FABRICIO ALVES OLIVEIRA

Códigos Parametrizados Afins

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2014

FABRICIO ALVES OLIVEIRA

Códigos Parametrizados Afins

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria Algébrica.

Orientador: Prof. Dr. Victor Gonzalo Lopez Neumann.

UBERLÂNDIA - MG
2014

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU , MG, Brasil

O48c
2014

Oliveira, Fabricio Alves, 1989-
Códigos parametrizados afins / Fabricio Alves Oliveira. - 2014.
54 p. : il.

Orientador: Victor Gonzalo Lopez Neumann.

Dissertação (mestrado) – Universidade Federal de Uberlândia, Programa de Pós-Graduação em Matemática.
Inclui bibliografia.

1. Matemática - Teses. 2. Códigos numéricos - Teses. 3. Bases de Gröbner - Teses. I. Neumann, Victor Gonzalo Lopez. II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Matemática. III.Título.

CDU: 51

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 152
Campus Santa Mônica, Uberlândia - MG, CEP 38400-902

ALUNO: Fabricio Alves Oliveira.

NÚMERO DE MATRÍCULA: 11212MAT003.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Códigos Parametrizados Afins.

ORIENTADOR: Prof. Dr. Victor Gonzalo Lopez Neumann.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 27 de fevereiro de 2014, às 10h00min, pela seguinte Banca Examinadora:

NOME	**ASSINATURA**
Prof. Dr. Victor Gonzalo Lopez Neumann UFU - Universidade Federal de Uberlândia	
Prof. Dr. Paulo Roberto Brumatti UNICAMP - Universidade Estadual de Campinas	
Prof. Dr. Cícero Fernandes de Carvalho UFU - Universidade Federal de Uberlândia	

Uberlândia-MG, 27 de fevereiro de 2014.

Agradecimentos

Agradeço primeiramente a Deus. Agradeço a agência CAPES pelo fornecimento da bolsa de pesquisa ao longo da Pós-Graduação e aos professores Cícero Fernandes de Carvalho e Victor Gonzalo Lopez Neumann pelos ensinamentos, conselhos e dedicação em todos os seminários. Ao Prof. Dr. Paulo Roberto Brumatti por ter aceito o convite para fazer parte da minha banca. Não poderia deixar de agradecer a todos meus amigos da Pós-Graduação, em especial Grégory e Rafaela que compartilharam todos os momentos ao longo desses dois anos. Ainda, agradeço aos meus companheiros de seminários, Cirilo, Nathália e Alexandre por toda atenção e observações que contribuíram para o enriquecimento deste trabalho. Finalmente, agradeço a pessoas muito especiais na minha vida, que me acompanharam nesse período e me deram forças para continuar, meus irmãos peruanos, Nathali e Eduard e ao meu amor Ricardo, por todo apoio e compreensão nos momentos em que estive ausente.

OLIVEIRA, F. A. *Códigos Parametrizados Afins*. 2014. 53 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho apresentamos uma classe especial de códigos lineares: os códigos parametrizados afins. Mostramos que esses códigos são de fácil construção e que, dado um código parametrizado afim, pode-se facilmente obter um código parametrizado projetivo equivalente a ele. Também estudamos algumas teorias que nos serviram como base teórica tais como: a teoria de Bases de Groebner e a Pegada de um ideal e alguns tópicos de geometria algébrica e álgebra comutativa. Este trabalho tem por objetivo principal obter os parâmetros básicos (comprimento, dimensão e distância mínima) dos códigos parametrizados afins e relacioná-los com os códigos parametrizados projetivos, assim como na referência [7]. Encerramos aplicando a teoria de Bases de Groebner a Pegada de um ideal para obter os parâmetros básicos do código parametrizado no toro afim.

Palavras-chave: Bases de Groebner; Pegada; Códigos Parametrizados; Comprimento, Distância mínima; Dimensão.

OLIVEIRA, F. A. *Parameterized Affine Codes*. 2014. 53 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work, we present a special class of linear codes: parameterized affine codes. We show that these codes are easy to construct and that given a parameterized affine code one can easily obtain an equivalent projective parameterized code equivalent to it. We also studied some topics which served as the theoretical foundations for the work, such as the theory of Groebner Bases, the footprint of an ideal and some topics of algebraic geometry and commutative algebra. This work has as main goal to obtain the basic parameters (length, dimension and minimum distance) of parameterized codes related and also to relate them to the projective parameterized codes, as done in [7]. We finish by applying the theory of Groebner Bases to the footprint of a certain ideal in order to obtain the basic parameters of the parameterized code over an affine torus.

Keywords: Groebner Bases; Footprint; Parameterized Codes; Length; Minimum Distance; Dimension.

Sumário

Introdução

A teoria dos códigos corretores de erros é um campo de pesquisa ativo em diversas áreas do conhecimento: matemática, computação, estatística, engenharia elétrica entre outras. Os códigos com capacidade para detectar e corrigir erros estão presentes no nosso cotidiano de várias maneiras, ao ouvir um CD de música, assistir a um filme em DVD, trocar informações entre computadores ou celulares. Esses códigos são utilizados quando as mensagens são transmitidas com algum tipo de ruído, ou seja, quando não transmitem a mensagem tal como foi enviada. Um código corretor de erros procura, essencialmente, acrescentar de uma forma organizada, alguns dados a cada informação que se pretende transmitir para que possa recuperar a informação detectando e corrigindo eventuais erros que possam surgir. A classe de códigos mais utilizadas na prática é a chamada classe dos códigos lineares.

Neste trabalho apresentamos um tipo especial de códigos lineares, os códigos parametrizados por monômios. Nosso objetivo principal é obter os parâmetros básicos do código parametrizado afim e mostrar que existe uma equivalência entre códigos parametrizados afins e projetivos. Para isso, utilizaremos alguns tópicos de álgebra linear, corpos finitos, geometria algébrica e álgebra comutativa.

No primeiro capítulo apresentamos alguns conceitos e resultados básicos da teoria de códigos lineares que serão utilizados nos capítulos 3 e 4. Relembramos os conceitos de código linear, comprimento, dimensão e distância mínima de um código linear, além de rever algumas propriedades a respeito de corpos finitos.

No capítulo 2, introduzimos a teoria de Bases de Groebner e a Pegada de um Ideal. Para isso relembramos algumas propriedades a respeito dos ideais monomiais e do algoritmo da divisão em um anel de polinômios em várias variáveis. Em seguida, demonstramos o Teorema da Base de Hilbert, definimos as bases de Groebner e apresentamos suas principais propriedades. Finalizamos o capítulo definindo a pegada de um ideal monomial e a relacionamos com as variedades afins, quando a pegada é um conjunto finito.

No capítulo 3, apresentamos os protagonistas deste trabalho: os códigos parametrizados afins. Mostramos que tais códigos são de fácil construção, estão intimamente relacionados com os códigos parametrizados projetivos e obtemos vários resultados interessantes a respeito desses dois códigos lineares.

No capítulo 4, utilizamos a teoria do capítulo 2 para obter os parâmetros básicos de uma família de códigos parametrizados: os códigos parametrizados no toro afim.

Fabricio Alves Oliveira
Uberlândia-MG, 27 de fevereiro de 2014.

Capítulo 1

Conceitos e Resultados Preliminares

Este capítulo tem por finalidade estabelecer conceitos, notações e resultados básicos da teoria de códigos lineares que serão utilizados nos capítulos seguintes. O leitor menos familiarizado com estes conceitos pode consultar qualquer livro sobre códigos corretores de erros, uma sugestão é a referência [6].

1.1 Códigos Lineares

Seja $K = \mathbb{F}_q$ um corpo finito com q elementos. Consideremos o K-espaço vetorial

$$K^n = \underbrace{K \times \cdots \times K}_{n \text{ vezes}}$$

de dimensão n, cujos elementos são n-uplas $a = (a_1, \cdots, a_n)$ com $a_i \in K, i = 1, \ldots, n$.

Definição 1.1.1 *Um subespaço vetorial* $C \subset K^n$ *é chamado* **código linear**.

Assim, todo código linear é, por definição, um K-espaço vetorial de dimensão finita.
De maneira usual, denotaremos por $\#A$ o número de elementos de um conjunto A.

Definição 1.1.2

(i) *Dados* $a = (a_1, \cdots, a_n)$ *e* $b = (b_1, \cdots, b_n) \in K^n$ *definimos a* **distância de Hamming** *entre* a *e* b *como sendo o número de coordenadas que estes elementos diferem, ou seja,*

$$d(a, b) := \#\{i : \ a_i \neq b_i, \ 1 \leq i \leq n\}.$$

(ii) *O* **peso** *de um elemento* $a = (a_1, \cdots, a_n) \in K^n$ *é definido como*

$$\omega(a) := \#\{i : \ a_i \neq 0\}.$$

Em outras palavras, temos que $\omega(a) = d(a, 0)$.

Observação 1.1.3 *A distância de Hamming é uma métrica sobre* K^n. *Mais especificamente, dados* a, b *e* c *em* K^n, *temos que:*

(i) $d(a, b) \geq 0$ *e vale a igualdade se e só se* $a = b$;

(ii) $d(a, b) = d(b, a)$;

(iii) $d(a,b) \leq d(a,c) + d(c,b)$;

(iv) $d(a,b) = d(a-b,0)$.

Definição 1.1.4 *Seja* $C \subset K^n$ *um código linear.*

(i) *Chamamos o número* n *de* **comprimento** *de* C *e a dimensão de* C *como* K*-espaço vetorial,* $\dim_K C$*, de* **dimensão** *do código* C.

(ii) *A* **distância mínima** *de* C *é o número*

$$\begin{aligned} d_{\min}(C) &= \min\{d(a,b) : a,b \in C \text{ e } a \neq b\} \\ &= \min\{\omega(a) = d(a,0) : a \in C, a \neq 0\}. \end{aligned}$$

O comprimento, a dimensão e a distância mínima constituem os *parâmetros básicos* de um código linear. A importância da distância mínima situa-se em relação à capacidade de correção de erros do código. Já a dimensão é uma medida da quantidade de informação que o código pode transportar. A importância do comprimento é que quanto maior for o código, mais energia deve ser gasta para transmitir cada palavra do código.

Assim, o código ideal teria uma dimensão e uma distância mínima grandes e um comprimento curto, mas estas condições não podem ser satisfeitas ao mesmo tempo. Mais especificamente, se um código linear tem comprimento n, dimensão k e distância mínima d, então vale a **cota de Singleton**:

$$d \leq n - k + 1.$$

Definição 1.1.5 *Seja* $C \subset K^n$ *um código linear de dimensão* k *e distância mínima* d*. Dizemos que* C *é um código* **MDS (Maximum Distance Separable)** *quando vale a igualdade na cota de Singleton, isto é, se* $d = n - k + 1$.

Observação 1.1.6 *Seja* $m = \dim_K C$ *e seja* $\{v_1, \ldots, v_m\}$ *uma base para* C*. Sabemos da Álgebra Linear que todo elemento de* C *se escreve de modo único na forma*

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m,$$

onde $\lambda_i \in K$*, para todo* $i = 1, \ldots, m$*. Pelo Princípio Multiplicativo de Contagem, segue que* C *possui* q^m *elementos, ou seja,* $\#C = q^m$.

Definição 1.1.7

(i) *Dizemos que uma função* $F : K^n \longrightarrow K^n$ *é uma* **isometria linear** *de* K^n *se ela é uma transformação linear que preserva distâncias de Hamming, ou seja,*

$$d(F(a), F(b)) = d(a,b), \text{ para todo } a, b \in K^n.$$

(ii) *Sejam* C *e* C' *dois códigos lineares em* K^n*. Dizemos que* C' *é* **equivalente** *a* C *quando existe uma isometria linear* F *de* K^n *tal que* $F(C) = C'$.

Decorre imediatamente da definição que dois códigos equivalentes têm os mesmos parâmetros.

1.2 Corpos Finitos

Seja p um número primo positivo em $\mathbb{Z}$. Vamos denotar por $\mathbb{Z}_p$ o corpo $\mathbb{Z}/p\mathbb{Z}$ e vamos denotar por $\mathbb{N} = \{0, 1, 2, \ldots\}$.
Seja F um corpo com elemento unidade 1. Vamos denotar

$$\underbrace{1 + \cdots + 1}_{n \text{ parcelas}} \text{ por } n \cdot 1.$$

Seja F um corpo finito com elemento unidade 1. Considere o conjunto

$$\Lambda_F = \{n \in \mathbb{N} : n \cdot 1 = 0\}.$$

Observe que $\{n \cdot 1 : n \in \mathbb{N}\} \subset F$. Como F é finito, existem $n_1 < n_2$ tais que $n_1 \cdot 1 = n_2 \cdot 1$. Logo, $(n_2 - n_1) \cdot 1 = 0$, com $n_2 - n_1 > 0$. Assim, $n_2 - n_1 \in \Lambda_F$ e, portanto $\Lambda_F \neq \emptyset$.

Definição 1.2.1 *A* **característica** *de um corpo finito* F *é o inteiro positivo*

$$\text{char}(F) = \min \Lambda_F.$$

Seja K um subcorpo de F. Como $\Lambda_K = \Lambda_F$, temos que $\text{char}(K) = \text{char}(F)$.

Recordemos algumas propriedades dos corpos finitos. Todas as demonstrações podem ser encontradas na referência [6].

Proposição 1.2.2 *Seja* F *um corpo finito de característica* p *e seja* $m = p^r$*, para algum* $r \in \mathbb{N}$*. Temos que:*

(a) p *é um número primo.*

(b) *Se* $n \in \mathbb{Z}$ *e* $a \in F$ *são tais que* $n \cdot a = 0$*, então* n *é múltiplo de* p *ou* $a = 0$*.*

(c) F *contém um subcorpo isomorfo a* $\mathbb{Z}_p$*. Em particular,* F *tem* p^n *elementos, para algum natural* n*.*

(d) $(a + b)^m = a^m + b^m$ *e* $(a - b)^m = a^m - b^m$*.*

Mais ainda, se F *possui* q *elementos, então*

(e) $a^{q-1} = 1$*, para todo* $a \in F^* = F \setminus \{0\}$*.*

(f) $a^{q^r} = a$*, para todo* $a \in F$ *e para todo* $r \in \mathbb{N}$*.*

O próximo teorema nos garante a existência de polinômios irredutíveis em $F[x]$, onde F é um corpo finito e a unicidade de corpos finitos com o mesmo número de elementos.

Teorema 1.2.3

(i) *Seja* F *um corpo finito. Para cada inteiro positivo* n*, existe pelo menos um polinômio irredutível de grau* n *em* $F[x]$*.*

(ii) *Dois corpos finitos com o mesmo número de elementos são isomorfos.*

Capítulo 2

Bases de Groebner e a Pegada de um Ideal

A teoria de bases de Groebner fornece uma abordagem uniforme para a resolução de uma ampla gama de problemas em geometria algébrica, álgebra comutativa e na teoria de ideais polinomiais. Essa teoria tem se mostrado uma ferramenta atraente em álgebra computacional, pois revela uma maneira simples de entender e de implementar algoritmos computacionais, fazendo com que ela seja aplicada em várias áreas da ciência e engenharia e não apenas pelos matemáticos.

2.1 Monômios e Ordens Monomiais

Definição 2.1.1 *Um* **monômio** *em* $x_1, \ldots, x_n$ *é um produto da forma* $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$*, onde todos os expoentes são inteiros não negativos. Vamos utilizar a notação multi-índice para monômios. Escreveremos* $x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$*, onde* $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$*. O* **grau** *desse monômio é a soma* $|\alpha| := \alpha_1 + \cdots + \alpha_n$*.*

Vamos denotar por $\mathcal{M}$ o conjunto de todos os monômios em $\mathbb{F}[x_1, \ldots, x_n]$.
Seja $\mathbb{F}$ um corpo. Um polinômio f em $\mathbb{F}[x_1, \ldots, x_n]$ é uma combinação linear de monômios com coeficientes em $\mathbb{F}$. Dessa forma podemos escrever

$$f = \sum_{\alpha} a_\alpha x^\alpha, \quad a_\alpha \in \mathbb{F},$$

que é uma soma sob um número finito de n-uplas $\alpha = (\alpha_1, \ldots, \alpha_n)$. Chamamos a_α de **coeficiente** do monômio x^α. Se $a_\alpha \neq 0$, então $a_\alpha x^\alpha$ é um **termo** de f. O **grau total** de f, denotado por $\deg(f)$, é o máximo $|\alpha|$ tal que $a_\alpha \neq 0$.

Definição 2.1.2

(i) *Sejam* $f_1, \ldots, f_s$ *polinômios em* $\mathbb{F}[x_1, \ldots, x_n]$*. Definimos o* **ideal gerado** *por* $f_1, \ldots, f_s$ *como sendo o conjunto*

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

Observe que este conjunto é, de fato, um ideal de $\mathbb{F}[x_1, \ldots, x_n]$*.*

(ii) *Chamamos um ideal* I *de* $\mathbb{F}[x_1,\dots,x_n]$ *de* **finitamente gerado** *se existem* $f_1,\dots,f_s \in \mathbb{F}[x_1,\dots,x_n]$ *tais que* $I = \langle f_1,\dots,f_s\rangle$*, e dizemos que* $\{f_1,\dots,f_s\}$ *é uma* **base** *para* I*.*

Definição 2.1.3 *Uma* **ordem monomial** $\preceq$ *em* $\mathcal{M} \subset \mathbb{F}[x_1,\dots,x_n]$ *é qualquer relação em* $\mathbb{N}^n$ *satisfazendo:*

(i) $\preceq$ *é uma ordem total em* $\mathbb{N}^n$*;*

(ii) *se* $\alpha \preceq \beta$ *em* $\mathbb{N}^n$ *e* $\gamma \in \mathbb{N}^n$*, então* $\alpha+\gamma \preceq \beta+\gamma$*;*

(iii) *todo subconjunto não vazio de* $\mathbb{N}^n$ *possui elemento mínimo em relação a* $\preceq$*.*

Vejamos dois exemplos de ordens monomiais:

Exemplo 2.1.4

(i) A *ordem lexicográfica* (com $x_n \preceq \cdots \preceq x_1$) é definida por $x^\alpha \preceq_{\text{lex}} x^\beta$ se $\alpha = \beta$ ou se a primeira entrada entrada diferente de zero da esquerda para direita de $\beta-\alpha$ for positiva. Assim, nós temos por exemplo que $x_2^{1000} \preceq_{\text{lex}} x_1$ e $x_1^2x_3^{2013} \preceq_{\text{lex}} x_1^2x_2$.

(ii) A *ordem lexicográfica graduada* (com $x_n \preceq \cdots \preceq x_1$) é definida por $x^\alpha \preceq x^\beta$ se $\alpha = \beta$ ou $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$ ou se $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ então $x^\alpha \preceq_{\text{lex}} x^\beta$, onde $\preceq_{\text{lex}}$ é a ordem lexicográfica, definida anteriormente.
Temos por exemplo que $x_1^3x_2^2 \preceq x_1x_2^2x_3^3$, pois o grau do primeiro é menor que o grau do segundo. E $x_1x_2x_3^5 \preceq x_1x_2^2x_3^4$, pois embora eles possuam o mesmo grau, temos que $x_1x_2x_3^5 \preceq_{\text{lex}} x_1x_2^2x_3^4$.

Definição 2.1.5 *Seja*

$$f = \sum_{i=1}^m a_i x^{\alpha_i} \in \mathbb{F}[x_1,\dots,x_n]$$

um polinômio não nulo, onde $a_i \in \mathbb{F}, a_i \neq 0$ *e* $x^{\alpha_i} \in \mathcal{M}$ *para todo* $i = 1,\dots,m$*, e seja* $\preceq$ *uma ordem monomial definida em* $\mathcal{M}$*. Então o* **multigrau** *de* f *(com respeito a* $\preceq$*) é dado por* $\text{mdeg}(f) := \max\{\alpha_i \in \mathbb{N}^n : i = 1,\dots,m\}$*, o* **monômio líder** *de* f *(com respeito a* $\preceq$*) é* $\text{lm}(f) := x^{\text{mdeg}(f)}$*, o* **coeficiente líder** *de* f *(com respeito a* $\preceq$*) é* $\text{lc}(f) := a_{\text{mdeg}(f)}$ *e o* **termo líder** *de* f *(com respeito a* $\preceq$*) é* $\text{lt}(f) := a_{\text{mdeg}(f)}x^{\text{mdeg}(f)}$*.*

Assim, por exemplo, se $f(x_1,x_2,x_3) = 4x_1^3x_2^4+5x_1x_3^8+2 \in \mathbb{R}[x_1,x_2,x_3]$ e nós considerarmos o conjunto dos monômios com a ordem lexicográfica, então temos que $\text{lm}(f) = x_1^3x_2^4$ e $\text{lt}(f) = 4x_1^3x_2^4$, por outro lado, se considerarmos a ordem graduada lexicográfica, teremos que $\text{lm}(f) = x_1x_3^8$ e $\text{lt}(f) = 5x_1x_3^8$.

Uma ferramenta importante na teoria de Bases de Groebner é a divisão de um polinômio por uma lista de polinômios não nulos.

