Tiago Natã Kinhirin Sanson

Bases de Gröbner e algumas aplicações

Florianópolis
22 de julho de 2026

Sumário

1 Introdução **1**

2 Álgebra e Geometria **2**

3 Bases de Gröbner **3**
3.1 Ordem Monomial 3
3.2 Divisão em $k[x_1, \ldots, x_n]$ 4
3.3 Bases de Gröbner 5
3.4 Critério e Algorítmo de Buchberger 7
3.5 Aplicações 8

1 Introdução

O objetivo do presente trabalho é trazer uma introdução a bases de Gröbner de uma forma compreensível e suscinta. Mostrando desde a motivação até algumas aplicações mais complicadas.

2 Álgebra e Geometria

Essa secção serve para mostrar um monte de definições que serão usadas no decorrer do artigo, alguns exemplos também serão apresentados.

Definição 1 *Sejam k um corpo e $p_1, \ldots, p_s \in k[x_1, \ldots, x_n]$ (isto é, $p_1, \ldots, p_s$ são polinômios em $k[x_1, \ldots, x_n]$). Definimos o conjunto*

$$\mathbf{V}(p_1, \ldots, p_s) = \{(a_1, \ldots, a_s) \in k^n : f_j(a_1, \ldots, a_n) = 0,\ \forall j \in \{1, \ldots, s\}\}$$

Como a ***Variedade algébrica*** *definida por $p_1, \ldots, p_s$*

Exemplo 1 *Considere o anel de polinômios $\mathbb{R}[x, y, z]$ e o polinômio $p(x, y, z) = x^2 + y^2 + z^2 - 1$. $V(p(x, y, z))$ será uma esfera em $\mathbb{R}^3$.*

Exemplo 2 *No mesmo anel de polinômios, tome os polinômios $p_1(x, y, z) = x^2 - y^3$, $p_2(x, y, z) = x^2 - z^3$. $V(p_1, p_2)$ será equivalente a intersecção das variedades $V(p_1)$ e $V(p_2)$, que podem ser vistas nas imagens abaixo*

Definição 2 *Sejam k um corpo e $k[x_1, \ldots, x_n]$ um anel de polinômios. Dizemos que $I \subset k[x_1, \ldots, x_n]$ é um* ***Ideal*** *se satizfaz:*

- $0 \in I$
- $f, g \in I \Rightarrow f + g \in I$
- $f \in I, h \in k[x_1, \ldots, x_n] \Rightarrow hf \in I$

Temos as outras definições padrão de ideias, como conjutos geradores de ideais (que serão denotados por $I = \langle i_1, \ldots, i_s \rangle$).

Uma notação que será utilizada quando necessário será a seguinte para polinômios:

$$p(x) = \sum_{\alpha} a_\alpha x^\alpha,\ a \in k$$

em que α é uma n-upla, ou seja, um monomio desse polinômio será da forma

$$a_\alpha x_1^{\alpha(1)} \ldots x_n^{\alpha(n)}$$

3 Bases de Gröbner

As bases de Gröbner são uma ferramenta muito forte para a solução de três tipos de problemas:

1. A aderência em Ideais: dados $f \in k[x_1, \ldots, x_n]$ e um ideal $I = \langle p_1, \ldots, p_s \rangle$. A pergunta é: $f \in I$?

2. Solução de equações polinomiais: Encontrar todas as soluções em k^n para o sistema

$$\begin{cases} p_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ p_s(x_1, \ldots, x_n) = 0 \end{cases}$$

3. Implicitação de uma variedade: Seja $V \subseteq k^n$ dada de forma paramétrica por

$$\begin{cases} x_1 = g_1(t_1, \ldots, t_m) \\ \vdots \\ x_n = g_n(t_1, \ldots, t_m) \end{cases}$$

   Então, se os g_i são polinômios (ou funções racionais) para todo i em $\{1, \ldots, n\}$, então ou V será uma variedade ou parte de uma. o problema é: Achar o sistema que define essa variedade

Vamos analisar no fim deste artigo os dois primeiros.

Para todos estes, precisamos construir as bases propriamente ditas e, também, resolver um problema especial: todo ideal tem base finita? Veremos que sim.

3.1 Ordem Monomial

Nossa ideia é generalizar o algorítmo da divisão em $\mathbb{Z}$ para polinômios em k, para tanto, precisamos naturalmente de uma ordem.

