Seminário: Teorias O-minimais e Geometria Algébrica Real

Ricardo Bianconi

1º Semestre de 2010

O Teorema de Tarski-Seidenberg

1 Corpos reais fechados

Um corpo K é chamado de **corpo real** se $-1 \notin \sum K^2$, isto é, o elemento -1 não pode ser obtido como soma de quadrados de elementos de K. Disto decorre que a característica de K deve ser zero, pois se tivéssemos $1 + 1 + \ldots + 1 = 0$ (ou $p \cot 1 = 0$, para algum número primo p), então teríamos $-1 = (p-1) \cdot 1 \in \sum K^2$.

Um corpo real K é dito **real fechado** se toda extensão algébrica própria $K \subsetneq L$, L não pode ser corpo real. Ou seja, K seria um elemento maximal na classe de todos os corpos reais, ordenados pela extensão de corpos.

Teorema 1.1 Se K for um corpo real fechado, então existe uma única ordem $<$ em K, compatível com as operações de K.

Demonstração: Seja P o conjunto de todos os elementos de $K \setminus \{0\}$ que puderem ser escritos como soma de quadrados (ou seja, $P = \sum K^2$). Definimos a relação binária $<$ em K por $a < b$ se, e somente se, $(b - a) \in P$.

Observemos que se $a = \sum_1^n x_i^2 \in P$, então

$$\frac{1}{a} = \frac{1}{\sum_1^n x_i^2} = \frac{\sum_1^n x_i^2}{(\sum_1^n x_i^2)^2} \in P.$$

Com o mesmo tipo de truque, podemos mostrar que se $a, b \in P$, então $(a + b) \in P$, e $ab \in P$.

Temos que $a \not< a$, pois $0 = a - a \notin P$; se $a < b$, então $b \not< a$, pois, senão, $-1 = (b-a)/(a-b) \in \sum K^2$; e se $a < b$ e $b < c$, então $a < c$, pois $c - a = (c - b) + (b - a)$.

Portanto, a relação $<$ é pelo menos uma ordem parcial, que respeita a soma, produto e inverso.

Agora, suponhamos que exista $a \in K \setminus \{0\}$, $a \notin P$. Seja $L = K(\sqrt{a}) \cong K[X]/(x^2 - a)$. Os elementos de $K[\sqrt{a}]$ são da forma $c + d\sqrt{a}$, com $c, d \in K$. Como assumimos a hipótese de que K é real fechado, essa extensão, por ser própria (pois, se $\sqrt{a} \in K$, $a = (\sqrt{a})^2 \in P$), não pode ser um corpo real e, portanto, existem $n \in \mathbb{N}$ e $c_i, d_i \in K$, $0 \leq i \leq n$, tais que $-1 = \sum_i (c_i + d_i\sqrt{a})^2 = \sum_i c_i^2 + a\sum_i d_i^2 + 2\sqrt{a}\sum_{i<j} c_i d_j$, ou seja, como $-1 \in K$, temos $-1 = \sum_i c_i^2 + a\sum_i d_i^2$. Daí decorre que

$$a = -\frac{1 + \sum_i c_i^2}{\sum_i d_i^2} \in -P.$$

Assim, para todo $a \in K$, ou $a = 0$, ou $a \in P$, ou $a \in -P$. Isto reflete na relação $<$ como a propriedade de que, para todo $a, b \in K$, ou $a < b$, ou $a = b$, ou $b < a$. Ou seja, a relação $<$ é uma ordem total.

Só falta provar sua unicidade. Seja $\prec$ uma ordem total em K, respeitando a soma, produto e inverso. Seja $\mathcal{P} = \{a \in K : 0 \prec a\}$. Então, como $a^2 = (-a)^2$ e como $\prec$ deve respeitar as operações de soma e produto, temos que $P \subseteq \mathcal{P}$. Mas, se $a \in K$, $a \neq 0$ e $a \notin P$, então $(-a) \in P$, devemos ter $0 \prec -a$ e, portanto, $-a \in \mathcal{P}$, o que implica que $p = \mathcal{P}$, ou seja, $\prec = <$. □

Dado um corpo real K, um subconjunto $Q \subset K$ é chamado de **cone** se for fechado pela soma, produto e se contiver todos os quadrados de elementos de K (ou seja $K^2 \subset P$). Se também $-1 \notin Q$, dizemos que Q é um **cone próprio**. Por exemplo, o conjunto de todas as somas de quadrados de elementos de K forma um cone próprio.

Observemos que se P for um cone próprio, então $P \cap (-P) = \{0\}$.

Teorema 1.2 Todo corpo real pode ser ordenado, com uma ordem compatível com as operações do corpo.

Demonstração: Seja $\mathscr{P}$ o conjunto de todos os cones próprios de K, ordenados pela inclusão. Sabemos que $\mathscr{P} \neq \varnothing$. Seja $(I, <)$ uma ordem linear não vazia, e seja $P_i \in \mathscr{P}$, $i \in I$, uma cadeia (isto é, se $i < j$, então $P_i \subseteq P_j$).

Então $\bigcup_{i\in I} P_i \in \mathscr{P}$ é limitante superior daquela cadeia. Portanto, pelo Lema de Zorn, existe pelo menos um elemento $P \in \mathscr{P}$ maximal.

