: opírá se o axiom výběru. Důkaz najdete ve druhém vydání linal2.pdf, ale nebudu jej požadovat ke zkoušce.

Pozorování: Je-li báze konečná, pak se dá lin. nezávislá množina doplnit na bázi postupným přidáváním vektorů z vnějšku lineárního obalu (použije se věta ze slídu [16]).

Stejný počet prvků v bázi

Věta 1: Dvě báze stejného lineárního prostoru mají stejný počet prvků.

Důkaz: pomocí tzv. Steinitzovy věty o výměně:

Věta (Steintz): Nechť M je libovolná množina, N je konečná lineárně nezávislá množina vektorů tak, že $N \subseteq \langle M\rangle$. Pak lze z množiny M odebrat tolik vektorů, kolik jich je v N, a přidat tam všechny vektory z N. Nově vzniklá množina má stejný lineární obal jako $\langle M\rangle$. (Důkaz Steintzovy věty: viz linal.pdf.)

Důkaz věty 1: Nechť B_1 a B_2 jsou dvě báze. Protože B_1 je lin. nezávislá a $B_1 \subseteq \langle B_2\rangle$, má podle Steinitzovy věty B_1 nejvýše tolik vektorů jako B_2. Je také B_2 lin. nezávislá a $B_2 \subseteq \langle B_1\rangle$, takže počet vektorů je stejný.

Dimenze

Definice: Počet prvků báze lineárního prostoru L je *dimenze* L, značíme $\dim L$.

Pozorování: Předchozí věta nám zaručuje, že definice má smysl.

Příklady:

- $\dim \mathbf{R}^n = n$,
- dimenze prostoru polynomů je ∞,
- dimenze prostoru orientovaných úseček je 3,
- dim. podprostoru orientovaných úseček ve společné rovině je 2,
- dim. podprostoru orientovaných úseček ve společné přímce je 1,

Dimenze podprostoru

Dimenze podprostoru je menší nebo rovna dimenzi prostoru.

(Důkaz: Bázi podprostoru lze doplnit na bázi prostoru.)

V případě konečné dimenze a vlastního podporostoru je dimenze podprostoru menší.

(Důkaz: K bázi podprostoru přidáme vektor z vnějšku podprostoru. Tím zůstane množina lin. nezávislá. Případně ji doplníme na bázi prostoru.)

Podmínka konečnosti dimenze je nutná: Například prostor polynomů, i podprostor $\langle 1, x^2, x^4, \ldots\rangle$ mají stejnou dimenzi ∞.

Rovnost obalů

Dva obaly $\langle U\rangle = \langle \vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n\rangle$ a $\langle V\rangle = \langle \vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\rangle$ se rovnají, právě když

$$\dim\langle \vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n, \vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\rangle = \dim\langle U\rangle = \dim\langle V\rangle.$$

Důkaz*: Nechť $\langle U\rangle = \langle V\rangle$, Pak $U \subseteq \langle U\rangle$, $V \subseteq \langle V\rangle = \langle U\rangle$, takže $U \cup V \subseteq \langle U \cup V\rangle = \langle V\rangle = \langle U\rangle$, tj. $\dim\langle U \cup V\rangle = \dim\langle V\rangle = \dim\langle U\rangle$.

Nechť nyní $\dim\langle U \cup V\rangle = \dim\langle V\rangle = \dim\langle U\rangle$. Protože $\langle U\rangle \subseteq \langle U \cup V\rangle$, ale mají stejné dimenze, musí se podprostor $\langle U\rangle$ rovnat lineárnímu prostoru $\langle U \cup V\rangle$.

Počet prvků lineárně nezávislé množiny

Nechť $\dim L = n$, $M \subseteq L$, počet prvků M je m. Potom:

- Je-li M lin. nezávislá, pak $m \le n$.
- Je-li $m > n$, pak je M lineárně závislá.
- Je-li $m = n$ a M je nezávislá, pak $\langle M\rangle = L$.
- Je-li $m = n$ a $\langle M\rangle = L$, pak M je nezávislá.
- Je-li M je nezávislá a $\langle M\rangle = L$, pak $m = n$.

Souřadnice vektoru vzhledem k bázi

Na co máme bázi? Abychom vzhledem k ní mohli přidělit každému vektoru uspořádanou n-tici čísel, tzv. *souřadnice vektoru*.

Definice: Souřadnice vektoru $\vec{x}$ vzhledem k uspořádané bázi $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n$ jsou uspořádaná n-tice reálných čísel $\alpha_1, \alpha_2, \ldots, \alpha_n$ taková, že

$$\vec{x} = \alpha_1 \vec{b}_1 + \alpha_2 \vec{b}_2 + \cdots + \alpha_n \vec{b}_n.$$

Existence souřadnic pro každý $\vec{x} \in L$? Protože $\langle B\rangle = L$.

Jednoznačnost souřadnic? Protože B je lineárně nezávislá.

Příklady

Vzhledem k bázi $((1,0,0),(0,1,0),(0,0,1))$ má vektor $\vec{x} = (a,b,c)$ souřadnice (a,b,c).

Vzhledem k bázi $(1,x,x^2)$ má vektor ax^2+bx+c souřadnice (c,b,a).

Vzhledem k bázi $x^2+2, 2x, x-1$ má vektor ax^2+bx+c souřadnice:

$$\left(a,\ \frac{-2a+b+c}{2},\ 2a-c\right).$$

Souřadnice vektorů vzhledem k bázi v prostoru orientovaných úseček zjistíme geometricky.

Standardní báze v $\mathbf{R}^n$

je báze $((1,0,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,0,0,\ldots,1))$.

Má zajímavou vlastnost: vzhledem k ní má vektor $\vec{x} = (x_1,x_2,\ldots,x_n)$ souřadnice $(x_1,x_2,\ldots,x_n)$. Protože

$$(x_1,x_2,\ldots,x_n) = x_1(1,0,\ldots,0) + x_2(0,1,\ldots,0) + \cdots + x_n(0,0,\ldots,1).$$

Lineární zobrazení

- Zachovává operace + a · lineárního postoru.
- Přenáší vztahy mezi vektory jednoho prostoru do druhého.

a) algebra-all, 5, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) Viz p. d. 4/2010

Zobrazení (zatím ne nutně lineární)

- přiřazuje každému prvku x jedné množiny (L_1) jednoznačně prvek y množiny druhé (L_2). Značíme $a : L_1 \to L_2$.
- prvku x zobrazení A přiřadí prvek y, který nazýváme *hodnota zobrazení v bodě x* nebo *obraz prvku x* a značíme jej $A(x)$. Mluvíme-li o obrazu prvku x, pak prvek x nazýváme *vzor*.
- množině $M \subseteq L_1$ zobrazení A přiřadí množinu hodnot $A(M)$.
- zobrazení je *prosté* (injektivní), pokud každým dvěma různým vzorům přiřadí různé obrazy.
- zobrazení je *na L_2* (surjektivní), pokud každý prvek v L_2 má svůj vzor.
- zobrazení je *bijektivní*, je-li prosté a na.

Definice lineárního zobrazení

Zobrazení $A : L_1 \to L_2$ *je lineární* (homomorfismus), pokud jsou L_1 a L_2 lineární prostory a pokud zobrazení „zachovává operace“, tj. $\forall \vec{x}, \vec{y} \in L_1$, $\forall \alpha \in \mathbf{R}$ je:

$$A(\vec{x} + \vec{y}) = A(\vec{x}) + A(\vec{y}), \qquad A(\alpha \cdot \vec{x}) = \alpha \cdot A(\vec{x}).$$

Operace $+, \cdot$ vlevo obou rovností jsou operacemi v L_1 a operace $+, \cdot$ vpravo jsou operacemi v L_2.

Příklady: Funkce $f : \mathbf{R} \to \mathbf{R}$, $f(x) = ax$, dále zobrazení, které přiřadí diferencovatelné funkci derivaci, integrovatelné funkci určitý integrál, funkci posloupnost $f(1), f(2), \ldots$, posloupnosti po částech konstantní funkci, orientované úsečce její průmět do roviny, vektoru souřadnice, …

Zajímavý příklad: $f : \mathbf{R}^+ \to \mathbf{R}$ (operace na $\mathbf{R}^+$ jsou $x \oplus y = xy$, $\alpha \odot x = x^\alpha$, operace na $\mathbf{R}$ jsou „obvyklé“), $f(x) = \ln(x)$.

Princip superpozice

Lineární zobrazení $A : L_1 \to L_2$ převádí lineární kombinace vzorů v L_1 na lineární kombinace obrazů v L_2 se stejnými koeficienty, tedy:

$$A(\alpha_1 \vec{x}_1 + \alpha_2 \vec{x}_2 + \cdots + \alpha_n \vec{x}_n) = \alpha_1 A(\vec{x}_1) + \alpha_2 A(\vec{x}_2) + \cdots + \alpha_n A(\vec{x}_n)$$

Zachování obalů

Důsledek principu superpozice je: $A(\langle M \rangle) = \langle A(M) \rangle$, neboli:

- Je-li P lineární podprostor v L_1, je $A(P)$ lineární podprostor v L_2.
- $A(L_1)$ je lineární podprostor v L_2.

Jádro lineárního zobrazení

Definice: *Jádro* lineárního zobrazení $A : L_1 \to L_2$ je podmnožina $\mathrm{Ker}\, A \subseteq L_1$ definovaná vztahem

$$\mathrm{Ker}\, A = \{\vec{x} \in L_1,\ A(\vec{x}) = \vec{o}\},$$

tj. je to množina vzorů, které mají nulový obraz.

Věta: Jádro lineárního zobrazení $A : L_1 \to L_2$ je lineární podprostor v L_1.

Důkaz: nechť $A(\vec{x}) = \vec{o}, A(\vec{y}) = \vec{o}$. Pak $A(\vec{x} + \vec{y}) = A(\vec{x}) + A(\vec{y}) = \vec{o} + \vec{o} = \vec{o}$. Dále $A(\alpha \vec{x}) = \alpha A(\vec{x}) = \alpha \vec{o} = \vec{o}$.

Cvičení: Najděte jádra dříve zmíněných příkladů lin. zobrazení.

Defekt a hodnost lineárního zobrazení

Definice: *Defekt* lineárního zobrazení $a : L_1 \to L_2$ je $\dim \mathrm{Ker}\, A$. *Hodnost* lineárního zobrazení $a : L_1 \to L_2$ je $\dim A(L_1)$.

Lapidárně: Defekt určuje, kolik dimenzí se „ztratí“ při přechodu od vzorů k obrazům. Hodnost je dimenze podprostoru všech obrazů.

Cvičení: Najděte defekty a hodnosti dříve zmíněných příkladů lin. zobrazení.

Příklad $A : \mathbf{R}^4 \to \mathbf{R}^3$

Zobrazení A je v bodě $(x_1, x_2, x_3, x_4) \in \mathbf{R}^4$ definováno hodnotou:

$$A(x_1, x_2, x_3, x_4) =$$
$$= (x_1 + 2x_2 + 2x_3 + 4x_4,\ 2x_1 + x_2 + 3x_3 + x_4,\ 3x_1 + 3x_2 + 5x_3 + 5x_4)$$

Toto zobrazení je zjevně lineární. Najdeme jeho jádro, defekt a hodnost.

Defekt plus hodnost

Věta: Defekt plus hodnost lineárního zobrazení $A : L_1 \to L_2$ je rovno dimezni L_1.

Důkaz (jen náčtr, podrobně viz linal2.pdf)

Prosté lineární zobrazení

Věta: Lineární zobrazení je prosté právě když má nulový defekt.

Důkaz: Nemá-li nulový defek, zjevně není prosté. Má-li nulový defekt a není prosté, odvodíme spor. $A(\vec{x}) = A(\vec{y})$, tj. $A(\vec{x}) - A(\vec{y}) = A(\vec{x} - \vec{y}) = \vec{o}$, takže v jádru leží $\vec{x} - \vec{y} \neq \vec{o}$, takže A nemá nulový defekt.

Věta: Lineární zobrazení je prosté právě když lineárně nezávislé vzory převede na lineárně nezávislé obrazy.

Důkaz: Není-li prosté, pak má nenulový defekt a netriviální jádro. Existuje tedy nenulový vektor (lin. nezávislý), který se zobrazí na nulový vektor (lin závislý).

Je-li prosté a obrazy nezávislých vzorů jsou lin. závislé, pak dostaneme spor s principem superpozice (ukázat podrobněji...).

Zobrazení lineárně závislých vzorů

vytvoří vždy lin. závislý obraz. Stačí použít princip superpozice.

Izomorfismus

Zobrazení $A : L_1 \to L_2$, které je lineární, prosté a na L_2 se nazývá *izomorfismus*.

Pozorování: Izomorfismus převádí:

- LN množiny na LN množiny (protože je prostý a lineární),
- lin. kombinace na lin. kombinace obrazů (protože je lineární),
- LZ množiny na LZ (protože je lineární),
- podprostory na podprostory (protože je lineární),
- lineární obaly na lineární obaly (protože je lineární),
- báze na báze (protože převádí LN množiny na LN množiny),

Izomorfismus zachovává dimenze převedených podprostorů a zaručí, že $\dim L_1 = \dim L_2$ (protože je lineární prostý a na).

Vlastnosti izomorfismů

- Složení izomorfisu je izomorfismus
- Inverze k izomorfismu existuje a je to izomorfismus

Zobrazení souřadnic je izomorfismus

Je třeba ověřit

- linearitu,
- zda je toto zobrazení prosté
- zda je „na“ $\mathbf{R}^n$.

Izomorfní lin. prostory konečné dimenze

Definice: Dva lineární prostory L_1 a L_2 jsou *izomorfní*, existuje-li izomorfismus $A : L_1 \to L_2$.

Pozorování: Každý lineární prostor L konečné dimenze n je izomorfní s $\mathbf{R}^n$. Tím izomorfismem jsou souřadnice vzhledem k bázi.

Věta: Každé dva lineární prostory stejné konečné dimenze jsou vzájemně izomorfní. (Důkaz plyne z vlastností izomorfismu.)

Důležité: Z pohledu lineární algebry (vlastností vzešlých z axiomů linearity) není mezi dvěma izomorfními lineárními prostory žádný rozdíl. Můžeme si vybrat, ve kterém z těchto dvou lineárních prostorů budeme algebraický problém řešit. Obvykle se problém řeší v $\mathbf{R}^n$, kde můžeme využít algoritmy související s maticemi.

Matice

- mezi sebou sčítáme a násobíme konstantou (lineární prostor)
- měníme je na jiné matice eliminační metodou
- násobíme je mezi sebou
- ...

a) algebra-all, 6, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) Viz p. d. 4/2010

Základní pojmy

Matice je tabulka čísel s konečným počtem řádků a sloupců.

Množina $\mathbf{R}^{m,n}$ je množina matic s reálnými čísly s m řádky a n sloupci. Takovým maticím též říkáme *matice typu* (m,n).

Na jednotlivé řádky v matici typu (m,n) můžeme pohlížet jako na vektory z $\mathbf{R}^n$ a na jednotlivé sloupce můžeme pohlížet jako na vektory z $\mathbf{R}^m$.

Číslo na i-tém řádku a j-tém sloupci matice se nazývá (i,j)-tý prvek matice a používají se pro něj indexy: $a_{i,j}$ (v tomto pořadí).

Matice budeme značit velkým tučným písmenem ($\mathbf{A}$, $\mathbf{B}$, atd.).

Nulová matice obsahuje samé nuly.

Čtvercová matice je matice typu (n,n).

Sčítání matic, násobení matic konstantou

Mezi sebou sčítáme jen matice stejného typu. Součet má stejný typ. Násobek kontantou α má také stejný typ jako původní matice.

$$\mathbf{A}+\mathbf{B} = \begin{pmatrix} a_{1,1}+b_{1,1}, & a_{1,2}+b_{1,2}, & \dots, & a_{1,n}+b_{1,n} \\ a_{2,1}+b_{2,1}, & a_{2,2}+b_{2,2}, & \dots, & a_{2,n}+b_{2,n} \\ & & \vdots & \\ a_{m,1}+b_{m,1}, & a_{m,2}+b_{m,2}, & \dots, & a_{m,n}+b_{m,n} \end{pmatrix},$$

$$\alpha\cdot\mathbf{A} = \begin{pmatrix} \alpha a_{1,1}, & \alpha a_{1,2}, & \dots, & \alpha a_{1,n} \\ \alpha a_{2,1}, & \alpha a_{2,2}, & \dots, & \alpha a_{2,n} \\ & & \vdots & \\ \alpha a_{m,1}, & \alpha a_{m,2}, & \dots, & \alpha a_{m,n} \end{pmatrix}.$$

Množina matic $\mathbf{R}^{m,n}$ s tímto + a $\cdot$ tvoří lineární prostor.

Cvičení: Najděte bázi a dimenzi lineárního prostoru matic $\mathbf{R}^{3,2}$.

Modifikace matic eliminační metodou

Vznikne-li matice $\mathbf{B}$ z matice $\mathbf{A}$ konečným počtem řádkových úprav eliminační metody, píšeme $\mathbf{A} \sim \mathbf{B}$. Jsou to (obecně) *různé* matice.

Pozorování: Je-li $\mathbf{A} \sim \mathbf{B}$ pak také $\mathbf{B} \sim \mathbf{A}$. Jinými slovy: každá změna eliminační metodou je vratná.

Stačí si uvědomit, jak pracují tři základní operace v GEM: prohození řídků, pronásobení řádku nenulovou konstantou a přičtení násobku řádku k jinému.

Eliminace zachovává obal řádků

Věta: Gaussova eliminační emtoca zachovává lineární obal řádků matice.

Jinými slovy: je-li $\mathbf{A} \sim \mathbf{B}$, pak lineární obal řádků matice $\mathbf{A}$ je roven lineárnímu obalu řádků matice $\mathbf{B}$.

Důkaz: Přehození řádků: lin. obal se nezmění, to je zřejmé. Další dva typy opearci v GEM přidávají k řádkům lineární kombinaci (tím nezmění lineární obal) a odeberou jeden vektor (lin. obal se může zmenšit). On se ale nezmenší, protože eliminace je vratná.

Hodnost matice

Definice: *Hodnost matice* $\mathbf{A}$ je dimenze lineárního obalu řádků matice $\mathbf{A}$. Značíme $\hod \mathbf{A}$, anglicky „rank of matrix $\mathbf{A}$“.

Pozorování: Gaussova eliminační metoda nemění hodnost matice, tedy je-li $\mathbf{A} \sim \mathbf{B}$, pak $\hod \mathbf{A} = \hod \mathbf{B}$.

Metoda počítání hodnosti: Máme-li spočítat $\hod \mathbf{A}$, eliminujeme $\mathbf{A}$ na matici $\mathbf{B}$ schodového tvaru. Počet nenulových řádků této matice je $\hod \mathbf{B}$ a tedy i $\hod \mathbf{A}$.

Proč? Neulové řádky v matici $\mathbf{B}$ tvoří bázi svého lineárního obalu. Jsou totiž lineárně nezávislé.

Poznámky k hodnosti

- Souvislost mezi hodností matice a hodnosti lineárního zobrazení ukážeme později.
- Metoda počítání hodnosti je metodou počítání dimenze lineárního obalu.
- **Pozor:** Hodnost nelze definovat pomocí uvedené metody protože eliminační metoda není jednoznačný proces, tj. nemáme záruku stejného počtu nenulových řádků po provedení eliminace.
- Pozor na alternativní definici: hodnost jako maximální počet lineárně nezávislých řádků. Je třeba si uvědomit, co to znamená.
- Hodnost je přirozené číslo, které nemusí být jednoznačně stanoveno pro „nepřesné matice“ a „nepřesné výpočty“ (tzv. numericky nestabilní matice).

GEM zachovává lineární nezávislost řádků

Věta: Je-li $\mathbf{A} \sim \mathbf{B}$ pak $\mathbf{A}$ obsahuje lineárně nezávislé řádky právě tehdy když $\mathbf{B}$ obsahuje lin. nezávislé řádky.

Důkaz: Má-li $\mathbf{A}$ lin. nezávislé řádky, pak tvoří bázi svého lin. obalu, takže $\hod \mathbf{A}$ je rovna počtu řádků matice $\mathbf{A}$. Je také rovna hodnosti matice $\mathbf{B}$ (která má stejný počet řádků jako matice $\mathbf{A}$), takže $\mathbf{B}$ musí mít lin. nezávislé řádky.

Metoda ověření závislosti: Zapíšeme zkoumané vektory do řádků matice $\mathbf{A}$ a převedeme na schodovitý tvar $\mathbf{B}$. Zkoumané vektory jsou lin. závislé právě tehdy když $\mathbf{B}$ obsahuje nulový řádek.

Metody týkající se lineárních obalů

- $\overrightarrow{v} \in \langle \overrightarrow{u}_1, \overrightarrow{u}_2, \dots, \overrightarrow{u}_n \rangle$ právě když

$$\dim\langle \overrightarrow{u}_1, \overrightarrow{u}_2, \dots, \overrightarrow{u}_n \rangle = \dim\langle \overrightarrow{u}_1, \overrightarrow{u}_2, \dots, \overrightarrow{u}_n, \overrightarrow{v} \rangle.$$

Metoda: Vektor $\overrightarrow{v}$ leží v lineárním obalu vektorů $\overrightarrow{u}_1, \overrightarrow{u}_2, \dots, \overrightarrow{u}_n$, když hodnost matice obsahující v řádcích vektory $\overrightarrow{u}_1, \overrightarrow{u}_2, \dots, \overrightarrow{u}_n$ je stejná jako hodnost matice, ve které je navíc přidán řádek $\overrightarrow{v}$.

- $\langle \overrightarrow{u}_1, \overrightarrow{u}_2, \dots, \overrightarrow{u}_n \rangle = \langle \overrightarrow{v}_1, \overrightarrow{v}_2, \dots, \overrightarrow{v}_n \rangle$ právě když

$$\dim\langle \overrightarrow{u}_1, \overrightarrow{u}_2, \dots, \overrightarrow{u}_n \rangle = \dim\langle \overrightarrow{v}_1, \overrightarrow{v}_2, \dots, \overrightarrow{v}_n \rangle = \\ = \dim\langle \overrightarrow{u}_1, \overrightarrow{u}_2, \dots, \overrightarrow{u}_n, \overrightarrow{v}_1, \overrightarrow{v}_2, \dots, \overrightarrow{v}_n \rangle$$

Metoda: Ověříme rovnost hodností příslušných matic.

Hodnost transponované matice

Definice: *Transponovaná matice* k matici $\mathbf{A}$ (značíme $\mathbf{A}^T$) je matice, ve které jsou řádky původní matice $\mathbf{A}$ zapsány do sloupců.

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

Věta: $\hod \mathbf{A} = \hod \mathbf{A}^T$, jinými slovy: dimenze lineárního obalu řádků matice je rovna dimenzi lineárního obalu sloupců matice.

Důkaz: Je-li $\hod \mathbf{A} = k$, pak $\mathbf{A}$ má k lineárně nezávislých řádků. Jejich nezávislost lze ověřit z definice nezávislosti, což vede na soustavu s maticí $\mathbf{A}^T$ (až na vynechání některých sloupců). Aby soustava měla jen nulové řešení, musí mít lineárně nezávislé rovnice. Takže (po doplnění vynechaných sloupců) musí $\mathbf{A}^T$ mít aspoň k lineárně nezávislých řádků, tedy $\hod \mathbf{A} \le \hod \mathbf{A}^T$. Rovnost pak plyne z výše uvedeného pozorování.

Násobení matic

- je asociativní, není komutativní
- k regulárním maticím existují inverzní matice

Maticové násobení

Definice: Pro matice $\mathbf{A} \in \mathbf{R}^{m,n}$ a $\mathbf{B} \in \mathbf{R}^{n,p}$ existuje maticový součin $\mathbf{A} \cdot \mathbf{B} = \mathbf{C} \in \mathbf{R}^{m,p}$ (v tomto pořadí). Jednotlivé prvky součinu $c_{i,k}$ jsou dány vzorcem:

$$c_{i,k} = a_{i,1}b_{1,k} + a_{i,2}b_{2,k} + \cdots + a_{i,n}b_{n,k} = \sum_{j=1}^{n} a_{i,j}b_{j,k}.$$

Příklad: Je-li $\mathbf{A} \in \mathbf{R}^{3,4}$ a $\mathbf{B} \in \mathbf{R}^{4,5}$, pak $\mathbf{A} \cdot \mathbf{B}$ je definováno, ale $\mathbf{B} \cdot \mathbf{A}$ není definováno.

Pozorování: Aby bylo definováno $\mathbf{A} \cdot \mathbf{B}$, musí mít $\mathbf{A}$ stejný počet sloupců jako má $\mathbf{B}$ řádků. Výsledná matice má tolik řádků, jako má řádků matice $\mathbf{A}$ a tolik sloupců, jako má sloupců matice $\mathbf{B}$.

Příklady násobení

$$\begin{pmatrix}1&2&3\end{pmatrix}\cdot\begin{pmatrix}4\\5\\6\end{pmatrix}=\begin{pmatrix}1\cdot4+2\cdot5+3\cdot6\end{pmatrix}$$

$$\begin{pmatrix}4\\5\\6\end{pmatrix}\cdot\begin{pmatrix}1&2&3\end{pmatrix}=\begin{pmatrix}4&8&12\\5&10&15\\6&12&18\end{pmatrix}$$

$$\begin{pmatrix}1&1\\-1&-1\end{pmatrix}\cdot\begin{pmatrix}1&1\\1&1\end{pmatrix}=\begin{pmatrix}2&2\\-2&-2\end{pmatrix}$$

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

Poznatky z předchozích příkladů:

- Maticové násobení není komutativní ani pro čtvercové matice
- Neplatí pravidlo: součin nenulových matic musí být nenulová matice
- Co tedy platí? ...

Vlastnosti maticového násobení:

- $(\mathbf{A}\cdot\mathbf{B})\cdot\mathbf{C}=\mathbf{A}\cdot(\mathbf{B}\cdot\mathbf{C})$ ... asociativní zákon
- $(\mathbf{A}+\mathbf{B})\cdot\mathbf{C}=\mathbf{A}\cdot\mathbf{C}+\mathbf{B}\cdot\mathbf{C}$ ... distributivní zákon
- $\mathbf{C}\cdot(\mathbf{A}+\mathbf{B})=\mathbf{C}\cdot\mathbf{A}+\mathbf{C}\cdot\mathbf{B}$ ... distributivní zákon
- $\alpha(\mathbf{A}\cdot\mathbf{B})=(\alpha\mathbf{A})\cdot\mathbf{B}=\mathbf{A}\cdot(\alpha\mathbf{B})$ ... konstanta
- $(\mathbf{A}\cdot\mathbf{B})^T=\mathbf{B}^T\cdot\mathbf{A}^T$ ... transponovaná matice

Příklad: soustavy lin. rovnic

Nechť $\mathbf{A}\in\mathbf{R}^{m,n}$.

$$\mathbf{A}\cdot\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}=\begin{pmatrix}b_1\\b_2\\\vdots\\b_m\end{pmatrix}$$

Toto je soustava lineárních rovnic s m rovnicemi a n neznámými.

Stručně zapisujeme: $\mathbf{A}\cdot\mathbf{x}=\mathbf{b}$. Matice $\mathbf{A}$ se nazývá *matice soustavy*, jednosloupcová matice $\mathbf{b}$ je *vektor pravých stran*. Úkolem je nalézt všechny jednosloupcové matice $\mathbf{x}$, které vyhovují maticové rovnici.

Blokové násobení

Nechť $\mathbf{A}$ a $\mathbf{B}$ jsou matice sestavené po blocích takto:

$$\mathbf{A}=\begin{pmatrix}\mathbf{A}_{1,1}&\mathbf{A}_{1,2}\\\mathbf{A}_{2,1}&\mathbf{A}_{2,2}\end{pmatrix},\quad\mathbf{B}=\begin{pmatrix}\mathbf{B}_{1,1}&\mathbf{B}_{1,2}\\\mathbf{B}_{2,1}&\mathbf{B}_{2,2}\end{pmatrix}$$

Nechť uvedené bloky jsou matice takového typu, že násobení matic $\mathbf{A}_{i,j}\cdot\mathbf{B}_{j,k}$ je definováno pro všechny případy, které se vyskytují v následujícím vzorci. Pak

$$\mathbf{A}\cdot\mathbf{B}=\begin{pmatrix}\mathbf{A}_{1,1}\cdot\mathbf{B}_{1,1}+\mathbf{A}_{1,2}\cdot\mathbf{B}_{2,1}&\mathbf{A}_{1,1}\cdot\mathbf{B}_{1,2}+\mathbf{A}_{1,2}\cdot\mathbf{B}_{2,2}\\\mathbf{A}_{2,1}\cdot\mathbf{B}_{1,1}+\mathbf{A}_{2,2}\cdot\mathbf{B}_{2,1}&\mathbf{A}_{2,1}\cdot\mathbf{B}_{1,2}+\mathbf{A}_{2,2}\cdot\mathbf{B}_{2,2}\end{pmatrix}$$

... analogicky pro jinak vytvořené bloky. Například:

$$\mathbf{A}\cdot\begin{pmatrix}\mathbf{B}_1&\mathbf{B}_2&\dots&\mathbf{B}_p\end{pmatrix}=\begin{pmatrix}\mathbf{A}\cdot\mathbf{B}_1&\mathbf{A}\cdot\mathbf{B}_2&\dots&\mathbf{A}\cdot\mathbf{B}_p\end{pmatrix}$$

Výpočetní složitost maticového násobení

Předpokládejme dvě matice $\mathbf{A},\mathbf{B}\in\mathbf{R}^{n,n}$. K výpočtu $\mathbf{A}\cdot\mathbf{B}$ (podle definice) potřebujeme n^3 operací (násobení dvou čísel). Nedalo by se ušetřit?

- **Rekurzivní algoritmus násobení matic:** vychází z blokového násobení. Potřebuje $F(n)$ operací:

$$\begin{aligned}F(n)&=8F(n/2)=8(8F(n/4))=8(8(8F(n/2^3)))=\\&=\dots=8^mF(n/2^m)=8^mF(1)=\\&=8^m=(2^3)^m=2^{3m}=(2^m)^3=n^3.\end{aligned}$$

- **Rekurzivní Strassenův algoritmus:** vychází z blokového násobení, ale vystačí si se sedmi součiny. Potřebuje $F(n)$ operací:

$$\begin{aligned}F(n)&=7F(n/2)=7(7F(n/4))=7(7(7F(n/2^3)))=\\&=\dots=7^mF(n/2^m)=7^mF(1)=\\&=7^m=(2^{\log_2 7})^{\log_2 n}=2^{\log_2 7\cdot\log_2 n}=n^{\log_2 7}\doteq n^{2{,}807}.\end{aligned}$$

Strassenův algoritmus

$$\begin{aligned}\mathbf{X}_1&=(\mathbf{A}_1+\mathbf{A}_4)\cdot(\mathbf{B}_1+\mathbf{B}_4),\\\mathbf{X}_2&=(\mathbf{A}_3+\mathbf{A}_4)\cdot\mathbf{B}_1,\\\mathbf{X}_3&=\mathbf{A}_1\cdot(\mathbf{B}_2-\mathbf{B}_4),\\\mathbf{X}_4&=\mathbf{A}_4\cdot(\mathbf{B}_3-\mathbf{B}_1),\\\mathbf{X}_5&=(\mathbf{A}_1+\mathbf{A}_2)\cdot\mathbf{B}_4,\\\mathbf{X}_6&=(\mathbf{A}_3-\mathbf{A}_1)\cdot(\mathbf{B}_1+\mathbf{B}_2),\\\mathbf{X}_7&=(\mathbf{A}_2-\mathbf{A}_4)\cdot(\mathbf{B}_3+\mathbf{B}_4)\end{aligned}$$

Dá se ověřit, že platí:

$$\begin{pmatrix}\mathbf{A}_1&\mathbf{A}_2\\\mathbf{A}_3&\mathbf{A}_4\end{pmatrix}\cdot\begin{pmatrix}\mathbf{B}_1&\mathbf{B}_2\\\mathbf{B}_3&\mathbf{B}_4\end{pmatrix}=\begin{pmatrix}\mathbf{X}_1+\mathbf{X}_4-\mathbf{X}_5+\mathbf{X}_7&\mathbf{X}_3+\mathbf{X}_5\\\mathbf{X}_2+\mathbf{X}_4&\mathbf{X}_1-\mathbf{X}_2+\mathbf{X}_3+\mathbf{X}_6\end{pmatrix}$$

Komutující matice

Když platí: $\mathbf{A}\cdot\mathbf{B}=\mathbf{B}\cdot\mathbf{A}$, říkáme, že matice $\mathbf{B}$ komutuje s maticí $\mathbf{A}$.

Pozorování: Komutovat mohou pouze čtvercové matice stejného typu.

Úloha: Je pevně dána čtvercová matice $\mathbf{A}$, je třeba najít k ní množinu všech matic $\mathbf{B}$, které komutují s $\mathbf{A}$.

Pozorovaní: Uvedená množina matic $\mathbf{B}$, které komutují s danou maticí $\mathbf{A}$, tvoří lineární podprostor lineárního prostoru matic $\mathbf{R}^{n,n}$.

Inverzní matice

Čtvercovou matici s jedničkami na diagonále a nulami jinde značíme $\mathbf{E}$ a říkáme ji *jednotková matice*.

Pozorování: $\mathbf{A}\cdot\mathbf{E}=\mathbf{E}\cdot\mathbf{A}=\mathbf{A}$, analogie s čísly: $a\cdot 1=1\cdot a=a$.

Definice: *Inverzí matice* ke čtvercové matici $\mathbf{A}$ je taková matice $\mathbf{B}$, pro kterou je

$$\mathbf{A}\cdot\mathbf{B}=\mathbf{B}\cdot\mathbf{A}=\mathbf{E}.$$

(viz též analogie s čísly). Inverzní matici značíme $\mathbf{A}^{-1}$.

Pozorování: Pokud k matici $\mathbf{A}$ inverzní matice existuje, pak je určena jednoznačně. Důvod je zde:

$$\mathbf{B}_1=\mathbf{E}\cdot\mathbf{B}_1=(\mathbf{B}_2\cdot\mathbf{A})\cdot\mathbf{B}_1=\mathbf{B}_2\cdot(\mathbf{A}\cdot\mathbf{B}_1)=\mathbf{B}_2\cdot\mathbf{E}=\mathbf{B}_2$$

Otázka: Jak poznáme existenci inverzní matice k matici $\mathbf{A}$?

