Polynomiální inverzy matic

Důležitou vlastností generující matice je existence jejího polynomiálního pravého inverzu. *Pravým inverzem* matice $\mathbf{G}$ tvaru $b \times c$ rozumíme matici $\mathbf{G}'$ tvaru $c \times b$ takovou, že $\mathbf{G}\mathbf{G}' = I_b$. Pravý inverz zřejmě může existovat pouze pro matice s plnou hodností (tedy hodností b, pokud $b \leq c$), což budeme v této kapitole předpokládat. Pro generující matice je tato podmínka splňena vždy, ale výsledky této kapitoly platí, stejně jako výsledky o Smithově rozkladu, pro libovolné racionální matice.

> Pozn.: V kontextu konvolučních kódů znamená pravý inverz dekódovací zařízení. Existence polynomiálního pravého inverzu tedy znamená polynomiální dekódovač.

Pravý inverz matice snadno dostaneme z jejího Smithova rozkladu. Je-li totiž

$$\mathbf{G} = \mathbf{A} \cdot (\mathbf{C} \,|\, \mathbf{0}) \cdot \mathbf{B},$$

pak stačí položit

$$\mathbf{G}' = \mathbf{B}^{-1} \cdot \left(\frac{\mathbf{C}^{-1}}{\mathbf{0}} \right) \cdot \mathbf{A}^{-1}.$$

Všimněme si, že $\mathbf{A}^{-1}$ i $\mathbf{B}^{-1}$ jsou polynomiální. Změnou pořadí sloupců $\mathbf{B}^{-1}$ a řádků $\mathbf{C}^{-1}$ tedy dostáváme Smithův rozklad matice $\mathbf{G}'$. Nechť

$$\mathbf{C} = \begin{pmatrix} \frac{\alpha_1}{\beta_1} & & & \\ & \frac{\alpha_2}{\beta_2} & & \\ & & \ddots & \\ & & & \frac{\alpha_b}{\beta_b} \end{pmatrix}.$$

Pak je zřejmě $\mathbf{G}'$ polynomiální, pokud $\alpha_b = 1$. Opačná implikace není zcela zřejmá, ale také platí, jak ukazuje následující lemma, které poskytuje ještě jednu ekvivalentní charakteristiku existence polynomiálního pravého inverzu.

Lemma 1. Nechť $\mathbf{G}$ je generující matice typu $b \times c$ s b-tým invariantním faktorem α_b/β_b ve zkráceném tvaru. Následující podmínky jsou ekvivalentní

(1) $\alpha_b = 1$
(2) $\mathbf{G}$ má polynomiální pravý inverz.
(3) Pro každé $\mathbf{u} \in \mathbb{F}(D)^b$ platí: $\mathbf{u}\mathbf{G} \in \mathbb{F}[D]^c \Rightarrow \mathbf{u} \in \mathbb{F}[D]^b$.

Důkaz. Nechť je

$$\mathbf{A} \cdot (\mathbf{C} \,|\, \mathbf{0}) \cdot \mathbf{B},$$

Smithův rozklad matice $\mathbf{G}$.
(1) $\Rightarrow$ (2): Je-li $\alpha_b = 1$, pak $\alpha_1 = \alpha_2 = \cdots = \alpha_b = 1$. Pak je $\mathbf{C}^{-1}$ polynomiální a $\mathbf{B}'\mathbf{C}^{-1}\mathbf{A}^{-1}$ je polynomiální pravý inverz $\mathbf{G}$, kde $\mathbf{B}'$ je prvních b sloupců $\mathbf{B}^{-1}$.
(2) $\Rightarrow$ (3): Nechť je $\mathbf{G}'$ polynomiální pravý inverz matice $\mathbf{G}$. Je-li $\mathbf{u}\mathbf{G}$ polynom, je také $\mathbf{u} = \mathbf{u}\mathbf{G}\mathbf{G}'$ polynom.
(3) $\Rightarrow$ (1): Dokážeme nepřímo. Nechť je $\alpha_b \neq 1$ a položme $\mathbf{u} = \frac{\beta_b}{\alpha_b}\mathbf{e}_b\mathbf{A}^{-1}$. Protože $\frac{\beta_b}{\alpha_b}\mathbf{e}_b = \mathbf{u}\mathbf{A}^{-1}\mathbf{A}$ není polynomiální, není polynomiální ani $\mathbf{u}$. Naproti tomu $\mathbf{u}\mathbf{G}$ polynomiální je, protože to je b-tý řádek matice $\mathbf{B}$, jak snadno spočítáme. □

Připomeňme, že pracujeme s Laurentovými řadami, tedy s řadami ve formální proměnné D, které mají nějaký nenulový začátek (konečné zpoždění), ale nemusí mít konečný stupeň. Pokud bychom chtěli, mohli bychom namísto D uvažovat formální proměnnou D^{-1}.

Pozn.: V literatuře se invertovaná proměnná někdy používá, často z^{-1}, což má svoji logiku v analogii s reálnými čísly.