Afirmamos que P define uma ordem linear em K, que é compatível com as operações do corpo. Na verdade, como P é fechado pela soma, produto e inversa, basta mostrar que $K = P \cup (-P)$.

Seja $a \in K \setminus \{0\}$ e suponhamos que $-a \notin P$. Então $Q = \{x + ay : x, y \in P\}$ também é um cone próprio de F, pois evidentemente é fechado pela soma e produto, continua contendo K^2. Se $-1 \in Q$, então existiriam $x, y \in P$, tais que $-1 = x + ay$, o que implicaria que, ou $y = 0$ e $-1 = x \in P$, ou $y \neq 0$ e $(-a) = (1+x)/y = y(1+x)(1/y)^2 \in P$, contradizendo as hipóteses.

Como P é maximal, devemos ter que $a \in P$. □

Teorema 1.3 Sejam K, um corpo ordenado, e $f \in K[X]$, um polinômio irredutível de grau $n > 1$. Suponha que existam $a, b \in K$, tais que $a < b$ e $f(a)f(b) < 0$. Então o corpo $L = K[X]/(f)$ admite uma ordem $<$ que estende a de K e tal que $a < x + (f) < b$.

Demonstração: Suponhamos que $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$. Podemos supor que $f(a) < 0$ e $f(b) > 0$, sendo que o outro caso é simétrico e demonstrado de modo análogo. Podemos também supor que não existam $c, d \in K$, tais que $a < c < d < b$, com $f(c) > 0$ e $f(d) < 0$, simplesmente substituindo o intervalo $]a, b[$ por um outro menor dentro dele.

Sejam $I = \{t \in]a, b[: f(t) < 0\} \cup]-\infty, a]$ e $J = \{t \in]a, b[: f(t) > 0\} \cup [b, \infty[$. Então $K = I \cup J$ (pois f não pode ter raiz em K) e definem um corte em K.

Seja $\xi = x + (f) \in L$. Estendemos a ordem de K ao conjunto $K + \xi K$, impondo que $I < \xi < J$. Observando que se $a \in K$, $a \neq 0$, então o par (aI, aJ) (ou (aJ, aI), se $a < 0$) ainda determina um corte me K, definimos $aI < a\xi < aJ$, se $a > 0$, ou $aJ < a\xi < aI$, se $a < 0$. Daí, estendemos a ordem a todo $K + \xi K$ por translações. Certamente essa ordem respeita a soma.

Para estender a ordem a $K + \xi K + \xi^2 K$, fazemos do mesmo jeito, usando os cortes correspondentes aos quadrados dos elementos de I e de J, tratando, é claro, dos casos em que $0 \in I$ e $0 \in J$.

Desse modo podemos ir estendendo a ordem até abarcar todo o corpo L. □

Com isto, podemos demonstrar as seguintes equivalências.

Teorema 1.4 Seja K um corpo real. As seguintes asserções são equivalentes :

1. K é real fechado.
2. K admite uma única ordem $<$, tal que, para todo polinômio $f \in K[X]$ e todos $a, b \in K$, se $a < b$ e $f(a)f(b) < 0$, então existe $c \in]a, b[$, tal que $f(c) = 0$.
3. K admite uma única ordem $<$, tal que, para todo $a \in K$, $0 < a$, existe $b \in K$, $a = b^2$, e, também, todo polinômio $f \in K[X]$ de grau ímpar admite uma raiz em K.
4. $K[i]$ é um corpo algebricamente fechado.

Demonstração: Vamos demonstrar as seguintes implicações: $1 \to 2 \to 3 \to 4 \to 1$.

1 → 2 : Seja K um corpo real fechado e sejam $a, b \in K$, $a < b$, e $f \in K[X]$, tal que $f(a)f(b) < 0$. Então $f(x)$ deve possuir um fator irredutível g, responsável por essa mudança de sinal de f (ou seja, $g(a)g(b) < 0$ e g deve entrar na decomposição de f com um grau ímpar - caso contrário, vemos que f não poderia trocar de sinal). Se o grau de g for 1, certamente terá uma raiz no intervalo $]a, b[$. Caso o grau de g fosse $n > 1$, póderíamos estender a ordem de K à extensão algébrica própria $L = K[X]/(g)$, como acima, contradizendo a hipótese de que K é real fechado.

2 → 3 : Seja $a \in K$, $a > 0$. O polinômio $f(x) = x^2 - a$ satisfaz $f(0) = -a < 0$ e $f(1 + a) = a^2 + a + 1 > 0$ e, portanto, deve admitir uma raiz $c \in]0, 1 + a[$. Agora, se $f \in K[X]$ for polinômio de grau ímpar, digamos $g(x) = a_{2n+1}x^{2n+1} + \ldots + a_0$, com $a_{2n+1} > 0$, por exemplo, então para $x \leq -1 - (1/a_{2n+1}) \sum_{j=0}^{2n} |a_j|$, temos que $f(x) < 0$ e se $x \geq 1 + (1/a_{2n+1}) \sum_{j=0}^{2n} |a_j|$, então $f(x) > 0$ e, portanto, deve possuir uma raiz nesse intervalo.