Regulární a singulární matice

Definice: Čtvercová matice je *regulární*, pokud má inverzní matici. Čtvercová matice je *singulární*, pokud nemá inverzní matici.

Pozorování: Součin regulárních matic je regulární matice. Má-li matice $\mathbf{A}$ inverzní matici $\mathbf{A}^{-1}$ a dále má-li matice $\mathbf{B}$ inverzní matici $\mathbf{B}^{-1}$, pak inverzní matice k $\mathbf{A}\cdot\mathbf{B}$ je $\mathbf{B}^{-1}\cdot\mathbf{A}^{-1}$. Platí totiž:

$$(\mathbf{B}^{-1}\cdot\mathbf{A}^{-1})\cdot(\mathbf{A}\cdot\mathbf{B})=\mathbf{B}^{-1}\cdot(\mathbf{A}^{-1}\cdot\mathbf{A})\cdot\mathbf{B}=\mathbf{B}^{-1}\cdot\mathbf{E}\cdot\mathbf{B}=\mathbf{B}^{-1}\cdot\mathbf{B}=\mathbf{E},$$
$$(\mathbf{A}\cdot\mathbf{B})\cdot(\mathbf{B}^{-1}\cdot\mathbf{A}^{-1})=\mathbf{A}\cdot(\mathbf{B}\cdot\mathbf{B}^{-1})\cdot\mathbf{A}^{-1}=\mathbf{A}\cdot\mathbf{E}\cdot\mathbf{A}^{-1}=\mathbf{A}\cdot\mathbf{A}^{-1}=\mathbf{E}.$$

Výpočet inverzní matice eliminací

Algoritmus: Má-li $\mathbf{A}$ lineárně nezávislé řádky, pak existuje $\mathbf{A}^{-1}$ a lze ji vypočítat takto:

$$(\mathbf{A}\,|\,\mathbf{E})\sim(\mathbf{E}\,|\,\mathbf{A}^{-1})$$

Ke zdůvodnění této metody potřebujeme zavést tři typy čtvercových matic, které (pokud jimi násobíme vybranou matici zleva) „emulují“ jednotlivé kroky eliminační metody. Součin těchto elementárních matic emulující všechny provedené kroky je matice $\mathbf{P}$, pro kterou platí:

Věta: Je-li $\mathbf{A}\sim\mathbf{B}$, pak existuje regulární $\mathbf{P}$ taková, že $\mathbf{B}=\mathbf{P}\cdot\mathbf{A}$.

Podmínky regularity matice

Následující podmínky jsou ekvivalentní s regularitou matice $\mathbf{A}\in\mathbf{R}^{n,n}$:

- $\mathbf{A}$ má inverzní matici (viz definice).
- Maticová rovnice $\mathbf{A}\cdot\mathbf{X}=\mathbf{B}$ má řešení pro každou $\mathbf{B}\in\mathbf{R}^{n,m}$.
- Matice $\mathbf{A}$ má lineárně nezávislé řádky.
- $\operatorname{hod}\mathbf{A}=n$.
- existuje eliminační proces, který provede $\mathbf{A}\sim\mathbf{E}$.
- $\det\mathbf{A}\neq 0$ (o determinantech pohovoříme později)

Hodnost součinu

Věta: Je-li $\mathbf{P}$ regulární a platí-li $\mathbf{B}=\mathbf{P}\cdot\mathbf{A}$, pak $\mathbf{A}\sim\mathbf{B}$.

Důkaz: $\mathbf{P}\sim\mathbf{E}$ a stejné kroky eliminace použijeme na $(\mathbf{P}\,|\,\mathbf{B})$, tj.:

$$(\mathbf{P}\,|\,\mathbf{B})=(\mathbf{P}\,|\,\mathbf{P}\cdot\mathbf{A})\sim(\mathbf{E}\,|\,\mathbf{X})=\mathbf{P}^{-1}(\mathbf{P}\,|\,\mathbf{P}\cdot\mathbf{A})=(\mathbf{E}\,|\,\mathbf{A}),$$

takže $\mathbf{A}\sim\mathbf{B}$.

Věta: Násobíme-li matici $\mathbf{A}$ jakoukoli regulární maticí, nezmění se hodnost. Tedy: $\operatorname{hod}\mathbf{A}=\operatorname{hod}(\mathbf{P}\cdot\mathbf{A})$.

Věta: $\operatorname{hod}(\mathbf{A}\cdot\mathbf{B})\leq\min(\operatorname{hod}\mathbf{A},\operatorname{hod}\mathbf{B})$

Důkaz*: $\operatorname{hod}\mathbf{A}=k$, tj. $\mathbf{A}\sim\mathbf{C}$, $\mathbf{C}$ má k nenulových řádků. Existuje tedy $\mathbf{P}$ regulární, že $\mathbf{A}=\mathbf{P}\cdot\mathbf{C}$. Dále platí:

$$\operatorname{hod}(\mathbf{A}\cdot\mathbf{B})=\operatorname{hod}(\mathbf{P}\cdot\mathbf{C}\cdot\mathbf{B})=\operatorname{hod}(\mathbf{C}\cdot\mathbf{B})\leq k.$$

LU rozklad

- $\mathbf{A}=\mathbf{L}\cdot\mathbf{U}$
- někdy je třeba prohodit sloupce/řádky

a) algebra-all, 8, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) Viz p. d. 4/2010

Terminologie

Definice: Čtvercová matice je *horní trojúhelníková*, pokud má nenulové prvky soustředěny jen v horním trojúhelníku, jinými slovy, pokud má pod diagonálou jen nulové prvky.

Čtvercová matice se nazývá *dolní trojúhelníková*, pokud má nenulové prvky soustředěny v dolním trojúhelníku, jinými slovy, pokud má nad diagonálou jen nulové prvky.

Pozorování: Čtvercovou matici lze přímým chodem eliminační metody převést na horní trojúhelníkovou matici. Schodovitá čtvercová matice je totiž horní trojúhelníková.

Na co LU rozklad

Nechť $\mathbf{A}$ je regulární čtvercová matice. Předpokládejme, že se podaří najít dolní trojúhelníková matice $\mathbf{L}$ a horní trojúhelníková matice $\mathbf{U}$ tak, že $\mathbf{A}=\mathbf{L}\cdot\mathbf{U}$. Máme za úkol řešit soustavu

$$\mathbf{A}\cdot\mathbf{x}=\mathbf{b}$$

Nahradíme v soustavě matici $\mathbf{A}$ součinem $\mathbf{L}\cdot\mathbf{U}$ a označíme $\mathbf{U}\cdot\mathbf{x}=\mathbf{z}$. Dostáváme:

$$\mathbf{L}\cdot\mathbf{U}\cdot\mathbf{x}=\mathbf{b}\quad\text{právě když}\quad\mathbf{L}\cdot\mathbf{z}=\mathbf{b},\quad\mathbf{U}\cdot\mathbf{x}=\mathbf{z}.$$

Nejprve vyřešíme soustavu $\mathbf{L}\cdot\mathbf{z}=\mathbf{b}$ dopřednou substitucí a potom dosadíme $\mathbf{z}$ do pravé strany soustavy $\mathbf{U}\cdot\mathbf{x}=\mathbf{z}$, kterou řešíme zpětnou substitucí.

Algoritmus LU rozkladu

Na matici $\mathbf{A}$ provádíme jen jeden typ eliminační úpravy: přičtení α-násobku nějakého řádku k jinému, který je napsán pod ním. Tuto úpravu lze „emulovat“ násobením zleva maticí $\mathbf{L}_i$, která je jistě dolní trojúhelníková.

$$\mathbf{A} \sim \mathbf{A}_1 = \mathbf{L}_1\mathbf{A} \sim \mathbf{A}_2 = \mathbf{L}_2(\mathbf{L}_1\mathbf{A}) \sim$$
$$\sim \mathbf{A}_3 = \mathbf{L}_3(\mathbf{L}_2(\mathbf{L}_1\mathbf{A})) \sim \cdots \sim \mathbf{U} = (\mathbf{L}_k \cdots \mathbf{L}_3\mathbf{L}_2\mathbf{L}_1)\mathbf{A}$$

Součin dolních trojúhelníkových matic s jedničkami na diagonále je dolní trojúhelníková matice s jedničkami na diagonále. Inverze dolní trojúhelníkové matice s jedničkami na diagonále je dolní trojúhelníková matice s jedničkami na diagonále. Takže:

$$\mathbf{L}'\mathbf{A} = \mathbf{U}, \qquad \mathbf{A} = (\mathbf{L}')^{-1}\mathbf{U} = \mathbf{L}\mathbf{U}.$$

Příklad

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 4 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -5 \\ 0 & -6 & -12 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -4 & 0 & 1 \end{pmatrix} \cdot \mathbf{A} \sim$$

$$\sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -5 \\ 0 & 0 & 18 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -6 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -4 & 0 & 1 \end{pmatrix} \cdot \mathbf{A} = \mathbf{L}_2 \cdot \mathbf{L}_1 \cdot \mathbf{A}$$

$$\mathbf{L} = \mathbf{L}_1^{-1} \cdot \mathbf{L}_2^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 6 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 6 & 1 \end{pmatrix}$$

$$\mathbf{U} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -5 \\ 0 & 0 & 18 \end{pmatrix}$$

Jak vzniká matice L

Platí $\mathbf{L} = (\mathbf{L}_k \cdots \mathbf{L}_3\mathbf{L}_2\mathbf{L}_1)^{-1} = \mathbf{L}_1^{-1}\mathbf{L}_2^{-1}\mathbf{L}_3^{-1} \cdots \mathbf{L}_k^{-1}$. Je:

$$\mathbf{L}_i^{-1} = \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 \\ & & \dots & & \dots & \\ 0 & 0 & \dots & 1 & \dots & 0 \\ & & \dots & & \dots & \\ 0 & 0 & \dots & -\alpha & \dots & 0 \\ & & \dots & & \dots & \\ 0 & 0 & \dots & 0 & \dots & 1 \end{pmatrix},$$

kde α_i je koeficient eliminačního kroku. Celkový součin matic $\mathbf{L}_1^{-1}\mathbf{L}_2^{-1}\mathbf{L}_3^{-1} \cdots \mathbf{L}_k^{-1}$ (v uvedeném pořadí) obsahuje pod diagonálou na odpovídajících místech opačné hodnoty koeficientů všech eliminačních kroků, které byly v eliminaci provedeny.

Jiný příklad

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 1 \\ 4 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & -5 \\ 0 & -6 & -12 \end{pmatrix}$$

Nelze pokračovat v eliminaci bez prohození řádků…

Problém

Přestože $\mathbf{A}$ je regulární, může se stát, že během eliminace se objeví nulový diagonální prvek. Klasická eliminace pak dovoluje prohodit řádky. To je ale emulováno násobením zleva permutační maticí $\mathbf{P}_{i,j}$, která není dolní trojúhelníková. Výsledný součin emulačních matic pak není dolní trojúhelníková matice.

Je tedy třeba prohodit řádky matice $\mathbf{A}$ tak, aby nová matice $\mathbf{A}'$ tento problém neměla a dala se rozložit na $\mathbf{L}\cdot\mathbf{U}$. Nechť $\mathbf{P}'$ je vhodná permutační matice. Pak $\mathbf{P}' \cdot \mathbf{A}$ prohazuje řádky. Předpokládejme:

$$\mathbf{A}' = \mathbf{P}' \cdot \mathbf{A} = \mathbf{L} \cdot \mathbf{U}.$$

Označme $(\mathbf{P}')^{-1} = \mathbf{P}$. To je také permutační matice. Platí totiž $(\mathbf{P}')^{-1} = (\mathbf{P}')^T$. S tímto označením dostáváme rozklad:

$$\mathbf{A} = \mathbf{P} \cdot \mathbf{L} \cdot \mathbf{U}$$

Otázka

Nechť $\mathbf{A}$ je regulární.

Půjde vždy najít takové prohození řádků matice $\mathbf{A}$, aby pak eliminace s jediným povoleným typem operace (přičtení α-násobku řádku k řádku pod ním) dovedla převést matici na horní trojúhelníkovou?

Odpověď: Ano.

Zdůvodnění: pokud narazíme při eliminaci na potřebu prohodit řádky, prohodíme je ve výchozí matici $\mathbf{A}$ a eliminujeme znovu od začátku. Tuto metodu „pokus-omyl“ opakujeme tak dlouho, až se povede matici $\mathbf{A}$ s prohozenými řádky eliminovat na $\mathbf{U}$.

Praktický výpočet LU rozkladu

se samozřejmě nedělá metodou pokus-omyl. Koeficienty eliminačních kroků násobíme -1 a ukládáme postupně do matice $\mathbf{L}$, která je na počátku eliminace jednotková. Při potřebě prohodit řádky prohodíme také řádky v matici $\mathbf{L}$, ale necelé: při prohazování k-tého řádku s $(k+j)$-tým v eliminované matici prohodíme v matici $\mathbf{L}$ tytéž řádky, ale jen po sloupec $k-1$.

Další vylepšené numerické metody LU rozkladu mají stejnou složitost jako algoritmus pro maticové násobení.

Shrnutí

Věta: Ke každé regulární matici $\mathbf{A}$ existují matice:

- $\mathbf{P}$ … permutační matice,
- $\mathbf{L}$ … dolní trojúhelníková matice s jedničkami na diagonále,
- $\mathbf{U}$ … horní trojúhelníková matice,

tak, že $\mathbf{A} = \mathbf{P} \cdot \mathbf{L} \cdot \mathbf{U}$.

Poznámka: při výskytu nulového prvku na diagonále lze také místo řádků prohodit sloupce. Pak se permutační matice $\mathbf{P}_{i,j}$ „nemíchají“ s maticemi $\mathbf{L}_i$, neboť násobí matici $\mathbf{A}$ zprava. Dostáváme pak vzorec: $\mathbf{A} = \mathbf{L} \cdot \mathbf{U} \cdot \mathbf{P}$.

Determinant

- je číslo jistým způsobem charakterizující čtvercovou matici
- $\det \mathbf{A} = 0$ pro singulární matici, $\det \mathbf{A} \neq 0$ pro regulární matici
- používá se při řešení lineárních soustav
- … a v mnoha dalších aplikacích

a) algebra-all, 9, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) Viz p. d. 4/2010

Definice determinantu

Definice: Nechť $\mathbf{A} = (a_{i,j}) \in \mathbf{R}^{n,n}$ je čtvercová matice. Číslo

$$\sum_{\text{permutace } \pi=(i_1,i_2,\dots,i_n)} \operatorname{sgn}\pi \cdot a_{1,i_1} a_{2,i_2} \cdots a_{n,i_n}$$

nazýváme *determinantem matice* $\mathbf{A}$ a značíme je $\det \mathbf{A}$.

Poznámka: Abychom tomu vzorci porozumněli a dokázali z něj odvodit základní vlastnosti determinantů, potřebujeme si připomenout vlastnosti permutací…

Permutace

Permutace n prvků je uspořádaná n-tice čísel z množiny $\{1, 2, \dots, n\}$, přitom každé číslo je v n-tici zastoupeno právě jednou.

Příklad: $(3, 1, 2, 5, 4)$ je permutace pěti prvků.

$(i_1, i_2, \dots, i_n)$ je permutace z n prvků, pokud $i_j \in \{1, 2, \dots, n\}$ a $i_j \neq i_k$ pro $j \neq k$.

Jiný pohled: Permutace je bijektivní zobrazení na $\{1, 2, \dots, n\}$.

Vztah mezi těmito pohledy: Je-li dána n-tice $(i_1, i_2, \dots, i_n)$, pak je dáno zobrazení $z : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ předpisem $z(j) = i_j$. Je-li dáno zobrazení z, pak lze sestrojit n-tici $(z(1), z(2), \dots, z(n))$.

Permutace, vlastnosti

- Skládáním permutací (jako zobrazení) dostáváme permutaci.
- Generická (jednotková) permutace je $(1, 2, \dots, n)$.
- Každá permutace má svou inverzní permutaci.
- Počet permutací n prvků je $n!$.

Znaménko permutace

inverze v permutaci $(i_1, i_2, \dots, i_n)$ je výskyt jevu:

$$i_j > i_k \text{ a současně } j < k.$$

Příklad: inverze permutace $(3, 1, 2, 5, 4)$ jsem vyznačil pomocí oblouků:

$$(\overbrace{3, 1}, 2, \overbrace{5, 4})$$

Tato permutace má tři inverze.

Definice: Má-li permutace π sudý počet inverzí, je $\operatorname{sgn}\pi = +1$, má-li π lichý počet inverzí, je $\operatorname{sgn}\pi = -1$.
Číslu $\operatorname{sgn}\pi$ říkáme *znaménko permutace*.

Příklad: $\operatorname{sgn}(3, 1, 2, 5, 4) = -1$.
Znaménko generické permutace je $+1$.

Cvičení: jaké znaménko má permutace $(n, n-1, \dots, 3, 2, 1)$?

Přechod sudá – lichá

Prohození dvou prvků v permutaci změní znaménko permutace.

Důkaz: V následující permutaci prohodím prvky x a y:

$$(\dots \text{prvky vlevo} \dots, x, \dots \text{prvky uvnitř} \dots, y, \dots \text{prvky vpravo} \dots)$$

Inverze, které nenavazují na prvek x nebo y zůstávají nezměněny. Inverze mezi prvky vlevo a x nebo y zůstávají nezměněny. Inverze mezi x nebo y a prvky vpravo zůstávají nezměněny. Inverze mezi x nebo y a prvky uvnitř po dvou vznikají nebo zanikají nebo se nemění. Inverze mezi x a y vznikne nebo zanikne.

Důsledek: Znaménko permutace poznáme podle počtu *transpozic* (jednoho prohození dvou prvků), které je potřeba na permutaci provést, aby byla převedena na generickou permutaci.

Návrat k definici deterinantu

Definice: Nechť $\mathbf{A} = (a_{i,j}) \in \mathbf{R}^{n,n}$ je čtvercová matice. Číslo

$$\det \mathbf{A} = \sum_{\text{permutace } \pi=(i_1,i_2,\dots,i_n)} \operatorname{sgn}\pi \cdot a_{1,i_1} a_{2,i_2} \cdots a_{n,i_n}$$

- Užitečná je představa šachových věží.
- Příklad pro matice typu $(1, 1), (2, 2), (3, 3)$ … Sarrusovo pravidlo.
- Pozor, pro matice větších typů Sarrusovo pravidlo nelze použít!

Determinant horní trojúhelníkové matice

$$\det \begin{pmatrix} a_{1,1}, & a_{1,2}, & \dots, & a_{1,n-1}, & a_{1,n} \\ 0, & a_{2,2}, & \dots, & a_{2,n-1}, & a_{2,n} \\ 0, & 0, & \dots, & a_{3,n-1}, & a_{3,n} \\ & & \vdots & & \\ 0, & 0, & \dots, & 0, & a_{n,n} \end{pmatrix}$$

je roven součinu prvků na diagonále: $a_{1,1} \cdot a_{2,2} \cdot a_{3,3} \cdots a_{n,n}$.

Vidí všichni proč?

Základní vlastnosti determinantu

- Prohození řádků změní znaménko determinantu
- Matice se dvěma stejnými řádky má nulový determinant
- Pronásobení jediného řádku α-krát zvětší α-krát i determinant
- Je-li jeden řádek zapsaný jakou součet dvou částí, pak determinat takové matice je roven součtu determinantů matic, ve kterých jsou místo tohoto řádku jen jeho části:

$$\det\begin{pmatrix}\vdots\\ \overrightarrow{a}_i\\ \vdots\end{pmatrix} + \det\begin{pmatrix}\vdots\\ \overrightarrow{b}_i\\ \vdots\end{pmatrix} = \det\begin{pmatrix}\vdots\\ \overrightarrow{a}_i + \overrightarrow{b}_i\\ \vdots\end{pmatrix}.$$

- Třetí typ kroku eliminační metody nezmění determinant.

Metoda výpočtu determinantu

Algoritmus: Eliminací převedeme danou matici $\mathbf{A}$ na horní trojúhelníkovou matici $\mathbf{U}$. Pokud během eliminace použijeme první nebo druhý typ kroku eliminace, je potřeba si poznamenat, jak se změnil determinant. Třetí typ kroku nemění determinant vůbec. Konečně $\det\mathbf{U}$ je součin prvků na diagonále.

Složitost algoritmu: n^3. Výrazná úspora proti vzorci v definici, který ma složitost $n!$.

Příklad

$$\begin{vmatrix}1&2&3&3\\2&4&1&4\\4&2&1&2\\3&1&2&1\end{vmatrix} = \begin{vmatrix}1&2&3&3\\0&0&-5&-2\\0&-6&-11&-10\\0&-5&-7&-8\end{vmatrix} = (-1)^4\begin{vmatrix}1&2&3&3\\0&6&11&10\\0&0&5&2\\0&5&7&8\end{vmatrix} =$$

$$\frac{1}{6}\begin{vmatrix}1&2&3&3\\0&6&11&10\\0&0&5&2\\0&30&42&48\end{vmatrix} = \frac{1}{6}\begin{vmatrix}1&2&3&3\\0&6&11&10\\0&0&5&2\\0&0&-13&-2\end{vmatrix} =$$

$$\frac{1}{6}\cdot\frac{1}{5}\begin{vmatrix}1&2&3&3\\0&6&11&10\\0&0&5&2\\0&0&-65&-10\end{vmatrix} = \frac{1}{30}\begin{vmatrix}1&2&3&3\\0&6&11&10\\0&0&5&2\\0&0&0&16\end{vmatrix} = 16.$$

Za chvíli uvidíme, že to lze spočítat jednodušeji…

Řádky a sloupce jedno jest

Tvrzení: $\det\mathbf{A} = \det\mathbf{A}^T$.

Důkaz: Mám permutaci $(i_1, i_2, \dots, i_n)$ a podle ní provedu sloupcový výběr prvků matice a vynásobím mezi sebou:

$$a_{i_1,1}\cdot a_{i_2,2}\cdots a_{i_n,n} = a_{1,j_1}\cdot a_{2,j_2}\cdots a_{n,j_n}$$

Součin reálných čísel je komutativní, tak jsem činitele uspořádal podle velikosti řádkového indexu. Jaký je vztah mezi permutacemi: $(i_1, i_2, \dots, i_n)$ a $(j_1, j_2, \dots, j_n)$? Jsou si vzájmně inverzní. A inverzní permutace mají stejné znaménko. Takže vzorce s řádkovým i sloupcovým výběrem dávají stejný výsledek.

Důsledek: Při eliminaci za účelem výpočtu determinantu lze libovolně přecházet mezi řádkovými a sloupcovými úpravami.

Regulární a singulární matice

Věta: Matice $\mathbf{A}$ je regulární, právě když $\det\mathbf{A} \neq 0$.

Důkaz: $\mathbf{A}$ je regulární právě když $\mathbf{A} \sim \mathbf{E}$. Dále si stačí uvědomit, že Gaussova eliminace nemění *nulovost* determinantu.

Determinant součinu matic

Věta: Pro dvě čtvercové matice typu (n, n) platí

$$\det(\mathbf{A}\cdot\mathbf{B}) = (\det\mathbf{A})\cdot(\det\mathbf{B}).$$

Důkaz*: Lze provést $\mathbf{A} \sim \mathbf{U}_1$ řádkovými eliminačními úpravami, aby se nezměnil determinant. Dále lze převést $\mathbf{B}$ na $\mathbf{U}_2$ sloupcovými eliminačními úpravami tak, že se nezmění determinant. Snadno se ukáže, že

$$\det(\mathbf{U}_1\cdot\mathbf{U}_2) = (\det\mathbf{U}_1)\cdot(\det\mathbf{U}_2)$$

Existují matice $\mathbf{P}_1, \mathbf{P}_2$ tak, že $\mathbf{U}_1 = \mathbf{P}_1\mathbf{A}$, $\mathbf{U}_2 = \mathbf{B}\mathbf{P}_2$. Stejné řádkové i sloupcové úpravy provedeme na $\mathbf{A}\cdot\mathbf{B}$, tedy $\mathbf{P}_1\mathbf{A}\cdot\mathbf{B}\mathbf{P}_2 = \mathbf{U}_1\cdot\mathbf{U}_2$. Úpravy nemění determinant, takže

$$\begin{aligned}\det(\mathbf{A}\cdot\mathbf{B}) &= \det(\mathbf{P}_1\mathbf{A}\cdot\mathbf{B}\mathbf{P}_2) = \det(\mathbf{U}_1\cdot\mathbf{U}_2) =\\ &= (\det\mathbf{U}_1)\cdot(\det\mathbf{U}_2) = (\det\mathbf{A})\cdot(\det\mathbf{B}).\end{aligned}$$

Důsledky věty o determinantu součinu

- $\det\mathbf{A}^{-1} = 1/\det\mathbf{A}$
- Je-li $\mathbf{A} = \mathbf{L}\mathbf{U}$ rozklad matice $\mathbf{A}$, pak $\det\mathbf{A} = \det\mathbf{U}$, tedy $\det\mathbf{A}$ je roven součinu diagonálních prvků v matici $\mathbf{U}$.
  (připomínám, že matice $\mathbf{L}$ má na diagonále jedničky).

Rozvoj determinantu podle řádku

Terminologie: Vyřadíme-li ze čtvercové matice $\mathbf{A} \in \mathbf{R}^{n,n}$ i-tý řádek a j-tý sloupec, dostáváme matici $\mathbf{A}_{i,j} \in \mathbf{R}^{n-1,n-1}$. Číslo

$$D_{i,j} = (-1)^{i+j}\det\mathbf{A}_{i,j}$$

se nazývá *doplněk matice* $\mathbf{A}$ *v pozici* (i,j).

Věta o rozvoji: Nechť $D_{i,j}$ jsou doplňky čtvercové matice $\mathbf{A} = (a_{i,j})$. Pak platí

$$\det\mathbf{A} = a_{r,1}D_{r,1} + a_{r,2}D_{r,2} + \cdots + a_{r,n}D_{r,n}.$$

Náznak důkazu: vytkněte ze součtu z definice determinantu $a_{r,1}$ (jen z těch sčítanců, kde se $a_{r,1}$ vyskytuje), dále vytkněte a_{r_2} atd. až $a_{r,n}$. V závorkách po vytknutí dostanete $D_{r,i}$.

Rozjímání nad větou o rozvoji

- Protože $\det\mathbf{A} = \det\mathbf{A}^T$, platí analogická věta o rozvoji podle sloupce
- Je-li v řádku/sloupci hodně nul, je v součtu podle věty o rozvoji hodně nulových sčítanců. Stačí zapsat jen ty nenulové a redukovat výpočet determinantu matice typu (n,n) na několik (málo) determinantů matic typu $(n-1,n-1)$.
- Pozor: rekurzivní volání výpočtu determinantu podle věty o rozvoji má složitost $n!$, takže tento algoritmus je nepoužitelný.
- Důsledkem věty o rozvoji je tvrzení:

$$0 = a_{r,1}D_{k,1} + a_{r,2}D_{k,2} + \cdots + a_{r,n}D_{k,n} \quad \text{pro } r \neq k.$$

  Stačí provést větu o rozvoji na matici se dvěma stejnými řádky.
- Věta o rozvoji má řadu dalších teoretických důsledků, některé se dozvíme později…

Příklad

$$\begin{vmatrix} 1 & 2 & 3 & 3 \\ 2 & 4 & 1 & 4 \\ 4 & 2 & 1 & 2 \\ 3 & 1 & 2 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 & 1 \\ 2 & 4 & 1 & 0 \\ 4 & 2 & 1 & 0 \\ 3 & 1 & 2 & 0 \end{vmatrix} = -\begin{vmatrix} 2 & 4 & 1 \\ 4 & 2 & 1 \\ 3 & 1 & 2 \end{vmatrix} =$$

$$-\begin{vmatrix} 2 & 4 & 1 \\ 2 & -2 & 0 \\ -1 & -7 & 0 \end{vmatrix} = 2\begin{vmatrix} 1 & -1 \\ 1 & 7 \end{vmatrix} = 2\cdot 8 = 16.$$

Inverzní matice pomocí doplňků

Je-li $\mathbf{A} \in \mathbf{R}^{n,n}$ regulární, pak

$$\mathbf{A}^{-1} = \frac{1}{\det\mathbf{A}}\mathbf{D}^T,$$

kde $\mathbf{D} = (D_{i,j})$ je matice doplňků $\mathbf{A}$ v pozicích (i,j).

Důkaz: Ověříme, že $\mathbf{A}\mathbf{A}^{-1} = \mathbf{E}$.
Označíme $\mathbf{A} = (a_{i,j})$, $\mathbf{D}^T = (D_{k,j})$, $\mathbf{E} = (e_{i,k})$.

$$e_{i,k} = \sum_{j=1}^{n} a_{i,j}\frac{1}{\det\mathbf{A}}D_{k,j} = \frac{1}{\det\mathbf{A}}(a_{i,1}D_{k,1} + a_{i,2}D_{k,2} + \cdots + a_{i,n}D_{k,n}) =$$

$$= \begin{cases} \dfrac{1}{\det\mathbf{A}}\det\mathbf{A} = 1 & \text{pro } i = k, \\ \dfrac{1}{\det\mathbf{A}}\cdot 0 = 0 & \text{pro } i \neq k. \end{cases}$$

Využili jsme větu o rozvoji determinantu podle i-tého řádku.

Příklad: inverze k matici typu (2, 2)

Je dána matice

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Matice doplňků k této matici je

$$\mathbf{D} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

Takže

$$\mathbf{A}^{-1} = \frac{1}{\det\mathbf{A}}\mathbf{D}^T = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Příklad: inverze matice pomocí doplňků

Je dána matice $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ -1 & 0 & 1 \\ 2 & 2 & 1 \end{pmatrix}$.

Matice doplňků je:

$$\mathbf{D} = \begin{pmatrix} +\begin{vmatrix} 0 & 1 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} -1 & 1 \\ 2 & 1 \end{vmatrix} & +\begin{vmatrix} -1 & 0 \\ 2 & 2 \end{vmatrix} \\ -\begin{vmatrix} 2 & 3 \\ 2 & 1 \end{vmatrix} & +\begin{vmatrix} 1 & 3 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} 1 & 2 \\ 2 & 2 \end{vmatrix} \\ +\begin{vmatrix} 2 & 3 \\ 0 & 1 \end{vmatrix} & -\begin{vmatrix} 1 & 3 \\ -1 & 1 \end{vmatrix} & +\begin{vmatrix} 1 & 2 \\ -1 & 0 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} -2 & 3 & -2 \\ 4 & -5 & 2 \\ 2 & -4 & 2 \end{pmatrix},$$

takže: $\det\mathbf{A} = -2$, $\mathbf{A}^{-1} = \dfrac{1}{\det\mathbf{A}}\mathbf{D}^T = -\dfrac{1}{2}\begin{pmatrix} -2 & 4 & 2 \\ 3 & -5 & -4 \\ -2 & 2 & 2 \end{pmatrix}$.

Soustavy lineárních rovnic

- vlastnosti množin řešení
- metody hledání řešení
- nejednoznačnost zápisu řešení

a) algebra-all, 10, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) Viz p. d. 4/2010

Terminologie

Definice: Nechť $\mathbf{A} = (a_{i,j}) \in \mathbf{R}^{m,n}$ je matice, $\mathbf{b} \in \mathbf{R}^{m,1}$ je jednosloupcová matice. Maticová rovnost

$$\mathbf{A}\cdot\mathbf{x} = \mathbf{b}$$

s neznámou jednosloupcovou maticí $\mathbf{x} \in \mathbf{R}^{n,1}$ nazýváme *soustavou lineárních rovnic* (m rovnic, n neznámých). $\mathbf{A}$ je *matice soustavy*, $\mathbf{b}$ je *sloupec pravých stran*, $(\mathbf{A}|\mathbf{b})$ je *rozšířená matice soustavy*.

Je-li $\mathbf{o} \in \mathbf{R}^{m,1}$ nulový sloupcový vektor, pak $\mathbf{A}\cdot\mathbf{x} = \mathbf{o}$ je *homogenní soustava lineárních rovnic*.

Řešení soustavy je takový vektor z $\mathbf{R}^n$, který, zapsaný do sloupce místo neznámé matice $\mathbf{x}$, splňuje danou maticovou rovnost.

Úloha: Najít všechna řešení, tj. vymezit podmnožinu $M \subseteq \mathbf{R}^n$ všech řešení soustavy.

Dva pohledy na soustavu lin. rovnic

Pohled po řádcích, tedy po jednotlivých rovnicích. Každá rovnice sama vymezuje podmnožinu všech svých řešení $M_i \subseteq \mathbf{R}^n$, $i \in \{1,2,\ldots,m\}$. Geometricky je M_i nadrovinou (podprostorem dimenze $n-1$ posunutým z počátku do nějakého jiného bodu). Všechny rovnice mají být splněny současně, hledáme tedy společný *průnik* všech těchto nadrovin M_i.

Pohled po sloupcích. Rozepišme matici soustavy $\mathbf{A}$ do sloupců: $\mathbf{A} = (\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)$. Soustava $\mathbf{A}\cdot\mathbf{x} = \mathbf{b}$ přechází na:

$$\mathbf{A}\cdot\mathbf{x} = (\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n)\cdot\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = x_1\mathbf{A}_1 + x_2\mathbf{A}_2 + \cdots + x_n\mathbf{A}_n = \mathbf{b}$$

Hledáme tedy koeficienty lineární kombinace sloupců matice $\mathbf{A}$, které zaručí, že se daná kombinace rovná pravé straně $\mathbf{b}$.

K čemu slouží eliminační metoda

Má-li soustava $\mathbf{A}\cdot\mathbf{x}=\mathbf{b}$ množinu řešení M a je

$$(\mathbf{A}\,|\,\mathbf{b}) \sim (\mathbf{C}\,|\,\mathbf{d})$$

pak soustava $\mathbf{C}\cdot\mathbf{x}=\mathbf{d}$ má stejnou množinu řešení M.

Když eliminujeme na schodovitou matici $\mathbf{C}$, pak půjde u soustavy $\mathbf{C}\cdot\mathbf{x}=\mathbf{d}$ hledaná množina řešení M lépe najít.

Frobeniova věta, řešitelnost soustavy

Věta: Soustava $\mathbf{A}\cdot\mathbf{x}=\mathbf{b}$ má aspoň jedno řešení právě tehdy, když $\hod\mathbf{A}=\hod(\mathbf{A}\,|\,\mathbf{b})$.

