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. Několik prvních členů x_0 až x_{k-1} je pevně určeno. Každý další člen je lineární kombinace k předcházejících členů, tedy platí

$$x_{n+k} = \alpha_{k-1}x_{n+k-1} + \alpha_{k-2}x_{n+k-2} + \cdots + \alpha_1 x_{n+1} + \alpha_0 x_n$$

pro pevná čísla α_0 až α_{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 pro obecnou lineární rekurenci. Tedy pro zadané k a koeficienty $\alpha_0, \ldots, \alpha_{k-1}$ popsat, jak se matice A zkonstruuje a pochopitelně dokázat, že má požadované vlastnosti. Tím také 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. Brzo 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:

$$P_\pi = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \qquad \text{a} \qquad P_\sigma = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

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.

Úloha 2.4. Ukažte, že pro libovolnou permutační matici P_π existuje mocnina k, že $P_\pi^k = I_n$.

3 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 jste si ukázali na cvičeních v zimním semestru.

- 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 3.1. 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 3.2. 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 3.3. 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 3.4. 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 3.5. Nechť $\mathbf{b}_1, \ldots, \mathbf{b}_k$ je báze vektorového prostoru, potom její různé lineární kombinace definují různé vektory. Tedy formálně:

$$\sum_{i=1}^{k} \alpha_i \mathbf{b}_i = \sum_{i=1}^{k} \bar{\alpha}_i \mathbf{b}_i \Longrightarrow \forall i : \alpha_i = \bar{\alpha}_i.$$

Dokažte.

Nápověda. Co by jinak bylo špatně? Opravdu by $\mathbf{b}_1, \ldots, \mathbf{b}_k$ byla báze, kdyby to neplatilo?

Dokončení důkazu

A na závěr složme oba poznatky dohromady.

Úloha 3.6. Dokažte, že každé konečné těleso $\mathbb{F}$ má p^k prvků.

Nápověda. Kolik rozdílných lineárních kombinací vektorů z $\mathbf{b}_1, \ldots, \mathbf{b}_k$ existuje? Proč z toho plyne, že těleso $\mathbb{F}$ má přesně p^k prvků?

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 :)).

4 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 4.1. 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 $\max_{\mathbf{x}}\{\mathbf{c}^\mathsf{T}\mathbf{x} : A\mathbf{x} = \mathbf{b}\}$.

5 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 5.1. Jak bude vypadat součin L_5U_5?

Úloha 5.2. Zobecněte získaný výsledek a popište součin L_nU_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_nU_n a udělat její LDU dekompozici. Co budou asi matice L a U? Za každý různý důkaz budou další body (různost posuzuje cvičící :)).