GRÉGORY DURAN CUNHA

A Distância Mínima de Códigos Parametrizados no Toro Projetivo

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2014

GRÉGORY DURAN CUNHA

A Distância Mínima de Códigos Parametrizados no Toro Projetivo

Dissertação que será 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. Cícero Fernandes de Carvalho.

UBERLÂNDIA - MG
2014

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

C972d 2014

Cunha, Grégory Duran, 1989-
A distância mínima de códigos parametrizados no toro projetivo / Grégory Duran Cunha. - 2014.
67 p. : il.

Orientador: Cícero Fernandes de Carvalho.

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. Carvalho, Cícero Fernandes de. 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: Grégory Duran Cunha.

NÚMERO DE MATRÍCULA: 11212MAT006.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: A Distância Mínima de Códigos Parametrizados no Toro Projetivo.

ORIENTADOR: Prof. Dr. Cícero Fernandes de Carvalho.

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 14h30min, pela seguinte Banca Examinadora:

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

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; ao meu orientador Cícero Fernandes de Carvalho pelos ensinamentos e conselhos dados e aos professores Victor Gonzalo Lopez Neumann e Paulo Roberto Brumatti por terem aceito o convite para fazerem parte da minha banca.

CUNHA, G. D. *A Distância Mínima de Códigos Parametrizados no Toro Projetivo*. 2014. 66 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Este trabalho tem como objetivo apresentar os parâmetros de códigos parametrizados no toro algébrico projetivo. Também apresentamos uma caracterização para toros utilizando o conceito de "clutters". As ferramentas utilizadas provêm da teoria de bases de Groebner e da geometria algébrica. A tese contem uma breve introdução a esses conceitos, bem como os fatos básicos da teoria de corpos finitos e códigos lineares. Apresentamos ainda uma cota ótima para a regularidade do ideal de um toro projetivo.

Palavras-chave: Bases de Groebner; Clutter; Códigos de Avaliação; Distância mínima; Interseção Completa; Pegada.

CUNHA, G. D. *The minimum distance of parameterized codes on projective tori*. 2014. 66 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

This work aims at presenting the parameters of codes parameterized on the algebraic projective torus. We also present a characterization for the torus using the concept of clutters. The tool that we use come from Groebner basis theory and algebraic geometry. The thesis contains a brief introduction to these concepts as well as the basic facts from finite field theory and linear codes theory. We also present an optimal bound for the regularity of the ideal of a projective torus.

Keywords: Clutter; Complete Intersection; Evaluation Codes; Footprint; Groebner bases; Minimum distance.

Sumário

Introdução

Este trabalho trata de códigos corretores de erros, em particular, dos parâmetros básicos que são: distância mínima, dimensão e comprimento. Os códigos corretores de erros participam da vida moderna de inúmeras formas como, por exemplo, nas comunicações via satélite, na telefonia celular e na comunicação entre computadores. Um dos fundadores da teoria dos códigos corretores de erros foi o matemático americano *Claude Elwood Shannon*. Em 1948, Shannon publicou um importante artigo científico que tinha como título: *"A Mathematical Theory of Communication"*, enfocando o problema de qual é a melhor forma para codificar uma informação que um emissor queira transmitir para um receptor. Inicialmente, os maiores interessados na teoria dos códigos foram os matemáticos que a desenvolveram consideravelmente nas décadas de 50 e 60. A partir da década de 70, com as pesquisas espaciais e a grande popularização dos computadores, essa teoria começou a interessar também aos engenheiros, e desde então tem sido muito estudada.

Este trabalho está dividido em cinco capítulos. No primeiro capítulo, veremos alguns conceitos e resultados sobre bases de Groebner tais como: critério de Buchberger, algoritmo de Buchberger, base de Groebner minimal e base de Groebner reduzida. Além de exemplos, também incluímos uma série de resultados sobre estes conceitos. No segundo capítulo, apresentamos a definição do espaço projetivo n-dimensional, interpretação geométrica e algumas propriedades. Em seguida, definimos polinômios homogêneos, variedades projetivas, ideais homogêneos e vimos as propriedades que serão mais utilizadas no desenvolvimento deste trabalho.

O capítulo 3 trata de corpos finitos, que é uma ferramenta essencial para este trabalho. Iniciamos com algumas propriedades sobre a característica de um corpo finito, em seguida provamos alguns resultados auxiliares com a finalidade de provar a existência e unicidade de corpos finitos. O capítulo 4, traz somente uma breve introdução à teoria de códigos lineares para familiarizar o leitor com as definições e notações. Este capítulo contém os seguintes conceitos: definição de código linear, peso, distância de Hamming, comprimento, dimensão, distância mínima, cota de Singleton e códigos MDS.

No capítulo 5 introduzimos o conjunto tórico algébrico $X \subset \mathbb{P}^{s-1}$ parametrizado por s monômios de $K[y_1, \ldots, y_n]$. Assim, construímos o código parametrizado de ordem d, denotado por $C_X(d)$, como sendo a imagem de uma aplicação de avaliação. Um caso particular é quando consideramos o código $C_{\mathbb{T}}(d)$, onde $\mathbb{T}$ é um toro projetivo em $\mathbb{P}^{s-1}$. Neste capítulo 5, exibimos o índice de regularidade do ideal $I(\mathbb{T})$, além disso, encontramos o comprimento, a dimensão e a distância mínima do código $C_{\mathbb{T}}(d)$. Na parte final, provamos que quando X é uma interseção completa associada a um clutter, temos que $X = \mathbb{T}$, e isso nos permite encontrar uma cota ótima para a regularidade do ideal $I(X)$.

