A. Zkouška z MB141, 25. 5. 2022

Příklad. 1A. [6 bodů] V $\mathcal{A}_4$ jsou dány tři body body $A = [1, 2, 1, 2]$, $B = [2, 0, 1, 3]$, $C = [0, 1, -2, 4]$ a afinní podprostor $\mathcal{M}$ zadaný rovnicí

$$x_1 + x_2 - x_3 - x_4 = -1.$$

(a) Napište parametrickou rovnici roviny ρ, která je určena body A, B, C. [2 body]
(b) Napište obecný (implicitní) popis roviny ρ pomocí soustavy rovnic. [2 body]
(c) Spočítejte průnik $\rho \cap \mathcal{M}$. [2 body]

Řešení. **(a)** Parametrická rovnice roviny ρ je

$$A + a(B - A) + b(C - A) = [1, 2, 1, 2] + a(1, -2, 0, 1) + b(-1, -1, -3, 2).$$

(b) Nejdříve najdeme homogenní soustavu rovnic pro zaměření roviny ρ. Pro hledané koeficienty c_1, c_2, c_3, c_4 rovnic $c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 = 0$ musí platit soustava rovnic

$$c_1 - 2c_2 + c_4 = 0, \quad -c_1 - c_2 - 3c_3 + 2c_4 = 0$$

Její řešení je $s(1, 1, 0, 1) + t(2, 1, -1, 0)$. Homogenní rovnice jsou

$$x_1 + x_2 + x_4 = 0, \quad 2x_1 + x_2 - x_3 = 0.$$

Dosazením souřadnic bodu A do levých stran dostaneme soustavu rovnic pro π

$$x_1 + x_2 + x_4 = 5, \quad 2x_1 + x_2 - x_3 = 3.$$

(c) Průnik $\rho \cap \mathcal{M}$ spočítáme tak, že parametrické vyjádření roviny ρ

$$x_1 = 1 + a - b,\ x_2 = 2 - 2a - b,\ x_3 = 1 - 3b,\ x_4 = 2 + a + 2b$$

dosadíme do rovnice pro $\mathcal{M}$. Dostaneme rovnici

$$-2a - b = -1,$$

která má řešení $a = t$, $b = 1 - 2t$. Dosazením do parametrické rovnice pro ρ dostaneme parametrické vyjádření průniku, kterým je přímka

$$[0, 1, -2, 4] + t(3, 0, 6, -3) = [0, 1, -2, 4] + p(1, 0, 2, -1).$$

Jiným způsobem lze průnik spočítat řešením tří rovnic z obecných popisů afinních podprostorů. Matice soustavy je

$$\left(\begin{array}{cccc|c} 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & 0 & 1 & 5 \\ 2 & 1 & -1 & 0 & 3 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 5 \\ 0 & -1 & 1 & 2 & 5 \\ 0 & 0 & 1 & 2 & 6 \end{array}\right)$$

Řešením je přímka $[4, 1, 6, 0] + p(1, 0, 2, -1) = [0, 1, -2, 4] + p(1, 0, 2, -1)$.

Řešení, které hledá prvně parametrické vyjádření pro $\mathcal{M}$ a průnik hledá z parametrických vyjádření obou afinních podprostorů je nešikovné, zdlouhavé, a proto při něm dojde lehce k chybě. □

Bodování. Parametrické vyjádření roviny ρ za **2 body**. Soustava rovnic pro ρ, správný postup **1 bod**, výsledek **1 bod**. Vhodný postup výpočtu průniku **1 bod** , správný výsledek **1 bod**. □

Příklad. **2A.** [6 bodů] Ukažte, že matice

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

je ortogonální, a zjistěte, jaké geometrické zobrazení v $\mathcal{E}_3$ popisuje předpis $\varphi(x) = Ax$, kde $x = (x_1, x_2, x_3)^T$ je sloupec standardních souřadnic v $\mathcal{E}_3$. V případě symetrie popište explicitně osu nebo rovinu symetrie, v případě otočení určete osu otáčení a kosinus úhlu otočení.

