Universidade Técnica de Lisboa

Instituto Superior Técnico

Departamento de Matemática

Bases de Gröbner e Aplicações

Filipe Casal

Projecto em Matemática

Licenciatura em Matemática Aplicada e Computação

Orientadora:

Prof[a]. Margarida Mendes Lopes

Dezembro de 2010

Conteúdo

Capítulo 1

Introdução

Este trabalho foi realizado no âmbito da cadeira de Projecto em Matemática e aborda tópicos de geometria algébrica computacional e da álgebra comutativa. Está escrito não com o intuito de ser uma abordagem profunda ao assunto mas como texto introdutório e motivador do que é possível fazer com algumas ferramentas da geometria algébrica, em particular as Bases de Gröbner.

A resolução de sistemas de equações lineares é feita através de um conhecido algoritmo, a eliminação de Gauss. Já a resolução de sistemas de equações polinomiais é um problema bastante mais complexo, normalmente resolvido com recurso a métodos numéricos, uma vez que nem existem fórmulas explícitas para equações de $5^{\underline{o}}$ ou maior grau numa variável. No entanto, em meados do século xx, Buchberger desenvolveu a teoria das bases de Gröbner que pode ser vista como uma generalização da eliminação de Gauss para sistemas lineares ou do máximo divisor comum para polinómios numa só variável. Acontece que esta poderosa ferramenta permite atacar problemas como a resolução de sistemas de equações polinomiais, obtenção de fórmulas explícitas de superfícies a partir de parametrizações, determinar a pertença de polinómios a ideais, a igualdade entre ideais, ou ainda aplicações à teoria de grafos, apenas para referir alguns.

O texto está estruturado da seguinte forma:

- o segundo capítulo introduz o leitor às bases de Gröbner, e mostra como estas resolvem algumas questões em geometria e álgebra;
- no terceiro capítulo é feita uma análise das propriedades das bases de Gröbner que permitem resolver sistemas de equações polinomiais;
- no quarto capítulo falaremos de aplicações das bases de Gröbner à álgebra, teoria de grafos e robótica;
- o quinto capítulo contém algoritmos que implementámos no sistema *Mathematica* para o cálculo de bases de Gröbner;
- finalmente no sexto capítulo faremos um resumo dos resultados obtidos, falaremos do potencial que as bases de Gröbner têm para resolver os mais diversos problemas e apresentaremos alguns temas que podem ser aprofundados após a introdução às bases de Gröbner que é feita aqui.

Capítulo 2

Bases de Gröbner

2.1 Preliminares

Seja $k[x_1, \ldots, x_n]$ o anel de polinómios a n variáveis sobre um corpo k e $k^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in k\}$ o espaço afim de dimensão n sobre k. Um polinómio f em $k[x_1, \ldots, x_n]$ é da forma $f = \sum_\alpha a_\alpha x^\alpha$, e também pode ser visto como a função $f : k^n \to k$, que faz corresponder a um elemento do espaço afim um elemento de k. Caso k seja finito, a dualidade polinómio/função pode dar origem a confusões.

Exemplo 1. *Considere-se $f = x(x-1)(x-2) \in \mathbb{F}_3[x]$. Verifica-se que $f(z) = 0, \forall z \in \mathbb{F}_3$ e no entanto $f \neq 0$.*

Dado um corpo k e polinómios $f_1, \ldots, f_s$ em $k[x_1, \ldots, x_n]$ define-se por $\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n : f_i(a_1, \ldots, a_n) = 0, 1 \leq i \leq s\}$ como a *variedade afim* definida por $f_1, \ldots, f_s$. A variedade afim definida por $f_1, \ldots, f_s$ é portanto o conjunto dos zeros que os polinómios $f_1, \ldots, f_s$ têm em comum.

Exemplo 2. *Dá-se a $\boldsymbol{V}(y - x^2, z - x^3) \subset \mathbb{R}^3$ o nome de cúbica torcida. Esta variedade pode ser vista como a imagem da aplicação $c : \mathbb{A}^1 \to \mathbb{A}^3$ definida por $t \longmapsto (t, t^2, t^3)$. Tem como superfície tangente $c(t) + uc'(t) = (t, t^2, t^3) + u(1, 2t, 3t^2) = (t + u, t^2 + 2tu, t^3 + 3t^2u)$. Mais à frente veremos como desta parametrização podemos deduzir a equação que define a superfície tangente da cúbica torcida apenas em termos de x, y, z.*

Dadas V e W, duas variedades afins, podemos construir $V \cap W$ e $V \cup W$ que são ainda variedades. Estas são dadas pelas fórmulas

$$V \cap W = \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t), V \cup W = \mathbf{V}(f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t)$$

No estudo da álgebra comutativa as estruturas que mais interessam analisar são os ideais que podemos definir da seguinte maneira:

Um subconjunto $I \subset k[x_1, \ldots, x_n]$ diz-se um *ideal* se:

i. $0 \in I$;

ii. se $f, g \in I$ então $f + g \in I$;

iii. se $f \in I$ e $h \in k[x_1, \ldots, x_n]$, então $hf \in I$.

Define-se o *ideal gerado* por $f_1, \ldots, f_s$ como

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \right\}.$$

Introduzimos também a definição de *ideal de uma variedade* – dada uma variedade afim $V \subset k^n$, o seu ideal é $\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0, \text{ para todo o } (a_1, \ldots, a_n) \in V\}$. O ideal da variedade é portanto o conjunto de todos os polinómios que se anulam nos pontos de V.

Exemplo 3. *Voltando ao Exemplo 2, seja* $V = \boldsymbol{V}(y - x^2, z - x^3)$. *Vejamos que* $\boldsymbol{I}(V) = \langle y - x^2, z - x^3 \rangle$. *Mostramos primeiro que dado um* $f \in \mathbb{R}[x, y, z]$ *este pode ser escrito na forma* $f = h_1(y - x^2) + h_2(z - x^3) + r$, *onde* $h_1, h_2 \in \mathbb{R}[x, y, z]$ *e* $r \in \mathbb{R}[x]$. *Caso f seja um monómio,*$x^\alpha y^\beta z^\gamma$ *temos que*

$$\begin{aligned} x^\alpha y^\beta z^\gamma &= x^\alpha (x^2 + (y - x^2))^\beta (x^3 + (z - x^3))^\gamma \\ &= x^\alpha (x^{2\beta} + \textit{ termos em } y - x^2)(x^{3\gamma} + \textit{ termos em } z - x^3) \\ &= h_1(y - x^2) + h_2(z - x^3) + x^{\alpha + 2\beta + 3\gamma} \end{aligned}$$

Caso f seja um polinómio, é portanto uma combinação de monómios, e logo terá uma decomposição semelhante à que vimos. Vejamos então que $\boldsymbol{I}(V) = \langle y - x^2, z - x^3 \rangle$. *Tem-se que* $y - x^2, z - x^3 \in \boldsymbol{I}(V)$ *pela definição de cúbica torcida. Dado que* $\boldsymbol{I}(V)$ *é um ideal,* $h_1(y - x^2) + h_2(z - x^3) \in \boldsymbol{I}(V)$ *e logo* $\langle y - x^2, z - x^3 \rangle \subset \boldsymbol{I}(V)$. *Para a outra inclusão, seja* $f \in \boldsymbol{I}(V)$ *e tome-se a decomposição anterior* $f = h_1(y - x^2) + h_2(z - x^3) + r$. *Usando a parametrização da cúbica, dado que f é zero em V temos que*

$$0 = f(t, t^2, t^3) = h_1 \cdot 0 + h_2 \cdot 0 + r(t)$$

e logo r é o polinómio nulo, pelo que f é da forma $h_1(y - x^2) + h_2(z - x^3)$ *e portanto* $\boldsymbol{I}(V) = \langle y - x^2, z - x^3 \rangle$.

Esta noção ilustrada no exemplo é muito importante: dados polinómios $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ podemos construir

$$\begin{array}{ccccc} \textit{polinómios} & \rightsquigarrow & \textit{variedade} & \rightsquigarrow & \textit{ideal} \\ f_1, \ldots, f_s & \hookrightarrow & \mathbf{V}(f_1, \ldots, f_s) & \hookrightarrow & \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)) \end{array}$$

e perguntarmo-nos quando é que $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)) = \langle f_1, \ldots, f_s \rangle$? Ou pelo menos, qual a sua relação? Podemos assim colocar certas questões que gostaríamos de ver respondidas:

- Dado um ideal $I \subset k[x_1, \ldots, x_n]$ podemos escrevê-lo como $\langle f_1, \ldots, f_s \rangle$ para alguns $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$? Ou seja, é I finitamente gerado?
- Dados $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ existe algum algoritmo que decida se um dado $f \in k[x_1, \ldots, x_n]$ está em $\langle f_1, \ldots, f_s \rangle$?
- Dados conjuntos de polinómios $\{f_1, \ldots, f_s\}$ e $\{g_1, \ldots, g_t\}$ podemos decidir se $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$?
- Dados $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, qual a relação exacta entre $\langle f_1, \ldots, f_s \rangle$ e $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$?

2.2 Relações de ordem em $k[x_1, \ldots, x_n]$

Chamamos a um elemento de $\mathbb{T}^n = \{x_1^{\beta_1} \ldots x_n^{\beta_n} : \beta_i \in \mathbb{N} \text{ para todo o } i = 1, \ldots, n\}$ um monómio. Dado um monómio em $k[x_1, \ldots, x_n]$, $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, podemos fazê-lo corresponder unicamente a um n-tuplo em $\mathbb{N}^n$, $\alpha = (\alpha_1, \ldots, \alpha_n)$. Assim, podemos estabelecer relações de ordem para monómios em $k[x_1, \ldots, x_n]$ usando relações de ordem em $\mathbb{N}^n$ para n-tuplos, onde $x^\alpha > x^\beta$ sse $\alpha > \beta$. Vamos impor três condições nestas relações de ordem: que sejam totais, ou seja, que dados quaisquer dois elementos α e $\beta \in \mathbb{N}^n$ se tem que $\alpha > \beta$ ou $\beta > \alpha$ ou $\alpha = \beta$; que dados $\alpha, \beta, \gamma \in \mathbb{N}^n$ com $\alpha > \beta$, então $\alpha + \gamma > \beta + \gamma$; além disso é necessário que $>$ seja uma boa ordenação de $\mathbb{N}^n$, ou seja, que todo o subconjunto não vazio de $\mathbb{N}^n$ tenha elemento mínimo para a relação $>$.

Dado $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ dizemos que o *grau total do monómio* definido por α é $|\alpha| = \sum_{i=1}^n \alpha_i$. Considerem-se então dois monómios $\alpha = (\alpha_1, \ldots, \alpha_n)$ e $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. Três das possíveis relações de ordem são definidas por:

- **Ordem lexicográfica** - $\alpha >_{lex} \beta$ se em $\alpha - \beta$ a entrada mais à esquerda não nula é positiva.
- **Ordem por graus lexicográfica** - $\alpha >_{grlex} \beta$ se $|\alpha| > |\beta|$ ou se $|\alpha| = |\beta|$ então $\alpha >_{lex} \beta$.
- **Ordem inversa por graus lexicográfica** - $\alpha >_{grevlex} \beta$ se $|\alpha| > |\beta|$ ou se $|\alpha| = |\beta|$ se tem que em $\alpha - \beta$ a entrada mais à direita não nula é negativa.

Dados $f = \sum_\alpha a_\alpha x^\alpha$ e $>$ uma relação de ordem para monómios, temos ainda de definir:

- **Multigrau** - $\text{multideg}(f) = \max(\alpha \in \mathbb{N}^n : a_\alpha \neq 0)$;
- **Coeficiente máximo** - $\text{LC}(f) = a_{\text{multideg}(f)} \in k$;
- **Monómio máximo** - $\text{LM}(f) = x^{\text{multideg}(f)}$;
- **Termo máximo** - $\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f)$.

Exemplo 4. *Considere-se o polinómio em* $\mathbb{R}[x, y, z]$, $f = x^3 + xy^4z^2 + y^6z$. *Tem-se que, ordenando do maior termo para o menor,*

$$f = x^3 + xy^4z^2 + y^6z, \text{ na ordem } lex$$
$$f = xy^4z^2 + y^6z + x^3, \text{ na ordem } grlex$$
$$f = y^6z + xy^4z^2 + x^3, \text{ na ordem } grevlex$$

2.3 Algoritmo de divisão em $k[x_1, \ldots, x_n]$

O algoritmo apresentado nesta secção vai ser usado para tentarmos decidir se um dado polinómio $f \in k[x_1, \ldots, x_n]$ está num ideal $I = \langle f_1, \ldots, f_s \rangle$. Se considerarmos o anel dos polinómios a uma variável, $k[x]$, uma vez que é um domínio de ideais principais (ver [2]), qualquer ideal $\langle f_1, \ldots, f_s \rangle$ é da forma $\langle m \rangle$. Além disto sabemos também que este polinómio m que gera $\langle f_1, \ldots, f_s \rangle$ é $\text{mdc}(f_1, \ldots, f_s)$, o máximo divisor comum dos polinómios $f_1, \ldots, f_s$. Após encontrarmos o máximo divisor comum dos polinómios do ideal, para o algoritmo decidir se $f \in \langle f_1, \ldots, f_s \rangle = \langle \text{mdc}(f_1, \ldots, f_s) \rangle = \langle m \rangle$ divide f por m e obtemos uma decomposição da forma $f = m \cdot q + r$. Caso r seja o polinómio nulo obtemos que $f \in \langle f_1, \ldots, f_s \rangle$; caso $r \neq 0$ temos que o polinómio f não pertence ao ideal. O que queremos obter agora é um algoritmo que resolva

este problema em $k[x_1, \ldots, x_n]$. Até nota em contrário, assumimos estar a trabalhar com uma qualquer relação de ordem fixa.

Teorema 1. *Seja $F = (f_1, \ldots, f_s)$ um s-tuplo de polinómios em $k[x_1, \ldots, x_n]$. Então todo o polinómio $f \in k[x_1, \ldots, x_n]$ pode ser escrito na forma*

$$f = a_1 f_1 + \ldots + a_s f_s + r$$

onde $a_i, r \in k[x_1, \ldots, x_n]$ e, ou $r = 0$ ou r é uma combinação linear, com coeficientes em k , de monómios, nenhum dos quais divisíveis por $LT(f_1), \ldots, LT(f_s)$.