Em polinômios de uma variável só, temos uma ordem natural, que seria analisar os expoentes e ver qual expoente é maior. Nesse mesmo espírito, define-se:

Definição 3 *Uma relação $>$ em $\mathbb{Z}^n_{\geq 0}$ é dita uma **ordem monomial** se valem*

- *$>$ é de ordem total em $\mathbb{Z}^n_{\geq 0}$*
- *Sejam $a, b \in \mathbb{Z}^n_{\geq 0}$, se $a > b$ e $c \in \mathbb{Z}^n_{\geq 0}$, $a + c > b + c$*
- *$>$ é bem ordenada*

Agora, para organizarmos a "força"de cada variável, introduziremos a ordem lexicográfica (que, daqui em diante, chamaremos de **lex**)

Definição 4 *Seja $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_n)$. diremos que $a >_{lex} b$ se o termo não nulo mais da esquerda do vetor $(a - b)$ for maior que zero*

Exemplo 3 *Seja* $a = (5, 2, 3)$ *e* $b(3, 1, 4)$. *Temos que* $a - b = (2, 1, -1)$, *logo* $a >_{lex} b$

Exemplo 4 *Podemos ver as variáveis* $x_1 \dots x_n$ *sendo escritas como n-uplas tal que* $x_i = (0, \dots, 0, \underbrace{1}_{i\text{-ésimo termo}}, 0, \dots, 0)$ *e, aplicando a ordem lexicográfica,*

$$(1, 0, \dots, 0) >_{lex} (0, 1, 0, \dots) >_{lex} > \dots$$

em outras palavras,

$$x_i >_{lex} x_j \iff i > j$$

A ordem lexicográfica é um exemplo de ordem monomial. Um outro exemplo interessante de ordem monomial é a ordem lexicográfica graduada

Definição 5 *Sejam* $a, b \in \mathbb{Z}^n_{\geq 0}$, *dizemos que* $a > b$ *se a soma dos termos de a for maior que a soma dos termos em b ou, caso sejam igual,* $a >_{lex} b$

Definição 6 *Sejam* $p(X) = \sum_\alpha a_\alpha x^\alpha$, $X = [x_1, \dots, x_n]$ *um polinômio em* $k[x_1, \dots, x_n]$ *e* $>$ *uma ordem monomial. Dizemos que:*

1. *O* ***grau máximo*** *de* p *é*

$$multideg(p) = \max\{\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0\}$$

2. *O* ***coeficiente lider*** *de* p *é*

$$LC(p) = a_m ultideg(p)$$

3. *O monômiolider de* p *é*

$$LM(p) = x^{multideg(p)}$$

4. *O* ***termo lider*** *de* p *é*

$$LT(p) = LC(p)LM(p)$$

3.2 Divisão em $k[x_1, \dots, x_n]$

Com toda essa carga, podemos finalmente analisar o algorítmo da divisão em $k[x_1, \dots, x_n]$.

Teorema 1 *Sejam* $>$ *uma ordem monomial em* $\mathbb{Z}^n_{\geq 0}$ *e* $F = (f_1, \dots, f_s)$ *uma s-upla ordenada de polinômios em* $k[x_1, \dots, x_n]$. *Então, todo* $f \in k[x_1, \dots, x_n]$ *pode ser escrito como*

$$f = \sum_{j=1}^{s} f_j q_j + r$$

Em que $q_j, r \in k[x_1, \dots, x_n]$, $r = 0$ *ou* r *é uma combinação linear de monômios em* $k[x_1, \dots, x_n]$ *tal que nenhum deles pode ser divisível pelos* $LT(f_j)$, $\forall j \in \{1, \dots, s\}$. r *é chamado o* ***resto*** *de* f *pela divisão por* F. *Além disso, se* $q_j f_j \neq 0$, $multideg(f) \geq multideg(q_j f_j)$

A demonstração envolve a construção de um algorítmo muito similar ao algorítmo da divisão em $\mathbb{Z}$.

