CAP. 3 - MATRIZES POLINOMIAIS

1. Introdução

Uma matriz P(s) (lxm) cujos elementos $p_{ij}(s)$ são polinômios com coeficientes reais na variável s é dita matriz polinomial em s. Uma matriz Q(s) (lxm) cujos elementos $q_{ij}(s) = a_{ij}(s)/b_{ij}(s)$ são funções racionais na variável s ($q_{ij}(s) = a_{ij}(s)/b_{ij}(s)$ onde $a_{ij}(s), b_{ij}(s)$ são polinômios em s com b_{ij} polinômio não nulo) é dita matriz racional em s. A teoria que desenvolveremos aqui é geral, podendo a variável formal s ser substituída por exemplo pela variável de Laplace "s" ou o operador "p" de diferenciação.

Lembremos que o conjunto $\mathbb{A}(s)$ dos polinômios sobre uma variável s com coeficientes reais possui uma estrutura de anel comutativo (define-se soma e multiplicação, mas a multiplicação não possui inverso, pois o inverso de um polinômio é uma função racional). Já o conjunto $\mathbb{K}(s)$ das funções racionais sobre s possui uma estrutura de corpo. Note agora que dois polinômios $q_1(s)$ e $q_2(s)$ são dependentes

Considere agora o conjunto $\mathbb{A}^n(s)$ constituído das n-uplas ordenadas $(p_1(s),.....,p_n(s))$ onde $p_i \in \mathbb{A}(s)$. Seja $\mathbb{K}^n(s)$ o conjunto das n-uplas de elementos de $\mathbb{K}(s)$. Vê-se que $\mathbb{K}^n(s)$ é um espaço vetorial de dimensão n sobre o corpo $\mathbb{K}(s)$. Ademais, podemos considerar que $\mathbb{A}^n(s)$ é um subconjunto (mas não um subespaço) de $\mathbb{K}^n(s)$ (Embora isto não será necessário, ressaltamos que $\mathbb{A}^n(s)$ possui uma estrutura de módulo sobre o anel $\mathbb{A}(s)$).

Assim, uma matriz (n,m) polinomial T(s) pode ser considerada como uma transformação linear de $\mathbb{K}^m(s)$ em $\mathbb{K}^n(s)$. O ***pôsto*** p de T(s) será o número de vetores linha (ou coluna) linearmente independentes. Note que p será determinado pela maior ordem de um determinante menor não nulo. Por exemplo, sejam as matrizes

$$P(s) = \begin{bmatrix} s+1 & s+3 \\ s^2+3s+3 & s^2+5s+4 \end{bmatrix}$$

$$Q(s) = \begin{bmatrix} s+1 & s+3 \\ s^2+3s+2 & s^2+5s+6 \end{bmatrix}$$

Note que $\det P(s) = -2(s+1)$ e portanto o pôsto de P(s) é igual a 2. Por outro lado $\det Q(s) = 0$ e portanto o pôsto de Q(s) é igual a 1, já que (s+1) é um menor não nulo. Seja T(s) polinomial com m linhas e n colunas. Seja $\rho = \min\{n, m\}$. Note que o pôsto p de T(s) é tal que $p \leq \rho$. Dizemos que uma matriz polinomial T(s) possui ***pôsto pleno*** quando $p = \rho$. Dizemos que uma matriz (n, m) polinomial T(s) possui ***pôsto pleno para todo s*** se para todo $z \in \mathbb{C}$ temos que o pôsto de T(z) sobre o corpo

complexo é o máximo valor possível (isto é, dado pelo $\min\{n,m\}$). Por exemplo, a matriz P(s) não possui *pôsto pleno para todo s* porque para $s=-1$ temos que o determinante de P(−1) é nulo. No entanto P(s) possui *pôsto pleno.* A matriz