Řešení. Sloupce matice jsou na sebe kolmé a mají jednotkovou velikost. Proto je matice ortogonální. Jinak to lze ověřit tak, že spočítáme $A \cdot A^T = E$.

Spočítáme determinant matice A. Ten je roven 1, proto musí mít matice vlastní číslo 1 a proto je také dané zobrazení otočení kolem osy procházející počátkem se směrovým vektorem, který je vlastním vektorem k vlastnímu číslu 1.

Jinak. Zkusíme, zda matice má vlastní číslo 1 a -1. Zjistíme, že má pouze jedno reálné vlastní číslo, a to 1. Proto je dané zobrazení otočení kolem osy procházející počátkem se směrovým vektorem, který je vlastním vektorem k vlastnímu číslu 1.

Spočítáme vlastní vektor k vlastnímu číslu 1. Jsou to násobky vektoru $u = (1, 1, 3)^T$. Je dobré provést kontrolu tím, že se přesvědčíme, že skutečně $Au = u$.

Nyní zjistíme úhel otočení α. Vezmeme nějaký nenulový vektor kolmý k u, např. $v = (1, -1, 0)^T$. Spočítáme

$$Av = \left(-\frac{1}{3}, \frac{4}{3}, -\frac{1}{3}\right)^T.$$

Cosinus úhlu otočení bude

$$\cos\alpha = \frac{\langle v, Av\rangle}{||v|| \cdot ||Av||} = -\frac{5}{6}.$$

Závěr: Dané zobrazení je otočení kolem osy $[0, 0, 0] + a(1, 1, 3)$ o úhel α.

□

Bodování. Kontrola ortogonality **1 bod**.

Výpočet determinantu **1 bod**, výpočet vlastního vektoru k 1 **1 bod**

NEBO zjištění, že 1 je vlastní číslo, ale -1 nikoliv **1 bod**, výpočet vlastního vektoru k 1 **1 bod** .

Úvaha, že jde o otočení kolem osy určené vlastním vektorem k 1 **1 bod**.

Volba kolmého vektoru v a jeho zobrazení Av **1 bod**.

Výpočet cosinu úhlu otočení **1 bod**.

□

Příklad. **3A.** [6 bodů] Profesor má 3 oblíbené otázky, z kterých se u každého zkouškového termínu jedna objeví. Profesor nikdy nepoužije stejné otázky po sobě. Když naposledy použil otázku 1, hodí mincí a v případě, že padne líc, zadá otázku 2. Když použil otázku 2, hází 2 mincemi a přejde k otázce 3, pokud je líc na obou mincích. Pokud naposledy zadal otázku 3, tak si hodí 3 mincemi a přejde k otázce 1, když na všech třech padl líc.

(a) Modelujte zadávání otázek pomocí Markovova procesu. Určete jeho matici. [2 body]
(b) Pomocí maticového násobení zjistěte, jaká je pravděpodobnost, že u třetího termínu zadá otázku 2, jestliže u prvního zadal otázku 1. [1 bod]
(c) Za předpokladu, že tímto způsobem zadává otázky hodně dlouho, zjistěte, kterou otázku zadává nejčastěji - výsledek vyjádřete v procentech a vysvětlete, jak jste k němu dospěli. [3 body]

Řešení. Matice Markovova procesu je

$$M = \begin{pmatrix} 0 & 3/4 & 1/8 \\ 1/2 & 0 & 7/8 \\ 1/2 & 1/4 & 0 \end{pmatrix}$$

Spočteme-li $M^2 = M \cdot M$, dostaneme matici se všemi vstupy kladnými. Proto je M primitivní matice.

Pravděpodobnost, že profesor zadá u třetího termínu 2. otázku, když u prvního zadal 1. otázku je dána druhou složkou součinu

$$M \cdot M \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

a ta je $7/16$.