O seguinte algoritmo – que recebe como argumentos o polinómio dividendo f e os polinómios divisores $f_1, \ldots, f_s$, e devolve os quocientes $a_1, \ldots, a_s$ e o resto da divisão r – calcula esta divisão:

Algoritmo 1 Divisão em $k[x_1, \ldots, x_n]$

```
a_1 = 0, ..., a_s = 0
r = 0
p = f
while p ≠ 0 do
  i = 1
  divoc = false
  while i ≤ s ∧ divoc = false do
    if LT(f_i) divide LT(p) then
      a_i = a_i + LT(p)/LT(f_i)
      p = p − (LT(p)/LT(f_i)) · f_i
      divoc = true
    else
      i = i + 1
    end if
  end while
  if divoc = false then
    r = r + LT(p)
    p = p − LT(p)
  end if
end while
```

O problema aparenta estar resolvido com este algoritmo de divisão mas acontece que $k[x_1, \ldots, x_n]$ não é domínio de ideais principais, pelo que não sabemos como, dado um dado ideal, encontrar um único gerador do ideal e aplicar o mesmo raciocínio utilizado em $k[x]$ – ou pelo menos encontrar um conjunto finito de geradores desse mesmo ideal onde aplicar o algoritmo de divisão que acabámos de ver. Além disso, pode dar-se o caso em que o resto da divisão não é zero e o polinómio pertence ao ideal, ou seja, dado um qualquer conjunto de geradores do ideal, a condição de que o resto da divisão é nulo é apenas condição suficiente para a pertença ao ideal. No entanto, para um certo tipo de bases esta equivalência verifica-se e serão essas bases que queremos encontrar.

Exemplo 5. *Sejam $f_1 = xy + 1$ e $f_2 = y^2 - 1 \in k[x, y]$ com a ordem lexicográfica. Dividindo $f = xy^2 - x$ por $F = (f_1, f_2)$ obtém-se*

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y)$$

enquanto que se dividirmos por $F' = (f_2, f_1)$ *obtemos*

$$xy^2 - x = 0 \cdot (xy + 1) + x \cdot (y^2 - 1) + 0.$$

A primeira divisão mostra que mesmo estando f *em* $\langle f_1, f_2 \rangle$ *é possível obtermos* $r \neq 0$ *na divisão.*

Seguimos então à procura das bases com "boas" propriedades para depois aplicarmos o algoritmo de divisão. Como vimos, queremos que a condição $r = 0$ seja equivalente à pertença do polinómio ao ideal. Às bases com esta propriedade damos o nome de *Bases de Gröbner* e serão o nosso objecto de estudo principal. Para obtermos as Bases de Gröbner necessitamos primeiro do *Teorema da Base de Hilbert*, um famoso teorema da álgebra cuja demonstração é tradicionalmente feita por *reductio ad absurdum*. Apresentamos outro caminho para este teorema de modo a obtermos uma versão construtiva do mesmo, e assim prosseguirmos na busca de um algoritmo que construa as bases de Gröbner. Para isto precisamos ainda de introduzir a noção de ideal de monómios e o Lema de Dickson.

Um ideal $I \subset k[x_1, \ldots, x_n]$ diz-se um *ideal de monómios* se os seus geradores, possivelmente infinitos, forem monómios. Escrevemos que $I = \langle x^\alpha : \alpha \in A \rangle$, onde $A \subset \mathbb{N}^n$ é possivelmente infinito.

Lema 1. *Seja* $I = \langle x^\alpha : \alpha \in A \rangle$ *um ideal de monómios. Então* x^β *está no ideal sse* x^β *é divisível por* x^α *para algum* $\alpha \in A$ *sse todas as entradas de* $\beta - \alpha$ *são maiores ou iguais a zero.*

de onde se obtém,

Lema 2 (Dickson, [1])**.** *Um ideal de monómios* $I = \langle x^\alpha : \alpha \in A \rangle \subset k[x_1, \ldots, x_n]$ *pode ser escrito na forma* $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$ *onde* $\alpha(1), \ldots, \alpha(s) \in A$*. Isto é,* I *é finitamente gerado.*

O Lema de Dickson é uma importante ferramenta, uma vez que dado um ideal que tem um conjunto infinito de geradores encontra-nos uma base finita para esse ideal. Obviamente que ainda estamos apenas a considerar ideais de monómios mas, como veremos de seguida, o caso geral também se verifica.

Para um ideal $I \subset k[x_1, \ldots, x_n]$ definimos agora o *ideal dos seus termos máximos* como $\mathrm{LT}(I) = \{cx^\alpha : \text{existe } f \in I \text{ com } \mathrm{LT}(f) = cx^\alpha\}$. Denotamos por $\langle \mathrm{LT}(I) \rangle$ o ideal gerado pelos elementos de $\mathrm{LT}(I)$.

Lema 3. *Seja* $I \subset k[x_1, \ldots, x_n]$ *um ideal. Então verifica-se:*

i. $\langle LT(I) \rangle$ *é um ideal de monómios;*

ii. existem $g_1, \ldots, g_s \in I$ *tais que* $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle$.

Seguindo por esta ordem de ideias apresentamos um importante teorema da álgebra que nos consegue responder ao primeiro problema apresentado, será que qualquer ideal $I \subset k[x_1, \ldots, x_n]$ é finitamente gerado? A resposta afirmativa é dada pelo Teorema da Base de Hilbert,

Teorema 2 (da Base de Hilbert, [1])**.** *Todo o ideal* $I \subset k[x_1, \ldots, x_n]$ *tem um conjunto finito de geradores. Ou seja,* $I = \langle g_1, \ldots, g_s \rangle$ *para alguns* $g_1, \ldots, g_s \in I$.

É à custa deste teorema que se demonstra que muitos dos algoritmos que apresentamos à frente terminam, uma vez que este teorema é equivalente à condição da cadeia ascendente de ideais:

Teorema 3. *Seja* $I_1 \subset I_2 \subset I_3 \subset \ldots$ *uma cadeia ascendente de ideais de* $k[x_1, \ldots, x_n]$ *. Então existe um* $N \geq 1$ *tal que* $I_N = I_{N+1} = I_{N+2} = \ldots$.

2.4 Bases de Gröbner

Um subconjunto finito $G = \{g_1, \ldots, g_s\}$ de um ideal I diz-se uma *base de Gröbner* se

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

Pode-se mostrar que todo o ideal não nulo possui uma base de Gröbner e, além disso, que qualquer base de Gröbner de um ideal gera esse mesmo ideal. Vamos agora verificar que utilizando uma base de Gröbner, o resto da divisão em $k[x_1, \ldots, x_n]$ fica unicamente determinado.

Proposição 1. *Seja $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner de um ideal $I \subset k[x_1, \ldots, x_n]$ e seja $f \in k[x_1, \ldots, x_n]$. Então existe um único $r \in k[x_1, \ldots, x_n]$ tal que:*

- *nenhum termo de r é divisível por algum $LT(g_i)$;*
- *existe $g \in I$ tal que $f = g + r$.*

Em particular, r é o resto da divisão de f por G, independentemente da ordem pela qual G está listado.

Demonstração. Seja $f \in k[x_1, \ldots, x_n]$. Tem-se, pelo algoritmo da divisão, que podemos escrever $f = \sum_{i=1}^{s} a_i g_i + r$ onde nenhum termo de r é divisível por algum $\mathrm{LT}(g_i)$. Existe portanto um $g \in I$ tal que $f = g + r$ – consideremos $g = \sum_{i=1}^{s} a_i g_i$. Note-se que g pertence a I pois todos os g_i estão em I. Suponhamos agora que existem g, r, g', r' tais que $f = g + r = g' + r'$.Temos que $g - g' = r' - r$, e, como tanto g como g' estão em I, $g - g' \in I$. Portanto $r' - r \in I$, donde sucede que $\mathrm{LT}(r' - r) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$, por G ser de Gröbner. Mas se $\mathrm{LT}(r' - r) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$ então teríamos que $\mathrm{LT}(r' - r)$ seria divisível por algum $\mathrm{LT}(g_i)$, o que é absurdo, pois tanto r como r' foram obtidos pelo algoritmo da divisão que garante que nenhum deles é divisível por algum $\mathrm{LT}(g_i)$ pelo que a soma deles também não o será. Tem-se portanto que $r = r'$. □

Estamos agora em condições de responder à segunda pergunta colocada no início – dados polinómios $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ existe algum algoritmo que decida se f está em $\langle f_1, \ldots, f_s\rangle$? Mais uma vez a resposta é afirmativa,

Corolário 1. *Seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner de um ideal $I \subset k[x_1, \ldots, x_n]$ e seja $f \in k[x_1, \ldots, x_n]$. Então $f \in I$ sse o resto da divisão de f por G é zero.*

O único problema com que nos deparamos agora é que esta condição apenas funciona caso tenhamos uma base de Gröbner *a priori*. Caso não seja o caso teremos de encontrar uma base de Gröbner primeiro e será sobre esse assunto que nos vamos debruçar agora.

Vamos denotar o resto da divisão de f pelo s-tuplo ordenado $F = (f_1, \ldots, f_s)$ por $\overline{f}^F$. Definimos ainda mais dois conceitos: dados polinómios $f, g \in k[x_1, \ldots, x_n]$ não nulos com $\mathrm{multideg}(f) = \alpha$ e $\mathrm{multideg}(g) = \beta$ seja $\gamma = (\gamma_1, \ldots, \gamma_n)$, onde cada $\gamma_i = \max(\alpha_i, \beta_i)$ e definimos que x^γ é o *mínimo múltiplo comum* de $\mathrm{LM}(f)$ e $\mathrm{LM}(g)$, escrito $x^\gamma = \mathrm{mmc}(\mathrm{LM}(f), \mathrm{LM}(g))$. O *S-polinómio* de f e g é dado por

$$S(f, g) = \frac{x^\gamma}{LT(f)} f - \frac{x^\gamma}{LT(g)} g.$$

Exemplo 6. *Sejam, por exemplo, $f(x, y) = x^2 + xy$ e $g(x, y) = x^2y^2 + x \in \mathbb{R}[x, y]$ na ordem lexicográfica. Tem-se que* $\mathrm{mmc}(LM(f), LM(g)) = x^2y^2$ *e logo o S-polinómio de f e g é*

$$\begin{aligned} S(f, g) &= \frac{x^2y^2}{x^2}(x^2 + xy) - \frac{x^2y^2}{x^2y^2}(x^2y^2 + x) \\ &= xy^3 - x \end{aligned}$$

Este novo conceito, o S-polinómio, é o que nos vai permitir construir a base de Gröbner. Vejamos como: queremos obter um subconjunto finito $G = \{g_1, \ldots, g_s\}$ de um ideal I tal que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. Um problema que surge imediatamente na construção de G é a possibilidade de existir uma combinação dos g_i de maneira a que o termo máximo desta combinação se cancela, ou seja o termo máximo não vai pertencer ao ideal gerados pelos $\mathrm{LT}(g_i)$. Por outro lado esta combinação de g_i está em I pelo que o seu termo máximo está no ideal gerado pelos termos máximos dos polinómios de I, e daí a nossa igualdade não se verifica. Os S-polinómios foram especificamente criados para cancelar os termos máximos e quando acrescentados a G esta ambiguidade desaparece.

Com isto, conseguimos enunciar um importante resultado,

Teorema 4 (Critério de Buchberger)**.** *Seja I um ideal. Então a base ordenada $G = (g_1, \ldots, g_t)$ é uma base de Gröbner de I sse para todos os pares $i \neq j$, $\overline{S(g_i, g_j)}^G = 0$.*

Do critério de Buchberger podemos retirar uma ideia sobre como construir uma base de Gröbner para um ideal I: calculamos $\overline{S(g_i, g_j)}^G$ para todos os polinómios da base conhecida (que se sabe ser finita pelo Teorema da base de Hilbert); caso todos sejam zero já temos uma base de Gröbner; caso contrário, acrescentamos aos geradores $\overline{S(g_i, g_j)}^G$ e calculamos os novos S-polinómios tal como o seu resto da divisão por G. O algoritmo continua assim até todos os restos das divisões de S-polinómios pelos geradores seja zero. Podemos agora tentar escrever um algoritmo que calcule uma base de Gröbner para um ideal.

Este algoritmo recebe um conjunto finito de geradores de I, $F = (f_1, \ldots, f_s)$ e devolve uma base de Gröbner G para I:

Algoritmo 2 Algoritmo de Buchberger

```
G = F
repeat
  G' = G
  for cada par {p, q}, p ≠ q em G' do
    S = S(p, q)^G'
    if S ≠ 0 then
      G = G ∪ {S}
    end if
  end for
until G = G'
```

Uma vez que este algoritmo trabalha de uma maneira um pouco cega, é natural que as bases de Gröbner criadas contenham muito mais geradores de que necessitariam pelo que é útil o seguinte lema:

Lema 4. *Seja G uma base de Gröbner para o ideal I e $p \in G$ um polinómio tal que $LT(p) \in \langle LT(G - \{p\}) \rangle$. Então $G - \{p\}$ também é uma base de Gröbner para I.*

Podemos assim definir ainda uma base de Gröbner *minimal*, que obedece a

i. $\mathrm{LC}(p) = 1$ para todo o $p \in G$;

ii. para todo o $p \in G, LT(p) \notin \langle LT(G - \{p\}) \rangle$.

E caso uma base verifique i. e

iii. para todo o $p \in G$, nenhum monómio de p está em $\langle LT(G - \{p\})\rangle$

diz-se uma base de Gröbner *reduzida*. As bases reduzidas são bastante especiais:

Proposição 2. *Seja $I \neq 0$ um ideal. Então, para uma relação de ordem de monómios, I tem uma única base de Gröbner reduzida.*

Esboço da demonstração. Aplicando o algoritmo de Buchberger obtemos uma base de Gröbner para I. Em seguida, utilizando o Lema 4 e acertando os coeficientes máximos dos geradores conseguimos eliminar geradores da base de Gröbner tornando-a minimal. Seja $G = \{g_1, \ldots, g_t\}$ uma base minimal de I. Para a tornar reduzida, considere-se o seguinte processo: actualizar G onde cada g_i é substituído por $\overline{g_i}^{G\setminus g_i}$. Isto torna a base reduzida. Para provar a unicidade, tomam-se duas bases de Gröbner reduzidas, G e $\hat{G}$. Por maioria de razão, são também bases minimais e mostra-se que $\mathrm{LT}(G) = \mathrm{LT}(\hat{G})$ e que têm o mesmo número de geradores. Basta em seguida raciocinar por absurdo e a demonstração fica completa.

Esta proposição resolve o terceiro problema colocado na primeira secção para determinar quando é que dois conjuntos de polinómios geram o mesmo ideal. Para fazermos isto basta calcular a base de Gröbner reduzida de cada um deles e aí os ideais gerados serão o mesmo sse as suas bases de Gröbner reduzidas o forem.

2.5 Melhoramentos do algoritmo de Buchberger

Nesta secção iremos apresentar alguns critérios que melhoram a eficiência do algoritmo de Buchberger. Para o fazermos vamos primeiro definir um novo conceito, a redução.

Seja $G = \{g_1, \ldots, g_s\} \subset k[x_1, \ldots, x_n]$. Dado $f \in k[x_1, \ldots, x_n]$ dizemos que f *se reduz a zero módulo* G, escrito $f \to_G 0$, se f pode ser escrito na forma $f = \sum_{i=1}^{s} a_i g_i$ satisfazendo que $a_i g_i \neq 0$ implica $\mathrm{multideg}(f) \geq \mathrm{multideg}(a_i g_i)$.