$$R(s)=\begin{bmatrix} s+1 & 0 & s+2 \\ 1 & 1 & 1 \end{bmatrix}$$

possui pôsto pleno para todo s porque os dois determinantes menores (s+1) e −(s+2), extraídos respectivamente das duas primeiras colunas e das duas últimas colunas, não se anulam simultâneamente. Já a matriz

$$P_1(s)=\begin{bmatrix} s+1 & 0 & (s+1)(s+2) \\ 1 & 1 & 0 \end{bmatrix}$$

não possui *pôsto pleno para todo s* porque todos os determinantes menores de ordem 2 se anulam para $s=1$. No entanto $P_1(s)$ possui *pôsto pleno.* Em geral, se T(s) é uma matriz polinomial (n,m) com $\rho=\min\{n,m\}$, e $\{p_1(s), \ldots, p_r(s)\}$ é o conjunto de determinantes menores de ordem ρ, podemos dizer que:

(i) T(s) possui *pôsto pleno* se houver algum polinômio $p_i(s)$ não nulo.

(ii) T(s) possui *pôsto pleno para todo s* se os polinômios $\{p_1(s), \ldots, p_r(s)\}$ são primos entre si. (não se anulam simultaneamente para nenhum $s_0 \in \mathbb{C}$)

Uma matriz polinomial quadrada é dita ser ***unimodular*** se o seu determinante for um polinômio constante não nulo. Note que uma matriz quadrada possui pôsto pleno para todo s se e só se ela for unimodular (pois um polinômio não constante possui pelo menos um raiz). Um exemplo de matriz T(s) unimodular é dada por

$$T(s)=\begin{bmatrix} s+1 & 1 \\ s+2 & 1 \end{bmatrix}$$

já que $\det T(s) = -1$.

2. Matrizes Unimodulares e Operações Elementares

Nesta seção mostraremos que toda matriz unimodular pode ser obtida da matriz identidade (e vice-versa) a partir de operações elementares de linha e coluna. São consideradas operações elementares :

(i) Troca entre a linha(coluna) i e a linha(coluna) j.

(ii) Multiplicação da linha (coluna) i por um número real não nulo x.

(iii) Adição a uma linha(coluna) i de um múltiplo polinomial de uma linha(coluna) j.

Note que as operações elementares não acrescentam raízes ao polinômio det T(s). De fato, a operação (i) troca o sinal do deeterminante, a operação (ii) multiplica o determinante por uma constante x real não nula e a operação (iii) não altera o determinante. As operações de elementares de linhas(colunas) (i), (ii), (iii) são respectivamente denotadas por

(i) $\ell_i \leftrightarrow \ell_j$ $(\mathcal{C}_i \leftrightarrow \mathcal{C}_i)$

(ii) $\ell_i \leftarrow x.\ell_i$ $(\mathcal{C}_i \leftarrow x.\mathcal{C}_i)$

(iii) $\ell_i \leftarrow \ell_i + p(s).\ell_j$ $(\mathcal{C}_i \leftarrow \mathcal{C}_i + p(s).\mathcal{C}_j)$

É fácil verificar que cada operação elementar de linha(coluna) equivale à multiplicação à esquerda(direita) por matrizes unimodulares adequadas. Por exemplo, no caso em que as matrizes são (2,2) é fácil ver que operações de linha (i), (ii), (iii) são realizadas pela multiplicação à esquerda pelas seguintes matrizes :

(i) $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, troca entre a primeira e a segunda linhas.

(ii) $\begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix}$, multiplica a primeira linha por x.

(iii) $\begin{bmatrix} 1 & p(s) \\ 0 & 1 \end{bmatrix}$, soma à primeira linha p(s) vezes a segunda linha.

Proposição 3.1 : As seguintes afirmativas são equivalentes para uma matriz quadrada polinomial W(s)

(i) W(s) pode ser obtida da identidade por um número finito de operações elementares.

(ii) det W(s) é um polinômio constante não nulo (número real não nulo).

(iii) $W^{-1}(s)$ é uma matriz polinomial.