3 → 4 : Suponhamos que K satisfaça a condição 3. Consideremos, primeiramente um polinômio não constante $f \in K[X]$ e mostremos que ele tem raiz em $K[i]$. Seja $N = 2^m n$ o grau de f, com n ímpar. Se $m = 0$, por hipótese, f já tem uma raiz em $K \subset K[i]$. Suponha que essa afirmação valha para $m - 1$ e provemos que também valerá para m. Sejam $y_1, \ldots, y_N$ as raízes de f num fecho algébrico de K e formemos, para $h \in \mathbb{Z}$,

$$g_h = \prod_{1 \leq \lambda < \mu \leq N} (x - y_\lambda - y_\mu - h y_\lambda y_\mu).$$

Como esse polinômio é simétrico nas raízes $y_1, \ldots, y_N$, $g_h \in K[X]$. O seu grau é $N(N-1)/2 = 2^{m-1}n'$, com n' ímpar. Por hipótese de indução, g_h tem uma raiz em $K[i]$ e, portanto, existem $\lambda < \mu$ (dependentes de h), tais que $y_\lambda + y_\mu + hy_\lambda y_\mu \in K[i]$. Como $\mathbb{Z}$ é infinito e o conjunto dos pares $(\lambda(h), \mu(h))$ de índices dessas raízes é finito, existem $h_1, h_2 \in \mathbb{Z}$, com $h_1 \neq h_2$, mas $(\lambda(h_1), \mu(h_1)) = (\lambda(h_2), \mu(h_2)) = (\lambda, \mu)$, ou seja, $y_\lambda + y_{\mu(h_j)} + h_j y_\lambda y_\mu \in K[i]$, $j = 1, 2$. Isso implica que $y_\lambda y_\mu \in K[i]$ e, portanto, que $y_\lambda + y_\mu \in K[i]$, o que significa que y_λ e y_μ são soluções de uma equação de segundo grau com coeficientes em $K[i]$.

Para terminarmos essa parte, precisamos mostrar que uma equação de segundo grau com coeficientes em $K[i]$ tem suas raízes em $K[i]$. Para isso, usaremos a fórmula de Bhaskara, o que envolve o cálculo de uma raiz quadrada. Se mostrarmos que, para todo $a, b \in K$, existem $u, v \in K$, tais que $(u+vi)^2 = a+bi$, estaremos feitos. Para isso, temos que resolver em $K[i]$ a equação $(u+vi)^2 = a+bi$ nas variáveis u e v, ou seja, o sistema $u^2 - v^2 = a$ e $2uv = b$. Se $b = 0$, podemos resolver em K a equação. Se $b \neq 0$, então $u \neq 0$ e podemos fazer $v = b/(2u)$, obtendo a equação $u^2 - (b/2u)^2 = a$ ou $4u^4 - 4au^2 - b^2 = 0$. Observemos que seu discriminante $16a^2 + 16b^2 \geq 0$ e, portanto, existe $c \geq 0$, tal que $c^2 = a^2 + b^2$ - representemos $c = \sqrt{a^2 + b^2}$. Assim, temos as soluções $u^2 = (a \pm c)/2$. Note-se que $c \geq a$ e, portanto, a solução $(a + c)/2 \geq 0$. Seja $d \geq 0$, tal que $d^2 = (a + c)/2$. Então, fazendo $u = d$ e $v = b/(2d)$, vemos que $(u + vi)^2 = a + bi$.

$\mathbf{4} \to \mathbf{1}$: Como $K[i]$ é algebricamente fechado, toda extensão algébrica de K deve ser isomorfa a um subcorpo de $K[i]$, estendendo K. Como $K[i]$ é de grau 2 sobre K, essa extensão só pode ser K ou $K[i]$. Como $i^2 = -1$, a única extensão algébrica e real de k é o próprio K. □

São importantes dois teoremas do Cálculo para as aplicações a seguir.

Teorema 1.5 (Teorema de Rolle) Sejam K um corpo real fechado, $f \in K[X]$, f' a derivada formal de f, e $a, b \in K$, com $a < b$. Se $f(a) = f(b)$, então existe $c \in]a, b[$, tal que $f'(c) = 0$.

Demonstração: Tomando $g(X) = f(X) - f(a)$ e diminuindo o intervalo, se necessário, podemos supor que a e b são duas raízes consecutivas de $f(X)$. Escrevamos $f(X) = (X - a)^m (X - b)^n g(X)$, sendo que $g(X)$ não se anula no intervalo $[a, b]$. Então $f'(X) = (X - a)^{m-1}(X - b)^{n-1}[m(X - b)g(X) + n(X - a)g(X) + (X - a)(X - b)g'(X)]$. O polinômio entre os colchetes vale $m(a - b)g(a)$ em $X = a$ e $n(b - a)g(b)$ em $X = b$. Como o sinal de $g(X)$

tem que ser o mesmo em $X = a$ e em $X = b$, vemos que o polinômio entre colchetes troca de sinal e, portanto, tem uma raiz $c \in]a, b[$. Daí, $f'(c) = 0$. □

Teorema 1.6 (Teorema do Valor Médio) Sejam K um corpo real fechado, $f \in K[X]$, f' a derivada formal de f, e $a, b \in K$, com $a < b$. Existe $c \in]a, b[$, tal que

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

Demonstração: Basta aplicar o Teorema de Rolle ao polinômio $g(X) = [(f(X) - f(a))/(b - a)]$. □

Como consequência desses resultados, valem em geral os critérios conhecidos para avaliar o crescimento e decrescimento de uma função polinomial.

