1 Matice pro výpočet lineárních rekurencí (20 bodů)

Na úvod si ve stručnosti popišme, jak počítat Fibonacciho čísla pomocí umocňování matic; ve větších podrobnostech popsáno na konci kapitoly 3.1 textu Povídání o Lineární algebře. Nechť f_n je n-té Fibonacciho číslo, definováno takto:

$$f_0 = 0, \qquad f_1 = 1, \qquad f_{n+2} = f_{n+1} + f_n.$$

Uvažme matici A a vynásobme jí zprava vektorem obsahující dvě po sobě jdoucí Fibonacciho čísla:

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} f_{k+1} \\ f_k \end{pmatrix} = \begin{pmatrix} f_k + f_{k+1} \\ f_{k+1} \end{pmatrix} = \begin{pmatrix} f_{k+2} \\ f_{k+1} \end{pmatrix},$$

tedy násobením A se posouváme v posloupnosti Fibonacciho čísel o jedna doprava. Proto platí, že

$$\underbrace{A \cdot A \cdots A}_{n\text{-krát}} \cdot \begin{pmatrix} f_1 \\ f_0 \end{pmatrix} = A^n \cdot \begin{pmatrix} f_1 \\ f_0 \end{pmatrix} = \begin{pmatrix} f_{n+1} \\ f_n \end{pmatrix},$$

kde první rovnost platí díky asociativitě. Navíc A^n umíme spočítat v čase $\mathcal{O}(\log n)$.[1]

Zkusíme výše uvedený postup zobecnit. Máme nějakou obecnou zadanou lineární rekurentní posloupnost. První členy x_0 až x_{k-1} jsou předepsány. Každý další člen je lineární kombinace k předcházejících členů, tedy platí

$$x_{n+k} = c_{k-1}x_{n+k-1} + c_{k-2}x_{n+k-2} + \cdots + c_1 x_{n+1} + c_0 x_n$$

pro pevné koeficienty c_0 až c_{k-1}.

Příklad. Posloupnost může mít třeba určené první tři členy $x_0 = 1$, $x_1 = 2$, $x_2 = 3$ a další členy jsou určeny předpisem $x_{n+3} = x_{n+2} - x_{n+1} + 3x_n$. Začátek posloupnosti vypadá takto:

$$(1, 2, 3, 4, 7, 12, 17, 26, 45, \ldots).$$

Úloha 1.1. Zobecněte postup výpočtu pro obecnou lineární rekurenci. Pro zadané k a koeficienty $c_0, \ldots, c_{k-1}$ popište, jak se matice A zkonstruuje. Pochopitelně také dokážte, že má požadované vlastnosti. Tím pochopíte, jak jsme matici A pro Fibonacciho čísla získali.

Nápověda. Zkuste nejprve uvažovat posloupnosti pro $k = 2$, tedy posloupnosti, které závisí pouze na dvou předcházejících členech.

Poznámka. Matice A je zajímavá, i když nechceme zkonstruovat rychlý algoritmus. V létě si ukážeme, jak z ní lze vydolovat vzorec pro n-tý člen lineární rekurence. K tomu se budou hodit vlastní čísla matice A. Ta nám umožní převést matici do Jordanova tvaru, ve kterém bude vzorec přímo vidět.

2 Permutační matice (25 bodů)

Permutace již známe z diskrétní matematiky. Permutace π je bijektivní zobrazení $\pi : X \to X$, tedy různým prvkům z X přiřazujeme různé prvky. Intuitivně je permutace pouze nějaké přeuspořádání prvků v X. Nás budou zajímat permutace množiny $X = \{1, 2, \ldots, n\}$.

Pro permutaci π je permutační matice P_π čtvercová matice $n \times n$ daná předpisem:

$$(P_\pi)_{ij} = \begin{cases} 1 & \text{pro } \pi(i) = j, \\ 0 & \text{jinak.} \end{cases}$$

[1] Využijeme půlení, neboť $a^n = \left(a^{\frac{n}{2}}\right)^2$. Pokud tento algoritmus neznáte, zkuste si rozmyslet detaily.