Grégory Duran Cunha
Uberlândia-MG, 27 de fevereiro de 2014.

Capítulo 1

Bases de Groebner

1.1 Bases de Groebner

Definição 1.1.1 *Um monômio em* $x_1, \ldots, x_n$ *é um produto da forma* $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$*, onde todos os expoentes são inteiros não negativos. O grau total deste monômio é a soma* $\alpha_1 + \cdots + \alpha_n$*.*

Poderemos simplificar a notação dos monômios da seguinte maneira: seja $\alpha = (\alpha_1, \ldots, \alpha_n)$ uma n-upla de inteiros não negativos. Então definimos $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Quando $\alpha = (0, \ldots, 0)$, temos que $x^\alpha = 1$, também definimos $|\alpha| = \alpha_1 + \cdots + \alpha_n$ como sendo o grau total do monômio x^α.

Definição 1.1.2 *Seja* $f = \sum_\alpha a_\alpha x^\alpha$ *um polinômio em* $K[x_1, \ldots, x_n]$*.*

(i) *Chamamos* a_α *de coeficiente do monômio* x^α*;*

(ii) *Se* $a_\alpha \neq 0$*, então chamamos* $a_\alpha x^\alpha$ *um termo de* f*;*

(iii) *O grau total de* f *é denotado por* $\deg(f)$*, é máximo* $|\alpha|$ *tal que* $a_\alpha \neq 0$*.*

Definição 1.1.3 *Uma ordem monomial* $\succeq$ *no conjunto dos monômios* $\mathbb{M}_n \subseteq K[x_1, \ldots, x_n]$ *é qualquer relação* $\succeq$ *em* $\mathbb{N}^n$*, ou equivalentemente, qualquer relação no conjunto dos monômios* x^α*,* $\alpha \in \mathbb{N}^n$*, satisfazendo:*

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

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

(iii) $\succeq$ *é uma boa ordem em* $\mathbb{N}^n$*, isso significa que todo subconjunto não vazio de* $\mathbb{N}^n$ *possui elemento mínimo em relação a* $\succeq$*.*

As ordens monomiais mais utilizadas são: lexicográfica, lexicográfica graduada e lexicográfica graduada reversa.

Seja $f = \sum_\alpha a_\alpha x^\alpha$ um polinômio não nulo em $K[x_1, \ldots, x_n]$ e $\geq$ uma ordem monomial. Definimos:

(i) O multigrau de f é $\mathrm{mdeg}(f) = \max\{\alpha \in \mathbb{N}^n : a_\alpha \neq 0\} \in \mathbb{N}^n$
(o máximo é tomado com relação à ordem $\geq$)

(ii) O coeficiente líder de f é $\mathrm{lc}(f) = a_{\mathrm{mdeg}(f)}$

(iii) O monômio líder de f é $\mathrm{lm}(f) = x^{\mathrm{mdeg}(f)}$

(iv) O termo líder de f é $\mathrm{lt}(f) = \mathrm{lc}(f) \cdot \mathrm{lm}(f)$

Exemplo 1.1.4 *Seja* $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ *e considere a ordem lexicográfica. Então,*

$\mathrm{mdeg}(f) = (3, 0, 0)$

$\mathrm{lc}(f) = -5$

$\mathrm{lm}(f) = x^3$

$\mathrm{lt}(f) = -5x^3$

Dado um ideal $I \subseteq K[x_1, \ldots, x_n]$, podemos definir o ideal dos termos líderes e dos monômios líderes:

Definição 1.1.5 *Seja* I *um ideal em* $K[x_1, \ldots, x_n]$*, com* $I \neq 0$*.*

(i) *Denotamos por* $\mathrm{lt}(I)$ *o conjunto dos termos líderes dos elementos de* I *e por* $\mathrm{lm}(I)$ *o conjunto dos monômios líderes dos elementos de* I*. Então*

$$\mathrm{lt}(I) = \{cx^\alpha : \exists f \in I \text{ tal que } \mathrm{lt}(f) = cx^\alpha\},$$

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

(ii) *Denotamos por* $\langle \mathrm{lt}(I) \rangle$ *o ideal gerado pelos elementos de* $\mathrm{lt}(I)$ *e por* $\langle \mathrm{lm}(I) \rangle$ *o ideal gerado pelos elementos de* $\mathrm{lm}(I)$*.*

Definição 1.1.6 *Fixe uma ordem monomial. Um subconjunto finito* $G = \{g_1, \ldots, g_t\}$ *de um ideal* I *é chamado uma base de Groebner se*

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

Definição 1.1.7 *Vamos denotar o resto na divisão de* f *pela* s*-upla ordenada* $F = (f_1, \ldots, f_s)$ *por* $\overline{f}^F$*.*

Definição 1.1.8 *Sejam* $f, g \in K[x_1, \ldots, x_n]$ *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*. Nós chamamos* x^γ *o mínimo múltiplo comum de* $\mathrm{lm}(f)$ *e* $\mathrm{lm}(g)$*, e denotamos por* $x^\gamma = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$*.*

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

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

Exemplo 1.1.9 *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,*

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

Assim,

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

Lema 1.1.10 *Seja* $\sum_{i=1}^{s} c_i f_i$ *com* $c_i \in K$ *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* K*-combinação linear de* S*-polinômios* $S(f_j, f_k)$, *com* $1 \leq j, k \leq s$. *Além disso,* $\operatorname{mdeg}(S(f_j, f_k)) < \delta$.