Teorema 1.7 Sejam K um corpo real fechado, $f \in K[X]$, f' a derivada formal de f, e $a, b \in K$, com $a < b$. Se $f'(x) > 0$, para todo $x \in]a, b[$, então $f(X)$ é estritamente crescente nesse intervalo. Se $f'(x) < 0$, para todo $x \in]a, b[$, então $f(X)$ é estritamente decrescente nesse intervalo. □

Teorema 1.8 Seja K um corpo ordenado e $f(X) \in K[X]$ um polinômio não constante. Então:

1. Se o grau de f for par e seu coeficiente do termo de maior grau for positivo, então

$$\lim_{x \to \infty} f(X) = \lim_{x \to -\infty} f(X) = +\infty.$$

2. Se o grau de f for ímpar e seu coeficiente do termo de maior grau for positivo, então

$$\lim_{x \to \infty} f(X) = -\lim_{x \to -\infty} f(X) = +\infty.$$

3. Nos casos em que o coeficiente do termo de maior grau for negativo, basta trocar os sinais dos limites.

Demonstração: Basta fazer as desigualdades usuais. □

2 O Teorema de Tarski-Seidenberg

Dado um corpo real fechado K, munido da única ordem compatível $<$, dizemos que um subconjunto $E \subset K^n$ é **semi-algébrico** se for uma combinação booleana de conjuntos dos tipos

$$\begin{aligned} V^+(P) &= \{x \in K^n : P(x) > 0\}, \\ V^0(P) &= \{x \in K^n : P(x) = 0\}, \\ V^-(P) &= \{x \in K^n : P(x) < 0\}, \end{aligned}$$

sendo que $P \in K[X]$, $X = (X_1, \ldots, X_n)$.

Queremos demonstrar o Teorema de Tarski e Seidenberg, que afirma que a projeção de um conjunto semi-algébrico também é semi-algébrico. A idéia da demonstração é considerar o caso em que a projeção é $\Pi : K \times K^n \to K^n$, e eliminar dos polinômios a variável X, correspondente à primeira coordenada.

Vamos introduzir uma notação que ressalta mais o caráter combinatório dos argumentos usados a seguir.

Definimos a função que indica o sinal de um elemento de K por $\mathbf{sn} : K \to \{-1, 0, 1\}$, $\mathbf{sn}(0) = 0$, $\mathbf{sn}(x) = 1$ se $x > 0$ e $\mathbf{sn}(x) = -1$ se $x < 0$.

Dado um polinômio não nulo $f \in K[X]$, suponhamos que tenha $N \geq 0$ raízes $x_1 < \ldots < x_n \in K$. Denominamos $x_0 = -\infty$ e $x_{N+1} = +\infty$. Sejam $I_k =]x_k, x_{k+1}[$. Então, como K é real fechado, o sinal de f em cada um desses intervalos não pode mudar, senão haveria outra raiz de f nesse intervalo. Denotaremos por $\mathbf{sn}(f(I_k))$ o valor desse sinal.

Definimos o vetor linha, com $2n+1$ posições, denominado $\mathsf{Sn}_K(f)$, e que codificará as variações de sinais de $f(x)$:

$$\left[\begin{array}{ccccccc} \mathbf{sn}(f(I_0)) & \mathbf{sn}(f(x_1)) & \mathbf{sn}(f(I_1)) & \ldots & \mathbf{sn}(f(x_n)) & \mathbf{sn}(f(I_n)) \end{array} \right]$$

No caso de vários polinômios $f_1, \ldots, f_N \in K[X]$, representamos na matriz, cujas linhas serão os vetores linhas $\mathsf{Sn}_K(f_j)$, denominada de $\mathsf{Sn}_K(f_1, \ldots, f_N)$, as variações de sinais de todos eles, sendo que, agora, a lista $x_1, \ldots, x_n \in K$ contém as raízes de todos os polinômios $f_1, \ldots, f_N$, em ordem crescente (sem contar multiplicidade de raízes).

Suponhamos que os graus dos polinômios $f_1, \ldots, f_N$ sejam no máximo m. Então existirão no máximo $n = Nm$ elementos $x_1 < \ldots < x_n$ contendo as raízes de todos aqueles polinômios. Seja $W_{N,m}$ o conjunto de todas as matrizes, cujas entradas sejam -1, 0, ou 1, com N linhas e $2k+1$ colunas, com $0 \leq k \leq Nm$. Dentre elas estão as possíveis matrizes da forma $\mathsf{Sn}_K(f_1, \ldots, f_N)$. É claro que nem todas as matrizes de $W_{N,m}$ são desse tipo, pois

podemos ter, por exemplo, matrtizes em que uma linha contém dois zeros seguidos, mas a linha não seja toda nula.

Lema 2.1 Seja $\varepsilon : \{1, \ldots, N\} \to \{-1, 0, 1\}$ uma função. Existe uma parte $W(\varepsilon)$ de $W_{N,m}$, tal que, para todo corpo real fechado K e toda sequência de polinômios $f_1, \ldots, f_N \in K[X]$, de graus sejam no máximo m, o sistema

$$\left\{ \begin{array}{rcl} \mathbf{sn}(f_1(x)) & = & \varepsilon(1) \\ \vdots & \vdots & \vdots \\ \mathbf{sn}(f_N(x)) & = & \varepsilon(N) \end{array} \right.$$

tem uma solução $x \in K$ se, e somente se, $\mathsf{Sn}_K(f_1, \ldots, f_N) \in W(\varepsilon)$.