Tedy je to nula-jedničková matice, která má v každém řádku přesně jednu jedničku na pozici $(i, \pi(i))$.

Příklad. Ukážeme si dva příklady. Pro $n = 5$ mějme permutace π a σ dané následujícím předpisem (v druhém řádku je zapsáno, kam se čísla zobrazují):

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \qquad \text{a} \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}.$$

Tyto permutace mají permutační matice P_π a P_σ (s vynechanými nulami):

$$P_\pi = \begin{pmatrix} & 1 & & & \\ & & 1 & & \\ 1 & & & & \\ & & & & 1 \\ & & & 1 & \end{pmatrix} \qquad \text{a} \qquad P_\sigma = \begin{pmatrix} & & 1 & & \\ 1 & & & & \\ & 1 & & & \\ & & & & 1 \\ & & & 1 & \end{pmatrix}.$$

Pro permutační matice vyřešte následující:

Úloha 2.1. Proč se permutačním maticím říká permutační? Uvažte, co permutační matice provádí s maticí A (pochopitelně správné velikosti), pokud ji násobí zleva či zprava.

Úloha 2.2. Permutační matice stejné velikosti lze násobit. Pro libovolné n-prvkové permutace π a σ má $P_\pi P_\sigma$ smysl. Ukažte, že součin permutačních matic je opět permutační matice a objevte, v jakém je vztahu k permutacím π a σ.

Úloha 2.3. Permutační matice mají plnou hodnost, $\operatorname{rank}(P_\pi) = n$. Tedy vždy existuje inverzní matice. Zjistěte pro libovolnou permutaci π, jak vypadá inverzní matice P_π^{-1}.

Úloha 2.4. Ukažte, že pro libovolnou permutační matici P_π existuje mocnina $k \geq 1$, že $P_\pi^k = I_n$. Jaká je nejmenší možná hodnota k?

3 Matice Pascalova trojúhelníku (20 bodů)

Část Pascalova trojúhelníku můžeme zapsat do matice $n \times n$ třemi způsoby: L_n je dolní trojúhelníková matice, U_n je horní trojúhelníková a S_n má zapsaný Pascalův trojúhelník po diagonálách. Formálně, pokud číslujeme prvky matice od 0 do $n - 1$:

$$(L_n)_{i,j} = \binom{i}{j}, \qquad (U_n)_{i,j} = \binom{j}{i}, \qquad (S_n)_{i,j} = \binom{i+j}{i},$$

kde pochopitelně $\binom{i}{j} = 0$ pro nesmyslné hodnoty $j > i$.

Příklad. Například pro $n = 5$ vypadají matice takto (s vynechanými nulami):

$$L_5 = \begin{pmatrix} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 3 & 1 & \\ 1 & 4 & 6 & 4 & 1 \end{pmatrix}, \qquad U_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ & 1 & 2 & 3 & 4 \\ & & 1 & 3 & 6 \\ & & & 1 & 4 \\ & & & & 1 \end{pmatrix}, \qquad S_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 6 & 10 & 15 \\ 1 & 4 & 10 & 20 & 35 \\ 1 & 5 & 15 & 35 & 70 \end{pmatrix}.$$

Úloha 3.1. Jak bude vypadat součin $L_5 U_5$?

Úloha 3.2. Zobecněte získaný výsledek a popište součin $L_n U_n$. Pochopitelně pokud odvodíte obecný vztah, nemusíte řešit předchozí úlohu.

Nápověda. Zkuste objevit co nejvíc důkazů. Lze si součin rozepsat formálně pomocí definice součinu a vzpomenout si na sumy kombinačních čísel. Další možné řešení je provést Gaussovu eliminaci vzniklé matice $L_n U_n$ a udělat její LDU dekompozici. Co budou asi matice L a U? Za každý různý důkaz budou další body (různost posuzuje cvičící :)).

