ZÁKLADNÍ, REDUKOVANÉ A KANONICKÉ MATICE

Připomeňme, že pro polynomiální matici $\mathbf{G}$ máme definován *vnější stupeň*, $\operatorname{extdeg}\mathbf{G}$, jako součet stupňů jejích řádků. Definujeme také *vnitřní stupeň*, $\operatorname{intdeg}\mathbf{G}$, jako největší stupeň subdeterminantu řádu b.

Polynomiální matice $\mathbf{G}$ se nazývá *základní*, pokud splňuje ekvivalentní podmínky následující věty.

Věta. *Nechť je $\mathbf{G}$ polynomiální matice $b\times c$. Následující podmínky jsou ekvivalentní:*

(1) *$\mathbf{G}$ má nejmenší vnitřní stupeň ze všech polynomiálních matic s ní ekvivalentních.*
(2) *Smithova normální forma $\mathbf{G}$ je $(\mathbf{I}_c \mid \mathbf{0})$.*
(3) *Subdeterminanty matice $\mathbf{G}$ řádu b jsou nesoudělné.*
(4) *Matice $\mathbf{G}(\alpha)$ má hodnost b pro každé α z algebraického uzávěru $\mathbb{F}$.*
(5) *Matici $\mathbf{G}$ lze doplnit $c-b$ řádky na unimodulární.*
(6) *$\mathbf{G}$ má polynomiální pravý inverz.*
(7) *Je-li $\mathbf{uG}$ polynomiální, pak je polynomiální také $\mathbf{u}$.*

Důkaz. (2) $\Leftrightarrow$ (3) Obě podmínky jsou podle definice Smithovy normální formy ekvivalentní rovnosti $\gamma_b = 1$.

(3) $\Leftrightarrow$ (4) Subdeterminanty řádu b jsou nesoudělné, právě když nemají žádný společný kořen v algebraickém uzávěru $\mathbb{F}$. To je ekvivalentní tomu, že pro libovolné α je alespoň jeden takový subdeterminant nenulový, a matice $\mathbf{G}(\alpha)$ má tedy plnou hodnost.

(1) $\Rightarrow$ (2) Nechť $\mathbf{G} = \mathbf{A}(\mathbf{C}\,|\,\mathbf{0})\mathbf{B}$ je Smithův rozklad. Pak je polynomiální matice $\mathbf{B}_1$ sestávající z prvních b řádků matice $\mathbf{B}$ ekvivalentní matici $\mathbf{G}$ a ze vztahu $\mathbf{G} = \mathbf{ACB}_1$ plyne

$$\operatorname{intdeg}\mathbf{G} = \deg|\mathbf{C}| + \operatorname{intdeg}\mathbf{B}_1\,.$$

Z minimality $\operatorname{intdeg}\mathbf{G}$ plyne $\deg\gamma_1\cdots\gamma_b = 0$, a tedy $\gamma_b = 1$.

(2) $\Rightarrow$ (5) Je-li $\mathbf{C} = \mathbf{I}_b$, pak $\mathbf{G} = \mathbf{AB}_1$. Nechť je $\mathbf{B}_2$ matice tvořená posledními $c-b$ řádky $\mathbf{B}$. Pak je matice

$$\begin{pmatrix}\mathbf{A} & \mathbf{0}\\ \mathbf{0} & \mathbf{I}_c\end{pmatrix}\mathbf{B} = \begin{pmatrix}\mathbf{AB}_1\\ \mathbf{B}_2\end{pmatrix} = \begin{pmatrix}\mathbf{G}\\ \mathbf{B}_2\end{pmatrix}$$

unimodulární.

(5) $\Rightarrow$ (6) Nechť je $\mathbf{M} = \begin{pmatrix}\mathbf{G}\\ \mathbf{G}_1\end{pmatrix}$ unimodulární a nechť $\mathbf{G}'$ je prvních b sloupců matice $\mathbf{M}^{-1}$. Pak $\mathbf{GG}' = \mathbf{I}_b$.

(6) $\Rightarrow$ (1) Nechť je $\mathbf{G}'$ polynomiální pravý inverz matice $\mathbf{G}$. Každá matice ekvivalentní s $\mathbf{G}$ je tvaru $\mathbf{TG}$. Je-li $\mathbf{TG}$ polynomiální, pak je také $\mathbf{T} = \mathbf{TGG}'$ polynomiální a platí

$$\operatorname{intdeg}\mathbf{TG} = \deg|\mathbf{T}| + \operatorname{intdeg}\mathbf{G} \le \operatorname{intdeg}\mathbf{G}\,.$$

Ekvivalence (2) $\Leftrightarrow$ (6) $\Leftrightarrow$ (7) je předmětem charakterizace existence pravého polynomiálního inverzu.