Demonstração. Seja $d_i := \operatorname{lc}(f_i)$, assim $\operatorname{lc}(c_i f_i) = c_i d_i$. Como $\operatorname{mdeg}(f_i) = \delta, \forall i = 1, \ldots, s$ 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 $\operatorname{lt}(\sum_{i=1}^{s} c_i f_i) = (\sum_{i=1}^{s} c_i d_i)\, x^{\delta}$, logo $\operatorname{mdeg}(\sum_{i=1}^{s} c_i f_i) = \delta$, 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 $\operatorname{lm}(f_i) = x^{\delta}, \forall i = 1, \ldots, s$, temos $\operatorname{lcm}(\operatorname{lm}(f_j), \operatorname{lm}(f_k)) = x^{\delta}$ para todo $i \in \{1, \ldots, s\}$.
Observe que

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

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 $\operatorname{lt}(p_i) = 1 x^{\delta}, \forall i = 1, \ldots, s$, temos que

$$\operatorname{mdeg}(S(f_j, f_k)) = \operatorname{mdeg}(p_j - p_k) < \delta.$$

■

Teorema 1.1.11 (Critério de Buchberger) *Sejam* $I \subseteq K[x_1, \ldots, x_n]$ *um ideal e* $G = \{g_1, \ldots, g_t\}$ *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 $\langle \operatorname{lt}(I) \rangle = \langle \operatorname{lt}(g_1), \ldots, \operatorname{lt}(g_t) \rangle$, basta mostrar que $\operatorname{lt}(I) \subseteq \langle \operatorname{lt}(g_1), \ldots, \operatorname{lt}(g_t) \rangle$.
Seja $f \in I \backslash \{0\}$. Como $I = \langle g_1, \ldots, g_t \rangle$, existem $h_1, \ldots, h_t \in K[x_1, \ldots, x_n]$ tais que

$$f = h_1 g_1 + \cdots + h_t g_t. \tag{1.1}$$

Assim,

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

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

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

Assim, $\mathrm{mdeg}(f) \leq \delta$. Agora, considere todas as possíveis maneiras em que f pode ser expressada na forma (1.1). 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 (1.1) para f tal que δ é minimal. Escolhido este δ minimal, é verdade que $\mathrm{mdeg}(f) = \delta$ (isto será provado!). Como $\delta = \max\{m(1), \ldots, m(t)\}$ temos que

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

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

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

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

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

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

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

$$\mathrm{mdeg}((h_i - \mathrm{lt}(h_i)) g_i) = \mathrm{mdeg}(h_i - \mathrm{lt}(h_i)) + \mathrm{mdeg}(g_i) <$$

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

Assim, a segunda e a terceira soma tem mdeg $< \delta$. Como $\mathrm{mdeg}(f) < \delta$, temos que a primeira soma também tem mdeg $< \delta$. Seja $\mathrm{lt}(h_i) = c_i X^{\alpha(i)}$, então a primeira soma $\sum_{m(i)=\delta} \mathrm{lt}(h_i) g_i = \sum_{m(i)=\delta} c_i X^{\alpha(i)} g_i$ tem exatamente a forma descrita no lema anterior, com $f_i = x^{\alpha(i)} g_i$, ou seja, $\mathrm{mdeg}(f_i) = \delta$ para todo i e $\mathrm{mdeg}\left(\sum_{m(i)=\delta} c_i f_i\right) < \delta$. 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 $x^{\gamma_{jk}} = \operatorname{lcm}(\operatorname{lm}(g_j), \operatorname{lm}(g_k))$. Então, existem constantes $c_{jk} \in K$ tais que

$$\sum_{m(i)=\delta} \operatorname{lt}(h_i) g_i = \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k). \tag{1.2}$$

Vejamos que $x^{\delta-\gamma_{jk}}$ é um monômio:
Seja $x^{\beta(i)} := \operatorname{lm}(g_i)$, para todo i. Como $\operatorname{mdeg}(x^{\alpha(i)} g_i) = \delta$ 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

$$\operatorname{mdeg}(a_{ijk} g_i) \leq \operatorname{mdeg}(S(g_j, g_k)). \tag{1.3}$$

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

$$\operatorname{mdeg}(b_{ijk} g_i) = \operatorname{mdeg}(x^{\delta-\gamma_{jk}} a_{ijk} g_i) = \operatorname{mdeg}(x^{\delta-\gamma_{jk}}) + \operatorname{mdeg}(a_{ijk} g_i) \overset{(1.3)}{\leq}$$

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

De (1.2) segue que

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

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

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

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

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

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

Exemplo: Sejam $g_1 = y - x^2$ e $g_2 = z - x^3$ em $K[x, y, z]$ 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.

1.2 O Algoritmo de Buchberger

Sabemos que todo ideal em $K[x_1, \ldots, x_n]$ 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 partindo de uma dada base para I. Mas, primeiro vejamos isto por um exemplo:

Considere o anel $K[x, y]$ 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 1.2.1 *O anel* $K[x_1, \ldots, x_n]$ *é noetheriano, isto é, dada uma cadeia ascendente de ideais em* $K[x_1, \ldots, x_n]$

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

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 $K[x_1, \ldots, x_n]$, de fato, $I \neq \emptyset$ pois $0 \in I$. Dados $f, g \in I$ e $p \in K[x_1, \ldots, x_n]$, existem índices j, k tais que $f \in I_j$ e $g \in I_k$, digamos que $I_j \subseteq I_k$. 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 $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$. 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, $f_i \in I_{j_i} \subseteq I_N$, para todo $i \in \{1, \ldots, s\}$. Logo,

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

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

Teorema 1.2.2 (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 $F \subseteq G$