4 Mocniny Jordanovy matice (20 bodů)

Jordanova matice je *bloková diagonální matice* složená z čtvercových bloků umístěných podél diagonály, které se nazývají *Jordanovy buňky*. Jordanova buňka J_λ je matice, která má na diagonále hodnotu λ, nad diagonálou proužek jedniček a zbytek matice je nulový, příklad Jordanovy buňky 5×5 je na obrázku vlevo. Jordanova matice je složena z bloků umístěných na diagonálu, a každý blok je jedna Jordanova buňka. Příklad Jordanovy matice je na obrázku vpravo.

$$J_\lambda = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \lambda & 1 & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix} \qquad J = \begin{pmatrix} J_{\lambda_1} & & & \\ & J_{\lambda_2} & & \\ & & J_{\lambda_3} & \\ & & & J_{\lambda_4} \end{pmatrix}$$

Jordanova věta je jeden z fundamentálních výsledků lineární algebry a říká následující:

Věta (Jordanova normální forma)**.** *Pro každou čtvercovou matici A existuje regulární matice S a Jordanova matice J, že*

$$A = SJS^{-1}.$$

Například pro matici A pro výpočet Fibonacciho čísel z prvního úkolu (či konce kapitoly 3.1 textu Povídání o lineární algebře) dostáváme následující na první pohled odpudivou Jordanovu normální formu:

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \frac{1-\sqrt{5}}{2} & \frac{1+\sqrt{5}}{2} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \frac{1+\sqrt{5}}{2} & \\ & \frac{1-\sqrt{5}}{2} \end{pmatrix} \begin{pmatrix} -\frac{1}{\sqrt{5}} & \frac{\sqrt{5}+1}{2\sqrt{5}} \\ \frac{1}{\sqrt{5}} & \frac{\sqrt{5}-1}{2\sqrt{5}} \end{pmatrix} = SJS^{-1}.$$

Je velice užitečné umět pro matici A spočítat její k-tou mocninu A^k, s tím jsme se už setkali v prvním úkolu pro výše uvedenou A. Přesně v takové situaci se hodí Jordanova věta, která umožňuje A^k přesně určit. Platí totiž:

$$A^k = SJS^{-1}SJS^{1-} \cdots SJS^{-1} = SJ^kS^{-1}.$$

Tedy v případě k-té mocniny stačí umocňovat pouze Jordanovu matici. Například můžete zkusit z výše uvedeného rozkladu vyvodit vzorec pro k-té Fibonacciho číslo

$$f_k = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^k - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^k.$$

Cílem této úlohy je zjistit, jak vypadá k-tá mocnina Jordanovy matice. To lze samozřejmě spočítat přímo z definice maticového násobení, i když postup je to trochu pracný. Ukážeme si trikový výpočet založený na binomické větě. Pro začátek jedna ze základních vlastností blokových diagonálních matic:

Úloha 4.1. Předpokládejme, že umíme umocňovat Jordanovy buňky, tedy známe J_λ^k. Určete J^k v závislosti na J_λ^k.

4.1 Binomická věta

Binomická věta z kombinatoriky je následující identita, která platí pro všechna reálná čísla a a b a přirozená čísla k:

$$(a+b)^k = \binom{n}{0}a^0b^n + \binom{n}{1}a^1b^{n-1} + \binom{n}{2}a^2b^{n-2} + \cdots + \binom{n}{n-1}a^{n-1}b^1 + \binom{n}{n}a^nb^0.$$

Přesně v této podobě však binomická věta pro matice fungovat nemůže, totiž například:

$$(A+B)(A+B) = A(A+B) + B(A+B) = A^2 + AB + BA + B^2.$$

Protože součin matic obecně nekomutuje, neplatí obecně rovnost $(A+B)^2 = A^2 + 2AB + B^2$. Pokud se však $AB = BA$, binomická věta platí. Speciálně jsme ukázali na cvičeních, že αI_n komutuje s libovolnou maticí A.

Úloha 4.2. Čemu se rovná $(A + \alpha I_n)^k$?

4.2 Mocnina Jordanovy buňky

Zbývá vyřešit, jak vypadá k-tá mocnina Jordanovy buňky J_λ^k. To uděláme ve dvou krocích:

Úloha 4.3. Jak vypadá k-tá mocnina J_0^k?

Nápověda. Tady stačí postupovat z definice násobení, ale výsledek vyjde velice hezky.