$\square$

Pro polynomiální matici $\mathbf{G}$ se stupni řádků ν_i definujme *matici nejvyšších koeficientů* $\overline{\mathbf{G}}$ jako matici $b\times c$ nad $\mathbb{F}$, kde $(\overline{\mathbf{G}})_{ij}$ je koeficient u D^{ν_i} v polynomu $\mathbf{g}_i^{(j)}$.

Dále řekneme, že matice $\mathbf{G}$ má *očekávaný stupeň výstupu*, pokud pro každé $\mathbf{u} \neq \mathbf{0}$ platí

$$\deg \mathbf{uG} = \max_i(\deg \mathbf{u}^{(i)} + \nu_i)\,.$$

Polynomiální matice se nazývá *redukovaná*, pokud splňuje ekvivalentní podmínky následující věty.

Věta. *Nechť je $\mathbf{G}$ polynomiální matice $b \times c$. Následující podmínky jsou ekvivalentní:*

(1) $\mathbf{G}$ má nejmenší vnější stupeň ze všech matic $\mathbf{TG}$, kde $\mathbf{T}$ je unimodulární.

(2) Matice nejvyšších koeficientů $\overline{\mathbf{G}}$ má hodnost b.

(3) $\operatorname{intdeg} \mathbf{G} = \operatorname{extdeg} \mathbf{G}$.

(4) Matice $\mathbf{G}$ má očekávaný stupeň výstupu.

Důkaz. (1) $\Rightarrow$ (2) Předpokládejme, že $\overline{\mathbf{G}}$ nemá plnou hodnost. Nechť $z\overline{\mathbf{G}} = 0$, kde $0 \neq z = (z_1, z_2, \ldots, z_b) \in \mathbb{F}^b$ a nechť je $\ell \leq b$ nejvyšší index, pro který je $z_\ell \neq 0$. Bez újmy na obecnosti také jako obvykle předpokládáme $\nu_1 \leq \nu_2 \leq \cdots \leq \nu_b$. Nyní platí, že stupeň

$$\mathbf{g}'_\ell := \sum_{i=1}^{\ell} z_i D^{\nu_\ell - \nu_i} \mathbf{g}_i$$

je menší než ν_i. Je-li tedy $\mathbf{T}$ matice přičítající $z_i D^{\nu_\ell - \nu_i}$-násobky řádků $i < \ell$ k z_ℓ-násobku ℓ-tého řádku, má $\mathbf{TG}$ menší vnější stupeň než $\mathbf{G}$. Matice $\mathbf{T}$ je však unimodulární.

(2) $\Leftrightarrow$ (3) Z definice determinantu snadno odvodíme, že pro libovolnou podmatici $\mathbf{M}$ velikosti $b \times b$ matice $\mathbf{G}$ je $\deg |\mathbf{M}|$ nejvýše $\nu = \operatorname{extdeg} \mathbf{G} = \sum \nu_i$ a koeficient u D^ν je navíc roven $\left|\overline{M}\right|$, kde $\overline{M}$ je odpovídající podmatice $\overline{\mathbf{G}}$ (viz dodatek k této kapitole). Protože $\operatorname{intdeg} \mathbf{G}$ je definován jako $\max \deg |\mathbf{M}|$, platí pro libovolnou polynomiální matici $\mathbf{G}$ nerovnost $\operatorname{intdeg} \mathbf{G} \leq \operatorname{extdeg} \mathbf{G}$ a rovnost nastává, právě když existuje $\mathbf{M}$ taková, že $\left|\overline{M}\right| \neq 0$, tedy právě když má $\overline{\mathbf{G}}$ plnou hodnost.

(2) $\Leftrightarrow$ (4) Zvolme $\mathbf{u} \neq \mathbf{0}$ a položme $d = \max(\deg \mathbf{u}^{(i)} + \nu_i)$. Nechť je $\overline{v}$ vektor koeficientů u D^d ve vektoru $\mathbf{v} = \mathbf{uG}$. Zřejmě $\deg \mathbf{uG} \leq d$ a rovnost platí, právě když je $\overline{v}$ nenulové. Položme $u = (u_1, u_2, \ldots, u_b)$, kde u_i je koeficient $\mathbf{u}^{(i)}$ u $D^{d-\nu_i}$. Všimněme si, že $u \neq 0$ a ověřme, že $\overline{v} = u\overline{\mathbf{G}}$. Má-li tedy $\overline{\mathbf{G}}$ plnou hodnost, je $\overline{v} \neq 0$ a výstup $\mathbf{uG}$ má očekávaný stupeň. Pokud naopak $\overline{\mathbf{G}}$ plnou hodnost nemá, existuje $\mathbf{u}$, pro které je $\overline{v} = 0$, což dosvědčuje, že $\mathbf{G}$ nemá očekávaný stupeň výstupu.

