DEPARTAMENTO DE MATEMÁTICA APLICADA

Relatório Técnico

RT-MAP-0002

ÁLGEBRA DIFERENCIAL EM TEORIA DE CONTROLE

Carlos Juiti Watanabe
Paulo Sérgio Pereira da Silva
Pedro Aladar Tonelli

Abril 2000

UNIVERSIDADE DE SÃO PAULO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
SÃO PAULO — BRASIL

ÁLGEBRA DIFERENCIAL EM TEORIA DE CONTROLE

CARLOS JUITI WATANABE
PAULO SÉRGIO PEREIRA DA SILVA
PEDRO ALADAR TONELLI

RESUMO. Em sistemas de controle, estamos interessados em estudar equações diferenciais da forma $\dot{x} = f(x, u)$, onde $x \in \mathbb{R}^n$ e $u \in \mathbb{R}^m$; o parâmetro u é chamado controle ou entrada e x é chamado variável de estado. Quando $f(x, u)$ é um polinômio em x e u, podemos estudar esse tipo de sistema de um ponto de vista algébrico diferencial. Neste trabalho apresentamos uma equivalência entre duas definições de sistemas relativamente *flat*, utilizando a teoria de álgebra diferencial como em [Fli89]

1. INTRODUÇÃO

Diremos que um anel $(k, +, \cdot)$ é diferencial se existir uma operação (que chamaremos de derivação) $'$ que satisfaz as seguintes condições:

- $(a + b)' = a' + b'$;
- $(a \cdot b)' = a \cdot b' + b \cdot a'$.

Se o anel tiver estrutura de corpo, então diremos que k é um corpo diferencial.

Um corpo E/k é uma extensão diferencial se $E \supset k$ e as derivações em E são derivações em k. Seja E uma extensão diferencial de k e $X \subset E$ um subconjunto qualquer. Denotaremos $k\{X\}$ o anel diferencial gerado por X e suas derivadas, e $k\langle X\rangle$ o corpo de frações diferencial gerado por k, X e as derivadas de X [Kap78].

Se X e U são conjuntos de variáveis diferenciais livres e $J \subset k\{X, U\}$ é um ideal primo, podemos considerar $F := Q(k\{X, U\}/J)$ o corpo de frações do quociente do anel $k\{X, U\}$ pelo ideal primo J. Esta é uma extensão de k.

Além disso, F é extensão diferencial de k que contém as raízes dos polinômios diferenciais contidos em J, em particular, dos geradores de J. Dessa forma, podemos fazer aplicações da teoria algébrica diferencial para estudar sistemas de equações diferenciais.

Em teoria de controle, a equação de estados é, normalmente, da forma

$$\begin{cases} \dot{x}_i = f_i(x,u) & i = 1,\dots,n \\ y_j = \phi_j(x,u) & j = 1,\dots,r \end{cases}. \tag{$*$}$$

Para ilustrar como a álgebra diferencial pode nos auxiliar no estudo de alguns desses sistemas, vamos considerar o conjunto de relações polinomiais

$$\begin{cases} \dot{x}_i - f_i(x,u) & i = 1,\dots,n \\ y_j - \phi_j(x,u) & j = 1,\dots,r \end{cases}$$

que gera um ideal primo[1] e fazemos a construção citada anteriormente.

Assim estudaremos algumas estruturas num anel/corpo que contém as raízes do sistema $(*)$. A aplicação que estudaremos será um estudo de equações da forma $\dot{x} = P(x,u)$, onde P é uma relação polinomial entre x, u e, eventualmente, as derivadas de u.

2. Resultado Principal

A seguir daremos uma série de definições introduzidos por Fliess em [Fli89] que generalizam o exemplo 1.

Diremos que uma extensão diferencial E/k é *finitamente gerada* se existir uma família finita $F \subset E$ tal que $E = k\langle F\rangle$.

Definição. Um *sistema de controle* é uma extensão diferencial, com a derivação $'$ definida em k, E/k finitamente gerada.

Por simplicidade, diremos apenas sistema ao nos referirmos a sistema de controle.

Definição. *Entrada* (u) de um sistema é uma base de transcendência diferencial de E/k.

Definição. Um *estado* x *relativo a uma entrada* (u), é uma base de transcendência algébrica de $E/k\langle u\rangle$.

[1] a demonstração desse fato foge um pouco ao escopo desta seção, assim, isso será feita no apêndice.

Exemplo 1. Considere o sistema: $\dot{x} = x + u$ então uma entrada é u e um estado é x.

Quando não houver perigo de ambigüidade, diremos apenas estado.