Lema 5. *Seja $G = (g_1, \ldots, g_s)$ um s-tuplo de polinómios em $k[x_1, \ldots, x_n]$ e $f \in k[x_1, \ldots, x_n]$. Então $\overline{f}^G = 0$ implica $f \longrightarrow_G 0$ mas o recíproco pode não se verificar.*

Exemplo 7. *Seja $G = (xy + 1, y^2 - 1)$ e $f = xy^2 - x$, na ordem lexicográfica. Tem-se que $\overline{f}^G = -x - y$ e no entanto $f \longrightarrow_G 0$ uma vez que também podemos escrever $f = 0 \cdot (xy+1) + x \cdot (y^2 - 1)$. Como $\mathrm{multideg}(xy^2 - x) \geq \mathrm{multideg}(xy^2 - x)$ segue que $f \longrightarrow_G 0$.*

Note-se ainda que caso G seja uma base de Gröbner então $f \longrightarrow_G 0 \Leftrightarrow \overline{f}^G = 0$. Assim encontrámos um novo critério para encontrar uma base de Gröbner:

Teorema 5. *Uma base $G = \{g_1, \ldots, g_s\}$ para um ideal I é base de Gröbner sse $S(g_i, g_j) \longrightarrow_G 0$ para todo o par (i, j) com $i \neq j$.*

Vamos reflectir um pouco em como podemos optimizar o algoritmo de Buchberger e, para isso, vamos recordar que este é basicamente constituído por dois passos em cada ciclo:

i. o cálculo dos S-polinómios;

ii. a redução dos S-polinómios módulo G.

Recorde-se ainda que o algoritmo termina e devolve a base de Gröbner pretendida assim que todos os S-polinómios se reduzem a zero. Destes dois, o passo mais moroso é sem dúvida a redução dos S-polinómios, uma vez que invoca o algoritmo de divisão e à medida que a base aumenta de tamanho, também o algoritmo de divisão fica mais demorado. É ainda de reparar que à medida que o cálculo da base de Gröbner progride, são acrescentados em cada novo ciclo um conjunto de S-polinómios cada vez maior. Como o algoritmo termina, a quantidade de S-polinómios que reduz para zero aumenta muito com a evolução do algoritmo e muitos dos cálculos executados não ajudam na construção da base de Gröbner (apenas confirmam que já é uma base de Gröbner). De facto, existe um ponto antes de o algoritmo terminar em que já temos a base de Gröbner pretendida mas não o sabemos. O que tentamos agora fazer é encontrar critérios que consigam "prever" quando é que um dado S-polinómio vai reduzir a zero, tornando assim o cálculo da base de Gröbner mais eficiente.

Proposição 3. *Dado um conjunto finito $G \subset k[x_1, \ldots, x_n]$, com $f, g \in G$ tais que* $\mathrm{mmc}(LM(f), LM(g)) = LM(f) \cdot LM(g)$ *então* $S(f, g) \longrightarrow_G 0$.

Demonstração. Sem perda de generalidade admita-se que $\mathrm{LC}(f)=\mathrm{LC}(g) = 1$. Tem-se que $f = \mathrm{LM}(f) + p$ e $g = \mathrm{LM}(g) + q$. Calculando o S-polinómio de f e g obtemos

$$\begin{aligned} S(f,g) &= \frac{LM(g) \cdot LM(f)}{LM(f)} f - \frac{LM(g) \cdot LM(f)}{LM(g)} g \\ &= LM(g)f - LM(f)g \\ &= (g-q)f - (f-p)g \\ &= gf - qf - fg + gp \\ &= gp - fq \longrightarrow_G 0 \end{aligned}$$

□

Seja $F = (f_1, \ldots, f_s) \in (k[x_1, \ldots, x_n])^s$. Uma *syzygy* nos termos máximos $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ é um s-tuplo $S = (h_1, \ldots, h_s) \in (k[x_1, \ldots, x_n])^s$ tal que $\sum_{i=1}^{s} h_i \cdot \mathrm{LT}(f_i) = 0$. Denotamos por $S(F) \subset (k[x_1, \ldots, x_n])^s$ o conjunto de todas as *syzygies* em $\mathrm{LT}(f)$. Além disso, um elemento $S = (c_1 x^{\alpha(1)}, \ldots, c_s x^{\alpha(s)}) \in S(F)$ diz-se *homogéneo de multigrau* $\alpha \in \mathbb{N}^n$ se $\alpha(i) + \mathrm{multideg}(f_i) = \alpha$ sempre que $c_i \neq 0$.

Exemplo 8. *Seja $F = (f_1, \ldots, f_s)$ um s-tuplo de polinómios de $k[x_1, \ldots, x_n]$ e x^γ o mínimo múltiplo comum dos termos máximos de f_i, f_j. Verifica-se que a* syzygy $S_{i,j} = \frac{x^\gamma}{LT(f_i)} e_i - \frac{x^\gamma}{LT(f_j)} e_j$ *dos termos máximos de f_i, f_j é homogénea de grau γ. Tem-se*

$$\begin{aligned} S_{i,j} &= (0, \ldots, \frac{x^\gamma}{LT(f_i)}, 0, \ldots, 0, -\frac{x^\gamma}{LT(f_j)}, 0, \ldots, 0) \\ &= (0, \ldots, \frac{x^{\gamma - \mathrm{multideg}(f_i)}}{LC(f_i)}, 0, \ldots, 0, -\frac{x^{\gamma - \mathrm{multideg}(f_j)}}{LC(f_j)}, 0, \ldots, 0), \end{aligned}$$

pelo que

$$\begin{cases} \alpha(i) = \gamma - \mathrm{multideg}(f_i) \\ \alpha(j) = \gamma - \mathrm{multideg}(f_j) \end{cases} \Leftrightarrow \begin{cases} \gamma = \alpha(i) + \mathrm{multideg}(f_i) \\ \gamma = \alpha(j) + \mathrm{multideg}(f_j) \end{cases}$$

Podemos agora ver que toda a *syzygy* pode ser escrita como combinações das *syzygies* definidas no exemplo anterior.

Proposição 4. *Dado $F = (f_1, \ldots, f_s)$ toda a* syzygy *$S \in S(F)$ pode ser escrita na forma $S = \sum_{i<j} u_{ij} S_{ij}$ onde cada $u_{ij} \in k[x_1, \ldots, x_n]$.*

Uma observação interessante é a que não precisamos de todas as S_{ij} para gerar as *syzygies* em $S(F)$.

Exemplo 9. *Seja $F = (x^2y^2 + z, xy^2 - y, x^2y + yz)$ na ordem lexicográfica. Verifica-se que*

$$S_{12} = (\frac{x^2y^2}{x^2y^2}, -x, 0) = (1, -x, 0)$$
$$S_{13} = (1, 0, -y)$$
$$S_{23} = (0, x, -y).$$

Tem-se que $S_{23} = S_{13} - S_{12}$. Por isto, S_{23} diz-se redundante *e que $\{S_{12}, S_{13}\}$ forma uma base para as* syzygies *$S(F)$.*

Podemos agora dar um novo critério para o algoritmo de Buchberger,

Teorema 6 ([1])**.** *Uma base $G = (g_1, \ldots, g_s)$ para um ideal I é base de Gröbner sse para todo o elemento $S = (h_1, \ldots, h_s)$ duma base homogénea para as* syzygies *$S(G)$ se tem*

$$S \cdot G = \sum_{i=1}^{s} h_i g_i \longrightarrow_G 0.$$

Temos agora uma condição mais forte do que o Teorema 3 nos dava para decidir se uma base é de Gröbner ou não. No entanto, este critério só será bom caso consigamos encontrar bases para $S(G)$ pequenas. Para isso obtemos a seguinte proposição,

Proposição 5. *Dado $G = (g_1, \ldots, g_s)$, suponhamos que temos:*

i. um subconjunto $\mathcal{S} \subset \{S_{ij} : 1 \leq i < j \leq t\}$ que é base para $S(G)$;

ii. elementos $g_i, g_j, g_k \in G$ distintos tais que $LT(g_k)$ divide mmc$(LT(g_i), LT(g_j))$.

Tem-se que se $S_{ik}, S_{jk} \in S$ então $\mathcal{S} - \{S_{ij}\}$ também é base de $S(G)$.

Podemos agora implementar uma nova versão do algoritmo de Buchberger – recebe um s-tuplo F de polinómios geradores de I e devolve uma base de Gröbner G para I:

Algoritmo 3 Algoritmo de Buchberger com critérios

$B = \{(i,j) : 1 \leq i < j \leq s\}$
$G = F$
$t = s$
while $B \neq \emptyset$ **do**
  Selecciona $(i,j) \in B$
  if $\text{mmc}(LT(f_i), LT(f_j)) \neq LT(f_i) \cdot LT(f_j) \wedge\ crit(f_i, f_j, B) = false$ **then**
    $S = \overline{S(f_i, f_j)}^{G}$
    if $S \neq 0$ **then**
      $t = t + 1$
      $f_t = S$
      $G = G \cup \{f_t\}$
      $B = B \cup \{(i,t) : 1 \leq i \leq t-1\}$
    end if
  end if
  $B = B - \{(i,j)\}$
end while

Observação: $crit(f_i, f_j, B)$ é true se existe algum $k \notin \{i,j\}$ para qual os pares $[i,k]$ e $[j,k] \notin B$ e LT(f_k) divide mmc(LT(f_i),LT(f_j)).

Nota: $[i,j] := (\min(i,j), \max(i,j))$

Capítulo 3

Nullstellensatz, geometria, eliminação e extensão

Neste capítulo vamos ver como o cálculo de bases de Gröbner de um ideal pode eliminar variáveis facilitando, ou mesmo resolvendo, problemas complexos.

3.1 O *Nullstellensatz* de Hilbert

Nesta secção vamos enunciar outro famoso teorema de Hilbert, este conhecido pelo seu nome alemão, *Nullstellensatz*, que se traduz para o teorema do lugar dos zeros. Este teorema vai-nos permitir obter informações sobre variedades de ideais em $k[x_1, \ldots, x_n]$. Nesta secção vamos denotar por $K = \bar{k}$, o fecho algébrico de k, quando necessitamos de trabalhar com um corpo algebricamente fechado. Podemos assim estender as definições dadas no capítulo 2 sobre variedades. Dado um subconjunto $S \subseteq k[x_1, \ldots, x_n]$, a variedade $\mathbf{V}_K(S) \subseteq K^n$ é $\mathbf{V}_K(S) = \{(a_1, \ldots, a_n \in K^n : f(a_1, \ldots, a_n) = 0$ para todo o $f \in S\}$. Relembramos ainda do capítulo 2 que o ideal de uma variedade V é definido por $\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0$ para todo o $(a_1, \ldots, a_n) \in V\}$.

Existem várias variantes do *Nullstellensatz* – nós vamos apresentar duas delas, conhecidas como *Nullstellensatz* fraco e forte. Note-se que apesar da facilidade com que os conseguímos apresentar, estes teoremas de Hilbert são bastante profundos.

Teorema 7 (*Nullstellensatz* de Hilbert fraco, [8])**.** *Seja I um ideal de $k[x_1, \ldots, x_n]$. Então $\boldsymbol{V}_K(I) = \emptyset$ sse $I = k[x_1, \ldots, x_n]$.*

Note-se que no caso $K = \mathbb{C}$ este teorema pode quase ser interpretado como o Teorema fundamental da álgebra para polinómios em mais do que uma variável.

Para enunciar o *Nullstellensatz* forte teremos de introduzir um novo conceito: dado um ideal I de $k[x_1, \ldots, x_n]$, o *radical* de I é $\sqrt{I} = \{f \in k[x_1, \ldots, x_n] : \exists j \in \mathbb{N} : f^j \in I\}$. O radical de um ideal é sempre um ideal e tem-se ainda que $V_K(I) = V_K(\sqrt{I})$.

Estamos agora em condições de apresentar o *Nullstellensatz* forte,

Teorema 8 (*Nullstellensatz* forte, [8])**.** $\boldsymbol{I}(V_K(I)) = \sqrt{I}$ *para qualquer ideal de* $k[x_1, \ldots, x_n]$.

De onde podemos ver que dois ideais I e J correspondem à mesma variedade sse os seus radicais são o mesmo.

Exemplo 10. *É fácil perceber que* $V_{\mathbb{R}}(x^2+y^2) = V_{\mathbb{R}}(x,y) = \{(0,0)\}$. *Por outro lado,* $V_{\mathbb{C}}(x^2+y^2)$ *é a união de duas rectas,* $y = \pm ix$ *e* $V_{\mathbb{C}}(x,y) = \{(0,0)\}$. *Deste simples exemplo se percebe a importância que tem o corpo ser algebricamente fechado – em* $\mathbb{R}$ *não tínhamos capacidade de diferenciar os dois ideais (através da análise das variedades associadas) enquanto que isso já é possível em* $\mathbb{C}$.

Consideremos um ideal $I = \langle f_1, \ldots, f_s \rangle$ de $k[x_1, \ldots, x_n]$ e a sua base de Gröbner reduzida, $G = \{g_1, \ldots, g_t\}$, para uma qualquer relação de ordem e vejamos como o *Nullstellensatz* fraco pode ser imediatamente aplicado para mostrar um resultado muito útil: caso $G = \{1\}$, temos que o ideal I é todo o $k[x_1, \ldots, x_n]$ e portanto pelo *Nullstellensatz* fraco temos que a variedade do ideal é vazia e logo os polinómios $f_1, \ldots, f_s$ não terão nenhum zero em comum; caso $G \neq \{1\}$, pela mesma ordem de ideais, teremos que os polinómios têm pelo menos um zero em comum. Tudo isto pode ser resumido a

$$V_K(I) = \emptyset \text{ sse } 1 \in G.$$

Esta fórmula começa a relacionar a existência de soluções para sistemas de equações polinomiais com a forma das bases de Gröbner e cada vez mais veremos aplicações das bases de Gröbner nesse sentido. O seguinte teorema, apesar de parecer um lema técnico é de facto um grande passo para compreendermos a razão pela qual quando uma base de Gröbner é calculada numa ordem lexicográfica aparecem equações com certas variáveis eliminadas.

Teorema 9 ([8])**.** *Dado um ideal* $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$ *e a sua base de Gröbner reduzida para a ordem lexicográfica,* $G = \{g_1, \ldots, g_t\}$*, as seguintes afirmações são equivalentes:*

i. a variedade $V_K(I)$ *é finita.*

ii. para cada $i = 1, \ldots, n$*, existe* $j \in \{1, \ldots, t\}$ *tal que* $LT(g_j) = x_i^{\nu}$*, onde* $\nu \in \mathbb{N}$.

iii. a dimensão da base do espaço vectorial $k[x_1, \ldots, x_n]\ /I$ *é finita.*

Um ideal $I \neq k[x_1, \ldots, x_n]$ que satisfaz qualquer uma das asserções do teorema diz-se de *dimensão zero* ou *zero dimensional*. Estes ideais são de extrema importância – são tais que quando a sua base de Gröbner é calculada na ordem lexicográfica apresentam uma forma triangular muito à semelhança das matrizes em escada da álgebra linear como podemos perceber pelo seguinte corolário,

Corolário 2. *Dado um ideal* I *zero dimensional seja* $G = \{g_1, \ldots, g_t\}$ *a sua base de Gröbner reduzida na ordem lexicográfica com* $x_1 < \ldots < x_n$*. Então existe uma indexação dos polinómios* $g_1, \ldots, g_t$ *tal que* $g_i \in k[x_1, \ldots, x_i]$ *e que* $LT(g_i)$ *é uma potência da variável* x_i.