(3) $\Rightarrow$ (1) Z rovnosti $\operatorname{intdeg} \mathbf{TG} = \deg |\mathbf{T}| + \operatorname{intdeg} \mathbf{G}$ vidíme, že všechny unimodulárně ekvivalentní matice mají stejný vnitřní stupeň. Z výše uvedené nerovnosti $\operatorname{intdeg} \mathbf{G} \leq \operatorname{extdeg} \mathbf{G}$ nyní plyne, že $\operatorname{extdeg} \mathbf{G}$ je v rámci unimodulárně ekvivalentních matic minimální, je-li roven $\operatorname{intdeg} \mathbf{G}$. $\square$

Matice, která je základní a redukovaná, se nazývá *kanonická*. Zásadní důležitost kanonických matic vyplývá z následující věty.

Věta (O stavovém prostoru kódu)**.** *Dimenze stavového prostoru $\Sigma_\mathcal{C}$ je rovna vnějšímu stupni libovolné kanonické matice.*

Důkaz. Nechť $\mathbf{G} = (\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_b)$ je kanonická matice $\mathcal{C}$. Ukážeme, že

$$\mathbf{b}_{i,j} = D^{-j}\mathbf{g}_i,\ i = 1, 2, \ldots, b,\ j = 1, 2, \ldots, \nu_i$$

je báze $\Sigma_\mathcal{C}$. Zvolme libovolný prvek kódu a napišme ho ve tvaru $\mathbf{uG}$. Rozložme $\mathcal{Z}(\mathbf{u}) = \mathbf{s} + \mathbf{t}$ tak, aby platilo

$$\deg \mathbf{s}^{(i)} < -\nu_i, \qquad \operatorname{del} \mathbf{t}^{(i)} \geq -\nu_i\,.$$

Jinak řečeno, $\mathcal{Z}(\mathbf{u})$ je rozděleno na složku $\mathbf{t}$, která v čase nula ještě ovlivňuje stav kódovače $\mathbf{G}$ v přímé formě, a na „již zapomenutou složku“ $\mathbf{s}$, pro kterou je $\mathcal{K}(\mathbf{sG}) = \mathbf{0}$. Máme tedy

$$\mathcal{K}(\mathbf{uG}) = \mathcal{K}((\mathbf{s} + \mathbf{t} + \mathcal{K}(\mathbf{u}))\mathbf{G}) = \mathcal{K}(\mathbf{sG}) + \mathcal{K}(\mathbf{tG}) + \mathcal{K}(\mathcal{K}(u)\mathbf{G}).$$

Protože $\mathcal{K}(\mathcal{K}(\mathbf{u})\mathbf{G})$ i $\mathcal{K}(\mathbf{sG})$ leží v $\mathcal{C}^*$, reprezentuje $\mathbf{uG}$ stejný stav jako $\mathbf{tG}$. Vektor $\mathbf{tG}$ je ovšem podle definice lineární kombinací vektorů $\mathbf{b}_{i,j}$ (nad $\mathbb{F}$), konkrétně

$$\mathbf{tG} = \sum_{i=1}^{b} \sum_{j=1}^{\nu_i} u_{-j}^{(i)} \mathbf{b}_{i,j} \,.$$

Ukázali jsme, že třídy $[\mathbf{b}_{i,j}]_{\mathcal{C}}$ generují $\Sigma_{\mathcal{C}}$.

Zbývá ukázat lineární nezávislost. Nechť pro nějaké nenulové $\mathbf{u} = \left(\mathbf{u}^{(1)}, \ldots, \mathbf{u}^{(b)}\right)$, kde

$$\mathbf{u}^{(i)} = \sum_{j=1}^{\nu_i} u_{-j}^{(i)} D^{-j} \,,$$

platí

$$\sum_{i=1}^{b} \sum_{j=1}^{\nu_i} u_{-j}^{(i)} \mathbf{b}_{i,j} \in \mathcal{C}^*.$$

