MB141, 13. 9. 2023, zkouška, skupina Y

Příklad. 1A. [2 body] Uvažujme vektorový prostor $\mathbb{R}^4$. Rozhodněte, které z vektorů

$$u_1 = (2, 0, 1, 1), \qquad u_2 = (1, -1, -5, -1)$$

patří do podprostoru P generovaného vektory

$$v_1 = (1, 1, -1, -1), \qquad v_2 = (1, 3, 3, 1), \qquad v_3 = (0, 1, 2, 3).$$

Řešení. Vektory v_1, v_2, v_3 naskládáme jako sloupce nalevo do maticového schématu. Kdybychom testovali jeden vektor, zařadili bychom ho napravo a zjišťovali, zda navyšuje hodnost matice, či ekvivalentně, zda má odpovídající soustava rovnic řešení. Úpravy na schodový tvar by se ovšem prováděly pro oba vektory u_1, u_2 stejně, můžeme si tedy postup racionalizovat a vyřešit jediným schématem, kde vypíšeme vpravo oba vektory:

$$\left(\begin{array}{ccc|cc} 1 & 1 & 0 & 2 & 1 \\ 1 & 3 & 1 & 0 & -1 \\ -1 & 3 & 2 & 1 & -5 \\ -1 & 1 & 3 & 1 & -1 \end{array}\right) \sim \cdots \sim \left(\begin{array}{ccc|cc} 1 & 1 & 0 & 1 & 2 \\ 0 & 2 & 1 & -2 & -2 \\ 0 & 0 & 2 & 2 & 5 \\ 0 & 0 & 0 & 7 & 0 \end{array}\right)$$

Sloupec vektoru u_1 vyčnívá za poslední schod určený levou stranou, zvýšil by tak hodnost hodnost matice, a proto v podprostoru P neleží. Naopak u_2 se do tohoto posledního schodu vejde, tj. je nutně lineární kombinací vektorů v_1, v_2, v_3 a patří tedy do P. □

Příklad. 1B. [2 body] Nechť zobrazení $f : \mathbb{R}^3 \to \mathbb{R}^3$ je symetrií (zrcadlením) podle roviny $\rho : x_2 = 0$. Najděte matici M takovou, že v souřadnicích standardní báze je $f(x) = Mx$.

Řešení. Normálovým vektorem roviny ρ je $n = (0, 1, 0)$. Ten se při zrcedlení zobrazí na opačný vektor: $f(n) = -n$. V rovině ρ leží mimo jiné další dva vektory standardní báze $u = (1, 0, 0)$ a $v = (0, 0, 1)$ a ty zůstávají při zrcadlení na místě: $f(u) = u, f(v) = v$. Protože známe obrazy všech vektorů standardní báze, jejich prostým poskládáním do sloupců dostáváme ihned matici M:

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

□

Příklad. 1C. [2 body] V prostoru $\mathbb{R}^3$ určete průnik roviny $\rho : x - 3y + 2z = 1$ a přímky $p : x - y = 1, y - z = -1$. Jaká je jejich vzájemná poloha?

Řešení. Body průniku musí současně vyhovovat všem rovnicím, budeme je tedy řešit jako soustavu lineárních rovnic:

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

Soustava zřejmě nemá řešení, podprostory jsou tedy rovnoběžné. □

Příklad. 2A. [2 body] Najděte celá čísla x, y, aby platilo

$$23x + 18y = 1.$$

Řešení. Čísla $23, 18$ jsou nesoudělná, tedy podle Bezoutovy věty má rovnice řešení. Toto řešení lze nalézt postupným dělením se zbytkem podle Eukleidova algoritmu a zpětným dosazováním:

$$\begin{aligned} 23 &= 18 + 5, & 18(x+y) + 5x &= 1, \\ 18 &= 3 \cdot 5 + 3, & 5(4x+3y) + 3(x+y) &= 1, \\ 5 &= 3 + 2, & 3(5x+4y) + 2(4x+3y) &= 1, \\ 3 &= 2 + 1, & 2(9x+7y) + (5x+4y) &= 1. \end{aligned}$$