Seja E/k um sistema de controle, então dado qualquer elemento $a \in E$, a obedece a uma relação polinomial da seguinte forma:

$$p_a(a, x, u, \dots, u^{(\alpha)}) = 0.$$

Se $x = \{x_1, \dots, x_n\} \subset E$ então cada um dos elementos x_i de x obedece alguma relação polinomial da forma

$$p_i(\dot{x}_i, x, u, \dots, u^{(\alpha_i)}) = 0.$$

Por simplicidade, onde se lê polinômio diferencial $q(x, u)$ entenda-se polinômio diferencial q que depende das variáveis x, u, $\dot{x}$, $\dot{u}$, ...

Teorema 1. *Se E/k é um sistema de controle e k tem característica zero então a dimensão do estado é finita, isto é, o número de elementos da base de transcendência algébrica é finito para qualquer entrada (u).*

Demonstração. Sejam $\{u_1, \dots, u_m\}$ uma entrada do sistema e x uma variável de estado. Se não existisse um polinômio diferencial tal que $p(x, u_1, \dots, u_m) = 0$, então qualquer derivada de x não satisfaria uma equação polinomial não nula, ou seja, $\{x\} \cup \{u_1, \dots, u_m\}$ seria um conjunto diferencialmente algebricamente independente, o que contraria a hipótese de $\{u_1, \dots, u_m\}$ ser uma entrada do sistema E/k. $\square$

Definição. Um sistema E/k é chamado de sistema *flat* se existir uma família $y = \{y_1, \dots, y_n\}$ contida em uma extensão *algébrica* D/E tal que y é uma base de transcendência diferencial de D/k e $D/k\langle y\rangle$ é *algébrico.*

Observe que um sistema *flat* é um sistema no qual não aparecem as variáveis de estado.

Definição. Dado um sistema E/k, um *subsistema* de E/k é uma extensão S, de k que está contido em E e tal que S/k seja um sistema.

Definição (*Flatness relativo*). Dado um subsistema S/k do sistema E/k, dizemos que E é *relativamente flat* com relação a S se E/S for *flat.*

Definição. Dizemos que um subconjunto Y de uma extensão E de k é diferencialmente algebricamente livre ou independente sobre k, se não existir um polinômio diferencial p não nulo com coeficientes em k, tal que $p(Y) = 0$.

Definição (Extensões Algebricamente Disjuntas). Dizemos que dois subsistemas E_1/k e E_2/k de um sistema E/k são *diferencialmente algebricamente disjuntos ou diferencialmente algebricamente independentes* se para L_1 e L_2 diferencialmente algebricamente livres sobre k, então

1. $L_1 \cap L_2 = \varnothing$;
2. $L_1 \cup L_2$ é diferencialmente algebricamente livre sobre k.

Definição (Decomposição). Dizemos que E/k é *decomposto* pelos subsistemas E_1 e E_2 se os sistemas são diferencialmente independentes sobre k e E é algébrico sobre $k\langle E_1, E_2\rangle$.

Definição. Uma *saída* de um sistema E/k é qualquer conjunto de elementos de E.

Definição. Uma saída y ($y \subset E$) de um sistema E/k é chamada *saída flat* se y for uma base de transcendência diferencial de alguma extensão algébrica D/E.

Lema 2. *Sejam E/k uma extensão diferencial de corpos e M, N duas partes de E. São equivalentes:*

1. *$M \cup N$ é diferencialmente algebricamente livre sobre k e $M \cap N = \varnothing$;*
2. *M é diferencialmente algebricamente livre sobre k e N é algebricamente livre sobre $k\langle M\rangle$;*
3. *N é diferencialmente algebricamente livre sobre k e M é algebricamente livre sobre $k\langle N\rangle$.*

Demonstração. É suficiente demonstrar a equivalência de 1 e 2.

(1. $\Rightarrow$ 2.): M é uma parte própria de $M \cup N$ (que é diferencialmente algebricamente livre sobre k). Se N não fosse diferencialmente algebricamente livre sobre $k\langle M\rangle$, existiria um polinômio diferencial p não nulo, com coeficientes em $k\langle M\rangle$ tal que $p(y) = 0$ para $y = \{y_1, \dots, y_n\} \subset N$. Tirando o m.m.c. dos denominadores dos coeficientes de p, obtemos um polinômio diferencial não nulo $q(x, y)$ com

coeficientes em k em que $x = \{x_1, \ldots, x_m\} \subset M$, $y \subset N$. Portanto M e N não seriam algebricamente livres.