Z pohledu formální řády, tedy pokud nechceme za proměnnou dosazovat, na volbě nezáleží. Je ale důležité mít na paměti následující vztahy. Těleso $\mathbb{F}((D^{-1}))$ není rovno tělesu $\mathbb{F}((D))$, přičemž jejich průnik jsou právě řady s konečným nosičem. Naproti tomu $\mathbb{F}(D)$ a $\mathbb{F}(D^{-1})$ splývají. Racionální matici proto můžeme vždy chápat obojím způsobem, aniž by to mělo na výklad nějaký vliv. Rozdíl se ovšem ukáže v případě Smithova rozkladu, protože ten se vztahuje k základnímu okruhu, kterým je buď $\mathbb{F}[D]$, nebo $\mathbb{F}[D^{-1}]$. Podobně je rozdíl mezi polynomiálním pravým inverzem (podle definice chápaným nad $\mathbb{F}[D]$), a *pravým inverzem polynomiálním v* D^{-1}, tedy pravým inverzem s koeficienty v $\mathbb{F}[D^{-1}]$, který budeme značit $\mathbf{G}'_{-1}$. Tento druh inverzu bude později hrát důležitou roli a platí pro něj alternativa předchozího lemmatu.

Lemma 2. Nechť $\mathbf{G}$ je racionální matice typu $b \times c$ a α_b/β_b je b-tý invariantní faktor matice $\mathbf{G}$ v okruhu $\mathbb{F}[D^{-1}]$ ve zkráceném tvaru. Následující podmínky jsou ekvivalentní

(1) $\alpha_b = 1$
(2) $\mathbf{G}$ má pravý inverz polynomiální v D^{-1}.
(3) Pro každé $\mathbf{u} \in \mathbb{F}(D)^b$ platí: $\mathbf{uG} \in \mathbb{F}[D^{-1}]^c \Rightarrow \mathbf{u} \in \mathbb{F}[D^{-1}]^b$.

Důkaz. Plyne z předchozího lemmatu po substituci D^{-1} za D, vzhledem k tomu, že $\mathbb{F}(D) = \mathbb{F}(D^{-1})$. □

**

Mezi existencí dvou polynomiálních pravých inverzů (v D a D^{-1}) je poměrně úzká souvislost. Uvažme nejprve, že pokud α_b je v libovolné polynom, který nemá tvar D^k, pak je $\mathbf{u} = \frac{\beta_b}{\alpha_b}\mathbf{e}_b$ Laurentova řada s nekonečným nosičem, zatímco nosič $\mathbf{uG}$ je konečný. Z toho je snadno vidět, že podmínka (3) je (pro vhodný D-posun $\mathbf{u}$) porušena v obou případech, a matice $\mathbf{G}$ tedy nemá ani jeden polynomiální pravý inverz.

Pozn.: Takové matici se říká *katastrofická*. Katastrofa spočívá v tom, že konečné kódové slovo je někdy třeba dekódovat na nekonečný vzor, což díky linearitě znamená, že konečný počet chyb při přenosu může vést k nekonečně velké chybě při dekódování.

Asymetrie mezi existencí polynomiálních pravých inverzů tedy může nastat, jen pokud je α_b v jednom případě 1 a v druhém D^k. To je vidět i z toho, že vyjádření $\frac{\mathbf{p}}{\mathbf{q}}$ v D odpovídá pro nějaké ℓ vyjádření $\frac{D^{-\ell}\mathbf{p}}{D^{-\ell}\mathbf{q}}$ v D^{-1}. Z definice invariantních faktorů pomocí determinantů tedy plyne, že se dvě uvažované podoby Smithovy matice mohou lišit pouze v mocninách D.

1. Příklad

$$\mathbf{G}_1 = \begin{pmatrix} 1+D & D & 1 \\ D & 1+D & 1 \end{pmatrix}$$

Matice $\mathbf{G}_1$ má polynomiální pravý inverz

$$\mathbf{G}_1' = \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 1+D & D \end{pmatrix}$$

a Smithův rozklad

$$\mathbf{G}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1+D & D & 1 \\ D & 1+D & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

přičemž

$$\begin{pmatrix} 1+D & D & 1 \\ D & 1+D & 1 \\ 1 & 0 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1+D & D & 1 \end{pmatrix}$$

V $\mathbb{F}[C]$, $C = D^{-1}$, platí

$$\mathbf{G}_1 = \begin{pmatrix} C^{-1} & 0 \\ 0 & C^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1+C & 1 & C \\ 1 & 1+C & C \end{pmatrix}$$

a Smithův rozklad je

$$\mathbf{G}_1 = \begin{pmatrix} 1+C & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} C^{-1} & 0 & 0 \\ 0 & C & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1+C & C \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

přičemž

$$\begin{pmatrix} 1 & 1+C & C \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1+C & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Platí $\mathcal{K}(\mathbf{u})\mathbf{G}_1 = \mathcal{K}(\mathcal{Z}(\mathbf{u})\mathbf{G}_1) = (1,1,0)$ pro

$$\mathbf{u} = \left(D^{-1}+1, 1\right)$$

2. Příklad

$$\mathbf{G}_2 = \begin{pmatrix} D^2+D & 1 & D^2 \\ D^2 & \frac{D+1}{D} & D^2+D+1 \end{pmatrix} = \begin{pmatrix} \frac{1+C}{C^2} & 1 & \frac{1}{C^2} \\ \frac{1}{C^2} & C+1 & \frac{C^2+C+1}{C^2} \end{pmatrix}$$

Smithovy rozklady:

$$\mathbf{G}_2 = \begin{pmatrix} D & D+1 \\ 1+D & D \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{D} & 0 & 0 \\ 0 & D & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & D \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 1+C+C^2 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{C^2} & 0 & 0 \\ 0 & C & 0 \end{pmatrix} \cdot \begin{pmatrix} C+1 & C^2 & 1 \\ 1 & C & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Platí:

$$(D^{-1}+1, 1) \cdot \mathbf{G}_2 = (1,0,1)$$

a

$$(C^{-1}+1+C, C^{-1}) \cdot \mathbf{G}_2 = (1, C, 0)\,.$$