Prova :

(i)⇒(ii) Lembremos que cada operação elementar equivale a multiplicar a matriz por uma outra matriz

W_i cujo determinante é um número real. Como o determinante do produto é o produto dos determinantes, segue-se que (ii) é verdadeiro.

(ii)⇔(iii) Como

$$W^{-1}(s) = \text{adj}[W(s)]/\det W(s)$$

e adj[W(s)] é uma matriz polinomial, é claro que (ii)⇒(iii). Se W^{-1} é polinomial, segue-se que para todo $z \in \mathbb{C}$ temos que $W^{-1}(z)$ é bem definida e é a inversa de W(z). Logo det W(s) não pode se anular para nenhum $s \in \mathbb{C}$ e portanto (iii)⇒(ii).

(ii)⇒(i)

Consequência do fato da forma de Smith de W(s) ser igual a identidade (ver seção 7).

3. Máximo Divisor Comum à Direita (MDCD)

Os divisores comuns matriciais são úteis para caracterização de observabilidade e controlabilidade de descrições polinomiais. Tal conceito generaliza a noção de mdc de polinômios para matrizes polinomiais. Nesta seção fixaremos as idéis no que diz respeito aos MDCD (máximo divisor comum à direita). O leitor não terá dificuldade em obter os resultados duais relativos ao MDCE pela permutação da palavra ***direita*** por ***esquerda***, ***linha*** por ***coluna*** e a ordem de algumas multiplicações matriciais. Na prática podemos obter os resultados análogos para o MDCE de um par de matrizes A(s) e B(s) se aplicarmos os resultados sobre o MDCD para o par de matrizes A'(s) e B'(s).

Definição 3.2: Sejam N(s) e D(s) um par de matrizes polinomiais respectivamente (l, m) e (m, m). (mesmo número de colunas). Um ***máximo divisor comum à direita*** (MDCD) é uma matriz quadrada R(s) (m, m) tal que

(i) R(s) é um ***divisor comum à direita***, isto é :

$$N(s) = \bar{N}(s)\,R(s)$$

$$D(s) = \bar{D}(s)\,R(s)$$

onde $\bar{N}$ e $\bar{D}$ são matrizes polinomiais respectivamente (l, m) e (m, m).

(ii) Se $R_1(s)$ é um outro ***divisor comum à direita*** então $R_1(s)$ é um divisor de R(s), isto é, existe W(s) polinomial tal que

$$R(s) = W(s)R_1(s)$$

Observação 3.3: Dado um par N, D de matrizes polinomiais onde D é (m, m) e N é (l, m), defina a matriz T(s) (l+m, m) pondo :

$$T(s) = \begin{bmatrix} D(s) \\ N(s) \end{bmatrix}$$

Note que existe uma matriz unimodular U(s) (m+1, m+1) correspondente a uma sequência de operações elementares de linha (vide forma de Hermite na seção 7) tal que

$$U(s) = \begin{bmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{bmatrix}$$

$$\begin{bmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{bmatrix} \begin{bmatrix} D(s) \\ N(s) \end{bmatrix} = \begin{bmatrix} R(s) \\ 0 \end{bmatrix} \tag{3.1}$$

onde R(s) é (m, m). Mostraremos que, nestas condições, R é um MDCD. De fato, seja $V(s) = U^{-1}(s)$ a matriz polinomial dada por

$$V(s) = \begin{bmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{bmatrix}$$

então

$$\begin{bmatrix} D(s) \\ N(s) \end{bmatrix} = \begin{bmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{bmatrix} \begin{bmatrix} R(s) \\ 0 \end{bmatrix}$$

portanto

$$D = V_{11} R$$
$$N = V_{21} R$$

e logo R é um divisor comum à direita do par N, D. Da eq. (3.1) segue-se que

$$R = U_{11} D + U_{12} N$$

Assim, se R_1 é outro divisor comum à direita, isto é, se $N = N_1 R_1$ e $D = D_1 R_1$, segue-se que

$$R = U_{11} D_1 R_1 + U_{12} N_1 R_1 = (U_{11} D_1 + U_{12} N_1) R_1$$

logo $R = W R_1$ onde $W = (U_{11} D_1 + U_{12} N_1)$. Assim R_1 é um divisor de R e portanto R é um MDCD.