$G := F$
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 $G' \subseteq G$ temos que $lt(G') \subseteq lt(G)$, e logo $\langle lt(G') \rangle \subseteq \langle lt(G) \rangle$. Observe que

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

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 $lt(r)$ não é divisível por nenhum dos termos líderes dos elementos de G', e portanto $lt(r) \notin \langle lt(G') \rangle$, mas como $r \in G$ temos $lt(r) \in \langle lt(G) \rangle$. Assim, é verdade que

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

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

$$\langle lt(G_1) \rangle \subseteq \langle lt(G_2) \rangle \subseteq \langle lt(G_3) \rangle \subseteq \cdots$$

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

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

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 $lt(S_N)$ 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. ■

Lema 1.2.3 *Seja* G *uma base de Groebner para um ideal polinomial* I. *Seja* $p \in G$ *um polinômio tal que* $lt(p) \in \langle lt(G - \{p\}) \rangle$. *Então,* $G - \{p\}$ *é também uma base de Groebner para* I.

Demonstração. Como $G - \{p\} \subseteq G$, temos que $lt(G - \{p\}) \subseteq lt(G)$, logo $\langle lt(G - \{p\}) \rangle \subseteq \langle lt(G) \rangle$. Por hipótese, $lt(p) \in \langle lt(G - \{p\}) \rangle$, logo $lt(G) \subseteq lt(G - \{p\})$, daí $\langle lt(G) \rangle \subseteq \langle lt(G - \{p\}) \rangle$.
Portanto, $\langle lt(G - \{p\}) \rangle = \langle lt(G) \rangle$.
Como G é uma base de Groebner para I, temos que $\langle lt(G - \{p\}) \rangle = \langle lt(G) \rangle = \langle lt(I) \rangle$. Logo, $G - \{p\}$ é uma base de Groebner para I. ■

Definição 1.2.4 Uma base de Groebner minimal para um ideal polinomial I é uma base de Groebner para I tal que:

(i) $lc(p) = 1$, para todo $p \in G$;

(ii) Para todo $p \in G$, $lt(p) \notin \langle lt(G - \{p\}) \rangle$.

Exemplo: Considere a ordem lexicográfica graduada e a seguinte lista de polinômios:

$$\begin{aligned} f_1 &= x^3 - 2xy \\ f_2 &= x^2y - 2y^2 + x \\ f_3 &= -x^2 \\ f_4 &= -2xy \\ f_5 &= -2y^2 + x \end{aligned}$$

Considere $I = \langle f_1, f_2\rangle$. Vimos anteriormente que $G = \{f_1, \ldots, f_5\}$ é uma base de Groebner para I. Veja que

$$\begin{aligned} lt(f_1) &= -xlt(f_3) \\ lt(f_2) &= -\tfrac{1}{2}xlt(f_4). \end{aligned}$$

Pelo lema anterior temos que $\{f_3, f_4, f_5\}$ é uma base de Groebner para I.
Agora considere

$$\begin{aligned} \widetilde{f_3} &= -1f_3 = x^2 \\ \widetilde{f_4} &= -\tfrac{1}{2}f_4 = xy \\ \widetilde{f_5} &= -\tfrac{1}{2}f_5 = y^2 - \tfrac{1}{2}x \end{aligned}$$

e $\widetilde{G} = \{\widetilde{f_3}, \widetilde{f_4}, \widetilde{f_5}\}$. Como $lt(\widetilde{f_i}) \notin \langle lt(\widetilde{G} - \{\widetilde{f_i}\})\rangle, i = 3,4,5$ e $lc(p) = 1, \ \forall \ p \in \widetilde{G}$, segue que $\widetilde{G}$ é uma base de Groebner minimal para I.

Observação: Infelizmente um ideal $I \subseteq K[x_1, \ldots, x_n]$ pode ter muitas bases de Groebner minimais. Por exemplo, o ideal I considerado acima também tem a seguinte base de Groebner minimal

$$\widehat{f_3} = x^2 + aXY, \ \widehat{f_4} = xy \ \text{ e } \ \widehat{f_5} = y^2 - \frac{1}{2}x,$$

com $a \in K$.

Definição 1.2.5 Uma base de Groebner reduzida para um ideal I é uma base de Groebner G para I tal que:

(i) $lc(p) = 1$, para todo $p \in G$;

(ii) Para todo $p \in G$, nenhum monômio de p pertence a $\langle lt(G - \{p\})\rangle$.

Se fizermos $a = 0$ na observação acima, obtemos uma base de Groebner reduzida para I.

Proposição 1.2.6 *Seja* $I \neq 0$ *um ideal polinomial. Então, fixada uma ordem monomial,* I *tem uma única base de Groebner reduzida.*

Demonstração. Seja G uma base de Groebner minimal para I. Vamos dizer que $g \in G$ é *reduzido* em G se nenhum monômio de g pertence a $\langle lt(G - \{g\})\rangle$.
Nosso objetivo é modificar G até que todos os seus elementos sejam reduzidos.

Afirmação 1: Se g é reduzido em G e H é uma outra base de Groebner minimal para I, com $g \in H$ e $lt(H) = lt(G)$, então g é reduzido em H.

De fato: Como $lt(G) = lt(H)$ e $g \in G \cap H$ temos que $lt(G - \{g\}) = lt(H - \{g\})$, logo $\langle lt(G - \{g\})\rangle = \langle lt(H - \{g\})\rangle$. Como g é reduzido em G, temos que nenhum monômio de g pertence a $\langle lt(G - \{g\})\rangle = \langle lt(H - \{g\})\rangle$, portanto g é reduzido em H.

