1 Matice pro výpočet lineárních rekurencí

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

Řešení
Představme si, že máme máme vektor

$$\mathbf{v} = (x_{n+k-1}, x_{n+k-2}, \ldots, x_{n+1}, x_n)^T$$

(první prvek je aktuální člen, zbytek máme „uložený“, abychom mohli spočítat další člen). Nyní bychom chtěli získat další člen posloupnosti a zároveň zachovat „tvar“ $\mathbf{b}$, tedy aby výsledek byl

$$\mathbf{u} = (x_{n+k}, x_{n+k-1}, \ldots, x_{n+2}, x_{n+1})^T \,.$$

Když se na rovnici $A\mathbf{v} = \mathbf{u}$ podíváme po řádcích, tak zjistíme, že pro každé $0 \leq i < k$ hledáme vektor $\mathbf{a}_{i*}$ (řádek matice A)[a] tak, aby $\mathbf{a}_{i*} \cdot \mathbf{v} = u_i = x_{n+k-i}$, což je pro $0 < i < k$ triviální, jelikož x_{n+k-i} už je ve vektoru $\mathbf{v}$:

$$(\mathbf{a}_{i*})_{i-1} = a_{i(i-1)} = 1, \qquad (\mathbf{a}_{i*})_j = a_{ij} = 1, \qquad 0 \leq j < k, j \neq i-1$$

$$\begin{aligned} \mathbf{a}_{i*} \cdot \mathbf{v} &= 0 \cdot x_{n+k-1} + \ldots + 0 \cdot x_{n+k-(i-2)} + 1 \cdot x_{n+k-(i-1)} + 0 \cdot x_{n+k-i} + \ldots + 0 \cdot x_n = \\ &= x_{n+k-(i-1)} = u_i \end{aligned}$$

Jediný řádek, který nám zbývá, je $\mathbf{a}_{0*}$. My si ale můžeme všimnout, že $x_{n+k} = \mathbf{c} \cdot \mathbf{v}$, jelikož x_{n+k} je lineární kombinací $\mathbf{v}$ právě s koeficienty $\mathbf{c}$. Tj. pro nultý řádek matice A platí $\mathbf{a}_{0*} \cdot \mathbf{v} x_{n+k} = \mathbf{c} \cdot \mathbf{v}$, což splníme volbou „zvolíme“ (pro konkrétní $x_{\ldots}$ může existovat i jiná možnost, obecně ale musí platit:) $\mathbf{a}_{0*} = \mathbf{v}$.

Z konstrukce víme, že naše matice A bude mít požadované vlastnosti, a bude tvaru:

$$A = \begin{pmatrix} c_{k-1} & c_{k-2} & \ldots & c_1 & c_0 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

[a] V této úloze čísluji od nuly, aby byl pohodlnější zápis některých indexů.

2 Permutační matice

Příklad (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.

Řešení
Na násobení matice A permutační maticí P_π zleva se podíváme řádkovým pohledem, tedy i-tý řádek výsledné matice je i-tý řádek P_π krát A, tedy lineární kombinace řádků A s koeficienty $(P_\pi)_{i*}$. To znamená, že i-tý řádek výsledné matice je $\pi(i)$-tý řádek A, protože $\pi(i)$-tý člen $(P_\pi)_{i*}$ je 1, kdežto ostatní jsou nuly. Proto je permutační.

Na násobení matice A permutační maticí P_π zprava se naopak podíváme sloupcovým pohledem, tedy $\pi(i)$-tý sloupec výsledné matice je A krát $\pi(i)$-tý sloupec P_π, tedy lineární kombinace sloupů A s koeficienty $(P_\pi)_{*\pi(i)}$. To znamená, že $\pi(i)$-tý sloupce výsledné matice je i-tý sloupec A, protože i-tý člen $(P_\pi)_{*\pi(i)}$ je 1, kdežto ostatní jsou nuly. Taktéž proto permutační.

Příklad (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.

Řešení
Z předchozího příkladu víme, že násobením permutační maticí permutujeme řádky / sloupce, tedy součin dvou permutačních maticí bude permutační matice, jelikož permutací řádků / sloupců nezměníme počet 1 a 0 v řádcích ani sloupcích.