Note que R não é único (um MDCD não posssui unicidade). No entanto, se R_1 e R_2 são MDCD's, existem matrizes polinomiais W_1 e W_2 tais que

$$R_1 = W_1 R_2$$
$$R_2 = W_2 R_1$$

Em geral não podemos afirmar que W_1 é a inversa de W_2 ou que W_1 e W_2 são unimodulares. No entanto tal fato é verdadeiro no caso em que podemos exibir um MDCD não singular :

Proposição 3.4: Sejam R_1, R_2 MDCD's de um par N, D. Então, se R_1 é não singular, R_2 também o é

$$R_2 = WR_1$$

onde W é uma matriz unimodular. Em outras palavras os MDCD's diferem por fatores unimodulares à esquerda.

Prova : Sabemos que

$$R_1 = W_1 R_2$$
$$R_2 = W_2 R_1$$

portanto

$$R_1 = W_1 W_2 R_1 \tag{3.2}$$

Assim, multiplicando-se a equação (3.2) à esquerda pela matriz racional R_1^{-1} teremos que $W_1 W_2 = I$. Logo a inversa de W_1 é polinomial (a matriz W_2) e vice-versa. Portanto W_1 e W_2 são unimodulares.

Observação 3.5: Os casos mais importantes que estudaremos serão casos onde a matriz D do par N, D é não singular, isto é det D é um polinômio não nulo. Nesse caso, se R é um MDCD de N, D a equação $D = \bar{D}R$ implica em que (det D) = (det $\bar{D}$)(det R). Logo det R não pode ser nulo e o resultado da proposição acima poderá ser aplicado. □

Proposição 3.6: Se T(s) possui pôsto pleno, onde

$$T(s) = \begin{bmatrix} D(s) \\ N(s) \end{bmatrix}$$

então todos os MDCD's são não singulares e diferem por fatores unimodulares à esquerda.

Prova : Seja U(s) uma matriz unimodular tal que

$$U(s)\begin{bmatrix} D(s) \\ N(s) \end{bmatrix} = \begin{bmatrix} R(s) \\ 0 \end{bmatrix}$$

Da observação 3.3, teremos que R(s) é um MDCD. Como U(s) é não singular (pois U(s) é unimodular) segue-se da álgebra linear que o pôsto de U(s)T(s) é pleno. Logo R(s) é não singular e da proposição 3.4 teremos o resultado desejado. □

4. Matrizes Primas à Direita

Nesta seção estudaremos o conceito de matrizes primas à direita como uma generalização do conceito de polinômios primos entre si.

Definição 3.7: Dizemos que um par de matrizes polinomiais N(s), D(s) onde N é (l, m) e D é (m, m), é primo à direita quando todos os seus MDCD's são unimodulares.

Observação 3.8 : Pela proposição 3.4, se um MDCD é unimodular todos os outros o serão.

Teorema 3.9: As seguintes afirmativas são equivalentes :

(i) N, D são primas à direita.

(ii) A matriz

$$T = \begin{bmatrix} D \\ N \end{bmatrix}$$

possui *pôsto pleno para todo* $s \in \mathbb{C}$.

(iii) Existem P (m, l) , Q (l, l) polinomiais tais que a matriz

$$\begin{bmatrix} D & -P \\ N & Q \end{bmatrix}$$

é unimodular.