Demonstração: Basta tomar $W(\varepsilon)$ como sendo o conjunto de todas as matrizes de $W_{N,m}$ que contenham uma coluna da forma

$$\left[\begin{array}{c} \varepsilon(1) \\ \vdots \\ \varepsilon(N) \end{array} \right]$$

□

Lembramos que, para que uma matriz $A \in W_{N,m}$ seja da forma $\mathsf{Sn}_K(f_1, \ldots, f_N)$, suas linhas devem ser da forma

$$\left[\begin{array}{ccccccccc} \pm 1 & & 0 & & \pm 1 & \ldots & \pm 1 & 0 & \pm 1 \end{array} \right],$$

ou seja, os zeros somente podem aparecer entre dois elementos não nulos, mas poderemos ter dois elementos consecutivos não nulos. O único caso em que poderá haver zeros consecutivos é o de um polinômio identicamente nulo, situação em que a linha somente conterá zeros.

Exemplo 2.1 Vamos escrever a matriz $\mathsf{Sn}_K(f_1, f_2)$, sendo $f_1(X) = X^2 - 3X + 2 = (X - 1)(X_2)$ e $f_2(X) = X^3 - X = X(X - 1)(X + 1)$: os zeros dos dois polinômios são, em ordem crescente, -1, 0, 1, 2, ou seja, quatro raízes e, portanto, cinco intervalos: $]-\infty, -1[$, $\{-1\}$, $]-1, 0[$, $\{0\}$, $]0, 1[$, $\{1\}$, $]1, 2[$, $\{2\}$, $]2, \infty[$:

$$\mathsf{Sn}_K(f_1, f_2) = \left[\begin{array}{rrrrrrrrr} 1 & 1 & 1 & 1 & 1 & 0 & -1 & 0 & 1 \\ -1 & 0 & 1 & 0 & -1 & 0 & 1 & 1 & 1 \end{array} \right]$$

O processo de eliminação da variável X do sistema consiste em tomar um dos polinômios de grau máximo da lista, diganmos que seja f_N, e substituí-lo por sua derivada. Para não perdermos informação acerca do sistema original, acrescentamos à lista, os restos da divisão de f_N por $f_1, \ldots, f_{N-1}$ e f'_N, obtendo os polinômios $g_1, \ldots, g_N$, cujos graus são mernores do que N. A partir da matriz $\mathsf{Sn}_K(f_1, \ldots, f_{N-1}, f'_N, g_1, \ldots, g_N)$, podemos recuperar a matriz $\mathsf{Sn}_K(f_1, \ldots, f_N)$.

Teorema 2.1 Existe um algoritmo que, dada matriz da forma $\mathsf{Sn}_K(f_1, \ldots, f_{N-1}, f'_N, g_1, \ldots, g_N)$, como definida acima, recupera de modo único a matriz $\mathsf{Sn}_K(f_1, \ldots, f_N)$.

Demonstração: Sejam $x_1 < \ldots < x_k$, $k \leq 2Nm$ as raízes em K dos polinômios $f_1, \ldots, f_{N-1}, f'_N, g_1, \ldots, g_N$, que não seja identicamente nulos. Sejam $x_{i_1}, \ldots, x_{i_M}$ a subsequência composta pelas raízes de $f_1, \ldots, f_{N-1}, f'_N$. Convencionemos que $i_0 = 0$ com $x_0 = -\infty$ e $i_{M+1} = N + 1$, com $x_{N+1} = +\infty$.

Observemos que se x_{i_j} for um zero de f_r (ou f'_N, respectivamente), então $f_N(x_{i_j}) = g_r(x_{i_j})$ (ou $f_N(x_{i_j}) = g_N(x_{i_j})$, respectivamente). Seja $\theta : \{1, \ldots, M\} \to \{1, \ldots, N\}$ uma função que associe a cada j o índice $\theta(j) = r$, tal que $f_N(x_{i_j}) = g_r(x_{i_j})$. No caso de x_{i_j} ser uma raiz de mais de um daqueles polinômios, podemos escolher o menor índice r, tal que a condição é satisfeita.

Se algum dos x_{i_j} for raiz de um g_r, sabemos que deverá ser também raiz de f_N. Precisamos achar as possíveis raízes de f_N.

O caso inicial é aquele em que $M = 0$, ou seja, os polinômios $f_1, \ldots, f_{N-1}, f'_N$ não tem raízes em K. Isto quer dizer que o sinal de f'_N é sempre positivo ou negativo. Em ambos os casos, o grau de f'_N deve ser par e, portanto, o grau de f_N será ímpar, o que implica que f_N tem uma raiz em $K =]x_0, x_1[$.

Agora trataremos dos casos em que $M > 0$.