Důkaz: (sloupcový pohled): soustava má řešení právě když vektor $\mathbf{b}$ leží v lineárním obalu sloupcových vektorů $\mathbf{A}_1,\mathbf{A}_2,\ldots,\mathbf{A}_n$, což je právě tehdy, když $\hod\mathbf{A}=\hod(\mathbf{A}\,|\,\mathbf{b})$. Využijeme také toho, že hodnost matice není jen dimenze lin. obalu řádků, ale je to také dimenze lineárního obalu sloupců matice, neboť $\hod\mathbf{A}=\hod\mathbf{A}^T$.

Důkaz: (eliminační pohled): Po eliminaci na schodovitou matici máme soustavu $\mathbf{C}\cdot\mathbf{x}=\mathbf{d}$ která nemá řešení právě tehdy, když existuje nulový řádek v matici $\mathbf{C}$ s nenulovým číslem na pravé straně. Tj. právě tehdy když $\hod\mathbf{C}\neq\hod(\mathbf{C}\,|\,\mathbf{d})$. Eliminační metoda ovšem nemění hodnost.

Homogenní soustava Ax = o

- Homogenní soustava lineárních rovnic má vždy nulové řešení.
- Množinou řešení M_0 homogenní soustavy je vždy podprostor:

$\mathbf{u}\in M_0,\ \mathbf{v}\in M_0,\quad$ tj. $\quad\mathbf{Au}=\mathbf{o},\quad\mathbf{Av}=\mathbf{o}.$

$$\mathbf{A}(\mathbf{u}+\mathbf{v})=\mathbf{Au}+\mathbf{Av}=\mathbf{o}+\mathbf{o}=\mathbf{o},\quad\text{tj. }\mathbf{u}+\mathbf{v}\in M_0.$$

$\mathbf{u}\in M_0,\ \alpha\in\mathbf{R},\quad$ tj. $\quad\mathbf{Au}=\mathbf{o}.$

$$\mathbf{A}(\alpha\mathbf{u})=\alpha\mathbf{A}(\mathbf{u})=\alpha\,\mathbf{o}=\mathbf{o},\quad\text{tj.}\quad\alpha\,\mathbf{u}\in M_0.$$

Jak vyřešit homogenní soustavu

- Nejprve převedeme eliminací na soustavu se stejnou množinou řešení, ale se schodovitou maticí soustavy:

$$(\mathbf{A}\,|\,\mathbf{o}) \sim (\mathbf{C}\,|\,\mathbf{o})$$

- Každá nenulová rovnice v soustavě $\mathbf{Cx}=\mathbf{o}$ umožní spočítat jednu neznámou (při zpětné substituci zespoda nahoru). Těmto proměnným říkáme *vázané proměnné*. Ostatní (takto nespočítané) proměnné jsou *volné proměnné*, neboli parametry. Nechť $t_1,t_2,\ldots,t_k$ jsou všechny volné proměnné. Můžeme volit tyto hodnoty za $(t_1,t_2,\ldots,t_k)$

$$(1,0,\ldots,0),\quad(0,1,\ldots,0),\quad\ldots,\quad(0,0,\ldots,1)$$

  a pro každou tuto volbu volných proměnných dopočítáme proměnné vázané. Dostáváme tak lineárně nezávislou množinu řešení, která je bází podprostoru M_0 všech řešení.

Příklad (homogenní soustava)

Řešme soustavu $\mathbf{A}\cdot\mathbf{x}=\mathbf{o}$ s maticí:

$$\mathbf{A}=\begin{matrix}x_1,\\1\\1\\2\\3\end{matrix}\!\!\begin{matrix}x_2,\\3\\1\\8\\9\end{matrix}\!\!\begin{matrix}x_3,\\2\\1\\5\\6\end{matrix}\!\!\begin{matrix}x_4,\\0\\-1\\3\\2\end{matrix}\!\!\begin{matrix}x_5\\3\\5\\7\\12\end{matrix}\sim\begin{matrix}x_1,\\1\\0\\0\\0\end{matrix}\!\!\begin{matrix}x_2,\\3\\2\\0\\0\end{matrix}\!\!\begin{matrix}x_3,\\2\\1\\0\\0\end{matrix}\!\!\begin{matrix}x_4,\\0\\3\\2\\0\end{matrix}\!\!\begin{matrix}x_5\\3\\1\\3\end{matrix}$$

Vázané proměnné: $x_1,\ x_2,\ x_4$, volné proměnné: $x_3,\ x_5$.

Při volbě $x_3=1,\ x_5=0$ vychází: $x_4=0,\ x_2=-1/2,\ x_1=-1/2,$
při volbě $x_3=0,\ x_5=1$ vychází: $x_4=-3/2,\ x_2=7/4,\ x_1=-33/4.$

Takže mám dvě lineárně nezávislá řešení:

$$(-1/2,-1/2,1,0,0),\ (-33/4,7/4,0,-3/2,1).$$

Všechna řešení tvoří lineární obal těchto dvou řešení:

$$M_0=\langle(-1,-1,2,0,0),\ (-33,7,0,-6,4)\rangle$$

Dimenze prostoru řešení

- Dimenze prostoru řešení homogenní soustavy je rovna počtu volných proměnných,
- což je rovno počtu všech proměnných minus počtu vázaných proměnných,
- což je rovno počtu všech proměnných minus počtu nenulových rovnic soustavy $\mathbf{Cx}=\mathbf{o}$ se schodovitou maticí,
- což je rovno počtu všech rovnic minus hodnost matice soustavy.

Závěr: Nechť M_0 je množina řešení soustavy $\mathbf{Ax}=\mathbf{o}$ s m rovnicemi a n neznámými. Pak

$$\dim M_0=n-\hod\mathbf{A}.$$

Dva podprostory v $\mathbf{R}^n$ vymezené maticí A

Nechť je dána matice $\mathbf{A}\in\mathbf{R}^{m,n}$

- Označme R lineární obal řádků matice $\mathbf{A}$. Je to podprostor v $\mathbf{R}^n$.
- Označme M_0 množinu všech řešení homogenní soustavy $\mathbf{Ax}=\mathbf{o}$. Je to rovněž podprostor v $\mathbf{R}^n$. Nazývá se *nulovým prostorem matice* $\mathbf{A}$.
- Do řádků matice $\mathbf{B}$ napišme nějakou bázi prostoru M_0.

Platí:

- Každý vektor z M_0 řeší soustavu $\mathbf{Ax}=\mathbf{o}$.
- Každý vektor z R řeší soustavu $\mathbf{Bx}=\mathbf{o}$.
- Je-li $\vec{u}\in R$ a $\vec{v}\in M_0$, pak $\vec{u}\cdot\vec{v}^T=0$.
- $\dim R+\dim M_0=n=\dim\mathbf{R}^n$

Algoritmus hledání báze nulového prostoru

Algoritmus: Nechť $\mathbf{A}\sim(\mathbf{E}\,|\,\mathbf{C})$, kde $\mathbf{E}$ je jednotková matice. Pak řádky matice $(-\mathbf{C}^T\,|\,\mathbf{E}')$ obsahují bázi řešení soustavy $\mathbf{Ax}=\mathbf{o}$.

Poznámka: $\mathbf{E}'$ je zde také jednotková matice, ovšem obecně jiného typu než matice $\mathbf{E}$.

Důkaz: Řádky matice $(-\mathbf{C}^T\,|\,\mathbf{E}')$ jsou lineárně nezávislé a jejich počet je roven $n-\hod\mathbf{A}$. Takže lin. obal těchto řádků má stejnou dimenzi, jako prostor řešení M_0. Stačí ukázat, že každý řádek matice $(-\mathbf{C}^T\,|\,\mathbf{E}')$ řeší soustavu $\mathbf{Ax}=\mathbf{o}$:

$$(\mathbf{E}\,|\,\mathbf{C})\cdot\begin{pmatrix}-\mathbf{C}\\\hline\mathbf{E}'\end{pmatrix}=\mathbf{E}\cdot(-\mathbf{C})+\mathbf{C}\cdot\mathbf{E}'=-\mathbf{C}+\mathbf{C}=\mathbf{O}.$$

Poznámka: nelze-li provést $\mathbf{A}\sim(\mathbf{E}\,|\,\mathbf{C})$, pak je možné dostat $(\mathbf{E}\,|\,\mathbf{C})$ po vhodné permutaci sloupců (změna pořadí neznámých). Zpětnou permutaci sloupců pak provedeme na matici $(-\mathbf{C}^T\,|\,\mathbf{E}')$ a máme hledanou bázi prostoru řešení.

Příklad

Metodou ze slídu [11] vyřešíme soustavu ze slídu [8]. Matici převedeme Gauss-Jordanovou eliminací:

$$\mathbf{A} = \begin{pmatrix} 1 & 3 & 2 & 0 & 3 \\ 1 & 1 & 1 & -1 & 5 \\ 2 & 8 & 5 & 3 & 7 \\ 3 & 9 & 6 & 2 & 12 \end{pmatrix} \sim \begin{matrix} x_1, & x_2, & x_3, & x_4, & x_5 \\ \end{matrix} \begin{pmatrix} 1 & 0 & 1/2 & 0 & 33/4 \\ 0 & 1 & 1/2 & 0 & -7/4 \\ 0 & 0 & 0 & 1 & 3/2 \end{pmatrix}$$

Prohodíme sloupce a přejdeme od matice $(\mathbf{E}\,|\,\mathbf{C})$ k matici $(-\mathbf{C}^T\,|\,\mathbf{E}')$:

$$\begin{matrix} x_1, & x_2, & x_4, & x_3, & x_5 \\ \end{matrix} \begin{pmatrix} 1 & 0 & 0 & 1/2 & 33/4 \\ 0 & 1 & 0 & 1/2 & -7/4 \\ 0 & 0 & 1 & 0 & 3/2 \end{pmatrix}, \quad \begin{matrix} x_1, & x_2, & x_4, & x_3, & x_5 \\ \end{matrix} \begin{pmatrix} -1/2 & -1/2 & 0 & 1 & 0 \\ -33/4 & 7/4 & -3/2 & 0 & 1 \end{pmatrix}$$

Po zpětném prohození sloupců dostáváme v řádcích bázi množiny řešení M_0:

$$\begin{matrix} x_1, & x_2, & x_3, & x_4, & x_5 \\ \end{matrix} \begin{pmatrix} -1/2 & -1/2 & 1 & 0 & 0 \\ -33/4 & 7/4 & 0 & -3/2 & 1 \end{pmatrix}$$

Nehomogenní soustava lineárních rovnic

Terminologie: Jakékoli řešení soustavy $\mathbf{Ax} = \mathbf{b}$ nazýváme *partikulární řešení* této soustavy.

Soustava $\mathbf{Ax} = \mathbf{o}$ se nazývá *přidružená homogenní soustava* k soustavě $\mathbf{Ax} = \mathbf{b}$.

Věta: Množina M všech řešení soustavy $\mathbf{Ax} = \mathbf{b}$ je buď prázdná, nebo je tvaru

$$M = \mathbf{v} + M_0$$

kde $\mathbf{v}$ je partikulární řešení soustavy $\mathbf{Ax} = \mathbf{b}$ a M_0 je množina všech řešení přidružené homogenní soustavy $\mathbf{Ax} = \mathbf{o}$.

Důkaz: Označme $\mathbf{v}$ partikulární řešení a nechť $\mathbf{u} \in M_0$. Stačí ověřit, že $\mathbf{v}+\mathbf{u} \in M$. Dále musíme ověřit, že pro každé $\mathbf{w} \in M$ existuje $\mathbf{u} \in M_0$ tak, že $\mathbf{v} + \mathbf{u} = \mathbf{w}$.

Poznámka: Výhodná je geometrická představa, udělejte si náčrtek.

Jak vyřešit nehomogenní soustavu

- Najít jedno partikulární řešení $\mathbf{v}$.
- Vyřešit přidruženou homogenní soustavu, najít M_0.
- Všechna řešení napsat ve tvaru $M = \mathbf{v} + M_0$.

Jediný problém: najít partikulární řešení $\mathbf{v}$. Typický postup:

- Eliminovat $(\mathbf{A}\,|\,\mathbf{b}) \sim (\mathbf{C}\,|\,\mathbf{d})$, na soustavu se schodovitou maticí.
- Sloupce s volnými proměnnými odstranit (tj. dosadit za volné proměnné nuly). Vzniká soustava s regulární čtvercovou maticí.
- Dořešit tuto soustavu zpětným chodem eliminace.
- K řešení připsat nuly na místa volných proměnných.

Příklad (nehomogenní soustava)

Soustava ze slídu [8] je doplněna o pravou stranou. Gauss-Jordanovou eliminací upravím rozšířenou matici soustavy:

$$\left(\begin{array}{ccccc|c} 1 & 3 & 2 & 0 & 3 & 3 \\ 1 & 1 & 1 & -1 & 5 & -2 \\ 2 & 8 & 5 & 3 & 7 & 13 \\ 3 & 9 & 6 & 2 & 12 & 11 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 1/2 & 0 & 33/4 & -3 \\ 0 & 1 & 1/2 & 0 & -7/4 & 2 \\ 0 & 0 & 0 & 1 & 3/2 & 1 \end{array}\right)$$

Odstraním sloupce odpovídající volným proměným:

$$\begin{matrix} x_1, & x_2, & x_4 \\ \end{matrix} \left(\begin{array}{ccc|c} 1 & 0 & 0 & -3 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{array}\right)$$

Partikulární řešení je $(-3, 2, 0, 1, 0)$ a množina všech řešení je

$$M = (-3, 2, 0, 1, 0) + \langle (-1, -1, 2, 0, 0),\ (-33, 7, 0, -6, 4) \rangle.$$

Problém nejednoznačnosti zápisu řešení

Stejná množina řešení soustavy $\mathbf{Ax} = \mathbf{b}$ se dá vyjádřit různými vektory báze řešení přidružené homogenní soustavy a různými partikulárními řešeními. Jak poznat, že:

$$\overrightarrow{v} + \langle \overrightarrow{u}_1, \overrightarrow{u}_2, \ldots, \overrightarrow{u}_k \rangle \;=\; \overrightarrow{w} + \langle \overrightarrow{z}_1, \overrightarrow{z}_2, \ldots, \overrightarrow{z}_k \rangle \,?$$

Stačí porovnat hodnosti následujících matic:

$$\operatorname{hod} \begin{pmatrix} \overrightarrow{u}_1 \\ \vdots \\ \overrightarrow{u}_k \\ \overrightarrow{z}_1 \\ \vdots \\ \overrightarrow{z}_k \\ \overrightarrow{w} - \overrightarrow{v} \end{pmatrix} = \operatorname{hod} \begin{pmatrix} \overrightarrow{u}_1 \\ \vdots \\ \overrightarrow{u}_k \end{pmatrix} = \operatorname{hod} \begin{pmatrix} \overrightarrow{z}_1 \\ \vdots \\ \overrightarrow{z}_k \end{pmatrix}$$

Viz též stranu [9] k tématu „matice“.

Soustavy se čtvercovou maticí A

- Je-li matice **A regulární**, pak soustava má jediné řešení.
- Je-li matice **A regulární**, pak lze soustavu $\mathbf{A}\,\mathbf{x} = \mathbf{b}$ řešit vynásobením této rovnosti inverzní maticí $\mathbf{A}^{-1}$ zleva:

$$\mathbf{A}^{-1}\mathbf{A}\,\mathbf{x} = \mathbf{A}^{-1}\,\mathbf{b}, \quad \text{tj.} \quad \mathbf{x} = \mathbf{A}^{-1}\,\mathbf{b}.$$

- Je-li matice **A regulární**, je možné také provést LU rozklad této matice a řešit jednu soustavu dopřednou substitucí a další zpětnou substitucí. Viz stranu [3] k tématu „LU rozklad“. Je to nepatrně numericky výhodnější než počítat inverzní matici.
- Je-li matice **A regulární** a zajímají nás jen některé složky řešení, je možné použít *Cramerovo pravidlo*, viz následující stranu.
- Je-li **A singulární**, pak po eliminaci $(\mathbf{A}\,|\,\mathbf{b}) \sim (\mathbf{C}\,|\,\mathbf{d})$ dostáváme soustavu s maticí $\mathbf{C}$, která není čtvercová. Dále je nutné použít postupy uvedené na předchozích stranách.

Cramerovo pravidlo

Nechť $\mathbf{A}$ je regulární čtvercová matice. Pak pro i-tou složku řešení soustavy $\mathbf{A}\,\mathbf{x} = \mathbf{b}$ platí

$$x_i = \frac{\det \mathbf{B}_i}{\det \mathbf{A}},$$

kde matice $\mathbf{B}_i$ je shodná s maticí $\mathbf{A}$ až na i-tý sloupec, který je zaměněn za sloupec pravých stran.

Důkaz: Využijeme vztah $\mathbf{x} = \mathbf{A}^{-1} \cdot \mathbf{b}$ a zaměříme se v maticovém součinu na výpočet i-tého řádku v matici $\mathbf{x}$. Přitom matici $\mathbf{A}^{-1}$ zapíšeme pomocí doplňků. Viz stranu [19] k tématu „determinant“.

Příklad

Vyřešíme soustavu s parametrem $p \in \mathbf{R}$, která má rozšířenou matici:

$$(\mathbf{A}\,|\,\mathbf{b}) = \left(\begin{array}{ccc|c} 2 & -p & -1 & 3 \\ 1 & -7 & -5 & 0 \\ -1 & 3 & p & -1 \end{array}\right)$$

Je $\det \mathbf{A} = (p-2)(p-17)$. Takže pro $p = 17$ nebo $p = 2$ je matice soustavy singulární:

$$p = 17: \left(\begin{array}{ccc|c} 2 & -17 & -1 & 3 \\ 1 & -7 & -5 & 0 \\ -1 & 3 & 17 & -1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & -7 & -5 & 0 \\ 0 & -1 & 3 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right) \ldots M = \emptyset$$

$$p = 2: \left(\begin{array}{ccc|c} 2 & -2 & -1 & 3 \\ 1 & -7 & -5 & 0 \\ -1 & 3 & 2 & -1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & -7 & -5 & 0 \\ 0 & 4 & 3 & 1 \end{array}\right) \cdots$$

$$\ldots\ M = (5/3, 0, 1/3) + \langle (1, 3, -4) \rangle$$

Příklad (pokračování)

Pro $p \neq 17$ a $p \neq 2$ je matice soustavy regulární a soustava má jediné řešení. Najdeme toto řešení pomocí Cramerova pravidla.

$$\det\begin{pmatrix} 3 & -p & -1 \\ 0 & -7 & -5 \\ -1 & 3 & p \end{pmatrix} = -26(p-2), \quad \det\begin{pmatrix} 2 & 3 & -1 \\ 1 & 0 & -5 \\ -1 & -1 & p \end{pmatrix} = -3(p-2)$$

$$\det\begin{pmatrix} 2 & -p & 3 \\ 1 & -7 & 0 \\ -1 & 3 & -1 \end{pmatrix} = -(p-2). \quad \text{Protože } \det\mathbf{A} = (p-2)(p-17), \text{ je:}$$

$$x_1 = \frac{-26(p-2)}{(p-2)(p-17)} = \frac{26}{17-p}, \quad x_2 = \frac{3}{17-p}, \quad x_3 = \frac{1}{17-p}.$$

Pro případ $p \neq 17$ a $p \neq 2$ obsahuje množina M jediné řešení:

$$M = \left\{ \left(\frac{26}{17-p}, \frac{3}{17-p}, \frac{1}{17-p} \right) \right\}.$$

Maticová rovnice AX = B

- Je-li $\mathbf{A}$ regulární matice, pak rovnice má jediné řešení $\mathbf{X} = \mathbf{A}^{-1}\mathbf{B}$.
- Jinak stačí matice $\mathbf{X}$ a $\mathbf{B}$ rozepsat do sloupců:

  $$\mathbf{X} = (\mathbf{X}_1\ \mathbf{X}_2\ \ldots\ \mathbf{X}_k), \quad \mathbf{B} = (\mathbf{B}_1\ \mathbf{B}_2\ \ldots\ \mathbf{B}_k),$$

  takže maticová rovnice přechází na k soustav lineárních rovnic

  $$\mathbf{A}\mathbf{X}_1 = \mathbf{B}_1, \quad \mathbf{A}\mathbf{X}_2 = \mathbf{B}_2, \quad \ldots \mathbf{A}\mathbf{X}_k = \mathbf{B}_k.$$

  Tyto soustavy mají společnou matici soustavy, tj. společnou přidruženou homogenní soustavu, tj. společnou množinu M_0 všech řešení přidružené homogenní soustavy. Pro každou soustavu zvlášť je třeba spočítat partikulární řešení.
- Množina všech řešení je množna všech matic $\mathbf{X}$, které mají ve sloupcích odpovídající partikulární řešení, ke kterým je v každém sloupci (nezávisle) přičtena množina řešení M_0.

[1]

Matice lineárních zobrazení

- matice určuje zobrazení $A(x) = \mathbf{A}\mathbf{x}$
- zobrazení $A : \mathbf{R}^n \to \mathbf{R}^m$ určuje matici
- zobrazení lin. prostorů konečné dimenze mají matici vzhledem k vybraným bázím

a) algebra-all, 11, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/20010, g) Viz p. d. 4/2010

Připomenutí

Zobrazení $A : L_1 \to L_2$ je *lineární*, když

- $A(\vec{x} + \vec{y}) = A(\vec{x}) + A(\vec{y})$,
- $A(\alpha \cdot \vec{x}) = \alpha \cdot A(\vec{x})$.

Což je ekvivalentní s principem superpozice:

- $A(\alpha_1\vec{x}_1 + \cdots + \alpha_n\vec{x}_n) = \alpha_1 A(\vec{x}_1) + \cdots + \alpha_n A(\vec{x}_n)$

Je dána matice $\mathbf{A} \in \mathbf{R}^{m,n}$, pak máme zobrazení $A : \mathbf{R}^n \to \mathbf{R}^m$.

Skutečně, zobrazení $A : \mathbf{R}^n \to \mathbf{R}^m$ dané předpisem

$$A(\mathbf{x}) = \mathbf{A} \cdot \mathbf{x}$$

je lineární.

Poznámka: vektory z $\mathbf{R}^n$, $\mathbf{R}^m$ nyní považujeme za *sloupcové vektory*.

Příklad

Zobrazení $A : \mathbf{R}^4 \to \mathbf{R}^3$ je určeno maticí $\mathbf{A} \in \mathbf{R}^{3,4}$:

$$A(x_1,x_2,x_3,x_4) = \begin{pmatrix} 1 & 3 & 2 & 2 \\ 3 & 1 & 0 & 2 \\ 5 & 7 & 4 & 6 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \mathbf{A} \cdot \mathbf{x} =$$

$$= (x_1 + 3x_2 + 2x_3 + 2x_4,\ 3x_1 + x_2 + 2x_4,\ 5x_1 + 7x_2 + 4x_3 + 6x_4)^T$$

- jádro tohoto zobrazení je nulový prostor matice $\mathbf{A}$.
- hodnost zobrazení A je hodnost matice $\mathbf{A}$
- věta $\operatorname{def} A + \operatorname{hod} A = \dim L_1$ přechází na větu $\dim M_0 + \operatorname{hod}\mathbf{A} =$ počet proměnných.

Hodnost zobrazení je hodnost matice

Věta: Nechť $\mathbf{A} \in \mathbf{R}^{m,n}$. Hodnost lineárního zobrazení $A : \mathbf{R}^n \to \mathbf{R}^m$, které je dáno předpisem $A(\mathbf{x}) = \mathbf{A} \cdot \mathbf{x}$, je rovna hodnosti matice $\mathbf{A}$, tedy:

$$\operatorname{hod} A = \operatorname{hod}\mathbf{A}$$

Důkaz: hodnost zobrazení je dimenze obalu obrazů bázových vektorů, což je dimenze obalu sloupců matice, což je hodnost matice.

Lineární prostor lineárních zobrazení

- Všechna lineární zobrazení $A : L_1 \to L_2$ označím T.
- Symboly A a B na této stránce jsou prvky z T.
- Definujeme $A + B : L_1 \to L_2$ předpisem $(A+B)(x) = A(x) + B(x)$.
- Pozorování: Součet prvků z T je prvek z T.
- Definujeme $\alpha \cdot A : L_1 \to L_2$ předpisem $(\alpha \cdot A)(x) = \alpha \cdot A(x)$.
- Pozorování: α-násobek prvku z T je prvek z T.
- Uvedené operace splňují axiomy lineárního prostoru (díky tomu, že L_2 je lineární prostor), takže:
- T je lineární prostor lineárních zobrazení.

Lin. zobrazení určeno hodnotami na bázi

Věta: Jsou-li známy hodnoty lineárního zobrazení $A : L_1 \to L_2$ na konečné bázi B lin. prostoru L_1, je tím zobrazení A jednoznačně určeno na celém L_1.

Důkaz: $A(\alpha_1 \vec{b}_1 + \cdots + \alpha_n \vec{b}_n) = \alpha_1 A(\vec{b}_1) + \cdots + \alpha_n A(\vec{b}_n)$
Zobrazení souřadnic je lineární, takže takto dodefinované zobrazení A je lineární. Na bázových vektorech má předepsané hodnoty.

Jednoznačnost: Kdyby existovalo další lineární zobrazení B se stejnými hodnotami na bázi B, pak $A - B$ je lineární zobrazení s nulovými hodnotami na bázi a podle principu superpozice musí být $A - B$ nulové zobrazení všude. Takže $A = B$.

Příklad

Je dáno

$$A(1,1,2) = (1,0,1,0),\ A(1,2,2) = (2,0,2,0),\ A(2,1,5) = (1,2,2,1).$$

Protože trojice vektorů $(1,1,2)$, $(1,2,2)$, $(2,1,5)$ tvoří bázi v $\mathbf{R}^3$, existuje jediné lineární zobrazení s uvedenou vlastností. Najdeme vzorec pro $A(x_1,x_2,x_3)$:

$$\begin{aligned}
(x_1,x_2,x_3) &= \alpha(1,1,2) + \beta(1,2,2) + \gamma(2,1,5)\\
(x_1,x_2,x_3) &= (8x_1 - x_2 - 3x_3)\cdot(1,1,2) + (-3x_1 + x_2 + x_3)\cdot(1,2,2) +\\
&\quad + (x_3 - 2x_1)\cdot(2,1,5),\\
A(x_1,x_2,x_3) &= A((8x_1 - x_2 - 3x_3)(1,1,2) + (-3x_1 + x_2 + x_3)(1,2,2) +\\
&\quad + (x_3 - 2x_1)(2,1,5)) =\\
&= (8x_1 - x_2 - 3x_3)(1,0,1,0) + (-3x_1 + x_2 + x_3)(2,0,2,0) +\\
&\quad + (x_3 - 2x_1)(1,2,2,1) =\\
&= (x_2,\ -4x_1 + 2x_3,\ -2x_1 + x_2 + x_3,\ -2x_1 + x_3).
\end{aligned}$$

Každé lin. zobrazení $A : \mathbf{R}^n \to \mathbf{R}^m$ má svou matici $\mathbf{A} \in \mathbf{R}^{m,n}$

Věta: Pro každé lineární zobrazení $A : \mathbf{R}^n \to \mathbf{R}^m$ existuje jediná matice $\mathbf{A} \in \mathbf{R}^{m,n}$, pro kterou je

$$A(\mathbf{x}) = \mathbf{A} \cdot \mathbf{x}$$

Důkaz: Nechť $\mathbf{A} = (A(\mathbf{e}_1)\, A(\mathbf{e}_2)\ \ldots\ A(\mathbf{e}_n))$. Zřejmě platí $A(\mathbf{x}) = \mathbf{A} \cdot \mathbf{x}$ pro $\mathbf{x} \in \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$.
Zobrazení A i zobrazení $\mathbf{A} \cdot \mathbf{x}$ jsou lineární zobrazení, která se shodují na bázi $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$. Takže se shodují všude.

Důsledek: Vzorec pro hodnoty jakéhokoli lineárního zobrazení z $\mathbf{R}^n$ do $\mathbf{R}^m$ má vždy tvar $\mathbf{A} \cdot \mathbf{x}$.

Od zobrazení k matici

$$A : L_1 \to L_2 \quad \longleftrightarrow \quad A' : \mathbf{R}^n \to \mathbf{R}^m \quad \longleftrightarrow \quad \mathbf{A} \in \mathbf{R}^{m,n}$$

Každému lineárnímu zobrazení $A : L_1 \to L_2$ lineárních prostorů konečné dimenze přiřadíme matici takto:

- V L_1 zvolíme uspořádanou bázi (B).
- V L_2 zvolíme uspořádanou bázi (C).
- Zobrazení souřadnic $L_1 \to \mathbf{R}^n$ vzhledem k (B) označíme C_1.
- Zobrazení souřadnic $L_2 \to \mathbf{R}^m$ vzhledem k (C) označíme C_2.
- Nechť $A' = C_2 \circ A \circ C_1^{-1}$.
- Zobrazení A' je lineární a má svou matici $\mathbf{A}$.

Matice $\mathbf{A}$ se nazývá *matice zobrazení A vzhledem k bázím (B) a (C)*.

Vlastnosti matice zobrazení

$\mathbf{A}$ je matice zobrazení A vzhledem k bázím (B) a (C) právě tehdy když:

- $$\mathbf{A} \cdot \begin{pmatrix}\text{souřadnice}\\ \text{vektoru}\\ \vec{u}\\ \text{vzhledem}\\ \text{k } (B)\end{pmatrix} = \begin{pmatrix}\text{souřadnice}\\ \text{vektoru}\\ A(\vec{u})\\ \text{vzhledem}\\ \text{k } (C)\end{pmatrix}$$
- $(A(\vec{b}_1)\ A(\vec{b}_2)\ \ldots\ A(\vec{b}_n)) = (\vec{c}_1\ \vec{c}_2\ \ldots\ \vec{c}_m) \cdot \mathbf{A}$.
- $\mathbf{A}$ obsahuje v i-tém sloupci souřadnice vektoru $A(\vec{b}_i)$ vzhledem k bázi (C)

Příklad

Nechť P_3 jsou polynomy nejvýše třetího stupně. Je dáno lineární zobrazení $A : P_3 \to P_3$, které derivuje polynomy. Najdeme jeho matici vzhledem k uspořádaným bázím $(1, x, x^2, x^3)$ a $(1, x, x^2, x^3)$.

Matice má ve sloupcích souřadnice obrazů bázových vektorů, tj.

$$A(1) = 0, \quad A(x) = 1, \quad A(x^2) = 2x, \quad A(x^3) = 3x^2$$

Souřadnice těchto obrazů vzhledem k bázi $\{1, x, x^2, x^3\}$ napíšeme do sloupců matice:

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

Zkuste „derivovat“ polynomy pomocí maticového násobení…

Skládání zobrazení $\longleftrightarrow$ součin matic

Věta: Nechť lineární zobrazení A má matici $\mathbf{A}$ a lineární zobrazení B á matici $\mathbf{B}$ (vzhledem k odpovídajícím bázím). Pak složené lineární zobrazení $B \circ A$ má matici $\mathbf{B} \cdot \mathbf{A}$ (vzhledem k odpovídajícím bázím).

Poznámka: Je-li $A : L_1 \to L_2$ a $B : L_2 \to L_3$, pak „odpovídající báze“ jsou uspořádané báze (U) v L_1, (V) v L_2 a (W) v L_3. V uvedené větě se pak pracuje s maticí $\mathbf{A}$ vzhledem k (U), (V), s maticí $\mathbf{B}$ vzhledem k (V), (W) a s maticí $\mathbf{B} \cdot \mathbf{A}$ vzhledem k (U), (W).

Důkaz věty se opírá o rovnost

$$\mathbf{B}\cdot\mathbf{A}\cdot\begin{pmatrix}\text{souřadnice}\\ \text{vektoru}\\ \vec{u}\\ \text{vzhledem}\\ \text{k } (U)\end{pmatrix} = \mathbf{B}\cdot\begin{pmatrix}\text{souřadnice}\\ \text{vektoru}\\ A(\vec{u})\\ \text{vzhledem}\\ \text{k } (V)\end{pmatrix} = \begin{pmatrix}\text{souřadnice}\\ \text{vektoru}\\ B(A(\vec{u}))\\ \text{vzhledem}\\ \text{k } (W)\end{pmatrix}.$$

Příklad

Matice

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

je matice derivace vzhledem k uspořádaným bázím $(1, x, x^2, x^3)$ a $(1, x, x^2, x^3)$. Podle věty o složeném zobrazení je $\mathbf{A}^2$ matice druhé derivace a $\mathbf{A}^3$ matice třetí derivace.

Zobrazení $A : L \to L$

Definice: Zobrazení do stejné množiny se nazývá *transformace*. Lineární zobrazení do stejného lineárního prostoru se nazývá *lineární transformace*.

Matice transformace $A : L \to L$ *vzhledem k bázi* (B) je matice lineárního zobrazení A vzhledem k bázím (B) a (B).

Příklady

- $\mathbf{A} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ je matice *projekce*.
- $\mathbf{A} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ je matice *rotace*.
- $\mathbf{A} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ je (pro $a \neq 0$, $b \neq 0$) matice *změny měřítka*.
- Další transformace vznikají skládáním těchto elementárních transformací, jejich matice jsou pak součinem těchto elementárních matic.

Příklad

Nechť osa o prochází počátkem a svírá s osou x úhel α. Najdeme matici osové soměrnosti podle osy o..

Osová souměrnost vzniká jako složení následujících zobrazení:

- otočení o úhel $-\alpha$,
- zrcadlení, tj. změna měřítka s parametry 1, –1,
- otočení zpět o úhel α.

Matici tohoto složeného zobrazení spočítáme jako součin matic uvedených zobrazení zapsaných „zprava doleva“:

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix} =$$
$$= \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}$$

Nestandardní báze, příklad

Najdeme matici zobrazení $A : \mathbf{R}^3 \to \mathbf{R}^4$, které je dané předpisem

$$A(x_1, x_2, x_3) = (x_2,\ -4x_1 + 2x_3,\ -2x_1 + x_2 + x_3,\ -2x_1 + x_3),$$

vzhledem k bázím $(B) = ((1,1,2),(1,2,2),(2,1,5))$ a (S_4)

Protože $A(1,1,2) = (1,0,1,0)$, $A(1,2,2) = (2,0,2,0)$, $A(2,1,5) = (1,2,2,1)$, a protože složky těchto obrazů jsou rovny souřadnicím vzhledem ke standardní bázi (S_4), stačí složky těchto obrazů napsat do sloupců hledané matice:

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

Pokud bychom měli hledat matici zobrazení $A : L_1 \to L_2$ vzhledem k nestandardní bázi v L_2, budeme mít více problémů...