Při dlouhodobém zadávání se pravděpodobnosti zadání jednotlivých otázek blíží pravděpodobnostnímu vektoru, který je vlastním vektorem matice M k vlastnímu číslu 1. Řešíme proto homogenní soustavu

$$(M - E)x = 0.$$

Její matici upravíme na schodovitý tvar

$$\begin{pmatrix} -1 & 3/4 & 1/8 \\ 1/2 & -1 & 7/8 \\ 1/2 & 1/4 & -1 \end{pmatrix} \sim \begin{pmatrix} 4 & -8 & 7 \\ 0 & -2 & 3 \\ 0 & 0 & 0 \end{pmatrix}.$$

Vlastní vektory jsou $a(5, 6, 4)$. Pravděpodobnostní vektor je

$$(1/3, 2/5, 4/15).$$

V dlouhodobém horizontu pokládá profesor nejčastěji otázku 2, a to s pravděpodobností $2/5$, tj. 40%. □

Bodování. Správná matice **2 body**.

Výpočet $7/16$ **1 bod**.

Soustava pro vlastní vektor a její úprava na schodovitý tvar **1 bod**.

Správné řešení ve formě pravděpodobnostního vektoru **1 bod**.

Správné určení otázky a správná procenta **1 bod**. □

Příklad. **4A.** [6 bodů] Julie a Romeo komunikují šifrou Elgamal. Oba se dohodli na prvočísle $p = 19$ a na primitivním kořenu $g = 10$. Julie si za svůj tajný klíč zvolila číslo $a = 11$, Romeo má svůj tajný klíč b.

(a) Ověřte, že 10 je skutečně primitivní kořen modulo 19. [1 bod]
(b) Jaký údaj poskytla Julie Romeovi? [1 bod]
(c) Romeo posléze poslal Julii jako zprávu dvojici čísel $(g^b \equiv 7,\ 4)$. Pomozte Julii s dešifrováním zprávy. [4 body]

Proveďte celý výpočet bez použití kalkulačky nebo jakéhokoliv softwaru.

Řešení. **(a)** $\varphi(19) = 18 = 2 \cdot 3^2$. Proto $10^{18} \equiv 1 \mod 19$. Počítáme modulo 19

$$10^6 \equiv 100^3 \equiv 5^3 \equiv 6 \cdot 5 \equiv 11,$$
$$10^9 \equiv 10^6 \cdot 100 \cdot 10 \equiv 11 \cdot 5 \cdot 10 \equiv 11 \cdot 12 \equiv 8 \cdot 7 \equiv 18.$$

Tedy 10 je primitivní kořen.

(b) Julie poskytla údaj

$$g^a \equiv 10^{11} \equiv 10^9 \cdot 100 \equiv (-1) \cdot 5 \equiv 14, \mod 19.$$

(c) Romeo zašifroval zprávu M jako dvojici $(g^b, M(g^a)^b) = (7, 4)$. Proto dešifrujeme takto

$$M \equiv M(g^a)^b \cdot \left(g^b\right)^a)^{-1} \equiv 4 \cdot \left(7^{11}\right)^{-1} \equiv 4 \cdot (11)^{-1} \equiv 4 \cdot 7 \equiv 9 \mod 19.$$

Výpočet

$$7^{11} \equiv 49^5 \cdot 7 \equiv 11^5 \cdot 7 \equiv (-8)^5 \cdot 7 \equiv -64^2 \cdot 56 \equiv -7^2(-1) \equiv 11 \mod 19.$$

Inverze k $11 \mod 19$ se najde jako číslo a takové, že $11a + 19b = 1$ pro nějaké b. Jednoduše $(a, b) = (7, -4)$. Inverze je tedy 7.