(2. $\Rightarrow$ 1.): Temos claramente que $N \cap k\langle M\rangle = \varnothing$ e conseqüentemente $N \cap M = \varnothing$. Resta mostrar que quaisquer subconjuntos finitos $y \subset N$ e $x \subset M$ que são diferencialmente algebricamente livres sobre k, tem sua união diferencialmente algebricamente livre. Supondo, por absurdo, que $M \cup N$ não seja um conjunto diferencialmente algebricamente livre, então existiriam $x = \{x_1, \ldots, x_m\} \subset M$ e $y = \{y_1, \ldots, y_n\} \subset N$ e um polinômio diferencial P, não nulo, em $k\{x_1, \ldots, x_m, y_1, \ldots, y_n\}$ tal que $P(x_1, \ldots, x_m, y_1, \ldots, y_n) = 0$. Seja $g(y_1, \ldots, y_n) := p(x_1, \ldots, x_m, y_1, \ldots, y_n)$ um polinômio diferencial em $k\langle M\rangle\{y\}$ e a relação $p(x_1, \ldots, x_m, y_1, \ldots, y_n) = 0$ se escreve $g(y_1, \ldots, y_n) = 0$. Como N é diferencialmente algebricamente livre sobre $k\langle M\rangle$, os coeficientes de $g(y_1, \ldots, y_n)$ são nulos. Mas os coeficientes de g são da forma $q(x_1, \ldots, x_m)$, ou seja, são polinômios diferenciais em $k\langle M\rangle$, o que mostra que M não seria diferencialmente algebricamente livre sobre k.

□

Teorema 3. *Sejam E/k um sistema e L/k um subsistema de E/k. Então são equivalentes:*

1. *O sistema E/k é relativamente* flat *com respeito ao subsistema L/k;*
2. *Existe uma extensão algébrica D de E e um subsistema* flat *F/k de D/k tal que D se decompõe em relação a F e a L.*

Demonstração. (1. $\Rightarrow$ 2.) Se E/L é *flat* , tomamos $y = \{y_1, \ldots, y_m\}$ uma saída *flat* em uma extensão algébrica D de E. Fazemos $F = k\langle y\rangle$. Então L/k e F/k são diferencialmente independentes sobre k e D é algébrico sobre $k(F, L) = L(F)$. Para mostrar que y é algebricamente livre sobre k, suponhamos que exista p polinômio diferencial tal que $p(y) = 0$, p com coeficientes em k. Como $k \subset L$, podemos imaginar que p é um polinômio com coeficientes em L, como $p(y) = 0$, e y é uma base de transcendência diferencial de E/L, temos que $p \equiv 0$.

(2. $\Rightarrow$ 1.) Seja y uma base de transcendência diferencial de E/k onde E é uma extensão algébrica finita de F. Podemos supor que

D contém E, pois caso contrário, fazemos a extensão $D(E)$ que continua sendo uma extensão algébrica finita sobre E. Como D se decompõe em relação aos sistemas F e L, isto é, D é algébrico sobre $k\langle F, L\rangle = L\langle F\rangle$. Dessa forma, precisamos mostrar que y é uma base de transcendência diferencial de D/L e que D é algébrico sobre $L\langle y\rangle$. Como D é algébrico sobre $L\langle F\rangle = k\langle F, L\rangle = L\langle y\rangle$, temos que D é algébrico sobre $L\langle F\rangle = L\langle y\rangle$. Pelo lema anterior, temos que y é uma base de transcendência diferencial de D/L. □

3. Apêndice

Neste apêndice, mostraremos que o ideal diferencial gerado pelas relações $\begin{cases} \dot{X}_i - f_i(X,U) & i = 1, \ldots, n \\ Y_j - \varphi_j(X,U) & j = 1, \ldots, r \end{cases}$ é um ideal primo no anel diferencial $k\{X_1, \ldots, X_n, Y_1, \ldots, Y_r, U_1, \ldots, U_s\}$. Um resultado mais geral é obtido em [Dio92] em que é citado um resultado encontrado em [Kol73].

3.1. Definições E Notações Gerais. Denotaremos por R um anel diferencial comutativo com unidade genérico e p um elemento de $R\{y_1, \ldots, y_n\} \setminus R$. Seja Δ um conjunto de derivações comutativo e Θ representa o monóide, com $1 = Id$, gerado por Δ.

A classe de p é o maior r tal que y_r realmente aparece em p. Denotaremo-lo por $cl(p)$.

A ordem de p em relação a y_r é o maior j tal que $y_r^{(j)}$ que realmente aparece em p. Denotaremo-lo por $o_r(p)$. Se a $r = cl(p)$ então denotaremos $o_r(p)$ simplesmente por $o(p)$.

O grau de um polinômio p em relação à variável $y_r^{(j)}$ é o maior expoente de $y_r^{(j)}$ que realmente aparece em p. Denotaremo-lo por $d_{r,j}(p)$. Se $r = cl(p)$ e $j = o(p)$ então denotaremos $d_{r,j}(p)$ simplesmente por $d(p)$.

O líder de p é $u_p \doteq y_r^{(j)}$, onde $r = cl(p)$ e $j = o(p)$.

O inicial, I_p, de p é o coeficiente da maior potência de u_p.