Ou seja, o polinómio g_1 da base de Gröbner apenas tem como variáveis o x_1, o polinómio g_2 apenas tem como variáveis x_1, x_2 e assim sucessivamente. Este corolário é basicamente uma maneira mais explícita de escrever a afirmação *ii.* do teorema anterior e com isto conseguimos entender porque é que a ordem lexicográfica elimina variáveis. Na próxima secção vamos enunciar outros teoremas que nos ajudam na resolução de sistemas de equações polinomiais.

3.2 Teoremas da eliminação e da extensão

Nesta secção vamos enunciar dois importantes teoremas para de seguida vermos algumas das suas aplicações à resolução de sistemas de equações polinomiais e à obtenção das equações explícitas de variedades, partindo de uma sua parametrização.

Para motivarmos estes teoremas, vejamos um exemplo prático,

Exemplo 11. *Consideremos o sistema de equações*

$$\begin{cases} x^2+y^2+z^2=4 \\ x^2+2y^2=5 \\ xz=1 \end{cases}$$

Calculando a base de Gröbner do ideal $I=\langle x^2+y^2+z^2-4, x^2+2y^2-5, xz-1\rangle$ *na ordem* lex *com* $x>y>z$ *obtemos a base* $G=\{1-3z^2+2z^4, -1+y^2-z^2, x-3z+2z^3\}$. *Note-se como* $g_1=1-3z^2+2z^4\in k[z]$. *Assim, e factorizando* $g_1=(z-1)(z+1)(2z^2-1)$ *podemos começar a resolver o sistema (que lembra um sistema triangular da álgebra linear) por substituição. De* $g_1=0$ *obtemos que* $z=\pm 1, \pm\frac{1}{\sqrt{2}}$, *substituindo e resolvendo* $g_2=0$ *e por fim substituindo em* g_3 *as soluções para* y *e* z *obtemos as oito soluções do sistema,* $\{(1,\pm\sqrt{2},1),(-1,\pm\sqrt{2},-1),(\sqrt{2},\pm\frac{\sqrt{6}}{2},\frac{1}{\sqrt{2}}),(-\sqrt{2},\pm\frac{\sqrt{6}}{2},-\frac{1}{\sqrt{2}})\}$.

O que é que nos permitiu encontrar estas soluções? Em primeiro lugar conseguimos através da criação da base de Gröbner obter um polinómio numa só variável (ou seja *eliminámos* variáveis). Após resolvermos esta equação em $k[z]$, conseguimos *estender* as soluções de g_1 para soluções do sistema inicial. Podemos formalizar a noção de eliminação facilmente – basta reparar que o que aconteceu foi $g_1\in I\cap k[z]$. No caso geral temos que:

Dados $I=\langle f_1,\ldots,f_s\rangle\subset k[x_1,\ldots,x_n]$, o *j-ésimo ideal de eliminação*, I_j, é o ideal de $k[x_{j+1},\ldots,x_n]$ definido por $I_j=I\cap k[x_{j+1},\ldots,x_n]$.

Ou seja, o ideal I_j contém todos os polinómios do ideal original que não contêm as variáveis $x_1,\ldots,x_j$. Portanto, "eliminar" as variáveis $x_1,\ldots,x_j$ é equivalente a encontrar um polinómio não nulo em I_j. Apresentamos um dos teoremas da secção que nos diz que a base de Gröbner de um ideal de eliminação é apenas o conjunto de polinómios da base de Gröbner do ideal original que apenas contêm as variáveis $x_1,\ldots,x_j$,

Teorema 10 (da Eliminação, [1])**.** *Se* G *é uma base de Gröbner na ordem lexicográfica com* $x_1>x_2>\ldots>x_n$ *do ideal* $I\subset k[x_1,\ldots,x_n]$ *então para todo* $0\leq j\leq n$, *o conjunto* $G_j=G\cap k[x_{j+1},\ldots,x_n]$ *é base de Gröbner para* I_j.

Discutamos agora a extensão de soluções das equações em I_j para soluções em I. Dado um ideal I e a sua variedade afim, $\mathbf{V}(I)$, a nossa ideia intuitiva consiste em, depois de fixarmos um ideal de eliminação, I_l, e neste encontrarmos uma *solução parcial* (ou seja encontrar um ponto em $\mathbf{V}(I_l)$), por exemplo $(a_{l+1},\ldots,a_n)$, estender a solução para a variedade $\mathbf{V}(I_{l-1})$, e, continuar desta forma, até encontrarmos uma solução em $\mathbf{V}(I)$. Pode acontecer que, dadas soluções em $\mathbf{V}(I_t)$ para $t>0$, estas não consigam ser estendidas para uma solução na variedade do ideal original, mas temos um teorema que nos dá um critério de extensão,

Teorema 11 (da extensão, [1])**.** *Dado* k *algebricamente fechado, seja um ideal* $I=\langle f_1,\ldots,f_s\rangle\subset k[x_1,\ldots,x_n]$ *e* I_1 *o primeiro ideal de eliminação de* I. *Escreva-se, para cada* $1\leq i\leq s$

$$f_i=g_i(x_2,\ldots,x_n)x_1^{N_i}+\text{termos onde } x_1 \text{ tem grau menor que } \mathrm{N_i},$$

onde $N_i\geq 0$ *e* $g_i\in k[x_2,\ldots,x_n]$ *são não nulos. Supondo que temos uma solução parcial* $(a_2,\ldots,a_n)\in \boldsymbol{V}(I_1)$ *e caso a solução parcial não anule todos os* $g_1,\ldots,g_s$, *então existe* $a_1\in k$ *tal que* $(a_1,\ldots,a_n)\in \boldsymbol{V}(I)$.

Isto diz-nos que se as soluções parciais não anulam os coeficientes g_i então a solução parcial estende para uma solução total, $(a_1, \ldots, a_n) \in \mathbf{V}(I)$.

Exemplo 12. *Seja $I = \langle xy - 1, xz - 1\rangle \subset \mathbb{C}[x, y, z]$. Uma base de Gröbner de I é $G = \{-1 + xz, y - z\}$ pelo que $G_1 = \{y - z\}$, ou seja, as soluções parciais são da forma $(y, z) = (a, a) \in \mathbb{C}^2$. Como podemos escrever os polinómios de I na forma $f_1 = g_1(y, z)x - 1$ e $f_2 = g_2(y, z)x - 1$, onde $g_1(y, z) = y$ e $g_2(y, z) = z$, e $\boldsymbol{V}(g_1, g_2) = \{(0, 0)\}$ temos que todas as soluções parciais da forma (a, a) se estendem desde que $a \neq 0$ e temos portanto que os pontos de $\boldsymbol{V}(I)$ são da forma $(\frac{1}{a}, a, a)$ com $a \neq 0$.*

Verifica-se então que, caso $\mathbf{V}(g_1, \ldots, g_i) = \emptyset$, por exemplo quando um dos g_i é constante não nulo, então qualquer solução parcial vai estender para uma solução que está na variedade do ideal original. O seguinte corolário é exactamente isso que nos diz:

Corolário 3 (do Teorema da extensão)**.** *Dado k algebricamente fechado, seja um ideal $I = \langle f_1, \ldots, f_s\rangle \subset k[x_1, \ldots, x_n]$ e I_1 o primeiro ideal de eliminação de I. Assuma-se que existe um i tal que*

$$f_i = cx_1^N + (\text{termos onde } x_1 \text{ tem grau menor que N}),$$

onde $N > 0$ e $c \neq 0$. Então, se temos uma solução parcial $(a_2, \ldots, a_n) \in \boldsymbol{V}(I_1)$ existe um $a_1 \in k$ tal que $(a_1, a_2, \ldots, a_n) \in \boldsymbol{V}(I)$.

3.3 Geometria e eliminação

Nesta secção vamos enunciar os teoremas da secção anterior dando uso a ferramentas geométricas. Relembre-se que K é um corpo algebricamente fechado. Definimos a aplicação *projecção*

$$\pi_j : K^n \to K^{n-j}$$

por $(a_1, \ldots, a_n) \longmapsto (a_{j+1}, \ldots, a_n)$. Em particular, dada uma variedade $V \subset K^n$ temos que $\pi_j(V) \subset K^{n-j}$. Obtemos com esta definição um lema que relaciona $\pi_j(V)$ e o j-ésimo ideal de eliminação:

Lema 6. *Seja $I = \langle f_1, \ldots, f_s\rangle$ um ideal de $K[x_1, \ldots, x_n]$ e $I_j = I \cap K[x_{j+1}, \ldots, x_n]$ o seu j-ésimo ideal de eliminação. Então temos que*

$$\pi_j(V) \subset \boldsymbol{V}(I_j) \subset K^{n-j}.$$

Chamámos aos pontos de uma variedade de um ideal de eliminação (os elementos de $\mathbf{V}(I_j)$) as soluções parciais das equações originais. Com a definição de projecção podemos descrever explicitamente as soluções parciais que estendem para soluções totais:

$$\pi_j(V) = \{(a_{j+1}, \ldots, a_n) \in \mathbf{V}(I_j) : \exists a_1, \ldots, a_j \in K \text{ com } (a_1, \ldots, a_j, a_{j+1}, \ldots, a_n) \in V\}.$$

A projecção de uma variedade não é necessariamente uma variedade como vimos no exemplo anterior. Tínhamos que $I = \langle xy - 1, xz - 1\rangle \subset \mathbb{C}[x, y, z]$ e que as soluções parciais eram o conjunto $\mathbf{V}(I_1) = \{(a, a) : a \in \mathbb{C}\}$. Por outro lado, o conjunto das soluções parciais que estendem para um ponto de $\mathbf{V}(I)$ são $\pi_1(V) = \{(a, a) : a \in \mathbb{C} - \{0\}\}$ que não é uma variedade.

Dado isto, podemos enunciar o teorema da extensão em termos geométricos:

Teorema 12 (Versão geométrica do Teorema da extensão, [1]). *Dada uma variedade $V = \boldsymbol{V}(f_1, \ldots, f_s) \subset K^n$ e sejam os g_i como construídos no Teorema da extensão. Então, se I_1 é o primeiro ideal de eliminação do ideal $\langle f_1, \ldots, f_s \rangle$ temos que se verifica a igualdade em K^{n-1}*

$$\boldsymbol{V}(I_1) = \pi_1(V) \cup (\, \boldsymbol{V}(g_1, \ldots, g_s) \cap \boldsymbol{V}(I_1)).$$

Obtém-se então outro importante teorema que relaciona $\mathbf{V}(I_j)$ com $\pi_j(V)$.

Teorema 13 (do Fecho, [1]). *Dada uma variedade $V = \boldsymbol{V}(f_1, \ldots, f_s) \subset K^n$ e I_j o j-ésimo ideal de eliminação do ideal $\langle f_1, \ldots, f_s \rangle$ verificam-se as condições:*

i. $\boldsymbol{V}(I_j)$ é a menor variedade que contém $\pi_j(V) \subset K^{n-j}$.

ii. sempre que $V \neq \emptyset$ então existe uma variedade afim $W \subsetneq \boldsymbol{V}(I_j)$ tal que $\boldsymbol{V}(I_j) \setminus W \subset \pi_j(V)$.

O nome deste teorema é justificado por razões mais profundas: podemos definir uma topologia, a topologia de *Zariski*, onde o fecho topológico de $\pi_j(V)$ é exactamente a menor variedade que o contém, $\mathbf{V}(I_j)$.

Interpretando geometricamente o corolário do teorema da extensão obtido anteriormente temos obviamente que

Corolário 4. *Dada uma variedade $V = \boldsymbol{V}(f_1, \ldots, f_s) \subset K^n$, suponhamos que um dos f_i é da forma $f_i = cx_1^N +$ termos onde x_1 tem grau menor que N, onde $N > 0$ e $c \neq 0$. Então, se I_1 é o primeiro ideal de eliminação verifica-se a igualdade,*

$$\boldsymbol{V}(I_1) = \pi_1(V).$$

Podemos também facilmente relacionar estes resultados com os obtidos anteriormente sobre ideais de dimensão zero:

Proposição 6. *Seja $I = \langle f_1, \ldots, f_s \rangle \subset K[x_1, \ldots, x_n]$ um ideal, $V = \boldsymbol{V}(f_1, \ldots, f_s) \subset K^n$ a variedade associada e I_1 o seu primeiro ideal de eliminação. Se I tem dimensão zero então verifica-se a igualdade,*

$$\boldsymbol{V}(I_1) = \pi_1(V).$$

Demonstração. Seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner reduzida na ordem lexicográfica com $x_1 < \ldots < x_n$ do ideal I. Como I tem dimensão zero, pelo corolário 2, temos que G tem uma forma triangular, ou seja cada g_i ordenando os monómios na relação lexicográfica é:

$$\begin{aligned} g_1 &= x_1^{\nu_1} + p_1(x_1) \\ g_2 &= x_2^{\nu_2} + p_2(x_1, x_2) \\ &\vdots \\ g_n &= x_n^{\nu_n} + p_n(x_1, \ldots, x_n) \end{aligned}$$

onde em cada p_n a variável x_n tem grau menor que ν_n. Como o ideal gerado pela base de Gröbner é igual ao ideal inicial temos que $\mathbf{V}(G) = \mathbf{V}(I)$ e, pela mesma ordem de ideias (o ideal gerado por G_1 é o mesmo que o primeiro ideal de eliminação de I, I_1), temos que $\mathbf{V}(G_1) = \mathbf{V}(I_1)$. Uma solução parcial de I_1 (que é um ponto de $\mathbf{V}(G_1)$) é da forma $(a_2, \ldots, a_n) \in K^n$ e temos que, como os termos máximos dos polinómios g_n são apenas na variável x_n a solução parcial estende para uma solução em $\mathbf{V}(I)$, pelo corolário 4. Como considerámos uma solução parcial qualquer temos que todas as soluções parciais estendem para uma solução de $\mathbf{V}(I)$ e logo $\mathbf{V}(I_1) = \pi_1(V)$. □

3.4 Problema da representação explícita

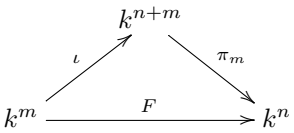
Nesta secção vamos abordar o problema da representação explícita, ou seja, dado um corpo k infinito e uma parametrização polinomial $F : k^m \to k^n$ definida por

$$\begin{cases} x_1 = f_1(t_1, \ldots, t_m) \\ \quad \vdots \\ x_n = f_n(t_1, \ldots, t_m), \end{cases} \tag{1}$$

obter uma representação explícita (*ie.* apenas em termos de $x_1, \ldots, x_n$) da variedade definida pelos polinómios anteriores. Para compreendermos este teorema utilizamos alguns resultados que vimos nas secções anteriores:

Teorema 14 (da representação polinomial)**.** *Considere-se o sistema (1), o ideal associado* $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle \subset k[t_1, \ldots, t_m, x_1, \ldots, x_n]$ *e* $I_m = I \cap k[x_1, \ldots, x_n]$ *o seu m-ésimo ideal de eliminação. Então* $\mathbf{V}(I_m)$ *é a menor variedade em* k^n *que contém* $F(k^m)$*.*

Quando $k = K$ este teorema resulta de uma simples aplicação do Teorema do fecho – as equações de (1) definem a variedade $V = \mathbf{V}(x_1 - f_1, \ldots, x_n - f_n) \subset k^{n+m}$ e os pontos de V são da forma $(t_1, \ldots, t_m, f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m))$, ou seja o grafo de F. Considerando ainda $\iota : k^m \to k^{n+m}$ definida por $\iota(t_1, \ldots, t_m) = (t_1, \ldots, t_m, f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m))$ temos que



ou seja, $F = \pi_m \circ \iota$ donde sai que $F(k^m) = \pi_m(\iota(k^m)) = \pi_m(V)$ e logo, pelo teorema do fecho temos que $\mathbf{V}(I_m)$ é a menor variedade que contém $F(k^m)$.