□

Bodování. **(a)** Za $\varphi(19)$, jeho rozklad a za 6. a 9. mocninu 10 **1 bod**.
(b) Ví, co má počítat, a správná mocnina **1 bod**.
(c) Správný vzorec **2 body**.
Mocnina a inverze **1 bod**.
Správný výsledek **1 bod**. □

B. Zkouška z MB141, 25. 5. 2022

Příklad. 1B. [6 bodů] V $\mathcal{A}_4$ jsou dány tři body body $P = [2,1,1,2]$, $Q = [0,2,1,3]$, $R = [1,0,-2,4]$ a afinní podprostor $\mathcal{N}$ zadaný rovnicí

$$x_1 + x_2 - x_3 - x_4 = -1.$$

(a) Napište parametrickou rovnici roviny π, která je určena body P, Q, R. [2 body]
(b) Napište obecný (implicitní) popis roviny π pomocí soustavy rovnic. [2 body]
(c) Spočítejte průnik $\pi \cap \mathcal{N}$. [2 body]

Řešení. **(a)** Parametrická rovnice roviny π je

$$P + a(Q-P) + b(R-P) = [2,1,1,2] + a(-2,1,0,1) + b(-1,-1,-3,2).$$

(b) Nejdříve najdeme homogenní soustavu rovnic pro zaměření roviny ρ. Pro hledané koeficienty c_1, c_2, c_3, c_4 rovnic $c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 = 0$ musí platit soustava rovnic

$$-2c_1 + c_2 + c_4 = 0, \quad -c_1 - c_2 - 3c_3 + 2c_4 = 0$$

Její řešení je $s(1,1,0,1) + t(1,2,-1,0)$. Homogenní rovnice jsou

$$x_1 + x_2 + x_4 = 0, \quad x_1 + 2x_2 - x_3 = 0.$$

Dosazením souřadnic bodu P do levých stran dostaneme soustavu rovnic pro ρ

$$x_1 + x_2 + x_4 = 5, \quad x_1 + 2x_2 - x_3 = 3.$$

(c) Průnik $\pi \cap \mathcal{N}$ spočítáme tak, že parametrické vyjádření roviny π

$$x_1 = 2 - 2a - b,\ x_2 = 1 + a - b,\ x_3 = 1 - 3b,\ x_4 = 2 + a + 2b$$

dosadíme do rovnice pro $\mathcal{N}$. Dostaneme rovnici

$$-2a - b = -1,$$

která má řešení $a = t$, $b = 1 - 2t$. Dosazením do parametrické rovnice pro π dostaneme parametrické vyjádření průniku, kterým je přímka

$$[1,0,-2,4] + t(0,3,6,-3) = [1,0,-2,4] + p(0,1,2,-1).$$

Jiným způsobem lze průnik spočítat řešením tří rovnic z obecných popisů afinních podprostorů. Matice soustavy je

$$\left(\begin{array}{cccc|c} 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & 0 & 1 & 5 \\ 1 & 2 & -1 & 0 & 3 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 5 \\ 0 & 1 & 0 & 1 & 4 \\ 0 & 0 & 1 & 2 & 6 \end{array}\right)$$

Řešením je přímka $[1,4,6,0] + p(0,1,2,-1) = [1,0,-2,4] + p(0,1,2,-1)$.

Řešení, které hledá prvně parametrické vyjádření pro $\mathcal{N}$ a průnik hledá z parametrických vyjádření obou afinních podprostorů je nešikovné, zdlouhavé, a proto při něm dojde lehce k chybě. □

Bodování. Parametrické vyjádření roviny π za **2 body**. Soustava rovnic pro π, správný postup **1 bod**, správný výsledek **1 bod**. Vhodný postup výpočtu průniku **1 bod**, správný výsledek **1 bod**. □

Příklad. **2B.** [6 bodů] Ukažte, že matice

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

je ortogonální, a zjistěte, jaké geometrické zobrazení v $\mathcal{E}_3$ popisuje předpis $\varphi(x) = Bx$, kde $x = (x_1, x_2, x_3)^T$ je sloupec standardních souřadnic v $\mathcal{E}_3$. V případě symetrie popište explicitně osu nebo rovinu symetrie, v případě otočení určete osu otáčení a kosinus úhlu otočení.