Úloha 4.4. Jak vypadá k-tá mocnina J_λ^k?

Nápověda. Využijte binomickou větu.

5 Matice s vzorem šachovnice (25 bodů)

Na cvičení jsme dokázali, že třídy $\mathcal{U}$ horních trojúhelníkových matic, $\mathcal{L}$ dolních trojúhelníkových matic a $\mathcal{D}$ diagonálních matic jsou uzavřené na sčítání, násobení a inverze (pochopitelně pouze pokud inverze existují). Tedy například pro $A, B \in \mathcal{U}$ platí $A + B \in \mathcal{U}$, $AB \in \mathcal{U}$ a $A^{-1} \in \mathcal{U}$, pokud operace dávají smysl.

V této úloze chceme zjistit, jestli něco podobného platí pro dvě třídy matic $\check{\mathcal{S}}_\ell$ a $\check{\mathcal{S}}_s$ se šachovnicovým vzorem. Nejprve definujme tyto třídy. Čtvercová matice A patří do $\check{\mathcal{S}}_\ell$, právě když $(A)_{i,j} = 0$, kdykoliv $i + j$ je liché. Podobně čtvercová matice B patří do $\check{\mathcal{S}}_s$, právě když $(B)_{i,j} = 0$, kdykoliv $i + j$ je sudé. Na ostatní políčka matic neklademe žádné předpoklady, tedy například nulová matice patří do obou tříd.

Příklad. Několik příkladů těchto matic (s vynechanými nulami mimo šachovnicový vzor):

$$\underbrace{\begin{pmatrix} 1 & \\ & 2 \end{pmatrix}, \begin{pmatrix} 0 & & 1 \\ & 5 & \\ 0 & & 2 \end{pmatrix}, \begin{pmatrix} 1 & & 0 & \\ & 3 & & 17 \\ 0 & & \frac{1}{2} & \\ & 1 & & 0 \end{pmatrix}}_{\in \check{\mathcal{S}}_\ell} \quad \text{a} \quad \underbrace{\begin{pmatrix} & 1 \\ 2 & \end{pmatrix}, \begin{pmatrix} & 1 & \\ 3 & & 2 \\ & 0 & \end{pmatrix}, \begin{pmatrix} & 4 & & 0 \\ 4 & & 2 & \\ & 2 & & 7 \\ 0 & & 7 & \end{pmatrix}}_{\in \check{\mathcal{S}}_s}.$$

Úloha 5.1. Rozhodněte, zda jsou třídy $\check{\mathcal{S}}_\ell$ a $\check{\mathcal{S}}_s$ uzavřené na součet.

Úloha 5.2. Rozhodněte, zda jsou třídy $\check{\mathcal{S}}_\ell$ a $\check{\mathcal{S}}_s$ uzavřené na součin? Jsou součiny matic z těchto tříd v nějakém dalším vztahu; třeba pro AB, pokud $A \in \check{\mathcal{S}}_\ell$ a $B \in \check{\mathcal{S}}_s$?

Úloha 5.3. Rozhodněte, zda jsou třídy $\check{\mathcal{S}}_\ell$ a $\check{\mathcal{S}}_s$ uzavřené na inverze (opět s předpokladem, že pro A inverzní matice A^{-1} existuje)? Lze pro některé rozměry s jistotou říct, že matice není invertovatelná?

Nápověda. Inverze se počítá pomocí Gaussovy eliminace, která převede tvar $(A \mid I_n)$ na tvar $(I_n \mid A^{-1})$. Nelze nějak vhodně využít vlastností šachovnicového vzoru?

6 Konečná tělesa existují jen pro mocniny prvočísla (40 bodů)

V této úloze si ukážeme část z důkazu následující algebraické věty.

Věta. *Konečné těleso $\mathbb{F}$ řádu $ř$ existuje, právě když $ř$ je mocnina prvočísla p^k.*

Dokonce platí, že konečně těleso daného řádu je určeno jednoznačně (až na přejmenování prvků, kterému se odborně říká *isomorfismus*). Tato věta tedy opodstatňuje označení $\mathbb{GF}(p^k)$, neboť těleso řádu p^k je jednoznačně určené. V důkazu ukážeme, že každé takové těleso je vysoce symetrický objekt, který v sobě skrývá vektorový prostor. To je poměrně překvapivé, neboť v definici tělesa se vektorové prostory vůbec nevyskytují a naopak ty se definují pomocí těles.