Teorema 2.1.6 (Algoritmo da Divisão) *Considere uma ordem monomial* $\preceq$ *em* $\mathcal{M}$*. Seja* $G = (g_1,\dots,g_s)$ *uma* s*-upla ordenada de polinômios não nulos em* $\mathbb{F}[x_1,\dots,x_n]$*. Então, cada* $f \in \mathbb{F}[x_1,\dots,x_n]$ *pode ser escrito como*

$$f = q_1g_1 + \cdots + q_sg_s + r$$

onde $q_i, r \in \mathbb{F}[x_1,\dots,x_n]$*, e* $r = 0$ *ou nenhum monômio que aparece em* r *é múltiplo de* $\text{lm}(g_i)$*, para algum* $i \in \{1,\dots,s\}$*.*

Demonstração. Uma prova deste teorema poderá ser encontrada no capítulo 2 da referência [5]. □

É importante observar no algoritmo da divisão acima que se o resto r não é zero, então o monômio líder de r é menor ou igual do que o monômio líder de f. Além disso, uma importante propriedade do algoritmo da divisão em $K[x]$ não é sempre válida: a unicidade do resto.

2.2 Ideais Monomiais

Definição 2.2.1 *Um ideal* $I \subset \mathbb{F}[x_1, \ldots, x_n]$ *é um* **ideal monomial** *se existe um subconjunto não vazio* $A \subset \mathbb{N}^n$ *tal que*

$$I = \langle x^\alpha : \alpha \in A \rangle := \left\{ \sum_{\alpha \in B} f_\alpha x^\alpha : f_\alpha \in \mathbb{F}[x_1, \ldots, x_n],\ B \subset A \ \text{ é finito} \right\}.$$

Proposição 2.2.2 *Seja* $I = \langle x^\alpha : \alpha \in A \rangle$ *um ideal monomial. Então um monômio* $x^\beta \in I$ *se, e somente se,* x^α *divide* x^β *para algum* $\alpha \in A$.

Demonstração. ($\Rightarrow$) Seja $x^\beta \in I$. Então $x^\beta = \sum_{i=1}^{k} h_i x^{\alpha_i}$, onde $\alpha_i \in A$ e $h_i = \sum_{j=1}^{t_i} a_{ij} x^{\gamma_{ij}}$, $a_{ij} \in K$. Podemos supor que

$$x^\beta = (a_{11} x^{\gamma_{11}} x^{\alpha_1} + \cdots + a_{1t_1} x^{\gamma_{1t_1}} x^{\alpha_1}) + \cdots + (a_{k1} x^{\gamma_{k1}} x^{\alpha_k} + \cdots + a_{kt_k} x^{\gamma_{kt_k}} x^{\alpha_k})$$

logo o multigrau de algum monômio do lado direito é β.

($\Leftarrow$) Seja $\alpha \in A$ tal que $x^\beta = p x^\alpha$. Logo, $x^\beta \in I$. □

Dado um ideal $I \subset \mathbb{F}[x_1, \ldots, x_n]$, podemos definir o ideal dos termos líderes:

Definição 2.2.3 *Seja* I *um ideal em* $\mathbb{F}[x_1, \ldots, x_n]$*, com* $I \neq 0$.

(i) *O* **conjunto dos termos líderes** *dos elementos de* I *é dado por*

$$\mathrm{lt}(I) = \{ c x^\alpha : \exists f \in I \ \text{ tal que } \mathrm{lt}(f) = c x^\alpha \}.$$

(ii) *O* **ideal dos termos líderes** *de* I *é o ideal gerado pelos elementos de* $\mathrm{lt}(I)$ *e será denotado por* $\langle \mathrm{lt}(I) \rangle$.

Analogamente, definimos o **conjunto do monômios líderes de** I, $\mathrm{lm}(I)$, *e o* **ideal dos monômios líderes de** I, *denotado por* $\langle \mathrm{lm}(I) \rangle$.

Seja $I \neq 0$ um ideal finitamente gerado em $\mathbb{F}[x_1, \ldots, x_n]$, digamos $I = \langle f_1, \ldots, f_s \rangle$.
É claro que $\langle \mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s) \rangle \subset \langle \mathrm{lt}(I) \rangle$:
Seja $f \in \langle \mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s) \rangle$, então $f = g_1 \mathrm{lt}(f_1) + \cdots + g_s \mathrm{lt}(f_s)$, com $g_i \in \mathbb{F}[x_1, \ldots, x_n]$. Para cada $i \in \{1, \ldots, s\}$, temos $\mathrm{lt}(f_i) \in \mathrm{lt}(I) \subset \langle \mathrm{lt}(I) \rangle$. Assim, cada parcela de f pertence a $\langle \mathrm{lt}(I) \rangle$ e, *a fortiori* $f \in \langle \mathrm{lt}(I) \rangle$.

Lema 2.2.4 (Lema de Dickson) *Seja* $I = \langle x^\alpha : \alpha \in A \rangle$ *um ideal monomial em* $\mathbb{F}[x_1, \ldots, x_n]$. *Então* I *pode ser escrito da forma* $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$, *onde* $\alpha_1, \ldots, \alpha_s \in A$. *Em particular,* I *possui uma base finita.*

Demonstração. Uma prova do Lema de Dickson pode ser encontrada no capítulo 2 da referência [5]. □

Observação 2.2.5 *Em geral,* ***não*** *é verdade que* $\langle \mathrm{lt}(I)\rangle \subset \langle \mathrm{lt}(f_1),\ldots,\mathrm{lt}(f_s)\rangle$*:*
Seja $I = \langle f_1, f_2\rangle$*, onde* $f_1 = x^3 - 2xy$ *e* $f_2 = x^2y - 2y^2 + x$*, e considere a ordem lexicográfica graduada. Como* $x^2 = xf_2 - yf_1$*, temos que* $x^2 \in I$*. Assim,*

$$x^2 = \mathrm{lt}(x^2) \in \mathrm{lt}(I) \subset \langle \mathrm{lt}(I)\rangle.$$

Mas, $x^2 \notin \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2)\rangle$*, pois* $\langle \mathrm{lt}(f_1), \mathrm{lt}(f_2)\rangle = \langle x^3, x^2y\rangle$ *é um ideal monomial e* x^2 *não é múltiplo de* x^3 *nem de* x^2y*.*

Proposição 2.2.6 *Seja* $I \subset \mathbb{F}[x_1,\ldots,x_n]$ *um ideal, com* $I \neq 0$*. Então:*

(i) $\langle \mathrm{lt}(I)\rangle$ *é um ideal monomial.*

(ii) *Existem* $g_1,\ldots,g_t \in I$ *tais que* $\langle \mathrm{lt}(I)\rangle = \langle \mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)\rangle$*.*

Demonstração.

(i) Considere o ideal monomial $\langle \mathrm{lm}(g) : g \in I\backslash\{0\}\rangle$.
Observe que $\langle \mathrm{lm}(g) : g \in I\backslash\{0\}\rangle = \langle \mathrm{lt}(g) : g \in I\backslash\{0\}\rangle$, de fato:
Seja $f \in \langle \mathrm{lm}(g) : g \in I\backslash\{0\}\rangle$, então existe um subconjunto finito $A \subseteq I\backslash\{0\}$ tal que

$$f = \sum_{g\in A} a_g \mathrm{lm}(g) = \sum_{g\in A} a_g (\mathrm{lc}(g))^{-1}\mathrm{lc}(g)\mathrm{lm}(g) = \sum_{g\in A} a_g (\mathrm{lc}(g))^{-1}\mathrm{lt}(g),$$

logo, $f \in \langle \mathrm{lt}(g) : g \in I\backslash\{0\}\rangle$.
Agora seja $f \in \langle \mathrm{lt}(g) : g \in I\backslash\{0\}\rangle$, então existe um subconjunto finito $B \subseteq I\backslash\{0\}$ tal que

$$f = \sum_{g\in B} a_g \mathrm{lt}(g) = \sum_{g\in B} a_g \mathrm{lc}(g)\mathrm{lm}(g),$$

portanto, $f \in \langle \mathrm{lm}(g) : g \in I\backslash\{0\}\rangle$.
Como $\langle \mathrm{lt}(I)\rangle = \langle \mathrm{lt}(g) : g \in I\backslash\{0\}\rangle = \langle \mathrm{lm}(g) : g \in I\backslash\{0\}\rangle$, segue que $\langle \mathrm{lt}(I)\rangle$ é um ideal monomial.

(ii) Como $\mathrm{lt}(I)$ é um ideal monomial, pelo Lema de Dickson, existem $g_1,\ldots,g_t \in I$ tais que $\langle \mathrm{lt}(I)\rangle = \langle \mathrm{lm}(g_1),\ldots,\mathrm{lm}(g_t)\rangle$. Observe que $\langle \mathrm{lm}(g_1),\ldots,\mathrm{lm}(g_t)\rangle = \langle \mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)\rangle$, de fato: Dado $f \in \langle \mathrm{lm}(g_1),\ldots,\mathrm{lm}(g_t)\rangle$, temos que

$$f = \sum_{i=1}^{t} a_i \mathrm{lm}(g_i) = \sum_{i=1}^{t} a_i (\mathrm{lc}(g_i))^{-1}\mathrm{lc}(g_i)\mathrm{lm}(g_i) = \sum_{i=1}^{t} a_i (\mathrm{lc}(g_i))^{-1}\mathrm{lt}(g_i) \in \langle \mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)\rangle.$$

Dado $f \in \langle \mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)\rangle$, temos

$$f = \sum_{i=1}^{t} a_i \mathrm{lt}(g_i) = \sum_{i=1}^{t} a_i \mathrm{lc}(g_i)\mathrm{lm}(g_i) \in \langle \mathrm{lm}(g_1),\ldots,\mathrm{lm}(g_t)\rangle.$$

Portanto, $\langle \mathrm{lt}(I)\rangle = \langle \mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)\rangle$.

□

Observação 2.2.7 *Utilizando a notação da proposição anterior temos que*

$$\langle \mathrm{lt}(I)\rangle = \langle \mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)\rangle = \langle \mathrm{lm}(g_1),\ldots,\mathrm{lm}(g_t)\rangle = \langle \mathrm{lm}(I)\rangle.$$

Teorema 2.2.8 (Teorema da Base de Hilbert) *Todo ideal* $I \subset \mathbb{F}[x_1,\ldots,x_n]$ *é finitamente gerado, isto é, existem* $g_1,\ldots,g_t \in I$ *tais que* $I = \langle g_1,\ldots,g_t\rangle$.

Demonstração. Se $I = \{0\}$, nada a provar. Se $I \neq \{0\}$, sabemos que

$$\langle \mathrm{lt}(I)\rangle = \langle \mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)\rangle,$$

para alguns $g_1,\ldots,g_t \in I$. Vamos mostrar que $I = \langle g_1,\ldots,g_t\rangle$.
É claro que $\langle g_1,\ldots,g_t\rangle \subset I$. Seja $f \in I$. Aplicando o algoritmo da divisão para dividir f por $(g_1,\ldots,g_t)$, obtemos

$$f = a_1g_1 + \cdots + a_tg_t + r,$$

onde nenhum termo de r é divisível por nenhum dos $\mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)$.
Observe que $r = f - a_1g_1 - \cdots - a_tg_t$, e logo $r \in I$.
Se $r \neq 0$, então $\mathrm{lt}(r) \in \mathrm{lt}(I) \subset \langle \mathrm{lt}(I)\rangle = \langle \mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)\rangle$, logo $\mathrm{lt}(r)$ é divisível por algum $\mathrm{lt}(g_i)$, absurdo! Logo, $r = 0$.
Assim, podemos escrever $f = a_1g_1 + \cdots + a_tg_t$ e portanto, $f \in \langle g_1,\ldots,g_t\rangle$.
Isso mostra que $I = \langle g_1,\ldots,g_t\rangle$. □

2.3 Bases de Groebner

O conceito de bases de Groebner apareceu pela primeira vez na tese de doutorado do matemático austríaco Bruno Buchberger, publicada em 1965 (veja [2]). Seu orientador, Wolfgang Groebner, propôs o seguinte problema para sua tese: dado um ideal $I \subset \mathbb{F}[x_1,\ldots,x_n]$, encontrar uma base para $\mathbb{F}[x_1,\ldots,x_n]/I$ como um $\mathbb{F}$-espaço vetorial.

Quando estamos trabalhando com um anel de polinômios em uma única variável a resposta é conhecida: I é gerado por um certo polinômio de grau d (no caso em que $I \neq 0$) e $\{1 + I, x + I, \ldots, x^{d-1} + I\}$ forma uma base para $\mathbb{F}[x]/I$.

Agora, quando estamos trabalhando com um anel de mais de uma variável a situação muda radicalmente. Pelo Teorema da Base de Hilbert, nós sabemos que I é gerado por um número finito de polinômios, mas I não é necessariamente um ideal principal; mais ainda o anel quociente $\mathbb{F}[x_1,\ldots,x_n]/I$ pode ser um $\mathbb{F}$-espaço vetorial de dimensão infinita.

A ideia de Buchberger para solucionar o problema acima foi fixar uma ordem monomial em $\mathcal{M}$ e determinar um conjunto especial de geradores para I cuja propriedade principal é que as classes dos monômios que não são múltiplos de nenhum dos monômios líderes dos polinômios que estão nessa base especial, formam uma base para $\mathbb{F}[x_1,\ldots,x_n]/I$ como $\mathbb{F}$-espaço vetorial. Em 1976 Buchberger decidiu chamar essa base especial para I de "bases de Groebner" em virtude da influência das ideias de seu orientador em seu trabalho de tese (veja [3]).

Definição 2.3.1 *Seja* $I \subset \mathbb{F}[x_1,\ldots,x_n]$ *um ideal não nulo e fixe uma ordem monomial* $\preceq$ *em* $\mathcal{M}$. *Um conjunto* $\{g_1,\ldots,g_t\} \subset I$ *é uma* **base de Groebner** *para* I *(com respeito a* $\preceq$*) se*

$$\langle \mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)\rangle = \langle \mathrm{lt}(I)\rangle.$$

O lema a seguir nos fornece uma maneira elegante de definir uma base de Groebner para um ideal.

Lema 2.3.2 *O conjunto* $G = \{g_1,\ldots,g_t\} \subset I$ *é uma base de Groebner para* I *(com respeito a* $\preceq$*) se para todo* $f \in I, f \neq 0$ *temos que* $\mathrm{lm}(f)$ *é múltiplo de* $\mathrm{lm}(g_i)$ *para algum* $i \in \{1,\ldots,t\}$.

Demonstração. Seja $f \in I$, com $f \neq 0$, então

$$\mathrm{lm}(f) \in \langle \mathrm{lm}(I) \rangle = \langle \mathrm{lt}(I) \rangle \overset{\text{hip.}}{=} \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t) \rangle.$$

Como $\langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t) \rangle$ é um ideal monomial, segue que $\mathrm{lm}(f)$ é múltiplo de $\mathrm{lm}(g_i)$, para algum $i = 1, \ldots, t$. Por outro lado, é claro que $\langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle \subset \langle \mathrm{lt}(I) \rangle$. Vejamos que $\langle \mathrm{lt}(I) \rangle \subset \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle$. Como $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lm}(I) \rangle$, basta mostrar que $\langle \mathrm{lm}(I) \rangle \subset \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle$, ou seja, $\mathrm{lm}(I) \subset \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle$. Seja $f \in I, f \neq 0$. Por hipótese, existe $i \in \{1, \ldots, t\}$ tal que $\mathrm{lm}(f)$ é múltiplo de $\mathrm{lm}(g_i)$, logo $\mathrm{lm}(f) \in \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle$. Portanto, $\mathrm{lm}(I) \subset \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle$ como queríamos. □

Fixada uma ordem monomial, segue da Proposição 2.2.6 que todo ideal $I \subset \mathbb{F}[x_1, \ldots, x_n]$, com $I \neq \{0\}$, possui uma base de Groebner. Mais ainda, qualquer base de Groebner para um ideal I é uma base para I.
Vejamos algumas propriedades das bases de Groebner.

Proposição 2.3.3 *Seja* $G = \{g_1, \ldots, g_t\}$ *uma base de Groebner para um ideal* $I \subset \mathbb{F}[x_1, \ldots, x_n]$ *e seja* $f \in \mathbb{F}[x_1, \ldots, x_n]$. *Então existe um único* $r \in \mathbb{F}[x_1, \ldots, x_n]$ *com as seguintes propriedades:*

(i) *Nenhum termo de* r *é divisível por qualquer dos termos* $\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t)$.

(ii) *Existe* $g \in I$ *tal que* $f = g + r$.

Em particular, r *é o resto da divisão de* f *por* G*, não importando a ordem dos elementos de* G.

Demonstração. O algoritmo da divisão nos dá $f = a_1 g_1 + \cdots + a_t g_t + r$, onde r satisfaz (i). Para provar (ii), considere $g = a_1 g_1 + \cdots + a_t g_t \in I$. Basta provar a unicidade de r.
Suponha que $f = g + r = g' + r'$ satisfazendo (i) e (ii). Então,

$$r - r' = g' - g \in I.$$

Se tivermos $r \neq r'$, então

$$\mathrm{lt}(r - r') \in \langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle.$$

Logo, $\mathrm{lt}(r - r')$ é divisível por algum $\mathrm{lt}(g_i)$. Então $\mathrm{lm}(r - r')$ é divisível por $\mathrm{lt}(g_i)$. Por outro lado, como $\mathrm{lm}(r - r')$ é um monômio de r ou de r', não ocorre que $\mathrm{lm}(r - r')$ seja divisível por $\mathrm{lt}(g_i)$. Absurdo! Portanto, $r = r'$. □

Corolário 2.3.4 *Seja* $G = \{g_1, \ldots, g_t\}$ *uma base de Groebner para um ideal* $I \subset \mathbb{F}[x_1, \ldots, x_n]$ *e seja* $f \in \mathbb{F}[x_1, \ldots, x_n]$. *Então* $f \in I$ *se, e somente se, o resto da divisão de* f *por* G *é zero.*

Demonstração. ($\Leftarrow$) Se o resto é zero, é claro que $f \in I$.

($\Rightarrow$) Seja $f \in I$, então $f = f + 0$ satisfaz as duas condições da Proposição 2.3.3 Pela unicidade do resto, segue o resultado. □

Definição 2.3.5 *Sejam* $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ *polinômios não nulos.*

(i) *Se* $\mathrm{mdeg}(f) = \alpha$ *e* $\mathrm{mdeg}(g) = \beta$*, então seja* $\gamma = (\gamma_1, \ldots, \gamma_n)$*, onde* $\gamma_i = \max\{\alpha_i, \beta_i\}$ *para cada* i. *Dizemos que* x^γ *é o* **mínimo múltiplo comum** *de* $\mathrm{lm}(f)$ *e* $\mathrm{lm}(g)$*, e denotamos por* $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$.

(ii) *O* **S-polinômio** *de* f *e* g *é a combinação dada por*

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

Exemplo 2.3.6 *Sejam* $f = x^3y^2 - x^2y^3 + x$ *e* $g = 3x^4y + y^2$ *em* $\mathbb{R}[x,y]$ *com a ordem lexicográfica graduada. Então* $\gamma = (4,2)$*. Logo,*

$$\operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g)) = \operatorname{lcm}(x^3y^2, x^4y) = x^4y^2.$$

Assim, o S*-polinômio de* f *e* g *é dado por*

$$S(f,g) = \frac{x^4y^2}{x^3y^2}f - \frac{x^4y^2}{3x^4y}g = Xf - \frac{1}{3}Yg = -x^3y^3 + x^2 - \frac{1}{3}y^3.$$

Lema 2.3.7 *Seja* $\sum_{i=1}^{s} c_i f_i$ *com* $c_i \in \mathbb{F}$ *e* $\operatorname{mdeg}(f_i) = \delta \in \mathbb{N}^n$*, para todo* i*. Se* $\operatorname{mdeg}\left(\sum_{i=1}^{s} c_i f_i\right) < \delta$*, então* $\sum_{i=1}^{s} c_i f_i$ *é uma* $\mathbb{F}$*-combinação linear de* S*-polinômios* $S(f_j, f_k)$*, com* $1 \le j,k \le s$*. Além disso,* $\operatorname{mdeg}\left(S(f_j,f_k)\right) < \delta$*.*

Demonstração. Seja $d_i := \operatorname{lc}(f_i)$, assim $\operatorname{lc}(c_i f_i) = c_i d_i$. Como $\operatorname{mdeg}(f_i) = \delta, \forall i = 1,\dots,s$ e $\operatorname{mdeg}\left(\sum_{i=1}^{s} c_i f_i\right) < \delta$, temos que $\sum_{i=1}^{s} c_i d_i = 0$ (do contrário, teríamos $\operatorname{lt}\left(\sum_{i=1}^{s} c_i f_i\right) = \left(\sum_{i=1}^{s} c_i d_i\right) x^\delta$, logo $\operatorname{mdeg}\left(\sum_{i=1}^{s} c_i f_i\right) = \delta$, absurdo!).
Defina $p_i = \dfrac{f_i}{d_i}$ e observe que p_i tem coeficiente líder 1. Assim,

$$\begin{aligned}
\sum_{i=1}^{s} c_i f_i &= \sum_{i=1}^{s} c_i d_i p_i \\
&= c_1 d_1 p_1 + \cdots + c_s d_s p_s \\
&= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) \\
&\quad + (c_1 d_1 + \cdots + c_s d_s) p_s
\end{aligned}$$

Como $\operatorname{lm}(f_i) = x^\delta, \forall i = 1,\dots,s$, temos $\operatorname{lcm}(\operatorname{lm}(f_j), \operatorname{lm}(f_k)) = x^\delta$ para todo $i \in \{1,\dots,s\}$.
Observe que

$$S(f_j,f_k) = \frac{x^\delta}{lt(f_j)}f_j - \frac{x^\delta}{lt(f_k)}f_k = \frac{x^\delta}{d_j X^\delta}f_j - \frac{x^\delta}{d_k X^\delta}f_k = \frac{f_j}{d_j} - \frac{f_k}{d_k} = p_j - p_k.$$

Daí,

$$\sum_{i=1}^{s} c_i f_i = c_1 d_1 S(f_1,f_2) + (c_1 d_1 + c_2 d_2) S(f_2,f_3) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s) + 0 p_s.$$

Finalmente, como $\operatorname{lt}(p_i) = 1x^\delta, \forall i = 1,\dots,s$, temos que $\operatorname{mdeg}(S(f_j,f_k)) = \operatorname{mdeg}(p_j - p_k) < \delta$.
□

Vejamos agora um conhecido critério que nos permite decidir quando uma determinada base para um ideal é uma base de Groebner para ele.