O separante, S_p, é o polinômio diferencial $\dfrac{\partial p}{\partial u_p}$.

Exemplo 2. Considere em $\mathbb{R}\{x, y\}$ (identificamos $x_1 := x$ e $x_2 := y$), com a derivação $'$, os seguintes polinômios $p(x,y) = {x^{(3)}}^2 + 5y^{(2)}x^3 - 7x^9y^7x^{(2)}{y^{(3)}}^2$ e $q(x,y) = {y^{(7)}}^3 y^2 x x^{(3)} - 3y^{(2)}x^{(3)}x$. Então temos:

	p	q
classe	2	2
ordem	3	7
líder	$y^{(3)}$	$y^{(7)}$
inicial	$-7x^9y^7x^{(2)}$	$y^2xx^{(3)}$
separante	$-14x^9y^7x^{(2)}y^{(3)}$	$3{y^{(7)}}^2y^2xx^{(3)}$

3.2. **Ranking.** Em [Kol73], Kolchin define *rank* (rk) no anel diferencial $R\{y_1,\dots,y_n\}$ como uma ordem em $R\{y_1,\dots,y_n\}$, que deve satisfazer as duas seguintes condições para todo $u,v\in R\{y_1,\dots,y_n\}$, e $\theta\in\Theta$,

1. $\mathrm{rk}(u)\le\mathrm{rk}(\theta u)$;
2. $\mathrm{rk}(u)\le\mathrm{rk}(v)\Longrightarrow\mathrm{rk}(\theta u)\le\mathrm{rk}(\theta v)$.

Nós estamos interessados em estudar sistemas de equações diferenciais com apenas uma derivação, a saber $' := \dfrac{d}{dt}$. Dessa forma, um possível *rank* definido em $R\{y_1,\dots,y_n\}$ com apenas uma derivação, é a aplicação $R\{y_1,\dots,y_n\}\setminus R\to\mathbb{N}^3$ definida da seguinte maneira:

$$\begin{array}{rcl} R\{y_1,\dots,y_n\}\setminus R & \to & \mathbb{N}^3 \\ p & \mapsto & (cl(p),\, o(p),\, d(p)) \end{array}$$

Observe que se invertermos as posições da classe com a ordem, na tripla, obtemos outro *rank* possível. Também podemos fazer uma mesclagem, em que as derivadas das variáveis y_i tenham *rank* menor que o *rank* de y_j para $i<j$.

Assim, como não existe unicidade do *rank* e a partir deste ponto, neste texto, quando se falar em *rank* será o $p\mapsto(cl(p),o(p),d(p))$ exceto menção em contrário.

3.3. **Conjuntos Auto-Reduzidos.** Consideremos dois polinômios p e F no conjunto $R\{y_1,\dots,y_\mu\}\setminus R$. Se F é livre de toda derivada própria de u_p, então F é dito **parcialmente reduzido** em relação a p. Se F é parcialmente reduzido em relação a p e $\deg_{u_p}F<\deg_{u_p}p$, então F é dito **reduzido** em relação a p.

Dizemos que um polinômio F é (parcialmente) reduzido em relação a um conjunto $A\subset R\{y_1,\dots,y_\mu\}\setminus R$ se F for (parcialmente) reduzido em relação aos elementos de A.

Dizemos que um conjunto $A \subset R\{y_1, \dots, y_\mu\} \setminus R$ é auto-reduzido se cada elemento A_i de A é reduzido em relação ao conjunto $A \setminus \{A_i\}$.

Observação 1. Em um conjunto auto-reduzido A o líder de um polinômio não pode ser líder de outro polinômio de A.

Exemplo 3. Considere em $\mathbb{R}\{X_1, \dots, X_n\}$, com a derivada $'$, um conjunto de polinômios diferenciais $\{P_i : i = 1, \dots, n\}$, nos quais $X_j^{(r)}$ não aparece em P_i para $i \neq j$ qualquer que seja $r \in \mathbb{N}$. Então o conjunto $\{P_i : i = 1, \dots, n\}$ é auto-reduzido.

Dado um ranking para polinômios em $R\{y_1, \dots, y_r\}$, definimos o **rank de um conjunto auto-reduzido de n polinômios** que, por abuso de linguagem denotaremos por rk, como a $3n$-upla formada pelas concatenações dos *rank*'s dos polinômios quando colocados em ordem crescente.

Podemos colocar a seguinte ordem para comparar os *rank*'s de dois conjuntos auto-reduzidos:

- Ordenamos A e B através de seus *rank*'s lexicograficamente até $\min\{\#A, \#B\}$ e caso $\mathrm{rk}(A_i) = \mathrm{rk}(B_i)$ para todo $1 \leq i \leq \min\{\#A, \#B\}$, o conjunto que tiver maior cardinalidade tem *rank* menor;
- Caso $\mathrm{rk}(A_i) = \mathrm{rk}(B_i)$ para todo $1 \leq i \leq \#A = \#B$, então A e B são ditos de mesmo *rank*.