Hodnost matice je hodnost zobrazení

- Tuto skutečnost jsme zatím dokázali pro speciální zobrazení tvaru $\mathbf{A} \cdot \mathbf{x}$.
- Pro obecné lineární zobrazení $A : L_1 \to L_2$ také platí

$$\operatorname{hod} A = \operatorname{hod} \mathbf{A},$$

protože $\operatorname{hod} A = \operatorname{hod} A'$, kde $A' = C_2 \circ A \circ C_1^{-1}$. Platí:

$$\begin{aligned} \operatorname{hod} A &= \dim A(L_1) = \dim A(\langle \vec{b}_1, \vec{b}_2, \dots, \vec{b}_n \rangle) = \\ &= \dim \langle A(\vec{b}_1), A(\vec{b}_2), \dots, A(\vec{b}_n) \rangle = \\ &= \dim \langle C_2^{-1} \circ A' \circ C_1(\vec{b}_1),\ \dots,\ C_2^{-1} \circ A' \circ C_1(\vec{b}_n) \rangle = \\ &= \dim\ C_2^{-1}(\langle A'(\vec{e}_1), A'(\vec{e}_2), \dots, A'(\vec{e}_n) \rangle) = \\ &= \dim \langle A'(\vec{e}_1), A'(\vec{e}_2), \dots, A'(\vec{e}_n) \rangle = \\ &= \dim A'(\langle \vec{e}_1, \vec{e}_2, \dots, \vec{e}_n \rangle) = \dim A'(\mathbf{R}^n) = \operatorname{hod} A' \end{aligned}$$

Uvedené rovnosti platí, protože C_1 a C_2 jsou izomorfismy.

Transformace je prostá právě když má regulární matici

Nechť L má konečnou dimenzi, $\dim L = n$.

Věta: Lineární transformace $A : L \to L$ je prostá právě když:

- je na
- má regulární matici

Důkaz: A je prostá právě když $\operatorname{def} A = 0$.

Protože $\operatorname{def} A + \operatorname{hod} A = \dim L$, je $\operatorname{def} A = 0$ právě když $\operatorname{hod} A = n$. To platí právě když $A(L) = L$, tj. A je na L.

Uvedené vlastnosti jsou splněny právě když $\operatorname{hod} \mathbf{A} = n$, kde $\mathbf{A}$ je matice zobrazení A, tj. právě když $\mathbf{A}$ je regulární.

Prostor lineárních zobrazení je izomrofní s lineárním prostorem matic

- Každému zobrazení $A : L_1 \to L_2$ (kde $\dim L_1 = n$, $\dim L_2 = m$) je jednoznačně přiřazena matice $\mathbf{A} \in \mathbf{R}^{m,n}$ vzhledem k bázím (B) a (C).
- Toto přiřazení je zobrazení prosté a na.
- Toto přiřazení je dokonce lineární zobrazení. Stačí ověřit, že součet dvou zobrazení A a B s maticemi $\mathbf{A}$ a $\mathbf{B}$ (vzhledem ke zvoleným bázím) má matici $\mathbf{A} + \mathbf{B}$. Dále je třeba ověřit, že α násobek lineárního zobrazení má matici, která je rovna α násobku původní matice.
- Mám na mysli zobrazení a píšu jeho matici. Mám na mysli matici a vnímám ji jako zobrazení. Je to jedno.

Změna báze

- matice přechodu od báze k bázi
- jak se změní souřadnice vektoru při změně báze?
- jak se změní matice lineárního zobrazení při změně báze?
- jak se změní matice transformace při změně báze?

Matice přechodu

Definice: Nechť $(B) = (\overrightarrow{b}_1, \overrightarrow{b}_2, \dots, \overrightarrow{b}_n)$ a $(C) = (\overrightarrow{c}_1, \overrightarrow{c}_2, \dots, \overrightarrow{c}_n)$ jsou dvě báze stejného lineárního prostoru L. Pak existuje jediná lineární transformace $A : L \to L$, pro kterou je

$$A(\overrightarrow{b}_i) = \overrightarrow{c}_i, \quad \forall i \in \{1, 2, \dots, n\}$$

Matice této lineární transformace vzhledem k bázi (B) se nazývá *matice přechodu od báze (B) k bázi (C)*.

- Značení: $\mathbf{P}_{B\to C}$ je matice přechodu od (B) k (C).

Vlastnosti matice přechodu

- $\mathbf{P}_{B\to C}$ má v i-tém sloupci souřadnice vektoru $\overrightarrow{c}_i$ vzhledem k bázi (B).
- $(\overrightarrow{c}_1\ \overrightarrow{c}_2\ \dots\ \overrightarrow{c}_n) = (\overrightarrow{b}_1\ \overrightarrow{b}_2\ \dots\ \overrightarrow{b}_n) \cdot \mathbf{P}_{B\to C}$,
- $\mathbf{P}_{B\to C}$ je matice identity vzhledem k bázím (C) a (B)
- Pro každý vektor $\overrightarrow{u} \in L$ je

$$\mathbf{P}_{B\to C} \cdot \begin{pmatrix} \text{souřadnice} \\ \text{vektoru} \\ \overrightarrow{u} \\ \text{vzhledem} \\ \text{k } (C) \end{pmatrix} = \begin{pmatrix} \text{souřadnice} \\ \text{vektoru} \\ \overrightarrow{u} \\ \text{vzhledem} \\ \text{k } (B) \end{pmatrix}.$$

Pozor, je to opačně, než by odpovídalo názvu matice přechodu!

Matice přechodu je regulární

Platí:

- $\mathbf{P}_{B\to C}$ je regulární.
- $\mathbf{P}_{B\to C} \cdot \mathbf{P}_{C\to D} = \mathbf{P}_{B\to D}$
- $(\mathbf{P}_{B\to C})^{-1} = \mathbf{P}_{C\to B}$

Důkaz: Protože má matice $\mathbf{P}_{B\to C}$ lin. nezávislé sloupce, je regulární. Součin matic přechodu vyplývá z věty o matici složeného zobrazení. Je potřeba v tomto případě skládat identické zobrazení a jeho matice vzhledem k různým bázím. Konečně třetí puntík je důsledkem druhého.

Příklad

Jsou dány $(S) = (1, x, x^2)$ a $(C) = (x^2 + x,\ x - 1,\ x + 2)$, dvě báze lineárního prostoru všech polynomů nejvýše druhého stupně. Najdeme matici přechodu $\mathbf{P}_{S\to C}$. Ta obsahuje ve sloupcích souřadnice bázových prvků $\overrightarrow{c}_i$ vzhledem k bázi (S), tedy

$$\mathbf{P}_{S\to C} = \begin{pmatrix} 0 & -1 & 2 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Jsou-li (α, β, γ) souřadnice polynomu p vzhledem k (C), pak

$$\begin{pmatrix} 0 & -1 & 2 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} -\beta + 2\gamma \\ \alpha + \beta + \gamma \\ \alpha \end{pmatrix}$$

jsou souřadnice téhož polynomu vzhledem k bázi (S), neboli

$$p(x) = \alpha x^2 + (\alpha + \beta + \gamma)x - \beta + 2\gamma.$$

Algoritmus pro sestavení matice přechodu

- Matici přechodu $\mathbf{P}_{S\to B}$ od standardní báze (S) k bázi (B) sestavíme snadno: do sloupců zapíšeme souřadnice vektorů $\overrightarrow{b}_i$ vzhledem k bázi (S).
- Platí: $\mathbf{P}_{B\to C} = \mathbf{P}_{B\to S} \cdot \mathbf{P}_{S\to C} = (\mathbf{P}_{S\to B})^{-1} \cdot \mathbf{P}_{S\to C}$.
- Protože $(\mathbf{A}\,|\,\mathbf{B}) \sim (\mathbf{E}\,|\,\mathbf{A}^{-1}\mathbf{B})$, stačí napsat následující dvoublokovou matici a eliminovat:

$$(\mathbf{P}_{S\to B}\,|\,\mathbf{P}_{S\to C}) \sim (\mathbf{E}\,|\,\mathbf{P}_{S\to B}^{-1} \cdot \mathbf{P}_{S\to C}) = (\mathbf{E}\,|\,\mathbf{P}_{B\to C}).$$

V pravém bloku po eliminaci najdeme hledanou matici $\mathbf{P}_{B\to C}$

Příklad

Jsou dány báze $(B) = (x^2 + 1, x^2 + 2, x + 3)$ a $(C) = (x^2 + x,\ x - 1,\ x + 2)$ lineárního prostoru polynomů nejvýše druhého stupně. Najdeme matici přechodu $\mathbf{P}_{B\to C}$.

Zvolme bázi, vzhledem ke které se souřadnice dobře hledají, například $(S) = (1, x, x^2)$. Podle algoritmu z předchozí stránky sestavíme $(\mathbf{P}_{S\to B}\,|\,\mathbf{P}_{S\to C})$ a eliminujeme na tvar $(\mathbf{E}\ |\ \mathbf{P}_{B\to C})$.

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

V pravém bloku po eliminaci máme matici $\mathbf{P}_{B\to C}$. Známe-li souřadnice polynomu vzhledem k (C), pak násobením maticí $\mathbf{P}_{B\to C}$ získáme souřadnice polynomu vzhledem k (B). Kdybychom potřebovali ze souřadnice vzhledem k (B) spočítat souřadnice vzhledem k (C), použijeme inverzní matici $(\mathbf{P}_{B\to C})^{-1} = \mathbf{P}_{B\to C}$.

Změna matice zobrazení při změně báze

Nechť $\mathbf{A}$ je matice zobrazení $A : L_1 \to L_2$ vzhledem k bázím (B) a (C). Nechť $\mathbf{A}'$ je matice téhož zobrazení, ovšem vzhledem k bázím (B') a (C'). Pak

$$\mathbf{P}_{C'\to C} \cdot \mathbf{A} \cdot \mathbf{P}_{B\to B'} = \mathbf{A}'$$

Náčrt důkazu:

$$\mathbf{P}_{C'\to C} \cdot \mathbf{A} \cdot \mathbf{P}_{B\to B'} \cdot \begin{pmatrix} \text{souřadnice} \\ \overrightarrow{u} \\ \text{vzhledem} \\ \text{k } (B') \end{pmatrix} = \mathbf{P}_{C'\to C} \cdot \mathbf{A} \cdot \begin{pmatrix} \text{souřadnice} \\ \overrightarrow{u} \\ \text{vzhledem} \\ \text{k } (B) \end{pmatrix} =$$

$$= \mathbf{P}_{C'\to C} \cdot \begin{pmatrix} \text{souřadnice} \\ \overrightarrow{A}(u) \\ \text{vzhledem} \\ \text{k } (C) \end{pmatrix} = \begin{pmatrix} \text{souřadnice} \\ \overrightarrow{A}(u) \\ \text{vzhledem} \\ \text{k } (C') \end{pmatrix}$$

Důsledky věty o změně matice

Nechť $\mathbf{A}$ je matice zobrazení $A : L_1 \to L_2$ vzhledem k bázím (B) a (C). Pak

- $\mathbf{P}_{C'\to C} \cdot \mathbf{A}$ je matice zobrazení A vzhledem k bázím (B) a (C').
- $\mathbf{A} \cdot \mathbf{P}_{B\to B'}$ je matice zobrazení A vzhledem k bázím (B') a (C).

Nechť $\mathbf{A}$ je matice transformace $A : L \to L$ vzhledem k bázi (B). Pak

- $\mathbf{P}_{B'\to B} \cdot \mathbf{A} \cdot \mathbf{P}_{B\to B'}$ je matice transformace A vzhledem k bázi (B'), neboli:
- $(\mathbf{P}_{B\to B'})^{-1} \cdot \mathbf{A} \cdot \mathbf{P}_{B\to B'}$ je matice transformace A vzhledem k (B').

Příklad

Nechť $A(x_1,x_2,x_3) = (x_1+x_2, x_2+x_3, x_3+x_1)$. Najdeme matici této transformace ke standardní bázi (S). Dále najdeme matici této transformace vzhledem k bázi $(B) = ((2,2,2),(3,3,0),(4,0,0))$.

$$\mathbf{A}_S = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad \mathbf{P}_{S\to B} = \begin{pmatrix} 2 & 3 & 4 \\ 2 & 3 & 0 \\ 2 & 0 & 0 \end{pmatrix}.$$

Matice $\mathbf{A}_B$ transformace A vzhledem k bázi (B) spočítáme takto:

$$\mathbf{A}_B \;=\; \mathbf{P}_{B\to S}\cdot\mathbf{A}_S\cdot\mathbf{P}_{S\to B} \;=\; (\mathbf{P}_{S\to B})^{-1}\cdot\mathbf{A}_S\cdot\mathbf{P}_{S\to B} = \begin{pmatrix} 2 & \frac{3}{2} & 2 \\ 0 & 0 & -\frac{4}{3} \\ 0 & \frac{3}{4} & 1 \end{pmatrix}$$

Algoritmus: sestavení matice zobrazení vzhledem k libovolným bázím

Je dáno lineární zobrazení $A : L_1 \to L_2$. Najdeme matici tohoto zobrazení vzhledem k bázím (B) a (C).

Nechť (S) je báze L_2, vzhledem ke které se souřadnice dobře hledají. Sestavíme matici $(\mathbf{P}_{S\to C}\,|\,\mathbf{A}_{B,S})$, ve které $\mathbf{A}_{B,S}$ značí matici zobrazení A vzhledem k bázím (B), (S). Eliminujeme na tvar $(\mathbf{E}\mid\mathbf{X})$. Pak $\mathbf{X}$ je hledaná matice zobrazení A vzhledem k bázím (B) a (C).

Proč? Je $(\mathbf{P}_{S\to C}\mid\mathbf{A}_{B,S}) \sim (\mathbf{E}\mid\mathbf{P}_{C\to S}\cdot\mathbf{A}_{B,S})$.
Přitom $\mathbf{P}_{C\to S}\cdot\mathbf{A}_{B,S}$ je maticí zobrazení $\mathbf{A}$ vzhledem k (B) a (C).

Poznámka: matice $\mathbf{P}_{S\to C}$ a $\mathbf{A}_{B,S}$ lze sestavit snadno.

Příklad

Je dáno zobrazení $A : P_3 \to P_2$, které derivuje polynomy nejvýše třetího stupně. Najdeme matici tohoto zobrazení vzhledem k:

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

Zvolím $(S) = (x^2, x, 1)$. To je báze, vzhledem ke které se souřadnice polynomů z P_2 dobře hledají. Je:

$A(x^3+x+2) = 3x^2+1$, $A(x^2+2x+3) = 2x+2$, $A(x^2+2) = 2x$, $A(x-1) = 1$

Sestavím matici $(\mathbf{P}_{S\to C}\,|\,\mathbf{A}_{B,S})$ a eliminuji:

$$\left(\begin{array}{ccc|cccc} 1 & 1 & 0 & 3 & 0 & 0 & 0 \\ -1 & -1 & 1 & 0 & 2 & 2 & 0 \\ 1 & -1 & 4 & 1 & 2 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cccc} & -4 & -3 & -4 & \frac{1}{2} \\ \mathbf{E} & 7 & 3 & 4 & -\frac{1}{2} \\ & 3 & 2 & 2 & 0 \end{array}\right)$$

Hledaná matice je v pravém bloku po eliminaci.

Příklad

Je dána matice $\mathbf{A}'$ zobrazení vzhledem k bázím (B) a (S_2). Hledáme matici $\mathbf{A}$ zobrazení vzhledem k bázím (S_1) a (S_2).

Jinými slovy: známe zobrazení A na bázi (B) a hledáme vzorec, který udává hodnotu tohoto zobrazení v libovolném bodě. Například je známo

$A(1,1,2) = (1,0,1,0)$, $A(1,2,2) = (2,0,2,0)$, $A(2,1,5) = (1,2,2,1)$.

Řešení. Podle strany [9] je $\mathbf{A} = \mathbf{A}'\cdot\mathbf{P}_{B\to S_1} = \mathbf{A}'\cdot(\mathbf{P}_{S_1\to B})^{-1}$. Matici přechodu $\mathbf{P}_{S_1\to B}$ sestavíme snadno. Jde tedy o to ji invertovat a násobit zprava s danou maticí $\mathbf{A}'$.

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 2 \\ 1 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & 1 \\ 2 & 2 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ -4 & 0 & 2 \\ -2 & 1 & 1 \\ -2 & 0 & 1 \end{pmatrix}$$

Příklad

Nechť osa o prochází počátkem a svírá s osou x úhel α. Najdeme matici osové souměrnosti podle osy o.

Zvolíme bázi (B) tak, aby vektor $\overrightarrow{b}_1$ ležel v ose o a $\overrightarrow{b}_2$ byl na ní kolmý. Vzhledem k této bázi je matice osové souměrnosti rovna

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Nyní provedeme přechod od báze (B) k bázi (S). Matice osové souměrnosti vzhledem k (S) je

$$\mathbf{P}_{S\to B}\cdot\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\cdot\mathbf{P}_{B\to S},$$

$$\mathbf{P}_{S\to B} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}, \quad \mathbf{P}_{S\to B} = \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix},$$

Srovnejte tento příklad se stranou 17 kapitoly „matice zobrazení“.

Příklad

Nechť $A : L \to L$ je lineární transformace, která zobrazí bázi (B) na bázi (C). Víme, že matice přechodu $\mathbf{P}_{B\to C}$ je rovna matici této transformace A vzhledem k bázi (B). Jak vypadá matice stejné transformace vzhledem k bázi (C)?

Řešení: Označme matici zobrazení A vzhledem k (B) symbolem $\mathbf{A}_B$ a hledanou matici označme $\mathbf{A}_C$. Je $\mathbf{A}_B = \mathbf{P}_{B\to C}$. Podle důsledku ze strany [9] je

$$\mathbf{A}_C = (\mathbf{P}_{B\to C})^{-1}\cdot\mathbf{A}_B\cdot\mathbf{P}_{B\to c} = (\mathbf{P}_{B\to C})^{-1}\cdot\mathbf{P}_{B\to c}\cdot\mathbf{P}_{B\to c} = \mathbf{P}_{B\to c}$$

Ejhle, matice transformace A vzhledem k bázi (C) je *stejná*, jako matice této transformace vzhledem k bázi (B) a je to matice přechodu od (B) k (C).

Afinní transformace

- je posunutí plus lineární transformace
- má svou matici vzhledem k homogenním souřadnicím
- využití například v počítačové grafice

a) algebra-all, 13, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) Viz p. d. 4/2010

Idea afinního prostoru

- Lineární prostor V volných vektorů: dvě orientované úsečky reprezentují stejný volný vektor, pokud jsou rovnoběžné, stejně velké a stejně orientované.
- Sčítání a násobení konstantou v lineárním prostoru V provedeme pomocí vhodně zvolených reprezentatnů stejně jako v U_O.
- Kromě vektorů z V budeme v afinním prostoru pracovat s množinou bodů $\mathbf{X}$. Nové operace:
- bod1 + vektor = bod2. Na bod1 navážeme reprezentanta vektoru a koncový bod tohoto vektoru je výsledek operace.
- bod1 – bod2 = vektor. Výsledkem je vektor s reprezentantem, který má počáteční bod2 a koncový bod1.

Definice afinního prostoru

Definice: Nechť V je lineární prostor a $\mathbf{X}$ je libovolná množina. Dvojici množin $(\mathbf{X}, V)$ nazýváme *afinní prostor*, pokud kromě operací + a · na V je definována operace $+ : \mathbf{X} \times V \to \mathbf{X}$ s vlastnostmi:

(1) $P + \vec{o} = P \qquad \forall\, P \in \mathbf{X}$ ($\vec{o} \in V$ je nulový vektor),
(2) $(P + \vec{u}) + \vec{v} = P + (\vec{u} + \vec{v}) \qquad \forall\, P \in \mathbf{X},\ \vec{u} \in V,\ \vec{v} \in V,$
(3) $\forall\, P \in \mathbf{X}, Q \in \mathbf{X}$ existuje jediný $\vec{u} \in V$ tak, že $P = Q + \vec{u}$

Vektor $\vec{u}$ z vlastnosti (3) značíme $P - Q$ nebo $\overrightarrow{QP}$.

Množina $\mathbf{X}$ a lineární prostor V mohou být jakékoli takové, aby šlo definovat operaci + s uvedenými vlastnostmi.

Dobrá a postačující představa afinního prostoru je lineární prostor V volných vektorů a množina $\mathbf{X}$ bodů.

Souřadnicový systém afinního prostoru

Dimenze afinního prostoru je dimenze lineárního prostoru V.

Nadále budeme předpokládat afinní prostory s konečnou dimenzí (zejména s dimenzí 3 nebo 2).

Zvolme bázi (B) prostoru V a dále bod $O \in \mathbf{X}$. Dvojici (O, B) nazýváme souřadnicovým systémem afinního prostoru.

Vektor $\vec{u} \in V$ má souřadnice vzhledem k (O, B) definovány jako jeho souřadnice vzhledem k bázi (B).

Bod $P \in \mathbf{X}$ má souřadnice vzhledem k (O, B) definovány jako souřadnice vektoru $\overrightarrow{OP}$. Tomuto vektoru říkáme *radiusvektor bodu P*.

Vlastnosti souřadnic v afinním prostoru

Nechť C je zobrazení souřadnic, $\vec{u}, \vec{v} \in V, P, Q \in \mathbf{X}, \alpha \in \mathbf{R}$. Pak

(1) $C(\vec{u} + \vec{v}) = C(\vec{u}) + C(\vec{v})$
(2) $C(\alpha \cdot \vec{u}) = \alpha \cdot C(\vec{u})$
(3) $C(Q + \vec{u}) = C(Q) + C(\vec{u})$
(4) $C(P - Q) = C(P) - C(Q)$

Důkaz: (1) a (2): jsou to obvyklé souřadnice vektoru. (3), (4): stačí souřadnice bodů vyjádřit jako souřadnice jejich radiusvektorů.

Homogenní souřadnice

Nechť má afinní prostor dimenzi n.

Homogenní souřadnice vektoru v souřadnicovém systému (O, B) je uspořádaná $(n+1)$-tice; prvních n složek obsahuje souřadnice vektoru, poslední složka obsahuje nulu.

Homogenní souřadnice bodu v souřadnicovému systému (O, B) je uspořádaná $(n+1)$-tice; prvních n složek obsahuje souřadnice bodu, poslední složka obsahuje jedničku.

Pozorování: Tvrzení z předchozí strany [5] o souřadnicích platí i v případě, že C značí homogenní souřadnice.

Matice v homogenních souřadnicích

Zobrazení $A : \mathbf{X} \to \mathbf{X}$, pro které existuje matice $\mathbf{A} \in \mathbf{R}^{n+1,n+1}$ s vlastností:

$$\mathbf{A} \cdot \begin{pmatrix} \text{homogenní} \\ \text{souřadnice} \\ \text{bodu } P \\ \text{vzhledem} \\ \text{k } (O,B) \end{pmatrix} = \begin{pmatrix} \text{homogenní} \\ \text{souřadnice} \\ \text{bodu } A(P) \\ \text{vzhledem} \\ \text{k } (O,B) \end{pmatrix}$$

se nazývá transformace s maticí $\mathbf{A}$ v homogenních souřadnicích.

Pozorování: Matice $\mathbf{A}$ musí být tvaru:

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}' & \mathbf{t} \\ \mathbf{o} & 1 \end{pmatrix}$$

kde $\mathbf{A}' \in \mathbf{R}^{n,n}$, $\mathbf{t} \in \mathbf{R}^{n,1}$, $\mathbf{o} \in \mathbf{R}^{1,n}$ je nulový vektor.

Vlastnosti matice v homogenních souřadnicích

$$\begin{pmatrix} \mathbf{A}' & \mathbf{t} \\ \mathbf{o} & 1 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{p} \\ 1 \end{pmatrix} = \begin{pmatrix} \mathbf{A}' \cdot \mathbf{p} + \mathbf{t} \\ 1 \end{pmatrix}$$

tj. bod je transformován lineární transformací s maticí $\mathbf{A}'$ a následně posunut o $\mathbf{t}$.

$$\begin{pmatrix} \mathbf{A}' & \mathbf{t} \\ \mathbf{o} & 1 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{u} \\ 0 \end{pmatrix} = \begin{pmatrix} \mathbf{A}' \cdot \mathbf{u} \\ 0 \end{pmatrix}$$

tj. vektor je pouze transformován lineární transformací s maticí $\mathbf{A}'$.

Příklad 2D

Obecná matice transformace v homogenních souřadnicích má tvar:

$$\begin{pmatrix} a & b & c \\ d & e & f \\ 0 & 0 & 1 \end{pmatrix}.$$

Je tedy určena šesti parametry.

Bod se souřadnicemi (x, y) přejde při transformaci s touto maticí na bod se souřadnicemi (x', y'):

$$\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} ax + by + c \\ dx + ey + f \\ 1 \end{pmatrix},$$

takže bod se transformuje lineárně a posune o vektor (c, f).

Příklad 3D

Obecná matice transformace v homogenních souřadnicích má tvar:

$$\begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Je určena dvanácti parametry.

Transformace bodu probíhá podle následujícího vzorce:

$$\begin{pmatrix} x' \\ y' \\ z' \\ 1 \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \\ 1 \end{pmatrix} = \begin{pmatrix} ax + by + cz + d \\ ex + fy + gz + h \\ ix + jy + kz + l \\ 1 \end{pmatrix}$$

Skládání transformací — součin matic

Věta: Nechť $\mathbf{A}$ a $\mathbf{B}$ jsou matice transformací A a B v homogenních souřadnicích

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}' & \mathbf{t} \\ \mathbf{o} & 1 \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} \mathbf{B}' & \mathbf{s} \\ \mathbf{o} & 1 \end{pmatrix}$$

Pak složená transformace $B \circ A$ má matici:

$$\mathbf{B} \cdot \mathbf{A} = \begin{pmatrix} \mathbf{B}' & \mathbf{s} \\ \mathbf{o} & 1 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{A}' & \mathbf{t} \\ \mathbf{o} & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{B}' \cdot \mathbf{A}' & \mathbf{B}' \cdot \mathbf{t} + \mathbf{s} \\ \mathbf{o} & 1 \end{pmatrix}.$$

Poznámka: Je $(B \circ A)(x) = (B(A(x))$.

Důkaz věty se provede analogicky, jako důkaz věty o složeném lineárním zobrazení.

Inverzní transformace — inverzní matice

Věta: Má-li transformace A regulární matici $\mathbf{A}$ v homogenních souřadnicích, pak je prostá a na a A^{-1} má matici $\mathbf{A}^{-1}$ v homogenních souřadnicích.

Pozorování:

$$\text{Je-li} \quad \mathbf{A} = \begin{pmatrix} \mathbf{A}' & \mathbf{t} \\ \mathbf{o} & 1 \end{pmatrix}, \quad \text{pak} \quad \mathbf{A}^{-1} = \begin{pmatrix} (\mathbf{A}')^{-1} & -(\mathbf{A}')^{-1}\mathbf{t} \\ \mathbf{o} & 1 \end{pmatrix}$$

Inverzní matice k $\mathbf{A}$ existuje, právě když $\mathbf{A}'$ je regulární.

Příklad: elementární transformace ve 2D

Změna měřítka má matici v homogenních souřadnicích:

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Rotace o úhel α má matici v homogenních souřadnicích:

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

Posunutí o vektor se souřadnicemi (t_x, t_y) má matici v homogenních souřadnicích:

$$\begin{pmatrix} 1 & 0 & t_x \\ 0 & 1 & t_y \\ 0 & 0 & 1 \end{pmatrix}$$

Další transformace vznikají skládáním těchto transformací.

Příklad

Najdeme matici (v homogenních souřadnicích) rotace o úhlel α kolem bodu $(2,3)$.

Uvedená transformace je složením následujících transformací:

- posunutí o vektor $(-2,3)$,
- rotace o úhel α,
- posunutí o vektor $(2,3)$.

Matice výsledné transformace je součinem matic:

$$\big(\text{posunutí o } (2,3)\big) \cdot \big(\text{rotace o úhel } \alpha\big) \cdot \big(\text{posunutí o } (-2,-3)\big) =$$

$$= \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{pmatrix} = \cdots$$

Příklad, pokračování

$$\cdots = \begin{pmatrix} \cos\alpha & -\sin\alpha & -2\cos\alpha + 3\sin\alpha + 2 \\ \sin\alpha & \cos\alpha & -2\sin\alpha - 3\cos\alpha + 3 \\ 0 & 0 & 1 \end{pmatrix}.$$

Takže bod o souřadnicích (x,y) přechází po této transformaci na bod o souřadnicích $(x'y')$, pro který platí:

$$\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha & -2\cos\alpha + 3\sin\alpha + 2 \\ \sin\alpha & \cos\alpha & -2\sin\alpha - 3\cos\alpha + 3 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} =$$

$$= \begin{pmatrix} (\cos\alpha)x - (\sin\alpha)y - 2\cos\alpha + 3\sin\alpha + 2 \\ (\sin\alpha)x + (\cos\alpha)y - 2\sin\alpha - 3\cos\alpha + 3 \\ 1 \end{pmatrix}$$

Afinní transformace

Definice: Nechť $(\mathbf{X}, V)$ je afinní prostor. Transformace $A : \mathbf{X} \to \mathbf{X}$ se nazývá *afinní*, pokud existuje lineární transformace $A' : V \to V$ tak, že

$$A(P + \vec{u}) = A(P) + A'(\vec{u}) \qquad \forall\, P \in \mathbf{X}, \vec{u} \in V.$$

Zvolme bod $O \in \mathbf{X}$. Protože pro každý $P \in \mathbf{X}$ platí $P = O + \overrightarrow{OP}$, je $A(P) = A(O) + A'(\overrightarrow{OP})$, takže každá afinní transformace je jednoznačně určena hodnotou $A(O)$ a lineární transformací $A' : V \to V$.

Protože každá lineární transformace $A' : V \to V$ je jednoznačně určena hodnotami na bázi $(B) = (\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n)$, je každá afinní transformace jednoznačně určena hodnotami v $n+1$ bodech:

$$O, \quad O + \vec{b}_1, \quad O + \vec{b}_2, \quad \ldots, \quad O + \vec{b}_n.$$

Matice afinní transformace

je její matice v homogenních souřadnicích. Je třeba ukázat:

- Každá transformace, která má matici v homogenních souřadnicích, je afinní.
- Každá afinní transformace má matici v homog. souřadnicích.

Puntík první: Je dána matice $\mathbf{A}$ nějaké transformace v homogenních souřadnicích vzhledem k (O,B). Matice hledaného zobrazení A' je také matice $\mathbf{A}$. Jsou-li $\mathbf{p}$ souřadnice bodu $P \in \mathbf{X}$ a $\mathbf{u}$ souřadnice vektoru $\vec{u} \in V$, pak

$$\mathbf{A} \cdot \begin{pmatrix} \mathbf{p} + \mathbf{u} \\ 1 \end{pmatrix} = \mathbf{A} \cdot \begin{pmatrix} \mathbf{p} \\ 1 \end{pmatrix} + \mathbf{A} \cdot \begin{pmatrix} \mathbf{u} \\ 0 \end{pmatrix}.$$

Puntík druhý: Hledaná matice obsahuje ve sloupcích homogenní souřadnice obrazů báze následované homogenními souřadicemi obrazu bodu O. Taková matice určuje hodnoty afinní transformace na bodech $O, O+\vec{b}_i$, takže určuje afinní transformaci jednoznačně.

Vlastnosti afinní transformace

- Skládání afinních transformací je afinní transformace
- Afinní transformace je prostá právě když je na právě když má regulární matici v homogenních souřadnicích.
- Je-li afiní transformace prostá, pak její inverze je také afiní transformace.
- Prostá afinní transformace zobrazuje rovnoběžné přímky na rovnoběžné přímky.

Příklad

Je dána afinní tansformace ve 2D prostoru taková, že posune počátek souřadnicového systému do bodu $(3,2)$ a transformuje první bázový vektor na vektor se souřadnicemi $(-1,2)$, druhý bázový vektor transformuje na vektor se souřadnicemi $(4,1)$.

Najdeme matici v homogenních souřadnicích této transformace.

Podle předchozího matice obsahuje homogenní souřadnice obrazů báze a v posledním sloupci homogenní souřadnice obrazu počátku. Tedy

$$\mathbf{A} = \begin{pmatrix} -1 & 4 & 3 \\ 2 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Pronásobíme-li pixelové souřadnice každého pixelu touto maticí, dostáváme pixelové souřadnice obazu: maticovým násobením můžeme tansformovat dvourozměrný obrázek.

Vlastní číslo, vektor

- motivace: směr přímky, kterou lin. transformace nezmění
- invariantní podprostory
- charakteristický polynom
- báze, vzhledem ke které je matice transformace nejjednodušší
- podobnost s diagonální maticí

a) algebra-all, 14, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) Viz p. d. 4/2010

Motivace

Je dána transformace $A : \mathbf{R}^2 \to \mathbf{R}^2$. Najdeme takovou přímku p procházející počátkem, aby $A(p) = p$.

$$p = \{t\,\overrightarrow{u};\, t \in \mathbf{R}\}, \qquad A(p) = \{A(t\,\overrightarrow{u});\, t \in \mathbf{R}\} = \{t\,A(\overrightarrow{u});\, t \in \mathbf{R}\}$$

Musí tedy existovat $\lambda \in \mathbf{R}$ tak, aby $A(\overrightarrow{u}) = \lambda\,\overrightarrow{u}$. Přitom $\overrightarrow{u}$ musí být nenulový vektor.

Zvolme v R^2 nějakou bázi (např. standardní). Nechť $\mathbf{x}$ jsou souřadnice $\overrightarrow{u}$ vzhledem k této bázi a $\mathbf{A}$ je matice transforamce A vzhledem k této bázi. Pak musí

$$\mathbf{A}\mathbf{x} = \lambda\mathbf{x}, \quad \mathbf{x} \neq \mathbf{o}, \quad \text{tj.} \quad (\mathbf{A} - \lambda\mathbf{E})\,\mathbf{x} = \mathbf{o}, \quad \mathbf{x} \neq \mathbf{o}$$

Takže matice $\mathbf{A} - \lambda\mathbf{E}$ musí být singulární, neboli $\det(\mathbf{A} - \lambda\mathbf{E}) = 0$.