Agora, dado $g \in G$ seja $g' = \overline{g}^{\,G-\{g\}}$ e considere $G' = (G - \{g\}) \bigcup \{g'\}$.

Afirmação 2: G' é uma base de Groebner minimal para I e g' é reduzido em G'.

- $lt(g') = lt(g)$:
  Como G é uma base de Groebner minimal para I, temos que $lt(g) \notin \langle lt(G - \{g\})\rangle$, logo $lt(g)$ não é divisível por nenhum dos termos líderes dos polinômios de $G - \{g\}$. Assim, $lt(g)$ será o termo líder do resto g' na divisão de g por $G - \{g\}$. Logo, $lt(g) = lt(g')$.

- G' é uma base de Groebner para I.
  Como $g \in I$ e $G - \{g\} \subset I$ segue que o resto g' pertence a I. Logo, $G' \subset I$. Sabemos que $lt(g') = lt(g)$, então $lt(G') = lt(G)$, logo $\langle lt(G')\rangle = \langle lt(G)\rangle = \langle lt(I)\rangle$, portanto G' é uma base de Groebner para I.

- G' é uma base de Groebner minimal para I.
  Como G é minimal, basta provar que $lt(g') \notin \langle lt(G' - \{g'\})\rangle$ e que $lc(g') = 1$.
  É claro que $lc(g') = 1$, pois $lt(g') = lt(g)$ e $lc(g) = 1$.
  De $G' - \{g'\} = G - \{g\}$ vem que $lt(G' - \{g'\}) = lt(G - \{g\})$, assim $\langle lt(G' - \{g'\})\rangle = \langle lt(G - \{g\})\rangle$. Como G é minimal e $g \in G$, temos que $lt(g') = lt(g) \notin \langle lt(G - \{g\})\rangle = \langle lt(G' - \{g'\})\rangle$, logo G' é minimal.

- g' é reduzido em G'.
  Como g' é o resto na divisão de g por $G - \{g\}$, segue que nenhum monômio de g' pertence ao ideal $\langle lt(G - \{g\})\rangle = \langle lt(G' - \{g'\})\rangle$. Logo, g' é reduzido em G'.

Agora, aplicando o processo acima em todos os elementos de G obtemos uma base de Groebner reduzida para I, já que este processo não modifica termos líderes.

Para provar a unicidade, considere G e $\widetilde{G}$ duas bases de Groebner reduzidas para I.

Afirmação 3: $lt(G) = lt(\widetilde{G})$

Observe que $\langle lt(G)\rangle = \langle lt(I)\rangle = \langle lt(\widetilde{G})\rangle$. Então $lt(G) \subseteq \langle lt(\widetilde{G})\rangle$ e $lt(\widetilde{G}) \subseteq \langle lt(G)\rangle$.
Seja $lt(g) \in lt(G)$, então $lt(g) \in \langle lt(\widetilde{G})\rangle$, logo $lt(g)$ é divisível por algum $lt(\widetilde{g})$ em $lt(\widetilde{G})$. Como $lt(\widetilde{g}) \in \langle lt(G)\rangle$, temos que $lt(\widetilde{g})$ é divisível por algum $lt(g_k)$ em $lt(G)$. Como G é reduzida, em particular minimal, segue que $lt(g) = lt(g_k)$.
Como $lt(\widetilde{g}) \mid lt(g)$ e $lt(g) \mid lt(\widetilde{g})$ temos que $lt(g) = lt(\widetilde{g}) \in lt(\widetilde{G})$, pois g e $\widetilde{g}$ tem coeficiente líder 1.
Portanto, $lt(G) = lt(\widetilde{G})$.

Como G e $\widetilde{G}$ são bases minimais, temos que $\#G = \#lt(G) = \#lt(\widetilde{G}) = \#\widetilde{G}$.
Como $lt(G) = lt(\widetilde{G})$, dado $g \in G$, existe $\widetilde{g} \in \widetilde{G}$ tal que $lt(g) = lt(\widetilde{g})$. Se provarmos que $g = \widetilde{g}$, concluímos que $G = \widetilde{G}$.
Como $g, \widetilde{g} \in I$ temos que $g - \widetilde{g} \in I$, e como G é uma base de Groebner para I, temos que $\overline{g - \widetilde{g}}^{G} = 0$. Vejamos que $\overline{g - \widetilde{g}}^{G} = g - \widetilde{g}$:
Como G é reduzida, temos que nenhum monômio de g pertence a $\langle lt(G - \{g\})\rangle$, então nenhum monômio de g, exceto $lm(g)$, pertence a $\langle lt(\widetilde{G})\rangle = \langle lt(G)\rangle$. Como g e $\widetilde{g}$ tem o mesmo termo líder, segue que este termo líder não aparece em $g - \widetilde{g}$, logo nenhum monômio de $g - \widetilde{g}$ pertence a $\langle lt(G)\rangle$. Portanto, $g - \widetilde{g}$ é resto na divisão de $g - \widetilde{g}$ por G. Logo, $g - \widetilde{g} = \overline{g - \widetilde{g}}^{G} = 0$ e portanto, $g = \widetilde{g}$. ■

Como consequência da proposição acima, temos o seguinte fato:

$\langle f_1, \ldots, f_s\rangle = \langle g_1, \ldots, g_t\rangle \iff \langle f_1, \ldots, f_s\rangle$ e $\langle g_1, \ldots, g_t\rangle$ tem a mesma base de Groebner reduzida.

