MB141, 23. 5. 2023, zkouška, skupina Y

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

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

patří do podprostoru P generovaného vektory

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

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:

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

Sloupec vektoru u_2 vyčnívá za poslední schod určený levou stranou, zvýšil by tak hodnost hodnost matice, a proto v podprostoru P neleží. Naopak u_1 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 $\rho : x_3 = 0$. Najděte matici M takovou, že v souřadnicích standardní báze je $f(x) = Mx$.

Řešení. Normálovým vektorem roviny ρ je $n = (0, 0, 1)$. 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 $v = (0, 1, 0)$ 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:

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

Soustava má zřejmě nekonečně mnoho řešení (s jedním parametrem), průnikem je tak celá přímka p a platí $p \subseteq \rho$. □

Příklad. **2A.** [2 body] Určete zbytek po dělení čísla $9^{(9^9)}$ třinácti.

Řešení. Podle malé Fermatovy věty platí $9^{12} \equiv 1 \pmod{13}$, čehož využijeme ke snížení exponentu 9^9 na jeho zbytek po dělení dvanácti. Platí $9^2 \equiv 9 \pmod{12}$, takže $9^9 = 9 \cdot ((9^2)^2)^2 \equiv 9 \pmod{12}$; podobně $9^2 \equiv 3 \pmod{13}$, proto $9^{9^9} \equiv 9^9 = 9 \cdot ((9^2)^2)^2 \equiv 9 \cdot (3^2)^2 \equiv 9 \cdot 9^2 \equiv 9 \cdot 3 \equiv 1 \pmod{13}$. Zbytek po dělení čísla 9^{9^9} třinácti je 1. □

Příklad. **2B.** [5 bodů] Alice a Bob používají pro šifrovanou komunikaci protokol ElGamal. Veřejnými informacemi jsou modul 13 a primitivní kořen $g = 6$.

a) Ověřte, že g je skutečně primitivní kořen.

b) Útočnici Evě se podařilo vyzvědět společný soukromý klíč $g^{ab} = 7$, z nějž díky výpočtům v části a) zvládla určit exponent $ab = ?$, a také Bobův soukromý klíč $b = 5$. Pomozte Evě dokončit rozbití šifry a určete Alicin soukromý klíč a.

Řešení. a) Číslo g je primitivním kořenem, pokud $\phi(13) = 12$ je nejmenší přirozený exponent x, pro nějž je $g^x \equiv 1 \pmod{13}$. Protože $12 = 2^2 \cdot 3$, stačí prověřit mocniny g pro maximální dělitele 12, což jsou 4 a 6. (Pokud $g^4 \not\equiv 1$ a $g^6 \not\equiv 1$, pak $g^x \equiv 1$ až pro $x = 12$.) Dostáváme (vše v modulu 13):

$$\begin{aligned} 6^2 &= 36 \equiv -3, \\ 6^4 &\equiv (-3)^2 \equiv -4 \not\equiv 1, \\ 6^6 &\equiv (-3)^3 \equiv -4 \cdot (-3) \equiv -1 \not\equiv 1, \end{aligned}$$

tedy $g = 6$ je primitivní.

b) Potřebujeme s co nejmenší námahou zjistit exponent ab ze znalosti společného klíče $g^{ab} \equiv 7$, odkud se znalostí b už snadno určíme a. Ve výpočtech z a) jsme zjistili, že $6^1 \equiv 6$ a $6^6 \equiv -1$, z čehož plyne $6^7 \equiv 6^{1+6} \equiv 6 \cdot (-1) \equiv -6 \equiv 7$. To znamená, že $ab \equiv 5a \equiv 7 \pmod{12}$ a tedy $a \equiv 11 \pmod{12}$. □

Příklad. **3A.** [2 body] Určete vzdálenost bodu $A = [5, 2]$ od přímky $p : x + 3y = 1$ v rovině $\mathbb{R}^2$.

Řešení. Vzdálenost se bude realizovat ve směru kolmém na přímku, tedy ve směru normálového vektoru $n = (1, 3)$. 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

$$(5 + t) + 3(2 + 3t) = 1,$$

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

$$d(A, p) = \|tn\| = |t| \cdot \|n\| = |-1| \cdot \sqrt{1^2 + 3^2} = \sqrt{10}.$$

□

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

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

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

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

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 $x = (3, 3, 1)$. Jeho vydělením číslem $3 + 3 + 1 = 7$ dostaneme pravděpodobnostní vektor $(3/7, 3/7, 1/7)$. Stav A tedy bude navštěvován s pravděpodobností $3/7$. □