Exemplo 4. Consideremos em $\mathbb{R}\{x_1, x_2\}$ a derivada $'$ e os polinômios $P = x_1^{(3)}$, $Q = x_1^{(2)}(x_2')^3$. Então $\{P, Q\}$ forma um conjunto auto-reduzido. P é um polinômio cujo líder é $x_1^{(3)}$, cujo inicial é 1 e cujo separante é 1; Q é um polinômio cujo líder é x_2', cujo inicial é $x_1^{(2)}$ e cujo separante de Q é $3(x_1^{(2)})^2$. O *rank* de $\{P, Q\}$ é $(\underbrace{1,3,1}_{\text{rank de } P}, \underbrace{2,1,3}_{\text{rank de } Q})$.

Um conjunto A de um ideal diferencial $\mathfrak{a}$ é chamado de conjunto característico se for um elemento minimal de

$$\{X | X \subset A, X \text{ é auto-reduzido e } I_Y, S_Y \notin \mathfrak{a} \text{ para todo } Y \subset X\}.$$

3.4. O algoritmo de Redução.

3.4.1. *Divisão Euclidiana.* A divisão euclidiana que introduziremos aqui é uma generalização da divisão euclidiana de polinômios, pois pode ser usada em anéis sem inverso multiplicativo. Como resultado dessa divisão, obtemos um polinômio $R^{\#}$ e um inteiro σ tais que $I_Q^{\sigma} P_0 \equiv R^{\#}$ (mod Q). Sejam P_0 e Q polinômios em $R[Y]$, com $Q \neq 0$.

entrada: P_0 e Q

saída: $R^{\#}$ e σ

$i := 0$

$\sigma_0 := 0$

enquanto $(P_0 \neq 0)$ **e** $(\deg_Y P_0 \geq \deg_Y Q)$ **faça**

$d_i := \deg_Y P_i - \deg_Y Q$

$P_{i+1} := I_Q P_i - I_{P_i} Y^{d_i} Q$

$\sigma_{i+1} := \sigma_i + 1$

$i := i + 1$

fim de laço

$R^{\#} := P_i$

$\sigma := \sigma_i$

Observação 2. Observemos que, em cada passo do laço, P_{i+1} tem grau menor que o grau de P_i em Y. Notemos também, que esse processo deve parar, pois a seqüência (d_i) é estritamente decrescente, o que mostra que se P_i nunca for o polinômio nulo, o processo termina; além disso, o natural σ, obtido no término do processo, é o menor valor que podemos colocar como expoente de I_Q para que $I_Q^{\sigma} P \equiv R^{\#}$ (mod (Q)).

3.4.2. *Redução Parcial.* Seja P um polinômio diferencial e $A \subset R\{Y_1, \ldots, Y_n\}$. Queremos encontrar um polinômio $R^{\dagger}$ e um número inteiro σ tais que $R^{\dagger}$ seja parcialmente reduzido em relação a A e $R^{\dagger} \equiv S_A P \bmod [A]$.

entrada: P_0, A

saída: $R^{\dagger}$ e σ

$i := 0$

$\sigma_0 := 0$

se em P_i só há variáveis que não estão no conjunto

$\{Y_j | j$ é a classe de $A_i\}$ **então vá para** *fim:*

enquanto $\mathrm{rk}(P_i) >= \min\{\mathrm{rk}(A_i) | A_i \in A\}$ **faça**

$v := \max_{1 \leq j \leq n} \{j$ t.q. P_i não é reduzido em relação a $A_j\}$

$\theta A_v :=$ a derivada de A_v tal que θA_v tem menor *rank* possível e o líder de θA_v aparece em P_i

$P_{i+1} :=$ resto da divisão euclidiana de P_i por θA_v
$\tau :=$ inteiro obtido na divisão euclidiana de P_i por A_i
$\sigma_{i+1} := \sigma_i + \tau$
$i := i + 1$
fim de laço
fim: $R^\dagger := P_i$
$\sigma := \sigma_i$

Observação 3. Em cada passo, fazemos a multiplicação de P_i por um separante de um A_j e com isso não introduzimos termos que tenham *rank* maior que o *rank* de $\theta_j u_{A_j}$ e, portanto, a seqüência dos índices j na qual P_i é reduzido em relação a A_j é estritamente decrescente. Ao final, obtemos um polinômio $P^\dagger$ tal que $P^\dagger$ é livre de toda derivada própria de elementos de A, isto é, $P^\dagger$ é parcialmente reduzido em relação a A.