Teorema 2.3.8 (Critério de Buchberger) *Sejam* $I \subset \mathbb{F}[x_1,\dots,x_n]$ *um ideal e* $G = \{g_1,\dots,g_t\}$ *uma base para* I*. Então,* G *é uma base de Groebner para* I *se e somente se para todos* $i \neq j$ *o resto na divisão de* $S(g_i,g_j)$ *por* G *(listada em alguma ordem) é zero.*

Demonstração. ($\Rightarrow$) Dados $i \neq j$, temos que

$$S(g_i, g_j) \in \langle g_1, \ldots, g_t \rangle = I.$$

Como G é uma base de Groebner para I temos que o resto na divisão de $S(g_i, g_j)$ por G é zero.

($\Leftarrow$) Para provar que $\langle lt(I) \rangle = \langle lt(g_1), \ldots, lt(g_t) \rangle$, basta mostrar que $lt(I) \subset \langle lt(g_1), \ldots, lt(g_t) \rangle$. Seja $f \in I \backslash \{0\}$. Como $I = \langle g_1, \ldots, g_t \rangle$, existem $h_1, \ldots, h_t \in \mathbb{F}[x_1, \ldots, x_n]$ tais que

$$f = h_1 g_1 + \cdots + h_t g_t. \tag{2.1}$$

Assim,

$$mdeg(f) \leq \max\{mdeg(h_i g_i) : 1 \leq i \leq t\}.$$

Seja $m(i) := mdeg(h_i g_i)$, para $i = 1, \ldots, t$, e defina

$$\delta = \max\{m(1), \ldots, m(t)\}.$$

Assim, $mdeg(f) \leq \delta$. Agora, considere todas as possíveis maneiras em que f pode ser expressada na forma (2.1). Para cada expressão nós obtemos um $\delta \in \mathbb{N}^n$. Seja S o conjunto formado por todos estes δ. Como a ordem monomial é uma boa ordem, S possui elemento mínimo, logo podemos escolher uma expressão (2.1) para f tal que δ é minimal. Escolhido este δ minimal, é verdade que $mdeg(f) = \delta$ (isto será provado!). Como $\delta = \max\{m(1), \ldots, m(t)\}$ temos que

$$mdeg(f) = \delta = m(i) = mdeg(h_i g_i)$$

para algum $i \in \{1, \ldots, t\}$. Assim, $lt(f)$ é múltiplo de $lt(h_i g_i)$ e $lt(h_i g_i)$ é múltiplo de $lt(g_i)$, logo $lt(f)$ é múltiplo de $lt(g_i)$, e portanto $lt(f) \in \langle lt(g_1), \ldots, lt(g_t) \rangle$, e isso mostra que G é uma base de Groebner para I.

Agora, resta provar que $mdeg(f) = \delta$. Suponha por absurdo que $mdeg(f) < \delta$. Podemos escrever

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i = \sum_{m(i)=\delta} (h_i g_i + lt(h_i) g_i - lt(h_i) g_i) + \sum_{m(i)<\delta} h_i g_i =$$

$$\sum_{m(i)=\delta} (lt(h_i) g_i + (h_i - lt(h_i)) g_i) + \sum_{m(i)<\delta} h_i g_i =$$

$$\sum_{m(i)=\delta} lt(h_i) g_i + \sum_{m(i)=\delta} (h_i - lt(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i.$$

Observe que a segunda soma tem $mdeg < \delta$, de fato

$$mdeg((h_i - lt(h_i)) g_i) = mdeg(h_i - lt(h_i)) + mdeg(g_i) <$$

$$mdeg(h_i) + mdeg(g_i) = mdeg(h_i g_i) = m(i) = \delta.$$

Assim, a segunda e a terceira soma tem $mdeg < \delta$. Como $mdeg(f) < \delta$, temos que a primeira soma também tem $mdeg < \delta$. Seja $lt(h_i) = c_i X^{\alpha(i)}$, então a primeira soma $\sum_{m(i)=\delta} lt(h_i) g_i = \sum_{m(i)=\delta} c_i X^{\alpha(i)} g_i$ tem exatamente a forma descrita no lema anterior, com $f_i = x^{\alpha(i)} g_i$, ou seja, $mdeg(f_i) = \delta$ para todo i e $mdeg\left(\sum_{m(i)=\delta} c_i f_i\right) < \delta$. Então, este lema garante que $\sum_{m(i)=\delta} c_i X^{\alpha(i)} g_i$

é uma K-combinação linear dos S-polinômios $S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k)$ e $\mathrm{mdeg}(S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k)) < \delta$. Observe que

$$S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k) = \frac{x^\delta}{x^{\alpha(j)}\mathrm{lt}(g_j)}x^{\alpha(j)}g_j - \frac{x^\delta}{x^{\alpha(k)}\mathrm{lt}(g_k)}x^{\alpha(k)}g_k = \frac{x^\delta}{\mathrm{lt}(g_j)}g_j - \frac{x^\delta}{\mathrm{lt}(g_k)}g_k =$$

$$\frac{x^\delta}{x^{\gamma_{jk}}}\frac{x^{\gamma_{jk}}}{\mathrm{lt}(g_j)}g_j - \frac{x^\delta}{x^{\gamma_{jk}}}\frac{x^{\gamma_{jk}}}{\mathrm{lt}(g_k)}g_k = \frac{x^\delta}{x^{\gamma_{jk}}}\left(\frac{x^{\gamma_{jk}}}{\mathrm{lt}(g_j)}g_j - \frac{x^{\gamma_{jk}}}{\mathrm{lt}(g_k)}g_k\right) = x^{\delta-\gamma_{jk}}S(g_j, g_k),$$

onde $x^{\gamma_{jk}} = \mathrm{lcm}(\mathrm{lm}(g_j), \mathrm{lm}(g_k))$. Então, existem constantes $c_{jk} \in K$ tais que

$$\sum_{m(i)=\delta} \mathrm{lt}(h_i)g_i = \sum_{j,k} c_{jk}x^{\delta-\gamma_{jk}}S(g_j, g_k). \tag{2.2}$$

Vejamos que $x^{\delta-\gamma_{jk}}$ é um monômio:
Seja $x^{\beta(i)} := \mathrm{lm}(g_i)$, para todo i. Como $\mathrm{mdeg}(x^{\alpha(i)}g_i) = \delta$ temos que $\delta = \alpha(i) + \beta(i)$ para todo i. Denotando $\alpha(i) = (\alpha_{i1}, \ldots, \alpha_{in})$ e $\beta(i) = (\beta_{i1}, \ldots, \beta_{in})$ temos que $\gamma_{j,k}$ é obtido de $\beta(j)$ e $\beta(k)$ da seguinte maneira:

$$\gamma_{j,k} = (\max\{\beta_{j1}, \beta_{k1}\}, \ldots, \max\{\beta_{jn}, \beta_{kn}\}).$$

Se $\delta = (\delta_1, \ldots, \delta_n)$, então $\delta_i \geq \max\{\beta_{ji}, \beta_{ki}\}$, para todo i, de fato, como $\delta = \alpha(j) + \beta(j)$ temos que $\delta_i = \alpha_{ji} + \beta_{ji} \geq \beta_{ji}$, e como $\delta = \alpha(k) + \beta(k)$, temos que $\delta_i = \alpha_{ki} + \beta_{ki} \geq \beta_{ki}$. Portanto, $\delta_i \geq \max\{\beta_{ji}, \beta_{ki}\}$, para todo i. Isso mostra que x^δ é múltiplo de $x^{\gamma_{jk}}$, e logo $x^{\delta-\gamma_{jk}}$ é um monômio.

Dividindo cada S-polinômio por $g_1, \ldots, g_t$, por hipótese o resto é zero, assim temos

$$S(g_j, g_k) = a_{1jk}g_1 + \cdots + a_{tjk}g_t = \sum_{i=1}^{t} a_{ijk}g_i$$

para alguns $a_{ijk} \in K[x_1, \ldots, x_n]$. O algoritmo da divisão também nos garante que para todos i, j, k temos

$$\mathrm{mdeg}(a_{ijk}g_i) \leq \mathrm{mdeg}(S(g_j, g_k)). \tag{2.3}$$

Daí,

$$x^{\delta-\gamma_{jk}}S(g_j, g_k) = x^{\delta-\gamma_{jk}}\sum_{i=1}^{t} a_{ijk}g_i = \sum_{i=1}^{t} b_{ijk}g_i$$

onde $b_{ijk} = x^{\delta-\gamma_{jk}}a_{ijk}$. Veja que

$$\mathrm{mdeg}(b_{ijk}g_i) = \mathrm{mdeg}(x^{\delta-\gamma_{jk}}a_{ijk}g_i) = \mathrm{mdeg}(x^{\delta-\gamma_{jk}}) + \mathrm{mdeg}(a_{ijk}g_i) \overset{(2.3)}{\leq}$$

$$\mathrm{mdeg}(x^{\delta-\gamma_{jk}}) + \mathrm{mdeg}(S(g_j, g_k)) = \mathrm{mdeg}(x^{\delta-\gamma_{jk}}S(g_j, g_k)) = \mathrm{mdeg}(S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k)) < \delta.$$

De (2.2) segue que

$$\sum_{m(i)=\delta} \mathrm{lt}(h_i)g_i = \sum_{j,k} c_{jk}x^{\delta-\gamma_{jk}}S(g_j, g_k) = \sum_{j,k} c_{jk}\left(\sum_i b_{ijk}g_i\right) = \sum_i \tilde{h}_i g_i.$$

Como $\mathrm{mdeg}(b_{ijk}g_i) < \delta$ segue que $\mathrm{mdeg}(\tilde{h}_i g_i) < \delta$ para todo i. Portanto, f se escreve como

$$f = \sum_i \tilde{h}_i g_i + \sum_{m(i)=\delta} (h_i - \mathrm{lt}(h_i))g_i + \sum_{m(i)<\delta} h_i g_i = p_1 g_1 + \cdots + p_t g_t$$

com $\mathrm{mdeg}(p_i g_i) < \delta$ para todo $i \in \{1, \ldots, t\}$. Logo,

$$\delta_0 := \max\{\mathrm{mdeg}(p_i g_i) : 1 \leq i \leq t\}$$

é tal que $\delta_0 \in S$ e $\delta_0 < \delta = \min S$, absurdo. □

Exemplo 2.3.9 *Sejam* $g_1 = y - x^2$ *e* $g_2 = z - x^3$ *em* $\mathbb{F}[x, y, z]$ *e considere o ideal* $I = \langle g_1, g_2 \rangle$. *Então,* $G = \{g_1, g_2\}$ *é uma base de Groebner para* I *com respeito à ordem lexicográfica com* $y > z > x$. *Para provar isso, considere o* S*-polinômio*

$$S(g_1, g_2) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = -zx^2 + xz^3.$$

Dividindo $S(g_1, g_2)$ *por* g_1, g_2 *obtemos*

$$-zx^2 + yx^3 = x^3 \cdot (y - x^2) + (-x^2) \cdot (z - x^3) + 0,$$

como o resto é zero, pelo Critério de Buchberger temos que $G = \{g_1, g_2\}$ *é uma base de Groebner para* I.

Agora, considere a ordem lexicográfica com $x > y > z$. *Neste caso, temos que*

$$S(g_1, g_2) = \frac{x^3}{-x^2}(-x^2 + y) - \frac{x^3}{-x^3}(-x^3 + z) = -xy + z.$$

Dividindo $S(g_1, g_2)$ *por* g_1, g_2 *obtemos*

$$-xy + z = 0 \cdot (-x^2 + y) + 0 \cdot (-x^3 + z) + (-xy + z).$$

Portanto, G *não é uma base de Groebner para* I.

Vamos denotar o resto na divisão de f pela s-upla ordenada $F = (f_1, \ldots, f_t)$ por $\overline{f}^F$.

Sabemos que todo ideal em $\mathbb{F}[x_1, \ldots, x_n]$ possui uma base de Groebner. Vejamos, agora um algoritmo que nos permite encontrar, de forma construtiva, uma base de Groebner para um ideal polinomial I a partir de uma base para I. Inicialmente, vejamos isto através de um exemplo:

Exemplo 2.3.10 *Considere o anel* $\mathbb{F}[x, y]$ *com a ordem lexicográfica graduada e seja* $I = \langle f_1, f_2 \rangle$, *onde* $f_1 = x^3 - 2xy$ *e* $f_2 = x^2y - 2y^2 + x$. *Dividindo* $S(f_1, f_2) = -x^2$ *por* $F = \{f_1, f_2\}$ *obtemos como resto*

$$\overline{S(f_1, f_2)}^F = -x^2 \neq 0.$$

Portanto, $F = \{f_1, f_2\}$ *não é uma base de Groebner para* I.

Seja $f_3 := -x^2$ *e considere agora* $F = \{f_1, f_2, f_3\}$. *Observe que*

$$\begin{aligned} &S(f_1, f_2) = -x^2, \\ &\overline{S(f_1, f_2)}^F = 0, \\ &S(f_1, f_3) = -2xy, \\ &\overline{S(f_1, f_3)}^F = -2xy \neq 0. \end{aligned}$$

Portanto, $F = \{f_1, f_2, f_3\}$ *não é uma base de Groebner para* I.

Seja $f_4 := -2xy$ *e considere agora* $F = \{f_1, f_2, f_3, f_4\}$. *Observe que*

$$\begin{aligned}\overline{S(f_1, f_2)}^F &= 0,\\ \overline{S(f_1, f_3)}^F &= 0,\\ \overline{S(f_1, f_4)}^F &= 0,\\ \overline{S(f_2, f_3)}^F &= -2y^2 + x \neq 0.\end{aligned}$$

Portanto, $F = \{f_1, f_2, f_3, f_4\}$ *não é uma base de Groebner para* I.

Seja $f_5 := -2y^2 + x$ *e considere agora* $F = \{f_1, f_2, f_3, f_4, f_5\}$. *Observe que*

$$\overline{S(f_i, f_j)}^F = 0, \quad \forall i, j \in \{1, \ldots, 5\}, i \neq j.$$

Portanto, $F = \{f_1, f_2, f_3, f_4, f_5\}$ *é uma base de Groebner para* I.

Lema 2.3.11 *O anel* $\mathbb{F}[x_1, \ldots, x_n]$ *é noetheriano, isto é, dada uma cadeia ascendente de ideais em* $\mathbb{F}[x_1, \ldots, x_n]$

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

existe um inteiro positivo N *tal que*

$$I_N = I_{N+1} = I_{N+2} = \cdots.$$

Demonstração. Seja

$$I := \bigcup_{i=1}^{\infty} I_i$$

e observe que I é um ideal em $\mathbb{F}[x_1, \ldots, x_n]$, de fato, $I \neq \emptyset$ pois $0 \in I$. Dados $f, g \in I$ e $p \in \mathbb{F}[x_1, \ldots, x_n]$, existem índices j, k tais que $f \in I_j$ e $g \in I_k$, digamos que $I_j \subset I_k$. Assim, $f, g \in I_k$. Como I_k é ideal temos que $f + g \in I_k$ e $fp \in I_k$, logo $f + g, fp \in I$. Pelo Teorema da Base de Hilbert, $I = \langle f_1, \ldots, f_s \rangle$, para alguns $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$. Para cada $i \in \{1, \ldots, s\}$, temos que $f_i \in I$, logo existe um índice j_i tal que $f_i \in I_{j_i}$. Seja

$$N := \max\{j_1, \ldots, j_s\}.$$

Assim, $f_i \in I_{j_i} \subset I_N$, para todo $i \in \{1, \ldots, s\}$. Logo,

$$I = \langle f_1, \ldots, f_s \rangle \subset I_N \subset I_{N+1} \subset \cdots \subset I.$$

Portanto, $I_N = I_{N+1} = I_{N+2} = \cdots$. □

Teorema 2.3.12 (Algoritmo de Buchberger) *Seja* $I = \langle f_1, \ldots, f_s \rangle \neq 0$ *um ideal polinomial. Então, uma base de Groebner para* I *pode ser construída em um número finito de operações através do seguinte algoritmo:*

INPUT: $F = (f_1, \ldots, f_s)$
OUTPUT: a Groebner basis $G = (g_1, \ldots, g_t)$ for I, with $F \subset G$

$G := F$
REPEAT
  $G' := G$
  FOR each pair $\{p, q\}, p \neq q$ in G' DO
    $S := \overline{S(p, q)}^{G'}$
    IF $S \neq 0$ THEN $G := G' \cup \{S\}$
UNTIL $G = G'$

Demonstração. Primeiramente, vejamos que em qualquer etapa do algoritmo temos que G é uma base para I, de fato, inicialmente isso é verdade pois $G = F$. Suponha que numa dada etapa temos que G' é uma base para I. Na etapa seguinte, dados $p, q \in G'$, com $p \neq q$, temos que $S(p,q) \in I$, pois $I = \langle G' \rangle$. Assim, o resto na divisão de $S(p,q)$ por G' pertence a I, ou seja $S = \overline{S(p,q)}^{G'} \in I$. Portanto, $G = G' \cup \{S\}$ é base para I. Agora, vamos mostrar que o algoritmo termina após um número finito de operações. Como $G' \subset G$ temos que $\mathrm{lt}(G') \subset \mathrm{lt}(G)$, e logo $\langle \mathrm{lt}(G') \rangle \subset \langle \mathrm{lt}(G) \rangle$. Observe que

$$G' \subset G \Rightarrow \langle \mathrm{lt}(G') \rangle \subset \langle \mathrm{lt}(G) \rangle,$$

de fato, se $G' \subset G$, então existe um resto $r = \overline{S(p,q)}^{G'}$ tal que $r \notin G'$ e $r \in G$. Sabemos que $\mathrm{lt}(r)$ não é divisível por nenhum dos termos líderes dos elementos de G', e portanto $\mathrm{lt}(r) \notin \langle \mathrm{lt}(G') \rangle$, mas como $r \in G$ temos $\mathrm{lt}(r) \in \langle \mathrm{lt}(G) \rangle$. Assim, é verdade que

$$\langle \mathrm{lt}(G') \rangle = \langle \mathrm{lt}(G) \rangle \Rightarrow G' = G.$$

Denotando por G_i a base para I obtida na i-ésima etapa do algoritmo, temos a seguinte cadeia ascendente de ideais em $\mathbb{F}[x_1, \ldots, x_n]$

$$\langle \mathrm{lt}(G_1) \rangle \subset \langle \mathrm{lt}(G_2) \rangle \subset \langle \mathrm{lt}(G_3) \rangle \subset \cdots$$

Como $\mathbb{F}[x_1, \ldots, x_n]$ é um anel noetheriano, existe um inteiro $N \geq 1$ tal que

$$\langle \mathrm{lt}(G_N) \rangle = \langle \mathrm{lt}(G_{N+1}) \rangle = \langle \mathrm{lt}(G_{N+2}) \rangle = \cdots$$

logo

$$G_N = G_{N+1} = G_{N+2} = \cdots.$$

Portanto, o algoritmo termina e a base obtida é $G = G_N$. Por fim, resta provar que G_N é uma base de Groebner para I. Sejam $p \neq q$ em G_N e considere $S_N := \overline{S(p,q)}^{G_N}$. Suponha por absurdo que $S_N \neq 0$, então $G_{N+1} = G_N \cup \{S_N\}$. Como $\mathrm{lt}(S_N)$ não é divisível por nenhum dos termos líderes dos elementos de G_N, temos que $S_N \notin G_N = G_{N+1}$, absurdo. Portanto, $S_N = 0$, e pelo critério de Buchberger G_N é uma base de Groebner para I. □

Vamos obter um critério mais simples para decidir quando uma base para um ideal é de Groebner. Para isso, precisaremos da seguinte definição

Definição 2.3.13 Seja $G = \{g_1, \ldots, g_t\} \subset \mathbb{F}[x_1, \ldots, x_n]$ e fixe uma ordem monomial em $\mathcal{M}$. Dado $f \in \mathbb{F}[x_1, \ldots, x_n]$, dizemos que f **reduz a zero módulo** G, e denotamos por $f \longrightarrow_G 0$, se f pode ser escrito na forma

$$f = a_1 g_1 + \cdots + a_t g_t, \text{ com } a_i \in \mathbb{F}[x_1, \ldots, x_n],$$

tal que sempre que $a_i g_i \neq 0$ devemos ter que $\mathrm{mdeg}(f) \geq \mathrm{mdeg}(a_i g_i)$.

Lema 2.3.14 *Seja* $G = (g_1, \ldots, g_t)$ *um conjunto ordenado de elementos de* $\mathbb{F}[x_1, \ldots, x_n]$ *e seja* $f \in \mathbb{F}[x_1, \ldots, x_n]$. *Se* $\overline{f}^{G} = 0$, *então* $f \longrightarrow_G 0$.