Jelikož i-tý řádek součinu $P_\pi P_\sigma$ je z předchozího příkladu $\pi(i)$-tý řádek P_σ, bude v i-tém řádku výsledku jednička na $\sigma(\pi(i)) = (\sigma \circ \pi)(i)$-tém řádku, tedy $P_\pi P_\sigma =)_{\sigma\circ\pi}$.

Příklad (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}.

Řešení
Z předchozího příkladu víme, že $P_\pi P_{\pi^{-1}} = P_{id} = \mathcal{I}$, tedy P_π^{-1} odpovídá $P_{\pi^{-1}}$ tj. (druhá rovnost platí z toho, že ve vyjádření inverzní matice je pouze prohozen sloupec a řádek oproti definici původní matice)

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

$$P_\pi^{-1} = P_\pi^T$$

Příklad (2.4)
Ukažte, že pro libovolnou permutační matici P_π existuje mocnina $k \geq 1$, že $P_\pi^k = \mathcal{I}_n$. Jaká je nejmenší možná hodnota k?

Řešení
Z předchozího příkladu víme, že ke každé permutační matici existuje inverzní matice. Z příkladu 2.2 víme, že všechny mocniny P_π budou zase permutační mocniny na stejné množině. Tedy jich může být pouze omezeně mnoho ($n!$), což znamená, že určitě existují dvě mocniny $i < j : P_\pi^i = P_\pi^j$. Tuto rovnost však můžeme vynásobit i-tou mocninou P_π^{-1}, čímž dostaneme $\mathcal{I} = P_\pi^{j-i}$, kde jistě $k = j - i > 0$.

Nejmenší k bez důkazu nejmenší společný násobek délek cyklů permutace π (menší permutace nejsou identity, tedy ani jim odpovídající matice nebudou jednotkové, na druhou stranu nejmenší společný násobek stačí, jelikož v tu chvíli se všechny cykly zobrazí na identitu).

3 Matice Pascalova trojúhelníku

Příklad (3.1)
Jak bude vypadat součin $L_5 U_5$?

Řešení

$$\begin{array}{cc}
 & \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 3 & 6 \\ 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 \\ 1 & 3 & 3 & 1 & 0 \\ 1 & 4 & 6 & 4 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 6 & 10 & 15 \\ 1 & 4 & 10 & 20 & 35 \\ 1 & 5 & 15 & 35 & 70 \end{pmatrix}
\end{array}$$

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

Řešení
Z předchozí úlohy už to celkem vypadá, že[a] $a_{ij} = \binom{i+j}{i}$. Tedy chceme dokázat:

$$a_{ij} \overset{\text{DEF}}{=} \sum_{k=0}^{\min\{i,j\}} \binom{i}{k}\binom{j}{k} \overset{?}{=} \binom{i+j}{i} = \binom{i+j}{j}.$$

[a] V této sekci číslujeme zase od nuly.

Důkaz (Kombinatorickým nahlédnutím)
V sumě vybíráme k prvků z i a k prvků z j. Tj. vybíráme k prvků z i a $j - k$ prvků z j. Tedy vybíráme dohromady j prvků z $j + i$, jelikož rozložení, kolik prvků vybereme z j a kolik z i „volí“ suma. $\square$

4 Mocniny Jordanovy matice

TODO

5 Matice s vzorem šachovnice

Příklad (5.1)
Rozhodněte, zda jsou třídy $_l$ a $_s$ uzavřené na součet.

Řešení
Jsou, jelikož se sčítají prvky na stejných pozicích, tedy nuly se sečtou na nuly a ostatní prvky se sečtou na ostatní, tedy zůstanou.