Číslu λ budeme říkat *vlastní číslo* a vektoru $\overrightarrow{u}$ říkáme *vlastní vektor* transformace A příslušející vlastnímu číslu λ.

Vlastní čísla jsou i komplexní

Kvadratická rovnice $\det(\mathbf{A} - \lambda\mathbf{E}) = 0$ (viz předchozí motivační příklad) může ale nemusí mít reálné kořeny. Pokud má dva různé reálné kořeny, pak existují dva směry, které transformace A nemění. Tj. existují dvě přímky, pro které je $A(p) = p$. Například zkosení, které $(1,0)$ nechá beze změny a $(0,1)$ zobrazí na $(1,1/2)$.

Pokud jsou kořeny rovnice $\det(\mathbf{A} - \lambda\mathbf{E}) = 0$ komplexní, pak neexistují přímky, pro které je $A(p) = p$ (například rotace). Pokud bychom chtěli najít vlastní vektory příslušející komplexním vlastním číslům, budou mít komplexní souřadnice. Je tedy potřeba pracovat s lineárním prostorem nad komplexními čísly.

Budeme potřebovat záruku existence vlastních čísel. Budeme tedy muset připustit komplexní vlastní čísla a pracovat s lineární prostorem L nad $\mathbf{C}$.

Invariantní podprostor

Nechť $A : L \to L$ je lineární transformace. Podprostor $P \subset L$, pro který platí $A(P) = P$ nazýváme *invariantní podprostor* vzhledem k A.

Předběžná úvaha:

Je-li L lineární prostor nad $\mathbf{C}$, pak zaručeně existují vlastní čísla $\lambda \in \mathbf{C}$, pro která je $A(\overrightarrow{x}) = \lambda\,\overrightarrow{x}$, $\overrightarrow{x} \neq \overrightarrow{o}$. Společně s nulovým vektorem tvoří všechny vlastní vektory příslušející pevně vybranému vlastnímu číslu λ invariantní podprostor.

Je-li L lineární prostor nad $\mathbf{R}$, pak kromě $\{\overrightarrow{o}\}$ a L další invariantní podprostory vzhledem k A nemusejí existovat: vlastní čísla mohou být jen komplexní. Například A je rotace.

Vlastní číslo, vlastní vektor matice

Definice: Nechť $\mathbf{A}$ je čtvercová matice typu (n,n) reálných nebo komplexních čísel. Číslo $\lambda \in \mathbf{C}$ se nazývá *vlastním číslem matice* $\mathbf{A}$, pokud existuje vektor $\mathbf{x} \in \mathbf{C}^{n,1}$, $\mathbf{x} \neq \mathbf{o}$, takový, že $\mathbf{A} \cdot \mathbf{x} = \lambda\,\mathbf{x}$. Vektor $\mathbf{x}$, který splňuje uvedenou rovnost, se nazývá *vlastní vektor matice* $\mathbf{A}$ *příslušný vlastnímu číslu* λ.

Pozorování: Z rovnosti $\mathbf{A} \cdot \mathbf{x} = \lambda\,\mathbf{x}$ plyne $(\mathbf{A} - \lambda\mathbf{E})\,\mathbf{x} = \mathbf{o}$. Protože z definice musí $\mathbf{x} \neq \mathbf{o}$, je třeba, aby soustava měla nenulové řešení, tedy musí $\det(\mathbf{A} - \lambda\mathbf{E}) = 0$.

Definice: Polynom v proměnné λ tvaru $\det(\mathbf{A} - \lambda\mathbf{E})$ se nazývá *charakteristický polynom matice* $\mathbf{A}$.

Pozorování: Charakteristický polynom je stupně n a jeho kořeny jsou vlastní čísla matice $\mathbf{A}$. Matice $\mathbf{A}$ má tedy (včetně násobností) n vlastních čísel.

Vlastní číslo, vlastní vektor transformace

Definice: Nechť L je lineární prostor konečné dimenze nad $\mathbf{C}$ a nechť $A : L \to L$ je lineární transformace. Číslo $\lambda \in \mathbf{C}$ se nazývá *vlastním číslem transformace* A, pokud existuje vektor $\overrightarrow{x} \in L$, $\overrightarrow{x} \neq \overrightarrow{o}$ takový, že $A(\overrightarrow{x}) = \lambda\,\overrightarrow{x}$. Vektor $\overrightarrow{x}$, který splňuje uvedenou rovnost, se nazývá *vlastní vektor transformace* A *příslušný vlastnímu číslu* λ.

Pozorování: Vlastní číslo transformace A je stejné jako vlastní číslo její matice $\mathbf{A}$ vzhledem k jakékoli bázi (B). Vlastní vektor matice $\mathbf{A}$ pak obsahuje souřadnice vlastního vektoru transformace A vzhledem k bázi (B).

Důsledek: Všechny matice stejné lineární transformace (vzhledem k různým bázím) mají shodná vlastní čísla (mají shodné spektrum).

Příklad

Je dána matice

$$\mathbf{A} = \begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \\ -4 & 4 & -1 \end{pmatrix}.$$

Najdeme její vlastní čísla a k nim příslušející vlastní vektory.

$$\det\begin{pmatrix} 5-\lambda & -2 & 2 \\ -1 & 4-\lambda & -1 \\ -4 & 4 & -1-\lambda \end{pmatrix} = -\lambda^3 - 8\lambda^2 + 21\lambda - 18 = -(\lambda-3)^2(\lambda-2)$$

Toto je charakteristický polynom matice $\mathbf{A}$. Má dvojnásobný kořen $\lambda = 3$ a jednonásobný kořen $\lambda = 2$. Tyto kořeny jsou vlastní čísla matice $\mathbf{A}$.

Najdeme ještě vlastní vektory příslušející vlastním číslům 3 a 2...

Příklad, pokračování

$$\lambda = 3: \quad \begin{pmatrix} 5-3 & -2 & 2 \\ -1 & 4-3 & -1 \\ -4 & 4 & -1-3 \end{pmatrix} \sim (1 \quad -1 \quad 1),$$

takže k $\lambda = 3$ přísluší vlastní vektory z $\langle (1,1,0), (-1,0,1) \rangle$.

$$\lambda = 2: \quad \begin{pmatrix} 5-2 & -2 & 2 \\ -1 & 4-2 & -1 \\ -4 & 4 & -1-2 \end{pmatrix} \sim \begin{pmatrix} -1 & 2 & -1 \\ 0 & 4 & -1 \end{pmatrix}.$$

takže k $\lambda = 2$ přísluší vlastní vektory z $\langle (-2,1,4) \rangle$.

Pro vlastní čísla a vlastní vektory platí např. následující vztahy:

$$\begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \\ -4 & 4 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = 3 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \\ -4 & 4 & -1 \end{pmatrix} \begin{pmatrix} -2 \\ 1 \\ 4 \end{pmatrix} = 2 \begin{pmatrix} -2 \\ 1 \\ 4 \end{pmatrix}$$

Jiný příklad

$$\text{Je dána matice} \quad \mathbf{B} = \begin{pmatrix} 2 & 4 & -3 \\ -1 & 10 & -6 \\ -1 & 8 & -4 \end{pmatrix}.$$

Její charakteristický polynom je

$$\det(\mathbf{B} - \lambda \mathbf{E}) = -\lambda^3 - 8\lambda^2 + 21\lambda - 18 = -(\lambda - 3)^2 (\lambda - 2).$$

Hledáme vlastní vektory příslušející vlastním číslům 3 a 2:

$$\lambda = 3: \quad \begin{pmatrix} 2-3 & 4 & -3 \\ -1 & 10-3 & -6 \\ -1 & 8 & -4-3 \end{pmatrix} \sim \begin{pmatrix} -1 & 4 & -3 \\ 0 & 1 & -1 \end{pmatrix} \quad \begin{matrix} \text{vlastní} \\ \text{vektor:} \\ (1,1,1) \end{matrix}$$

$$\lambda = 2: \quad \begin{pmatrix} 2-2 & 4 & -3 \\ -1 & 10-2 & -6 \\ -1 & 8 & -4-2 \end{pmatrix} \sim \begin{pmatrix} -1 & 8 & -6 \\ 0 & 4 & -3 \end{pmatrix} \quad \begin{matrix} \text{vlastní} \\ \text{vektor:} \\ (0,3,4) \end{matrix}$$

B má stejná vlastní čísla jako **A**, ale jiné invariantní prostory.

Podobné matice

Idea: Jak se „podobají“ matice **A** a **A**′ stejné lineární transformace A, jen vzhledem k různým bázím (B) a (B')? Platí:

$$\mathbf{A}' = (\mathbf{P}_{B \to B'})^{-1} \cdot \mathbf{A} \cdot \mathbf{P}_{B \to B'}$$

To nás ispiruje k následující

Definici: Říkáme, že dvě čtvercové matice $\mathbf{A}, \mathbf{B} \in \mathbf{R}^{n,n}$ jsou *podobné*, pokud existuje regulární matice $\mathbf{P} \in \mathbf{R}^{n,n}$ taková, že

$$\mathbf{B} = \mathbf{P}^{-1} \cdot \mathbf{A} \cdot \mathbf{P}.$$

Pozorování1: podobnost je relace ekvivalence.

Pozorování2: podobné matice mají stejná vlastní čísla.

Podobné matice mají stejný char. polynom

Tvrzení: Podobné matice mají stejný charakteristický polynom.

Důkaz: Nechť $\mathbf{B} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}$ je matice podobná s **A**. Je

$$\begin{aligned} \det(\mathbf{P}^{-1}\mathbf{A}\mathbf{P} - \lambda\,\mathbf{E}) &= \det(\mathbf{P}^{-1}\mathbf{A}\mathbf{P} - \lambda\,\mathbf{P}^{-1}\mathbf{E}\mathbf{P}) = \\ &= \det(\mathbf{P}^{-1}\mathbf{A}\mathbf{P} - \mathbf{P}^{-1}\lambda\,\mathbf{E}\mathbf{P}) = \\ &= \det(\mathbf{P}^{-1}(\mathbf{A} - \lambda\,\mathbf{E})\mathbf{P}) = \\ &= \det\mathbf{P}^{-1}\,\det(\mathbf{A} - \lambda\,\mathbf{E})\,\det\mathbf{P} = \det(\mathbf{A} - \lambda\,\mathbf{E}). \end{aligned}$$

Upozornění: Obrácené tvrzení „mají-li dvě matice stejný charakteristický polynom, pak jsou podobné“ neplatí. Za chvíli ukážeme, že matice **A** a **B** z předchozích příkladů nejsou podobné.

Podobnost s diagonální maticí

Úloha: Budeme se ptát, za jakých podmínek je čtvercová matice **A** podobná s diagonální maticí tvaru:

$$\mathbf{D} = \begin{pmatrix} \lambda_1 & 0 & 0 & \dots & 0 \\ 0 & \lambda_2 & 0 & \dots & 0 \\ 0 & 0 & \lambda_3 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda_n \end{pmatrix}.$$

Jiný pohled na úlohu: je dána transformace A svou maticí **A** vzhledem k nějaké bázi. Ptáme se, zda existuje jiná báze, vzhledem ke které je matice transformace A diagonální. Ptáme se tedy, zda lze vhodnou volbou báze co nejvíce zjednodušit matici transformace až na diagonální tvar.

Pokud se to povede, pak z pohledu takové báze je transformace A jen změnou měřítka ve směrech vektorů báze (resp. projekce).

Rovnost $\mathbf{A} \cdot \mathbf{P} = \mathbf{P} \cdot \mathbf{D}$

Věta: Nechť **A**, **P** a **D** jsou čtvercové matice typu (n,n), nechť **P** obsahuje nenulové sloupce a nechť **D** je diagonální. Pak platí

$$\mathbf{A} \cdot \mathbf{P} = \mathbf{P} \cdot \mathbf{D}$$

právě tehdy, když **D** obsahuje vlastní čísla matice **A** a i-tý sloupec matice **P** obsahuje vlastní vektor příslušející i-tému vlastnímu číslu v **D**.

Důkaz: Nechť **D** obsahuje na diagonále čísla λ_i. Roznásobením rovnosti $\mathbf{A} \cdot \mathbf{P} = \mathbf{P} \cdot \mathbf{D}$ po sloupcích matice $\mathbf{P} = (\mathbf{p}_1, \mathbf{p}_2, \dots, \mathbf{p}_n)$ dostáváme rovnosti $\mathbf{A} \cdot \mathbf{p}_i = \lambda_i \mathbf{p}_i$. Tyto rovnosti platí právě když λ_i je vlastní číslo matice **A** a $\mathbf{p}_i$ je k němu příslušející vlastní vektor.

Pozorování: Kdyby byla **P** regulární, pak $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$, takže **A** bude podobná s diagonální maticí.

Podmínka podobnosti s diagonální maticí

Tvrzení: Matice **A** typu (n,n) je podobná s diagonální maticí právě když má n lineárně nezávislých vlastních vektorů.

Skutečně, stačí tyto vektory napsat do sloupců matice **P**, dále sestavit diagonální matici **D** z odpovídajících vlastních čísel a platí rovnost z předchozí strany.

Věta: Různá vlastní čísla mají lineárně nezávislé vlastní vektory.

Důkaz: technický, viz skriptum.

Důsledek: Má-li matice **A** pouze jednonásobná vlastní čísla (těch je n a jsou vzájemně různá), pak je podobná s diagonální maticí.

Upozornění: Obrácené tvrzení „**A** je podobná s diagonální, pak má vzájemně různá vlastní čísla“ neplatí. Např. **E** má n-násobné vlastní číslo 1 a je přímo rovna diagonální matici.

Příklad

Matice **A** z předchozího příkladu je podobná s diagonální. Má tři lineárně nezávislé vlastní vektory, např.

$$(1,1,0), \ (-1,0,1), \ (-2,1,4).$$

Tudíž platí

$$\begin{pmatrix} 1 & -1 & -2 \\ 1 & 0 & 1 \\ 0 & 1 & 4 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 5 & -2 & 2 \\ -1 & 4 & -1 \\ -4 & 4 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & -2 \\ 1 & 0 & 1 \\ 0 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Matice **B** z předchozího příkladu není podobná s diagonální, protože nemá tři lineárně nezávislé vlastní vektory.

Takže: matice **A** a **B** nejsou vzájemně podobné, ačkoli mají stejný charakteristický polynom a stejná vlastní čísla.

Příklad: změna báze

Matice $\mathbf{A}$ z předchozího příkladu odpovídá transformaci:

$$\begin{aligned} x' &= 5x - 2y + 2z \\ y' &= -x + 4y - z \\ z' &= -4x + 4y - z \end{aligned}$$

Vzhledem k bázi $(C) = ((1,1,0), (-1,0,1), (-2,1,4))$ má tatáž transformace diagonální matici

$$\mathbf{D} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

takže v této bázi se souřadnice obrazu počítají takto:

$$x' = 3x, \quad y' = 3y, \quad z' = 2z.$$

Nutná podmínka podobnosti s diagonální maticí

Dá se ukázat, že dimenze nulového prostoru matice $\mathbf{A}-\lambda\mathbf{E}$ je vždy menší nebo rovna násobnosti vlastního čísla λ.

Matice $\mathbf{A}$ typu (n,n) je podobná s diagonální právě když má n lineárně nezávislých vlastních vektorů. To znamená, že má-li k násobné vlastní číslo λ, musí mu příslušet k lineárně nezávislých vektorů, neboli dimenze nulového prostoru matice $\mathbf{A}-\lambda\mathbf{E}$ musí být přesně rovna k.

Pokud tedy pro každé vícenásobné vlastní číslo λ je dimenze nulového prostoru matice $\mathbf{A}-\lambda\mathbf{E}$ přesně rovna násobnosti tohoto vlastního čísla, je matice $\mathbf{A}$ podobná s diagonální maticí.

Jordanův kanonický tvar

Dá se ukázat, že každá matice $\mathbf{A}$ je podobná aspoň se „skoro diagonální“ maticí tvaru:

$$\mathbf{J} = \begin{pmatrix} \mathbf{J}_1 & \mathbf{O} & \dots & \mathbf{O} \\ \mathbf{O} & \mathbf{J}_2 & \dots & \mathbf{O} \\ & & \dots & \\ \mathbf{O} & \mathbf{O} & \dots & \mathbf{J}_m \end{pmatrix}, \quad \text{kde} \quad \mathbf{J}_i = \begin{pmatrix} \lambda_i & 1 & 0 & \dots & 0 \\ 0 & \lambda_i & 1 & \dots & 0 \\ & & & \dots & \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & \lambda_i \end{pmatrix}$$

Čísla λ_i jsou vlastní čísla matice $\mathbf{A}$. Matici $\mathbf{J}$ se říká *Jordanův kanonický tvar matice* $\mathbf{A}$.

Na diagonále matice $\mathbf{J}$ se objeví každé vlastní číslo tolikrát, kolik je jeho násobnost.

Dimenze nulového prostoru matice $\mathbf{A}-\lambda\mathbf{E}$ odpovídá počtu Jordanových bloků $\mathbf{J}_i$ se stejným vlastním číslem λ. Takže tyto Jordanovy bloky se mohou pro stejné (vícenásobné) vlastní číslo opakovat.

Cvičení

- Vysvětlete, proč $\det\mathbf{A}$ je roven součinu vlastních čísel matice $\mathbf{A}$.
- Vysvětlete, proč $\det\mathbf{A}$ je roven absolutnímu členu charakteristického polynomu matice $\mathbf{A}$.
- Předpokládejte $\mathbf{A}$ matici podobnou s diagonální. Když do charakteristického polynomu matice $\mathbf{A}$ místo λ zapíšete matici $\mathbf{A}$, dostáváte nulovou matici. Proč?
- Předchozí tvrzení patí i pro matice, které nejsou podobné s diagonální maticí.

Skalární součin

- axiomatická definice
- odvození velikosti vektorů a úhlu mezi vektory
- geometrická interpretace
- ortogonalita
- vlastnosti ortonormálních bázi

a) algebra-all, 15, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) Viz p. d. 4/2010

Definice skalárního součinu

Nechť L je lineární prostor nad $\mathbf{R}$. Operaci $\cdot : L\times L \to \mathbf{R}$ nazýváme *skalární součin*, pokud pro všechna $\vec{x}, \vec{y}, \vec{z}$ splňuje:

(1) $\vec{x}\cdot\vec{y} = \vec{y}\cdot\vec{x}$,
(2) $(\vec{x}+\vec{y})\cdot\vec{z} = \vec{x}\cdot\vec{z} + \vec{y}\cdot\vec{z}$,
(3) $(\alpha\cdot\vec{x})\cdot\vec{y} = \alpha\cdot(\vec{x}\cdot\vec{y})$,
(4) $\vec{x}\cdot\vec{x} \geq 0$, $\vec{x}\cdot\vec{x} = 0$ jen tehdy, když $\vec{x} = \vec{o}$.

Poznámka: Je-li L lineární prostor nad $\mathbf{C}$, pak se skalárním součinem označuje operace $\cdot : L\times L \to \mathbf{C}$ se stejnými vlastnostmi, jako výše, až na první. Místo ní je:

$$\vec{x}\cdot\vec{y} = \overline{\vec{y}\cdot\vec{x}}$$

Čísla jsou si vzájemně komplexně sdružená.

Příklady skalárních součinů

- V $\mathbf{R}^n$ definujeme

  $$(x_1,x_2,\dots x_n)\cdot(y_1,y_2,\dots,y_n) = x_1y_1 + x_2y_2 + \dots + x_ny_n.$$

  Toto je skalární součin, skutečně splňuje axiomy (1) až (4).
- V prostoru orientovaných úseček definujeme skalární součin

  $$\vec{u}\cdot\vec{v} = \|\vec{u}\|\|\vec{v}\|\cos\alpha,$$

  kde $\|\dots\|$ značí velikost vektoru a α je úhel mezi vektory.
- V lineárním prostoru spojitých funkcí na intervalu $\langle 0,1\rangle$ definujeme skalární součin

  $$f\cdot g = \int_0^1 f(x)g(x)\,\mathrm{d}x$$

Další skalární součiny v $\mathbf{R}^n$

Na $\mathbf{R}^2$ je operace

$$(x_1,x_2)\circ(y_1,y_2) = (x_1,x_2)\begin{pmatrix}1&2\\2&6\end{pmatrix}\begin{pmatrix}y_1\\y_2\end{pmatrix} = x_1y_1 + 6x_2y_2 + 2x_1y_2 + 2x_2y_1.$$

také skalární součin. Na druhé straně třeba

$$(x_1,x_2)\circ(y_1,y_2) = (x_1,x_2)\begin{pmatrix}1&2\\2&2\end{pmatrix}\begin{pmatrix}y_1\\y_2\end{pmatrix} = x_1y_1 + 2x_2y_2 + 2x_1y_2 + 2x_2y_1$$

není skalární součin (neplatí axiom 4).

Obecně, je-li $\mathbf{A}$ symetrická a pozitivně definitní matice (všechny hlavní subdeterminanty jsou kladné), pak

$$\vec{x}\cdot\mathbf{A}\cdot\vec{y}^T$$

je skalární součin. Z tohoto pohledu nazýváme $\vec{x}\cdot\vec{y}^T$ *standardním* skalárním součinem na $\mathbf{R}^n$.

Skalární součin ⟶ velikost

V lineárním prostoru L se skalárním součinem definujeme *velikost* vektoru $\overrightarrow{x}$, neboli *normu* vektoru $\overrightarrow{x}$ vzorcem

$$\|\overrightarrow{x}\| = \sqrt{\overrightarrow{x}\cdot\overrightarrow{x}}.$$

Axiom (4) zaručuje, že velikost je definována pro libovolný vektor a že nulovou velikost má pouze nulový vektor.

Tvrzení: $\|\alpha\overrightarrow{x}\| = |\alpha|\cdot\|\overrightarrow{x}\|$, protože

$$\|\alpha\overrightarrow{x}\| = \sqrt{\alpha\overrightarrow{x}\cdot\alpha\overrightarrow{x}} = \sqrt{\alpha^2(\overrightarrow{x}\cdot\overrightarrow{x})} = \sqrt{\alpha^2}\sqrt{\overrightarrow{x}\cdot\overrightarrow{x}} = |\alpha|\cdot\|\overrightarrow{x}\|$$

Skalární součin ⟶ úhel mezi vektory

V lineárním prostoru L se skalárním součinem definujeme *úhel mezi dvěma nenulovými vektory* $\overrightarrow{x}$ a $\overrightarrow{y}$ jako takové $\phi\in\langle 0,\pi)$, pro které je

$$\cos\phi = \frac{\overrightarrow{x}\cdot\overrightarrow{y}}{\|\overrightarrow{x}\|\,\|\overrightarrow{y}\|}$$

Že $\cos\phi$ v uvedeném vzorci existuje pro libovolné dva nenulové vektory zaručuje

Schwartzova nerovnost: Pro libovolné dva vektory platí

$$|\overrightarrow{x}\cdot\overrightarrow{y}| \le \|\overrightarrow{x}\|\cdot\|\overrightarrow{y}\|.$$

Důkaz: $0\le(\overrightarrow{x}+\alpha\overrightarrow{y})\cdot(\overrightarrow{x}+\alpha\overrightarrow{y}) = \overrightarrow{x}\cdot\overrightarrow{x}+\alpha\cdot 2(\overrightarrow{x}\cdot\overrightarrow{y})+\alpha^2\cdot(\overrightarrow{y}\cdot\overrightarrow{y})$. Pro uvedený kvadratický polynom $A\alpha^2+B\alpha+C$ musí platit:

$$B^2-4AC\le 0,\quad \text{tj.}\quad B^2\le 4AC,\quad \text{tj.}\quad (-2(\overrightarrow{x}\cdot\overrightarrow{y}))^2\le 4\|\overrightarrow{x}\|^2\|\overrightarrow{y}\|^2,$$
$$\text{tj.}\quad \sqrt{(\overrightarrow{x}\cdot\overrightarrow{y})^2}\le\sqrt{\|\overrightarrow{x}\|^2}\sqrt{\|\overrightarrow{y}\|^2}\quad\text{tj.}\quad |\overrightarrow{x}\cdot\overrightarrow{y}|\le\|\overrightarrow{x}\|\cdot\|\overrightarrow{y}\|.$$

Skalární součin ⟶ vzdálenost vektorů

V lineárním prostoru L se skalárním součinem definujeme *vzdálenost mezi dvěma vektory* $\overrightarrow{x}$ a $\overrightarrow{y}$, neboli *metriku* vzorcem

$$\rho(\overrightarrow{x},\overrightarrow{y}) = \|\overrightarrow{x}-\overrightarrow{y}\|$$

Pro metriku patí **trojúhelníková nerovnost**:

$$\rho(\overrightarrow{x},\overrightarrow{y})+\rho(\overrightarrow{y},\overrightarrow{z}) \ge \rho(\overrightarrow{x},\overrightarrow{z}),$$

neboli $\|\overrightarrow{x}-\overrightarrow{y}\|+\|\overrightarrow{y}-\overrightarrow{z}\|\ge\|\overrightarrow{x}-\overrightarrow{z}\|$, která označení $\overrightarrow{a}=\overrightarrow{x}-\overrightarrow{y}$, $\overrightarrow{b}=\overrightarrow{y}-\overrightarrow{z}$ přechází na tvar

$$\|\overrightarrow{a}\|+\|\overrightarrow{b}\| \ge \|\overrightarrow{a}+\overrightarrow{b}\|.$$

Důkaz: $\|\overrightarrow{a}+\overrightarrow{b}\|^2 = (\overrightarrow{a}+\overrightarrow{b})\cdot(\overrightarrow{a}+\overrightarrow{b}) = \overrightarrow{a}\,\overrightarrow{a}+2\,\overrightarrow{a}\,\overrightarrow{b}+\overrightarrow{b}\,\overrightarrow{b} \le$
(Schwartzova nerovnost) $\le \|\overrightarrow{a}\|^2+2\|\overrightarrow{a}\|\cdot\|\overrightarrow{b}\|+\|\overrightarrow{b}\|^2 = (\|\overrightarrow{a}\|+\|\overrightarrow{b}\|)^2$.

Axiomy metriky a normy

Je-li na množině L zavedena metrika $\rho(x,y)$ s vlastnostmi

(1) $\rho(x,y)\ge 0$, $\rho(x,y)=0$ právě když $x=y$,
(2) $\rho(x,y)=\rho(y,x)$,
(3) $\rho(x,y)+\rho(y,z)\ge\rho(x,z)$,

říkáme množině L s metrikou ρ *metrický prostor*.

Je-li na lineárním prostoru L zavedena norma $\|\ldots\|$ s vlastnostmi

(1) $\|\overrightarrow{x}\|\ge 0$, $\|\overrightarrow{x}\|=0$ právě když $\overrightarrow{x}=\overrightarrow{o}$,
(2) $\|\alpha\overrightarrow{x}\| = |\alpha|\cdot\|\overrightarrow{x}\|$,
(3) $\|\overrightarrow{x}+\overrightarrow{y}\| \le \|\overrightarrow{x}\|+\|\overrightarrow{y}\|$,

říkáme prostoru L *lineární prostor s normou*.

My jsme odvodili normu a metriku ze skalárního součinu. Je ovšem možné je zavést jen podle uvedených axiomů, nebo zavést normu axiomaticky a odvodit metriku jako $\rho(\overrightarrow{x},\overrightarrow{y}) = \|\overrightarrow{x}-\overrightarrow{y}\|$

Příklady

Pythagorova věta: Pravoúhlý trojúhelník budou tvořit dva na sebe kolmé vektory $\overrightarrow{x}$ a $\overrightarrow{y}$. Jejich rozdíl tvoří přeponu.

$$\|\overrightarrow{x}-\overrightarrow{y}\|^2 = (\overrightarrow{x}-\overrightarrow{y})\cdot(\overrightarrow{x}-\overrightarrow{y}) = \overrightarrow{x}\cdot\overrightarrow{x}-2\overrightarrow{x}\cdot\overrightarrow{y}+\overrightarrow{y}\cdot\overrightarrow{y} = \|\overrightarrow{x}\|^2+\|\overrightarrow{y}\|^2$$

Ve výpočtu jsme využili toho, že dva nenulové vektory $\overrightarrow{x}$ a $\overrightarrow{y}$ jsou na sebe kolmé právě když $\overrightarrow{x}\cdot\overrightarrow{y}=0$.

Rovnoběžníková rovnost: součet druhých mocnin velikostí úhlopříček v rovnoběžníku je roven dvojnásobku součtu druhých mocnin velikostí sousedních stran.

$$\|\overrightarrow{x}+\overrightarrow{y}\|^2+\|\overrightarrow{x}-\overrightarrow{y}\|^2 = 2\left(\|\overrightarrow{x}\|^2+\|\overrightarrow{y}\|^2\right).$$

protože

$$\|\overrightarrow{x}+\overrightarrow{y}\|^2+\|\overrightarrow{x}-\overrightarrow{y}\|^2 = \|\overrightarrow{x}\|^2+2\overrightarrow{x}\cdot\overrightarrow{y}+\|\overrightarrow{y}\|^2+\|\overrightarrow{x}\|^2-2\overrightarrow{x}\cdot\overrightarrow{y}+\|\overrightarrow{y}\|^2.$$

Ortonormální báze

Na lineárním prostoru se skalárním součinem můžeme měřit velikosti vektorů a úhly mezi nenulovými vektory.

Zejména *kolmost* (ortogonalitu) dvou nenulových vektorů $\overrightarrow{x}$ a $\overrightarrow{y}$ poznáme podle podmínky $\overrightarrow{x}\cdot\overrightarrow{y}=0$.

Mezi různými bázemi se ukáže výhodné vybírat takové báze, ve kterých jsou si všechny vektory navzájem kolmé a mají jednotkovou velikost. Tyto báze nazýváme *ortonormální*.

Definice: Báze se nazývá *ortogonální*, pokud pro každé dva různé prvky báze $\overrightarrow{b}_i$ a $\overrightarrow{b}_j$ platí $\overrightarrow{b}_i\cdot\overrightarrow{b}_j=0$.

Báze se nazývá *ortonormální*, je-li ortogonální a všechny její prvky mají jednotkovou velikost, neboli

$$\overrightarrow{b}_i\cdot\overrightarrow{b}_j = \begin{cases}1 & \text{pro } i=j,\\ 0 & \text{pro } i\ne j.\end{cases}$$

Skalární součin počítaný pomocí souřadnic

Věta: Nechť (B) je konečná ortonormální báze lineárního prostoru L. Nechť $(x_1,x_2,\ldots,x_n)$ jsou souřadnice vektoru $\overrightarrow{x}$ vzhledem k bázi (B) a nechť $(y_1,y_2,\ldots,y_n)$ jsou souřadnice vektoru $\overrightarrow{y}$ vzhledem k bázi (B). Pak

$$\overrightarrow{x}\cdot\overrightarrow{y} = x_1y_1+x_2y_2+\cdots+x_ny_n.$$

Důkaz:

$$(x_1\overrightarrow{b}_1+x_2\overrightarrow{b}_2+\cdots+x_n\overrightarrow{b}_n)\cdot(y_1\overrightarrow{b}_1+y_2\overrightarrow{b}_2+\cdots+y_n\overrightarrow{b}_n) =$$
$$= x_1y_1\overrightarrow{b}_1\cdot\overrightarrow{b}_1+x_2y_1\overrightarrow{b}_2\cdot\overrightarrow{b}_1+\cdots+x_1y_2\overrightarrow{b}_1\cdot\overrightarrow{b}_2+\cdots+x_ny_n\overrightarrow{b}_n\cdot\overrightarrow{b}_n =$$
$$= x_1y_1\cdot 1+x_2y_1\cdot 0+\cdots+x_1y_2\cdot 0+\cdots+x_ny_n\cdot 1 =$$
$$= x_1y_1+x_2y_2+\cdots+x_ny_n.$$

Kolmost zaručuje lineární nezávislost

Věta: Nechť $\overrightarrow{x}_1,\overrightarrow{x}_2,\ldots,\overrightarrow{x}_n$ jsou nenulové vektory, které jsou na sebe navzájem kolmé. Pak jsou tyto vektory lineárně nezávislé.

Důkaz: Ověříme

$$\alpha_1\cdot\overrightarrow{x}_1+\alpha_2\cdot\overrightarrow{x}_2+\cdots+\alpha_n\cdot\overrightarrow{x}_n=\overrightarrow{o} \quad\Rightarrow\quad \alpha_i=0\quad\forall\, i$$

Vynásobíme-li obě strany rovnosti skalárně vektorem $\overrightarrow{x}_i$, dostáváme na levé straně součet nul s výjimkou jediného sčítance, protože vektor $\overrightarrow{x}_i$ je kolmý na všechny všechny ostatní vektory $\overrightarrow{x}_j$. Máme tedy

$$\alpha_i\,\overrightarrow{x}_i\cdot\overrightarrow{x}_i = \overrightarrow{o}\cdot\overrightarrow{x}_i = 0.$$

Protože $\overrightarrow{x}_i\cdot\overrightarrow{x}_i$ je nenulové číslo, musí být $\alpha_i=0$. Tuto operaci můžeme provést pro každý index $i\in\{1,2,\ldots,n\}$, takže všechna čísla čísla α_i jsou nutně nulová.

Souřadnice počítané ze skalárního součinu

Věta: Nechť $(B) = (\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n)$ je ortonormální báze lineárního prostoru se skalárním součinem. Pak souřadnice libovolného vektoru $\vec{x}$ vzhledem k bázi (B) jsou

$$(\vec{x}\cdot\vec{b}_1,\ \vec{x}\cdot\vec{b}_2,\ \ldots,\ \vec{x}\cdot\vec{b}_n).$$

Důkaz: Označme $\vec{y} = (\vec{x}\cdot\vec{b}_1)\,\vec{b}_1 + (\vec{x}\cdot\vec{b}_2)\,\vec{b}_2 + \cdots + (\vec{x}\cdot\vec{b}_n)\,\vec{b}_n$. Máme dokázat, že $\vec{x} = \vec{y}$. Násobme vektor $\vec{y}$ vektorem $\vec{b}_i$:

$$\vec{y}\cdot\vec{b}_i = ((\vec{x}\cdot\vec{b}_1)\,\vec{b}_1 + (\vec{x}\cdot\vec{b}_2)\,\vec{b}_2 + \cdots + (\vec{x}\cdot\vec{b}_n)\,\vec{b}_n)\cdot\vec{b}_i = \\ = (\vec{x}\cdot\vec{b}_i)\,\vec{b}_i\cdot\vec{b}_i = \vec{x}\cdot\vec{b}_i,$$

protože báze je ortonormální. Je $\vec{x}\cdot\vec{b}_i = \vec{y}\cdot\vec{b}_i\ \forall i \in \{1,2,\ldots,n\}$.