(iv) Existem matrizes polinomiais X (m, l) e Y (m, m) tais que

$$XN + YD = I_m$$

(v) Existem U (m+l, m+l) e W (m, m) polinomiais unimodulares tais que

$$U \begin{bmatrix} D \\ N \end{bmatrix} W = \begin{bmatrix} I_m \\ 0 \end{bmatrix}$$

Prova :

(v)⇒(ii) Basta notar que o pôsto de $\begin{bmatrix} D \\ N \end{bmatrix}$ para cada $s \in \mathbb{C}$ não é alterado pela multiplicação de matrizes unimodulares à esquerda e a direita, ja que $U(s_0)$ e $W(s_0)$ são não singulares para todo $s_0 \in \mathbb{C}$. Logo o pôsto de $\begin{bmatrix} D(s_0) \\ N(s_0) \end{bmatrix}$ é igual ao pôsto de $\begin{bmatrix} I_m \\ 0 \end{bmatrix}$ para todo $s_0 \in \mathbb{C}$.

(ii)⇒(v) Seja U(s) uma matriz unimodular tal que

$$U(s) \begin{bmatrix} D(s) \\ N(s) \end{bmatrix} = \begin{bmatrix} R(s) \\ 0 \end{bmatrix}$$

Como a multiplicação por U não altera o pôsto, segue-se que R(s) é não singular para todo s e portanto R(s) é unimodular.

(i)⇒(v) Seja U(s) unimodular como no caso anterior. Da observação 3.3 teremos que R(s) é um MDCD. Como supusemos N, D primos à direita, segue-se que R é unimodular. Assim podemos tomar $W = R^{-1}$.

(iii)⇒(iv) Seja

$$V(s) = \begin{bmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{bmatrix} = \begin{bmatrix} D & -P \\ N & Q \end{bmatrix}^{-1}$$

Como supusemos (iii) verdadeiro, segue-se que V(s) é polinomial. Assim

$$\begin{bmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{bmatrix} \begin{bmatrix} D & -P \\ N & Q \end{bmatrix} = \begin{bmatrix} I_m & 0 \\ 0 & I_l \end{bmatrix}$$

e portanto $V_{11}D+V_{12}N = I_m$.

(v)⇒(iii)

Se (v) é verdadeira, seja a matriz polinomial $V(s) = U^{-1}(s)$ dada por

$$U^{-1} = \begin{bmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{bmatrix}$$

onde V_{11} é um bloco (m, m), V_{12} é (m, l), V_{21} é (l, m) e V_{22} é (l, l). De (v) teremos

$$\begin{bmatrix} D(s) \\ N(s) \end{bmatrix} = U^{-1} \begin{bmatrix} W^{-1}(s) \\ 0 \end{bmatrix}$$

Logo

$$\begin{bmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{bmatrix} \begin{bmatrix} W^{-1} & 0 \\ 0 & I_l \end{bmatrix} = \begin{bmatrix} D & V_{12} \\ N & V_{22} \end{bmatrix}$$

Note que a matriz do lado esquerdo da equação acima é unimodular porque o produto de matrizes unimodulares é unimodular. Assim podemos tomar $P = -V_{12}$ e $Q = V_{22}$.

(iv)⇒(i)

Temos por hipótese que existem X, Y polinomiais tais que XN+YD = I. Seja R um MDCD. Portanto

$$N = \bar{N}R$$

$$D = \bar{D}R$$

Logo

$$X\bar{N}R+Y\bar{D}R = (X\bar{N}+Y\bar{D})R = I$$

E portanto a inversa existe e é R é polinomial. Logo R é unimodular. □

5. Matrizes Estáveis

Esta breve seção se destina somente à definição de matrizes estáveis e estavelmente primas. Tal definição servirá para a caracterização de estabilizabilidade e detetabilidade de descrições polinomiais.

Definição 3.10: Um polinômio p(s) é dito ser ***estável*** ou ***Hurwitz*** se as suas raízes estão no semiplano complexo de parte real estritamente negativa. Note que um polinômio constante não nulo é considerado estável.

Definição 3.11 : Uma matriz quadrada polinomial T(s) é dita ser estável se seu determinante det(T(s)) for um polinômio estável.