3.3 Bases de Gröbner

Agora podemos começar a traçar nossso caminho para as bases de Gröbner e resolver nosso problema de todo ideal ser finitamente gerado. Vejamos uma nova definição sobre ideais:

Definição 7 *Seja $I \subset k[x_1, \ldots, x_n]$ um ideal não nulo e $>$ uma ordem monomial. Então:*

1. *Definimos $LT(I)$ como os termos lideres de todos os $f \in I\backslash\{0\}$, isto é*

$$LT(I) := \bigcup_{f \in I\backslash\{0\}} LT(f)$$

2. *$\langle LT(I)\rangle$ é o ideal gerado pelos termos de $LT(I)$*

Uma coisa a se notar é que, se $I = \langle p_1, \ldots, p_s\rangle$, não necessariamente $\langle LT(I)\rangle = \langle LT(p_1), \ldots, LT(p_s)\rangle$, de fato

Exemplo 5 *Seja $I = \langle p_1, p_2\rangle \subset \mathbb{R}[x, y, z]$ com $p_1 = x + y$, $p_2 = x - z$, temos que $\langle LT(p_1), LT(p_2)\rangle = \langle x, x\rangle = \langle x\rangle$, mas $y \in LT(I)$, de fato*

$$y + z = (x + y) - (x - z)$$

Teorema 2 *Seja $I \subset k[x_1, \ldots, x_n]$ um ideal não nulo. Então*

1. *$\langle LT(I)\rangle$ é um ideal monomial, isto é, existe um subconjunto $A \subset Z^n_{\geq 0}$ (que pode ser infinito) tal que todos os elementos de I podem ser escrito como*

$$\sum_{\alpha \in A} h_\alpha x^\alpha,\ h \in k[x_1, \ldots, x_n]$$

   Neste caso, escrevemos $I = \langle x^\alpha : \alpha \in A\rangle$

2. *Existem $g_1, \ldots, g_t \in I$ tal que $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$*

Demonstração:

1. Tome os monomios lideres $LM(g), g \in I\backslash\{0\}$. Estes geram o ideal monomial $\langle LM(g) : g \in I\backslash\{0\}\rangle$ que por sua vez é igual a $\langle LT(g) : g \in I\backslash\{0\}\rangle$, pois diferem por um coeficiente não nulo e, temos que $\langle LT(g) : g \in I\backslash\{0\}\rangle = \langle LT(I)\rangle$ (pois $\langle LT(g) : g \in I\backslash\{0\}\rangle$ contém todos os termos lideres de ideais não nulos, que é exatamente o gerado pelo $LT(I)$.

2. Para provar este item, precisamos de um lema auxiliar

   Lema 1 (De Dickson) *Seja $I \subset k[x_1, \ldots, x_n]$ um ideal monomial. Então I pode ser escrito como $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s}\rangle$ com $\alpha_1, \ldots, \alpha_s \in A$*

   Demonstração (do lema:) ver em [O'Shea 2015], página 72 teorema 5. ■

   Como $LT(I)$ é gerado pelos monomiais $LM(g)$ com $g \in I\backslash\{0\}$, pelo lema de Dickson, $\langle LT(I)\rangle = \langle LM(g_1), \ldots, LM(g_t)\rangle$, com $g_1, \ldots, g_t \in I$ uma quantidade finita. Como $LM(g_j)$ difere de $LT(g_j)$ por uma constante diferente de 0, $LM(g_j) = LT(g_j),\ \forall j \in \{1, \ldots, t\}$, logo, $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$

com isso, podemos finalmente resolver o problema das bases finitas de ideais em um anel de polinômios e, definir a base de Gröbner.

Teorema 3 *(da base de Hilbert)*
Todo ideal $I \subset k[x_1, \ldots, x_n]$ possui gerador finito.

Demonstração: Se $I = \{0\}$, tome o gerador como $\langle 0 \rangle$. Suponha I não nulo.

Escolha uma ordem monomial, então I possuí um ideal de termos lideres $\langle LT(I) \rangle$, pelo Teorema 2, temos que $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle$. Afirmamos que $\langle g_1, \ldots, g_s \rangle = I$.

De fato, tome $f \in I$, vejamos que o resto de f por $g_1, \ldots, g_s$ é zero. temos, pelo algorítmo da divisão que

$$f = \sum_{j=1}^{s} q_j g_j + r, \ q_j \in k[x_1, \ldots, x_n]$$

Suponha que $r \neq 0$, então temos que

$$r = f - \sum_{j=1}^{s} q_j g_j \in I$$

Como r é diferente de zero, $LT(r) \in \langle LT(I) \rangle$ então, $LT(r)$ deve ser divisível por $LT(g_j)$ para algum $j \in \{1, \ldots, s\}$. Absurdo!