Co, kdyby $\vec{x} \neq \vec{y}$? Vektor $\vec{x} - \vec{y}$ je kolmý na všechny prvky $\vec{b}_i$, protože $(\vec{x} - \vec{y})\cdot\vec{b}_i = 0$. Pak jsou vektory $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n, \vec{x} - \vec{y}$ lineárně nezávislé, ale to je ve sporu s tím, že (B) je báze.

Básnička: čtvrtá dimenze

Jednou v hospodě u Karla čtvrtého,
uviděl jsem kus prostoru čtvrtého.

Čtyři půllitry u stropu nad sálem,
letěly k sobě kolmo navzájem,
což není možné v dimenzi třetí,
kde nejvýše tři půllitry k sobě letí.

Tak poznal jsem díky otci vlasti,
jaké jsou v půllitru skryty slasti.
Jak všem čechům rozšiřuje obzory
o n-dimenzionální prostory.

in: Emil Calda: Říkanky množinově nelogické

Geometrická představa skalárního součinu

Předpokládejme, že vektory $\vec{x}$ a $\vec{y}$ jsou orientované úsečky, navíc nechť $\vec{y}$ má jednotkovou velikost. Sestrojme z koncového bodu vektoru $\vec{x}$ kolmý průmět na přímku, procházející vektorem $\vec{y}$. Velikost tohoto kolmého průmětu (je-li na polopřímce společně s vektorem $\vec{y}$) je skalární součin $\vec{x}\cdot\vec{y}$. Je-li průmět na opačné polopřímce, pak skalární součin je záporný a jeho absolutní hodnota je rovna velikosti průmětu.

Tato geometrická interpretace vychází ze vzorce:

$$\vec{x}\cdot\vec{y}\ =\ \|\vec{x}\|\,\|\vec{y}\|\cos\phi.$$

Z tohoto pohledu říká věta ze stránky [13], že souřadnice vektoru jsou průměty vektoru na jednotlivé souřadnicové osy.

Úhly vektoru s osami

Věta: Nechť $(x_1, x_2, \ldots, x_n)$ jsou souřadnice vektoru $\vec{x}$ vzhledem k ortonormální bázi $(\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n)$. Pak úhel ϕ_i mezi vektorem $\vec{x}$ a vektorem $\vec{b}_i$ má velikost ϕ_i, pro kterou je

$$\cos\phi_i = \frac{x_i}{\|\vec{x}\|}.$$

Důkaz:

$$\cos\phi_i = \frac{\vec{x}\cdot\vec{b}_i}{\|\vec{x}\|\,\|\vec{b}_i\|} = \frac{\vec{x}\cdot\vec{b}_i}{\|\vec{x}\|} = \frac{x_i}{\|\vec{x}\|}.$$

V úpravách jsme využili toho, že $\|\vec{b}_i\| = 1$ (báze je ortonormální) a dále předchozí věty, podle které je $x_i = \vec{x}\cdot\vec{b}_i$.

Důsledek: $\cos^2\phi_1 + \cos^2\phi_2 + \cdots + \cos^2\phi_n = 1$

Schmidtův ortogonalizační proces

Zhruba: každou konečnou bázi lze „opravit“ tak, aby byla ortonormální. Oprava k-tého vektoru vždy probíhá v lineárním obalu prvních k vektorů. Tj. první vektor opravíme na přímce dané prvním vektorem, druhý vektor opravíme v rovině dané prvními dvěma vektory, atd.

Přesně: Nechť $\{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$ je libovolná báze. Pak existuje ortonormální báze $\{\vec{c}_1, \vec{c}_2, \ldots, \vec{c}_n\}$ taková, že

$$\langle\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_k\rangle = \langle\vec{c}_1, \vec{c}_2, \ldots, \vec{c}_k\rangle, \qquad \forall k \in \{1,2,\ldots,n\}.$$

Důkaz: oprava každého vektoru probíhá ve dvou krocích. Vektor se (uvnitř zmíněného lin. obalu) „natočí“ a následně se „normuje“:

$$\vec{b}'_{k+1} = \vec{b}_{k+1} - \sum_{i=1}^{k}(\vec{b}_{k+1}\cdot\vec{c}_i)\,\vec{c}_i, \qquad \vec{c}_{k+1} = \frac{\vec{b}'_{k+1}}{\|\vec{b}'_{k+1}\|}.$$

Ortogonální matice

Předpokládejme v $\mathbf{R}^n$ standardní skalární součin. Matice $\mathbf{A} \in \mathbf{R}^{n,n}$, která ve sloupcích obsahuje nějakou ortonormální bázi prostoru $\mathbf{R}^n$, se nazývá *ortogonální*.

Následující podmínky jsou ekvivalentní:

- $\mathbf{A}$ je ortogonální,
- $\mathbf{A}^T\cdot\mathbf{A} = \mathbf{E}$,
- $\mathbf{A}\cdot\mathbf{A}^T = \mathbf{E}$,
- $\mathbf{A}^T$ je ortogonální,
- $\mathbf{A}$ obsahuje v řádcích souřadnice ortonormální báze,
- $\mathbf{A}$ je maticí přechodu mezi dvěma ortonormálními bázemi.

Další vlastnosti ortogonální matice

- Je-li $\mathbf{A}$ ortogonální, pak $\det\mathbf{A} = 1$ nebo $\det\mathbf{A} = -1$.
- Je-li $\mathbf{A}$ ortogonální a je-li $\mathbf{x}$ sloupcový vektor, pak sloupcový vektor $\mathbf{A}\cdot\mathbf{x}$ má stejnou velikost jako vektor $\mathbf{x}$.
- Součin ortogonálních matic je ortogonální.

První puntík:

$$1 = \det\mathbf{E} = \det(\mathbf{A}\cdot\mathbf{A}^T) = (\det\mathbf{A})\,(\det\mathbf{A}^T) = (\det\mathbf{A})^2.$$

Druhý puntík:

$$\|\mathbf{Ax}\|^2 = (\mathbf{Ax})^T\cdot(\mathbf{Ax}) = \mathbf{x}^T\cdot\mathbf{A}^T\cdot\mathbf{A}\cdot\mathbf{x} = \mathbf{x}^T\cdot\mathbf{x} = \|\mathbf{x}\|^2.$$

Třetí puntík:

$$(\mathbf{A}\cdot\mathbf{B})^T\cdot(\mathbf{A}\cdot\mathbf{B}) = \mathbf{B}^T\cdot\mathbf{A}^T\cdot\mathbf{A}\cdot\mathbf{B} = \mathbf{B}^T\cdot\mathbf{E}\cdot\mathbf{B} = \mathbf{E}.$$

QR rozklad

Je-li $\mathbf{A}$ regulární matice, pak existuje ortogonální matice $\mathbf{Q}$ a horní trojúhelníková matice $\mathbf{R}$ tak, že

$$\mathbf{A} = \mathbf{Q}\cdot\mathbf{R}.$$

Důkaz: Sloupce matice $\mathbf{A}$ tvoří nějakou bázi (B). Na tuto bázi provedeme Schmidtův ortogonalizační proces a tím dostaneme ortonormální bázi (C). Zapíšeme ji do sloupců matice $\mathbf{Q}$. Matice $\mathbf{R}$ je maticí přechodu od ortonormální báze (C) k bázi (B). Obsahuje souřadnice vektorů $\vec{b}_k$ z báze (B) vzhledem k (C). Díky vlastnosti

$$\langle\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_k\rangle = \langle\vec{c}_1, \vec{c}_2, \ldots, \vec{c}_k\rangle, \qquad \forall k \in \{1,2,\ldots,n\}.$$

jsou souřadnice vektoru $\vec{b}_k$ vzhledem k (C) pro $i > k$ nulové, takže $\mathbf{R}$ je horní trojúhelníková.

Euklidovský prostor

- Euklidovy Základy (pohled do historie)
- dnešní definice
- kartézský souřadnicový systém
- vlastnosti „rovin“ v E_n
- speciální vlastnosti v E_3 (vektorový součin)

a) algebra-all, 16, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) Viz p. d. 4/2010

Euklides

Euklides (jiný překlad: Eukleides) byl řecký matematik (kolem roku 300 př. n. l.).

Hlavní dílo: Euklidovy *Základy* (ve 13 kapitolách). Po Bibli nejvíce publikované dílo až do 19. století.

Pokusil se o přesné formální vyjadřování, vybudoval geometrii systémem definice, věta, důkaz. Pokusil se definovat i nedefinovatelné:

- *bod* je to, co nemá části,
- *křivka* je délka bez šířky,
- *přímka* je křivka s body, která leží rovně,
- rozdělením přímého úhlu na dva stejné vzniká úhlel *pravý*,
- …

Euklidovy postuláty (axiomy)

Euklides si uvědomil, že některá tvrzení nelze dokázat, je nutné je předpokládat. Formuloval pět tzv. postulátů:

- Dva body určují jedinou úsečku, která v těch bodech končí.
- Každá úsečka může být prodloužena tak, že vznikne opět úsečka.
- Je možné nakreslit kružnici s libovolným středem a poloměrem.
- Všechny pravé úhly jsou si rovny.
- Jestliže přímka protíná dvě přímky tak, že vnitřní úhly na téže straně jsou menší než dva pravé úhly, pak se tyto dvě přímky protnou na stejné straně, na které jsou úhly menší než dva pravé.

Otazníky kolem pátého axiomu

Pátý axiom je formulován složitě, je v geometrii nutný?

Ukázalo se, že pátý axiom je (za předpokladu platnosti prvních čtyř) ekvivalentní s následujícími tvrzeními:

- Daným bodem lze k dané přímce vést jedinou rovnoběžku.
- Trojúhelníky mají součet vnitřních úhlů 180°.
- Platí Pythagorova věta.

Později se ukázalo (Gauss, Lobačevskij, Riemann), že užitečná je i geometrie bez pátého axiomu (tzv. neeuklidovská geometrie). Například dvourozměrná geometrie na sféře: trojúhelníky mají součet úhlů větší než 180°, každé dvě „přímky“ (nejkratší spojnice dvou bodů prodloužené na obou koncích) se protínají, tj. neexistuje rovnoběžka. Neplatí Pythagorova věta.

Euklidovský prostor dnes

V euklidovském prostoru chceme pracovat s přímkami (to umíme v afinním prostoru), dále chceme v rovinách vymezit kružnice. K tomu potřebujeme měřit vzdálenosti. Potřebujeme tedy metrický prostor. Metrika musí být odvozena z Pythagorovy věty (jinak by tato věta neplatila a neplatil by pátý Euklidův axiom). Tuto vlastnost splňuje metrika odvozená ze skalárního součinu. Konečně v euklidovském prostoru potřebujeme měřit úhly. K tomu také slouží skalární součin. Dnešní definice euklidovského prostoru je tedy následující:

Definice: *Euklidovský prostor* E_n je afinní prostor $(\mathbf{X}, V)$ dimenze n, přitom V je lineární prostor se skalárním součinem. Z tohoto součinu je odvozena norma a metrika na V. Metrika na $\mathbf{X}$ je definována takto: vzdálenost bodů P, Q je rovna velikosti vektoru $P–Q$.

Základní objekty v euklidovském prostoru

- **Přímka**: $p = \{A + t\vec{s},\ t \in \mathbf{R}\}$, kde $A \in \mathbf{X}$, $\vec{s} \in V$, $\vec{s} \neq \vec{o}$.

Přímka je tedy dána bodem A, kterým prochází a nenulovým *směrovým vektorem* $\vec{s}$. Může být též dána dvěma body A a B: $p = \{A + t(B-A),\ t \in \mathbf{R}\}$.

- **Úsečka** s koncovými body A, B: $u = \{A + t(B-A),\ t \in \langle 0,1\rangle\}$.
- **Kružnice** se středem S a poloměrem r: $k = \{X,\ \rho(S,X) = r\}$.

Kružnici lze takto definovat jen v E_2 (dimenzi 2). Pro větší dimenze je uvedená množina povrchem n-rozměrné koule.

- **Rovina**: $\sigma = \{A + t\vec{a} + u\vec{b},\ t,u \in \mathbf{R}\}$, $A \in \mathbf{X}$, $\vec{a}, \vec{b} \in V$ jsou LN.

Rovina je dána bodem a dvěma nezávislými směry.

- **Zobecněná rovina** (afinní podprostor): $\tau = A + \langle \vec{a}_1, \ldots, \vec{a}_k\rangle$,

Vztahy mezi přímkami

Dvě přímky $p = \{A_1 + t\vec{s}_1,\ t \in \mathbf{R}\}$ a $q = \{A_2 + t\vec{s}_2,\ t \in \mathbf{R}\}$ jsou *totožné*, právě když vektory $A_2 - A_1$ a $\vec{s}_1$ jsou LZ a současně směrové vektory $\vec{s}_1$, $\vec{s}_2$ jsou LZ.

Dvě přímky $p = \{A_1 + t\vec{s}_1,\ t \in \mathbf{R}\}$ a $q = \{A_2 + t\vec{s}_2,\ t \in \mathbf{R}\}$ jsou *rovnoběžné*, právě když nejsou totožné a vektory $\vec{s}_1$, $\vec{s}_2$ jsou LZ.

Dvě přímky $p = \{A_1 + t\vec{s}_1,\ t \in \mathbf{R}\}$ a $q = \{A_2 + t\vec{s}_2,\ t \in \mathbf{R}\}$ *leží ve společné rovině*, právě když vektory $A_2 - A_1$, $\vec{s}_1$, $\vec{s}_2$ jsou LZ.

Dvě přímky jsou *různoběžky* (protínají se v jednom bodě), právě když leží ve společné rovině a nejsou totožné ani rovnoběžné.

Dvě přímky jsou *mimoběžky* (míjejí se v prostoru), právě když neleží ve společné rovině.

Uvedené vztahy rozpoznáme *algebraickými metodami*: vyšetřením lineární závislosti nebo nezávislosti vektorů.

Příklad

Najdeme parametr $a \in \mathbf{R}$ takový, aby se přímky $p = (1,2,3) + \langle(2,2,5)\rangle$ a $q = (4,3,7) + \langle(3,a,1)\rangle$ protínaly.

Řešení: Přímky nejsou rovnoběžné ani totožné, protože jejich směrové vektory jsou lineárně nezávislé. Aby tyto přímky byly různoběžkami, musí být vektory $(3,1,4),(2,2,5),(3,a,1)$ lienárně závislé, takže když jejich souřadnice zapíšeme do řádků matice $\mathbf{A}$, musí mít tato matice nulový determinant:

$$\det\begin{pmatrix} 3 & 1 & 4 \\ 2 & 2 & 5 \\ 3 & a & 1 \end{pmatrix} = -5 - 7a = 0.$$

Takže $a = -\frac{5}{7}$.

Zobecněná rovina: afinní podprostor

Je dán bod $A \in \mathbf{X}$ a lineárně nezávislé vektory $\overrightarrow{u}_1, \overrightarrow{u}_2, \dots, \overrightarrow{u}_k$ v afiním prostoru $(\mathbf{X}, V)$. Množině

$$M = A + \langle \overrightarrow{u}_1, \overrightarrow{u}_2, \dots, \overrightarrow{u}_k \rangle$$

říkáme *zobecněná rovina*. Má dimenzi k.

Zobecněná rovina dimenze 1 je přímka.

Zobecněná rovina dimenze 2 je „skutečná“ rovina.

Pojem *zobecněná rovina* tedy zahrnuje pojmy přímka a rovina dokonce pro lineární prostory libovolné dimenze n. Zobecněná rovina je podprostor v afinním prostoru $(\mathbf{X}, V)$.

Přesněji, při označení $W = \langle \overrightarrow{u}_1, \overrightarrow{u}_2, \dots, \overrightarrow{u}_k \rangle$ je dvojice (M, W) afinní podprostor: operace afinního prostoru jsou na množině M a lineárním podprostoru W uzavřeny.

Vzájemná poloha zobecněných rovin

Označme $U = \langle \overrightarrow{u}_1, \overrightarrow{u}_2, \dots, \overrightarrow{u}_k \rangle$ a $V = \langle \overrightarrow{v}_1, \overrightarrow{v}_2, \dots, \overrightarrow{v}_m \rangle$. Nechť A a B jsou body v afinním prostoru $(\mathbf{X}, V)$ a nechť jsou dány dvě zobecněné roviny $M = A + U$ a $N = B + V$.

- M a N jsou *totožné*, právě když $U = V$ a $A - B \in U$.
- M *je obsažena v* N, právě když $U \subseteq V$ a $A - B \in V$.

Další pojmy se týkají jen zobecněných rovin M a N takových, že žádná není obsažena v druhé.

- M *je rovnoběžná s* N, právě když $U \subseteq V$ nebo $V \subseteq U$.
- Zobecněné roviny M a N *se protínají*, právě když $A - B \in U \cup V$.
- Zobecněné roviny *jsou mimoběžné*, právě když nejsou rovnoběžné a neprotínají se.
- M a N *jsou na sebe kolmé*, právě když $\overrightarrow{u}_i \cdot \overrightarrow{v}_j = 0$ pro všechna $i \in \{1, \dots, k\}$ a $j \in \{1, \dots, m\}$

Kartézský souřadný systém

Nechť $E_n = (\mathbf{X}, V)$ je euklidovský prostor. *Kartézský souřadný systém* tohoto prostoru je souřadnicový systém (O, B) afinního prostoru $(\mathbf{X}, V)$ takový, že báze (B) je ortonormální.

Nechť $(x_1, x_2, \dots, x_n)$ a $(y_1, y_2, \dots, y_n)$ jsou souřadnice vektorů $\overrightarrow{x}$ a $\overrightarrow{y}$ vzhledem ke **kartézkému** souřadnému systému. Pak

$$\overrightarrow{x} \cdot \overrightarrow{y} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n,$$
$$\|\overrightarrow{x}\| = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}.$$

Nechť $(a_1, a_2, \dots, a_n)$ a $(a'_1, a'_2, \dots, a'_n)$ jsou souřadnice bodů A a A' vzhledem ke **kartézkému** souřadnému systému. Pak vzdálenost těchto bodů se počítá „podle Pythagorovy věty“:

$$\rho(A, A') = \|A - A'\| = \sqrt{(a_1 - a'_1)^2 + (a_2 - a'_2)^2 + \cdots + (a_n - a'_n)^2}.$$

Idea analytické geometrie

Geometrické úlohy lze řešit algebraicky přechodem k souřadnicím vzhledem ke kartézskému souřadnému systému.

Geometrické konstrukce pravítkem a kružítkem v rovině sestávají z těchto elementárních úkonů:

- najít průsečík dvou přímek (pokud existuje),
- najít průsečík přímky s kružnicí (pokud existuje),
- najít průsečík dvou kružnic (pokud existuje).

Všechny tyto úkoly lze převést na výpočet souřadnic hledaných průsečíků vzhledem ke kartézskému souřadnicovému systému, pokud jsou dány souřadnice výchozích objektů (souřadnice bodu a směrového vektoru přímky, souřadnice středu a hodnota poloměru kružnice).

Příklad: průsečík přímek

V E_2 jsou dány přímky $p = (1,2) + \langle (3,4) \rangle$ a $q = (2,0) + \langle (1,3) \rangle$. Vektory a body jsou dány v kartézských souřadnicích. Najdeme průsečík přímek p, q.

Protože směrové vektory $(3,4)$ a $(1,3)$ jsou lineárně nezávislé, přímky se protínají (v E_2 neexistují mimoběžky). Průsečík najdeme v místě, pro které nastává rovnost:

$$(1,2) + t\,(3,4) = (2,0) + u\,(1,3)$$

To vede na soustavu dvou lineárních rovnic s neznámými t, u. Ta má řešení $t = 1$, $u = 2$, takže průsečík je v bodě

$$P = (1,2) + 1 \cdot (3,4) = (4,6).$$

Příklad: průsečík přímky a kružnice

V E_2 je dána přímka $p = (1,2) + \langle (3,4) \rangle$ a kružnice k se středem $(1,1)$ a poloměrem 3. Najdeme jejich průsečíky.

Vzdálenost středu kružnice od bodu $(1,2) + t\,(3,4)$ na přímce je

$$f(t) = \sqrt{(1 + 3t - 1)^2 + (2 + 4t - 1)^2} = \sqrt{25t^2 + 8t + 1}$$

Průsečík nastává v místě, kde $(f(t))^2 = 3^2$, neboli

$$25t^2 + 8t - 8 = 0, \qquad t_{1,2} = \frac{-8 \pm \sqrt{54}}{25},$$

takže jsme našli dva průsečíky:

$$(1,2) + \frac{-8 + \sqrt{54}}{25}(3,4) = \left(\frac{1}{25} + \frac{3\sqrt{54}}{25}, \quad \frac{18}{25} + \frac{4\sqrt{54}}{25} \right),$$

$$(1,2) + \frac{-8 - \sqrt{54}}{25}(3,4) = \left(\frac{1}{25} - \frac{3\sqrt{54}}{25}, \quad \frac{18}{25} - \frac{4\sqrt{54}}{25} \right).$$

Příklad: průsečík dvou kružnic

Jsou dány kružnice k_1 se středem $(1,1)$ a poloměrem 3 a kružnice k_2 se středem $(3,4)$ a poloměrem 2. Najdeme jejich průsečíky.

Průsečík má souřadnice (x, y), které vyhovují dvěma rovnicím:

$$(x-1)^2 + (y-1)^2 = 3^2$$
$$(x-3)^2 + (y-4)^2 = 2^2$$

Odečtením rovnic dostáváme lineární rovnici $2x + 3y = 14$. Dosazením $x = 7 - \frac{3}{2}y$ do první rovnice dostáváme kvadratickou rovnici $13y^2 - 80y + 112 = 0$, která má řešení $y_1 = 4, y_2 = \frac{28}{13}$. Použitím vzorce $x = 7 - \frac{3}{2}y$ dostáváme $x_1 = 1$ a $x_2 = \frac{49}{13}$, takže hledané průsečíky jsou

$$P_1 = (1,4), \qquad P_2 = \left(\frac{49}{13}, \frac{28}{13} \right).$$

Nekopírovat vždy konstrukci výpočtem

Ne vždy se vyplatí postupovat stejně jako při řešení úloh pravítkem a kružítkem jen výpočtem souřadnic postupně vznikajících průsečíků.

Například sestrojení kolmice na danou přímku p procházející daným bodem P uděláme kružítkem tak, že zapíchneme kružítko s dostatečně velkým poloměrem do P a najdeme průsečíky na p. Pak píchneme kružítko do těchto průsečíků se shodným poloměrem větším než polovina vzdálenosti průsečíků a najdeme průsečíky kružnic. Jejich spojnice je hledaná kolmice.

Analyticky ale stačí kolmici vyjádřit jako $P + \langle \overrightarrow{s}^{\perp} \rangle$, přičemž $\overrightarrow{s}^{\perp}$ je vektor kolmý na směrový vektor přímky p. Kolmý vektor k vektoru v rovině $\overrightarrow{s} = (u, v)$ je vektor $\overrightarrow{s}^{\perp} = (-v, u)$, protože skalární součin těchto dvou vektorů je nulový.

Dva popisy zobecněné roviny v $E_n,\ n \geq 3$

Zobecněná rovina M může být zadána dvěma způsoby:

- Bodem a směrovými vektory: $M = A + \langle \vec{u}_1, \vec{u}_2, \ldots, \vec{u}_k \rangle$.
- Soustavou lineárních rovnic $\mathbf{Bx} = \mathbf{b}$ takovou, že souřadnice všech bodů zobecněné roviny M tvoří množinu jejích řešení. Tuto soustavu nazýváme *soustavou zobecněné roviny M*.

Tyto dva popisy umíme převádět jeden na druhý:

- Je-li dána soustava zobecněné roviny, pak její směrové vektory jsou bázové vektory přidružené homogenní soustavy $\mathbf{Bx} = \mathbf{o}$ a bod A je partikulární řešení soutavy.
- Je-li dána zobecněná rovina směrovými vektory, pak zapíšeme jejich souřadnice do řádků matice $\mathbf{A}$ a vyřešíme $\mathbf{Ax} = \mathbf{o}$. Bázi řešení zapíšeme do řádků matice $\mathbf{B}$ a pravou stranu zjistíme dosazením souřadnic bodu A za neznámý vektor $\mathbf{x}$.

Příklady popisů přímky a roviny v E_3

Přímka: Je popsána bodem a směrovým vektorem $A + \langle \vec{s} \rangle$. Často se tento popis rozepisuje do souřadnic jako

$$x = a_1 + t\,s_1, \quad y = a_2 + t\,s_2, \quad z = a_3 + t\,s_3, \quad t \in \mathbf{R}.$$

Přímku můžeme také popsat soustavou dvou rovnic $\mathbf{Bx} = \mathbf{b}$. Není to typické, ale předvedeme si to. Bázi řešení soustavy s jednou rovnicí $s_1x + s_2y + s_3z = 0$ označíme $(u_1, u_2, u_3), (v_1, v_2, v_3)$. Hledaná soustava má pak matici obsahující tyto dva řádky a pravou stranu:

$$b_1 = u_1a_1 + u_2a_2 + u_3a_3, \quad b_2 = v_1a_1 + v_2a_2 + v_3a_3.$$

Rovina: Je popsána dvěma směrovými vektory $A + \langle \vec{u}, \vec{v} \rangle$. Vyřešením homogenní soustavy dvou rovnic se souřadnicemi těchto vektorů v řádcích matice dostáváme bázový vektor (n_1, n_2, n_3). Rovinu pak můžeme popsat *rovnicí roviny*

$$n_1x + n_2y + n_3z = d, \quad \text{kde} \quad d = n_1a_1 + n_2a_2 + n_3a_3.$$

Průsečíky zobecněných rovin

Dvě zobecněné roviny se mohou protínat. Průnik pak tvoří bod nebo zobecněnou rovinu. Jak tento průnik nalezneme?

Sestavíme soustavu první zob. roviny $\mathbf{Bx} = \mathbf{b}$ a druhé zob. roviny $\mathbf{B}'\mathbf{x} = \mathbf{b}'$. Řešíme pak soustavu, která vznikne sloučením těchto dvou soustav. Soustava má rozšířenou matici

$$\left(\begin{array}{c|c} \mathbf{B} & \mathbf{b} \\ \mathbf{B}' & \mathbf{b}' \end{array}\right)$$

a její řešení popisuje průnik daných zobecněných rovin.

Příklad: Průnik dvou rovin $ax + by + cz = d$ a $a'x + b'y + c'z = d'$ najdeme jako řešení soustavy

$$\begin{aligned} a\,x + b\,y + c\,z &= d \\ a'x + b'y + c'z &= d' \end{aligned}$$

Příklad: průsečík přímky s rovinou

Je dána přímka $p = (1,2,3) + \langle (2,2,1) \rangle$ a rovina $M = (2,3,4) + \langle (3,3,1), (3,4,3) \rangle$ v E_3. Najdeme jejich průsečík.

Podle předchozí stránky bychom mohli přímku p popsat dvěma rovnicemi a rovinu M třetí rovnicí a pak vyřešit soutavu těchto tří rovnic. Ovšem v tomto případě se většinou postupuje jinak:

Rovnice roviny M má tvar $5x - 6y + 3z = 4$ a přímka p má parametrické vyjádření $x = 1 + 2t$, $y = 2 + 2t$, $z = 3 + t$. Dosadíme parametrické vyjádření přímky do rovnice roviny:

$$5\,(1 + 2t) - 6\,(2 + 2t) + 3\,(3 + t) = 4.$$

Tato rovnice s jednou proměnnou má řešení $t = 2$. Průsečík je

$$P = (1,2,3) + 2\,(2,2,1) = (5,6,5).$$

Kolmice k zobecněné rovině v E_n

Je dána zobecněná rovina dimenze k:

$$M = A + \langle \vec{u}_1, \vec{u}_2, \ldots, \vec{u}_k \rangle.$$

Kolmice k M vedená z bodu B je zobecněná rovina N dimenze $n-k$, kterou lze zapsat ve tvaru

$$N = B + \langle \vec{u}_1, \vec{u}_2, \ldots, \vec{u}_k \rangle^\perp = B + \langle \vec{v}_1, \vec{v}_2, \ldots, \vec{v}_{n-k} \rangle.$$

přičemž vektory $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_{n-k}$ získáme následovně: Zvolíme kartézský souřadný systém a souřadnice vektorů vzhledem k tomuto souřadnému systému ztotožníme s vektory samotnými. Vektory $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_{n-k}$ pak tvoří bázi řešení homogenní soustavy $\mathbf{Ax} = \mathbf{o}$, kde matice $\mathbf{A}$ obsahuje v řádcích vektory $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_k$.

Příklady: V euklidovském prostoru E_3 je kolmice k rovině přímka a kolmice ke přímce je rovina.

Kolmice ve 2D a 3D

Kolmici v E_n počítáme řešením homogenní soustavy, jak bylo zmíněno na předchozí stránce. To je univerzální postup.

V případě E_2 a E_3 jsou ještě jiné postupy:

- V E_2 platí: $\langle (a,b) \rangle^\perp = \langle (-b,a) \rangle$.
- V E_3 platí pro lin. nezávislé vektory:

  $$\langle \vec{u}, \vec{v} \rangle^\perp = \langle \vec{u} \times \vec{v} \rangle,$$

  kde symbolem $\times$ je označem *vektorový součin*. O něm si povíme více později.

Kolmý průmět bodu do zobecněné roviny

Je dána zobecněná rovina $M = A + \langle \vec{u}_1, \vec{u}_2, \ldots, \vec{u}_k \rangle$ a bod B (typicky mimo M). Najdeme bod $B' \in M$ takový, že $B - B'$ je vektor kolmý na M. Bodu B' říkáme *kolmý průmět bodu B do zobecněné roviny M*.

Bod B' lze najít takto: sestrojíme kolmici $K = B + \langle \vec{u}_1, \vec{u}_2, \ldots, \vec{u}_k \rangle^\perp$. Průnik $M \cap K$ obsahuje jediný bod B'.

Jiný postup*: skalárním součinem lze počítat kolmý průmět vektoru na vektor. Označme symbolem p_i kolmý průmět vektoru $B-A$ na vektor $\vec{u}_i$. Pak je $B' = A + \sum p_i\,(\vec{u}_i / \|\vec{u}_i\|)$.

Pozorování: V bodě B' má zobecněná rovina M nejmenší vzdálenost od bodu B.

Důkaz: Je-li $C \in M$, pak $BB'C$ tvoří pravoúhlý trojúhelník a můžeme použít Pythagorovu větu.

Kolmý průmět zob. roviny do zob. roviny

Představme si, že například hledáme kolmý průmět přímky do roviny. Nebo děláme něco podobného ve více dimenzích…

Kolmý průmět zob. roviny $N = B + \langle \vec{v}_1, \vec{v}_2, \ldots, \vec{v}_m \rangle$ do zob. roviny $M = A + \langle \vec{u}_1, \vec{u}_2, \ldots, \vec{u}_k \rangle$ spočítáme v následujících krocích:

- Najdeme $\langle \vec{u}_1, \vec{u}_2, \ldots, \vec{u}_k \rangle^\perp = \langle \vec{w}_1, \vec{w}_2, \ldots, \vec{w}_{n-k} \rangle$.
- Označme $K = B + \langle \vec{v}_1, \vec{v}_2, \ldots, \vec{v}_m, \vec{w}_1, \vec{w}_2, \ldots, \vec{w}_{n-k} \rangle$. Je to zobecněná rovina, která je nejmenší taková, že obsahuje zobecněnou rovinu N a současně obsahuje směr kolmý na M.
- Hledaný kolmý průmět je průnik $M \cap K$.

Příklad: Kolmý průmět

Je dána přímka $p = (1,2,3) + \langle(5,2,2)\rangle$. Najdeme kolmý průmět této přímky do roviny $M = (2,2,1) + \langle(1,3,4),(3,2,6)\rangle$. Souřadnice jsou dány vzhledem ke kartézskému souřadnému systému.

Řešením homogenní soustavy s maticí

$$\begin{pmatrix} 1 & 3 & 4 \\ 3 & 2 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 4 \\ 0 & 7 & 6 \end{pmatrix}$$

je $\langle(10,6,-7)\rangle$, takže $\langle(1,3,4),(3,2,6)\rangle^\perp = \langle(10,6,-7)\rangle$. Kolmá rovina k M obsahující p je $K = (1,2,3) + \langle(5,2,2),(10,6,-7)\rangle$. Rovnice roviny M je $10x + 6y - 7z = 25$ a rovnice K je $-26x + 55y + 10z = 114$. Hledaný průmět je řešení soustavy s maticí

$$\left(\begin{array}{ccc|c} 10 & 6 & -7 & 25 \\ -26 & 55 & 10 & 114 \end{array}\right) \sim \left(\begin{array}{ccc|c} 10 & 6 & -7 & 25 \\ 0 & 353 & -41 & 895 \end{array}\right).$$

Hledaný průmět je $p' = (-524/41,\ 0,\ -895/41) + \langle(445,\ 41,\ 353)\rangle$.

Determinant měří objem rovnoběžnostěnu

Nechť $\overrightarrow{v}_1, \overrightarrow{v}_2, \ldots, \overrightarrow{v}_n$ jsou vektory, které tvoří hrany pomyslného n-dimenzionálního rovnoběžnostěnu. Vektory tvoří jen hrany, které se potkávají ve společném vrcholu. Ostatní hrany rovnoběžnostěnu je třeba dorýsovat doplněním na rovnoběžníky.

Tvrzení: Zapíšeme-li do sloupců matice $\mathbf{A}$ souřadnice vektorů $\overrightarrow{v}_i$ vzhledem k ortonormální bázi (B), pak absolutní hodnota determinantu matice $\mathbf{A}$ je rovna objemu zmíněného rovnoběžnostěnu.

Idea důkazu*: Jsou-li vektory LZ, pak je zřejmě objem nulový a je $\det\mathbf{A} = 0$. Jsou-li $\overrightarrow{v}_i$ LN, tvoří bázi a je možné ji Schmidtovým ortogonalizačním procesem upravit na ortonormální bázi (C). Napíšeme do sloupců matice $\mathbf{R}$ souřadnice $\overrightarrow{v}_i$ vzhledem k (C). Pak $\det\mathbf{R}$ je roven objemu rovnoběžnostěnu (důkaz indukcí, v indukčním kroku se použije vzorec „základna krát výška“). Matice přechodu od (B) k (C) je ortogonální a je tedy

$$\det\mathbf{A} = \det(\mathbf{P}_{B\to C}\cdot\mathbf{R}) = \det\mathbf{P}_{B\to C}\det\mathbf{R} = \pm 1\cdot\det\mathbf{R}$$

Příklady

Souřadnice uvedených bodů jsou v těchto příkladech vzhledem ke kartézskému souřadnému systému.