Definição 1.2.7 Seja $G = \{g_1, \ldots, g_t\} \subseteq K[x_1, \ldots, x_n]$ e fixe uma ordem monomial. Dado $f \in K[x_1, \ldots, x_n]$, dizemos que f reduz a zero módulo G (notação: $f \longrightarrow_G 0$) se f pode ser escrito na forma

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

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

Lema 1.2.8 *Seja* $G = (g_1, \ldots, g_t)$ *um conjunto ordenado de elementos de* $K[x_1, \ldots, x_n]$ *e seja* $f \in K[x_1, \ldots, x_n]$. *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 $\overline{f}^{\,G} = -x - y \neq 0$. 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 1.2.9 *Uma base* $G = \{g_1, \ldots, g_t\}$ *para um ideal polinomial* I *é uma base de Groebner se, e somente se,* $S(g_i, g_j) \longrightarrow_G 0$, $\forall\, i \neq j$.

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 1.2.10 *Dado um conjunto finito* $G \subseteq K[x_1, \ldots, x_n]$, *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 $S(f, g) = S(cf, dg), \forall c, d \in K$, 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

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

Vejamos que

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

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

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

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

Exemplo: Seja $G = \{yz + y, x^3 + y, z^4\}$ e use a ordem lexicográfica graduada em $K[x, y, z]$. Como

$$\text{lcm}(x^3, z^4) = x^3z^4 = \text{lm}(x^3 + y)\text{lm}(z^4),$$

segue da proposição anterior que $S(x^3 + y, z^4) \longrightarrow_G 0$. No entanto, usando o algoritmo da divisão, obtemos

$$S(x^3 + y, z^4) = (z^3 - z^2 + z - 1)(yz + y) + 0 \cdot (x^3 + y) + 0 \cdot (z^4) + y,$$

então, $\overline{S(x^3 + y, z^4)}^{\,G} = y \neq 0$.

Capítulo 2

Geometria Algébrica Projetiva

2.1 Espaço Projetivo

Vamos denotar o espaço afim K^n por $\mathbb{A}^n(K)$.

Defina uma relação de equivalência em $\mathbb{A}^{n+1}(K) \setminus \{0\}$ da seguinte maneira:

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \Leftrightarrow (x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n), \text{ para algum } \lambda \in K^*.$$

Definição 2.1.1 *O espaço projetivo n-dimensional sobre K é o conjunto*

$$\mathbb{P}^n(K) = \left(\mathbb{A}^{n+1}(K) \setminus \{0\}\right) / \sim$$

Denotamos um ponto p de $\mathbb{P}^n(K)$ por

$$p = [x_0, \ldots, x_n] = \{(y_0, \ldots, y_n) : (x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)\},$$

e dizemos que $(x_0, \ldots, x_n)$ são as coordenadas homogêneas de p.

Geometricamente, podemos pensar nos pontos de $\mathbb{P}^n(K)$ como o conjunto das retas passando pela origem em $\mathbb{A}^{n+1}(K)$.

Proposição 2.1.2 *Seja $U_0 = \{[x_0, \ldots, x_n] \in \mathbb{P}^n(K) : x_0 \neq 0\}$. Então a aplicação*

$$\begin{array}{rcl} \phi : \mathbb{A}^n(K) & \longrightarrow & \mathbb{P}^n(K) \\ (a_1, \ldots, a_n) & \longmapsto & [1, a_1, \ldots, a_n] \end{array}$$

é injetora e $\mathrm{Im}\phi = U_0$.

Demonstração. Como $\phi(a_1, \ldots, a_n) = [1, a_1, \ldots, a_n] \in U_0$, podemos considerar

$$\phi : \mathbb{A}^n(K) \longrightarrow U_0.$$

Defina $\psi : U_0 \longrightarrow \mathbb{A}^n(K)$ por $[a_0, a_1, \ldots, a_n] \longmapsto \left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right)$.
Vejamos que ψ está bem definida:
Sejam $[a_0, \ldots, a_n] = [b_0, \ldots, b_n]$ em U_0, então existe $\lambda \in K^*$ tal que $(b_0, \ldots, b_n) = \lambda(a_0, \ldots, a_n)$.
Assim, $b_i = \lambda a_i$, para $i = 0, \ldots, n$. Logo,

$$\left(\frac{b_1}{b_0}, \ldots, \frac{b_n}{b_0}\right) = \left(\frac{\lambda a_1}{\lambda a_0}, \ldots, \frac{\lambda a_n}{\lambda a_0}\right) = \left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right).$$

Vejamos que $\psi \circ \phi = Id_{\mathbb{A}^n(K)}$ e $\phi \circ \psi = Id_{U_0}$, de fato:

$$\psi \circ \phi(a_1, \ldots, a_n) = \psi([1, a_1, \ldots, a_n]) = \left(\frac{a_1}{1}, \ldots, \frac{a_n}{1}\right) = (a_1, \ldots, a_n)$$

e

$$\phi \circ \psi([a_0, \ldots, a_n]) = \phi\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) = \left[1, \frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right] = [a_0, a_1, \ldots, a_n].$$