3.4.3. *Redução*. Seja P um polinômio diferencial que é parcialmente reduzido em relação a $A \subset R\{Y_1, \ldots, Y_n\}$. Queremos encontrar um polinômio R^* e um número inteiro σ tais que R^* seja reduzido em relação a A e $S_A^\sigma P \equiv R^*$ mod $[A]$.

Lema 4. *Sejam P_0 um polinômio diferencial nas variáveis diferenciais $Y_1, \ldots, Y_n$ e suas derivadas com coeficientes em R e A um conjunto contido em $R\{Y_1, \ldots, Y_n\}$. Então P é reduzido em relação a A se e somente se fixado um* ranking *para as variáveis $Y_1, \ldots, Y_n$:*

1. $\mathrm{rk}(P) < \min\{\mathrm{rk}(A_i) | A_i \in A\}$ *ou;*
2. *se em P não aparecer $cl(A_i)$ para todo $A_i \in A$.*

Demonstração. ($\Longrightarrow$) Se P for parcialmente reduzido em relação a A então, ou $\mathrm{rk}(P) < \min\{\mathrm{rk}(A_i) | A_i \in A\}$, ou P só tem variáveis que não pertencem ao conjunto $\{Y_j | j$ é a classe de A_i para $A_i \in A\}$.
($\Longleftarrow$) Se P for tal que $\mathrm{rk}(P) < \min\{\mathrm{rk}(A_i) | A_i \in A\}$ então P é reduzido em relação a A. Se P for tal que em P só aparecem variáveis que não pertencem ao conjunto $\{Y_j | j$ é a classe de A_i para $A_i \in A\}$, então P é reduzido parcialmente em relação a A. □

entrada: P_0 e A
saída: R^* e σ

$i := 0$
enquanto P_i não for reduzido em relação a A faça
$j := \max\{A_k | P_i$ não é reduzido em relação a $A_k\}$
$i := i + 1$
$P_i :=$ resto da divisão euclidiana de P_{i-1} por A_j
quando escritos em termos de u_{A_j}
$\tau :=$ inteiro obtido na divisão euclidiana de P_{i-1} por A_j
$\sigma_i := \sigma_{i-1} + \tau$
fim de laço
$R^* := P$
$\sigma := \sigma_i$

Observação 4. Esse processo termina, pois $j_1 > j_2 > \cdots$, isto é, a seqüência (j_i) é estritamente decrescente, como de fato $j_i > j_{i+1}$, pois a multiplicação de P_{i-1} por I_{j_i} tem *rank* menor que o *rank* de u_{A_i}. Além disso, $P_i := I_{j_i} P_{i-1} - A_i Q_i$ tem *rank* menor ou igual a de P_{i-1} e P_i é reduzido em relação a $A_i, A_{i+1}, \ldots$.

Fixemos um *rank* em $k\{y_1, \ldots, y_\mu\}$. Então temos o seguinte

Lema 5 (Ritt). *Seja A um conjunto auto-reduzido de $\varnothing \neq \Sigma \subset k\{y_1, \ldots, y_\mu\}$. Então são equivalentes:*

a. *A é um conjunto característico de Σ;*
b. *todo polinômio, em Σ, reduzido em relação a A é nulo.*

Demonstração. (b. $\Rightarrow$ a.) Suponhamos que A não seja um conjunto característico de Σ, então existe um conjunto B tal que B é um conjunto característico de Σ e portanto $\mathrm{rk}(B) < \mathrm{rk}(A)$. Isto significa que B tem mais elementos que A e $\mathrm{rk}(A_i) = \mathrm{rk}(B_i)$ para $1 \leq i \leq \#A$ ou que existe um j tal que $\mathrm{rk}(B_j) < \mathrm{rk}(A_j)$ para algum $1 \leq j \leq \min\{\#A, \#B\}$. Se acontecer: B tem mais elementos que A e $\mathrm{rk}(A_i) = \mathrm{rk}(B_i)$ para todo $1 \leq i \leq \#A$ então $B_{\#A+1}$ é reduzido em relação a A. Se acontecer: $\mathrm{rk}(B_i) < \mathrm{rk}(A_i)$ para algum $1 \leq i \leq \min\{\#A, \#B\}$, então existe algum $1 \leq i \leq \min\{\#A, \#B\}$ tal que B_i é reduzido em relação a A.

