MB141, zkouška 15. 6. 2022

Příklad. **1A.** Určete vzdálenost přímek

$$p : [2,0,3] + a(1,-1,1) \quad \text{a} \quad q : [2,6,-1] + b(0,-1,3)$$

a body $P \in p$ a $Q \in q$, v nichž se vzdálenost (osa) realizuje.

Řešení. Položme $A = [2,0,3]$, $u = (1,-1,1)$, $B = [2,6,-1]$, $v = (0,-1,3)$. Rozdíl hledaných bodů $P = A + au \in p$ a $Q = B + bv \in q$ je kolmý na směrové vektory u a v obou přímek. Proto

$$\begin{aligned}\langle au - bv, u\rangle &= \langle B - A, u\rangle,\\ \langle au - bv, v\rangle &= \langle B - A, v\rangle\end{aligned}$$

To vede na soustavu pro neznámé a, b s maticí

$$\left(\begin{array}{cc|c} 2 & -5 & -9 \\ 3 & -4 & -10 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 1 & -1 \\ 0 & -7 & -7 \end{array}\right)$$

Řešení je $a = -2$, $b = 1$. Hledané body jsou

$$P = [2,0,3] - 2(1,-1,1) = [0,2,1], \quad Q = [2,6,-1] + (0,-1,3) = [2,5,2].$$

Vzdálenost je

$$\operatorname{dist}(p,q) = \operatorname{dist}(P,Q) = ||(2,3,1)|| = \sqrt{14}.$$

Alternativně lze najít směrový vektor n pro osu PQ jako kolmý na u i v a následně řešit rovnici $A + au + cn = B + bv$. □

Bodování. Sestavení rovnic (nebo nalezení kolmého vektoru a sestavení rovnic) **2 body**
Výpočet a, b **1 bod**
Body P, Q a vektor PQ **2 body**
Vzdálenost **1 bod** □

Příklad. 2A. Zobrazení $\varphi : \mathbb{R}^3 \to \mathbb{R}^3$ je symetrie podle přímky se směrovým vektorem $u = (1, 1, 2)$.

(a) Najděte matici A tak, aby ve standardních souřadnicích bylo

$$\varphi \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = A \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

(b) Je A ortogonální matice? Zdůvodněte svou odpověď.

(c) Najděte inverzní matici A^{-1}.

Řešení. **(a)** Symetrie podle přímky zobrazuje směrový vektor u na sebe. Dále platí, že libovolný vektor kolmý na směrový se zobrazí na opačný. Stačí tedy zvolit libovolné dva vzájemně nezávislé vektory v, w kolmé na u, např. $v = (1, -1, 0)$ a $w = (0, 2, -1)$. Trojice u, v, w tvoří bázi prostoru $\mathbb{R}^3$ a vztahy

$$\varphi(u) = u, \quad \varphi(v) = -v, \quad \varphi(w) = -w$$

jednoznačně určují zobrazení φ. Odtud již můžeme určit hodnoty zobrazení φ na vektorech e_1, e_2, e_3 standardní báze a tyto hodnoty tvoří sloupce hledané matice. Pro výpočet pišme vektory do řádků

$$\left(\begin{array}{ccc|ccc} & x & & & \varphi(x) & \\ 1 & 1 & 2 & 1 & 1 & 2 \\ 1 & -1 & 0 & -1 & 1 & 0 \\ 0 & 2 & -1 & 0 & -2 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} & x & & & \varphi(x) & \\ 6 & 0 & 0 & -4 & 2 & 4 \\ 0 & 6 & 0 & 2 & -4 & 4 \\ 0 & 0 & 3 & 2 & 2 & 1 \end{array}\right)$$

Tedy matice

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

(b) Sloupce matice jsou na sebe kolmé a mají jednotkovou velikost. Proto je matice ortogonální.

(c) Protože je A ortogonální je $A^{-1} = A^T = A$. Jiné zdůvodnění spočívá v tom, že se spočítá součin $A \cdot A = E$. □

Bodování. **(a)** Úvaha, kam se zobrazuje u **1 bod**
Výběr dvou nezávislých vektorů z kolmé roviny a úvaha, kam se zobrazují **1 bod**
Sestavení schématu/soustavy pro výpočet matice **1 bod**
Výpočet matice **1 bod**

(b) Zdůvodnění ortogonality **1 bod**

(c) Výpočet inverze **1 bod** □

Příklad. **3A.** Matematik musí v rámci plnění svých pracovních povinností mnohokrát denně procházet mezi kampusem a ulicí. Rád si přitom prodlužuje cestu průchodem botanickou zahradou. Dvě zahradní branky (mezi kampusem a zahradou a mezi ulicí a zahradou) náhodně a nezávisle zamyká a odemyká vrátný, v důsledku čehož bývá každá z nich otevřená s pravděpodobností $1/2$. Přímý průchod vrátnicí mezi kampusem a ulicí je vždy otevřený. Chování matematika je popsáno pravidly:

- Pokud se dostane do kampusu nebo na ulici *z jiného místa*, vykročí v příštím tahu směrem do zahrady.
- Pokud je v zahradě, snaží se pokračovat v načatém směru pochodu.
- Vždy když narazí na zamknutou branku, otočí se a v příštím tahu půjde ke druhému východu.