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

Řešení
$\check{S}_s$ nejsou uzavřené na součin, protože $\check{S}_s$„ $\ni$ “ $\begin{pmatrix} 01 \\ 10 \end{pmatrix}^2 = \begin{pmatrix} 10 \\ 01 \end{pmatrix} \in \check{S}_l$. Naopak $\check{S}_l$ uzavřené na součin je, jelikož $\forall C, D \in \check{S}_l$:

$$(CD)_{ij} = \sum_k c_{ik} d_{kj}$$

a kdykoliv je součet $i + j$ lichý, tak j je liché a i sudé, nebo naopak. Každopádně $k + j$ nebo $k + i$ musí být liché, protože pokud je k sudé, tak se sečte na liché s lichým, a pokud je liché, tak se sudým. Tedy pokaždé bude v součinu jedna nula, tedy se všechno sečte na 0. Tedy na pozicích $(CD)_{ij}$ s lichým $i + j$ bude nula, tedy $CD \in \check{S}_l$.

Matici $A \cdot B$ zase vyjádříme jako

$$(AB)_{ij} = \sum_k a_{ik} b_{kj}$$

pokud bude součet $i + j$ sudý, tak jsou i a j buď oba sudé nebo oba liché, tedy pro liché k bude buď $i + k$ liché, tj. $a_{ik} = 0$, nebo $j + k$ sudé, tedy $b_{kj} = 0$, pro sudé k to bude opačně. Tedy pro sudé $i + j$ bude $(AB)_{ij} = 0$, tedy $A \cdot B \in \check{S}_s$.

Příklad (5.3)
Rozhodněte, zda jsou třídy $\check{S}_l$ a $\check{S}_s$ 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?

Řešení
TODO

6 Konečná tělesa existují jen pro mocniny prvočísla

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

Důkaz
($\implies$): Pokud je $\mathbb{Z}_p$, tak p nemůže být 1, protože těleso musí mít alespoň 2 prvky. A pokud je p složené, tedy $\exists x, y : x, y \in \mathbb{N} \setminus \{1\} \land x \cdot y = p$, pak z definice $\mathbb{Z}_p$ máme, že v $\mathbb{Z}_p$: $x \cdot y = 0$, tedy alespoň jedno z x a y je nulové, tedy v $\mathbb{Z}$ násobek p, což je ale spor s tím, že $x \cdot y = p \land x \neq 1 \land y \neq 1 \land x, y \in \mathbb{N}$.

($\Leftarrow$): Komutativita, asociativita a distributivita plynou jednoduše z toho, že je to v podstatě klasické sčítání a násobení. Stejně tak inverzní prvek vzhledem k sčítání a to, že 1 a 0 jsou neutrální prvky. Jediná zajímavá vlastnost na důkaz je existence inverzního prvku: Nechť je tedy $a \neq 0 \in \mathbb{Z}_p$ prvek, u kterého hledáme inverzi. Stačí ukázat, že pro $x \neq y$ je $ax \neq ay$, protože pak zobrazení $x \to ax$ je prosté, tedy jelikož je z konečné množiny do oné samé, tak je bijekcí, tedy existuje prvek a^{-1}, který se zobrazí na $a \cdot a^{-1} = 1$. Pokud by tedy bylo $ax = ay$, tak můžeme přičíst inverzní prvek k ay vzhledem ke sčítání, tedy $ax - ay = 0$. Z distributivity $a(x - y) = 0$, tedy buď $a = 0$, ale to jsme vyloučili, nebo $x - y = 0$, tedy $x = y$. Tedy jsme dokázali obměnu implikace $x \neq y \implies ax \neq ay$. $\square$

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

Důkaz
Charakteristika nemůže být nulová, jelikož může nabývat konečně mnoha hodnot, tedy někdy musí nastat

$$\underbrace{1+\ldots+1}_{i} = \underbrace{1+\ldots+1}_{j},\ i > j,$$

ale pak

$$\underbrace{1+\ldots+1}_{i}\underbrace{-1-1-\ldots-1}_{j} = \underbrace{1+\ldots+1}_{i-j} = \underbrace{1+\ldots+1}_{j}\underbrace{-1-1-\ldots-1}_{j} = 0,$$

tedy charakteristika $\mathbb{F}$ není nula, jelikož jsme právě nalezly nějaké k (sice ne nejmenší, ale to (na přirozených číslech) už musí existovat, když 1 máme).