Plocha rovnoběžníka s vrcholy $(0,0)$, (a,b) (c,d), $(a+c,b+d)$ je rovna

$$\left|\det\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right| = |ad-bc|,$$

Objem čtyřstenu s vrcholy $(0,0,0)$, (a_1,a_2,a_3), (b_1,b_2,b_3), (c_1,c_2,c_3) je roven

$$\frac{1}{6}\left|\det\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}\right|,$$

protože čtyřstěn má objem roven jedné šestině objemu rovnoběžnostěnu.

Souřadnice můžeme zapsat i do řádků, protože $\det\mathbf{A} = \det\mathbf{A}^T$.

Orientace lineárního prostoru

V lineárním prostoru zvolíme jednu uspořádanou bázi (B) a prohlásíme ji kladně orientovanou. Všechny báze (C), pro které je $\det\mathbf{P}_{B\to C} > 0$, nazveme také kladně orientované. Všechny báze (C'), pro které je $\det\mathbf{P}_{B\to C'} < 0$, nazveme záporně orientované.

Obvyklá úmluva pro E_2: kladně orientovaná báze má druhý bázový vektor směřující vlevo od prvního.

Obvyklá úmluva pro E_3: když se na bázi díváme z vhodného místa, pak kladně orientovaná báze má první vektor orientovaný k nám, druhý doprava od nás a třetí nahoru.

Pozorovnání: determinant použitý při výpočtu objemu rovnoběžnostěnu je záporný, když souřadnice vektorů $\overrightarrow{v}_1, \overrightarrow{v}_2, \ldots, \overrightarrow{v}_n$ jsou zapsány vzhledem ke kladně orientované ortonormální bázi a vektory $\overrightarrow{v}_1, \overrightarrow{v}_2, \ldots, \overrightarrow{v}_n$ samotné tvoří záporně orientovanou bázi.

Speciální vlastnosti v E_3

- Je možné definovat *vektorový součin*.
- Kolmice k rovině je přímka, směrový vektor této kolmice je *normálový vektor roviny*.
- Normálový vektor je možné hledat pomocí vektorového součinu.
- Rovina je dána jedinou rovnicí se třemi neznámými, koeficienty této rovnice jsou souřadnice jejího normálového vektoru.

Vektorový součin

Definice: Vektorový součin dvou vektorů $\overrightarrow{u}$ a $\overrightarrow{v}$ z E_3 značíme $\overrightarrow{u}\times\overrightarrow{v}$ a je to:

- nulový vektor, pokud jsou $\overrightarrow{u}$ a $\overrightarrow{v}$ lineárně závislé, jinak:
- vektor kolmý na rovinu $\langle\overrightarrow{u},\overrightarrow{v}\rangle$ s velikostí plochy rovnoběžníka mezi $\overrightarrow{u}$ a $\overrightarrow{v}$. Báze $(\overrightarrow{u},\overrightarrow{v},\overrightarrow{u}\times\overrightarrow{v})$ je kladně orientovaná.

Pozorování: Vektorový součin je definován jednoznačně.
Platí $\|\overrightarrow{u}\times\overrightarrow{v}\| = \|\overrightarrow{u}\|\|\overrightarrow{v}\|\sin\alpha$, kde α je úhel mezi vektory $\overrightarrow{u}$ a $\overrightarrow{v}$.

Věta: Jsou-li (u_1,u_2,u_3) a (v_1,v_2,v_3) souřadnice vektorů $\overrightarrow{u}$ a $\overrightarrow{v}$ vzhledem ke kladně orientované ortonormální bázi, pak $\overrightarrow{u}\times\overrightarrow{v}$ má vzhledem k této bázi souřadnice:

$$\left(\begin{vmatrix} u_2 & u_3 \\ v_2 & v_3 \end{vmatrix}, -\begin{vmatrix} u_1 & u_3 \\ v_1 & v_3 \end{vmatrix}, \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix}\right)$$

Důkaz*: technický, viz skriptum.

Příklad: normálový vektor roviny

Je dána rovina $(2,2,2) + \langle(1,2,3),\ (3,1,1)\rangle$. Najedeme její normálový vektor. Souřadnice jsou uvedeny vzhledem ke kladně orientovanému kartézskému souřadnému systému.

Normálový vektor je roven vektorovému součinu $(1,2,3)\times(3,1,1)$, protože ten je (podle definice) kolmý na oba směrové vektory. Podle věty o souřadnicích vektorového součinu je

$$(1,2,3)\times(3,1,1) = \left(\begin{vmatrix} 2 & 3 \\ 1 & 1 \end{vmatrix}, -\begin{vmatrix} 1 & 3 \\ 3 & 1 \end{vmatrix}, \begin{vmatrix} 1 & 2 \\ 3 & 1 \end{vmatrix}\right) = (-1,8,-5)$$

Rovnice roviny tedy je $-x + 8y - 5z = 4$.

Jiná možnost, jak najdeme normálový vektor: vyřešíme homogenní soustavu s maticí

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 1 \end{pmatrix}.$$

Příklad: rovina daná třemi body

Jsou-li dány tři body A, B, C, které neleží ve společné přímce, pak jimi prochází jediná rovina $A + \langle(B-A),(C-A)\rangle$. Normálový vektor roviny je $(B-A)\times(C-A)$.

Třeba jsou dány body $(1,1,2),(2,3,5),(4,2,3)$ v kartézských souřadnicích. Pak rovina je dána vzorcem:

$$(1,1,2) + \langle(1,2,3),\ (3,1,1)\rangle$$

Protože $(1,2,3)\times(3,1,1) = (-1,8,-5)$, má rovina tento normálový vektor. Má tedy rovnici

$$-x + 8y - 5z = d, \qquad \text{přitom} \quad d = -1 + 8\cdot 1 - 5\cdot 2 = -3.$$

Příklad: vzdálenost bodu od přímky

Můžeme najít kolmý průmět bodu B do přímky (označíme B') a dále spočítáme velikost vektoru $B-B'$. Ovšem v E_3 máme vektorový součin a můžeme úlohu řešit ještě jinak (efektivněji):

Vzdálenost bodu B od přímky $A+\langle\overrightarrow{s}\rangle$ je výška rovnoběžníka vymezeného vektory $B-A$, $\overrightarrow{s}$ a ta je rovna ploše rovnoběžníka dělená velikostí základny. Vzdálenost bodu B od přímky tedy je

$$\frac{\|(B-A)\times\overrightarrow{s}\|}{\|\overrightarrow{s}\|}.$$

Příklad: vzdálenost bodu od roviny

Můžeme najít kolmý průmět bodu B do roviny (označíme B') a dále spočítáme velikost vektoru $B-B'$. Ovšem v E_3 máme vektorový součin a můžeme úlohu řešit ještě jinak (efektivněji):

Vzdálenost bodu B od roviny $A+\langle\overrightarrow{u},\overrightarrow{v}\rangle$ je rovna výšce rovnoběžnostěnu se stranami $B-A$, $\overrightarrow{u}$, $\overrightarrow{v}$ s podstavou $\overrightarrow{u}$, $\overrightarrow{v}$. Tato výška je rovna objemu tohoto rovnoběžnostěnu děleno plocha podstavy. Vzdálenost bodu B od roviny tedy je

$$\frac{\det\mathbf{A}}{\|\overrightarrow{u}\times\overrightarrow{v}\|},$$

kde matice $\mathbf{A}$ obsahuje v řádcích (nebo ve sloupcích) souřadnice vektorů $A-B$, $\overrightarrow{u}$, $\overrightarrow{v}$ vzhledem k nějaké ortonormální bázi.

Příklad: vzdálenost mimoběžek

Vzdálenost mimoběžek $A+\langle\overrightarrow{u}\rangle$ a $B+\langle\overrightarrow{v}\rangle$ je rovna výšce rovnoběžnostěnu vymezeného vektory $B-A$, $\overrightarrow{u}$, $\overrightarrow{v}$ se základnou $\overrightarrow{u}$, $\overrightarrow{v}$. Takže vzdálenost je rovna objemu tohoto rovnoběžnostěnu deleno plochou základny:

$$\frac{\det\mathbf{A}}{\|\overrightarrow{u}\times\overrightarrow{v}\|},$$

kde matice $\mathbf{A}$ obsahuje v řádcích (nebo ve sloupcích) souřadnice vektorů $A-B$, $\overrightarrow{u}$, $\overrightarrow{v}$ vzhledem k nějaké ortonormální bázi.

Příklad: kolmice v E_3

- Kolmice k přímce je rovina, která má normálový vektor rovný směrovému vektoru přímky.
- Kolmice k rovině je přímka, která má směrový vektor rovný normálovému vektoru roviny.

Rovina daná rovnicí $ax+by+cz=d$ má normálový vektor (a,b,c), takže přechod od roviny ke kolmé přímce nebo od přímky ke kolmé rovině je snadný.

Úhly mezi přímkami a rovinami

Úhel ϕ mezi vektory $\overrightarrow{u}$ a $\overrightarrow{v}$ vypočítáme ze vzorce pro skalární součin

$$\cos\phi=\frac{\overrightarrow{u}\cdot\overrightarrow{v}}{\|\overrightarrow{u}\|\|\overrightarrow{v}\|},\quad\text{tj.}\quad\phi=\arccos\frac{\overrightarrow{u}\cdot\overrightarrow{v}}{\|\overrightarrow{u}\|\|\overrightarrow{v}\|}.$$

- Úhel mezi dvěma přímkami je úhlel mezi směrovými vektory. Pokud $\phi>90^\circ$, je hledaný úhel $180^\circ-\phi$ (nebo ve vzorci v čitateli použít absolutní hodnotu).
- Úhel mezi rovinami je úhel mezi jejich normálovými vektory. Pokud $\phi>90^\circ$, je hledaný úhel $180^\circ-\phi$ (nebo ve vzorci v čitateli použít absolutní hodnotu).
- Úhel mezi přímkou a rovinou je 90° mínus úhel mezi směrovým vektorem přímky a normálovým vektorem roviny (ve vzorci v čitateli je třeba použít absolutní hodnotu).

Příklad: plocha trojúhelníka ABC

Trojúhelník má plochu poloviční ploše rovnoběžníka.

- V E_2 spočítáme plochu rovnoběžníka jako „objem rovnoběžnostěnu v E_2“, tedy spočítáme absolutní hodnotu determinantu matice $\mathbf{A}$, která obsahuje ve sloupcích souřadnice vektorů $B-A$, $C-A$ vzhledem k ortonormální bázi.

Příklad: $A=(1,2)$, $B=(3,4)$, $C=(5,8)$. Plocha trojúhelníka je:

$$S_\triangle=\frac{1}{2}\left|\det\begin{pmatrix}2&4\\2&6\end{pmatrix}\right|=2$$

- V E_3 spočítáme plochu rovnoběžníka jeko velikost vektorového součinu vektorů $B-A$, $C-A$.

Příklad: $A=(1,2,2)$, $B=(2,3,4)$, $C=(7,8,9)$.

$$S_\triangle=\frac{1}{2}\|(1,1,2)\times(6,6,7)\|=\frac{1}{2}\|(-5,5,0)\|=\frac{5\sqrt{2}}{2}.$$

Úvaha*: k-dimensionální objem v E_n.

Jak spočítat např. plochu rovnoběžníka v E_4? Tam to není ani objem rovnoběžnostěnu, ani nemáme možnost použít vektorový součin. Odpověď najdeme v důkazu ze stránky [26].

Úloha: Jsou dány lineárně nezávislé vektory $\overrightarrow{v}_1,\overrightarrow{v}_2,\ldots,\overrightarrow{v}_k$ v E_n, $k\le n$. Máme najít k-dimensionální objem v E_n.

Řešení: Vektory doplníme na bázi $\overrightarrow{v}_1,\overrightarrow{v}_2,\ldots,\overrightarrow{v}_k,\ldots,\overrightarrow{v}_n$ a zapíšeme jejich souřadnice do sloupců matice $\mathbf{A}$. Provedeme QR rozklad $\mathbf{A}=\mathbf{QR}$. Matici $\mathbf{R}$ „zmenšíme“ na matici $\mathbf{R}_k$, která obsahuje jen prvních k řádků a k sloupců. Hledaný k dimenzionální objem je roven $\det\mathbf{R}_k$.

Poznámka: doplnění na bázi není prakticky potřeba dělat. Software dokáže provést i neúplný QR rozklad obdélníkové matice $\mathbf{A}=\mathbf{Q}_k\mathbf{R}_k$. Zde matice $\mathbf{A}$ obsahuje ve sloupcích jen souřadnice vektorů $\overrightarrow{v}_1,\overrightarrow{v}_2,\ldots,\overrightarrow{v}_k$.

Grupy, tělesa

- grupa: množina s jednou „rozumnou“ operací
- příklady grup, vlastnosti
- těleso: množina se dvěma „rozumnými“ operacemi
- příklady těles, vlastnosti, charakteristika tělesa
- lineární prostor nad tělesem
- polynomy nad tělesem
- polynomy modulo polynom

Reálná čísla, inspirace

Na množině $\mathbf{R}$ reálných čísel máme operaci +. Přitom platí:

- $x+(y+z)=(x+y)+z$ … (asociativní zákon),
- existuje prvek $0\in\mathbf{R}$ takový, že $0+x=x+0=x\ \ \forall x\in\mathbf{R}$ … (existence neutrálního prvku),
- $\forall x\in\mathbf{R}$ existuje opačný prvek $y\in\mathbf{R}$ tak, že $x+y=y+x=0$ … (existence opačného prvku, značíme $y=-x$),
- $x+y=y+x$ … (komutativní zákon).

Na množině $\mathbf{R}$ máme také operaci $\cdot$, která splňuje:

- $x\cdot(y\cdot z)=(x\cdot y)\cdot z$ … (asociativní zákon),
- existuje prvek $1\in\mathbf{R}$ takový, že $1\cdot x=x\cdot 1=x\ \ \forall x\in\mathbf{R}$ … (existence jednotkového prvku),
- $\forall x\in\mathbf{R}, x\neq 0$ existuje prvek $y\in\mathbf{R}$ tak, že $x\cdot y=y\cdot x=1$ … (existence inverzního prvku, značíme $y=x^{-1}$),
- $x\cdot y=y\cdot x$ … (komutativní zákon).

Množina s jednou operací: grupoid, grupa

Definice: Předpokládejme množinu G a na ní operaci $\circ$.
Dále uvažujme vlastnosti:

(1) $x\circ(y\circ z)=(x\circ y)\circ z\ \ \forall x,y,z\in G$ … (asociativní zákon),

(2) existuje prvek $e\in G$ takový, že $e\circ x=x\circ e=x\ \ \forall x\in G$ … (existence neutrálního/jednotkového prvku),

(3) $\forall x\in G$ existuje prvek $y\in G$ tak, že $x\circ y=y\circ x=e$ … (existence opačného/inverzního prvku),

(4) $x\circ y=y\circ x\ \ \forall x,y\in G$ … (komutativní zákon).

- Množina G s operací $\circ$ se nazývá *grupoid*.
- Grupoid, kde platí asociativní zákon (1), se nazývá *pologrupa*.
- Pologrupa s vlastnostmi (2) a (3) se nazývá *grupa*.
- Grupa, kde platí komutativní zákon (4), je *komutativní grupa*.

Příklady

- $\mathbf{R}$ s operací + je komutativní grupa.
- $\mathbf{R}$ s operací $\cdot$ je pologrupa, $\mathbf{R}\setminus\{0\}$ je komutativní grupa.
- $\mathbf{Q}$, $\mathbf{Z}$ s operací + jsou komutativní grupy (podgrupy grupy $\mathbf{R}$ s +).
- $\mathbf{Z}\setminus\{0\}$ s operací $\cdot$ není grupa (je to pologrupa).
- Množina $\{e\}$ s operací $\circ$, pro kterou $e\circ e=e$, je grupa.
- Množina regulárních matic s maticovým násobením je grupa.
- Množina ctvercových matic s násobením je pologrupa.
- Množina funkcí $\mathbf{R}\to\mathbf{R}$ prostých a na s operací skládání je grupa.
- Množina bijektivních zobrazení $M\to M$ s op. skládání je grupa.
- Množina permutací s operací skládání je grupa
- Množina $\{0,1,\ldots,m-1\}$ s operací „+ modulo m“ je grupa.

Terminologie: jednotkový/neutrální prvek

Operace komutativní grupy bývá někdy označena symbolem +. V takovém případě prvek e z vlastnosti (2) grupy se nazývá *neutrální prvek* a prvek y z vlastnosti (3) se nazývá *opačný prvek*.

Neutrální prvek se v tomto případě značí symbolem 0 a opačný prvek k prvku x se značí $-x$. Operaci $a+(-b)$ značíme stručněji $a-b$ a říkáme ji *odečítání*.

Je-li operace grupy označena symbolem $\cdot$ (krát), pak prvku e z vlastnosti (2) grupy říkáme *jednotkový prvek* a prvku y z vlastnosti (3) říkáme *inverzní prvek*.

Jednotkový prvek v takovém případě značíme symbolem 1 a inverzní prvek k prvku x značíme x^{-1}. Je-li grupa komutativní, pak operaci $a\cdot b^{-1}$ značíme stručněji a/b a říkáme ji *dělení*.

Základní vlastnosti grupy

- Neutrální/jednotkový prvek je v grupě jediný.
  Kdyby byly dva e,f, pak $e=e\circ f=f$, takže nemohou být různé.
- Opačný/inverzní prvek existuje ke každému prvku $x\in G$ jediný.
  Kdyby existovaly y_1,y_2 tak, že $y_1\circ x=e$, $x\circ y_2=e$, pak
  $$y_1=y_1\circ e=y_1\circ(x\circ y_2)=(y_1\circ x)\circ y_2=e\circ y_2=y_2.$$
- Pologrupa G je grupou právě když pro každé $a,b\in G$ existují řešení rovnic
  $$a\circ x=b,\qquad y\circ a=b.$$
  Náznak důkazu: Je-li G grupa, pak $x=a^{-1}\circ b$ a $y=b\circ a^{-1}$ jsou řešení uvedených rovnic. Umíme-li řešit tyto rovnice, pak jednotkový prvek e je řešení rovnice $a\circ e=a$ (je třeba ukázat, že to nezávisí na volbě a). Dále inverzní prvek k a je řešení $a\circ x=e$ (je třeba ukázat, že je to totéž, jako řešení rovnice $y\circ a=e$).

Vlastnosti inverzních prvků grupy

- Jednotkový prvek e má inverzní prvek e (je inverzní sám sobě).
  Skutečně: $e=e\circ e$.
- Je-li a^{-1} invernzí prvek k a, je-li dále b^{-1} inverzní prvek k b, pak inverzní prvek k $a\circ b$ je tvaru $b^{-1}\circ a^{-1}$.
  Skutečně:
  $$(b^{-1}\circ a^{-1})\circ(a\circ b)=b^{-1}\circ(a^{-1}\circ a)\circ b=b^{-1}\circ e\circ b=b^{-1}\circ b=e,$$
  $$(a\circ b)\circ(b^{-1}\circ a^{-1})=a\circ(b\circ b^{-1})\circ a^{-1}=a\circ e\circ a^{-1}=a\circ a^{-1}=e.$$
- Je-li a^{-1} inverzní k a, pak a je inverzní k a^{-1}.
  Skutečně: $a^{-1}\circ a=a\circ a^{-1}=e$.

Mocnina

Je-li $a\in G$, pak symbolem a^k označme prvek $a\circ a\circ\cdots\circ a$ (k-krát).

Tvrzení: Je-li G konečná komutativní grupa s n prvky, pak pro každé $a\in G$ je
$$a^n=e.$$
Důkaz: Označme $G=\{g_1,g_2,\ldots,g_n\}$ a zvolme $a\in G$. Ukážeme, že
$$\{g_1,g_2,\ldots,g_n\}\ =\ \{a\circ g_1,a\circ g_2,\ldots,a\circ g_n\}.$$
Zobrazení, které přiřadí prvku g_i prvek $a\circ g_i$ je prosté, protože, pokud $a\circ g_i=a\circ g_j$, pak po aplikaci a^{-1} zleva máme $g_i=g_j$. Uvedené množiny jsou tedy stejně početné a tedy stejné a mají tedy stejný součin všech prvků:
$$a\circ g_1\circ a\circ g_2\circ\cdots\circ a\circ g_n\ =\ g_1\circ g_2\circ\cdots\circ g_n=u$$
Díky komutativnímu zákonu se rovnost dá přepsat na $a^n\circ u=u$ a dokazovaná rovnost plyne aplikací u^{-1} na obě strany rovnosti.

Podgrupy

Podgrupa P je podmnožina grupy G se stejnou operací, která je sama grupou. Tj. P musí mít (stejný) jednotkový prvek a každý prvek z P musí mít inverzi v P.

Příklady:

- $\mathbf{Q}$ a $\mathbf{Z}$ je podgrupa grupy $\mathbf{R}$ s operací +,
- $\mathbf{Q}\setminus\{0\}$ je podgrupa grupy $\mathbf{R}\setminus\{0\}$ s operací $\cdot$,
- symetrické matice tvoří podgrupu čtvercových matic s operací +,
- matice s det = 1 tvoří podgrupu regulárních matic s operací $\cdot$,
- Sudá čísla tvoří podgrupu $\mathbf{Z}$ s operací +,
- Kladná čísla tvoří podgrupu grupy $\mathbf{R}$ s operací $\cdot$.

Vlastnosti pologrupy „krát modulo m“

Předpokládejme množinu $\{0,1,2,\dots,m-1\}$ s operací „krát modulo m“, tj. $a \circ b = a \cdot b$ pro $a \cdot b < m$, jinak $a \circ b$ je zbytek po dělení čísla $a \cdot b$ číslem m. Je to pologrupa. Tato pologrupa má jednotkový prvek: 1.

Tvrzení: je-li m složené, tj. $m = n_1 \cdot n_2$, $(n_1 \neq 1,\ n_2 \neq 1)$ pak číslo n_1 nemá inverzní prvek.

Důkaz: $v \circ n_1 = z$, tj. $vn_1 = kn_1n_2 + z$, tj. $z = n_1(v - kn_2)$, takže z musí být násobek n_1 a nemůže tedy být roven jedné.

Tvrzení: je-li m prvočíslo, pak množina $\{1,2,\dots,m-1\}$ s operací $\circ$ je grupa.

Dokážeme*, že každý nenulový prvek a má inverzi. Platí totiž, že $\{a, 2 \circ a, \dots, (m-1) \circ a\} = \{1, \cdots, m-1\}$. Důvod: pro $k_1 \neq k_2$ je $a \circ k_1 \neq a \circ k_2$, protože z $a(k_1 - k_2) = km$ plyne $k_1 - k_2 = k'm$ (je a nesoudělné s m). Protože $0 \leq k_1 - k_2 < m$, musí $k' = 0$, takže $k_1 = k_2$.

Malá Fermatova věta

Nechť p je prvočíslo, nechť a je přirozené číslo, $a < p$. Pak

$$a^{p-1} = 1 \quad \text{(modulo } p\text{)}.$$

Důkaz: stačí si uvědomit, že grupa $\{1,2,\dots,p-1\}$ s operací „krát modulo p“ má $p-1$ prvků a použít větu ze stránky [8].

Množina se dvěma operacemi: okruh, těleso

Definice: *Okruh* je množina T s operacemi + a $\cdot$, pro které platí:

(1) T s operací + je komutativní grupa (neutrální prvek značíme 0),

(2) T s operací $\cdot$ je pologrupa,

(3) $\forall x,y,z \in T$ platí $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$, $(y+z) \cdot x = (y \cdot x) + (z \cdot x)$. … (distributivní zákon).

Definice: *Těleso* je množina T s operacemi + a $\cdot$, pro které platí:

(1) T s operací + je komutativní grupa (neutrální prvek značíme 0),

(2) $T \setminus \{0\}$ s operací $\cdot$ je grupa (jednotkový prvek značíme 1),

(3) $\forall x,y,z \in T$ platí $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$, $(y+z) \cdot x = (y \cdot x) + (z \cdot x)$. … (distributivní zákon).

Pozorování: Každé těleso musí mít aspoň dva prvky: 0 a 1.

Varianty okruhů a těles

Předpokládejme množinu T s vlastnostmi (1) a (3).

- Je-li T s operací $\cdot$ komutativní pologrupa, pak T se nazývá *komutativní okruh*.
- Je-li T s operací $\cdot$ pologrupa a má-li jednotkový prvek, pak T se nazývá *okruh s jednotkou*.
- Je-li T s operací $\cdot$ komutativní pologrupa a má-li jednotkový prvek, pak T se nazývá *komutativní okruh s jednotkou*.
- Je-li $T \setminus \{0\}$ s operací $\cdot$ komutativní grupa, pak T se nazývá *komutativní těleso*.

Poznámčička: příklad nekomutativního tělesa (kvaterniony) pro nedostatek místa vynecháme. Všechna ostatní tělesa, o kterých budeme mluvit, jsou komutativní tělesa. Takže slovo „komutativní“ nebudeme v případě těles nadále zdůrazňovat.

Příklady

- Množina reálných čísel s operacemi + a $\cdot$ tvoří těleso.
- Množiny $\mathbf{Q}$ a $\mathbf{C}$ s operacemi + a $\cdot$ jsou také tělesa.
- Množina $\mathbf{Z}$ s operacemi + a $\cdot$ je to komutativní okruh s jednotkou.
- Množina sudých celých čísel s + a $\cdot$ je komutativní okruh.
- Množina regulárních matic s operacemi + a $\cdot$ není těleso ani okruh, protože součet dvou reg. matic nemusí být regulární.
- Množina čtvercových matic (stejného typu) s operacemi + a $\cdot$ je nekomutativní okruh s jednotkou. Není to těleso.
- Množina $\{0,1\}$ s operacemi $0+0=0$, $0+1=1+0=1$, $1+1=0$, $0 \cdot a = a \cdot 0 = 0$, $1 \cdot a = a \cdot 1 = a$, tvoří těleso.
- Množina $\{0,1,\dots,p-1\}$ s operacemi „+ modulo p“ a „krát modulo p“ tvoří těleso, právě když je p prvočíslo. Jinak je to okruh.

Konečná (Galoisova) tělesa

Dá se ukázat, že pokud je těleso T konečné, pak nastává jen jedna z následujících možností:

- $T = \{0,1,2,\dots,p-1\}$ s operací „+ modulo p“ a „krát modulo p“, kde p je prvočíslo. Toto těleso se značí $\mathbf{Z}_p$ a má p prvků.
- T je množina všech polynomů nad $\mathbf{Z}_p$ stupně menšího než n s operacemi „plus a krát modulo ireducibilní polynom stupně n“. Toto těleso má p^n prvků, podrobněji se k němu vrátíme za chvíli.

Jiné konečné těleso (až na izomorfismus) neexistuje. Konečná tělesa se někdy značí GF(p^n), kde argument informuje o počtu prvků tělesa a GF je zkratka pro „Galois field“.

Příklady: neexistuje těleso, které má 6 prvků. Existuje ale těleso, které má 8 prvků: GF(2^3) nebo 9 prvků: GF(3^2).

$\mathbf{Z}_5$ je těleso, ale $\mathbf{Z}_8$ není těleso (je to jen okruh).

Základní vlastnosti tělesa

- Pro libovolné $a,b \in T$ je: $a \cdot b = 0$, právě když $a = 0$ nebo $b = 0$.
  Důkaz: Nechť $a \neq 0$ a $b \neq 0$. Pak $a \cdot b \neq 0$ z vlastnosti (2) definice tělesa. Obráceně: BÚNO $a = 0$, ukážeme, že $0 \cdot b = 0$. Platí:
  $$0 \cdot b = (0+0) \cdot b = 0 \cdot b + 0 \cdot b.$$
  Přičtením $-(0 \cdot b)$ k oběma stranám rovnosti máme $0 = 0 \cdot b$.
- Jestliže existuje konečný počet jedniček, které v součtu dají nulu, je nejmenší takový počet prvočíslo.
  Důkaz: Nejmenší počet jedniček, které dají v součtu nulu, označím λ. Pro spor budiž $\lambda = m \cdot n$, $m < \lambda$, $n < \lambda$. Pak
  $$\left(\sum_1^m 1\right) \cdot \left(\sum_1^n 1\right) = \sum_1^{m\,n} 1 = \sum_1^{\lambda} 1 = 0$$
  takže (dle předchozí vlastnosti) musí být aspoň jedna závorka nulová. Tj. existuje menší počet jedniček, které mají součet nula.

Charakteristika tělesa

Definice: Charakteristika tělesa λ je nejmenší počet jedniček, které dají v součtu nulu. Pokud konečný počet jedniček s touto vlastností neexistuje, klademe $\lambda = 0$.

Příklady:

- Tělesa $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ mají charakteristiku $\lambda = 0$.
- Těleso $\mathbf{Z}_p$ (p prvočíslo) má charakteristku $\lambda = p$.

Pozorování: z předchozí stránky víme, že charakteristika tělesa je rovna prvočíslu (je-li konečná).

Tvrzení:

- Je-li p charakteristika tělesa, pak $(a+b)^p = a^p + b^p$.
- V tělese $\mathbf{Z}_p$ dokonce platí: $a^p = a$ (díky malé Fermatově větě).
- V obecném tělese s charakteristikou p ovšem neplatí $a^p = a$.

Znovu definice lineárního prostoru

Definice: *Lineární prostor nad tělesem T* je neprázdná množina L s operacemi $+ : L\times L \to L$ a $\cdot : T\times L \to L$, které splňují vlastnosti:

(+) L s operací $+$ je komutativní grupa, nulový prvek značíme $\overrightarrow{o}$,

(A) $\alpha\cdot(\beta\cdot\overrightarrow{x}) = (\alpha\cdot\beta)\cdot\overrightarrow{x}$ pro všechna $\overrightarrow{x}\in L$, $\alpha,\beta\in T$,

(B) $\alpha\cdot(\overrightarrow{x}+\overrightarrow{y}) = \alpha\cdot\overrightarrow{x}+\alpha\cdot\overrightarrow{y}$ pro všechna $\overrightarrow{x},\overrightarrow{y}\in L$, $\alpha\in T$,

(C) $(\alpha+\beta)\cdot\overrightarrow{x} = \alpha\cdot\overrightarrow{x}+\beta\cdot\overrightarrow{x}$ pro všechna $\overrightarrow{x}\in L$, $\alpha,\beta\in T$,

(D) $1\cdot\overrightarrow{x} = \overrightarrow{x}$ pro všechna $\overrightarrow{x}\in L$.

Pozorování: Pro $T=\mathbf{R}$ se definice shoduje s původní definicí lin. prostoru. Stačí ověřit, že platí (7): $0\cdot\overrightarrow{x} = \overrightarrow{o}$ pro všechny $\overrightarrow{x}\in L$:

$$0\cdot\overrightarrow{x} = (0+0)\cdot\overrightarrow{x} = 0\cdot\overrightarrow{x}+0\cdot\overrightarrow{x},$$

k této rovnosti přičteme $-(0\cdot\overrightarrow{x})$ a dostáváme $\overrightarrow{o} = 0\cdot\overrightarrow{x}$.

Aritmetický lineární prostor T^n

je analogií lineárního prostoru $\mathbf{R}^n$. Množina T^n je množinou všech uspořádaných n-tic prvků z tělesa T s operacemi sčítání n-tic a násobení n-tice skalárem z T, které jsou definovány takto:

(1) $(a_1,a_2,\dots,a_n)+(b_1,b_2,\dots,b_n) = (a_1+b_1,a_2+b_2,\dots,a_n+b_n)$,

(2) $\alpha\cdot(a_1,a_2,\dots,a_n) = (\alpha\cdot a_1,\alpha\cdot a_2,\dots,\alpha\cdot a_n)$.

Pozorování: Tento lineární prostor má bázi

$$(1,0,\dots,0),\ (0,1,\dots,0),\ \dots,\ (0,0,\dots,1),$$

takže má dimenzi n.

Je-li T konečné těleso, které má m prvků, pak celkový počet vektorů v T^n je m^n.

Každý podprostor prostoru T^n dimenze k má m^k prvků, protože existuje m^k různých lineárních kombinací báze.

Příklad: lineární prostor $\mathbf{Z}_2^n$

je lineární prostor uspořádaných n-tic jedniček a nul nad tělesem $\mathbf{Z}_2$. Prvky tělesa $\mathbf{Z}_2 = \{0,1\}$ sčítáme podle pravidla

$$0+0=0,\quad 0+1=1+0=1,\quad 1+1=0$$

a vektory (uspořádané n-tice) sčítáme a násobíme po složkách, jako na předchozí stránce. Jmenovitě pro libovolný $\overrightarrow{u}\in\mathbf{Z}_2^n$ je $1\cdot\overrightarrow{u} = \overrightarrow{u}$ a $0\cdot\overrightarrow{u} = \overrightarrow{o}$. S jinými skaláry nepracujeme.

Příklad: soustava lineárních rovnic v $\mathbf{Z}_5$

Vyřešíme soustavu lineárních rovnic v $\mathbf{Z}_5$ s následující rozšířenou maticí. V první eliminační úpravě jsem sečetl první řádek s druhým a dále od třetího odečetl dvojnásobek prvního.

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

Množina řešení přidružené homogenní soustavy $M_0 = \langle(0,3,0,1)\rangle$ a partikulární řešení je např. $(1,4,0,0)$. Všechny principy lineární algebry (o dimenzích, lineárních obalech, bázích) zůstávají v platnosti. Rozdíl proti lin. prostoru nad $\mathbf{R}$ je jen ten, že zde jsou (pod)prostory konečné. Např. M_0 zde má pět prvků (vektor je možné násobit jen čísly $0,1,2,3,4,$), takže množinu řešení můžeme zapsat výčtem prvků:

$$M = \{(1,4,0,0),\ (1,2,0,1),\ (1,0,0,2),\ (1,3,0,3),\ (1,1,0,4)\}$$

Polynom nad komutativním tělesem T

je vzorec

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

kde $a_i\in T$. Tento vzorec vymezuje předpis pro hodnoty zobrazení z T do T (za x dosazujeme prvky z tělesa T a dostáváme hodnoty polynomu: prvky z tělesa T).