Řešení. Sloupce matice jsou na sebe kolmé a mají jednotkovou velikost. Proto je matice ortogonální. Jinak to lze ověřit tak, že spočítáme $B \cdot B^T = E$.

Spočítáme determinant matice B. Ten je roven 1, proto musí mít matice vlastní číslo 1 a proto je také dané zobrazení otočení kolem osy procházející počátkem se směrovým vektorem, který je vlastním vektorem k vlastnímu číslu 1.

Jinak. Zkusíme, zda matice má vlastní číslo 1 a -1. Zjistíme, že má pouze jedno reálné vlastní číslo, a to 1. Proto je dané zobrazení otočení kolem osy procházející počátkem se směrovým vektorem, který je vlastním vektorem k vlastnímu číslu 1.

Spočítáme vlastní vektor k vlastnímu číslu 1. Jsou to násobky vektoru $u = (1, 3, 1)^T$. Je dobré provést kontrolu tím, že se přesvědčíme, že skutečně $Bu = u$.

Nyní zjistíme úhel otočení β. Vezmeme nějaký nenulový vektor kolmý k u, např. $v = (-1, 0, 1)^T$. Spočítáme

$$Bv = \frac{1}{3}(1, 1, -4)^T.$$

Cosinus úhlu otočení bude

$$\cos\beta = \frac{\langle v, Bv\rangle}{||v|| \cdot ||Bv||} = -\frac{5}{6}.$$

Závěr: Dané zobrazení je otočení kolem osy $[0, 0, 0] + a(1, 3, 1)$ o úhel β.

□

Bodování. Kontrola ortogonality **1 bod**.

Výpočet determinantu **1 bod**, výpočet vlastního vektoru k 1 **1 bod**

NEBO zjištění, že 1 je vlastní číslo, ale -1 nikoliv **1 bod**, výpočet vlastního vektoru k 1 **1 bod** .

Úvaha, že jde o otočení kolem osy určené vlastním vektorem k 1 **1 bod**.

Volba kolmého vektoru v a jeho zobrazení Bv **1 bod**.

Výpočet cosinu úhlu otočení **1 bod**. □

Příklad. **3B.** [6 bodů] Profesor trpí syndromem vyhoření a u zkoušek už zadává jenom jeden ze tří testů A, B, C. Nikdy však nepoužije po sobě stejné testy. Když naposledy zadal test A, hodí si kostkou a v případě, že padne číslo dělitelné 3, zadá test B. Když použil test B, hází dvěma mincemi a přejde k testu C, pokud na obou padne líc. Když naposledy zadal test C, tak hází opět kostkou a přejde k testu A, pokud na kostce padne prvočíslo.

(a) Modelujte zadávání testů pomocí Markovova procesu. Určete jeho matici. [2 body]
(b) Pomocí maticového násobení zjistěte, jaká je pravděpodobnost, že u třetího termínu zadá test B, jestliže u prvního zadal test C. [1 bod]
(c) Za předpokladu, že tímto způsobem zadává testy hodně dlouho, zjistěte, který test zadává nejčastěji a s jakou pravděpodobností. Vysvětlete, jak jste k výsledku dospěli. [3 body]

Řešení. Matice Markovova procesu je

$$M = \begin{pmatrix} 0 & 3/4 & 1/2 \\ 1/3 & 0 & 1/2 \\ 2/3 & 1/4 & 0 \end{pmatrix}$$

Spočteme-li $M^2 = M \cdot M$, dostaneme matici se všemi vstupy kladnými. Proto je M primitivní matice.

Pravděpodobnost, že profesor zadá u třetího termínu test B, když u prvního zadal test C je dána druhou složkou součinu

$$M \cdot M \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

a ta je $1/6$.