Pokud by charakteristika složené číslo $(m \cdot n)$, pak:

$$0 = \underbrace{1+\ldots+1}_{m\cdot n} \overset{\text{asociativita}}{=} \underbrace{\underbrace{1+\ldots+1}_{m} + \ldots + \underbrace{1+\ldots+1}_{m}}_{n} \overset{\text{distributivita}}{=}$$

$$= \underbrace{(\underbrace{1+\ldots+1}_{m}) \cdot 1 + \ldots + (\underbrace{1+\ldots+1}_{m}) \cdot 1}_{n} \overset{\text{distributivita}}{=} (\underbrace{1+\ldots+1}_{m}) \cdot (\underbrace{1+\ldots+1}_{n})$$

Tedy z vlastností shrnutých v zadání je buď $(\overbrace{1+\ldots+1}^{m}) = 0$ nebo $(\overbrace{1+\ldots+1}^{n}) = 0$, tedy buď m nebo n je „menší charakteristika“ než $m \cdot n$, což je spor s definicí charakteristiky, tudíž charakteristika nemůže být složené číslo.

$1 \neq 0$, tedy nemůže být ani jedna. Tedy může být pouze prvočíslo. □

Příklad (6.3)
Ukažte, že prvky $0, \ldots, p-1$ (definované jako součet $0, \ldots, p-1$ jedniček) tvoří podtěleso totožně $\mathbb{Z}_p$. (p je charakteristika.)

Důkaz

Součet dvou prvků x, y je jednoduše $x+y = \overbrace{1+\ldots+1}^{x} + \overbrace{1+\ldots+1}^{y} = \overbrace{1+\ldots+1}^{x+y}$. Odtud můžeme odečíst dostatečněkrát $\overbrace{1+\ldots+1}^{p} = 0$, tedy získáme zase číslo od 0 do $p-1$, které je jistě zbytkem z $x+y$ po dělení p.

Součin dvou prvků x, y je stejně jako v předchozím důkazu $x \cdot y = (\overbrace{1+\ldots+1}^{x}) \cdot (\overbrace{1+\ldots+1}^{y}) = \overbrace{1+\ldots+1}^{x\cdot y}$. Odtud můžeme odečíst dostatečněkrát $\overbrace{1+\ldots+1}^{p} = 0$, tedy získáme zase číslo od 0 do $p-1$, které je jistě zbytkem z $x+y$ po dělení p. Tj. i násobení i sčítání odpovídá operacím v $\mathbb{Z}_p$. □

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

Důkaz
$\mathbf{V}$ splňuje všechny axiomy netýkající se tělesa nad kterým je, protože je zároveň tělesem. Obě distributivity a asociativita násobení skalárem jsou splněné z toho, že Z_p je podtěleso, tedy jeho prvky jsou i prvky $\mathbb{F}$, ve kterém distributivita platí z vlastností. $1 \cdot \mathbf{v} = \mathbf{v}$ splňuje z toho, že 1 je neutrálním prvkem (vzhledem k násobení) nejen v $\mathbb{Z}_p$, ale i v $\mathbb{F}$. □

Příklad (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 $\sum_{i=1}^k \alpha_i \mathbf{b}_i = \sum_{i=1}^k \overline{\alpha}_i \mathbf{b}_i$ implikuje, že $\alpha_i = \overline{\alpha}_i$.

Důkaz
Báze je lineárně nezávislá, tedy $\mathbf{o}$ lze vyjádřit právě jako lineární kombinaci s nulovými koeficienty. Tedy si $\sum_{i=1}^k \alpha_i \mathbf{b}_i = \sum_{i=1}^k \overline{\alpha}_i \mathbf{b}_i$ přepíšeme jako $\sum_{i=1}^k (\alpha_i - \overline{\alpha}_i)\mathbf{b}_i = \mathbf{o}$, a tudíž pro každé i je $\alpha - \overline{\alpha}_i = 0$, tj. $\alpha = \overline{\alpha}_i$. □