Demonstração. Aplicando o algoritmo da divisão para dividir f por G, obtemos

$$f = a_1 g_1 + \cdots + a_t g_t, \text{ com } \mathrm{mdeg}(f) \geq \mathrm{mdeg}(a_i g_i),$$

sempre que $a_i g_i \neq 0$. Portanto, $f \longrightarrow_G 0$. □

Observe que, em geral, a recíproca **não** é válida:

Se dividirmos $f = xy^2 - x$ por $G = (xy + 1, y^2 - 1)$ com respeito a ordem lexicográfica, obtemos

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

Então $\bar{f}^{\,G} = -x - y \neq 0$. Mas podemos escrever

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

e $\mathrm{mdeg}(xy^2 - x) \geq \mathrm{mdeg}(x \cdot (y^2 - 1))$, logo $f \longrightarrow_G 0$.

Teorema 2.3.15 *Uma base* $G = \{g_1, \ldots, g_t\}$ *para um ideal polinomial* I *é uma base de Groebner para* I *se, e somente se,* $S(g_i, g_j) \longrightarrow_G 0$*, para todo* $i \neq j$.

Demonstração. ($\Rightarrow$) Se G é uma base de Groebner para I, então $\overline{S(g_i, g_j)}^{\,G} = 0$, $\forall\, i \neq j$. Pelo lema anterior, vem que $S(g_i, g_j) \longrightarrow_G 0$, $\forall\, i \neq j$.

($\Leftarrow$) Suponha que $S(g_k, g_j) \longrightarrow_G 0$, $\forall\, k \neq j$. Então existem $a_1, \ldots, a_t \in K[x_1, \ldots, x_n]$ tais que

$$S(g_k, g_j) = \sum_{i=1}^{t} a_i g_i \text{ e } \mathrm{mdeg}(S(g_k, g_j)) \geq \mathrm{mdeg}(a_i g_i), \text{ se } a_i g_i \neq 0.$$

Isso é suficiente para concluir que G é uma base de Groebner para I, basta seguir o raciocínio da demonstração do Critério de Buchberger. □

Proposição 2.3.16 *Dado um conjunto finito* $G \subset \mathbb{F}[x_1, \ldots, x_n]$*, suponha que temos* $f, g \in G$ *tais que*

$$\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g)) = \mathrm{lm}(f)\mathrm{lm}(g),$$

isto significa que os monômios líderes de f *e* g *são relativamente primos. Então,* $S(f, g) \longrightarrow_G 0$.

Demonstração. Podemos assumir que $\mathrm{lc}(f) = \mathrm{lc}(g) = 1$, pois $S(f, g) = S(cf, dg)$, para todos $c, d \in \mathbb{F}$, de fato:

$$S(cf, dg) = \frac{x^\gamma}{\mathrm{lt}(cf)} cf - \frac{x^\gamma}{\mathrm{lt}(dg)} dg = \frac{x^\gamma}{c\,\mathrm{lt}(f)} cf - \frac{x^\gamma}{d\,\mathrm{lt}(g)} dg = \frac{x^\gamma}{\mathrm{lt}(f)} f - \frac{x^\gamma}{\mathrm{lt}(g)} g = S(f, g),$$

onde $x^\gamma = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$.
Escreva $f = \mathrm{lm}(f) + p$ e $g = \mathrm{lm}(g) + q$. Como $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g)) = \mathrm{lm}(f)\mathrm{lm}(g)$, temos que

$$\begin{aligned} S(f, g) &= \frac{\mathrm{lm}(f)\mathrm{lm}(g)}{\mathrm{lm}(f)} f - \frac{\mathrm{lm}(f)\mathrm{lm}(g)}{\mathrm{lm}(g)} g \\ &= \mathrm{lm}(g)(\mathrm{lm}(f) + p) - \mathrm{lm}(f)(\mathrm{lm}(g) + q) \\ &= \mathrm{lm}(g)\mathrm{lm}(f) + p\,\mathrm{lm}(g) - \mathrm{lm}(f)\mathrm{lm}(g) - q\,\mathrm{lm}(f) \\ &= p(g - q) - q(f - p) \\ &= pg - qf. \end{aligned}$$

Como $f, g \in G$, basta provar que

$$\mathrm{mdeg}(S(f, g)) \geq \mathrm{mdeg}(pg) \text{ e } \mathrm{mdeg}(S(f, g)) \geq \mathrm{mdeg}(qf).$$

Vejamos que

$$\mathrm{mdeg}(S(f, g)) = \max\{\mathrm{mdeg}(pg), \mathrm{mdeg}(qf)\}.$$

Isso segue do fato de que $\mathrm{lm}(pg)$ e $\mathrm{lm}(qf)$ são distintos e logo, não cancelam. Para provar isso, suponha que $\mathrm{lm}(pg) = \mathrm{lm}(qf)$, então

$$\mathrm{lm}(p)\mathrm{lm}(g) = \mathrm{lm}(q)\mathrm{lm}(f), \text{ daí } \mathrm{lm}(g) \mid \mathrm{lm}(q)\mathrm{lm}(f).$$

Como $\mathrm{lm}(g)$ e $\mathrm{lm}(f)$ são relativamente primos, vem que $\mathrm{lm}(g) \mid \mathrm{lm}(q)$, logo $\mathrm{lm}(g) \leq \mathrm{lm}(q)$, absurdo! Pois $\mathrm{lm}(g) > \mathrm{lm}(q)$, já que $g = \mathrm{lm}(g) + q$. □

Corolário 2.3.17 *Seja* $G = \{g_1, \ldots, g_t\}$ *uma base para um ideal polinomial* I. *Se* $\mathrm{lm}(g_i)$ *e* $\mathrm{lm}(g_j)$ *são primos entre si, para todo* $i \neq j$, *então* G *é uma base de Groebner para* I.

Demonstração. Segue imediatamente do Teorema 2.3.15 e da Proposição 2.3.16. □

2.4 A Pegada de um Ideal

Definição 2.4.1 *Seja* $I \subset \mathbb{F}[x_1, \ldots, x_n]$ *um ideal. A* **pegada** *de* I *(com respeito a uma ordem monomial fixada em* $\mathcal{M}$*) é o conjunto*

$$\Delta(I) = \{M \in \mathcal{M} : M \textit{ não é monômio líder de nenhum polinômio em } I\}.$$

A pegada de um ideal I está intimamente relacionada com uma base de Groebner para I (ambas definidas com respeito a mesma ordem monomial em $\mathcal{M}$).

Proposição 2.4.2 *Seja* $I \subset \mathbb{F}[x_1, \ldots, x_n]$ *um ideal e seja* $\{g_1, \ldots, g_t\}$ *uma base de Groebner para* I. *Então um monômio* M *pertence a* $\Delta(I)$ *se, e somente se,* M *não é múltiplo de* $\mathrm{lm}(g_i)$, *para todo* $i = 1, \ldots, t$.

Demonstração. ($\Rightarrow$) Óbvio (segue imediatamente da definição de $\Delta(I)$).
($\Leftarrow$) Do Lema 2.3.2, nós sabemos que se M não é múltiplo de $\mathrm{lm}(g_i)$, para todo $i = 1, \ldots, t$ então M não é monômio líder de nenhum polinômio em I, logo $M \in \Delta(I)$. □

Vimos que a demonstração acima é muito simples e utiliza apenas a definição de $\Delta(I)$ em uma direção e a definição de bases de Groebner na outra. Isso sugere que os conceitos de base de Groebner e pegada são equivalentes, e de fato são no seguinte sentido. Uma vez encontrada uma base de Groebner para um ideal I, podemos obter a pegada de I usando apenas a proposição acima. Por outro lado, nós podemos iniciar com a Definição 2.4.1 e então obter uma base de Groebner para I como sendo um conjunto $\{g_1, \ldots, g_t\} \subset I$ tal que o o conjunto dos monômios que são múltiplos de $\mathrm{lm}(g_i)$ para algum $i = 1, \ldots, t$ é exatamente $\mathcal{M} \setminus \Delta(I)$. No apêndice da referência [4] o autor mostra que tal conjunto existe e satisfaz as condições da Definição 2.3.1.

No próximo exemplo, vamos mostrar como utilizar a proposição acima para obter uma representação gráfica da pegada.

Exemplo 2.4.3 *Seja*

$$I = \langle x^3 - x, y^3 - y, x^2y - y\rangle \subset \mathbb{R}[x, y]$$

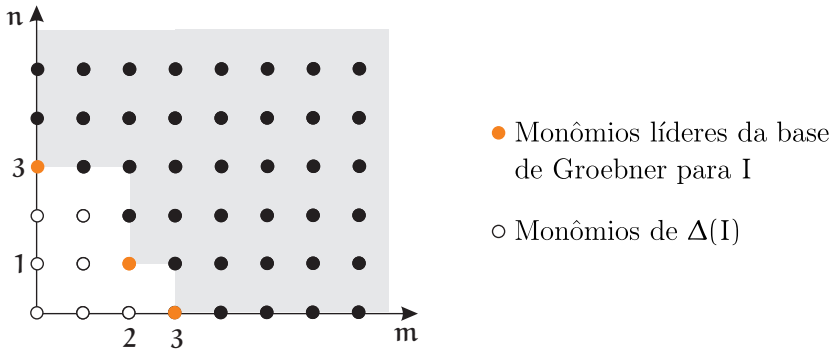
e considere $\mathcal{M}$ *com a ordem lexicográfica, onde* $y \preceq x$. *Veja que o conjunto*

$$B := \{x^3 - x, y^3 - y, x^2y - y\}$$

é uma base de Groebner para I. *De fato: se* $f_1 = x^3 - x, f_2 = y^3 - y$ *e* $f_3 = x^2y - y$, *calculando os* S*-polinômios de* f_1, f_2 *e* f_3, *obtemos*

$$\begin{aligned} S(f_1, f_2) &= x^3y - xy^3 = yf_1 - xf_2 \\ S(f_1, f_3) &= 0 \\ S(f_2, f_3) &= -x^2y + y^3 = f_2 - f_3 \end{aligned}$$

ou seja, o resto da divisão de $S(f_1, f_2), S(f_1, f_3)$ *e* $S(f_2, f_3)$ *por* B *é zero, logo pelo Critério de Buchberger* B *é uma base de Groebner para* I.
Temos que $\mathrm{lm}(x^3-x) = x^3, \mathrm{lm}(y^3-y) = y^3$ *e* $\mathrm{lm}(x^2y-y) = x^2y$. *Aplicando a proposição acima vamos determinar* $\Delta(I)$. *Na figura abaixo, podemos visualizar a pegada de* I, *onde representamos o monômio* $x^m y^n$ *pelo par de inteiros não negativos* (m, n).



Inicialmente marcamos os pontos $(3, 0), (0, 3)$ *e* $(2, 1)$ *que correspondem aos monômios líderes da base de Groebner* B. *A partir deles é fácil determinar os monômios que são múltiplos de pelo menos um deles (pontos pretos). Assim, determinamos o conjunto dos monômios que são monômios líderes dos polinômios de* I. *Então, segue da discussão feita anteriormente que a pegada de* I *corresponde aos pontos brancos, ou seja,* $\Delta(I) = \{1, x, x^2, y, xy, y^2, xy^2\}$.

O próximo teorema nos apresenta a solução do problema de tese de Buchberger.

Teorema 2.4.4 *Seja* $I \subset \mathbb{F}[x_1, \ldots, x_n]$ *um ideal. Então*

$$\mathcal{B} = \{M + I : M \in \Delta(I)\}$$

é uma base para $\mathbb{F}[x_1, \ldots, x_n]/I$ *como* $\mathbb{F}$*-espaço vetorial. Em particular,* $\dim(\mathbb{F}[x_1, \ldots, x_n]/I) = \#(\Delta(I))$.

Demonstração. Seja $f \in \mathbb{F}[x_1, \ldots, x_n]$, dividindo f por uma base de Groebner para I, nós temos que o resto é da forma $r = \sum_{i=1}^{t} a_i M_i$, onde $a_i \in \mathbb{F}$ e $M_i \in \Delta(I)$, para todo $i = 1, \ldots, t$. Como $f + I = r + I$, segue que $\mathcal{B}$ gera $\mathbb{F}[x_1, \ldots, x_n]/I$ como $\mathbb{F}$-espaço vetorial. Agora, vejamos que $\mathcal{B}$ é linearmente independente sobre $\mathbb{F}$. Suponha que $\sum_{i=1}^{\ell} b_i(M_i + I) = 0 + I$, onde $b_i \in \mathbb{F}$ e $M_i \in \Delta(I)$, para todo $i = 1, \ldots, \ell$. Então $\sum_{i=1}^{\ell} b_i M_i \in I$ e assim temos que ter $b_i = 0$, para todo $i = 1, \ldots, \ell$, do contrário, $\sum_{i=1}^{\ell} b_i M_i$ seria um elemento não nulo de I cujo monômio líder não é monômio líder de nenhum polinômio em I. Absurdo. □

Seja $I \subset \mathbb{F}[x_1, \ldots, x_n]$ um ideal e seja $\{f_1, \ldots, f_t\}$ uma base para I. Vamos denotar por $\Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$ o conjunto

$$\Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t)) := \{M \in \mathcal{M} : M \text{ não é múltiplo de } \mathrm{lm}(f_i), \text{ para todo } i = 1, \ldots, t\}.$$

Proposição 2.4.5 *Seja* $I \subset \mathbb{F}[x_1, \ldots, x_n]$ *um ideal e seja* $\{f_1, \ldots, f_t\}$ *uma base para* I. *Então*

(i) $\Delta(I) \subset \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$.

(ii) $\Delta(I) = \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$ *se, e somente se,* $\{f_1, \ldots, f_t\}$ *é uma base de Groebner para* I.

Demonstração.

(i) Seja $M \in \Delta(I)$. Então, pela definição de pegada temos que $M \notin \langle \mathrm{lm}(I) \rangle$. Como $\langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t) \rangle \subset \langle \mathrm{lm}(I) \rangle$, segue que $M \notin \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t) \rangle$, ou seja,

$$M \in \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t)).$$

(ii) ($\Rightarrow$) Seja $f \in I$. Basta provar que $\mathrm{lm}(f) \in \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t) \rangle$. Suponha, por absurdo, que $\mathrm{lm}(f) \notin \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t) \rangle$. Então $\mathrm{lm}(f) \in \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t)) = \Delta(I)$. Logo, $\mathrm{lm}(f) \notin \langle \mathrm{lm}(I) \rangle$ e assim, $f \notin I$. Absurdo.

($\Leftarrow$) Por (i) já temos que $\Delta(I) \subset \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$. Para provar a outra inclusão, seja $M \in \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$. Então, como $\{f_1, \ldots, f_t\}$ é uma base de Groebner para I, temos que $M \notin \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t) \rangle = \langle \mathrm{lm}(I) \rangle$, ou seja $M \in \Delta(I)$.

□

2.5 Variedades Afins e a Pegada de um Ideal

Nesta seção vamos apresentar uma relação entre a variedade afim associada a um ideal I e a sua pegada quando $\Delta(I)$ for um conjunto finito.

Definição 2.5.1 *Seja* $I \subset \mathbb{F}[x_1, \ldots, x_n]$ *um ideal. A* **variedade afim** *associada a* I *é o conjunto*

$$V(I) = \{(a_1, \ldots, a_n) \in \mathbb{F}^n : f(a_1, \ldots, a_n) = 0, \text{ para todo } f \in I\}.$$

É fácil ver que se $I = \langle g_1, \ldots, g_t \rangle$, então $(a_1, \ldots, a_n) \in V(I)$ se, e somente se, $g_i(a_1, \ldots, a_n) = 0$, para todo $i = 1, \ldots, t$.

Definição 2.5.2 *Seja* V *uma variedade afim. O* **ideal da variedade** V *é o conjunto de todos os polinômios que se anulam em* V*, ou seja,*

$$I(V) := \{f \in \mathbb{F}[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0, \text{ para todo } (a_1, \ldots, a_n) \in V\}.$$

É fácil ver que esse conjunto é, de fato um ideal de $\mathbb{F}[x_1, \ldots, x_n]$.

Proposição 2.5.3 *Se* W *é uma variedade afim, então* $V(I(W)) = W$.

Demonstração. Segue das definições de ideal de uma variedade e variedade afim que $W \subset V(I(W))$. Por outro lado, sabemos que $W = V(J)$, para algum ideal $J \subset \mathbb{F}[x_1, \ldots, x_n]$ e é claro que $J \subset I(W)$, logo $V(J) \supset V(I(W))$, isto é, $W \supset V(I(W))$. □

Lema 2.5.4 *Seja* $I \subset \mathbb{F}[x_1, \ldots, x_n]$ *um ideal e sejam* $p_1, \ldots, p_r$ *os pontos distintos de* $V(I)$. *Então existem polinômios* $f_1, \ldots, f_r \in \mathbb{F}[x_1, \ldots, x_n]$ *tais que* $f_i(p_j) = \delta_{ij}$*, para todos* $i, j \in \{1, \ldots, r\}$*, onde* δ_{ij} *é o delta de Kronecker.*

Demonstração. Sejam $p_i = (a_{i1}, \ldots, a_{in}) \in \mathbb{F}^n$, com $i = 1, \ldots, r$. Vejamos como obter f_1. Como todos os pontos são distintos, para $i \in \{2, \ldots, r\}$ existe $j_i \in \{1, \ldots, n\}$ tal que $a_{1j_i} \neq a_{ij_i}$. Seja

$$h_i = \frac{x_{j_i} - a_{ij_i}}{a_{1j_i} - a_{ij_i}},$$

então $h_i(p_1) = 1$ e $h_i(p_i) = 0$, para todo $i = 2, \ldots, r$. Tome

$$f_1 := \prod_{i=2}^{r} h_i,$$

assim, nós temos que $f_1(p_1) = 1$ e $f_1(p_i) = 0$, para todo $i = 2, \ldots, r$. Analogamente podemos obter $f_2, \ldots, f_r$. □

Teorema 2.5.5 *Seja* $I \subset \mathbb{F}[x_1, \ldots, x_n]$ *um ideal tal que* $\Delta(I)$ *é um conjunto finito. Então* $V(I)$ *é também um conjunto finito e* $\#(V(I)) \leq \#(\Delta(I))$.

Demonstração. Sejam $p_1, \ldots, p_r$ pontos distintos de $V(I)$. Do lema anterior nós sabemos que existem $f_1, \ldots, f_r \in \mathbb{F}[x_1, \ldots, x_n]$ tais que $f_i(p_j) = \delta_{ij}$, para todo $i, j \in \{1, \ldots, r\}$. Vejamos que $\{f_1 + I, \ldots, f_r + I\}$ é um conjunto linearmente independente em $\mathbb{F}[x_1, \ldots, x_n]/I$. De fato, suponha que $\sum_{i=1}^{r} a_i(f_i + I) = 0 + I$, onde $a_1, \ldots, a_r \in \mathbb{F}$, então $\sum_{i=1}^{r} a_i f_i \in I$. Logo, $\sum_{i=1}^{r} a_i f_i(p_j) = 0$, isto é, $a_j = 0$, para todo $j = 1, \ldots, r$. Assim, $\{f_1 + I, \ldots, f_r + I\}$ é linearmente independente em $\mathbb{F}[x_1, \ldots, x_n]/I$. Portanto,

$$\#(V(I)) = r \leq \dim(\mathbb{F}[x_1, \ldots, x_n]/I) = \#(\Delta(I)).$$

□

Capítulo 3

Códigos Parametrizados

3.1 Código Parametrizado Afim

Seja $K = \mathbb{F}_q$ um corpo finito com q elementos. Considere $\mathbb{A}^s = K^s$ o espaço afim sobre o corpo K e sejam $m_1, \ldots, m_s$ monômios em $K[x_1, \ldots, x_n]$, onde

$$\begin{aligned} m_1 &= x^{v_1} = x_1^{v_{11}} \cdots x_n^{v_{1n}} \\ m_2 &= x^{v_2} = x_1^{v_{21}} \cdots x_n^{v_{2n}} \\ &\vdots \\ m_s &= x^{v_s} = x_1^{v_{s1}} \cdots x_n^{v_{sn}} \end{aligned}$$

Definição 3.1.1 *O conjunto*

$$X := \{(m_1(a), \ldots, m_s(a)) \in \mathbb{A}^s : a = (a_1, \ldots, a_n) \in (K^*)^n\}$$

é chamado de **conjunto tórico algébrico afim** *parametrizado por* $m_1, \ldots, m_s$.

Como K é finito, temos que X é finito, digamos que

$$X = \{p_1, \ldots, p_m\}, \quad \text{onde } m = \#X.$$

Seja $S = K[t_1, \ldots, t_s]$ e seja $d \in \mathbb{N}$. Considere o conjunto

$$S_{\leq d} := \{f \in S : \deg(f) \leq d\} \cup \{0\}.$$

Observe que $S_{\leq d}$ é um K-espaço vetorial. Considere a aplicação

$$\begin{array}{rccc} \psi_d : & S_{\leq d} & \longrightarrow & K^m \\ & f & \longmapsto & (f(p_1), \ldots, f(p_m)) \end{array}$$

Vejamos que ψ_d é uma transformação linear:
Sejam $f, g \in S_{\leq d}$ e $\lambda \in K$. Temos que

$$\begin{aligned} \psi_d(f + \lambda g) &= ((f + \lambda g)(p_1), \ldots, (f + \lambda g)(p_m)) \\ &= (f(p_1) + \lambda g(p_1), \ldots, f(p_m) + \lambda g(p_m)) \\ &= (f(p_1), \ldots, f(p_m)) + \lambda(g(p_1), \ldots, g(p_m)) \\ &= \psi_d(f) + \lambda \psi_d(g). \end{aligned}$$

Definição 3.1.2

(a) *A imagem da transformação linear* ψ_d *é um código linear chamado* **código parametrizado afim de ordem** d *e denotado por*

$$\mathrm{Im}(\psi_d) = C_X(d).$$

(b) *O* **ideal anulador de** X *é o ideal de* S *que consiste de todos os polinômios de* S *que se anulam em* X*, ou seja,*

$$I(X) := \{f \in S : f(p) = 0, \text{ para todo } p \in X\}.$$

Definimos também $I(X)_{\leq d} := I(X) \cap S_{\leq d}$.