■

Assim, podemos identificar $\mathbb{P}^n(K) = U_0 \cup H$, onde

$$H = \{p \in \mathbb{P}^n(K) : p = [0, x_1, \ldots, x_n]\}.$$

Como ϕ é injetora e $Im\phi = U_0$ podemos identificar U_0 com $\mathbb{A}^n(K)$.
Como $\mathbb{P}^{n-1}(K) \longrightarrow H$, dada por $[x_1, \ldots, x_n] \longmapsto [0, x_1, \ldots, x_n]$ é uma bijeção, podemos identificar H com $\mathbb{P}^{n-1}(K)$. Assim, podemos escrever

$$\mathbb{P}^n(K) = \mathbb{A}^n(K) \cup \mathbb{P}^{n-1}(K).$$

Em particular, para $n = 1$ temos $\mathbb{P}^1(K) = \mathbb{A}^1(K) \cup \mathbb{P}^0(K)$, onde identificamos $\mathbb{P}^0(K)$ com o conjunto $\{[0, y] : y \in K\} = \{[0, 1]\}$. Então, $\mathbb{P}^0(K)$ tem um único ponto, e vamos denotá-lo por ∞. Portanto, a reta projetiva pode ser escrita como

$$\mathbb{P}^1(K) = \mathbb{A}^1(K) \cup \{\infty\}.$$

Vejamos que além de U_0 temos outras cópias de $\mathbb{A}^n(K)$ dentro de $\mathbb{P}^n(K)$.

Corolário 2.1.3 *Para cada* $i \in \{0, \ldots, n\}$ *seja*

$$U_i = \{[x_0, \ldots, x_n] \in \mathbb{P}^n(K) : x_i \neq 0\}.$$

(i) *Existe uma correspondência biunívoca entre* U_i *e* $\mathbb{A}^n(K)$*, para todo* $i = 0, \ldots, n$.

(ii) $\mathbb{P}^n(K) \setminus U_i$ *pode ser identificado com* $\mathbb{P}^{n-1}(K)$.

(iii) $\mathbb{P}^n(K) = \bigcup_{i=0}^{n} U_i$.

2.2 Variedades Projetivas

Nosso próximo objetivo é estender a definição de variedades ao espaço projetivo.
Por exemplo, se $f = x_1 - x_2^2 \in \mathbb{R}[x_0, x_1, x_2]$, podemos tentar construir $V(f) \subset \mathbb{P}^2(\mathbb{R})$ como sendo os pontos $[a, b, c]$ em $\mathbb{P}^2(\mathbb{R})$ tais que $f(a, b, c) = 0$. Nesse caso, como $f(1, 4, 2) = 0$ teríamos que $p = [1, 4, 2] \in V(f)$.
Observe que $2(1, 4, 2) = (2, 8, 4)$, logo $p = [2, 8, 4]$ e $f(2, 8, 4) = -8 \neq 0$, assim, $p \notin V(f)$.
Para evitar problemas desse tipo, vamos usar polinômios homogêneos para definir variedades projetivas.

Definição 2.2.1 *Um polinômio* f *é homogêneo de grau* d *se todo termo de* f *tem grau total igual a* d.

Exemplo 2.2.2 *Em* $K[x, y, z]$ *temos que* $x^2y^2 + 5x$ *não é homogêneo e* $x^7 + 2x^5y^2 - 3xy^6$ *é homogêneo de grau 7.*

Proposição 2.2.3 *Seja* $f \in K[x_0, \ldots, x_n]$ *um polinômio homogêneo de grau* d. *Se* $f(a_0, \ldots, a_n) = 0$ *então* $f(b_0, \ldots, b_n) = 0, \forall (b_0, \ldots, b_n) \in [a_0, \ldots, a_n]$. *Em particular,*

$$V(f) = \{[a_0, \ldots, a_n] \in \mathbb{P}^n(K) : f(a_0, \ldots, a_n) = 0\}$$

está bem definida como subconjunto de $\mathbb{P}^n(K)$.

Demonstração. Seja $(b_0, \ldots, b_n) \in [a_0, \ldots, a_n]$, digamos que $(b_0, \ldots, b_n) = \lambda(a_0, \ldots, a_n)$, para algum $\lambda \in K^*$.
Como f é homogêneo de grau d, temos que

$$f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \ldots, a_n) = 0.$$

Logo, $f(b_0, \ldots, b_n) = 0$. ■

Definição 2.2.4 *Sejam* $f_1, \ldots, f_s \in K[x_0, \ldots, x_n]$ *polinômios homogêneos. O conjunto*

$$V(f_1, \ldots, f_s) = \{[a_0, \ldots, a_n] \in \mathbb{P}^n(K) : f_i(a_0, \ldots, a_n) = 0, \forall i = 1, \ldots, s\}$$

é chamado de variedade projetiva definida por $f_1, \ldots, f_s$.

Vejamos agora uma relação entre variedades afins e variedades projetivas.

Proposição 2.2.5 *Seja* $V = V(f_1, \ldots, f_s)$ *uma variedade projetiva em* $\mathbb{P}^n(K)$. *Então* $W = V \cap U_0$ *pode ser identificado com a variedade afim* $V(g_1, \ldots, g_s) \subset \mathbb{A}^n(K)$, *onde* $g_i(y_1, \ldots, y_n) = f_i(1, y_1, \ldots, y_n)$, *para todo* $i = 1, \ldots, s$.