Definição 3.12 : Duas matrizes polinomiais D, N com D (m, m) e N (l, m) são ditas estavelmente primas à direita se todos os seus MDCD's são estáveis.

É claro que, se existir um MDCD estável, ele será não singular. Assim pela proposição 3.4 é fácil mostrar que todos os outros MDCD's também são estáveis. De fato, seja R um MDCD estável. Logo det(R) não pode ser um polinomio nulo e assim R é não singular. Logo, se R_1 é um outro MDCD, existe uma matriz unimodular W tal que $R = WR_1$. Logo teremos $\det R = \det W . \det R_1$. Como (det W) é uma constante não nula, segue-se que os polinômios det R e $\det R_1$ possuem as mesmas raízes.

6. Aplicações em Sistemas

Seja o sistema polinomial abaixo

$$T(\boldsymbol{p})\,\xi(t) = U(\boldsymbol{p})\,u(t)$$
$$y(t) = V(\boldsymbol{p})\,\xi(t) + W(\boldsymbol{p})\,u(t)$$

e suponha que $T(\boldsymbol{p})$ e $V(\boldsymbol{p})$ não são primas à direita, e seja $R(\boldsymbol{p})$ um MDCD de T, V (lembremos que

R não é unimodular). Assim :

$$T = \bar{T}R$$
$$V = \bar{V}R$$

Logo, de acordo com o Cap. 1, a função de transferência do sistema será dada por :

$$\begin{aligned} G(s) &= V(s)T^{-1}(s)U(s)+W(s) \\ &= \bar{V}(s)R(s)[\bar{T}(s)R(s)]^{-1}(s)U(s)+W(s) \\ &= \bar{V}(s)R(s)R^{-1}(s)T(s)^{-1}(s)U(s)+W(s) \\ &= \bar{V}(s)\bar{T}(s)U(s)+W(s) \end{aligned}$$

Note que os pólos do sistema são as raízes de $\det(T) = \det(\bar{T})\det(R)$. Portanto, as raízes do determinante de R(s) são pólos do sistema que não aparecerão, devido ao cancelamento, como pólos da função de transferência. Note que as raízes do det R são exatamente os valores de s tais que o pôsto da matriz

$$\begin{bmatrix} T(s) \\ V(s) \end{bmatrix}$$

não é pleno. Assim, as raízes de det R são denominadas de *zeros desacoplados da saída*, ou ainda *modos não observáveis*.

Um fenômeno análogo é verificado quando as matrizes $T(p)$ e $U(p)$ não são primas à esquerda, isto é, $T = W\bar{T}$ e $U = W\bar{U}$, onde W não é unimodular. Neste caso as raízes do det W concidem com os valores de s que baixam o posto de [T(s) U(s)]. Tais valores de s são denominadas *modos não controláveis* ou *zeros desacoplados da entrada. (faça como exercício)*

Voltar p/ 5 e definir estabilizabilidade e/ou detectabilidade

7. Forma de Hermite e forma de Smith

Iniciaremos esta seção enunciando um resultado auxiliar muito importante. Para isso suponha que $T(s)$ é uma matriz polinomial (m x n). Seja $\bar{T}(s)$ uma matriz obtida de T(s) por uma sequência de operações elementares de linha e/ou de coluna. Seja r um inteiro menor ou igual a $\min\{m,n\}$ e suponha que as listas de polinômios $\{p_1(s),\ldots,p_h(s)\}$ e $\{\bar{p}_1(s),\ldots,\bar{p}_h(s)\}$ sejam respectivamente os determinantes menores de ordem r de T(s) e $\bar{T}(s)$. Então :

Lema 3.13 : Seja q(s) o MDC da lista $\{p_1(s),\ldots,p_h(s)\}$ e $\bar{q}(s)$ o MDCD da lista $\{\bar{p}_1(s),\ldots,\bar{p}_h(s)\}$. Então $q(s) = \bar{q}(s)$. Em outras palavras, operações elementares de linha e coluna não alteram o MDC dos menores.