Note que $\ker(\psi_d) = I(X)_{\leq d}$. De fato:
Se $f \in \ker(\psi_d)$, então $f \in S_{\leq d}$ e $\psi_d(f) = 0$, isto é, $(f(p_1), \ldots, f(p_m)) = (0, \ldots, 0)$, logo $f(p_1) = \cdots = f(p_m) = 0$. Portanto, $f \in S_{\leq d}$ e se anula em todos os pontos de X, ou seja, $f \in I(X)_{\leq d}$. Para provar a outra inclusão, seja $f \in I(X)_{\leq d}$, então $f \in S_{\leq d}$ e $f \in I(X)$. Como $f \in I(X)$, segue que $\psi_d(f) = (f(p_1), \ldots, f(p_m)) = (0, \ldots, 0) = 0$, ou seja, $f \in \ker(\psi_d)$.

Observe que $I(X)_{\leq d}$ é um subespaço de $S_{\leq d}$ e vamos provar que $C_X(d)$ e $S_{\leq d}/I(X)_{\leq d}$ são isomorfos.

Proposição 3.1.3 *A aplicação*

$$\begin{array}{rcl} T : S_{\leq d}/I(X)_{\leq d} & \longrightarrow & C_X(d) \\ \overline{f} & \longmapsto & \psi_d(f) \end{array}$$

é um isomorfismo de K*-espaços vetoriais.*

Demonstração. Inicialmente, vejamos que T está bem definida. Sejam $\overline{f}, \overline{g} \in S_{\leq d}/I(X)_{\leq d}$ tais que $\overline{f} = \overline{g}$. Vamos mostrar que $T(\overline{f}) = T(\overline{g})$. De fato, como $\overline{f} = \overline{g}$, então $f - g \in I(X)_{\leq d}$. Como $\ker(\psi_d) = I(X)_{\leq d}$ e ψ_d é linear, temos que

$$\psi_d(f) - \psi_d(g) = \psi_d(f - g) = 0,$$

ou seja, $\psi_d(f) = \psi_d(g)$, isto é, $T(\overline{f}) = T(\overline{g})$.
Agora, vejamos que T é um isomorfismo. Temos que

(i) T é linear:
Sejam $\overline{f}, \overline{g} \in S_{\leq d}/I(X)_{\leq d}$ e $\lambda \in K$. Temos que

$$T(\overline{f} + \lambda\overline{g}) = T(\overline{f + \lambda g}) = \psi_d(f + \lambda g) = \psi_d(f) + \lambda\psi_d(g) = T(\overline{f}) + \lambda T(\overline{g}).$$

(ii) $\ker T = \{\overline{0}\}$:
Seja $\overline{f} \in \ker T$. Como $T(\overline{f}) = \psi_d(f) = 0$, temos que $f \in \ker(\psi_d) = I(X)_{\leq d}$. Logo, $\overline{f} = \overline{0}$.

(iii) $\mathrm{Im}T = C_X(d)$:
É claro que $\mathrm{Im}T \subset C_X(d)$. Para provar a outra inclusão, seja $a \in C_X(d) = \mathrm{Im}(\psi_d)$, então existe $f \in S_{\leq d}$ tal que $a = \psi_d(f)$, ou seja, $a = T(\overline{f}) \in \mathrm{Im}T$.

Portanto, T é um isomorfismo de K-espaços vetoriais. □

Proposição 3.1.4 *Seja* ψ_d *a aplicação dada acima. Então, temos que*

(a) ψ_d *é sobrejetora, para todo* $d \geq m-1$.

(b) $\psi_d(S_{\leq d}) \subset \psi_{d+1}(S_{\leq d+1})$, *para todo* $d \geq 1$.

Demonstração.

(a) Seja $d \geq m-1$. Inicialmente, vamos construir um polinômio $f_1 \in S_{\leq d}$ tal que

$$\psi_d(f_1) = e_1 \in K^m.$$

Considere

$$\begin{aligned} p_1 &= (p_{11}, p_{12}, \ldots, p_{1s}) \\ p_2 &= (p_{21}, p_{22}, \ldots, p_{2s}) \\ &\vdots \\ p_m &= (p_{m1}, p_{m2}, \ldots, p_{ms}). \end{aligned}$$

Como $p_1 \neq p_2$, podemos escolher $j \in \{1, \ldots, s\}$ tal que $p_{1j} \neq p_{2j}$. Defina

$$h_2 := \frac{t_j - p_{2j}}{p_{1j} - p_{2j}} \in K[t_1, \ldots, t_s].$$

Assim, temos que $h_2(p_1) = 1$ e $h_2(p_2) = 0$. Da mesma forma, definimos $h_3, \ldots, h_m \in K[t_1, \ldots, t_s]$ tais que $h_j(p_1) = 1$ e $h_j(p_j) = 0$, para todo $j = 3, \ldots, m$. Considere

$$f_1 := h_2 \cdot \ldots \cdot h_m.$$

Observe que $\deg(f_1) = m-1 \leq d$, logo $f_1 \in S_{\leq d}$. Mais ainda, $f_1(p_1) = 1$ e $f_1(p_j) = 0$, para todo $j = 2, \ldots, m$. Portanto, $\psi_d(f_1) = e_1$.
Analogamente, construímos $f_2, \ldots, f_m \in S_{\leq d}$ tais que $\psi_d(f_j) = e_j$, para todo $j = 2, \ldots, m$. Isso prova que ψ_d é sobrejetora, para todo $d \geq m-1$.

(b) Seja $d \geq 1$ e $(f(p_1), \ldots, f(p_m)) \in \psi_d(S_{\leq d})$. Então $f \in S_{\leq d} \subset S_{\leq d+1}$, logo $(f(p_1), \ldots, f(p_m)) \in \psi_{d+1}(S_{\leq d+1})$.

□

Definição 3.1.5 *A* **função afim de Hilbert** *de* $S/I(X)$ *é dada por*

$$H_X(d) := \dim_K S_{\leq d}/I(X)_{\leq d}.$$

Corolário 3.1.6

(a) $H_X(d) = m$, *para todo* $d \geq m-1$.

(b) $H_X(d)$ *é uma função crescente para todo* $d \geq 1$.

Demonstração.

(a) Vimos que

$$S_{\leq d}/I(X)_{\leq d} \simeq C_X(d).$$

Logo, para todo $d \geq m-1$, temos que

$$H_X(d) = \dim_K S_{\leq d}/I(X)_{\leq d} = \dim_k C_X(d) = \dim_K \mathrm{Im}(\psi_d) = \dim_K K^m = m.$$

(b) Pelo item (b) da Proposição 3.1.4, temos que $\psi_d(S_{\leq d}) \subset \psi_{d+1}(S_{\leq d+1})$. Logo,

$$\dim_K \psi_d(S_{\leq d}) \leq \dim_K \psi_{d+1}(S_{\leq d+1}), \text{ ou seja, } H_X(d) \leq H_X(d+1), \text{ para todo } d \geq 1.$$

□

3.2 Código Parametrizado Projetivo

Sobre $K^{s+1} \setminus \{(0,\dots,0)\}$ defina a seguinte relação de equivalência:

$$(a_0,\dots,a_s) \sim (b_0,\dots,b_s) \Leftrightarrow (a_0,\dots,a_s) = \lambda(b_0,\dots,b_s), \text{ para algum } \lambda \in K^*.$$

Definição 3.2.1 *O* **espaço projetivo** *de dimensão* s *sobre o corpo* K, $\mathbb{P}^s$, *é o conjunto das classes de equivalência de* $\sim$. *A classe de equivalência de um ponto* $(a_0,\dots,a_s) \in K^{s+1} \setminus \{(0,\dots,0)\}$ *será denotada por* $[a_0,\dots,a_s]$.

Relembremos que um polinômio é *homogêneo* quando é soma de termos de mesmo grau e um ideal é *homogêneo* se for gerado por polinômios homogêneos.

Definição 3.2.2 *O conjunto*

$$Y := \{[m_1(a),\dots,m_s(a),1] \in \mathbb{P}^s : a = (a_1,\dots,a_n) \in (K^*)^n\}$$

é chamado de **conjunto tórico algébrico projetivo** *parametrizado pelos monômios* $m_1,\dots,m_s,m_{s+1}$, *onde* $m_{s+1} = 1$.

A próxima proposição nos diz que os conjuntos tóricos algébricos afim e projetivo possuem o mesmo número de elementos.

Proposição 3.2.3 *A aplicação*

$$\begin{aligned} \rho : X &\longrightarrow Y \\ (x_1,\dots,x_s) &\longmapsto [x_1,\dots,x_s,1] \end{aligned}$$

é bijetora. Em particular, X *e* Y *têm a mesma cardinalidade.*

Demonstração. É claro que ρ é sobrejetora. Vejamos que ρ é injetora. Sejam $(x_1,\dots,x_s)$ e $(x'_1,\dots,x'_s)$ em X tais que $\rho(x_1,\dots,x_s) = \rho(x'_1,\dots,x'_s)$, isto é, $[x_1,\dots,x_s,1] = [x'_1,\dots,x'_s,1]$. Então existe $\lambda \in K^*$ tal que $(x_1,\dots,x_s) = \lambda(x'_1,\dots,x'_s,1)$. Da última coordenada temos que $\lambda = 1$, logo, $(x_1,\dots,x_s) = (x'_1,\dots,x'_s)$. Logo, ρ é injetora.

□

Observação 3.2.4 *Vimos que* $\#Y = \#X = m$. *Digamos que*

$$Y = \{[q_1],\dots,[q_m]\}.$$

Então, pela Proposição 3.2.3 podemos supor sem perda de generalidade que

$$[q_i] = [p_i,1], \text{ para todo } i = 1,\dots,m.$$

Vamos denotar o anel $K[t_1,\dots,t_s,u]$ por $S[u]$.
Seja $d \in \mathbb{N}$ e defina

$$S[u]_d := \{f \in S[u] : f \text{ é homogêneo de grau } d\} \cup \{0\}.$$

Note que $S[u]_d$ também é um K-espaço vetorial.

Seja $f_0(t_1,\dots,t_{s+1}) = t_1^d$ e considere a aplicação

$$\begin{aligned} \psi'_d : S[u]_d &\longrightarrow K^m \\ f &\longmapsto \left(\frac{f(q_1)}{f_0(q_1)},\dots,\frac{f(q_m)}{f_0(q_m)}\right) \end{aligned}$$

Vejamos que ψ'_d é uma transformação linear:
Para provar que ψ'_d está bem definida, sejam $[r] = [\widetilde{r}] \in Y$. Então, $r = \lambda\widetilde{r}$, para algum $\lambda \in K^*$. Digamos que $[r] = [r_1, \ldots, r_{s+1}]$ e $[\widetilde{r}] = [\widetilde{r}_1, \ldots, \widetilde{r}_{s+1}]$. Seja $f \in S[u]_d$, vamos provar que

$$\frac{f(r)}{f_0(r)} = \frac{f(\widetilde{r})}{f_0(\widetilde{r})}.$$

Observe que $f_0(r) = f_0(\lambda\widetilde{r}) = (\lambda\widetilde{r}_1)^d = \lambda^d f_0(\widetilde{r})$.
Como f é homogêneo de grau d, temos que $f(r) = f(\lambda\widetilde{r}) = \lambda^d f(\widetilde{r})$. Portanto,

$$\frac{f(r)}{f_0(r)} = \frac{\lambda^d f(\widetilde{r})}{\lambda^d f_0(\widetilde{r})} = \frac{f(\widetilde{r})}{f_0(\widetilde{r})}.$$

Vamos provar que ψ'_d é uma transformação linear. Sejam $f, g \in S[u]_d$ e $\lambda \in K$. Temos que

$$\begin{aligned}\psi'_d(f+\lambda g) &= \left(\frac{(f+\lambda g)(q_1)}{f_0(q_1)}, \ldots, \frac{(f+\lambda g)(q_m)}{f_0(q_m)}\right) = \left(\frac{f(q_1)+\lambda g(q_1)}{f_0(q_1)}, \ldots, \frac{f(q_m)+\lambda g(q_m)}{f_0(q_m)}\right)\\ &= \left(\frac{f(q_1)}{f_0(q_1)}, \ldots, \frac{f(q_m)}{f_0(q_m)}\right) + \lambda\left(\frac{g(q_1)}{f_0(q_1)}, \ldots, \frac{g(q_m)}{f_0(q_m)}\right) = \psi'_d(f) + \lambda\psi'_d(g).\end{aligned}$$

Definição 3.2.5

(a) *A imagem da transformação linear ψ'_d é um código linear chamado de* **código parametrizado projetivo de ordem d** *e denotamos por*

$$Im(\psi'_d) = C_Y(d).$$

(b) *O* **ideal anulador de Y** *é o ideal de $S[u]$ gerado pelos polinômios homogêneos de $S[u]$ que se anulam em Y, ou seja,*

$$I(Y) := \langle\{f \in S[u] : f \text{ é homogêneo e } f(a) = 0,\ \forall\, a \in Y\}\rangle$$

Definimos também $I(Y)_d := I(Y) \cap S[u]_d$.

Observe que $I(Y)_d$ é um ideal homogêneo de $S[u]$. Assim, como no caso afim, temos que $\ker(\psi'_d) = I(Y)_d$. De fato:
Dado $f \in \ker(\psi'_d)$ temos que $f \in S[u]_d$ e $\psi'_d(f) = 0$. Assim,

$$\left(\frac{f(q_1)}{f_0(q_1)}, \ldots, \frac{f(q_m)}{f_0(q_m)}\right) = (0, \ldots, 0), \text{ ou seja, } f(q_1) = \cdots = f(q_m) = 0.$$

Portanto, f é homogêneo de grau d e se anula em Y. Isso mostra que $f \in I(Y) \cap S[u]_d = I(Y)_d$.
Para provar a outra inclusão, seja $f \in I(Y)_d$, logo $f \in S[u]_d$ e $f \in I(Y)$. Do fato de $f \in I(Y)$, segue que

$$\psi'_d(f) = \left(\frac{f(q_1)}{f_0(q_1)}, \ldots, \frac{f(q_m)}{f_0(q_m)}\right) = \left(\frac{0}{f_0(q_1)}, \ldots, \frac{0}{f_0(q_m)}\right) = (0, \ldots, 0).$$

Logo, $f \in \ker(\psi'_d)$.

Note que $I(Y)_d$ é um subespaço de $S[u]_d$.

Proposição 3.2.6 *A aplicação*

$$\begin{array}{rccc} T': & S[u]_d/I(Y)_d & \longrightarrow & C_Y(d) \\ & \overline{f} & \longmapsto & \psi'_d(f) \end{array}$$

é um isomorfismo de $K-$espaços vetoriais.

Demonstração. Inicialmente, veja que T' está bem definida. Sejam $\overline{f}, \overline{g} \in S[u]_d/I(Y)_d$ tais que $\overline{f} = \overline{g}$. Então, $f - g \in I(Y)_d = \ker(\psi'_d)$. Logo,

$$\psi'_d(f) - \psi'_d(g) = \psi'_d(f - g) = 0,$$

ou seja, $\psi'_d(f) = \psi'_d(g)$.
Vamos provar que T' é um isomorfismo. De fato:

(i) T' é uma transformação linear:
Sejam $\overline{f}, \overline{g} \in S[u]_d/I(Y)_d$ e $\lambda \in K$. Assim, temos que

$$T'(\overline{f} + \lambda\overline{g}) = T'(\overline{f + \lambda g}) = \psi'_d(f + \lambda g) = \psi'_d(f) + \lambda\psi'_d(g) = T'(\overline{f}) + \lambda T'(\overline{g}).$$

(ii) $\ker T' = \{\overline{0}\}$:
Seja $\overline{f} \in \ker T'$. Como $T'(\overline{f}) = \psi'_d(f) = 0$, temos que $f \in \ker(\psi'_d) = I(Y)_d$. Logo, $\overline{f} = \overline{0}$.

(iii) $\mathrm{Im}T' = C_Y(d)$:
É claro que $\mathrm{Im}T' \subset C_Y(d)$. Seja $a \in C_Y(d) = \mathrm{Im}(\psi'_d)$, então existe $f \in S[u]_d$ tal que $a = \psi'_d(f)$, ou seja, $a = T'(\overline{f}) \in \mathrm{Im}T'$. Logo, $C_Y(d) \subset \mathrm{Im}T'$.

□

Vamos mostrar que os códigos parametrizados $C_X(d)$ e $C_Y(d)$ possuem os mesmos parâmetros básicos, ou seja, eles tem a mesma dimensão, comprimento e distância mínima. Para isso, precisaremos da seguinte definição e de mais alguns resultados.

Definição 3.2.7 *Seja* $f \in S_{\leq d}$. *A* **homogeneização de** f **com respeito a** u **e** d *é o polinômio dado por*

$$f^h(t_1, \ldots, t_s, u) := u^d f\left(\frac{t_1}{u}, \ldots, \frac{t_s}{u}\right).$$

Observe que f^h é um polinômio homogêneo de grau d.

Lema 3.2.8 *Considere a função homogeneização*

$$\begin{aligned} \varphi : S_{\leq d} &\longrightarrow S[u]_d \\ f(t_1, \ldots, t_s) &\longmapsto u^d f\left(\frac{t_1}{u}, \ldots, \frac{t_s}{u}\right) \end{aligned}$$

Temos que:

(a) φ *é um isomorfismo de* K*-espaços vetoriais.*

(b) $\varphi\left(I(X)_{\leq d}\right) = I(Y)_d$.

Demonstração.

(a) Veja que

(i) φ é linear: sejam $f, g \in S_{\leq d}$ e $\lambda \in K$. Então

$$\begin{aligned} \varphi(f(t_1, \ldots, t_s) + \lambda g(t_1, \ldots, t_s)) &= \varphi((f + \lambda g)(t_1, \ldots, t_s)) \\ &= u^d\left((f + \lambda g)\left(\frac{t_1}{u}, \ldots, \frac{t_s}{u}\right)\right) \\ &= u^d\left(f\left(\frac{t_1}{u}, \ldots, \frac{t_s}{u}\right) + \lambda g\left(\frac{t_1}{u}, \ldots, \frac{t_s}{u}\right)\right) \\ &= u^d f\left(\frac{t_1}{u}, \ldots, \frac{t_s}{u}\right) + \lambda u^d g\left(\frac{t_1}{u}, \ldots, \frac{t_s}{u}\right) \\ &= \varphi(f(t_1, \ldots, t_s)) + \lambda\varphi(g(t_1, \ldots, t_s)). \end{aligned}$$

(ii) $\ker(\varphi) = \{0\}$

Seja $f \in \ker(\varphi)$, então $f \in S_{\leq d}$ e $\varphi(f) = 0$, i.e., $u^d f\left(\frac{t_1}{u}, \ldots, \frac{t_s}{u}\right) = 0$. Tomando $u = 1$, obtemos $f(t_1, \ldots, t_s) = 0$. Portanto, $f = 0$.

(iii) $\mathrm{Im}(\varphi) = S[u]_d$

É claro que $\mathrm{Im}(\varphi) \subset S[u]_d$. Seja $F \in S[u]_d$, então $F = F(t_1, \ldots, t_s, u)$ e é um polinômio homogêneo de grau d. Tome $f(t_1, \ldots, t_s) = F(t_1, \ldots, t_s, 1)$, então $\varphi(f) = F$. De fato:

$$\begin{aligned}
\varphi(f(t_1, \ldots, t_s)) &= u^d f\left(\frac{t_1}{u}, \ldots, \frac{t_s}{u}\right) \\
&= u^d F\left(\frac{t_1}{u}, \ldots, \frac{t_s}{u}, 1\right) \\
&= F\left(u\frac{t_1}{u}, \ldots, u\frac{t_s}{u}, u\right) \\
&= F(t_1, \ldots, t_s, u).
\end{aligned}$$

De (i), (ii) e (iii) segue que φ é um isomorfismo.

(b) ($\subset$) Seja $f \in I(X)_{\leq d}$, então $f \in S_{\leq d}$ e $f \in I(X)$. Temos que

$$\varphi(f) = u^d f\left(\frac{t_1}{u}, \ldots, \frac{t_s}{u}\right) \in S[u]_d,$$

e vamos mostrar que $\varphi(f) \in I(Y)$. Para isso, seja $q_i \in Y, i = 1, \ldots, m$. Sabemos que $q_i = [p_i, 1]$, com $p_i \in X$. Digamos que $p_i = (p_i^1, \ldots, p_i^s)$, então

$$\varphi(f)(q_i) = f^h(q_i) = f^h(p_i, 1) = 1^d f\left(\frac{p_i^1}{1}, \ldots, \frac{p_i^s}{1}\right) = f(p_i^1, \ldots, p_i^s) = 0.$$

Logo, $\varphi(f) \in I(Y)$, e portanto, $\varphi(f) \in I(Y) \cap S[u]_d = I(Y)_d$.