Apesar de ser um resultado algo intuitivo depois do que vimos anteriormente, é também bastante poderoso na medida em que nos fornece um algoritmo para calcular a equação ou equações explícitas da menor variedade que contém a parametrização.

Capítulo 4

Aplicações

4.1 Aplicações à Álgebra e à Geometria

Nesta secção vamos aplicar o algoritmo de Buchberger para resolver problemas de ordem algébrica, além de conseguirmos calcular uma base de Gröbner para um dado ideal. Vamos também ilustrar com um exemplo prático como o cálculo de certas bases de Gröbner se pode tornar muito complexo em certas relações de ordem. Vamos apresentar algoritmos que resolvem os seguintes problemas:

i. dado um ideal I calcular uma base de Gröbner G para I;

ii. dado $f \in k[x_1, \ldots, x_n]$ e um ideal I determinar se $f \in I$;

iii. dado uma parametrização $F(\mathbf{t})$ determinar a equação explícita da variedade que é definida pela parametrização;

iv. determinar se dois ideais I e J são iguais;

v. encontrar representantes canónicos das classes de equivalência dos elementos de $k[x_1, \ldots, x_n]/I$;

vi. encontrar uma base para o espaço vectorial $k[x_1, \ldots, x_n]/I$;

vii. determinar as operações em $k[x_1, \ldots, x_n]/I$, ou seja determinar uma tabela de multiplicação, quando a base para o espaço vectorial $k[x_1, \ldots, x_n]/I$ é finita.

4.1.1 Algoritmos para a resolução de cada problema

Nesta secção apresentamos um método de resolução para cada um dos problemas apresentados, resumindo o que já vimos noutros capítulos e resolvendo novos problemas. Isto vai ser feito construindo um algoritmo em pseudo-código que calculará o pretendido – neste pseudo-código consideramos que:

- Buchberger$[I]$ calcula uma base de Gröbner para I.
- BuchbergerRed$[I]$ calcula uma base de Gröbner reduzida para I.
- Buchberger$_{ord}[I]$ calcula a base de Gröbner para a ordem *ord*.

i. Como vimos, para calcular a base de Gröbner de um dado ideal I basta aplicarmos o algoritmo de Buchberger, pelo que temos,

Algoritmo 4 Base de Gröbner

$G = \text{Buchberger}[I]$;

ii. Seja $f \in k[x_1, \ldots, x_n]$ e um ideal I. Para determinarmos se $f \in I$ basta calcularmos:

Algoritmo 5 Pertença a um ideal

$G = \text{Buchberger}[I]$;
if $\overline{f}^G = 0$ **then**
  $f \in I$
else
  $f \notin I$
end if

iii. Dada uma parametrização polinomial $F(t_1, \ldots, t_m) = (f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m))$ basta calcular uma base de Gröbner na ordem lexicográfica apropriada e as equações apenas em termo de $x_1, \ldots, x_n$ serão aquelas que definem a menor variedade que contém a superfície que está a ser parametrizada:

Algoritmo 6 Representação explícita

$I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$;
$G = \text{Buchberger}_{lex}[I]$ com $t_1 > \ldots > t_m > x_1 > \ldots > x_n$;
$Eqs = G \cap k[x_1, \ldots, x_n]$;

iv. Para determinarmos se dois ideais I e J são iguais basta calcularmos as respectivas bases de Gröbner reduzidas e ver se estas são iguais. Tem-se então:

Algoritmo 7 Igualdade de ideais

$G_I = \text{BuchbergerRed}[I]$;
$G_J = \text{BuchbergerRed}[J]$;
if $G_I = G_J$ **then**
  $I = J$
else
  $I \neq J$
end if

Como um ideal $I = \langle f_1, \ldots, f_s \rangle \subseteq J$ sse $f_1, \ldots, f_s \in J$ que sabemos calcular pelo algoritmo de ii), uma alternativa ao método do algoritmo 6 seria calcular cada uma das inclusões, $I \subseteq J$ e $J \subseteq I$, desta forma.

v. Como vimos anteriormente, o resto da divisão de um polinómio $f \in k[x_1, \ldots, x_n]$ por uma base de Gröbner G é único. Podemos então introduzir um novo conceito, se $f \longrightarrow_G r$ então r

diz-se a *forma normal de* f em relação a G, $N_G(f)$.

Facilmente se verifica que se $f, g \in k[x_1, \ldots, x_n]$ então $f \equiv g \ (mod\ I)$ sse $N_G(f) = N_G(g)$ e que além disso $\{N_G(f) : f \in k[x_1, \ldots, x_n]\}$ é um conjunto dos representantes canónicos das classes de equivalência em $k[x_1, \ldots, x_n]/I$.

vi. Seja I um ideal de $k[x_1, \ldots, x_n]$ e $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner de I. Uma vez que o conjuntos dos monómios em n variáveis, $\mathbb{T}^n$, formam uma base de $k[x_1, \ldots, x_n]$ como espaço vectorial, para determinarmos uma base para $k[x_1, \ldots, x_n]/I$ basta considerarmos as classes de equivalência de todos os monómios $\mathbf{x} \in \mathbb{T}^n$ tais que $\mathrm{LT}(g_i)$ não divide $\mathbf{x}$ para todo o $i = 1, \ldots, t$. Os geradores da base de $k[x_1, \ldots, x_n]/I$ poderão alterar dependendo da relação de ordem em que é calculada a base de Gröbner mas a dimensão da base é sempre a mesma.

vii. Caso estejamos na posse de uma base finita para $k[x_1, \ldots, x_n]/I$, $\{\psi_1, \ldots, \psi_n\}$, e G fosse uma base de Gröbner de I, para obtermos a tabuada da multiplicação em $k[x_1, \ldots, x_n]/I$ basta calcular a forma normal do produto dos vários representantes. Obteríamos portanto uma tabuada deste género:

$\times$	ψ_1	ψ_2	$\ldots$	ψ_n
ψ_1	$N_G(\psi_1^2)$	$N_G(\psi_1 \cdot \psi_2)$	$\ldots$	$N_G(\psi_1 \cdot \psi_n)$
ψ_2	$N_G(\psi_1 \cdot \psi_2)$	$N_G(\psi_2^2)$	$\ldots$	$N_G(\psi_2 \cdot \psi_n)$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
ψ_n	$N_G(\psi_1 \cdot \psi_n)$	$N_G(\psi_2 \cdot \psi_n)$	$\ldots$	$N_G(\psi_n^2)$

Tabela 4.1: Tabuada da multiplicação em $k[x_1, \ldots, x_n]/I$ com base $\{\psi_1, \ldots, \psi_n\}$

4.1.2 Exemplos de cada aplicação

i. Vejamos então o exemplo de um cálculo de uma base de Gröbner. Queremos calcular a base de Gröbner do ideal $I = \langle p, q \rangle$ onde $p = x^2 - y$ e $q = x + y^2$, na ordem lexicográfica. Começamos com $G = (p, q)$ e por calcular o S-polinómio:

$$\begin{aligned} S(p,q) &= \frac{x^2(x^2-y)}{x^2} - \frac{x^2(x+y^2)}{x} \\ &= x^2 - y - x^2 - xy^2 \\ &= -xy^2 - y \end{aligned}$$

O resto da divisão de $S(p, q)$ por G é $\overline{S(p,q)}^G = y^4 - y = s$. Temos agora que $G = (p, q, s)$. Calculemos então $S(p, s)$ e $S(q, s)$.

$$\begin{aligned} S(p,s) &= \frac{x^2y^4(x^2-y)}{x^2} - \frac{x^2y^4(y^4-y)}{y^4} \\ &= x^2y^4 - y^5 - x^2y^4 + x^2y \\ &= -x^2y - y^5 \end{aligned}$$

$$\begin{aligned} S(q,s) &= \frac{xy^4(x+y^2)}{x} - \frac{xy^4(y^4-y)}{y^4} \\ &= xy^4 + y^6 - xy^4 + xy \\ &= xy + y^6 \end{aligned}$$

Verifica-se que $\overline{S(p,s)}^G = 0$ e que $\overline{S(q,s)}^G = 0$ pelo que $G = \{x^2-y, x+y^2, y^4-y\}$ é uma base de Gröbner para I. No entanto não é uma base reduzida visto que $\mathrm{LT}(x^2-y) \in \langle \mathrm{LT}(G-\{x^2-y\})\rangle$. Pelo Lema 4 temos que $G-\{x^2-y\}$ será ainda uma base de Gröbner para I. Temos então a nossa base de Gröbner $G = \{x+y^2, y^4-y\}$. Caso utilizássemos o algoritmo melhorado de Buchberger, tínhamos imediatamente que, como tanto p e s e q e s são pares de polinómios relativamente primos, $\overline{S(p,s)}^G = 0$ e que $\overline{S(q,s)}^G = 0$, não sendo necessário calcular estas reduções. A optimização do algoritmo poupa, neste caso, o cálculo de duas divisões.

Vejamos como a eliminação de Gauss é um caso particular das bases de Gröbner. Para isso considere-se o sistema S,

$$\begin{cases} 2x + y - z = 8 \\ -3x - y + 2z = -11 \\ -2x + y + 2z = -3 \end{cases}$$

A base de Gröbner na ordem lexicográfica do ideal associado aos polinómios de S é $\{1+z, -3+y, -2+x\}$ que corresponde exactamente à solução do sistema linear S.

Outro caso particular das bases de Gröbner é o algoritmo de Euclides para determinar o máximo divisor comum entre polinómios numa só variável. Vejamos um exemplo e, para isso, considere-se o seguinte conjunto de polinómios em $k[x]$:

$$\begin{cases} x^2 + 7x + 6 = 0 \\ x^2 - 5x - 6 = 0 \end{cases}$$

A base de Gröbner obtida é $\{x+1\}$, que é de facto o máximo divisor comum entre $x^2+7x+6 = (x+1)(x+6)$ e $x^2-5x-6 = (x+1)(x-6)$.

ii. Podemos agora usar este resultado para responder à questão, será que $h = x^5y^6 - x^5y^3 + x^5 - x^4 - x^3y^2 - x^3y$ pertence ao ideal I? Vamos aplicar o algoritmo da divisão pelos geradores da base de Gröbner e, caso o resto seja zero, a resposta será afirmativa. Após aplicarmos o algoritmo obtemos que $h = (x^5y^2 + x^3)\cdot(y^4-y) + (x^4 - x^3y^2 - x^3)\cdot(x+y^2) + 0$ pelo que h pertence de facto ao ideal I.

iii. Verificámos no Exemplo 2 que a superfície tangente da cúbica torcida era parametrizada

pelas seguintes equações

$$\begin{cases} x = t + u \\ y = t^2 + 2tu \\ z = t^3 + 3t^2u \end{cases}$$

que pode ser vista como uma variedade em $\mathbb{R}^5$ definida pelas equações

$$\begin{cases} x - t - u = 0 \\ y - t^2 - 2tu = 0 \\ z - t^3 - 3t^2u = 0 \end{cases}$$

Vamos proceder ao cálculo da base de Gröbner com a ordem lexicográfica definida por $t > u > x > y > z$. A base obtida é $G = \{-3x^2y^2 + 4y^3 + 4x^3z - 6xyz + z^2, 2uy^3 + xy^3 - 4x^2yz + 5y^2z - 2uz^2 - 2xz^2, -2uy^2 - xy^2 + 2uxz + 2x^2z - yz, uxy - x^2y + 2y^2 - uz - xz, 2ux^2 - 2x^3 - 2uy + 3xy - z, u^2 - x^2 + y, t + u - x\}$. Tem-se portanto que $G \cap \mathbb{R}[x, y, z] = -3x^2y^2 + 4y^3 + 4x^3z - 6xyz + z^2$ é a equação da que define a menor variedade que contém a superfície tangente à cúbica torcida.

iv. Considerem-se os ideais $I = \langle x^2 + y^3 + 2y, yx^3 + 3xy\rangle$ e $J = \langle y^3x + x^4 + 1, yx^2 + 2x\rangle$. Vamos tentar determinar se $I = J$ e, para isso, procedemos ao cálculo das respectivas bases de Gröbner reduzidas na ordem *grevlex*. Estas são $G_I = \{x^2 + 2y + y^3, 3xy + x^3y, 3x^3 + x^5\}$ e $G_J = \{2 + xy, x^3 - \frac{y}{2} + y^3, -2x^2 - \frac{y^2}{2} + y^4\}$. Uma vez que as bases reduzidas não são iguais os ideais gerados também não o são, pelo que $I \neq J$.

vi. Considere-se o ideal $I = \langle x^4 + 1, xy - 1\rangle \subset \mathbb{R}[x, y]$. Queremos determinar uma base para o espaço vectorial $\mathbb{R}[x, y]/I$. Para isso considerem-se a bases de Gröbner de I na ordem lexicográfica com $x > y$ e na ordem inversa por graus lexicográfica também com $x > y$ que são respectivamente $G_{lex} = \{x + y^3, y^4 + 1\}$ e $G_{grevlex} = \{xy - 1, x^2 + y^2, y^3 + x\}$. Tem-se então que uma base para $\mathbb{R}[x, y]/I$ segundo G_{lex} é $\mathcal{B}_{lex} = \{1, y, y^2, y^3\}$ e a outra base é $\mathcal{B}_{grevlex} = \{1, x, y, y^2\}$. Como podemos observar, as duas bases de $\mathbb{R}[x, y]/I$ são distintas mas verifica-se que $\dim \mathcal{B}_{grevlex} = 4 = \dim \mathcal{B}_{grevlex}$.

vii. Considerando o exemplo anterior, vamos construir uma tabela de multiplicação em $\mathbb{R}[x, y]/\langle x^4 + 1, xy - 1\rangle$ tomando para isso a base de Gröbner na ordem *grevlex* com $x > y$, $G_{grevlex} = \{xy - 1, x^2 + y^2, y^3 + x\}$. Tem-se que o produto dos representantes canónicos de cada classe é o representante canónico do produto.