Logo, $r = 0$, o que implica que

$$f = \sum_{j=1}^{s} q_j g_j + 0 \in \langle g_1, \ldots, g_s \rangle$$

O que nos dá que $I \subset \langle g_1, \ldots, g_s \rangle$, finalizando a prova

■

Com isso, definimos uma base especial

Definição 8 *Fixe uma ordem monomial em um anel de polinômios $k[x_1, \ldots, x_n]$, um subconjunto finito $G = \{g_1, \ldots, g_s\}$ de um ideal $I \subset k[x_1, \ldots, x_n]$ diferente de zero é dita uma* ***base de Gröbner*** *se*

$$\langle LT(g_1), \ldots, LT(g_s) \rangle = \langle LT(I) \rangle$$

Da definição, não é claro que a base de Gröbner é uma base de Hilbert, mas de fato ela é e, mais ainda, todo ideal possui base de Gröbner, analisemos isso na proposição a seguir.

Corolário 1 *Todo ideal $I \subset k[x_1, \ldots, x_n]$ possui base de Gröbner, toda base de Gröbner é base de Hilbert*

Demonstração A demonstração é direta das construções do teorema 3.

Exemplo 6 *Em geral, não é verdade que uma base de Hilbert é uma base de Gröbner, com efeito, tome o ideal* $I = \langle z^2 + yx, y^2 - xz \rangle \subset \mathbb{R}[x, y, z]$. *Com a ordem lexicográfica* $x > y > z$, *o conjunto gerador não é uma base de Gröbner (mas claramente é base de Hilbert). De fato,* $\langle LT(z^2 + yx), LT(y^2 - xz) \rangle = \langle xy, xz \rangle$ *mas, conseguimos construir o seguinte polinômio com o ideal:*

$$y^3 + z^3 = (z^2 + yx)z + (y^2 - xz)y$$

que tem termo lider y^3, *que não está em* $\langle LT(z^2 + yx), LT(y^2 - xz) \rangle$, *mas está em* $\langle LT(I) \rangle$

3.4 Critério e Algorítmo de Buchberger

Depois de tudo isso, podemos analisar mais a fundo dois resultados importantíssimos para o cálculo de bases de Gröbner

Definição 9 *Sejam* $p, q \in k[x_1, \ldots, x_n]$ *dois polinômios não nulos e* $\alpha = multideg(p)$ $\beta = multideg(q)$. *O* ***Minimo multiplo comum*** *de* p *e* q *é dado por* $\gamma = (max(\alpha_j, \beta_j)_{j=1}^n)$

Definição 10 *O* ***Polinomio-S*** *associado a dois outros polinômios* p *e* q *é dado por*

$$S(p, q) = \frac{x^{mmc(p,q)}}{LT(p)}p - \frac{x^{mmc(p,q)}}{LT(q)}q$$

O polinômio-S é fundamental para a construção das bases de Gröbner - de fato, é o que tanto calcula quando verifica o que é uma base de Gröbner.

Teorema 4 (Critério de Buchberger) *Fixe uma ordem monomial e seja* I *um ideal polinomial. Então um conjunto* $G = \{g_1, \ldots, g_s\}$ *é dita uma base de Gröbner se, e somente se, o resto da divisão de todos os polinômios* $S(g_i, g_j)$ *por* G *é igual a zero.*

A demonstração desse teorema pode ser encontrada em [O'Shea 2015] Capitulo 2, §6, teorema 6

Aplicações sucessivas do critério de Buchberger em uma base de um ideal (ou até mesmo no gerador do ideal) e, colocando os polinomios-S que falham na nossa base, criam uma base de Gröbner: vamos formalizar isso.

Teorema 5 (Algoritmo de Buchberger) *Sejam* I *um ideal e* $F = \{p_1, \ldots, p_n\} \subset I$ *uma base de* I, *então, podemos construir uma base de Gröbner aplicando os seguintes passos:*

1. *Tome um par* $\{p_i, p_j\} \in F, i \neq j$.
2. *Calcule* $S(p_i, p_j)$ *e divida por* F
3. *se o resto for zero, faça para outros* i, j *até exaustar todos.*
4. *se o resto não for zero, adiciona* $S(p_i, p_J)$ *na lista e calcule os outros Polinomios-S, até que todas as divisões de* $S(p_i, p_j)$ *por* F *sejam zero.*

novamente, a demonstração pode ser encontrada em [O'Shea 2015] Capitulo 2, §7, teorema 2.