($\supset$) Seja $F \in I(Y)_d = I(Y) \cap S[u]_d$. Como $F \in S[u]_d$ e φ é sobrejetora, existe $f \in S_{\leq d}$ tal que $\varphi(f) = F$, vamos mostrar que $f \in I(X)$. Seja $p_i \in X, i = 1, \ldots, m$ e considere

$$\begin{aligned}
\varphi^{-1} : S[u]_d &\longrightarrow S_{\leq d} \\
f^h &\longmapsto f
\end{aligned}$$

a função inversa de φ, então, temos que

$$f(p_i) = \varphi^{-1}(\varphi(f)(q_i)) = \varphi^{-1}(F(q_i)) = \varphi^{-1}(0) = 0.$$

□

Teorema 3.2.9 *A aplicação* $\xi : C_X(d) \longrightarrow C_Y(d)$ *dada por*

$$(f(p_1), \ldots, f(p_m)) \overset{\xi}{\longmapsto} \left(\frac{f(p_1)}{f_0(p_1)}, \ldots, \frac{f(p_m)}{f_0(p_m)}\right)$$

é um isomorfismo de K*-espaços vetoriais.*

Demonstração. Inicialmente veja que a aplicação

$$\begin{array}{rcl} \phi : S_{\leq d} & \longrightarrow & S[u]_d/I(Y)_d \\ f & \longmapsto & \overline{f^h} \end{array}$$

é sobrejetora e que $\ker(\phi) = I(X)_{\leq d}$. De fato, note que ϕ é a composição de duas aplicações sobrejetoras ($\phi = \gamma \circ \varphi$ - como indicado no diagrama abaixo), logo é sobrejetora.

$$\begin{array}{ccccc} S_{\leq d} & \xrightarrow{\varphi} & S[u]_d & \xrightarrow{\gamma} & S[u]_d/I(Y)_d \\ f & \longmapsto & f^h & \longmapsto & \overline{f^h} \end{array}$$

Agora, vejamos que $\ker(\phi) = I(X)_{\leq d}$.
Seja $f \in \ker(\phi)$, então $\phi(f) = \overline{0}$, i.e., $\overline{f^h} = \overline{0}$. Logo, $f^h \in I(Y)_d$ e como $\varphi(I(X)_{\leq d}) = I(Y)_d$, segue que $f \in I(X)_{\leq d}$.
Por outro lado, seja $f \in I(X)_{\leq d}$. Como $\varphi(I(X)_{\leq d}) = I(Y)_d$, temos que $\varphi(f) \in I(Y)_d$. Logo, $\overline{\varphi(f)} = \overline{0}$, i.e., $\overline{f^h} = \overline{0}$. Portanto, $\phi(f) = \overline{f^h} = \overline{0}$, ou seja, $f \in \ker(\phi)$.
Assim, a aplicação

$$\begin{array}{rcl} \widetilde{\phi} : S_{\leq d}/I(X)_{\leq d} & \longrightarrow & S[u]_d/I(Y)_d \\ \overline{f} & \longmapsto & \phi(f) \end{array}$$

é um isomorfismo de K-espaços vetoriais.
Finalmente, pelas Proposições 3.1.3, 3.2.6 e do exposto acima segue que

$$\left.\begin{array}{rcl} S_{\leq d}/I(X)_{\leq d} & \simeq & C_X(d) \\ S[u]_d/I(Y)_d & \simeq & C_Y(d) \\ S_{\leq d}/I(X)_{\leq d} & \simeq & S[u]_d/I(Y)_d \end{array}\right\} \Rightarrow C_X(d) \simeq C_Y(d).$$

Explicitamente, temos o seguinte diagrama:

$$\begin{array}{ccccccc} C_X(d) & \xrightarrow{T^{-1}} & S_{\leq d}/I(X)_{\leq d} & \xrightarrow{\widetilde{\phi}} & S[u]_d/I(Y)_d & \xrightarrow{T'} & C_Y(d) \\ (f(p_1),\ldots,f(p_m)) & \longmapsto & \overline{f} & \longmapsto & \overline{f^h} & \longmapsto & \psi'_d(f^h) = \left(\frac{f^h(q_1)}{f_0(q_1)},\ldots,\frac{f^h(q_m)}{f_0(q_m)}\right), \end{array}$$

ou seja, $\xi = T' \circ \widetilde{\phi} \circ T^{-1}$ e é dada por

$$\xi(f(p_1),\ldots,f(p_m)) = \left(\frac{f^h(q_1)}{f_0(q_1)},\ldots,\frac{f^h(q_m)}{f_0(q_m)}\right) = \left(\frac{f(p_1)}{f_0(p_1)},\ldots,\frac{f(p_m)}{f_0(p_m)}\right).$$

□

Corolário 3.2.10 *Os códigos parametrizados* $C_X(d)$ *e* $C_Y(d)$ *têm os mesmos parâmetros básicos.*

Demonstração. É claro que os comprimentos de $C_X(d)$ e $C_Y(d)$ são iguais a m (uma vez que $C_X(d)$ e $C_Y(d)$ são subespaços de K^m). Também é claro que eles possuem a mesma dimensão, pois eles são isomorfos. Vejamos que $C_X(d)$ e $C_Y(d)$ têm a mesma distância mínima. Para isso, note que ξ preserva distâncias de Hamming, isto é,

$$d(\xi(a),\xi(b)) = d(a,b), \text{ para todos } a,b \in C_X(d).$$

De fato: sejam $a, b \in C_X(d)$. Digamos que $a = (f(p_1), \ldots, f(p_m))$ e $b = (\widetilde{f}(p_1), \ldots, \widetilde{f}(p_m))$, para alguns $f, \widetilde{f} \in S_{\leq d}$. Então, temos que

$$\begin{aligned} d(\xi(a), \xi(b)) &= d\left(\left(\frac{f(p_1)}{f_0(p_1)}, \ldots, \frac{f(p_m)}{f_0(p_m)}\right), \left(\frac{\widetilde{f}(p_1)}{f_0(p_1)}, \ldots, \frac{\widetilde{f}(p_m)}{f_0(p_m)}\right)\right) \\ &= d((f(p_1), \ldots, f(p_m)), (\widetilde{f}(p_1), \ldots, \widetilde{f}(p_m))) \\ &= d(a, b). \end{aligned}$$

Portanto,

$$\begin{aligned} d_{\min}(C_X(d)) &= \min\{d(a, b) : a, b \in C_X(d), a \neq b\} \\ &= \min\{d(\xi(a), \xi(b)) : \xi(a), \xi(b) \in C_Y(d)\} \\ &= d_{\min}(C_Y(d)). \end{aligned}$$

□

Corolário 3.2.11 *Os códigos parametrizados* $C_X(d)$ *e* $C_Y(d)$ *são equivalentes.*

Demonstração. Basta considerar a isometria linear $\xi : K^m \longrightarrow K^m$ dada por

$$(x_1, \ldots, x_m) \overset{\xi}{\longmapsto} \left(\frac{x_1}{f_0(p_1)}, \ldots, \frac{x_m}{f_0(p_m)}\right).$$

□

Proposição 3.2.12

(i) *A dimensão de* $C_X(d)$ *é crescente, como uma função de* d*, até atingir o valor constante igual a* m*.*

(ii) *A distância mínima de* $C_X(d)$ *é decrescente, como uma função de* d*, até atingir o valor constante igual a* 1*.*

Demonstração.

(i) Como $C_X(d)$ e $S_{\leq d}/I(X)_{\leq d}$ são isomorfos como K-espaços vetoriais, temos que

$$\dim C_X(d) = \dim_K (S_{\leq d}/I(X)_{\leq d}) = H_X(d).$$

Pelo Corolário 3.1.6, segue o resultado.

(ii) Temos que

$$d_{\min}(C_X(d)) = \min\{\omega(\psi_d(f)) : f \in S_{\leq d}, \psi_d(f) \neq 0\},$$

onde

$$\begin{aligned} \omega(\psi_d(f)) &= d(\psi_d(f), 0) \\ &= \#\{p \in X : f(p) \neq 0\} \\ &= \#X - \#\{p \in X : f(p) = 0\}. \end{aligned}$$

Seja $Z_X(f) := \{p \in X : f(p) = 0\}$. Note que o mínimo do conjunto $\{\omega(\psi_d(f)) : f \in S_{\leq d}, \psi_d(f) \neq 0\}$ é atingido quando $\#Z_X(f)$ for a maior possível.

Vamos mostrar que se $d_{min}(C_X(d)) > 1$ então $d_{min}(C_X(d)) > d_{min}(C_X(d+1))$. Pela definição de distância mínima é suficiente mostrar que

$$\max\{\#(Z_X(f)) : f \in S_{\leq d}, \psi_d(f) \neq 0\} < \max\{\#(Z_X(f)) : f \in S_{\leq d+1}, \psi_{d+1}(f) \neq 0\}.$$

Seja $f \in S_{\leq d}$, com $\psi_d(f) \neq 0$ e tal que $\#(Z_X(f))$ seja a maior possível. Como $d_{min}(C_X(d)) > 1$, então existem dois pontos distintos $a, b \in X$, com $a = (a_1, \ldots, a_s)$ e $b = (b_1, \ldots, b_s)$ tais que $f(a)$ e $f(b)$ são não nulos. Como $a \neq b$, temos que $a_k \neq b_k$ para algum $k = 1, \ldots, s$. Seja $g = f \cdot (a_k - t_k)$. Assim, temos que $g \in S_{\leq d+1}$, g não se anula em X (pois $g(b) = f(b)(a_k - b_k) \neq 0$) e g tem mais zeros do que f ($f(a) \neq 0$ e $g(a) = 0$). Isso prova a desigualdade acima e *a fortiori* que $d_{min}(C_X(d)) > d_{min}(C_X(d+1))$.
Para finalizar a demonstração vejamos que, se $d_{min}(C_X(d)) = 1$, então $d_{min}(C_X(d+1)) = 1$. De fato: como $d_{min}(C_X(d)) = 1$, então existe $f \in S_{\leq d}$ tal que $\omega(\psi_d(f)) = 1$. Como $S_{\leq d} \subset S_{\leq d+1}$, então $f \in S_{\leq d+1}$ e $\omega(\psi_{d+1}(f)) = 1$, logo $d_{min}(C_X(d+1)) = 1$.

□

Vamos trabalhar agora para obter expressões para $I(X)$ e $I(Y)$. Para isso precisaremos dos resultados que seguem abaixo.

Proposição 3.2.13 *Seja G um polinômio em $K[y_1, \ldots, y_n]$. Se G se anula em $(K^*)^n$ e o grau de G como um polinômio em y_i é menor que $q-1$, para todo $i = 1, \ldots, n$, então $G \equiv 0$.*

Demonstração. Vamos fazer indução sobre n. Se $n = 1$, então G é um polinômio em uma variável com $\deg(G) < q - 1$. Por hipótese, G se anula em K^*, isto é, G possui $q-1$ raízes. Relembre que um polinômio não nulo de grau r em uma variável pode ter no máximo r raízes distintas. Como o grau de G é menor do que a quantidade de raízes que ele possui, segue que $G \equiv 0$.
Suponha que a proposição é verdadeira para $n-1$ (com $n \geq 2$) e vamos prová-lo para n. Seja $G \in K[y_1, \ldots, y_n]$ satisfazendo as hipóteses da proposição. Podemos escrever G como um polinômio na variável y_n da seguinte forma

$$G = \sum_{j=1}^{s} G_j(y_1, \ldots, y_{n-1}) y_n^j,$$

onde $s = \deg_{y_n}(G) < q - 1$ e cada G_j é um polinômio em $K[y_1, \ldots, y_{n-1}]$ tal que o grau de G_j como um polinômio em y_i é menor que $q-1$, para todo $i = 1, \ldots, n-1$ e $j = 1, \ldots, s$.
Para cada $(n-1)$-upla fixada $(a_1, \ldots, a_{n-1}) \in (K^*)^{n-1}$, o polinômio em y_n obtido de G pela substituição dos valores $a_1, \ldots, a_{n-1}$ se anula para todo $a_n \in K^*$. Como o grau desse polinômio é menor do que $q-1$ e ele se anula em $q-1$ elementos, segue que ele é identicamente nulo, logo $G_j(a_1, \ldots, a_{n-1}) = 0$, para todo $(a_1, \ldots, a_{n-1}) \in (K^*)^{n-1}$. Pela hipótese de indução, segue que $G_j \equiv 0$, para todo $j = 1, \ldots, s$ e, portanto $G \equiv 0$. □

Proposição 3.2.14 *Sejam $B = K[y_1, \ldots, y_n, t_1, \ldots, t_s]$, $S = K[t_1, \ldots, t_s]$ e $I \subset B$ um ideal. Se G é uma base de Groebner para I com respeito a ordem lexicográfica (com $y_1 > y_2 > \cdots > y_n > t_1 > \cdots > t_s$), então $G' = G \cap S$ é uma base de Groebner para $I' = I \cap S$.*

Demonstração. Como $G' \subset I'$ por construção, é suficiente mostrar que

$$\langle \mathrm{lt}(I') \rangle = \langle \mathrm{lt}(G') \rangle,$$

pela definição de base de Groebner. Uma inclusão é óbvia e para provar a outra inclusão $\langle \mathrm{lt}(I') \rangle \subset \langle \mathrm{lt}(G') \rangle$, nós precisamos mostrar que dado $f \in I'$, o termo líder $\mathrm{lt}(f)$ é divisível por

$lt(g)$, para algum $g \in G'$.
Seja $f \in I' = I \cap S$, então $f \in I$ e como G é uma base de Groebner para I, o termo líder de f é divisível por $lt(g)$, para algum $g \in G$. Como $f \in I'$, isso nos diz que $lt(g)$ envolve apenas as variáveis $t_1, \ldots, t_s$. Agora, observe que, como estamos utilizando a ordem lexicográfica com $y_1 > \cdots > y_n > t_1 > \cdots > t_s$, qualquer monômio envolvendo $y_1, \ldots, y_n$ é maior do que todos os monômios em S, logo todos os monômios de g envolvem somente as variáveis $t_1, \ldots, t_s$ e portanto $g \in S$. Isso mostra que $g \in G'$ e conclui a demonstração. □

Definição 3.2.15 *Um* **binômio** *de S é um polinômio da forma* $t^a - t^b$*, com* $a, b \in \mathbb{N}^s$*. Um ideal gerado por binômios é dito um* **ideal binomial**.

Proposição 3.2.16 *O resto da divisão de um binômio em S por uma lista de binômios em S ou é zero ou é também um binômio.*

Demonstração. Inicialmente veja que a tese é verdadeira na divisão de um binômio por outro binômio. De fato, suponha que queremos dividir o binômio $t^\alpha - t^\beta$ por $t^\gamma - t^\delta$. É claro que se $t^\alpha - t^\beta$ for divisível por $t^\gamma - t^\delta$, então o resto da divisão será zero. Também é óbvio que se nenhum monômio de $t^\alpha - t^\beta$ for múltiplo de nenhum monômio de $t^\gamma - t^\delta$, então o resto da divisão será o próprio $t^\alpha - t^\beta$. Excetuando-se esses dois casos triviais, vejamos que em qualquer etapa da divisão o resto é sempre um binômio. Suponha que $t^\alpha = \mathrm{lm}(t^\alpha - t^\beta)$ e que $t^\gamma = \mathrm{lm}(t^\gamma - t^\delta)$. Temos dois casos:

- 1º caso: $t^\gamma \mid t^\alpha$
  Nesse caso, temos que $t^\alpha = t^\gamma t^\theta$, para algum $\theta \in \mathbb{N}^s$, logo
  $$t^\alpha - t^\beta = t^\theta(t^\gamma - t^\delta) + t^{\theta+\delta} - t^\beta,$$
  ou seja, o resto nessa etapa da divisão é o binômio $t^{\theta+\delta} - t^\beta$.
- 2º caso: $t^\gamma \nmid t^\alpha$ e $t^\gamma \mid t^\beta$
  Nesse caso, temos que $t^\beta = t^\gamma t^\theta$, para algum $\theta \in \mathbb{N}^s$, logo
  $$t^\alpha - t^\beta = t^\theta(t^\gamma - t^\delta) + t^\alpha - t^{\theta+\delta},$$
  ou seja, o resto nessa etapa da divisão é o binômio $t^\alpha - t^{\theta+\delta}$.

Assim, como as etapas da divisão se resumem a esses casos, segue que o resto da divisão de $t^\alpha - t^\beta$ por $t^\gamma - t^\delta$ ou é zero ou é um binômio. Como cada etapa da divisão de um binômio por uma lista de binômios é a divisão de um binômio por outro binômio, segue o resultado. □

Observação 3.2.17 *Note que se* $f = t^\alpha - t^\beta, g = t^\gamma - t^\delta$ *são binômios em S, então o S-polinômio de f e g também é um binômio. De fato: suponha que* $lt(f) = t^\alpha, lt(g) = t^\gamma$ *e* $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g)) = t^\theta$*, então:*

$$\begin{aligned} S(f,g) &= \frac{t^\theta}{lt(f)} f - \frac{t^\theta}{lt(g)} g \\ &= \frac{t^\theta}{t^\alpha}(t^\alpha - t^\beta) - \frac{t^\theta}{t^\gamma}(t^\gamma - t^\delta) \\ &= t^{\theta+\delta-\gamma} - t^{\theta+\beta-\alpha} \\ &= t^r - t^s, \end{aligned}$$

onde $r = \theta + \delta - \gamma$ *e* $s = \theta + \beta - \alpha$ *são elementos de* $\mathbb{N}^s$.

Lema 3.2.18 *Sejam* $B = K[y_1, \ldots, y_n, t_1, \ldots, t_s]$ *e* $S = K[t_1, \ldots, t_s]$. *Se* I *é um ideal binomial de* B, *então* $I \cap S$ *é um ideal binomial de* S.

Demonstração. Como I é um ideal binomial de B, temos que $I = \langle g_1, \ldots, g_t \rangle$, onde g_i é um binômio de B, para todo $i = 1, \ldots, t$. Considere em $\mathcal{M}$ a ordem lexicográfica com $y_1 > \cdots > y_n > t_1 > \cdots > t_s$. Utilizando o algoritmo de Buchberger podemos a partir de $\{g_1, \ldots, g_t\}$ obter uma base de Groebner G para I. Pela observação acima, da Proposição 3.2.16 e do algoritmo de Buchberger segue que G consiste de binômios e, da Proposição 3.2.14 segue que $G \cap S$ é uma base (de Groebner) para $I \cap S$, portanto, $I \cap S$ é um ideal binomial.

□

Teorema 3.2.19 *Sejam* $B = K[y_1, \ldots, y_n, t_1, \ldots, t_s]$ *e* $S = K[t_1, \ldots, t_s]$. *Temos que*

$$I(X) = \langle t_1 - y^{v_1}, \ldots, t_s - y^{v_s}, y_1^{q-1} - 1, \ldots, y_n^{q-1} - 1 \rangle \cap S$$

e $I(X)$ *é um ideal binomial.*

Demonstração. Seja $I' = \langle t_1 - y^{v_1}, \ldots, t_s - y^{v_s}, y_1^{q-1} - 1, \ldots, y_n^{q-1} - 1 \rangle \subset B$. Primeiro vamos mostrar a inclusão $I(X) \subset I' \cap S$. Seja $F = F(t_1, \ldots, t_s)$ um polinômio que se anula em X. Digamos que

$$F = \lambda_1 t^{m_1} + \cdots + \lambda_r t^{m_r}, \tag{3.1}$$

onde $\lambda_i \in K^*, m_i = (m_{i1}, \ldots, m_{is}) \in \mathbb{N}^s$, para $1 \leq i \leq r$. Para cada $1 \leq i \leq r$ e $1 \leq j \leq s$, temos que

$$t_j^{m_{ij}} = [(t_j - y^{v_j}) + y^{v_j}]^{m_{ij}}.$$

Aplicando o binômio de Newton no lado direito da equação acima, obtemos

$$t_j^{m_{ij}} = \left(\sum_{k=0}^{m_{ij}-1} \binom{m_{ij}}{k} (t_j - y^{v_j})^{m_{ij}-k} (y^{v_j})^k \right) + (y^{v_j})^{m_{ij}},$$

assim, temos que t^{m_i} pode ser escrito como

$$t^{m_i} = t_1^{m_{i1}} \cdots t_s^{m_{is}} = p_i + (y^{v_1})^{m_{i1}} \cdots (y^{v_s})^{m_{is}},$$

onde p_i é um polinômio do ideal $\langle t_1 - y^{v_1}, \ldots, t_s - y^{v_s} \rangle$. Substituindo $t^{m_1}, \ldots, t^{m_r}$ em (3.1), podemos escrever F como:

$$F = \sum_{j=1}^{s} g_j (t_j - y^{v_j}) + H(y^{v_1}, \ldots, y^{v_s}), \tag{3.2}$$

para alguns $g_1, \ldots, g_s$ em B. Considere em $\mathcal{M}$ a ordem lexicográfica com $y_1 > \cdots > y_n > t_1 > \ldots > t_s$. Pelo algoritmo da divisão em $K[y_1, \ldots, y_n]$ temos que

$$H(y^{v_1}, \ldots, y^{v_s}) = \sum_{k=1}^{n} h_k (y_k^{q-1} - 1) + G(y_1, \ldots, y_n), \tag{3.3}$$

para alguns $h_1, \ldots, h_n \in K[y_1, \ldots, y_n]$, onde os monômios que aparecem em G não são divisíveis por nenhum dos monômios $y_1^{q-1}, \ldots, y_n^{q-1}$, isto é, o grau de G como um polinômio em y_k é menor do que $q - 1$, para todo $k = 1, \ldots, n$. Substituindo (3.3) em (3.2), obtemos

$$F = \sum_{j=1}^{s} g_j (t_j - y^{v_j}) + \sum_{k=1}^{n} h_k (y_k^{q-1} - 1) + G(y_1, \ldots, y_n). \tag{3.4}$$