Co o tělesech už známe ...

V samotném důkazu můžeme použít *pouze axiomy tělesa* a jejich důsledky! Připomeňme si, co říkají axiomy tělesa:

- Těleso je struktura s dvěma operacemi – sčítáním a násobením.
- Těleso obsahuje dva speciální prvky, neutrální prvek na sčítání (budeme značit 0) a neutrální prvek na násobení (značíme 1).
- Z hlediska sčítání se těleso chová jako grupa – máme inverzní prvky a neutrální prvek.
- Z hlediska násobení se těleso bez 0 chová jako grupa – opět máme inverze a neutrální prvek.
- Navíc operace sčítání a násobení jsou dohromady svázané distributivitou.

Z axiomů lze odvodit i další vlastnosti těles, některé jsme již viděli.

- Neutrální prvky 0 a 1 a inverze pro obě operace jsou určeny jednoznačně. Ostatně to platí obecně i v grupách.
- Libovolný násobek 0 je zase nula: $a \cdot 0 = 0$.
- Pokud $a + b = a + c$, potom $b = c$.
- Podobně pro násobení a $a \neq 0$, pokud $a \cdot b = a \cdot c$, potom $b = c$.
- Neexistují dvě nenulová čísla a a b, že $a \cdot b = 0$.

$\mathbb{Z}_p$ je podtěleso $\mathbb{F}$

Na rozjezd vyřešíme tělesa s prvočíselnou velikostí. Uvažujme strukturu $\mathbb{Z}_k$ tvořenou čísly $0, \ldots, k-1$ a operacemi sčítaní a násobení definovanými jako zbytek po celočíselném sčítání a násobení.

Příklad. Například pro $\mathbb{Z}_4$ a prvky $a = 2$ a $b = 3$ dostaneme, že $a + b = 1$ a $a \cdot b = 2$, neboť přesně takové zbytky mají čísla 5 a 6 po dělení 4.

Úloha 6.1. Dokažte, že $\mathbb{Z}_p$ je těleso, právě když p je prvočíslo.

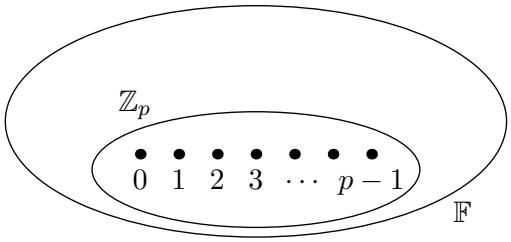
Nápověda. Pokud p není prvočíslo, není těžké nalézt dvojici, která porušuje poslední vlastnost. Pro prvočísla to se sčítáním bude docela jednoduché. Je však třeba pro každý prvek a ukázat, že násobení tímto prvkem je prosté, tedy že neexistuje dvě rozdílná čísla b a c, aby $a \cdot b = a \cdot c$.

Charakteristika tělesa je nejmenší přirozené číslo k takové, že součet k jedniček $1+1+\cdots+1 = 0$, případně 0, pokud takové k neexistuje (třeba reálná čísla).

Úloha 6.2. Dokažte, že pro každé konečné těleso $\mathbb{F}$ je jeho charakteristika nějaké prvočíslo p.

Nápověda. Ukažte nejprve, že charakteristika je nenulová. Poté zkuste dokazovat sporem. Kdyby charakteristika nebyla prvočíselná, co by bylo špatně?

Označme součet k jedniček pomocí k. V tělese tedy máme prvky $0, \ldots, p-1$. O dalších prvcích zatím nic nevíme.



Úloha 6.3. Ukažte, že prvky $0, \ldots, p-1$ tvoří podtěleso totožné $\mathbb{Z}_p$.

Cože? Těleso je vektorový prostor?

Nyní využijeme získané znalosti o tělesech a dokončíme důkaz překvapivým úskokem, však posuďte sami.