(a. $\Rightarrow$ b.) Suponhamos que A seja um conjunto característico e que Σ contenha um polinômio não nulo F que seja reduzido em relação a A. Se a classe de F for maior que a de $A_{\#A}$, conseguimos um conjunto auto-reduzido de *rank* menor que o de A, fazendo $A \cup \{F\}$;

caso contrário, se o elemento de A que não é excedido por F é A_j, então o conjunto $\{A_1, \dots, A_{j-1}, F\}$ tem *rank* menor que A. □

Um conjunto auto-reduzido $\mathcal{A}$ é dito coerente se dados $a, a' \in \mathcal{A}$ e se u_a e $u_{a'}$ (os líderes de a e a') com uma menor derivada comum $v = \theta_a u_a = \theta_{a'} u_{a'}$, então $S_{a'}\theta_a a - S_a \theta_{a'} a' \in (\mathcal{A}_v) : H_{\mathcal{A}}^{\infty}$, onde $\mathcal{A}_v$ é o conjunto dos polinômios diferenciais θb em que $\theta \in \Theta$, $b \in \mathcal{A}$ e $\mathrm{rk}(\theta u_b) < \mathrm{rk}(v)$. Denotaremos por (A) o ideal algébrico gerado por A, $[A]$ o ideal diferencial gerado por A. Se $\Sigma \subset R\{y_1, \dots, y_n\}$ e $\alpha \in R\{y_1, \dots, y_n\}$, então $\Sigma : \alpha^n$ denota o conjunto $\{x \in R\{y_1, \dots, y_n\} | \alpha^n x \in \Sigma$ para algum $n \in \mathbb{N}\}$ e $\Sigma : \alpha^\infty$ denota o conjunto $\bigcup_{n \in \mathbb{N}} \Sigma : \alpha^n$. Observemos que se Σ for um ideal, $\Sigma : \alpha^\infty$ também será um ideal.

Em [Kol73], Kolchin demonstra o seguinte resultado válido para anéis com várias derivações.

Lema 6 (Kolchin). *Sejam R um anel diferencial e A um subconjunto de $R\{y_1, \dots, y_\mu\}$ auto-reduzido, coerente. Então todo polinômio em $[A] : H_A^\infty$ reduzido em relação a A está em $(A) : H_A^\infty$.*

Em anéis diferenciais com apenas uma derivação, todo conjunto auto-reduzido é coerente. Assim, podemos tirar como corolário deste lema, o seguinte resultado:

Corolário 7. *Sejam R um anel diferencial, com a derivação $'$ e $A \subset R\{y_1, \dots, y_\mu\}$ um conjunto auto-reduzido. Então todo polinômio em $[A] : H_A^\infty$ reduzido em relação a A está em $(A) : H_A^\infty$.*

Como o corolário exige que o anel diferencial tenha apenas uma derivação – a demonstração a partir do lema (6) é imediata, porém por exigir mais sobre o anel diferencial, tal demonstração pode ser simplificada ao ponto que o mesmo argumento que será usado para demonstrar o lema (8) pode ser aplicado.

Observação 5. Se A é um conjunto auto-reduzido, então I_A e S_A são reduzidos em relação a A.

Definição. Um conjunto auto-reduzido é dito **ortonômico** se seus elementos tem grau 1 em seus líderes.

Observação 6. Se A é um conjunto auto-reduzido ortonômico, então o separante de $A_i \in A$ e o inicial de $A_i \in A$ coincidem.

Lema 8 (Diop, S.). *Se A é um conjunto auto-reduzido, coerente e ortonômico contido em $k\{Y_1, \dots, Y_\mu\}$ então*

a. *se $P \in [A] : I_A^\infty$ e P é reduzido em relação a A então $P = 0$.*

b. *$[A] : I_A^\infty$ é primo com conjunto característico A.*

Demonstração. a. Sejam $A_1, A_2, \cdots, A_m$ com $\mathrm{rk}(A_1) < \mathrm{rk}(A_2) < \cdots < \mathrm{rk}(A_m)$ os elementos de A. Suponhamos que exista $0 \neq P \in [A] : I_A^\infty$ que seja reduzido em relação a A. Pelo corolário 7, $P \in (A) : I_A^\infty$ então podemos escrever:

$$I_A^n P = \sum_{i=1}^{t} P_i A_i + P_0, \tag{1}$$

para algum $n \in \mathbb{N}$ e $P_0 = 0$. Como $P \neq 0$, então existe pelo menos um $P_i \neq 0$. Suponhamos, por absurdo, que s seja o menor valor que t pode assumir em (1) tal que, para algum $n \in \mathbb{N}$, P_0 seja livre de u_s. Escrevendo $P_i = P_i^0 + u_s Q_i$ para $1 \leq i \leq s$, onde Q_i é polinômio, $A_s = I_s u_s + R_s$, R_s livre de u_s, temos:

$$I_A^n P = (P_s^0 I_s + \sum_{i=1}^{s} Q_i A_i) u_s + \underbrace{(P_0 + P_s^0 R_s + \sum_{i=1}^{s-1} P_i^0 A_i)}_{\text{livre de } u_s}$$

Impondo que o polinômio que multiplica u_s seja 0, pois $I_A^n P$ é livre de u_s, temos: $I_A^n P = P_0 + P_s^0 R_s + \sum_{i=1}^{s-1} P_i^0 A_i$.