Para mostrar que $F \in I' \cap S$, devemos mostrar que $G \equiv 0$. Veja que G se anula em $(K^*)^n$: seja $x = (x_1, \ldots, x_n) \in (K^*)^n$, substituindo t_j por x^{ν_j}, para todo $j \in \{1, \ldots, s\}$ em (3.4) e usando o fato de que F se anula em X, temos que

$$0 = F(x^{\nu_1}, \ldots, x^{\nu_s}) = \sum_{j=1}^{s} g'_j(x^{\nu_j} - y^{\nu_j}) + \sum_{k=1}^{n} h_k(y_k^{q-1} - 1) + G(y_1, \ldots, y_n), \tag{3.5}$$

onde $g'_j = g_j(x^{\nu_1}, \ldots, x^{\nu_s}, y_1, \ldots, y_n)$, ou seja,

$$\sum_{j=1}^{s} g'_j(x^{\nu_j} - y^{\nu_j}) + \sum_{k=1}^{n} h_k(y_k^{q-1} - 1) + G(y_1, \ldots, y_n)$$

é igual ao polinômio nulo para todos os valores de $y_1, \ldots, y_n$. Assim, tomando $y_k = x_k$, para todo k na equação (3.5) segue que G se anula em $x = (x_1, \ldots, x_n)$. Logo, G se anula em $(K^*)^n$ e o grau de G como um polinômio na variável y_k é menor que $q - 1$, para todo $k = 1, \ldots, n$, então pela Proposição 3.2.13 segue que $G \equiv 0$.
Para mostrar a outra inclusão $I' \cap S \subset I(X)$, seja $F \in I' \cap S$. Como $F \in S$, então F envolve apenas as variáveis $t_1, \ldots, t_s$. Por outro lado, como $F \in I'$, temos que

$$F = \sum_{j=1}^{s} g_j(t_j - y^{\nu_j}) + \sum_{k=1}^{n} h_k(y_k^{q-1} - 1), \tag{3.6}$$

para alguns polinômios $g_1, \ldots, g_s, h_1, \ldots, h_n \in B$ e para todos $y_1, \ldots, y_n$. Seja $p = (x^{\nu_1}, \ldots, x^{\nu_s}) \in X$. Substituindo t_j por x^{ν_j} em (3.6), temos que

$$F(x^{\nu_1}, \ldots, x^{\nu_s}) = \sum_{j=1}^{s} g'_j(x^{\nu_j} - y^{\nu_j}) + \sum_{k=1}^{n} h'_k(y_k^{q-1} - 1), \tag{3.7}$$

onde $g'_j = g_j(x^{\nu_1}, \ldots, x^{\nu_s}, y_1, \ldots, y_n)$, $h'_k = h_k(x^{\nu_1}, \ldots, x^{\nu_s}, y_1, \ldots, y_n)$ e para quaisquer valores de $y_1, \ldots, y_n$. Tomando $y_k = x_k$ em (3.7), para todo $k = 1, \ldots, n$, temos que $F(p) = 0$, logo F se anula em X. Agora, como I' é um ideal binomial de B, segue do Lema 3.2.18 que $I(X)$ é um ideal binomial de S. □

Definição 3.2.20

(i) *Seja* f *um polinômio em* S *de grau* e. *A* **homogeneização de f com respeito a u** *é dada por*

$$f^h = u^e f\left(\frac{t_1}{u}, \ldots, \frac{t_s}{u}\right).$$

(ii) *Seja* I *um ideal em* $S = K[t_1, \ldots, t_s]$. *Definimos a* **homogeneização de** I **com respeito a** u *como sendo o ideal homogêneo de* $S[u]$ *dado por*

$$I^h = \langle f^h : f \in I \rangle,$$

onde f^h *é a homogeneização de* f *com respeito a* u.

Vamos mostrar que podemos obter o ideal anulador de Y a partir de $I(X)$, mais especificamente, vamos mostrar que

$$I(Y) = I(X)^h = \langle f^h : f \in I(X) \rangle \subset S[u],$$

onde f^h é a homogeneização de f com respeito a u.
Vamos utilizar uma ordem monomial específica em $S[u] = K[t_1, \ldots, t_s, u]$. Veja que todo monômio em $S[u]$ pode ser escrito como

$$t_1^{\alpha_1} \cdots t_s^{\alpha_s} u^r = t^\alpha u^r,$$

onde t^α não possui o fator u. Assim, podemos estender a ordem graduada $>$ dos monômios em S para uma ordem $>_h$ dos monômios em $S[u]$ da seguinte maneira:

$$t^\alpha u^r >_h t^\beta u^{r'} \iff (t^\alpha > t^\beta) \text{ ou } (t^\alpha = t^\beta \text{ e } r > r').$$

Observe que $t_i >_h u$ para todo $i = 1, \ldots, s$, basta ver que

$$t_i = t^{e_i} u^0 >_h u = t^0 u^1, \text{ pois } t^{e_i} > t^0.$$

Seja f um polinômio em S de grau d. Então, podemos escrever f de maneira única como

$$f = f_0 + f_1 + \cdots + f_d,$$

onde $\deg(f_i) = i$, para todo $i = 0, \ldots, d$. Dizemos que $f_0, \ldots, f_d$ são as *componentes homogêneas* de f.

Lema 3.2.21 *Sejam $f \in S = K[t_1, \ldots, t_s]$ e $>$ uma ordem graduada dos monômios em S, então*

$$\mathrm{lm}_{>_h}(f^h) = \mathrm{lm}_>(f).$$

Demonstração. Seja $f \in S$ e digamos que $t^\alpha = \mathrm{lm}_>(f)$. Como $>$ é uma ordem graduada, temos que t^α é um dos monômios que aparece na componente homogênea de f de maior grau. Quando homogeneizamos f com respeito a u temos que t^α não é modificado.
Seja $t^\beta u^r$ um monômio qualquer de f^h. Como t^β é um monômio de f temos que $t^\alpha > t^\beta$, logo $t^\alpha >_h t^\beta u^r$, portanto, $t^\alpha = \mathrm{lm}_{>_h}(f^h)$. □

Teorema 3.2.22 *Seja I um ideal em $S = K[t_1, \ldots, t_s]$ e seja $G = \{g_1, \ldots, g_r\}$ uma base de Groebner para I com respeito a alguma ordem monomial graduada em S. Então, $G^h = \{g_1^h, \ldots, g_r^h\}$ é uma base de Groebner para $I^h \subset S[u]$.*

Demonstração. Vamos provar o teorema mostrando que G^h é uma base de Groebner para I^h com respeito a ordem monomial $>_h$ definida acima. Como $g_i \in I$, para todo $i = 1, \ldots, r$, temos que $g_i^h \in I^h$, para todo $i = 1, \ldots, r$.
Para mostrar que G^h é uma base de Groebner para I^h, precisamos provar que

$$\langle \mathrm{lt}_{>_h}(I^h) \rangle = \langle \mathrm{lt}_{>_h}(g_1^h), \ldots, \mathrm{lt}_{>_h}(g_r^h) \rangle.$$

Seja $p \in I^h$ e vamos provar que $\mathrm{lm}_{>_h}(p) \in \langle \mathrm{lt}_{>_h}(g_1^h), \ldots, \mathrm{lt}_{>_h}(g_r^h) \rangle$.
Como I^h é um ideal homogêneo, todas as componentes homogêneas de p pertencem a I^h. Digamos que F é a componente homogênea de p de maior grau. Então, $F \in I^h$ e F é homogêneo. Observe que

$$\mathrm{lm}_{>_h}(p) = \mathrm{lm}_{>_h}(F).$$

Assim, basta provar que

$$\mathrm{lm}_{>_h}(F) \in \langle \mathrm{lt}_{>_h}(g_1^h), \ldots, \mathrm{lt}_{>_h}(g_r^h) \rangle.$$

Pelo Teorema da Base de Hilbert, existem $f_1, \ldots, f_m \in I$ tais que

$$I^h = \langle f_1^h, \ldots, f_m^h \rangle.$$

Como $F \in I^h$ temos que

$$F = \sum_{j=1}^{m} A_j f_j^h,$$

para alguns $A_1, \ldots, A_m \in S[u]$. Seja $f = F(t_1, \ldots, t_s, 1)$ a desomogeneização de F com respeito a u. Assim,

$$f = F(t_1, \ldots, t_s, 1) = \sum_{j=1}^{m} A_j(t_1, \ldots, t_s, 1) f_j^h(t_1, \ldots, t_s, 1) = \sum_{j=1}^{m} A_j(t_1, \ldots, t_s, 1) f_j.$$

Isso mostra que $f \in I$. Agora, homogeneizando f com respeito a u temos que

$$F = u^e f^h,$$

para algum $e \geq 0$. Assim, pelo Lema 3.2.21, segue que

$$lm_{>_h}(F) = u^e lm_{>_h}(f^h) = u^e lm_{>}(f). \tag{3.8}$$

Como G é uma base de Groebner para I, temos que

$$\langle lt_{>}(I) \rangle = \langle lt_{>}(g_1), \ldots, lt_{>}(g_r) \rangle.$$

Sabemos que $lt_{>}(f) \in lt_{>}(I)$, pois $f \in I$, logo

$$lt_{>}(f) \in \langle lt_{>}(g_1), \ldots, lt_{>}(g_r) \rangle,$$

ou seja, $lm_{>}(f)$ é divisível por $lm_{>}(g_i)$ para algum $i \in \{1, \ldots, r\}$.
Novamente, pelo Lema 3.2.21, temos que

$$lm_{>}(g_i) = lm_{>_h}(g_i^h).$$

Assim, $lm_{>}(f)$ é divisível por $lm_{>_h}(g_i^h)$ e sabemos, por (3.8), que $lm_{>_h}(F)$ é divisível por $lm_{>}(f)$, logo $lm_{>_h}(F)$ é divisível por $lm_{>_h}(g_i^h)$.
Isso prova que

$$lm_{>_h}(F) \in \langle lt_{>_h}(g_1^h), \ldots, lt_{>_h}(g_r^h) \rangle,$$

portanto, G^h é uma base de Groebner para I^h com respeito a ordem monomial $>_h$.

□

Teorema 3.2.23 *Se $f_1, \ldots, f_r$ é um base de Groebner para $I(X)$ com respeito a alguma ordem monomial graduada em S, então $f_1^h, \ldots, f_r^h$ é uma base de Groebner para $I(X)^h$ e vale que*

$$I(Y) = I(X)^h = \langle f_1^h, \ldots, f_r^h \rangle.$$

Demonstração. Vejamos que $I(Y) \subset I(X)^h$. Seja $f \in I(Y)$, então $f \in S[u]$ é um polinômio homogêneo de grau d que se anula em Y. Seja $g := f(t_1, \ldots, t_s, 1) \in S$. Observe que $f = u^e g^h$, para algum $e \geq 0$. Seja $(a_1, \ldots, a_s) \in X$. Como f se anula em $[a_1, \ldots, a_s, 1]$, temos que $f(a_1, \ldots, a_s, 1) = 0$, ou seja, $g(a_1, \ldots, a_s) = 0$, logo g se anula em X e, portanto, $f = u^e g^h \in I(X)^h$.
Para provar a outra inclusão $I(X)^h \subset I(Y)$, basta mostrar que os geradores de $I(X)^h$ se anulam em Y. Seja f um gerador de $I(X)^h$, então $f = g^h$, para algum $g \in I(X)$. Seja $[a_1, \ldots, a_s, 1] \in Y$, então $(a_1, \ldots, a_s) \in X$ e como $g \in I(X)$, temos que

$$f(a_1, \ldots, a_s, 1) = g^h(a_1, \ldots, a_s, 1) = g(a_1, \ldots, a_s) = 0,$$

portanto, $f \in I(Y)$. Agora, segue imediatamente do Teorema 3.2.22 que $f_1^h, \ldots, f_r^h$ é uma base de Groebner para $I(X)^h$ e, em particular $I(X)^h = \langle f_1^h, \ldots, f_r^h \rangle$. □

Definição 3.2.24 *A* **função de Hilbert** *de* $S[u]/I(Y)$ *é dada por*

$$H_Y(d) := \dim_k \left(S[u]_d/I(Y)_d\right).$$

De modo análogo ao que fizemos para a função afim de Hilbert de $S/I(X)$, pode-se mostrar que $H_Y(d) = m = \#Y$, para todo $d \geq m-1$. Vamos denotar por $h_Y(t) = \sum_{i=0}^{r} c_i t^i \in \mathbb{Q}[t]$ o **polinômio de Hilbert** de $S[u]/I(Y)$. O número inteiro $c_r r!$ é chamado **grau** de $S[u]/I(Y)$ e denotado por $\deg\left(S[u]/I(Y)\right)$. Sabemos que, para d suficientemente grande $H_Y(d) = h_Y(d)$, veja [5].

Proposição 3.2.25 *A dimensão e o comprimento de* $C_X(d)$ *são iguais a* $H_Y(d)$ *e* $\deg\left(S[u]/I(Y)\right)$*, respectivamente.*

Demonstração. Já vimos que $S[u]_d/I(Y)_d \simeq C_Y(d) \simeq C_X(d)$, logo

$$\dim_K(C_X(d)) = \dim_K(C_Y(d)) = \dim_K\left(S[u]_d/I(Y)_d\right) = H_Y(d).$$

Sabemos que o grau do polinômio de Hilbert de $S[u]/I(Y)$ é igual a dimensão da variedade projetiva Y (veja [5]). Como Y é finito, segue que $h_Y(t)$ é igual a uma constante c_0, assim, $\deg\left(S[u]/I(Y)\right) = c_0$. Por outro lado, para d suficientemente grande, temos que

$$\#Y = H_Y(d) = h_Y(d),$$

logo, $h_Y(t) = c_0 = \#Y$, para todo $t \in \mathbb{N}$ e, portanto, o comprimento de $C_X(d)$ é dado por

$$\#X = \#Y = \deg\left(S[u]/I(Y)\right).$$

□

Capítulo 4

Código Parametrizado no Toro Afim

Vamos utilizar a teoria de bases de Groebner e a pegada de um ideal para calcular os parâmetros básicos de uma certa família de códigos parametrizados afins.

4.1 Toro Afim e Código Parametrizado no Toro Afim

Seja $K = \mathbb{F}_q$ um corpo finito com q elementos. Seja T o conjunto tórico algébrico afim parametrizado por $m_1 = x_1, \ldots, m_s = x_s$, onde $m_1, \ldots, m_s \in K[x_1, \ldots, x_s]$. Assim, T é dado por

$$\begin{aligned} T &= \{(m_1(a), \ldots, m_s(a)) \in \mathbb{A}^s : a = (a_1, \ldots, a_s) \in (K^*)^s\} \\ &= \{(a_1, \ldots, a_s) \in \mathbb{A}^s : a_i \in K^*, \forall\ i = 1, \ldots, s\}. \end{aligned}$$

O conjunto T é chamado de **toro afim**. Como $\#(K^*) = q - 1$, segue que $\#T = (q-1)^s$. Digamos que

$$T = \{p_1, p_2, \ldots, p_{(q-1)^s}\}.$$

Sejam $f_1, \ldots, f_s \in K[t_1, \ldots, t_s]$ dados por $f_i := t_i^{q-1} - 1$, para todo $i = 1, \ldots, s$ e considere o ideal

$$I = \langle f_1, \ldots, f_s \rangle.$$

Veja que $V(I) = T$. De fato: seja $a = (a_1, \ldots, a_s) \in T$, então $a_i \in K^*$, para todo $i = 1, \ldots, s$ e $f_i(a_i) = a_i^{q-1} - 1 = 0$, para todo $i = 1, \ldots, s$. Logo, $a \in V(I)$. Por outro lado, seja $b = (b_1, \ldots, b_s) \in V(I)$. Temos que

$$f_i(b_1, \ldots, b_s) = 0 \Longrightarrow b_i^{q-1} - 1 = 0 \Longrightarrow b_i^{q-1} = 1,$$

logo $b_i \neq 0$, i.e., $b_i \in K^*$, para todo $i = 1, \ldots, s$. Logo, $b \in T$.

Observe que $\#(\Delta(I)) = (q-1)^s$. De fato: como $\mathrm{lm}(f_i) = t_i^{q-1}$, para todo $i = 1, \ldots, s$, temos que

$$\Delta(I) \subset \{t_1^{\alpha_1} . \cdots . t_s^{\alpha_s} : 0 \leq \alpha_i < q - 1, \forall\, i = 1, \ldots, s\}.$$

Logo,

$$(q-1)^s = \#T = \#V(I) \leq \#\Delta(I) \leq (q-1)^s,$$

ou seja, $\#(\Delta(I)) = (q-1)^s$.

Proposição 4.1.1 *A aplicação*

$$\begin{array}{rcl} \varphi : K[t_1,\ldots,t_s]/I & \longrightarrow & K^{(q-1)^s} \\ f+I & \longmapsto & (f(p_1),\ldots,f(p_{(q-1)^s})) \end{array}$$

é um isomorfismo de K*-espaços vetoriais.*

Demonstração. É claro que φ é uma transformação linear. Do Teorema 2.4.4 e do exposto acima segue que

$$\dim(K[t_1,\ldots,t_s]/I) = \#(\Delta(I)) = (q-1)^s.$$

Pelo Lema 2.5.4 existem polinômios $f_1,\ldots,f_{(q-1)^s} \in K[t_1,\ldots,t_s]$ tais que $f_i(p_j) = \delta_{ij}$ para todo $i,j \in \{1,\ldots,(q-1)^s\}$, então $\varphi(f_i) = e_i$, onde e_i é o i-ésimo vetor da base canônica de $K^{(q-1)^s}$, para todo $i = 1,\ldots,(q-1)^s$. Isso prova que φ é sobrejetora e *a fortiori* um isomorfismo. □

Para todo inteiro $d \geq 0$, considere o K-espaço vetorial de $K[t_1,\ldots,t_s]/I$ dado por

$$L_{\leq d} := \{p + I : p = 0 \text{ ou } \deg(p) \leq d\}.$$

Definição 4.1.2 *O* **código parametrizado no toro afim**, $C_T(d)$, *é a imagem* $\varphi(L_{\leq d})$.

É claro que o comprimento de $C_T(d)$ é igual a $(q-1)^s$.

Lema 4.1.3 $\{f_1,\ldots,f_s\}$ *é uma base de Groebner para* I.

Demonstração. Basta notar que os monômios líderes de f_i e f_j são primos entre si, para todos $i,j \in \{1,\ldots,s\}$, com $i \neq j$. □

Lema 4.1.4 *O ideal de* T *é* I*, isto é,* $I(T) = I$.

Demonstração. É claro que $I \subset I(T)$, daí $\Delta(I(T)) \subset \Delta(I)$. Como T é uma variedade afim, sabemos que $V(I(T)) = T$. Então, temos que

$$(q-1)^s = \#T = \#(V(I(T))) \leq \#(\Delta(I(T))) \leq \#(\Delta(I)) = (q-1)^s,$$

logo, $\#(\Delta(I(T))) = (q-1)^s$. Assim, $\Delta(I(T)) \subset \Delta(I)$ e eles possuem o mesmo número de elementos, portanto $\Delta(I(T)) = \Delta(I)$.
Pelo lema anterior, sabemos que $\{f_1,\ldots,f_s\}$ é base de Groebner para I, logo

$$\Delta(I) = \Delta(\mathrm{lm}(f_1),\ldots,\mathrm{lm}(f_s)),$$

então $\Delta(I(T)) = \Delta(\mathrm{lm}(f_1),\ldots,\mathrm{lm}(f_s))$. E como $f_i \in I(T)$, para todo $i = 1,\ldots,s$, segue que $\{f_1,\ldots,f_s\}$ é uma base (de Groebner) para $I(T)$. Portanto, $I(T) = \langle f_1,\ldots,f_s\rangle = I$. □

Seja $\Delta(I)_{\leq d} := \{M \in \Delta(I) : \deg(M) \leq d\}$.

Proposição 4.1.5 *O conjunto* $\left\{M + I : M \in \Delta(I)_{\leq d}\right\}$ *é uma base para* $L_{\leq d}$.

Demonstração. Pelo Teorema 2.4.4, nós sabemos que $\left\{M + I : M \in \Delta(I)_{\leq d}\right\}$ é um conjunto linearmente independente, e claramente está contido em $L_{\leq d}$.
Seja $f \in K[t_1,\ldots,t_s], f \neq 0$ tal que $\deg(f) \leq d$. Seja r o resto da divisão de f por $\{f_1,\ldots,f_s\}$. Do algoritmo da divisão, do fato de $\{f_1,\ldots,f_s\}$ ser uma base de Groebner para I e da Proposição 2.4.2, segue que r é uma combinação linear de monômios em $\Delta(I)_{\leq d}$, isso termina a demonstração. □

4.2 Dimensão e Distância Mínima

Agora, nós vamos calcular a dimensão e a distância mínima de $C_T(d)$. Como φ é um isomorfismo e $C_T(d) = \varphi(L_{\leq d})$, temos que $\dim C_T(d) = \dim_K L_{\leq d}$.

Proposição 4.2.1 *Para todo inteiro* $d \geq s(q-2)$ *temos que:*

(i) $\dim C_T(d) = \#(\Delta(I)_{\leq d}) = (q-1)^s$.

(ii) $d_{\min} C_T(d) = 1$.

Demonstração.

(i) Da Proposição 4.1.5 e do fato de φ ser um isomorfismo, segue que

$$\dim C_T(d) = \dim_K L_{\leq d} = \#(\Delta(I)_{\leq d}).$$

Agora, observe que, como $\{f_1, \ldots, f_s\}$ é uma base de Groebner para I, então

$$\Delta(I) = \{t_1^{\alpha_1} \cdot \cdots \cdot t_s^{\alpha_s} : 0 \leq \alpha_i \leq q-2, \forall\, i = 1, \ldots, s\}.$$

Como $d \geq s(q-2)$, temos que $\Delta(I)_{\leq d} = \Delta(I)$, logo $\#\Delta(I)_{\leq d} = \#\Delta(I) = (q-1)^s$.