Všechny jednotkové přesuny i neúspěšné pokusy o překonání branky trvají stejnou dobu. Modelujte pohyb matematika pomocí Markovova procesu. [Návod: stav je definován pozicí i orientací, celkem jich tak bude šest.]

(a) Napište matici tohoto procesu.
(b) Určete řádek a sloupec prvku matice označující přechod ze stavu „matematik je v zahradě a míří do kampusu“ do stavu „matematik je v kampusu a míří do zahrady“.
(c) Určete, na kterém místě se bude po delším čase matematik nacházet nejčastěji a určete s jakou pravděpodobností.
(d) Předpokládejme, že na začátku byl matematik v kampusu a hleděl k zahradě. Určete, s jakou pravděpodobností skončí za tři tahy na ulici.

Řešení. **(a)** Označme si třeba směr kampus–ulice–zahrada–kampus jako kladný a směr kampus–zahrada–ulice–kampus jako záporný. Pro posloupnost stavů $(K^-, K^+, Z^-, Z^+, U^-, U^+)$ dostaneme matici

$$M = \begin{pmatrix} 0 & 0 & 0 & 1/2 & 1 & 0 \\ 1/2 & 0 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 1/2 \\ 0 & 1 & 1/2 & 0 & 0 & 0 \end{pmatrix}$$

(b) V našem označení se jedná o přechod $Z^+ \to K^-$, tedy prvek v prvním řádku a čtvrtém sloupci.

(c) Spočítáme pravděpodobnostní vlastní vektor k vlastnímu číslu 1 matice M.

$$(M - E)x = 0, \quad x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 1.$$

To vede na homogenní soustavu

$$\begin{pmatrix} -1 & 0 & 0 & 1/2 & 1 & 0 \\ 1/2 & -1 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & -1 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & -1 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & -1 & 1/2 \\ 0 & 1 & 1/2 & 0 & 0 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & -2 \\ 0 & 0 & 1 & -2 & 0 & 1 \\ 0 & 0 & 0 & 5 & 0 & -5 \\ 0 & 0 & 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Řešení je $x = \frac{1}{10}(2, 1, 2, 2, 1, 2)^T$. Nejčastěji se matematik nachází v zahradě, a to s pravděpodobností $\frac{2}{10} + \frac{2}{10} = \frac{4}{10}$.

(d) Hledaná pravděpodobnost je součet páté a šesté složky vektoru $M^3 \cdot (1, 0, 0, 0, 0, 0)^T$ a to jsou $3/8$. □

Bodování. (a) Matice **2 body**
(b) Význam koeficientu **1 bod**
(c) Vlastní vektor **1 bod**, místo a pravděpodobnost **1 bod**
(d) Postup a výpočet **1 bod** □

Příklad. **4A.** Šifrou RSA s veřejným klíčem $n = 119$ a šifrovacím exponentem $e = 31$ bylo posláno číslo $Z = 53$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, 2, \ldots, 119\}$. [Návod: využívejte rozklad modulu na součin mocnin prvočísel.]

Řešení. K prolomení šifry potřebujeme najít inverzi d exponentu e modulo $\varphi(119) = 96$, což umíme provést několika způsoby. Např. rozložením $96 = 3 \cdot 32$ dostaneme soustavu kongruencí

$$31d \equiv 1 \mod 3, \qquad 31d \equiv 1 \mod 32,$$

které nejprve vyřešíme odděleně

$$d \equiv 1 \mod 3, \qquad d \equiv -1 \mod 32,$$

a poté najdeme společný výsledek pro původní modul $d \equiv 31 \mod 96$.

Dešifrování zprávy provedeme umocněním $Z^d \mod 119$. Opět se vyplatí využít rozklad modulu $119 = 7 \cdot 17$. S využitím malé Fermatovy věty v prvním kroku dostáváme

$$53^{31} \equiv 4^1 = 4 \mod 7$$

a

$$53^{31} \equiv 2^{15} = 2 \cdot 4^7 = 8 \cdot 16^3 \equiv 8 \cdot (-1)^3 = -8 \equiv 9 \mod 17,$$

odkud již určíme $53^{31} \equiv 60 \mod 119$. □

Bodování. Úvaha, že dešifrovaná zpráva je tvaru $Z^d \mod n$, kde $ed \equiv 1 \mod \varphi(n)$ **1 bod**
Výpočet $\varphi(n)$ **1 bod**
Výpočet inverze $d = e^{-1}$ **2 body**
Dešifrování zprávy **2 body** □