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

Důkaz
Nechť $\mathbf{V}$ je VP odpovídající $\mathbb{F}$. Potom je $\mathbf{V}$ jistě konečný, tedy má konečnou bázi o n prvcích. Každá lineární kombinace báze odpovídá jinému vektoru $\mathbf{V}$ (jak jsme ukázali v předchozím příkladu), tedy zobrazení lineární kombinace báze $\to$ prvek $\mathbf{V}$ je prosté. Naopak jelikož je to báze, tak generuje $\mathbf{V}$, tedy každý prvek $\mathbf{V}$ se dá vyjádřit jako lineární kombinace báze, tedy i zobrazení prvek $\mathbf{V} \to$ lineární kombinace báze je prosté. Tedy každý prvek se dá zobrazit bijekcí na lineární kombinaci báze.

Různé lineární báze se liší volbou koeficientů a všech n koeficientů volíme nezávisle z $|\mathbb{Z}_p| = p$ prvků, tedy máme p^n lineárních kombinací $\implies$ p^n prvků $\mathbf{V}$ resp. $\mathbb{F}$. □

7 Svědci a světci

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

Důkaz
($\implies$): Nechť tedy soustava $A\mathbf{x} = \mathbf{b}$ nemá řešení. Potom z Frobeniovy věty plyne $\operatorname{rank}(A) \neq \operatorname{rank}(A|\mathbf{b})$, navíc přidáním sloupce jsme jistě nemohly snižit rank, tedy $\operatorname{rank}(A|\mathbf{b}) > \operatorname{rank}(A)$. Tedy pokud z matice $(A|\mathbf{b})$ vybereme $\operatorname{rank}(A|\mathbf{b})$ nezávislých řádků, tak „ty samé“ řádky v matici A budou lineárně závislé.

Jelikož jsou lineárně závislé, tak můžeme vybrat nenulové (alespoň jeden je nenulový) koeficienty $\mathbf{y}'$ tak, aby lineární kombinace řádků A byla $\mathbf{o}$. Ale z LN řádků $(A|\mathbf{b})$ víme, že „stejná“ lineární kombinace řádků $(A|\mathbf{b})$ není nulová, tedy „stejná“ lineární kombinace prvků $\mathbf{b}$ musí být nenulová (všechny ostatní složky lineární kombinace řádků $(A|\mathbf{b})$ jsou z výběru $\mathbf{y}$ nulové).

Nyní se můžeme na součin $A^T\mathbf{c}$ podívat z pohledu, že výsledek je lineární kombinace sloupců A^T (tj. řádků A) s koeficienty $\mathbf{c}$. A součin $\mathbf{c}^T\mathbf{b}$ je lineární kombinace (s koeficienty $\mathbf{c}$) prvků $\mathbf{b}$. Tedy víme, že $A^T\mathbf{y}' = \mathbf{o}$ a $\mathbf{y}'^T\mathbf{b} = \alpha \neq 0$, což je skoro to, co chceme. Z axiomů tělesa víme, že (jelikož je $\alpha \neq 0$) existuje $-\alpha^{-1}$, tedy můžeme definovat $\mathbf{y} = -\alpha^{-1}\mathbf{y}'$. Následně z komutativity násobení skalárem $A^T\mathbf{y} = -\alpha^{-1}\mathbf{o} = \mathbf{o}$ a $\mathbf{y}^T\mathbf{b} = -\alpha^{-1}\alpha = -1$, tedy jsme právě z levé strany ekvivalence dokázali existenci $\mathbf{y}$ splňující podmínky pravé strany ekvivalence.

($\Leftarrow$) sporem: Nechť existuje řešení $A\mathbf{x} = \mathbf{b}$. Potom můžeme rozepsat z asociativity maticového násobení $-1 = \mathbf{y}^T\mathbf{b} = \mathbf{y}^T(A\mathbf{x}) = (\mathbf{y}^T A)\mathbf{x}$. My však víme, že $(AB)^T = B^T A^T$, tedy $-1 = (\mathbf{y}^T A)\mathbf{x} = (A^T\mathbf{y})^T\mathbf{x} = (\mathbf{o})^T\mathbf{x} = 0$ (součinem nulového vektoru s jakýmkoliv jiným jistě dostaneme 0). $\lightning$ $\square$