Prova : Exercício.

Para uma matriz T(s) polinomial (m x n) onde denotaremos cada elemento da linha i e da coluna j por $t_{ij}(s)$. Por simplicidade de notação, denotaremos algumas vezes o polinômio $t_{ij}(s)$ por t_{ij} apenas. Desta forma seja

$$T(s)=\begin{bmatrix} t_{11} & t_{12} & \cdots & t_{1n} \\ t_{21} & t_{22} & \cdots & t_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ t_{m1} & t_{m2} & \cdots & t_{mn} \end{bmatrix}$$

Por operações elementares de linha podemos fazer com que o elemento da posição que t_{11} ocupa seja o mdc de todos os elementos da primeira coluna de T(s). De fato, sabemos que se $r(s)$, $r_0(s)$ são polinômios com grau $[r(s)] \geq$ grau $[r_0(s)]$, então a sequência de divisões

$$\begin{aligned} r &= r_0 d_0 + r_1 \\ r_0 &= r_1 d_1 + r_2 \\ r_1 &= r_2 d_2 + r_3 \\ r_2 &= r_3 d_3 + r_4 \\ &\cdots\cdots\cdots \end{aligned}$$

é tal que, se $r_{i+1}(s) = 0$, então $r_i(s)$ é o mdc de $r(s)$ e $r_0(s)$, sendo que isto ocorre sempre para um número finito de divisões (porque os graus dos r_i vão baixando). Assim, a menos de uma troca de linhas, podemos considerar que t_{11} é o polinômio de menor grau da primeira coluna de T(s). Desta forma podemos dividir t_{21} por t_{11} , obtendo :

$$t_{21}(s) = t_{11}(s)\, d(s) + r(s)$$

assim se adicionarmos à segunda linha de T(s) a primeira linha multiplicada por $d(s)$ vamos obter uma matriz da forma :

$$\begin{bmatrix} t_{11} & t_{12} & \cdots & t_{1n} \\ r & t'_{22} & \cdots & t'_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ t_{m1} & t_{m2} & \cdots & t_{mn} \end{bmatrix}.$$

assim podemos trocar a primeira com a segunda linha e continuar este processo de maneira que num

número finito de operações elementares o primeiro elemento da primeira coluna seja o mdc da primeira coluna. Assim é imediato que por operações elementares de linha podemos obter uma matriz da forma

$$\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ 0 & r_{22} & \cdots & r_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & r_{m2} & \cdots & r_{mn} \end{bmatrix}.$$

Agora podemos trabalhar apenas com as (m-1) últimas linhas da matriz obtendo uma matriz da forma :

$$\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ 0 & r_{22} & \cdots & r_{2n} \\ 0 & 0 & \cdots & r_{3n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & r_{mn} \end{bmatrix}.$$

Note que, se o grau de r_{12} for maior ou igual ao grau de r_{22}, através de uma operação elementar de linha podemos baixar o grau de r_{12} de maneira que r_{22} passe a ser o polinômio de maior grau da segunda coluna (basta aplicar o algoritmo de divisão para r_{12} e r_{22}). Tais operações podem ser realizadas para todas as colunas até obter uma matriz polinomial tal que os polinômios da diagonal principal sejam os de maior grau em sua coluna e abaixo deles todos os polinômios sejam nulos.

Como operações elementares de linha equivalem a multiplicar à esquerda por uma matriz unimodular $U(s)$, podemos escrever :

Definição 3.14 (forma de Hermite triangular superior) : Seja $T(s)$ uma matriz polinomial (m x n). Seja $p = \min\{m, n\}$. Então existe uma matriz unimodular $U(s)$ tal que a matriz $R(s) = U(s)T(s)$, denominada forma de Hermite de $T(s)$, obedece as seguintes condições

(i) $r_{ii}(s)$ é o polinômio de maior grau da i-ésima coluna i=1,....,p.