Existirá uma raiz de f_N no intervalo $]-\infty, x_{i_1}[$ se, e somente se,

$$\mathbf{sn}(f'_N(]-\infty, x_{i_1}[))\mathbf{sn}(g_{\theta(1)}(x_{i_1})) = 1,$$

pois, ou f_N é crescente (e, portanto, $\lim_{x\to-\infty} f_N = -\infty$) e $f_N(x_{i_1}) > 0$ ou f_N é decrescente (e, portanto, $\lim_{x\to-\infty} f_N = +\infty$) e $f_N(x_{i_1}) < 0$.

Analogamente, existirá uma raiz de f_N no intevalo $]x_{i_M}, +\infty[$ se, e somente se, $\mathbf{sn}(f'_N(]x_{i_M}, \infty[))\mathbf{sn}(g_{\theta(M)}(x_{i_M})) = -1$.

Por fim, para $1 \leq k \leq M-1$, f_N terá uma raiz no intervalo $]x_{i_k}, x_{i_{k+1}}[$ se, e somente se, $\mathbf{sn}(g_{\theta(k)}(x_{i_k}))\mathbf{sn}(g_{\theta(k+1)}(x_{i_{k+1}})) = -1$, pois $f_N(x_{i_k}) = g_{\theta(k)}(x_{i_k})$ e $f_N(x_{i_{k+1}}) = g_{\theta(k+1)}(x_{i_{k+1}})$.

o próximo passo consiste em determinar os sinais dos f_j nos diversos pontos e intervalos.

Sejam $y_1 < \ldots < y_L$, $L \leq Nm$, as raízes de $f_1, \ldots, f_N$. Novamente convencionamos que $y_0 = -\infty$ e $y_{L+1} = +\infty$.

Primeiramente, observemos que $L \geq 1$, pois se nenhum dos polinômios entre $f_1, \ldots, f_{N-1}$ e f'_N não possuísem raízes, isto quer dizer que o sinal de f'_N seria constante e, portanto f_N seria estritamente crescente ou decrescente, o que implica que seus sinais "no infinito"deveriam ser opostos.

Para $j = 1, \ldots, N-1$, $k = 1, \ldots, M$ e $\ell = 1, \ldots, L$, temos:

1. se $y_\ell = x_{i_k}$, $\mathbf{sn}(f_j(y_\ell)) = \mathbf{sn}(f_j(x_{i_k}))$, e se $y_\ell \in]x_{i_k}, x_{i_{k+1}}[$, então $\mathbf{sn}(f_j(y_\ell)) = \mathbf{sn}(f_j(]x_{i_k}, x_{i_{k+1}}[))$;
2. se $y_\ell = x_{i_k}$ ou $y_\ell \in]x_{i_k}, x_{i_{k+1}}[$, então $\mathbf{sn}(f_j(]y_\ell, y_{\ell+1}[)) = \mathbf{sn}(f_j(]x_{i_k}, x_{i_{k+1}}[))$.

Só falta tratar dos sinais de f_N. Voltaremos a usar a função θ definida acima.

Para $k = 1 \ldots, M$ e $\ell = 1, \ldots, L$, temos:

1. se $y_\ell = x_{i_k}$, então $\mathbf{sn}(f_N(y_\ell)) = \mathbf{sn}(g_{\theta(k)}(x_{i_k}))$;
2. se $y_\ell \in]x_{i_k}, x_{i_{k+1}}[$, então $\mathbf{sn}(f_N(y_\ell)) = 0$ (pois, nesse caso, y_ℓ entrou na lista por ser raiz de f_N);
3. se $y_\ell = x_{i_k}$ e $\mathbf{sn}(g_{\theta(k)}) \neq 0$, então $\mathbf{sn}(f_N(]y_\ell, y_{\ell+1}[)) = \mathbf{sn}(g_{\theta(k)})$;
4. se $y_\ell = x_{i_k}$ e $\mathbf{sn}(g_{\theta(k)}) = 0$, então $\mathbf{sn}(f_N(]y_\ell, y_{\ell+1}[)) = \mathbf{sn}(f'_N(]x_{i_k}, x_{i_{k+1}}[))$;
5. se $y_\ell \in]x_{i_k}, x_{i_{k+1}}[$, então $\mathbf{sn}(f_N(]y_\ell, y_{\ell+1}[)) = \mathbf{sn}(f'_N(]x_{i_k}, x_{i_{k+1}}[))$
6. $\mathbf{sn}(f_N(]-\infty, y_1[)) = -\mathbf{sn}(f'_N(]-\infty, x_1[))$.

Com isto, terminamos a demonstração. □

Exemplo 2.2 Vamos fazer o estudo do exemplo anterior, em que $f_1(X) = X^2 - 3X + 2 = (X-1)(X-2)$ e $f_2(X) = X^3 - X = X(X-1)(X+1)$. Daí,

$f_2'(X) = 3X^2 - 1 = 3(X + \sqrt{3}/3)(X - \sqrt{3}/3)$, $g_1(X) = 6X - 6 = 6(X - 1)$ (resto da divisão de f_2 por f_1) e $g_2(X) = (-2/3)X$ (resto da divisão de f_2 por f_2'). Sua matriz de sinais $\mathsf{Sn}_K(f_1, f_2', g_1, g_2)$ é:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & -1 & 0 & 1 \\ 1 & 0 & -1 & -1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}$$

Temos que $x_1 = -\sqrt{3}/3$, $x_2 = 0$, $x_3 = \sqrt{3}/3$, $x_4 = 1$, $x_5 = 2$, $x_6 = +\infty$ e $x_0 = -\infty$. Destas, extraímos $x_{i_1} = x_1$, $x_{i_2} = x_3$, $x_{i_3} = x_4$ e $x_{i_4} = x_5$, que são as raízes de f_1 e f_2'.