Úloha 6.4. Dokažte, že každé konečné těleso $\mathbb{F}$ charakteristiky p je vektorový prostor $\mathbb{V}$ nad tělesem $\mathbb{Z}_p$. Operace $\mathbb{V}$ definujeme takto: sčítání vektorů odpovídá sčítání v tělese a skalární násobení násobením v tělese (protože $\mathbb{Z}_p$ je podtěleso $\mathbb{F}$, lze to takto definovat).

Nápověda. K tomu potřebujeme dokázat, že vzniklá struktura splňuje všechny axiomy vektorového prostoru. Neplyne to snadno z toho, že $\mathbb{F}$ je těleso?

Víme, že vektorové prostory tvoří silně předurčenou strukturu, pojďme toho tedy využít. Vektorový prostor $\mathbb{V}$ má totiž konečnou dimenzi k. Podle Steinitzovy věty víme, že existuje nějaká báze $\mathbf{b}_1, \ldots, \mathbf{b}_k$. Sice vůbec netušíme, jak vypadá, ale to nebudeme potřebovat – stačí vědět, že existuje.

Bude se hodit ještě jedno obecné tvrzení o bázích a lineárních kombinacích.

Úloha 6.5. Dokažte, že pokud $\mathbf{b}_1, \ldots, \mathbf{b}_k$ je báze vektorového prostoru, potom její různé lineární kombinace definují různé vektory. Tedy dokažte, že $\sum_{i=1}^{k} \alpha_i \mathbf{b}_i = \sum_{i=1}^{k} \bar{\alpha}_i \mathbf{b}_i$ implikuje, že $\alpha_i = \bar{\alpha}_i$.

Dokončení důkazu

A na závěr složme oba poznatky dohromady.

Úloha 6.6. Dokažte, že každé konečné těleso $\mathbb{F}$ má p^k prvků.

Nápověda. Kolik rozdílných lineárních kombinací vektorů $\mathbf{b}_1, \ldots, \mathbf{b}_k$ existuje?

Tím jsme ukázali neexistenci konečného tělesa velikosti, která není mocnina prvočísla. Také vám přijde trik hezký? Pokud jste se dostali až sem (a případně všechna tvrzení po cestě dokázali), máte můj obdiv (a zasloužíte si své body :)).

7 Svědci a světci (10 bodů)

Představme si, že po nás někdo chce vyřešit soustavu $A\mathbf{x} = \mathbf{b}$. To není nijak těžké, že? Ale co s tím, když takové řešení neexistuje? Na cvičeních jsme ukázali, jak za pomocí metody nejmenších čtverců soustavu co nejméně pozměnit, aby řešení existovalo. To je vhodné jen pro některé aplikace a pro jiné by se více hodilo mít *svědka* (neboli *certifikát*), pomocí kterého snadno dokážeme, že řešení neexistuje. Certifikáty hrají důležitou roli v teorii složitosti.

Zkusíme si vyrobit jeden takový certifikát pro to, že $A\mathbf{x} = \mathbf{b}$ nemá řešení. Stačí k tomu nalézt vektor $\mathbf{y}$ správných vlastností.

Úloha 7.1. Soustava $A\mathbf{x} = \mathbf{b}$ nemá řešení, právě když existuje $\mathbf{y}$, že $A^\mathsf{T}\mathbf{y} = \mathbf{0}$ a $\mathbf{y}^\mathsf{T}\mathbf{b} = -1$.

Nápověda. Zamyslete se nad tím, co úloha říká v řeči fundamentálních prostorů A. Rozmyslete si také, že bude platit i tvrzení, kde bychom nahradili -1 libovolnou jinou nenulovou konstantou.

Poznámka. V praxi se používají ještě o něco silnější tvrzení, tzv. *Farkašova lemmata*. Jsou to oddělovací lemmata pro systémy například $A\mathbf{x} \leq \mathbf{b}$ nebo dokonce $\max_{\mathbf{x}}\{\mathbf{c}^\mathsf{T}\mathbf{x} : A\mathbf{x} = \mathbf{b}\}$.