Soustava

$$9x + 7y = 0, \qquad 5x + 4y = 1$$

má řešení $x = -7, y = 9$ a to je i odpověď na původní úlohu. □

Příklad. **2B.** [5 bodů] a) Prolomte šifru RSA s veřejným klíčem $n = 247 = 13 \cdot 19, e = 23$, tj. najděte inverzi d k e modulo $\phi(n)$.

b) V daném kryptosystému zašifrujte zprávu $M = 15$ jako $C = M^e \pmod n$. Při výpočtu doporučujeme počítat C nejdřív zvlášť modulo 13 a modulo 19 a využít Eulerovy věty pro zjednodušení (zredukování) exponentu, poté dát tyto výsledky dohromady pomocí Čínské zbytkové věty.

Řešení. a) Protože $247 = 13 \cdot 19$, snadno určíme $\phi(n) = 12 \cdot 18 = 216$. Kongruence $23d \equiv 1 \pmod{216}$ má řešení $d \equiv 47$.

b) Dostáváme $15^{23} \equiv 2^{11} \equiv 2 \cdot 4^5 \equiv 8 \cdot 3^2 \equiv 7 \pmod{13}$ a $15^{23} \equiv (-4)^5 \equiv -4 \cdot (-3)^2 \equiv 2 \pmod{19}$. Z druhé kongruence $15^{23} = 19t + 2$, dosazením do první a vyřešením dostaneme $t \equiv 3 \pmod{13}$, takže $C \equiv 15^{23} \equiv 59 \pmod{247}$. □

Příklad. **3A.** [2 body] Určete vzdálenost bodu $A = [3, 2]$ od přímky $p : 2x - y = -1$ v rovině $\mathbb{R}^2$.

Řešení. Vzdálenost se bude realizovat ve směru kolmém na přímku, tedy ve směru normálového vektoru $n = (2, -1)$. Pata kolmice B na přímce p je tedy tvaru $A + tn$ pro vhodné t a současně splňuje rovnici přímky. Dosazením tohoto parametrického vyjádření dostaneme rovnici

$$2(3 + 2t) - (2 - t) = -1,$$

jejímž řešením je $t = -1$. Vzdálenost určíme jako velikost vektoru tn:

$$d(A, p) = \|tn\| = |t| \cdot \|n\| = |-1| \cdot \sqrt{2^2 + (-1)^2} = \sqrt{5}.$$

□

Příklad. **3B.** [5 bodů] Uvažujeme třístavový Markovův řetězec se stavy A, B, C a pravděpodobnostmi přechodů

$$\begin{aligned} &P(A \to A) = 0, && P(A \to B) = 1/2, && P(B \to A) = 1/3, \\ &P(B \to B) = 1/3, && P(A \to C) = 1/2, && P(C \to A) = 0, \\ &P(B \to C) = 1/3, && P(C \to B) = 1/2, && P(C \to C) = 1/2, \end{aligned}$$

a) Sestavte přechodovou pravděpodobnostní matici M a ověřte, že je primitivní, tj. že nějaká mocnina M^k má všechny členy kladné.

b) Určete pravděpodobnost, s jakou se bude po dostatečně dlouhé době systém dostávat do stavu A.

Řešení. a) Matici sestavujeme tak, aby vstupní stavy odpovídaly sloupcům a výstupní stavy řádkům. Při dodržení abecedního pořadí stavů dostaneme matici

$$M = \begin{pmatrix} 0 & 1/3 & 0 \\ 1/2 & 1/3 & 1/2 \\ 1/2 & 1/3 & 1/2 \end{pmatrix}.$$

Primitivnost můžeme prověřit symbolickým umocňováním matice $\left(\begin{smallmatrix} 0 & + & 0 \\ + & + & + \\ + & + & + \end{smallmatrix}\right)$, přičemž zjistíme, že již M^2 je pozitivní.

b) Hledáme vlastní vektor pro vlastní číslo 1, tj. řešíme homogenní soustavu $(M-E)x = 0$. Netriviálním řešením je například vektor $x = (1,3,3)$. Jeho vydělením číslem $1+3+3=7$ dostaneme pravděpodobnostní vektor $(1/7, 3/7, 3/7)$. Stav A tedy bude navštěvován s pravděpodobností $1/7$. □