A função θ fica assim determinada: $\theta(1) = 2$ (pois x_{i_1} é raiz de f_2'), $\theta(2) = 2$, $\theta(3) = 1$ e $\theta(4) = 1$.

Como $g_1(x_{i_3}) = 0$, sabemos que x_{i_3} é raiz de f_2.

Vamos procurar as outras (possíveis) raízes.

No intervalo $I_0 =]-\infty, x_{i_1}[$, temos que $\theta(1) = 2$, $\mathbf{sn}(g_2(x_{i_1})) = 1$ e $\mathbf{sn}(f_2'(I_1)) = 1$ e, portanto, existe uma raiz y_1 de f_2 em I_1.

No intervalo $I_4 =]x_{i_4}, \infty[$, temos $\theta(4) = 1$, $\mathbf{sn}(g_1(x_{i_4})) = 1$ e $\mathbf{sn}(f_2'(I_4)) = 1$ e, portanto, não há raiz de f_2 em I_4.

No intervalo $I_1 =]x_{i_1}, x_{i_2}[$, temos $\theta(1) = 2$, $\theta(2) = 2$, $\mathbf{sn}(g_2(x_{i_1})) = 1$ e $\mathbf{sn}(g_2(x_{i_2})) = -1$ e, portanto, existe uma raiz y_2 de f_2 em I_1.

No intervalo $I_2 =]x_{i_2}, x_{i_3}[$, temos $\theta(2) = 2$, $\theta(3) = 1$, $\mathbf{sn}(g_2(x_{i_2})) = -1$ e $\mathbf{sn}(g_1(x_{i_3})) = 0$ e, portanto, não há raiz de f_2 em I_2.

No intervalo $I_3 =]x_{i_3}, x_{i_4}[$, temos $\theta(3) = 1$, $\theta(4) = 1$, $\mathbf{sn}(g_1(x_{i_3})) = 0$, $\mathbf{sn}(g_1(x_{i_4})) = 1$ e, portanto, nenhuma raiz de f_2 em I_3.

Sejam y_1 e y_2 as raízes de f_2 acima encontradas, $y_3 = x_4$, $y_4 = x_5$, as raízes de f_1 e f_2.

Precisamos recuperar a informação dos sinais de f_1 e f_2 nos intervalos $J_0 =]-\infty, y_1[$, $J_1 =]y_1, y_2[$, $J_2 =]y_2, y_3[$, $J_3 =]y_3, y_4[$ e $J_4 =]y_4, \infty[$.

Temos que, seguindo o algoritmo descrito no teorema:

1. $\mathbf{sn}(f_1(J_0)) = \mathbf{sn}(f_1(I_0)) = 1$, pois $y_1 \in I_0$;
2. $\mathbf{sn}(f_1(J_1)) = \mathbf{sn}(f_1(I_0)) = 1$;
3. $\mathbf{sn}(f_1(J_2)) = \mathbf{sn}(f_1(I_1)) = 1$, pois $y_2 \in I_1$;
4. $\mathbf{sn}(f_1(J_3)) = \mathbf{sn}(f_1(I_4)) = -1$, pois $J_3 = I_4$ e $y_3 = x_4$;

5. $\mathbf{sn}(f_1(J_4)) = \mathbf{sn}(f_1(I_5)) = 1$, pois $J_4 = I_5$ e $y_4 = x_5$;
6. $\mathbf{sn}(f_2(J_0)) = -\mathbf{sn}(f_2'(I_0)) = -1$, pois $y_1 \in I_0$;
7. $\mathbf{sn}(f_2(J_1)) = \mathbf{sn}(f_2'(I_0)) = 1$;
8. $\mathbf{sn}(f_2(J_2)) = \mathbf{sn}(f_2'(I_1)) = -1$, pois $y_2 \in I_1$;
9. $\mathbf{sn}(f_2(J_3)) = \mathbf{sn}(f_2'(I_1)) = 1$, pois $y_3 = x_{i_3} = x_4$, $\theta(4) = 1$ e $g_1(x_4) = 0$;
10. $\mathbf{sn}(f_2(J_4)) = \mathbf{sn}(g_1(x_5)) = 1$, pois $y_4 = x_{i_4} = x_5$, $\theta(4) = 1$ e $g_1(x_5) \neq 0$. □

Com este algoritmo em mãos, podemos demonstrar o Teorema de Tarski-Seidenberg. Em vista do que foi exposto acima, o teorema pode ser enunciado da seguinte maneira.

Teorema 2.2 Sejam $f_i(X,Y) = a_{i,m_i}(Y)X^{m_i} + \ldots + h_{i,0}(Y) \in \mathbb{Z}[X,Y]$, $1 \leq i \leq N$, $Y = (Y_1, \ldots, Y_n)$, e $m = \max\{m_1, \ldots, m_N\}$. Seja $W' \subset W_{N,m}$ não vazio. Então, existe uma combinação booleana $\mathscr{B}(Y)$ de equações e desigualdades polinomiais em Y, com coeficientes em $\mathbb{Z}$, tal que, para todo corpo real fechado K, e todo $y \in K^n$,

$$\mathsf{Sn}_K(f_1(X,y), \ldots, f_N(X,y)) \in W'$$

se, e somente se, $\mathscr{B}(y)$ for verdadeira em K.