Existuje tedy nějaké $\mathbf{w}$, pro které

$$\mathcal{K}(\mathbf{uG}) = \mathbf{wG} \,.$$

Protože $\mathbf{G}$ má polynomiální inverz $\mathbf{G}'$, platí $\mathbf{w} = \mathcal{K}(\mathbf{uG})\mathbf{G}'$, a $\mathbf{w}$ je tedy polynomiální. Platí tedy $\deg(\mathbf{u} - \mathbf{w}) \geq 0$, a protože má $\mathbf{G}$ očekávaný stupeň výstupu, je i $\deg(\mathbf{u} - \mathbf{w})\mathbf{G} \geq 0$. To je však ve sporu s $\mathcal{K}((\mathbf{u} - \mathbf{w})\mathbf{G}) = \mathcal{K}(\mathbf{uG}) - \mathcal{K}(\mathbf{wG}) = \mathbf{0}$. Třídy $[\mathbf{b}_{i,j}]_{\mathcal{C}}$ jsou tedy lineárně nezávislé, čímž je důkaz dokončen. $\square$

Existují i nepolynomiální matice, jejichž kódovač v přímé formě má stupeň roven stupni kódu. (Také ty se někdy v literatuře nazývají kanonické a zabývat se jimi nebudeme.) Následující věta ovšem ukazuje, že neexistují žádné jiné takové matice polynomiální.

Věta. *Pro polynomiální matici* $\mathbf{G}$ *generující kód* $\mathcal{C}$ *platí* $\operatorname{extdeg} \mathbf{G} = \deg \mathcal{C}$, *právě když je* $\mathbf{G}$ *kanonická (tj. základní a redukovaná).*

Důkaz. „$\Rightarrow$“ Nechť platí $\operatorname{extdeg} \mathbf{G} = \deg \mathcal{C}$ a nechť $\mathbf{G}_1$ je nějaká základní a redukovaná matice generující $\mathcal{C}$. Takovou matici získáme tak, že zvolíme nějakou základní matici ekvivalentní s $\mathbf{G}$, a k ní poté unimodulárně ekvivalentní redukovanou. Násobení unimodulární maticí přitom nemění vnitřní stupeň, takže výsledná matice zůstává základní. Nyní platí

$$\operatorname{extdeg} \mathbf{G}_1 = \operatorname{intdeg} \mathbf{G}_1 \overset{(a)}{\leq} \operatorname{intdeg} \mathbf{G} \overset{(b)}{\leq} \operatorname{extdeg} \mathbf{G}.$$

Protože je $\operatorname{extdeg} \mathbf{G} = \operatorname{extdeg} \mathbf{G}_1 = \deg \mathcal{C}$, platí v obou neostrých nerovnostech rovnost. Přitom rovnost (a) znamená, že $\mathbf{G}$ je základní, (b) že je redukovaná.

„$\Leftarrow$“ Tato implikace je předmětem věty o stavovém prostoru kódu. $\square$

**

Dodatek:

Lemma. Pro libovolnou podmatici $\mathbf{M}$ velikosti $b \times b$ matice $\mathbf{G}$ je stupeň $|\mathbf{M}|$ nejvýše $\nu = \sum \nu_i$ a koeficient u D^ν je navíc roven $\left|\overline{M}\right|$, kde $\overline{M}$ je odpovídající podmatice $\overline{\mathbf{G}}$.

Důkaz. Označme $\mathbb{M}$ všechny bijekce množiny $\{1, 2, \dots, b\}$ a množiny indexů sloupců, ze kterých sestává $\mathbf{M}$. Pak má definice determinantu $\mathbf{M}$ podobu

$$|\mathbf{M}| = \sum_{\sigma \in \mathbb{M}} \prod_{i=1}^{b} \mathbf{g}_{i,\sigma(i)},$$

a tedy

$$\deg |\mathbf{M}| = \max_{\sigma \in \mathbb{M}} \deg \left(\prod_{i=1}^{b} \mathbf{g}_{i,\sigma(i)}, \nu \right) = \max_{\sigma \in \mathbb{M}} \sum_{i=1}^{b} \deg \mathbf{g}_{i,\sigma(i)} \leq \sum_{i=1}^{b} \nu_i = \nu \, .$$

Pro polynom $\mathbf{p} \in \mathbb{F}[D]$ označme $\operatorname{coeff}(\mathbf{p}, n)$ jeho koeficient u členu D^n. Z maximality ν_i dostáváme

$$\operatorname{coeff}(|\mathbf{M}|, \nu) = \sum_{\sigma \in \mathbb{M}} \operatorname{coeff} \left(\prod_{i=1}^{b} \mathbf{g}_{i,\sigma(i)}, \nu \right) = \sum_{\sigma \in \mathbb{M}} \left(\prod_{i=1}^{b} \operatorname{coeff}(\mathbf{g}_{i,\sigma(i)}, \nu_i) \right) = \left|\overline{M}\right| \, .$$

$\square$