Při dlouhodobém zadávání se pravděpodobnosti zadání jednotlivých testů blíží pravděpodobnostnímu vektoru, který je vlastním vektorem matice M k vlastnímu číslu 1. Řešíme proto homogenní soustavu

$$(M - E)x = 0.$$

Její matici upravíme na schodovitý tvar

$$\begin{pmatrix} -1 & 3/4 & 1/2 \\ 1/3 & -1 & 1/2 \\ 2/3 & 1/4 & -1 \end{pmatrix} \sim \begin{pmatrix} 2 & -6 & 3 \\ 0 & -9 & 8 \\ 0 & 0 & 0 \end{pmatrix}.$$

Vlastní vektory jsou $a(21, 16, 18)$. Pravděpodobnostní vlastní vektor je

$$(21/55, 16/55, 18/55).$$

V dlouhodobém horizontu zadává profesor nejčastěji test A, a to s pravděpodobností $21/55$. □

Bodování. Správná matice **2 body**.
Výpočet $1/6$ **1 bod**.
Soustava pro vlastní vektor a její úprava na schodovitý tvar **1 bod**.
Správné řešení ve formě pravděpodobnostního vektoru **1 bod**.
Správné určení otázky a správná procenta **1 bod**. □

Příklad. **4B.** [6 bodů] Desdemona a Othelo komunikují šifrou Elgamal. Oba se dohodli na prvočísle $p = 23$ a na primitivním kořenu $g = 10$. Desdemona si za svůj tajný klíč zvolila číslo $a = 9$, Othelo má svůj tajný klíč b.

(a) Ověřte, že 10 je skutečně primitivní kořen modulo 23. [5 bodů]
(b) Jaký údaj poskytla Desdemona Othelovi? [5 bodů]
(c) Othelo posléze poslal Desdemoně jako zprávu dvojici čísel $(g^b \equiv 2,\ 19)$. Pomozte Desdemoně s dešifrováním zprávy. [15 bodů]

Proveďte celý výpočet bez použití kalkulačky nebo jakéhokoliv softwaru.

Řešení. **(a)** $\varphi(23) = 22 = 2 \cdot 11$. Proto $10^{22} \equiv 1 \mod 23$. Počítáme modulo 23

$$10^2 \equiv 100 \equiv 8,$$
$$10^{11} \equiv 100^5 \cdot 10 \equiv 8^5 \cdot 10 \equiv 64^2 \cdot 80 \equiv 5^2 \cdot 11 \equiv 22.$$

Tedy 10 je primitivní kořen.

(b) Desdemona poskytla údaj

$$g^a \equiv 10^9 \equiv 100^4 \cdot 10 \equiv 8^4 \cdot 10 \equiv 5^2 \cdot 10 \equiv 20, \mod 23.$$

(c) Othelo zašifroval zprávu M jako dvojici $(g^b, M(g^a)^b) = (2, 19)$. Proto dešifrujeme takto

$$M \equiv M(g^a)^b \cdot \left(g^b)^a\right)^{-1} \equiv 19 \cdot \left(2^9\right)^{-1} \equiv 19 \cdot (6)^{-1} \equiv 19 \cdot 4 \equiv 7 \mod 23.$$

Výpočet

$$2^9 \equiv 16^2 \cdot 2 \equiv 7^2 \cdot 2 \equiv 3 \cdot 2 \equiv 6 \mod 23.$$

Inverze k $6 \mod 19$ se najde jako číslo a takové, že $6a + 23b = 1$ pro nějaké b. Jednoduše $(a, b) = (4, -1)$. Inverze je tedy 4. □

Bodování. **(a)** Za $\varphi(23)$, jeho rozklad a za 2. a 11. mocninu 10 **1 bod**.
(b) Ví, co má počítat, a správná mocnina **1 bod**.
(c) Správný vzorec **2 body**.
Mocnina a inverze **1 bod**.
Správný výsledek **1 bod**. □