$\times$	1	x	y	y^2
1	1	x	y	y^2
x	x	$-y^2$	1	y
y	y	1	y^2	$-x$
y^2	y^2	y	$-x$	-1

Tabela 4.2: Tabuada da multiplicação em $\mathbb{R}[x, y]/\langle x^4 + 1, xy - 1\rangle$

Vejamos como as entradas da tabuada foram preenchidas:

- o representante do produto de x por y é dado por $N_G(xy) = 1$ pois $xy = 1 \cdot (xy - 1) + 1$;

- pela mesma ordem de ideias temos que $N_G(x^2) = -y^2$ pois $x^2 = 1 \cdot (x^2 + y^2) - y^2$;
- $N_G(xy^2) = y$ pois $xy^2 = y \cdot (xy - 1) + y$;
- $N_G(y^3) = -x$ pois $y^3 = 1 \cdot (y^3 + x) - x$;
- $N_G(y^4) = -1$ pois $y^4 = y \cdot (y^3 + x) + (-1) \cdot (xy - 1) - 1$;

Observação: Vejamos como uma base de Gröbner, e a sua computação, se pode tornar muito complexa dependendo da relação de ordem utilizada. Consideremos para isso o ideal $I = \langle x^5 + y^4 + z^3 - 1, x^3 + y^2 + z^2 - 1\rangle$ e a respectiva base de Gröbner nas ordens *lex*, *grlex* e *grevlex*, definindo sempre $x > y > z$. Utilizando o algoritmo que implementámos em *Mathematica* obtivemos os seguintes resultados:

Resultados obtidos				
		Tempos de Execução (referentes a 10 observações)		
Ordem	Nº de geradores	Tempo Médio (s)	Tempo máximo (s)	Tempo mínimo (s)
lex	7	203.8063	214.6406	197.5000
grlex	5	4.2906	4.3750	4.2500
grevlex	4	3.8718	3.9063	3.8438

É de notar que apesar do número de geradores ser "aceitável"para qualquer uma das ordens, estes polinómios chegam a ter 53 termos (caso da ordem *lex*).

4.2 Aplicações à Teoria de Grafos

Nesta secção mostramos como as Bases de Gröbner podem ser aplicadas para resolver problemas de outras áreas da matemática como é o caso da teoria de grafos. Assumindo que apenas trabalhamos com grafos simples, isto é, sem lacetes ou arestas duplas, e denotando por v o número de vértices e por a o número de arestas de um grafo, vamos determinar se um certo grafo $\mathcal{G}$ é ou não $n-$colorável. Queremos com isto dizer que podemos colorir os v vértices de $\mathcal{G}$ com n cores de modo a que vértices adjacentes tenham cores diferentes. Vamos tentar resolver este problema codificando as relações entre os vértices com polinómios.

Considere-se $\zeta = e^{\frac{2\pi i}{n}} \in \mathbb{C}$ uma raíz-n da unidade. Note-se que $\mathbb{C}$ é um corpo algebricamente fechado. Representamos as n cores que pretendemos usar pelas n raízes-n da unidade, $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ e codificamos os vértices de $\mathcal{G}$ como as variáveis $x_1, \ldots, x_v$. A cada vértice teremos de lhe atribuir uma das cores, ou seja,

$$x_i^n - 1 = 0 \text{ para } 1 \leq i \leq v. \tag{1}$$

Além disso, se dois vértices estão ligados por uma aresta, terão de ter cores distintas e como,

$$\begin{aligned} & x_i^n = x_j^n \\ \Leftrightarrow\ & x_i^n - x_j^n = 0 \\ \Leftrightarrow\ & (x_i - x_j)(x_i^{n-1} + x_i^{n-2}x_j + \ldots + x_i x_j^{n-2} + x_j^{n-1}) = 0 \end{aligned}$$

e quando os vértices têm cores diferentes temos que $(x_i - x_j) \neq 0$ e logo temos de ter apenas a segunda parcela

$$x_i^{n-1} + x_i^{n-2}x_j + \ldots + x_i x_j^{n-2} + x_j^{n-1} = 0. \tag{2}$$

Note-se que esta expressão é a soma de todos os monómios em x_i e x_j de grau $n-1$. Considere-se agora o ideal $I \subset \mathbb{C}[x_1, \ldots, x_v]$ gerado pelos polinómios de (1) e pelos polinómios de (2) quando dois vértices x_i e x_j forem adjacentes. Tem-se então que

$$I = \{x_i^n - 1 : 1 \leq i \leq v\} \cup \{(x_i^{n-1} + x_i^{n-2}x_j + \ldots + x_i x_j^{n-2} + x_j^{n-1}) : x_i \text{ é adjacente a } x_j\}.$$

Uma coloração de $\mathcal{G}$ com n cores é um ponto em $\mathbf{V}(I)$ e temos, pelo *Nullstellensatz* fraco, que $\mathbf{V}(I) \neq \emptyset$ sse $I \neq \mathbb{C}[x_1, \ldots, x_v]$, ou seja:

Teorema 15. *Um grafo simples $\mathcal{G}$ é n-colorável sse $\boldsymbol{V}(I) \neq \emptyset$, onde I é o ideal com $v + a$ polinómios que considerámos anteriormente.*

Como vimos anteriormente, $\mathbf{V}(I) \neq \emptyset$ sse $1 \notin G$ onde G é uma base de Gröbner do ideal I e disto tiramos um corolário imediato do teorema anterior:

Corolário 5. *Um grafo simples $\mathcal{G}$ é n-colorável sse $1 \notin G$, onde G é uma base de Gröbner de I e onde I é o ideal com $v + a$ polinómios que considerámos anteriormente.*

Vejamos agora um exemplo prático destes teoremas e considere-se para isso o seguinte grafo $\mathcal{H}$:

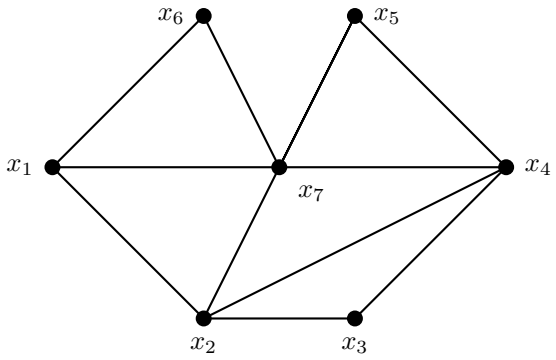


Figura 4.1: Grafo $\mathcal{H}$

Vejamos se $\mathcal{H}$ pode ser colorido com 3 cores. O ideal que temos de encontrar está em $\mathbb{C}[x_1, \ldots, x_7]$ uma vez que o grafo $\mathcal{H}$ tem sete vértices. Vamos considerar para o efeito as três cores 1, ζ e ζ^2, onde $\zeta = e^{\frac{2\pi i}{3}}$. Para construir o ideal associado a este problema temos de, para cada vértice x_i acrescentar ao ideal o polinómio $x_i^3 - 1$ e além destes, para cada dois vértices adjacentes x_i e x_j juntamos ao ideal o polinómio $x_i^2 + x_i x_j + x_j^2$. Temos portanto que o ideal é

$$I = \{x_i^3 - 1 : 1 \leq i \leq 7\} \cup \{x_i^2 + x_i x_j + x_j^2 : (i,j) \in \mathcal{A}\},$$

onde $\mathcal{A} = \{(1,2), (1,7), (1,6), (2,3), (2,4), (2,7), (3,4), (4,5), (4,7), (5,7), (6,7)\}$. A base de Gröbner associada a este ideal é $G = \{-1+x_7^3, x_6^2+x_6x_7+x_7^2, x_5-x_6, x_4+x_6+x_7, x_3-x_7, x_2-x_6, x_1+x_6+x_7\}$ e logo existe uma maneira de colorir $\mathcal{H}$ com três cores. Além disso os polinómios de G dão-nos as relações necessárias para obtermos uma coloração explícita.

Como obtivemos um polinómio numa só variável, $x_7^3 - 1$, x_7 é a variável à qual atribuímos cor primeiro, por exemplo $x_7 = 1$. Em seguida vemos que $x_6 \neq x_7$ e atribuímos por exemplo $x_6 = \zeta$ uma vez que $x_6^2 + x_6x_7 + x_7^2 \in G$ e este polinómio é zero sse $x_6 \neq x_7$. Em seguida temos que x_2 e x_5 também têm de ser iguais a ζ pois $x_5 - x_6, x_2 - x_6 \in G$ e além disso $x_3 = 1$ pois $x_3 - x_7 \in G$. Finalmente temos que x_1 e x_4 terão de ser iguais entre si mas diferentes de x_6 ou x_7 por causa dos polinómios $x_4 + x_6 + x_7, x_1 + x_6 + x_7 \in G$. Obtivemos assim uma coloração $\chi(\mathcal{H}) = \{1 \rightsquigarrow \{x_3, x_7\}, \zeta \rightsquigarrow \{x_2, x_5, x_6\}, \zeta^2 \rightsquigarrow \{x_1, x_4\}\}$ que é única a menos de permutação das cores.

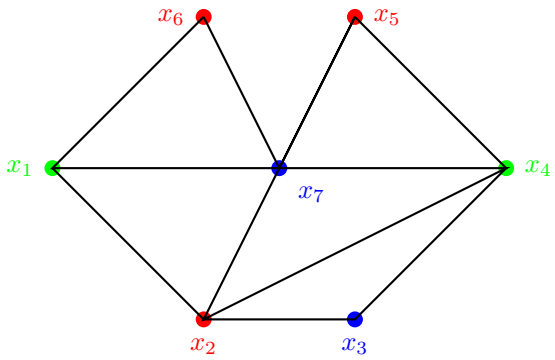


Figura 4.2: Grafo $\mathcal{H}$ colorido com 3 cores.

No entanto, se adicionarmos uma aresta entre os vértices x_5 e x_6 a $\mathcal{H}$ obtemos um novo grafo $\mathcal{H}'$ e verificamos que o novo ideal associado é $I' = I \cup \{x_5^2 + x_5x_6 + x_6^2\}$ e cuja base de Gröbner associada é $G' = \{1\}$ donde se conclui que $\mathcal{H}'$ já não é 3-colorável.

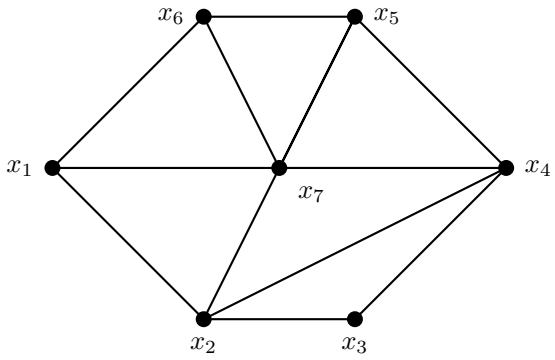


Figura 4.3: Grafo $\mathcal{H}'$ já não é 3-colorável.

4.3 Aplicações à Robótica

Nesta secção veremos como as bases de Gröbner podem ser aplicadas a áreas da engenharia, mais precisamente da robótica.

Vamos apenas considerar uma classe específica de braços robóticos, os chamados planares. Estes são braços robóticos cujas articulações podem ser apenas de dois tipos:

- articulações giratórias;

- articulações extensíveis.

As articulações giratórias permitem uma rotação relativa das secções ligadas à articulação. Já as extensíveis permitem que uma secção do braço robótico "estique" ou "encolha".

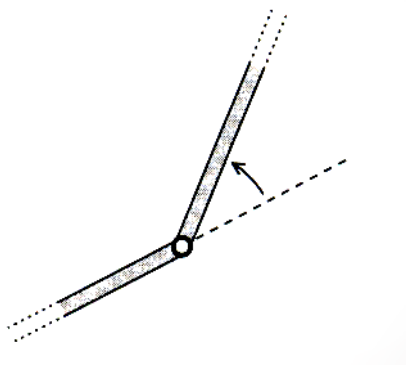


Figura 4.4: Articulação giratória

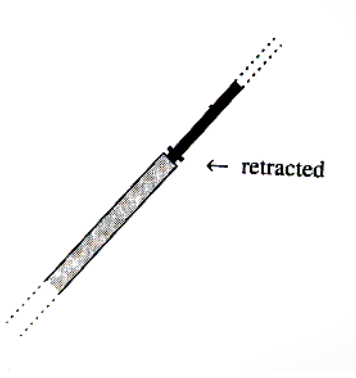


Figura 4.5: Articulação extensível

Considere-se o seguinte braço robótico planar:

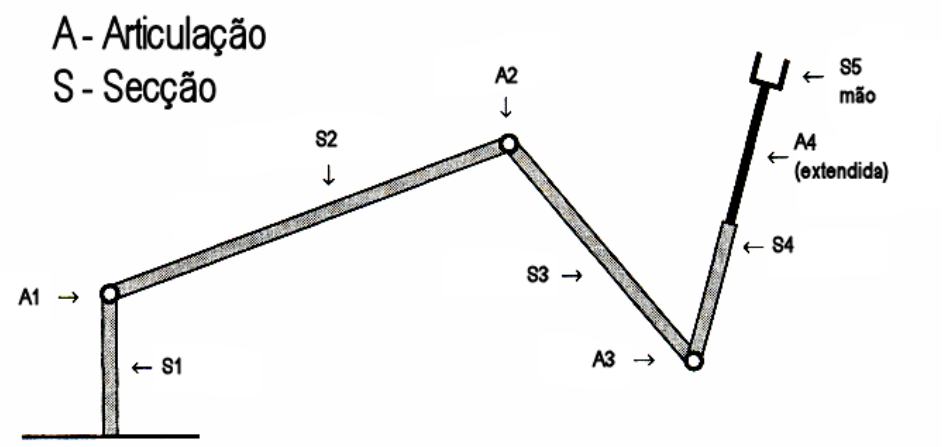


Figura 4.6: Braço robótico com articulações giratórias e extensível

Note-se como as secções e articulações estão numeradas por ordem crescente desde a secção que está fixa ao chão, S1, até à última secção (a mão), S5. Em geral, dada uma articulação giratória que ligue as secções i e $i+1$, uma descrição desta pode ser dada pelo ângulo (anti-horário) entre o segmento i ao $i+1$. Ou seja, todas as posições duma articulação giratória podem ser parametrizadas pelo círculo $\mathbb{S}^1$. De modo semelhante, as posições de uma articulação extensível são dadas por um intervalo $I = [l_0, l_t]$ onde l_0, l_t denotam o comprimento mínimo e máximo da articulação, respectivamente. Assim, dado um braço robótico planar com g articulações giratórias e p articulações extensíveis designamos $\mathcal{A} = \underbrace{\mathbb{S}^1 \times \ldots \times \mathbb{S}^1}_{g \text{ vezes}} \times I_1 \times \ldots \times I_p$ por *espaço das configurações*.

Podemos também pensar nas possíveis disposições da mão robótica: dado um sistema de eixos no plano podemos representar as posições da mão como pontos $(a, b) \in U \subset \mathbb{R}^2$. Além disso, a orientação da mão é determinada por um ângulo de $\mathbb{S}^1$. Deste modo definimos o *espaço operacional* como $\mathcal{O} = U \times \mathbb{S}^1$.