Não sabemos, a priori, se $P_0 + P_s^0 R_s$ é ou não livre de u_{s-1}. Porém, podemos, eventualmente, aumentar o valor de n para que possamos fazer a divisão de $P_0 + P_s^0 R_s$ por A_{s-1} e dessa maneira, observando que na divisão, não introduzimos elementos maiores que u_{s-1}, então podemos re-escrever $I_A^n P$ como $\widetilde{P}_0 + \sum_{i=1}^{s-1} \widetilde{P}_i A_i$ com $\widetilde{P}_0$ livre de u_{s-1}, o que contraria a minimalidade de s.

b. Pelo lema 5, temos que A é um conjunto característico de $[A] : I_A^\infty$. Sejam P^* e Q^* os reduzidos de P e Q respectivamente com relação a A. Então, do fato de A ser auto-reduzido e ortonômico temos que todo polinômio reduzido em relação a A é livre de qualquer líder dos elementos de A. Assim, o produto de reduzidos é reduzido e pela parte a. do lema, $P^*Q^* = 0$. Logo, lembrando que I_A e $S_A(= I_A)$ não estão em $[A] : I_A^\infty$ pois A é um conjunto característico, temos que P ou Q está em $[A] : I_A^\infty$, o que prova que $[A] : I_A^\infty$ é primo. □

3.4.4. *Aplicação.* Agora trabalharemos com o ideal diferencial gerado pelas relações polinomiais $\begin{cases} \dot{X}_i - f_i(X,U) & i = 1,...,n \\ Y_j - \phi_j(X,U) & j = 1,...,j \end{cases}$ no anel diferencial $\mathbb{R}\{X_1, \ldots, X_n, Y_1, \ldots, Y_j, U_1, \ldots, U_s\}$. Mostraremos que esse ideal diferencial é primo.

Definamos o seguinte *rank* para as variáveis diferenciais $\mathrm{rk}(X_1) < \mathrm{rk}(X_2) < \cdots < \mathrm{rk}(X_n) < \mathrm{rk}(Y_1) < \cdots < \mathrm{rk}(Y_r) < \mathrm{rk}(U_1) < \cdots < \mathrm{rk}(U_s) < \mathrm{rk}(U_1') < \cdots < \mathrm{rk}(U_s') < \mathrm{rk}(U_1'') < \cdots < \mathrm{rk}(U_s'') <$ todas as derivadas de elementos de U $< \mathrm{rk}(X_1') < \mathrm{rk}(X_2') < \cdots \mathrm{rk}(X_n') < \mathrm{rk}(Y_1') < \cdots < \mathrm{rk}(Y_r') < \cdots$.

Assim, $\{\dot{X}_i - f_i(X,U), Y_j - \phi_j(X,U) : i = 1,...,n \text{ e } j = 1,...,r\}$ é auto-reduzido. Como só temos uma derivação a ser considerada (a saber $\frac{d}{dt}$), claramente esse conjunto é coerente e ortonômico. Logo o ideal diferencial

$$[\dot{X}_i - f_i(X,U), Y_j - \phi_j(X,U) : i = 1,...,n \text{ e } j = 1,...,m] : 1^\infty =$$
$$= [\dot{X}_i - f_i(X,U), Y_j - \phi_j(X,U) : i = 1,...,n \text{ e } j = 1,...,m]$$

é um ideal primo.

Referências

[Bou81] N. Bourbaki. *Algèbre*, volume XI of *Éléments de Matématique*, chapter 5. Herman, 1981.

[Dio92] S. Diop. Differential-algebraic decision methods and some applications to system theory. *Theoretical Computer Science*, 98:137–161, 1992.

[Fli89] M. Fliess. Automatique et Corps Differentiéls. *Forum Math.*, 1:227–238, 1989.

[Kap78] I. Kaplanski. *Introduction to Differential Algebra*. Herman, 1978.

[Kol73] E. R. Kolchin. *Differential algebra and algebraic groups*. Academic Press, 1973.

[Rit50] J. F. Ritt. *Differential algebra*, volume 33. Amer. Math. Soc. Coll. Pub., New York, 1950.

[Sei52] A Seidenberg. Some basic theorems in differential algebra (characteristic p, arbitrary). *Trans. Amer. Math. Society*, 73, 1952.

RELATÓRIOS TÉCNICOS DO DEPARTAMENTO DE MATEMÁTICA APLICADA

2000

RT-MAP-0001 – Laécio C. Barros, Suzana A. O. Souza &
Pedro A. Tonelli
"TWO CASES OF ASYMPTOTIC SMOOTHNESS FOR FUZZY DYNAMICAL SYSTEMS"
February 16, 2000 – São Paulo – IME-USP – 10 pg.