Existe ainda uma forma de "enxugar"as bases de Gröbner, às vezes, temos termo que são desnecessários. Usemos a notação $\langle LT(G)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle$*, para* $\{g_1, \ldots, g_s\} \subset G$

Lema 2 *Seja* I *um ideal polinomial e* G *uma base de Gröbner de* I*. Seja* $p \in G$ *um polinômio tal que* $LT(p) \in \langle LT(G\ \{p\}\rangle$*, então* $G\ \{p\}$ *é uma base de Gröbner*

Demonstração Sabemos que $\langle LT(G)\rangle = \langle LT(I)\rangle$. Se $LT(p) \in \langle LT(G\backslash\{p\})\rangle$, temos que $\langle LT(G)\rangle = \langle LT(G\backslash\{p\})\rangle$. Pela definição, $\langle LT(G\backslash\{p\})\rangle$ é uma base de Gröbner

Com isso, podemos definir

Definição 11 *Uma* ***Base de Gröbner reduzida*** *para um ideal polinomial* I *é uma base de Gröbner* G *tal que*

- $LC(p) = 1,\ \forall p \in G$
- $\forall p \in G, p \notin \langle LT(G\backslash\{p\})\rangle$

Observação: Essa base é única

3.5 Aplicações

Sem mais delongas e definições e tudo mais, podemos agora falar finalmente sobre as aplicações. Em especial os dois problemas citados no início da secção. Começando pelo

A Aderência em Ideais

Com as bases de Gröbner, tudo fica mais fácil: com efeito, para um ideal I, basta encontrar uma base de Gröbner G e para verificar que uma função f está em I, divida f por G e analise o resto, se o resto for 0, $f \in I$

Exemplo 7 *Considere o ideal* $I = \langle xy - 1, y^2 - x\rangle \in \mathbb{Q}[x, y]$ *com a ordem lexicográfica* $x > y$ *vejamos se* $f(x, y) = x^3 - 1$ *está em* I

Calculando a base de Gröbner, teremos $G = \{y^3 - 1, x - y^2\}$*, fazendo o algorítmo da divisão de* f *por* G*, teremos:*

$$f(x, y) = (x^2 + xy^4 + y^4)(x - y^2) + (y^3 + 1)(y^3 - 1) + 0$$

Como o resto deu 0, $f \in I$

Solução de equações polinomiais

A ideia é, em geral, notar que as bases de Gröbner são uma combinação linear das equações, vejamos um exemplo

Exemplo 8 *Considere o sistema em* $\mathbb{C}[x, y, z]$ *e a ordem monomial* $x > y > z$

$$\begin{cases} xy - z & = 0 \\ x^2 - y + 1 & = 0 \\ y^2 - x & = 0 \end{cases} \tag{1}$$

Resolver essas equações é o mesmo que achar o lugar dos zeros do ideal $I = \langle xy - z, x^2 - y + 1, y^2 - x$ *analisemos sua base de Gröbner e vejamos como simplifica a questão.*

A base de Gröbner

$$G := \{1 - z + 3z^2 - 3z^3 + z^4, y - z + 2z^2 - z^3, x - z + z^2\}$$

Achar os zeros da base de Gröbner é o mesmo que achar os zeros do ideal, logo, resolver o sistema

$$\begin{cases} 1 - z + 3z^2 - 3z^3 + z^4 & = 0 \\ y - z + 2z^2 - z^3 & = 0 \\ x - z + z^2 & = 0 \end{cases} \tag{2}$$

é o mesmo que resolver o sistema em (1). É bem notável que (2) é mais facil de resolver, pois basta resolver a primeira linha, que são os zeros de um polinômio em uma variável. Resolvendo, ficamos com as soluções (aproximadas e não tão elegantes):

$$\begin{cases} z_1 = -0.01891 - (0.60257)i \\ z_2 = 0.01891 + (0.60257)i \\ {}_3 = 1.5189 - (0.6666)i \\ z_4 = 1.5189 + (0.6666)i \end{cases} \tag{3}$$

Então, basta substituir nas equações e teremos os resultados para a equação (2) e, também da (1)

Referências

[O'Shea 2015]O'SHEA, D. A. C. L. *Ideals, Varieties, and Algorithms An Introduction to Computational Algebraic Geometry and Commutative Algebra*. [S.l.]: Springer, 2015.