Rovnost polynomů: dva polynomy se rovnají, když se rovnají jejich odpovídající koeficienty (až na případné přebytečné nulové koeficienty s nejvyššími indexy).

Pozor: rovnost není zaručena rovností zobrazení $T\to T$.

Příklad: Polynom x^2+1 nad $\mathbf{Z}_2$ odpovídá zobrazení $0\to1$, $1\to0$. Polynom x^3+1 odpovídá stejnému zobrazení, ale není to stejný polynom.

Operace s polynomy nad tělesem

Součet, rozdíl nebo součin polynomů nad T provedeme jako součet, rozdíl nebo součin příslušných vzorců. Přitom provádíme výpočty s jednotlivými koeficienty polynomů za použití operací v tělese T.

Příklad: Sečteme polynomy nad $\mathbf{Z}_5$:

$$(2x^3+4x^2+2x+1)+(3x^2+2x) = 2x^3+(4+3)x^2+(2+2)x+1 = 2x^3+2x^2+4x+1.$$

Příklad: Vynásobíme polynomy nad $\mathbf{Z}_5$:

$$\begin{aligned}&(2x^3+4x^2+2x+1)\cdot(3x^2+2x) =\\ &= (2\cdot3)x^5+(4\cdot3)x^4+(2\cdot3)x^3+3x^2+(2\cdot2)x^4+(4\cdot2)x^3+(2\cdot2)x^2+2x =\\ &= x^5+2x^4+x^3+3x^2+4x^4+3x^3+4x^2+2x =\\ &= x^5+(2+4)x^4+(1+3)x^3+(3+4)x^2+2x =\\ &= x^5+x^4+4x^3+2x^2+2x\end{aligned}$$

Částečný podíl polynomů

Věta: pro každé dva polynomy p, q (q nenulový) existují jednoznačně polynomy r, z tak, že
1) $p = r\cdot q+z$,
2) stupeň z je menší než stupeň q.

Algoritmus částečného dělení polynomu polynomem lze použít stejně nad libovolným tělesem. Naučili jsme se ho používat pro polynomy nad $\mathbf{R}$ a nyní jej budeme používat pro polynomy nad libovolným tělesem. Zaskočit nás může jen úkon dělení koeficientu a koeficientem b, což je ale v každém komutativním tělese proveditelné jako $a\cdot b^{-1}$.

Příklad: algoritmus částečného podílu

Vydělíme polynomy nad $\mathbf{Z}_5$. V tomto případě si uvědomíme, že $3^{-1}=2$, protože $3\cdot2=1$ modulo 5. Takže například první krok algoritmu obsahuje výpočet $2x^3:3x^2 = (2\cdot3^{-1})x = (2\cdot2)x = 4x$

$$\begin{aligned}&(2x^3+4x^2+2x+1):(3x^2+2x) = 4x+2\\ &-(2x^3+3x^2)\\ &\qquad x^2+2x+1\\ &\quad-(x^2+4x)\\ &\qquad\quad -2x+1\end{aligned}$$

Podíl daných polynomů roven $4x+2$ a zbytek je $-2x+1 = 3x+1$.

Operace modulo polynom

Srovnejme dvě tvrzení:

- Pro každé dvě celá čísla a, b (b nenulové) existují celá čísla r, z tak, že $a = rb + z$, přitom $0 \le z < b$. Číslo z je zbytek po dělení a číslem b.
- Pro každé dva polynomy p, q (q nenulový) existují polynomy r, z tak, že $p = r \cdot q + z$, přitom $\mathrm{st}\, z < \mathrm{st}\, q$. Polynom z je zbytek po dělení p polynomem q.

Tak jako můžeme pro dvě čísla najít zbytek po dělení, můžeme pro dva polynomy najít zbytek po dělení. Je-li dán nenulový polynom, modul q, pak každý polynom p můžeme ztotožnit se zbytkem po dělení p polynomem q. Označíme-li z tento zbytek, pak říkáme:

$$p = z \quad \text{modulo } q.$$

Okruh polynomů modulo polynom

Zvolme nenulový polynom q stupně n jako modul a prvočíslo p. Symbolem $\mathbf{Z}_p[x]/q$ označíme množinu všech polynomů nad tělesem $\mathbf{Z}_p$, která má stupeň menší než n. Zavedeme tyto operace:

- **Sčítání** prvků z $\mathbf{Z}_p[x]/q$: provedeme jako obvyklé sčítání polynomů nad $\mathbf{Z}_p$. Stupeň součtu je jistě menší než n, takže leží v $\mathbf{Z}_p[x]/q$. Množina $\mathbf{Z}_p[x]/q$ s tímto sčítáním zjevně tvoří komutativní grupu.
- **Násobení** prvků a $\mathbf{Z}_p[x]/q$: provedeme obvyklé násobení polynomů nad $\mathbf{Z}_p$. Pokud stupeň výsledku je větší nebo roven n, provedeme navíc na výsledek operaci „modulo polynom q“. Množina $\mathbf{Z}_p[x]/q$ s tímto násobením je pologrupa.

Platí distributivní zákony: tj. množina $\mathbf{Z}_p[x]/q$ s uvedenými operacemi je okruh.

Ireducibilní polynom

Polynom q je *ireducibilní*, právě když jej nelze rozložit na součin dvou polynomů nižších stupňů.

Příklad: Polynom x^2+x+1 nad $\mathbf{Z}_2$ je ireducibilní, protože kdyby šel rozložit na součin polynomů nižších stupňů, pak je to součin kořenových činitelů, ale tento polynom v $\mathbf{Z}_2$ nemá kořeny (vyzkoušejte postupným dosazením čísel 0 a 1).

Příklad: Polynom $x^3 + x + 1$ nad $\mathbf{Z}_2$ je ireducibilní (ze stejných důvodů).

Příklad: Polynom $x^5 + x^4 + 1$ nad $\mathbf{Z}_2$ je reducibilní, protože

$$x^5 + x^4 + 1 = (x^3 + x + 1) \cdot (x^2 + x + 1).$$

V případě polynomu stupně 4. a více nám test existence kořenů k rozhodnutí o ireducibilitě nepomůže.

Polynomy modulo ireducibilní polynom

Dá se ukázat, že pokud je polynom q ireducibilní, pak okruh $\mathbf{Z}_p[x]/q$ je těleso, tj. každý polynom z množiny $\mathbf{Z}_p[x]/q$ má při operaci násobení inverzní polynom.

Důkaz* se dá provést anoalogicky, jako s čísly. Povšimneme si této podobnosti:

- p je prvočíslo, tj. nelze rozložit na součin menších čísel.
- q je ireducibilní, tj. nelze rozložit na součin polynomů menších stupňů.

Je možné přečíst důkaz tvrzení ze stránky [10] znovu, jen slovo číslo nahradíme slovem polynom, slovo prvočíslo slovem ireducibilní polynom a výrok „číslo a je menší než b“ výrokem „stupeň polynomu p je menší než stupeň q“.

Příklad: těleso $\mathbf{Z}_2[x]/(x^3 + x + 1)$

Modul $(x^3 + x + 1)$ je ireducibilní. Toto těleso obsahuje:

$$\mathbf{Z}_2[x]/x^3 + x + 1 \;=\; \{0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1\}$$

Sčítání prvků provádíme jako sčítání polynomů nad $\mathbf{Z}_2$, například:

$$(x + 1) + (x^2 + x) = x^2 + 1$$

Násobení prvků provádíme jako násobení polynomů nad $\mathbf{Z}_2$ s případnou dodatečnou operací „modulo $x^3 + x + 1$“. Například:

$$(x + 1) \cdot (x^2 + x) = x^3 + x = 1 \quad \text{modulo } (x^3 + x + 1)$$

Vidíme, že prvky $x + 1$ a $x^2 + x$ jsou si vzájemně inverzní.

Toto je příklad tělesa, který obsahuje 8 prvků, je to tedy $\mathrm{GF}(2^3)$.

- Má-li ireducibilní modul q stupeň n, je $\mathbf{Z}_p[x]/q = \mathrm{GF}(p^n)$.

Příklad: komplexní čísla

Polynom $x^2 + 1$ je nad $\mathbf{R}$ ireducibilní. Označme symbolem $\mathbf{R}[x]$ všechny polynomy nad $\mathbf{R}$ a dále $\mathbf{R}[x]/(x^2 + 1)$ bude značit množinu všech polynomů nejvýše prvního stupně s obvyklou operací + a s operací „krát modulo polynom $x^2 + 1$“. Takže

$$\mathbf{R}[x]/(x^2 + 1) = \{a + bx;\ a, b \in \mathbf{R}\}$$

Dva polynomy v $\mathbf{R}[x]/(x^2 + 1)$ sčítáme podle pravidla:

$$(a + bx) + (c + dx) = (a + c) + (b + d)x.$$

Dva polynomy v $\mathbf{R}[x]/(x^2 + 1)$ násobíme podle pravidla:

$$(a + bx) \cdot (c + dx) = bdx^2 + (ad + bc)x + ac = \\ = (ac - bd) + (ad + bc)x \quad \text{modulo } x^2 + 1$$

Nahrazením symbolu x symbolem i shledáváme, že
těleso $\mathbf{R}[x]/(x^2 + 1)$ je izomorfní s tělesem komplexních čísel.

Úvod do kódování

- samoopravné kódy: terminologie, princip
- blokové lineární kódy
- Hammingův kód
- cyklické kódy

a) algebra-all, 18, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) Viz p. d. 4/2010

Samoopravné kódy, k čemu to je

- Data jsou uložena (nebo posílána do linky) *kodérem* podle určitého pravidla (*kódování*). Posléze jsou čtena *dekodérem* a restaurována do původní podoby.
- Kodér může přidat k datům doplňující informaci (zhruba řečeno kontrolní součet) a umožnit tím dekodéru, aby poznal, zda při přenosu dat došlo k chybě. Dokonce při vhodně zvoleném kódování může dekodér chybu opravit.

Kód je množina slov (tj. úseků dat), které může generovat kodér.

Příklady kódů:

- ASCII (slova sedmibitová, ne všechna)
- Morseova abeceda (slova různě dlouhá, efektivní přenos)
- UTF-8 (slova různě dlouhá, délka rozpoznaná podle prefixu)

Binární, blokový kód

je kód, kde jsou všechna slova stejně dlouhá.

Definice: Nechť A je množina znaků (abeceda).
Slovo je konečná posloupnost znaků z množiny A.
Počet znaků ve slově je *délka slova*.
Kód K je množina všech slov, která generuje kodér.
Prvek kódu K se nazývá *kódové slovo*.
Blokový kód K obsahuje jen slova stejné délky.
Binární kód je kód se slovy nad abecedou $A = \{0, 1\}$.

Příklady:

- ASCII je binární blokový kód délky 7.
- Moreseovka není binární a není blokový kód.
- UTF-8 je binární, ale ne blokový kód.

Dále se budeme zabývat jen binárními blokovými kódy

Lineární kód

Binární blokový kód K délky n je podmnožinou lin. prostoru $\mathbf{Z}_2^n$.

Definice: Je-li K lienární podprostor $\mathbf{Z}_2^n$, pak se kód nazývá *lineární*. Je-li dimenze kódu k, pak mluvíme o lineárním (n, k) kódu.

Příklad: Kód s kontrolním bitem parity je lineární. Kodér přidává nulu nebo jedničku k informačním bitům tak, aby kódové slovo obsahovalo sudý počet jedniček. Množina všech slov délky n se sudým počtem jedniček je lineární podprostor lineárního prostoru $\mathbf{Z}_2^n$.

Generující a kontrolní matice

Generující matice lineárního kódu K je matice, která v řádcích obsahuje bázi kódu.

Kontrolní matice lineárního kódu K je matice $\mathbf{H}$, kro kterou platí, že K je řešením soustavy $\mathbf{H}\,\mathbf{x} = \mathbf{o}$.

Příklad: Předpokládejme lineární $(4, 3)$ kód s kontrolním bitem parity (přidávaný na konec slova za tři informační bity). Generující matice $\mathbf{G}$ a kontrolní matice $\mathbf{H}$ jsou:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \qquad \mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$$

Pozorování: Generující matice (n, k) kódu je typu (k, n) a kontrolní matice je typu $(n-k, n)$. Platí: $\mathbf{G} \cdot \mathbf{H}^T = \mathbf{O}$.

Výpočet jedné matice, známe-li druhou

Je-li dána generující (resp. kontrolní) matice, vyřešíme homogenní soustavu rovnic s touto maticí a bázi řešení zapíšeme do řádků kontrolní (resp. generující) matice.

Pro systematický kód dokonce platí:

Je-li $\mathbf{G} = (\mathbf{E} \,|\, \mathbf{C})$, pak $\mathbf{H} = (\mathbf{C}^T \,|\, \mathbf{E}')$.

Kodér a dekodér

Kodér lin. (n, k) kódu může převzít kódované slovo $\overrightarrow{u}$ (délky k) a vytvořit z něj kódové slovo $\overrightarrow{v}$ (délky n) maticovým násobením:

$$\overrightarrow{v} = \overrightarrow{u} \cdot \mathbf{G}.$$

Dekodér může zkontrolovat přijaté slovo $\overrightarrow{w}$ pomocí testu:

$$\mathbf{H} \cdot \overrightarrow{w}^T = \mathbf{o}.$$

Kódování je *systematické*, jsou-li informační bity (ze slova $\overrightarrow{u}$) beze změny zkopírovány do kódového slova a za nimi následují kontrolní bity. Pak může dekodér (po provedeném testu) rekonstruovat informační bity zkopírováním prvních k pozic přijatého slova.

Pozorování: Kódování je systematické, je-li generující matice tvaru $\mathbf{G} = (\mathbf{E} \,|\, \mathbf{C})$. Přidávané kontrolní bity pak kodér spočítá pomocí vzorce $\overrightarrow{v}' = \overrightarrow{u} \cdot \mathbf{C}$.

Příklad: opakovací kód

Kodér vezme kódované slovo $\overrightarrow{u}$ délky k a vytvoří kódové slovo délky $n = 2k$ tak, kódové slovo je tvaru $(\overrightarrow{u}, \overrightarrow{u})$, tj. kódované slovo je zdvojené.

Generující matice tohoto kódu je $\mathbf{G} = (\mathbf{E} \,|\, \mathbf{E})$ a kontrolní matice je také tvaru $\mathbf{H} = (\mathbf{E} \,|\, \mathbf{E})$. Uvědomte si, jak je kód pomocí $\mathbf{G}$ generován a jak je pomocí $\mathbf{H}$ kontrolován.

Nevýhoda: příliš mnoho kontrolních bitů za „málo muziky“.

Hammingova váha, vzdálenost

Definice: *Hammingova váha* slova $\overrightarrow{v}$ je počet jeho nenulových znaků. *Hammingova vzdálenost* dvou slov $\overrightarrow{v}$ a $\overrightarrow{w}$ je počet pozic, kde jsou znaky odlišné (pro binární kód je to váha slova $\overrightarrow{v} + \overrightarrow{w}$).

Kód K *objevuje* t *chyb*, pokud pro každé slovo $\overrightarrow{u} \in K$ a každé slovo $\overrightarrow{e}$ váhy menší nebo rovno t platí $\overrightarrow{u} + \overrightarrow{e} \notin K$.

Kód K *opravuje* t *chyb*, pokud pro každé slovo $\overrightarrow{u} \in K$ a každé slovo $\overrightarrow{e}$ váhy menší nebo rovno t platí: slovo $\overrightarrow{u}$ má od slova $\overrightarrow{u} + \overrightarrow{e}$ nejmenší vzdálenost mezi kódovými slovy.

Tvrzení 1: Je-li nejmenší vzdálenost mezi kódovými slovy d, pak kód objevuje $d - 1$ chyb a opravuje $t < \frac{d}{2}$ chyb.

Tvrzení 2: Nejmenší vzdálenost mezi kódovými slovy *lineárního* kódu je rovna nejmenší váze nenulového kódového slova.

Příklady

Kód s kontrolním bitem parity má nejmenší váhu nenulového slova 2, takže objevuje $2 - 1 = 1$ chybu ve slově. Opravuje méně než 2/2 chyb, tedy neopravuje žádnou chybu.

Opakovací kód mý rovněž nejmenší váhu nenulového slova 2.

Aby kód dokázal opravit jednu chybu ve slově, musí mít nejmenší váhu neulového slova rovnu třem.

Syndrom

Dekodér vyhodnotí $\mathbf{s} = \mathbf{H} \cdot \overrightarrow{w}^T$. Tomuto vektoru $\mathbf{s}$ říkáme *syndrom* přijatého slova $\overrightarrow{w}$. Přijaté slovo je kódové, právě když má nulový syndrom.

Kód rozpozná chybu $\overrightarrow{e}$, právě když $\mathbf{s} = \mathbf{H} \cdot \overrightarrow{e}^T$ je nenulový vektor.

Pozorování 1: Syndrom nezávisí na kódovém slově (jen na chybovém slově): $\mathbf{H} \cdot (\overrightarrow{v} + \overrightarrow{e})^T = \mathbf{H} \cdot \overrightarrow{v}^T + \mathbf{H} \cdot \overrightarrow{e}^T = \mathbf{o} + \mathbf{H} \cdot \overrightarrow{e}^T = \mathbf{H} \cdot \overrightarrow{e}^T$.

Pozorování 2: Lin. kód má minimální vzdálenost dvou slov d, právě když každý výběr $d-1$ sloupců z kontrolní matice $\mathbf{H}$ je lineárně nezávislý.

Jmenovitě: kód opravuje jednu chybu když každé dva sloupce kontrolní matice $\mathbf{H}$ jsou LN, tj. jsou nenulové a vzájemně různé (to v $\mathbf{Z}_2^{n-k}$ stačí). Kontrolní matice s touto vlastností je kontrolní matice *Hammingova kódu*.

Hammingův kód

Sloupce kontrolní matice $\mathbf{H}$ jsou prvky $\mathbf{Z}_2^{n-k}$. Počet nenulových a vzájemně různých sloupců je maximálně $2^{n-k}-1$. Počet sloupců udává délku kódu n, tedy $n = 2^{n-k}-1$. Délku kódu je tedy vhodné volit jako mocninu dvou bez jedné. Dostáváme tak Hammingovy kódy: $(7,4)$, $(15,11)$, $(31,26)$, $(63,57)$, ...

Příklad: Hammingův kód $(7,4)$ – délka 7, informační bity 4:

$$\mathbf{H} = \begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix}, \quad \mathbf{G} = \begin{pmatrix} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{pmatrix}.$$

Výhoda tohoto uspořádání: index bitu, který je potřeba opravit, je zapsán v syndromu jako číslo ve dvojkové soustavě.

Rozšířený Hammingův kód

je Hammingův kód, ke kterému kodér přidává kontrolní bit parity. Například $(8,4)$ kód má matice

$$\mathbf{H} = \begin{pmatrix} 0&0&0&1&1&1&1&0 \\ 0&1&1&0&0&1&1&0 \\ 1&0&1&0&1&0&1&0 \\ 1&1&1&1&1&1&1&1 \end{pmatrix}, \quad \mathbf{G} = \begin{pmatrix} 1&0&0&0&0&1&1&1 \\ 0&1&0&0&1&0&1&1 \\ 0&0&1&0&1&1&0&1 \\ 0&0&0&1&1&1&1&0 \end{pmatrix}.$$

Kód opraví jednu chybu (v prvních třech bitech je syndrom jako v $(7,4)$ kódu a čtvrtý bit musí být 1) a odhalí dvě chyby (v prvních třech bitech syndromu je nenulové číslo a čtvrtý bit je 0).

Nejmenší vzdálenost dvou slov v tomto kódu je 4.

Návrh počtu kontrolních bitů

Označme n délku binárního kódu, k dimenzi kódu (počet informačních bitů) a $c = n-k$ počet kontrolních bitů.

Lineární kód nemůže opravit více rozdílných chyb než je počet nenulových syndromů. Těch je 2^c-1. Počet různých chyb s váhou jedna je n. Proto, chceme-li opravit jednu chybu, musí $2^c - 1 \geq n$.

Počet různých chyb (včetně stavu „bez chyby“) s váhou nejvýše m je rovno

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{m}$$

Chceme-li opravovat m chyb ve slově, musí tedy počet kontrolních bitů splňovat:

$$2^c \geq \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{m}$$

Kódy navržené tak, že zde nastává rovnost, se nazývají *perfektní*.

Cyklické kódy

jsou běžně užívané samoopravné kódy (např. při zápisu/čtení CD). Viz google: CRC (cyclic redundancy check).

Definice: Kód K se nazývá *cyklický*, pokud

- je lineární a navíc
- je-li $\overrightarrow{v}$ kódové slovo, pak cyklický posun $\overrightarrow{v}$ je také kódové slovo.

Vhodná matematická reprezentace slov délky n jsou polynomy:

$$\overrightarrow{v} = (a_0, a_1, a_2 \ldots, a_{n-1}) \quad \leftrightarrow \quad v(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1}$$

Cyklický posun slova $\overrightarrow{v}$ o jednu pozici popíšeme násobením polynomu $v(x)$ polynomem x a ztotožněním $x^n = x^0$, neboli násobením v okruhu $\mathbf{Z}_p[x]/(x^n-1)$.

Od této chvíle nerozlišujeme mezi pojmem „slovo“ a „polynom“.

Základní vlastnosti cyklického kódu

Tvrzení: Je-li K cyklicý, $g \in K$ a je-li f libovolný polynom, pak $f \cdot g \in K$. Výpočet $f \cdot g$ je proveden v $\mathbf{Z}_p[x]/(x^n-1)$.

Důkaz: $(b_m x^m + \cdots + b_1 x + b_0) \cdot g$ v $\mathbf{Z}_p[x]/(x^n-1)$ je lineární kombinace cyklických posunů polynomu g.

Definice: Nenulový polynom cyklického kódu nejmenšího stupně nazýváme *generující polynom*.

Zřejmě pro generující polynom platí: $K = \{f \cdot g;\ f \text{ je lib. polynom}\}$.

Vlastnosti generujícího polynomu

Tvrzení: Nechť g je generující polynom (n,k) cyklického kódu K.

- polynom g más stupeň $n-k$,
- $\{g, x\cdot g, x^2\cdot g, \ldots, x^{k-1}\cdot g\}$ je báze kódu,
- polynom x^n-1 je dělitený polynomem g.

Důkaz: nechť $v \in K$. Vydělíme v polynomem g se zbytkem:
$v = f\cdot g + z$, protože $v \in K, f\cdot g \in K$, musí $z \in K$.
Protože $\mathrm{st}\, z < \mathrm{st}\, g$ a polynom g má nejmenší stupeň, musí $z = 0$.
Protože $\mathrm{st}\, v < n$, je $\mathrm{st}\, f < m = n - \mathrm{st}\, g$. Libovolný $v \in K$ lze zapsat jako

$$v = (f_{m-1}x^{m-1} + \cdots + f_1 x + f_0)\cdot g$$

neboli jako lineární kombinaci prvků $\{g, x\cdot g, x^2\cdot g, \ldots, x^{k-1}\cdot g\}$. Tyto prvky jsou LN, takže tvoří bázi kódu K. Je tedy $m = k$ a $\mathrm{st}\, g = n-k$.

Puntík třetí: dělitelnost ověříme analogicky (musí $z = 0$).

Generující polynom: postačující podmínka

Tvrzení: Aby byl polynom g generující polynom nějakého cyklického kódu, stačí, aby dělil polynom x^n-1 beze zbytku.

Důkaz: Zjistíme, že lin. obal všech cyklických posunů g neobsahuje nenulový polynom st. menšího než g. Nechť f je libovolný polynom.

$$f\cdot g = z \mod (x^n-1), \quad \text{tj.} \quad f\cdot g = u\cdot(x^n-1) + z$$

Je třeba ověřit, že $z = 0$ nebo $\mathrm{st}\, z \geq \mathrm{st}\, g$. Protože je $f\cdot g$ dělitelný g a $u\cdot(x^n-1)$ je dělitelný g, musí též z být dělitelný g, takže $z = v\cdot g$.

Návrh cyklického kódu: Zvolíme délku bloku n, rozložíme polynom x^n-1 na součin ireducibilních polynomů a generující polynom g zvolíme jako součin *některých* takto nalezených ireducibilních polynomů. Stupeň g je počet kontrolních bitů kódu.

Úmluva: Všechny gen. polynomy stejného kódu se liší až na skalární násobek. Volme takový, co má u nejvyšší mocniny jedničku.

Odhalení souvislé chyby

Souvislá chyba délky t je chyba měnící kódové slovo v úseku některých po sobě jdoucích t bitů, jinde je slovo nezměněno. Počet chyb (váha chybového slova) nemusí být t, ale je menší nebo rovna t.

Pozorování: Cyklický (n,k) kód odhaluje všechny souvislé chyby délky $n-k$.

Důkaz: Na souvislou chybu $\overrightarrow{e}$ můžeme provést (opakovaně) cyklický posun a získat polynom $\overrightarrow{e}'$, který je stupně menšího než $n-k$. Takže $\overrightarrow{e}'$ ani $\overrightarrow{e}$ není kódové slovo.

Poznámka: toto je důvod, proč se v praxi používají cyklické kódy. Chyby se totiž rády v konkrétním technickém prostředí soustřeďují do bloků (drupouty, škrábance na CD atd.).

Existují cyklické (n,k) kódy, které navíc *umějí opravit* všechny souvislé chyby délky $(n-k)/2$.

Příklad: Cyklický Hammingův kód

Sestavme $(7,4)$ cyklický kód, který má generující polynom x^3+x+1. Je to generující polynom, protože dělí polynom x^7-1. Kód má následující generující a kontrolní matici

$$\mathbf{G}=\begin{pmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\end{pmatrix},\quad \mathbf{H}=\begin{pmatrix}1&0&1&1&1&0&0\\1&1&1&0&0&1&0\\0&1&1&1&0&0&1\end{pmatrix},$$

takže vidíme, že $\mathbf{H}$ má různé a nenulové sloupce. Je to tedy Hammingův $(7,4)$ kód.

Hammingův $(7,4)$ kód, který kóduje podle této $\mathbf{G}$ a používá tuto kontrolní matici $\mathbf{H}$ umí odhalit i tři *souvislé* chyby. Od Hammingova kódu ze strany [12] se liší pořadím bitů kódového slova.

Generující a kontrolní matice

Protože cyklický kód má bázi $g,\ x\cdot g,\ x^2\cdot g,\ \ldots,\ x^{k-1}\cdot g$, kde g je generující polynom, $g(x)=g_0+g_1x+g_2x^2+\cdots+g_{n-k}x^{n-k}$, je generující matice tvaru

$$\mathbf{G}=\begin{pmatrix}g_0&g_1&g_2&\ldots&g_{n-k}&0&0&\ldots&0&0\\0&g_0&g_1&\ldots&g_{n-k-1}&g_{n-k}&0&\ldots&0&0\\0&0&g_0&\ldots&g_{n-k-2}&g_{n-k-1}&g_{n-k}&\ldots&0&0\\&&&\ldots&&&&\ldots&&\\0&0&0&\ldots&\ldots&g_0&g_1&\ldots&g_{n-k-1}&g_{n-k}\end{pmatrix}$$

Polynom $h=(x^n-1)/g$ se nazývá *kontrolní polynom*. Dá se ukázat, že matice s koeficienty kontrolního polynomu $h_k,h_{k-1},\ldots,h_1,h_0$ umístěnými (v tomto pořadí) opakovaně „podél vedlejší diagonály“, je maticí kontrolní. Ta se v případě cyklických kódu v dekóderu příliš nevyužívá.

Kodér a dekodér cyklického kódu

Kódování podle generující matice není systematické. Kodér z informačních bitů $\overrightarrow{u}$ vytvoří kódové slovo $\overrightarrow{u}\cdot\mathbf{G}$. Fakticky tedy vytváří kódové slovo ve tvaru $u\cdot g$.

Dekodér spočítá *syndrom* přijatého slova jako zbytek po dělení generujícím polynomem. Je-li nulový, je přijaté slovo kódové. Výsledek dělení obsahuje informační bity.

Pozorování: Syndrom nezávisí na kódovaném slovu, ale pouze na chybě:

$$f\cdot g+e=s_1 \bmod g,\quad e=s_2 \bmod g,\quad \text{pak}\quad s_1=s_2.$$

Důkaz: $f\cdot g+e=r_1\cdot g+s_1$, $e=r_2\cdot g+s_2$. s_1-s_2 je násobek g se stupněm menším, takže $s_1-s_2=0$.

Sytematické kódování

Kodér z informačních bitů $(u_1,u_2,\ldots,u_k)$ sestaví polynom:

$$u(x)=u_1x^{n-1}+u_2x^{n-2}+\cdots+u_{k-1}x^{n-k+1}+u_kx^{n-k},$$

vypočítá z jako zbytek po dělení u polynomem g a odešle kódové slovo $u-z$. Proč je kódové? Je $u=f\cdot g+z$. Protože $f\cdot g$ je násobek g, musí i $u-z$ být násobek g. Navíc součet $u-z$ nepoškodí posledních k informačních bitů.

Dekodér spočítá syndrom s jako zbytek po dělení přijatého slova polynomem g. Je-li $s=0$, je přijaté slovo kódové. Posledních k bitů obsahuje informaci.

O analýze syndromu si povíme za chvíli.

Zbytek po dělení polynomu polynomem

se v případě polynomů nad $\mathbf{Z}_2$ hledá snadno. V příkladu zapisujeme bity v opačném pořadí než dosud, tj.

$$(a_{n-1},a_{n-2},\ldots,a_1,a_0)\leftrightarrow a_{n-1}x^{n-1}+a_{n-2}x^{n-1}+\cdots+a_1x+a_0.$$

Příklad: Nechť $g=(1011)$. Chceme kódovat informaci (1111). Sestavíme polynom $u=(1111000)$ a dělíme ho polynomem g:

kodér:	dekodér:
1111000	1111111
1011	1011
0100000	0100111
1011	1011
0001100	0001011
1011	1011
$0000111=z$, $\quad u-z=1111111$	$0000000=s$ (syndrom)

Analýza syndromu

Sestavíme tabulku chyb a jejich syndromů:

$\overrightarrow{e}_1\leftrightarrow\overrightarrow{s}_1$, $\overrightarrow{e}_2\leftrightarrow\overrightarrow{s}_2$, …, $\overrightarrow{e}_m\leftrightarrow\overrightarrow{s}_m$. Tabulku vyplníme (dřív, než začneme kódovat) tak, že pro každou chybu e_i spočítáme zbytek při dělení polynomem g a dostaneme s_i.

Kdybychom měli v paměti uloženu tuto tabulku, pak pro každý syndrom $\overrightarrow{s}_i$ dekodér najde zpětně $\overrightarrow{e}_i$ a přijaté slovo $\overrightarrow{w}$ opraví takto: $\overrightarrow{v}=\overrightarrow{w}-\overrightarrow{e}_i$.

Problém: paměťová náročnost + nutnost pro každé přijaté slovo prohledat tabulku.

Analýza syndromu podle Meggitta

Učiňme pozorování na příkladu $(7,4)$ cyklického kódu. Tabulka $\overrightarrow{e}_i\leftrightarrow\overrightarrow{s}_1$, která obsahuje všechny chyby váhy 1, vypadá takto:

$$\begin{aligned}
e_1&=x^0 &\leftrightarrow\quad s_1&=1\\
e_2&=x^1 &\leftrightarrow\quad s_2&=x\\
e_3&=x^2 &\leftrightarrow\quad s_3&=x^2\\
e_4&=x^3 &\leftrightarrow\quad s_4&=x+1\\
e_5&=x^4 &\leftrightarrow\quad s_5&=x^2+x\\
e_6&=x^5 &\leftrightarrow\quad s_6&=x^2+x+1\\
e_7&=x^6 &\leftrightarrow\quad s_7&=x^2+1\quad \ldots \text{ syndrom posledního bitu}
\end{aligned}$$

Pro syndromy platí: $s_{i+1}=x\cdot s_i \bmod g$. Přitom $s_8=s_1$. Je tedy možné „protočit syndromy“ postupnou aplikací operace $x\cdot s_i \bmod g$.

V jednom okamžiku se z každého syndromu stane syndrom posledního bitu. Děláme-li současně cyklický posun přijatého slova, dostal se opravovaný bit na poslední pozici. Opravíme ho tam.

Algoritmus podle Meggitta

Sestavme seznam všech syndromů, které odpovídají všem chybám, které mají na poslední pozici jedničku (seznam všech syndromů posledníо bitu). Uložme tento seznam do paměti dekodéru. Seznam zdaleka neobsahuje všechny syndromy.

Nechť délka kódu je n. Dekodér provede postupně n cyklických posunů přijatého slova (tím ho dostane nakonec do původního stavu) a současně cyklicky protáčí syndrom podle vzorce $s_{i+1} = x \cdot s_i \bmod g$. Kdykoli se sydrom shoduje s některým syndromem posledního bitu (ze seznamu), opraví dekodér poslední bit (cyklicky pounutého) přijatého slova.

Opravuje-li kód jedinou chybu, obsahuje seznam jediný syndrom posledního bitu. Opravuje-li dvě chyby, pak seznam obsahuje n syndromů. Výpočet probíhá s lineární složitostí (existuje dobře popsaná hw implementace pomocí hradel).

Korekce souvislých chyb

Existují cyklické kódy, které opravují souvislé chyby délky t. Dá se ukázat, že pro takové kódy platí: pokud při „protáčení syndromu“ dospějeme k syndromu stupně menšího než t, pak lze naráz opravit v odpovídajícím (cyklicky posunutém) přijatém slově všechny kontrolní bity přímo podle (protočeného) syndromu.

Inspirace: podívejte se na první řádek tabulky na str. [26].

Příklady „větších“ cyklických kódů

- Golay code je perfektní kód opravující tři chyby. Je to cyklický $(23, 12)$ kód s generujícím polynomem:

$$1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}$$

- CRC 32 je metoda počítání kontrolních součtů (syndromů) dat libovolné délky s generujícím polynomem:

$$1 + x + x^2 + x^4 + x^5 + x^7 + x^8 + x^{10} + x^{11} + x^{12} + x^{16} + x^{22} + x^{23} + x^{26} + x^{32}$$

K hlubšímu zkoumání této problematiky můžete použít:

Jiří Adámek: Foundations of Coding, A Wiley-Interscience publication, 1991, ISBN 0-471-62187-0.

Poznámka: Prof. Jiří Adámek byl v letech 1990–1994 vedoucí naší katedry, nyní působí na University of Braunschweig.