(ii) $r_{ji}(s) = 0$ para $j > i$ e i=1,.....,p. Em outras palavras, os polinômios abaixo da diagonal principal são nulos.

Observação 3.15 : Se m > n , isto é, se o número de linhas é maior que o número de colunas então a forma de Hermite de T(s) é da forma :

$$R(s) = \begin{bmatrix} R_{11} \\ 0 \end{bmatrix}$$

onde R_{11} é uma matriz polinomial quadrada m x m triangular superior.

Observação 3.16 : O leitor não terá dificuldade em obter uma forma de Hermite trabalhando com as colunas da matriz T(s).(Forma de Hermite triangular inferior).

Teorema 3.17 : (Forma de Smith) Dada uma matriz P(s) (1 x m) polinomial com pôsto r , existem matrizes U(s) e V(s) respectivamente (1 x 1) e (m x m) tais que

$$U(s)\,P(s)\,V(s) = \Lambda(s)$$

onde $\Lambda(s)$ é (1 x m), possuindo a forma :

$$\Lambda(s) = \begin{bmatrix} \Gamma(s) & 0^{r \times (m-r)} \\ 0^{(l-r)\times r} & 0^{(l-r)\times(m-r)} \end{bmatrix}$$

onde

$$\Gamma(s) = \begin{bmatrix} \lambda_1 & 0 & \ldots\ldots & 0 \\ 0 & \lambda_2 & \ldots\ldots & 0 \\ \ldots\ldots & \ldots\ldots\ldots & & \\ 0 & 0 & \ldots\ldots & \lambda_r \end{bmatrix}$$

sendo $\Gamma(s)$ matriz diagonal quadrada de ordem igual ao pôsto de P(s) e os polinômios $\lambda_i(s)$ são mônicos únicos tais que λ_i divide λ_{i+1} . Mais ainda, λ_1 é o mdc de todos os elementos de P(s), o produto $\lambda_1\lambda_2$ é o mdc de todos os determinantes menores de ordem dois, ou seja, $\lambda_1\lambda_2 \ldots \lambda_p$ é o mdc de todos os determinantes menores de ordem p de P(s).

Demonstração : Faça operações elementares de linha e coluna até que o mdc de todos os elementos de P(s) apareça na posição p_{11}. Daí é imediato que com mais algumas operações elementares de linhas e de colunas vamos obter uma matriz da forma

$$\begin{bmatrix} \lambda_1 & 0 \\ 0 & T_1(s) \end{bmatrix}$$

Repita as operações acima para $T_1(s)$ e assim por diante, obtendo uma matriz na forma dada no enunciado do teorema.

Como operações elementares não alteram o pôsto de uma matriz polinomial, segue-se que $\Gamma(s)$ terá ordem r.

Para mostrar que $\lambda_1\lambda_2....\lambda_p$ é o mdc de todos os menores de ordem p basta notar que operações elementares não alteram o mdc dos menores de uma ordem p fixada (vide lema 3.13). Assim tal fato é deduzido imediatamente pelo formato de $\Lambda(s)$.

Para mostrar que λ_i divide λ_{i+1} , basta notar que da maneira que descrevemos a sequência de operações para obter $\Lambda(s)$, temos que λ_1 divide todos os elementos de $T_1(s)$ e portanto divide o mdc de todos os elementos de $T_1(s)$, dado exatamente por λ_2. Como o algoritmo descrito prossegue de forma análoga, conclui-se a propriedade desejada e isso termina a demonstração. □

Observação : Note que um processo de obter as matrizes U e V que transformam P em $\Lambda = UPV$ é fazer as operações elementares com a matriz :

$$\begin{bmatrix} I_l & P \\ 0 & I_m \end{bmatrix}$$

e obter ao final :

$$\begin{bmatrix} U & \Lambda \\ 0 & V \end{bmatrix}$$