Como apenas uma posição do actuador está definida por um conjunto de configurações das articulações, podemos construir uma aplicação $f : \mathcal{A} \longrightarrow \mathcal{O}$ que relaciona a configuração das articulações do braço com a posição do actuador.

Uma vez que já descrevemos as possíveis configurações das articulações e do actuador do braço robótico podemos tentar resolver dois problemas:

- dar uma descrição explícita da posição do actuador em termos dos ângulos e comprimentos das secções, ou seja determinar a aplicação f explicitamente;
- dada uma posição da mão, c, determinar uma, caso exista, disposição do braço onde a mão está na posição dada, ou seja, determinar um $j \in \mathcal{A}$ tal que $f(j) = c$.

O primeiro, simples de resolver, é também conhecido como Cinemática Directa ou *Forward Kinematic Problem*; já o segundo problema conhecido como *Inverse Kinematic Problem* é de resolução mais complexa e é muito estudado uma vez que tem aplicações à criação de animação 2D, 3D, jogos virtuais e muitas outras áreas. A título de exemplo, se um desenhador 3D quer colocar um boneco com a mão numa certa posição, o que este faz é colocar a mão nessa posição e

através de software de cinemática inversa o computador determina uma posição viável do braço e corpo do boneco para suportar a mão nessa posição. Imagine-se o que seria para o animador 3D ter de regular a posição de todas as articulações do corpo para obter a mão na posição desejada.

4.3.1 Cinemática Directa

Como vimos anteriormente este problema consiste em, dada uma descrição das articulações do braço robótico obter a posição da mão do mesmo. Também vimos anteriormente que a primeira secção do braço está fixa e, por isso, não pode rodar nem esticar. Deste modo, começamos por colocar um sistema de eixos de $\mathbb{R}^2$ com a origem coincidente com a primeira articulação. Chamamos a este sistema de coordenadas o *sistema global* de coordenadas. Além deste, em cada articulação giratória, numerada i, vamos construir um novo sistema de coordenadas local, (x_{i+1}, y_{i+1}), centrando a origem desses novos eixos na articulação i. O semi-eixo positivo de x_{i+1} está alinhado com a secção $i+1$ do braço e o eixo y_{i+1} fica colocado normal a este. Note-se que para $i \geq 2$ as coordenadas em (x_i, y_i) da articulação i são $(l_i, 0)$ onde l_i é o comprimento da secção i.

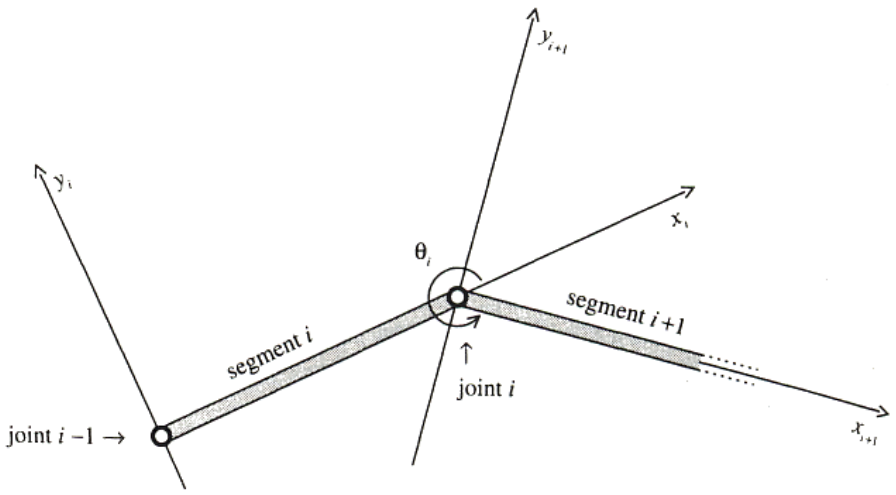


Figura 4.7: Exemplo dos vários sistemas de eixos usados

O nosso objectivo é agora determinar as coordenadas no sistema de eixos (x_i, y_i) dadas as coordenadas de um ponto no sistema (x_{i+1}, y_{i+1}). Considere-se então θ_i como o ângulo anti-horário entre o eixo-x_i e o eixo-x_{i+1}. Para obtermos as coordenadas em (x_i, y_i) de um ponto em (x_{i+1}, y_{i+1}), digamos (a_{i+1}, b_{i+1}), apenas precisamos de aplicar uma rotação de ângulo θ_i e uma translação pelo vector $(l_i, 0)$. Ou seja, temos que,

$$\begin{bmatrix} a_i \\ b_i \end{bmatrix} = \begin{bmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{bmatrix} \cdot \begin{bmatrix} a_{i+1} \\ b_{i+1} \end{bmatrix} + \begin{bmatrix} l_i \\ 0 \end{bmatrix}$$

ou ainda

$$\begin{bmatrix} a_i \\ b_i \\ 1 \end{bmatrix} = A_i \cdot \begin{bmatrix} a_{i+1} \\ b_{i+1} \\ 1 \end{bmatrix} = \begin{bmatrix} \cos\theta_i & -\sin\theta_i & l_i \\ \sin\theta_i & \cos\theta_i & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a_{i+1} \\ b_{i+1} \\ 1 \end{bmatrix}$$

Vejamos um exemplo prático e, para isso, considere-se o seguinte braço robótico:

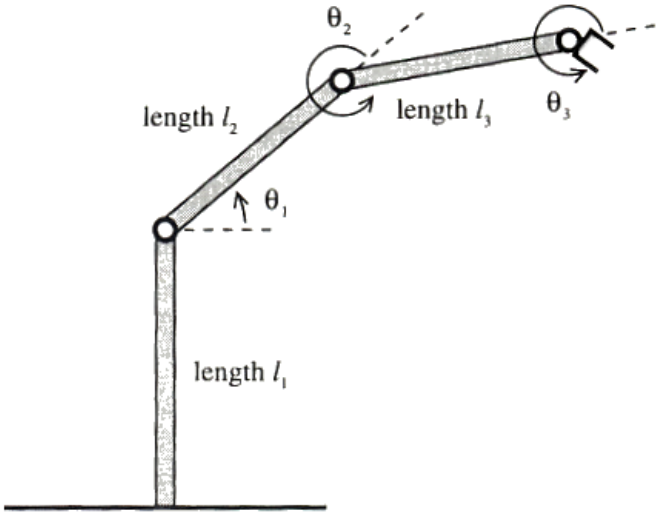


Figura 4.8: Braço robótico com 3 articulações giratórias

Começando por pontos no sistema de eixos (x_4, y_4) queremos determinar as suas coordenadas no sistema de eixos global, (x_1, y_1). Para isso, aplicamos o raciocínio anterior, notando que

$$A_1 = \begin{bmatrix} \cos\theta_1 & -\sin\theta_1 & 0 \\ \sin\theta_1 & \cos\theta_1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Assim, e construindo A_2 e A_3 como vimos, temos que partindo de um ponto em (x_4, y_4) e retrocedendo para (x_3, y_3), continuando deste modo obtemos os pontos em (x_1, y_1). Ou seja,

$$\begin{bmatrix} x_1 \\ y_1 \\ 1 \end{bmatrix} = A_1 \cdot A_2 \cdot A_3 \cdot \begin{bmatrix} x_4 \\ y_4 \\ 1 \end{bmatrix}$$

Realizando os cálculos temos que

$$\begin{bmatrix} x_1 \\ y_1 \\ 1 \end{bmatrix} = \begin{bmatrix} \cos(\theta_1+\theta_2+\theta_3) & -\sin(\theta_1+\theta_2+\theta_3) & l_3\cos(\theta_1+\theta_2)+l_2\cos\theta_1 \\ \sin(\theta_1+\theta_2+\theta_3) & \cos(\theta_1+\theta_2+\theta_3) & l_3\sin(\theta_1+\theta_2)+l_2\sin\theta_1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_4 \\ y_4 \\ 1 \end{bmatrix}$$

e como no sistema de eixos (x_4, y_4) as coordenadas da mão são $(0, 0)$ temos que

$$\begin{bmatrix} x_1 \\ y_1 \\ 1 \end{bmatrix} = \begin{bmatrix} l_3 \cos(\theta_1 + \theta_2) + l_2 \cos\theta_1 \\ l_3 \sin(\theta_1 + \theta_2) + l_2 \sin\theta_1 \\ 1 \end{bmatrix}$$

Isto determina a posição do actuador. Já a orientação deste é dada pelo ângulo entre o eixo-x_1 e o eixo-x_4, que é simplesmente $\theta_1 + \theta_2 + \theta_3$.

Assim, a aplicação que pretendíamos obter, $f : \mathcal{A} \longrightarrow \mathcal{O}$, é simplesmente dada por

$$f(\theta_1, \theta_2, \theta_3) = \begin{bmatrix} l_3 \cos(\theta_1 + \theta_2) + l_2 \cos\theta_1 \\ l_3 \sin(\theta_1 + \theta_2) + l_2 \sin\theta_1 \\ \theta_1 + \theta_2 + \theta_3 \end{bmatrix}$$

4.3.2 Cinemática Inversa

Propusémo-nos no início do capítulo a resolver dois problemas: determinar uma aplicação explícita que dadas as posições das articulações nos desse a posição do actuador do braço robótico e o respectivo problema inverso, dada uma posição do actuador, determinar configurações dos vários segmentos do braço que colocasse o actuador nessa posição. O primeiro problema foi resolvido na secção anterior e as única ferramentas utilizadas foram álgebra linear, nomeadamente matrizes de rotação. Para resolvermos o segundo problema já vamos utilizar bases de Gröbner.

Seja (x, y) um ponto de $\mathbb{R}^2$ e o uma orientação para a mão. Se tivermos $c = ((x, y), o)$ temos que c é um possível ponto do espaço operacional do braço robótico, $\mathcal{O}$. O nosso problema reduz-se a determinar, caso exista, a imagem inversa por f do ponto c, $f^{-1}(c)$, onde $f : \mathcal{A} \longrightarrow \mathcal{O}$ é a aplicação definida anteriormente.

Uma vez que este problema é de difícil resolução vamos apenas analisar a situação um caso particular, o braço robótico com três articulações giratórias apresentado na secção anterior.

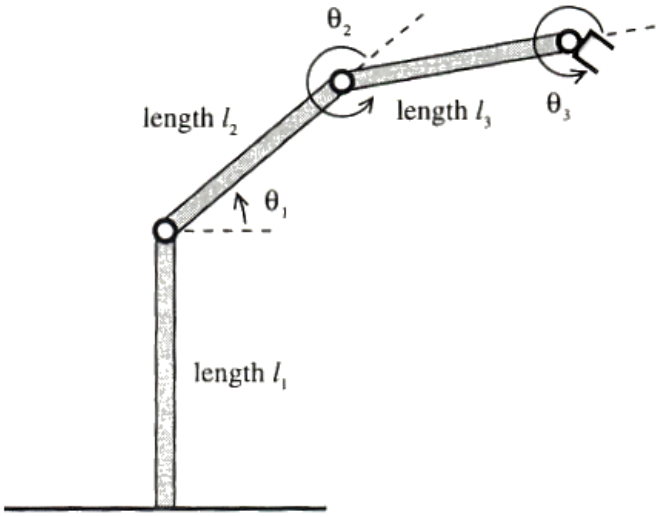


Figura 4.9: Braço robótico com 3 articulações giratórias

Vimos anteriormente que a aplicação explícita que resolvia o problema da cinemática directa deste problema era

$$f(\theta_1, \theta_2, \theta_3) = \begin{bmatrix} l_3 \cos(\theta_1 + \theta_2) + l_2 \cos\theta_1 \\ l_3 \sin(\theta_1 + \theta_2) + l_2 \sin\theta_1 \\ \theta_1 + \theta_2 + \theta_3 \end{bmatrix}$$

Antes de prosseguirmos necessitamos de transformar esta função numa aplicação polinomial. Isto é necessário pois vamos precisar de calcular bases de Gröbner e apenas o podemos fazer com funções polinomiais. Uma maneira de resolver isto é: uma vez que o seno e o coseno parametrizam a circunferência podemos fazer, para cada $i = 1, 2, 3$:

$$c_i = \cos\theta_i$$

$$s_i = \sin\theta_i$$

restringido a $c_i^2 + s_i^2 - 1 = 0$. Assim, e utilizando as fórmulas trigonométricas para a adição de ângulos temos que as coordenadas (x, y) da mão robótica são dadas por

$$\begin{bmatrix} l_3(c_1c_2 - s_1s_2) + l_2c_1 \\ l_3(s_1c_2 + s_2c_1) + l_2s_1 \end{bmatrix}$$

Podemos também observar que neste específico braço robótico, a mão pode estar orientada numa qualquer direcção uma vez que a sua articulação é giratória. Por isto vamos apenas analisar uma maneira de determinar ângulos das articulações para a posicionar numa certa posição.

Da fórmula obtida acima para a posição da mão temos que os possíveis pontos (a, b) de $\mathbb{R}^2$ em que esta pode estar são dados pelo seguinte sistema de equações polinomiais:

$$\begin{aligned} a &= l_3(c_1c_2 - s_1s_2) + l_2c_1 \\ b &= l_3(s_1c_2 + s_2c_1) + l_2s_1 \\ 0 &= c_1^2 + s_1^2 - 1 \\ 0 &= c_2^2 + s_2^2 - 1 \end{aligned}$$

Para resolvermos este sistema calculamos a base de Gröbner do ideal associado na ordem lexicográfica com $c_2 > s_2 > c_1 > s_1$. Obtemos a seguinte base:

$$\begin{aligned} & c_2 - \frac{a^2 + b^2 - l_2^2 - l_3^2}{2l_2l_3} \\ & s_2 + \frac{a^2 + b^2}{al_3}s_1 - \frac{a^2b + b^3 + b(l_2^2 - l_3^2)}{2a_2l_2l_3} \\ & c_1 + \frac{bs_1}{a} - \frac{a^2 + b^2 + l_2^2 - l_3^2}{2al_2} \\ & s_1^2 - \frac{a^2b + b^3 + b(l_2^2 - l_3^2)}{l_2(a^2 + b^2)}s_1 + \frac{(a^2 + b^2)^2 + (l_2^2 - l_3^2)^2 - 2a^2(l_2^2 + l_3^2) + 2b^2(l_2^2 - l_3^2)}{4l_2^2(a^2 + b^2)} \end{aligned}$$

De imediato podemos assumir que $l_2 \neq 0, l_3 \neq 0$ e vamos também assumir por agora que $a \neq 0$ e $a^2 + b^2 \neq 0$, de modo a não termos problemas com os denominadores. Vamos também *especializar* o sistema para o caso particular em que $l_2 = l_3 = 1$. Podia acontecer que os polinómios

da base de Gröbner não ficassem definidos nesta situação. Caso isso acontecesse, teríamos de fazer a substituição no sistema original e recalcular a base de Gröbner. Obtivemos portanto o seguinte conjunto de polinómios:

$$\begin{aligned}
&c_2 - \frac{a^2+b^2-2}{2} \\
&s_2 + \frac{a^2+b^2}{a}s_1 - \frac{a^2b+b^3}{2a} \\
&c_1 + \frac{b}{a}s_1 - \frac{a^2+b^2}{2a} \\
&s_1^2 - bs_1 + \frac{(a^2+b^2)^2-4a^2}{4(a^2+b^2)}
\end{aligned}$$

Resolvendo a última equação para s_1 temos que

$$s_1 = \frac{b}{2} \pm \frac{|a|\sqrt{4-(a^2+b^2)}}{2\sqrt{a^2+b^2}}$$

As soluções desta equação são reais sse $0 < a^2+b^2 \leq 4$. Geometricamente isto faz todo o sentido: uma vez que impusemos que $l_2 = l_3 = 1$, é quando as duas secções estão alinhadas que podem chegar mais longe, neste caso à circunferência de raio 2. Assim, faz sentido que os possíveis pontos em que a mão do braço robótico pode chegar estejam todos dentro do círculo de raio 2, ou seja que $a^2+b^2 \leq 4$. Após obtermos s_1 basta ir substituindo no resto das equações. Vejamos um exemplo: queremos determinar os ângulos θ_1 e θ_2 de modo a que o actuador deste mesmo braço esteja em $(1,0)$. Da última equação e substituindo temos que

$$\begin{aligned}
s_1 &= \frac{\sqrt{3}}{2}, -\frac{\sqrt{3}}{2} \\
c_1 &= -\frac{1}{2} \\
s_2 &= -s_1 \\
c_2 &= -\frac{1}{2} \\
\therefore\ \theta_1 &= -\theta_2 = \pm\frac{\pi}{3}
\end{aligned}$$

Esta solução era esperada pois a secção 1 e 2 do braço e o vector que vai de $(0,0)$ para $(1,0)$ formam um triângulo equilátero.