Observação: A equação $\mathsf{Sn}_K(f_1(X,Y), \ldots, f_N(X,Y)) \in W'$ define um conjunto semi-algébrico em K^{n+1}, e a combinação booleana $\mathscr{B}(Y)$ descreve sua projeção em K^n.

Demonstração: Faremos uma indução no grau máximo m e na quantidade de polinômios que atingem esse grau.

Se $m = 0$, nada é preciso fazer, pois, na verdade, teremos a equação $\mathsf{Sn}_K(f_1(Y), \ldots, f_N(Y)) \in W'$, que descreve a combinação booleana desejada.

Suponhamos demonstrado o teorema para graus máximos menores que m, e para grau m, mas com uma quantidade menor de polinômios que atinjam tal grau m.

Aplicando o teorema anterior, supondo que o grau de f_N seja m, obtemos a sequência de polinômios $f_1, \ldots, f_{N-1}, f_N'$ (derivada em relação à variável

$X)$, $g_1, \ldots, g_N \in \mathbb{Z}(Y)[X]$. Multiplicando $g_1, \ldots, g_N$ pelo quadrado dos eventuais denominadores dos coeficientes e juntando a condição de que eles não se anulem, podemos supor que $g_1, \ldots, g_N \in \mathbb{Z}[X, Y]$.

Precisamos, é claro, também fazer a disjunção das várias possibilidades de anulação dos coeficientes (que dependem apenas das variáveis Y), criando outras sequências de polinômios, mas todas elas com a quantidade de polinômios de graus máximos menor do que a da sequência original.

Seja $W'' \subset W_{2N,m}$ o conjunto de todas as matrizes de $W_{2N,m}$ que possam ser levadas a uma matriz de W' pelo algoritmo descrito no teorema anterior.

Com isto, reduzimos o problema a

$$\mathsf{Sn}_K(f_1(X,Y), \ldots, f'_N(X,Y), g_1(X,Y), \ldots, g_N(X,Y)) \in W'',$$

que contém um polinômio a menos que atinge o grau m, ou todos eles tem grau menor que m, caindo na hipótese de indução. □

O algoritmo descrito acima é essencialmente ineficiente. A quantidade de novos polinômios dobra a cada iteração.

Exemplo 2.3 Consideremos, a título de ilustração, a sequência composta por apenas um polinômio de segundo grau $f(X, A, B, C) = AX^2 + BX + C$, e busquemos condições nos coeficientes A, B e C para que valha $f = 0$. Então temos que dividir a solução em uma disjunção de casos:

1. $A = 0$ e tratar a sequência $(BX + C = 0)$;
2. $A \neq 0$, compreendendo os casos $A > 0$ e $A < 0$, tratando do polinômio $(AX^2 + BX + C = 0)$.

O resultado final será algo assim: $\mathscr{B}(A, B, C) \cong$ [($A = 0$ e condições acerca de $(BX + C = 0)$) ou ($A > 0$ e condições sobre $(AX^2 + BX + C = 0)$) ou ($A < 0$ e condições sobre $(AX^2 + BX + C = 0)$)].

Vamos detalhar apenas o caso em que $A > 0$, deixndo os demais casos aos leitores. As matrizes de $W(\varepsilon)$ que cabem neste caso são $[1, 0, 1]$ e $[1, 0, -1, 0, 1]$ (coeficiente de X^2 positivo e com uma ou duas raízes).

Temos que $f'(X, A, B, C) = 2AX + B$, e $g_1(X, A, B, C) = 4A^2C - AB^2$ (que é o resto da divisão de f por f' – ou seja, é $C - 4B^2/A$ – multiplicado pelo quadrado do denominador A).

As matrizes correspondentes para a sequência (f', g_1) são:

$$\begin{bmatrix} -1 & 0 & 1 \\ -1 & -1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Por fim, derivando f', obtemos a sequência $(2A, 4A^2C - AB^2, 0, 0)$ (não dependem mais de X). As matrizes correspondentes são as transpostas de $[1, -1, 0, 0]$, $[1, 0, 0, 0]$ e $[1, 1, 0, 0]$. Descartando as condições triviais (de que $0 = 0$, devido aos dois últimos polinômios nulos), obtemos as condições $A > 0$ e:

1. ou $4A^2C - AB^2 < 0$ (que corresponde a $\Delta = B^2 - 4AC > 0$);

2. ou x

Vamos mostrara que o caso da matriz $[1, 1, 0, 0]$, correspondente a $4A^2C - AB^2 > 0$ (ou $\Delta = B^2 - 4AC < 0$), não ocorre. Vamso ver qual matriz pode ser obtida para f, partindo dessa e da condição $A > 0$:

Para a sequência $(2AX + B, 4A^2C - AB^2)$, obtemos a matriz

$$\begin{bmatrix} -1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Para a sequencia $(AX^2 + BX + C)$ obtemos a matriz $[1]$, ou seja, nenhum zero. □