(ii) Como φ é um isomorfismo e $\varphi(L_{\leq d}) = K^{(q-1)^s}$, segue que $d_{\min} C_T(d) = 1$.

□

Teorema 4.2.2 *A dimensão de* $C_T(d)$ *para* $0 \leq d < s(q-2)$ *é dada por*

$$\dim(C_T(d)) = \sum_{j=0}^{\lfloor \frac{d}{q-1} \rfloor} (-1)^j \binom{s}{j} \binom{s+d-j(q-1)}{s}$$

onde o conjunto $\binom{a}{b} = 0$ *se* $a < b$.

Demonstração. Seja $0 \leq d < s(q-2)$ e seja $\mathcal{M}_{\leq d}$ o conjunto de todos os monômios de $K[t_1, \ldots, t_s]$ de grau até d. Para cada $j \in \{1, \ldots, s\}$ defina $M(j) := \{M \in \mathcal{M} : \mathrm{lm}(f_j) \mid M\}$. Assim, temos que

$$\Delta(I)_{\leq d} = \mathcal{M}_{\leq d} - \bigcup_{j=1}^{s} M(j)_{\leq d}.$$

Sabemos que $\#(\mathcal{M}_{\leq d}) = \binom{s+d}{d}$ e pelo Princípio da Inclusão-Exclusão, segue que

$$\begin{aligned}
\#\left(\bigcup_{j=1}^{s} M(j)_{\leq d}\right) &= \sum_{j=1}^{s} \#(M(j)_{\leq d}) - \sum_{2 \leq j_1 < j_2 \leq s} \#(M(j_1)_{\leq d} \cap M(j_2)_{\leq d}) + \cdots + (-1)^s \#\left(\bigcap_{j=2}^{s} M(j)_{\leq d}\right) \\
&= \left[\binom{s}{1}\binom{s+d-(q-1)}{s} - \binom{s}{2}\binom{s+d-2(q-1)}{s} + \binom{s}{3}\binom{s+d-3(q-1)}{s}\right. \\
&\quad \left. + \cdots + (-1)^{s+1}\binom{s}{s}\binom{s+d-s(q-1)}{s}\right]
\end{aligned}$$

Logo,

$$\begin{aligned}
\#(\Delta(I)_{\leq d}) &= \#(\mathcal{M}_{\leq d}) - \#\left(\bigcup_{j=1}^{s} M(j)_{\leq d}\right) \\
&= \binom{s}{0}\binom{s+d-0\cdot(q-1)}{s} - \binom{s}{1}\binom{s+d-1\cdot(q-1)}{s} \\
&\quad + \binom{s}{2}\binom{s+d-2(q-1)}{s} + \cdots + (-1)^s\binom{s}{s}\binom{s+d-s(q-1)}{s} \\
&= \sum_{j=0}^{s}(-1)^j\binom{s}{j}\binom{s+d-j(q-1)}{s},
\end{aligned}$$

admitindo que $\binom{a}{b} = 0$ quando $a < b$.

Seja $j \in \{0, \ldots, s\}$ tal que $d - j(q-1) \geq 0$ e $d - (j+1)(q-1) < 0$. Observe que

$$\frac{d}{q-1} - 1 < j \leq \frac{d}{q-1}, \text{ isto é, } j = \left\lfloor \frac{d}{q-1} \right\rfloor.$$

Assim, temos que

$$\dim C_T(d) = \#(\Delta(I)_{\leq d}) = \sum_{j=0}^{\lfloor \frac{d}{q-1} \rfloor}(-1)^j\binom{s}{j}\binom{s+d-j(q-1)}{s}.$$

□

Para obtermos a distância mínima de $C_T(d)$ para $0 \leq d < s(q-2)$, precisaremos do seguinte resultado:

Lema 4.2.3 *Seja* $0 \leq d < s(q-2)$ *um inteiro e seja* $m(\alpha_1, \ldots, \alpha_s) := \prod_{i=1}^{s}(q-1-\alpha_i)$, *onde* $0 \leq \alpha_i < q-1$ *são inteiros, para todo* $i = 1, \ldots, s$. *Então*

$$\min\{m(\alpha_1, \ldots, \alpha_s) : \alpha_1 + \cdots + \alpha_s \leq d\} = (q-1)^{s-k-1}(q-1)^{\ell},$$

onde k *e* ℓ *são unicamente determinados por* $k \geq 0, 1 \leq \ell \leq q-2$ *e* $d = k(q-2) + \ell$.

Demonstração. Considere o conjunto

$$N_d = \left\{ \alpha = (\alpha_1, \ldots, \alpha_s) \in \mathbb{N}^s : \sum_{i=1}^{s} \alpha_i \leq d \text{ e } 0 \leq \alpha_i < q-1, 1 \leq i \leq s \right\}.$$

Vamos denotar $s(\alpha) = \sum_{i=1}^{s} \alpha_i$ e $m(\alpha) = \prod_{i=1}^{s}(q-1-\alpha_i)$. Observe que $m(\alpha) > 0$, para todo $\alpha \in N_d$, pois $q-1-\alpha_i > 0$, para todo $i \in \{1, \ldots, s\}$. Nosso objetivo é calcular

$$\mu_d := \min\{m(\alpha) : \alpha \in N_d\}.$$

Inicialmente, observe que o mínimo é atingido quando $s(\alpha) = d$, isto é,

$$\mu_d = \min\{m(\alpha) : \alpha \in N_d \text{ e } s(\alpha) = d\}.$$

Seja $\alpha \in N_d$ tal que $s(\alpha) < d$. Vamos encontrar $\widetilde{\alpha} \in N_d$ tal que $s(\widetilde{\alpha}) = s(\alpha)+1$ e $m(\widetilde{\alpha}) < m(\alpha)$. Isso prova que se $\alpha \in N_d$ e $m(\alpha) = \mu_d$, então $s(\alpha) = d$.
Temos que $s(\alpha) < d < s(q-2)$. Observe que existe $i \in \{1, \ldots, s\}$ tal que $\alpha_i < q-2$, pois do contrário, $\alpha_i = q-2$, para todo i, logo, $s(\alpha) = s(q-2)$, que é um absurdo. Considere $\widetilde{\alpha} = (\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_s)$ tal que

$$\widetilde{\alpha}_j = \begin{cases} \alpha_j, & \text{se } j \neq i \\ \alpha_j + 1, & \text{se } j = i \end{cases}$$

Assim, $\widetilde{\alpha}_i = \alpha_i + 1 < q-2+1 = q-1$ e $\widetilde{\alpha}_j = \alpha_j < q-1$, para todo $j \neq i$. Além disso, $s(\widetilde{\alpha}) = s(\alpha) + 1 \leq d$, logo, $\widetilde{\alpha} \in N_d$. Observe que para $j \neq i$, temos que $q-1-\widetilde{\alpha}_j = q-1-\alpha_j$ e $q-1-\widetilde{\alpha}_i = q-1-\alpha_i-1 < q-1-\alpha_i$, portanto,

$$m(\widetilde{\alpha}) = \prod_{j=1}^{s}(q-1-\widetilde{\alpha}_j) < \prod_{j=1}^{s}(q-1-\alpha_j) = m(\alpha).$$

Seja $\alpha \in N_d$ com $s(\alpha) = d$. Como $s(\alpha) < s(q-2)$, existe $i \in \{1, \ldots, s\}$ tal que $\alpha_i < q-2$. Seja $j = \min\{i : \alpha_i < q-2\}$. Temos três possibilidades para j:

$$\text{(I) } j \leq k \qquad \text{(II) } j = k+1 \qquad \text{(III) } j > k+1$$

(I) Suponha que $j \leq k$. Nesse caso,

$$\begin{aligned} \alpha_1 + \cdots + \alpha_j &= (j-1)(q-2) + \alpha_j \\ &< (j-1)(q-2) + (q-2) \\ &= j(q-2) \\ &\leq k(q-2) \\ &< k(q-2) + \ell = d = s(\alpha). \end{aligned}$$

Assim, existe $j_1 > j$ tal que $\alpha_{j_1} > 0$. Seja $j' = \min\{j_1 : j_1 > j \text{ e } \alpha_{j_1} > 0\}$.

(I.1) Suponha que $\alpha_j + \alpha_{j'} \leq q-2$. Considere $\beta = (\beta_1, \ldots, \beta_s) \in \mathbb{N}^s$ tal que

$$\begin{cases} \beta_j &= \alpha_j + \alpha_{j'} \\ \beta_{j'} &= 0 \\ \beta_i &= \alpha_i, \text{ se } i \notin \{j, j'\} \end{cases}$$

Assim, $\beta_i < q-1$ para todo i e $s(\beta) = s(\alpha) = d$, logo, $\beta \in N_d$. Observe que α e β diferem apenas nas posições j e j'. É fácil ver que $(q-1-\alpha_j)(q-1-\alpha_{j'}) \geq (q-1-\beta_j)(q-1-\beta_{j'})$. Portanto,

$$m(\alpha) = \prod_{i=1}^{s}(q-1-\alpha_i) \geq \prod_{i=1}^{s}(q-1-\beta_i) = m(\beta).$$

(I.2) Suponha que $\alpha_j + \alpha_{j'} > q-2$. Considere $\beta = (\beta_1, \ldots, \beta_s) \in \mathbb{N}^s$ tal que

$$\begin{cases} \beta_j &= q-2 \\ \beta_{j'} &= \alpha_{j'} - (q-2-\alpha_j) \\ \beta_i &= \alpha_i, \text{ se } i \notin \{j, j'\} \end{cases}$$

Assim, $\beta_i < q-1$, para todo i, e $s(\beta) = s(\alpha) = d$. Logo, $\beta \in N_d$. Observe que α e β diferem apenas nas posições j e j'. Vejamos que $(q-1-\alpha_j)(q-1-\alpha_{j'}) \geq (q-1-\beta_j)(q-1-\beta_{j'})$. De fato, sejam $A = q-1-\alpha_j > 0$ e $B = q-1-\alpha_{j'} > 0$. Como

$A-1 \geq 0$ e $B-1 \geq 0$, temos que $(A-1)(B-1) \geq 0$, ou seja, $AB-A-B+1 \geq 0$, ou seja, $AB \geq A+B-1$. Assim, temos que

$$(q-1-\alpha_j)(q-1-\alpha_{j'}) \geq (q-1-\alpha_j)+(q-1-\alpha_{j'})-1.$$

Observe que

$$\begin{aligned}(q-1-\beta_j)(q-1-\beta_{j'}) &= q-1-(\alpha_{j'}-(q-2)+\alpha_j)\\ &= (q-1-\alpha_j)+(q-1-\alpha_{j'})-1\\ &\leq (q-1-\alpha_j)(q-1-\alpha_{j'}).\end{aligned}$$

Portanto, $m(\alpha) \geq m(\beta)$.

(II) Suponha que $j = k+1$. Nesse caso, temos que $\alpha_1 = \cdots = \alpha_k = q-2$ e $\alpha_{k+1} < q-2$. Se $\alpha_{k+1} = \ell$, então $\alpha_{k+2} = \cdots = \alpha_{s-1} = 0$. Tomamos $\beta = \alpha$, que teremos $m(\alpha) = m(\beta)$.
Se $\alpha_{k+1} < \ell$, temos que existe $j_2 > k+1$ tal que $\alpha_{j_2} > 0$. Seja

$$j' = \min\{j_2 : j_2 > k+1 \text{ e } \alpha_{j_2} > 0\}.$$

Observe que $\alpha_{k+1} + \alpha_{j'} \leq \ell \leq q-2$. Assim, como no caso (I.1), encontramos $\beta \in N_d$ com $s(\beta) = d$ tal que $m(\alpha) \geq m(\beta)$.

(III) Suponha $j > k+1$. Nesse caso, $\alpha_1 = \cdots = \alpha_{k+1} = q-2$. Como $s(\alpha) = d = k(q-2)+\ell$, com $1 \leq \ell \leq q-2$, temos que $\ell = q-2$ e que $\alpha_{k+2} = \cdots = \alpha_s = 0$. Tomamos $\beta = \alpha$, que teremos $m(\alpha) = m(\beta)$.

Seja $\gamma = (\gamma_1, \ldots, \gamma_s) \in \mathbb{N}^s$ tal que

$$\gamma_i = \begin{cases} q-2 & , \ 1 \leq i \leq k \\ \ell & , \ i = k+1 \\ 0 & , \ k+2 \leq i \leq s \end{cases}$$

Obtemos assim, um processo Γ que a cada $\alpha \in N_d$ com $s(\alpha) = d$, encontramos $\beta = \Gamma(\alpha)$ tal que $\beta \in N_d$ com $s(\beta) = d$ tal que $m(\alpha) \geq m(\beta)$. Basta mostrar que em um número finito de etapas este processo atinge o elemento γ.
Considere em N_d a ordem lexicográfica. Para todo $\alpha \in N_d$, com $s(\alpha) = d$ e $\alpha \neq \gamma$, temos que $\alpha < \Gamma(\alpha)$, logo em um número finito de etapas, temos que Γ atinge

$$\gamma = \max\{\alpha \in N_d : s(\alpha) = d\}.$$

Mostramos assim que $m(\gamma) \leq m(\alpha)$, para todo $\alpha \in N_d$ com $s(\alpha) = d$. Portanto,

$$\mu_d = m(\gamma) = (q-1-\ell)(q-1)^{s-k-1}.$$

□

Proposição 4.2.4 *Seja* $0 \leq d < s(q-2)$ *um inteiro, a distância mínima de* $C_T(d)$ *é igual a* $(q-1)^{s-k-1}(q-1-\ell)$*, onde* k *e* ℓ *são unicamente determinados por* $k \geq 0, 1 \leq \ell \leq q-2$ *e* $d = k(q-2)+\ell$.

Demonstração. Seja $f \in L_{\leq d}, f \neq 0$ e seja $J_f := \langle f, f_1, \ldots, f_s \rangle$. Temos que

$$\begin{aligned}\omega(\varphi(\bar{f})) &= d(\varphi(\bar{f}), 0)\\ &= \#\{p \in T : f(p) \neq 0\}\\ &= \#T - \#\{p \in T : f(p) = 0\}.\end{aligned}$$

Observe que $\#\{p \in T : f(p) = 0\} = \#(V(J_f))$. Logo, o peso de $\varphi(\bar{f})$ é dado por

$$\omega(\varphi(\bar{f})) = \#T - \#(V(J_f)) = (q-1)^s - \#(V(J_f)).$$

Do Teorema 2.5.5, temos que $\#(V(J_f)) \leq \#(\Delta(J_f))$. Sabemos que

$$\Delta(J_f) \subset \Delta(\mathrm{lm}(f), \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_s)),$$

logo $\#(\Delta(J_f)) \leq \#(\Delta(\mathrm{lm}(f), \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_s)))$. Note que

$$\begin{aligned} \Delta(\mathrm{lm}(f), \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_s)) &= \{M \in \Delta(I) : \mathrm{lm}(f) \nmid M\} \\ &= \Delta(I) - \{M \in \Delta(I) : \mathrm{lm}(f) \mid M\}. \end{aligned}$$

Digamos que $\mathrm{lm}(f) = t_1^{\alpha_1}.\cdots.t_s^{\alpha_s}$ e chame $\Delta_f := \{M \in \Delta(I) : \mathrm{lm}(f) \mid M\}$. Então, temos que

$$\#(\Delta_f) = \prod_{i=1}^{s}(q-1-\alpha_i).$$

De fato: se $M = t_1^{\beta_1}.\cdots.t_s^{\beta_s} \in \Delta_f$, então $M \in \Delta(I)$ e $\mathrm{lm}(f) \mid M$, ou seja, $\alpha_i \leq \beta_i \leq q-2$, para todo $i = 1, \ldots, s$. Assim, existem $q-1-\alpha_i$ possibilidades para cada β_i, com $i = 1, \ldots, s$. Logo, $\#(\Delta_f) = (q-1-\alpha_1).\cdots.(q-1-\alpha_s) = \prod_{i=1}^{s}(q-1-\alpha_i)$.

Então,

$$\begin{aligned} \#(\Delta(\mathrm{lm}(f), \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_s))) &= \#(\Delta(I)) - \#(\Delta_f) \\ &= (q-1)^s - \prod_{i=1}^{s}(q-1-\alpha_i). \end{aligned}$$

Portanto,

$$\#(V(J_f)) \leq \#(\Delta(J_f)) \leq \#(\Delta(\mathrm{lm}(f), \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_s))) = (q-1)^s - \prod_{i=1}^{s}(q-1-\alpha_i).$$

Assim, temos que

$$\omega(\varphi(\bar{f})) \geq (q-1)^s - (q-1)^s + \prod_{i=1}^{s}(q-1-\alpha_i) = \prod_{i=1}^{s}(q-1-\alpha_i).$$

Como $d_{\min}C_T(d) = \min\{\omega(\varphi(\bar{f})) : f \in L_{\leq d}, f \neq 0\}$, segue do lema anterior que

$$d_{\min}C_T(d) \geq (q-1)^{s-k-1}(q-1-\ell).$$

Para finalizar a demonstração, vejamos que essa cota é atingida. Sejam $A_1, \ldots, A_k, A_{k+1}$ subconjuntos de K^* tais que $\#A_1 = \cdots = \#A_k = q-2$ e $\#A_{k+1} = \ell$. Seja $g \in K[t_1, \ldots, t_s]$ dado por

$$g(t_1, \ldots, t_s) = \prod_{a_i \in A_1}(t_1 - a_i).\cdots.\prod_{b_i \in A_k}(t_k - b_i).\prod_{c_i \in A_{k+1}}(t_{k+1} - c_i).$$

Então, $\deg(g) = k(q-2) + \ell = d$ e g não se anula em $(q-1)^{s-k-1}(q-1-\ell)$ pontos de $T = (K^*)^s$. Logo,

$$\omega(\varphi(\bar{g})) = (q-1)^{s-k-1}(q-1-\ell).$$

□

Corolário 4.2.5 *Se* T *é um toro afim em* $\mathbb{A}^1$*, então* $C_T(d)$ *é um código MDS e sua distância mínima é dada por*

$$d_{min}(C_T(d)) = \begin{cases} q-1-d & se \quad 1 \leq d \leq q-3, \\ 1 & se \quad d \geq q-2. \end{cases}$$

Demonstração. Observe que $s = 1$. Se $d \geq q-2$, pela Proposição 4.2.1 segue que $d_{min}(C_T(d)) = 1$ e $\dim(C_T(d)) = \#T = q-1$, portanto,

$$d_{min}(C_T(d)) = \#T - \dim(C_T(d)) + 1,$$

isto é, $C_T(d)$ é um código MDS.
Se $d \leq q-3$, pela Proposição 4.2.4, temos que

$$d_{min}(C_T(d)) = (q-1)^{s-k-1}(q-1-\ell),$$

onde k e ℓ são unicamente determinados por $k \geq 0, 1 \leq \ell \leq q-2$ e $d = k(q-2)+\ell$. Como $d \leq q-3$, temos que $k = 0$ e $\ell = d$, logo $d_{min}(C_T(d)) = q-1-d$. Note que $\#T = q-1$ e pelo Teorema 4.2.2 temos que

$$\begin{aligned} \dim(C_T(d)) &= \sum_{j=0}^{1} (-1)^j \binom{1}{j} \binom{1+d-j(q-1)}{1} \\ &= \binom{1}{0}\binom{1+d}{1} - \binom{1}{1}\binom{1+d-(q-1)}{1} \\ &= \binom{1}{0}\binom{1+d}{1} = d+1, \end{aligned}$$

portanto, $d_{min}(C_T(d)) = \#T - \dim(C_T(d)) + 1$, ou seja, $C_T(d)$ é um código MDS.

□

Exemplo 4.2.6 *Seja* T *um toro afim em* $\mathbb{A}^2$ *e seja* $C_T(d)$ *o código parametrizado afim de grau* d *sobre o corpo* $K = \mathbb{F}_{11}$*. Sabemos que o comprimento de* $C_T(d)$ *é igual a* $\#T = 100$ *e usando os resultados vistos acima temos que*

d	$\dim_K(C_T(d))$	$d_{min}(C_T(d))$
1	3	90
2	6	80
3	10	70
4	15	60
5	21	50
6	28	40
7	36	30
8	45	20
9	55	10
10	64	9
11	72	8
12	79	7
13	85	6
14	90	5
15	94	4
16	97	3
17	99	2
18	100	1
19	100	1
20	100	1
⋮	⋮	⋮

Referências Bibliográficas

[1] T. Becker and V. Weipsfenning, "Gröbner Bases: A Computational aproach to Commutative Algebra", Springer Velarg, Berlin, 1993.

[2] B. Buchberger, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Mathematical Institute, University of Innsbruck, Austria. PhD Thesis. 1965. An English translation appeared in J. Symbolic Comput. 41 (2006) 475-511.

[3] B. Buchberger, A theoretical basis for the reduction of polynomials to canonical forms, SIGSAM Bull. (ACM Special Interest Group on Symbolic and Algebraic Manipulation) 10(3), 19-29, (1976).

[4] C. Carvalho, Gröbner bases methods in coding theory, Publications of CIMPA, Mexico, 2012.

[5] D.Cox, J.Little, D.O'Shea, Ideals, Varieties and Algorithms, second ed, Springer, Berlim, 1997.

[6] Hefez, A., Villela, M.L.T., Códigos Corretores de Erros, Série de Computação e Matemática, 2002.

[7] H.H. López, E. Sarmiento, M. Vaz Pinto and R. H. Villarreal, Parameterized affine codes, Studia Sci. Math. Hungar. 49 (2012), n. 3, 406-418.