Quando $a = b = 0$ o actuador está coincidente com a articulação 1. A nossa base de Gröbner não está definida nesta situação mas existem soluções. Existem até infinitas – como assumimos que $l_2 = l_3$ fazendo $\theta_2 = \pi$, ou seja, sobrepondo a secção 3 à secção 2, seja qual for θ_1, o actuador estará em $(0,0)$.

Caso $a = 0$ mas $b \neq 0$ temos problemas com os denominadores da base de Gröbner. Neste caso teremos de fazer as substituições antes do cálculo da base de Gröbner. A nova base é então:

$$\begin{aligned}
&c_2 - \frac{b^2-2}{2} \\
&s_2 - bc_1 \\
&c_1^2 + \frac{b^2-4}{4} \\
&s_1 - \frac{b}{2}
\end{aligned}$$

Apesar de ser um problema interessante e de resolução teoricamente simples recorrendo às bases de Gröbner, estudar o caso geral deste problema torna-se muito complexo por duas razões: pode dar-se o caso em que a especialização das bases de Gröbner para valores específicos não esteja definida e a base de Gröbner para o problema torna-se muito extensa para uma análise directa do problema. Ainda assim, mesmo trabalhando num caso particular, foi necessária a divisão do problema em vários casos (exactamente por causa do problema da especialização) e o recurso a software de manipulação algébrica.

Capítulo 5

Implementação no *Mathematica 7*

```
LT[p_, ord_, v_] := MonomialList[p, v, ord][[1]]

S[w_, ord_, v_] :=
 Expand[With[{lt1 = LT[w[[1]], ord, v], lt2 = LT[w[[2]], ord, v]},
   With[{lcm = PolynomialLCM[lt1, lt2]},
    lcm/lt1*w[[1]] - lcm/lt2*w[[2]]]]]

DivQ[f_, g_] := Variables[Denominator[g/f]] == {}

Divisao = Function[{w, f, ord, v},
   Module[{l, r, s, p, i, divq},
    s = Length[w];
    l = Table[0, {i, 1, s}];
    r = 0;
    p = f;
    While[Not[p === 0],
     i = 1;
     divq = False;
     While[i <= s && divq == False,
      If[DivQ[LT[w[[i]], ord, v], LT[p, ord, v]],
       l =
        Delete[Insert[l, l[[i]] + LT[p, ord, v]/LT[w[[i]], ord, v],
          i], i + 1];
       p = Expand[p - (LT[p, ord, v]/LT[w[[i]], ord, v]*w[[i]])];
       divq = True,
       i++]];
     If[divq == False,
      r = r + LT[p, ord, v];
      p = p - LT[p, ord, v]];
     ];
    {l, r}]];
```

```
Resto = Function[{f, w, ord, v},
   Module[{r, s, p, i, divq},
    s = Length[w];
    r = 0;
    p = f;
    While[Not[p === 0],
     i = 1;
     divq = False;
     While[i <= s && divq == False,
      If[DivQ[LT[w[[i]], ord, v], LT[p, ord, v]],
       p = Expand[p - (LT[p, ord, v]/LT[w[[i]], ord, v]*w[[i]])];
       divq = True,
       i++]];
     If[divq == False,
      r = r + LT[p, ord, v];
      p = p - LT[p, ord, v]];
     ];
    r]];

reduz[f_, ord_, v_] :=
 If[NumberQ[LT[f, ord, v][[1]]], Expand[f/LT[f, ord, v][[1]]], f]

Minimiza = Function[{g, ord, v}, Module[{i, r, s, l},
    i = 1;
    s = Length[g];
    r = g;
    l = {};
    While[i <= s,
     If[Or @@ (DivQ[LT[#, ord, v], LT[r[[i]], ord, v]] & /@
         Delete[r, i]),
      l = Append[l, {i}]];
     i = i + 1];
    reduz[#, ord, v] & /@ Delete[r, l]]];

Buchberger = Function[{w, ord, v}, Module[{g, loust, p, r},
    g = w;
    loust = Subsets[g, {2}];
    While[loust != {},
     p = First[loust];
     loust = Rest[loust];
     If[Not[(1 ===
         PolynomialGCD[LT[p[[1]], ord, v], LT[p[[2]], ord, v]])],
      r = Resto[S[p, ord, v], g, ord, v];
      If[Not[r === 0],
```

```
        loust = Join[loust, Tuples[{g, {r}}]];
        g = Join[g, {r}]]]];
    Minimiza[g, ord, v]]];

crit = Function[{g, o, v, B, T, s}, Module[{l, i, j},
    l = 1;
    While[l < s,
     If[MemberQ[B, {l, s}],
      i = 1;
      While[i < s,
       If[MemberQ[Join[B, T], {i, l}] && MemberQ[B, {i, s}],
        If[
         DivQ[LT[g[[l]], o, v],
          PolynomialLCM[LT[g[[i]], o, v], LT[g[[s]], o, v]]],
         B = DeleteCases[B, {i, s}]]];
       i = i + 1]];
     l = l + 1];
    i = 1;
    While[i < s,
     If[MemberQ[B, {i, s}],
      j = i + 1;
      While[j < s,
       If[MemberQ[B, {j, s}] && MemberQ[B, {i, j}],
        If[
         DivQ[LT[g[[s]], o, v],
          PolynomialLCM[LT[g[[i]], o, v], LT[g[[j]], o, v]]],
         B = DeleteCases[B, {i, j}]]];
       j = j + 1]];
     i = i + 1];
    B]];


Buchcrit = Function[{w, ord, v}, Module[{g, T, B, i, s, loust, p, r},
    g = w;
    s = Length[w];
    T = {};
    B = {{1, 2}};
    i = 2;
    While[i < s,
     B = Join[B, Table[{z, i + 1}, {z, 1, i}]];
     B = crit[g, ord, v, B, T, s];
     i = i + 1];
    While[B != {},
     p = First[B];
     B = Rest[B];
```

```
     T = Join[T, p];
     If[Not[(1 ===
         PolynomialGCD[LT[g[[p[[1]]]], ord, v],
          LT[g[[p[[2]]]], ord, v]])],
      r = Resto[S[{g[[p[[1]]]], g[[p[[2]]]]}, ord, v], g, ord, v];
      If[Not[r === 0],
       g = Join[g, {r}];
       s = s + 1;
       B = Join[B, Table[{z, s}, {z, 1, s - 1}]];
       B = crit[g, ord, v, B, T, s]]]];
    Minimiza[g, ord, v]]];

Buchbergerz = Function[{w, ord, v}, Module[{g, loust, p, r},
    g = w;
    loust = Subsets[g, {2}];
    While[loust != {},
     p = First[loust];
     loust = Rest[loust];
     r = Resto[S[p, ord, v], g, ord, v];
     If[Not[r === 0],
      loust = Join[loust, Tuples[{g, {r}}]];
      g = Join[g, {r}]]];
    Minimiza[g, ord, v]]];
```

Capítulo 6

Conclusão e outras considerações

6.1 Conclusão

Apesar do nome, a teoria das bases de Gröbner foi desenvolvida por Bruno Buchberger, cujo orientador de tese era sim Wolfgang Gröbner. Estava-se no ano de 1965 mas muitas das ideias apresentadas por Buchberger já tinham sido apresentadas ou discutidas por Euclides (com o algoritmo para o cálculo do máximo divisor comum de polinómios numa variável), Gauss, Macaulay ou Hironaka, que desenvolveu as *Standard Basis* em 1964. A grande contribuição de Buchberger foi não só analisar uma estrutura interessante do ponto de vista teórico, mas apresentar um algoritmo que calcula explicitamente as bases de Gröbner. Os dois exemplos ilustrados aqui, sobre grafos e robótica, foram pela primeira vez mencionados por David Bayer, na sua tese de doutoramento, em 1982.

Definitivamente as bases de Gröbner são uma poderosa ferramenta para resolver os mais variados problemas, mas vimos por exemplo no caso da robótica que tínhamos de analisar cada caso especificamente, caso contrário teríamos bases de Gröbner com demasiados geradores tornando assim o problema muito difícil de resolver.

Na nossa opinião as bases de Gröbner são bastante eficazes para resolver problemas de existência de solução – como no exemplo da coloração de grafos. Vimos neste caso que a resposta (sim ou não) era imediata, mas caso quiséssemos obter a coloração explícita já se tornaria um problema complicado pois teríamos de analisar todas as relações codificadas na base de Gröbner. Para grafos muito grandes tornar-se-ia também um problema de muito difícil resolução.

Ainda assim, pensamos que as bases de Gröbner são um tópico da matemática muito interessante e com inúmeras aplicações, tanto dentro como fora da matemática, tornando-se uma ferramenta muito poderosa, quando aliada a outras áreas como a análise numérica, para a resolução de sistemas de equações polinomiais.

6.2 Outras considerações

Além dos melhoramentos apresentados para o algoritmo de Buchberger podem também ser acrescentadas funções heurísticas para a escolha dos pares (i, j) no último algoritmo que vimos, entre as quais a *sugar* (consultar [7]). Estas estratégias optimizam o algoritmo de Buchberger tentando evitar o cálculo de divisões desnecessárias e, uma vez que são o passo mais moroso do algoritmo,

melhorar a eficiência deste.

Como pudemos ver na secção *Aplicações à álgebra e à geometria*, o cálculo de bases de Gröbner pode ser computacionalmente dispendioso em certas relações de ordem, nomeadamente na lexicográfica. Para uma certa classe de ideais (zero-dimensionais), Faugère *et al.* sugeriram o seguinte para tentar ultrapassar estes problemas: calcular a base de Gröbner para uma ordem pouco dispendiosa (computacionalmente falando) como a *grevlex* e depois tentar converter esta base para a ordem pretendida. Este processo chamado *Conversão de bases de Gröbner* pode ser aprofundado em [3].

Um processo semelhante a este mas que resulta para qualquer tipo de ideais e não apenas para ideais de dimensão zero foi obtido por Collart *et al.* e designa-se por *passeios de Gröbner*. O artigo onde este conceito é introduzido pela primeira vez é [4].

Além destes métodos alternativos para calcular bases de Gröbner (que ainda utilizam o algoritmo de Buchberger) e calculam *a priori* uma base numa ordem pouco dispendiosa computacionalmente e depois traduzem-na para outra ordem, Faugère apresenta em [5] e [6] novos algoritmos (o F_4 e o F_5) que dão uso a uma versão muito alterada do algoritmo de Buchberger e a ferramentas da álgebra linear. Estes algoritmos apresentam grande eficiência computacional, e o F_5 foi o primeiro algoritmo a conseguir calcular uma base de Gröbner de um certo ideal que pertence a uma classe de ideais muito complexos de calcular (ideais cíclicos).

Como vimos as bases de Gröbner permitem, em certos casos, resolver sistemas de equações polinomiais. Por isto, muitos problemas de engenharia que eram resolvidos aproximando-os por equações lineares, podem agora ser melhor aproximados utilizando polinómios e depois usando as bases de Gröbner para os resolver. Uma aplicação bastante interessante é na indústria do petróleo: devido à complexa distribuição do petróleo nos jazigos a quantidade total de petróleo extraída depende tanto do número de furos de extracção como da quantidade extraída em cada furo. Devido a tudo isto, normalmente a quantidade extraída é da ordem dos 10% da quantidade total de petróleo existente. Modelando este sistema com equações polinomiais e resolvendo-o com bases de Gröbner e métodos numéricos, a companhia *Shell* prevê que consiga agora atingir os 30% de petróleo extraído. Este projecto chamado *Algebraic Oil* é um acordo entre a Universidade de Passau, Alemanha, e a Shell e pode ser aprofundado em http://www.algebraic-oil.uni-passau.de/.

Uma lista com outras interessantes aplicações das bases de Gröbner que não mencionámos pode ser encontrada em http://moodle.risc.jku.at/file.php/65/main.pdf.

Actualmente Bruno Buchberger mantém actualizada toda a bibliografia sobre bases de Gröbner e tópicos relacionados em http://www.ricam.oeaw.ac.at/Groebner-Bases-Bibliography/.

Lista de Algoritmos

Bibliografia

[1] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties and Algorithms*. Springer, 2nd Edition, 1996.

[2] M. Ricou, R. Loja Fernandes, *Introdução à Álgebra*. IST Press, 2004.

[3] J. Faugère, P. Gianni, D. Lazard and T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*. J. Symbolic Comput. **16**, 329-344, 1993.

[4] S. Collart, M. Kalkbrenner, and D. Mall, *Converting bases with the Gröbner walk*. J. Symbolic Comp. **24**, 465-469, 1997.

[5] J. Faugère, *A new efficient algorithm for computing Gröbner bases (F4)*. Journal of Pure and Applied Algebra 139, 61-88, 1999.

[6] J. Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*. Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation ISSAC, 75-83, 2002.

[7] A. Giovini , T. Mora , G. Niesi , L. Robbiano , C. Traverso, *"One sugar cube, please"or selection strategies in the Buchberger algorithm*. Proceedings of the 1991 international symposium on Symbolic and algebraic computation, 49-54, 1991.

[8] W. Adams, P. Loustaunau, *An introduction to Gröbner Bases*, vol. 3 of Graduate Studies in Mathematics. American Mathematical Society, 1994.

[9] David Bayer, *The Division Algorithm and the Hilbert Scheme*, Ph.D. Thesis, Harvard University, Cambridge, MA, 1982.

[10] http://www.scholarpedia.org/article/Groebner_basis.