Demonstração. Sabemos que

$$\begin{array}{rcl} \psi : U_0 & \longrightarrow & \mathbb{A}^n(K) \\ [a_0, \ldots, a_n] & \longmapsto & \left(\dfrac{a_1}{a_0}, \ldots, \dfrac{a_n}{a_0}\right) \end{array}$$

é uma bijeção.
Vejamos que $\psi(W) \subseteq V(g_1, \ldots, g_s)$:
Seja $\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) = \psi([a_0, \ldots, a_n])$, onde $[a_0, \ldots, a_n] \in W$. Como $W = V \cap U_0, [a_0, \ldots, a_n] \in U_0$, logo $a_0 \neq 0$.
Como $[a_0, \ldots, a_n] = \left[1, \frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right] \in V$, temos que $f_i\left(1, \frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) = 0, \forall i = 1, \ldots, s$. Logo, $g_i\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) = 0, \forall i = 1, \ldots, s$. Portanto, $\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) \in V(g_1, \ldots, g_s)$.
Agora, vejamos que $V(g_1, \ldots, g_s) \subseteq \psi(W)$:
Seja $(a_1, \ldots, a_n) \in V(g_1, \ldots, g_s)$. Assim, $[1, a_1, \ldots, a_n] \in U_0$ e $f_i(1, a_1, \ldots, a_n) = g_i(a_1, \ldots, a_n) = 0, \forall i = 1, \ldots, s$.
Logo, $[1, a_1, \ldots, a_n] \in V \cap U_0 = W$, ou seja, $\psi^{-1}((a_1, \ldots, a_n)) \in W$, e portanto, $(a_1, \ldots, a_n) \in \psi(W)$. ■

Exemplo 2.2.6 *Considere a variedade projetiva* $V = V(x_1^2 - x_2x_0, x_1^3 - x_3x_0^2) \subseteq \mathbb{P}^3(\mathbb{R})$. *Para intersectar* V *com* U_0, *basta desomogeneizar os polinômios* $x_1^2 - x_2x_0$ *e* $x_1^3 - x_3x_0^2$ *fazendo* $x_0 = 1$. *Assim, obtemos*

$$W = V(x_1^2 - x_2, x_1^3 - x_3) \subseteq \mathbb{A}^3(\mathbb{R}).$$

Também podemos desomogeneizar com respeito a outras variáveis, por exemplo $V \cap U_1$ *é identificado com a variedade afim* $V(1 - x_2x_0, 1 - x_3x_0^2)$.

Definição 2.2.7 *Seja* $f \in K[x_1, \ldots, x_n]$ *com* $\deg f = d$. *Podemos escrever* f *de maneira única como*

$$f = \sum_{i=0}^{d} f_i,$$

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

Agora, vamos ver que uma variedade afim em U_i pode ser escrita como $V \cap U_i$ para alguma variedade projetiva V.
Por exemplo, considere a variedade afim $W = V(x_2 - x_1^3 + x_1^2)$ em $U_0 = \mathbb{A}^2(\mathbb{R})$. Como $f = x_2 - x_1^3 + x_1^2$ não é homogêneo, vamos incluir uma variável x_0 para tornar f homogêneo. Como f tem grau total 3, modificamos f de modo que todo termo tenha grau total igual a 3. Assim, obtemos

$$f^h = x_2x_0^2 - x_1^3 + x_1^2x_0.$$

Logo, $W = U_0 \cap V(f^h)$. Note que desomogeneizando f^h fazendo $x_0 = 1$, obtemos f.

Proposição 2.2.8 *Seja* $g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ *um polinômio de grau total* d.

(i) *Seja* $g = \sum_{i=0}^{d} g_i$ *a expansão de* g *como uma soma de componentes homogêneas, onde* g_i *tem grau total* i. *Então*

$$g^h(x_0, \ldots, x_n) = \sum_{i=0}^{d} g_i(x_1, \ldots, x_n)x_0^{d-i}$$

é um polinômio homogêneo de grau total d *em* $K[x_0, \ldots, x_n]$. *Chamamos* g^h *a homogeneização de* g *com respeito a* x_0.

(ii) *A homogeneização de* g *com respeito a* x_0 *pode ser calculada usando a fórmula*

$$g^h = x_0^d g\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right).$$

(iii) *Desomogeneizando* g^h *com respeito a* x_0 *obtemos* g, *isto é,*

$$g^h(1, x_1, \ldots, x_n) = g(x_1, \ldots, x_n).$$

(iv) *Seja* $F(x_0, \ldots, x_n)$ *um polinômio homogêneo e seja* x_0^e *a maior potência de* x_0 *que divide* F. *Se* $f = F(1, x_1, \ldots, x_n)$ *é uma desomogeneização de* F, *então* $F = x_0^e f^h$.

Demonstração.

(i) Como g_i tem grau total i segue que $g_ix_0^{d-i}$ tem grau total $i + d - i = d$. Logo,

$$g^h = g_0(x_1, \ldots, x_n)x_0^d + g_1(x_1, \ldots, x_n)x_0^{d-1} + \cdots + g_d(x_1, \ldots, x_n)x_0^{d-d}$$

é um polinômio homogêneo de grau total d em $K[x_1, \ldots, x_n]$.

(ii) Observe que

$$\begin{aligned}
x_0^d g\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) &= x_0^d \sum_{i=0}^{d} g_i\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \\
&= x_0 g_0\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) + x_0 g_1\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) + \cdots + x_0^d g_d\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \\
&= x_0^d g_0(x_1, \ldots, x_n) + x_0^d \frac{1}{x_0} g_1(x_1, \ldots, x_n) + \cdots + x_0^d \frac{1}{x_0^d} g_d(x_1, \ldots, x_n) \\
&= x_0^d g_0(x_1, \ldots, x_n) + x_0^{d-1} g_1(x_1, \ldots, x_n) + \cdots + x_0^{d-d} g_d(x_1, \ldots, x_n) \\
&= g^h.
\end{aligned}$$

(iii) Como $g^h(x_0,\ldots,x_n)=\sum_{i=0}^{d} g_i(x_1,\ldots,x_n)x_0^{d-i}$, temos que

$$g^h(1,x_1,\ldots,x_n)=\sum_{i=0}^{d} g_i(x_1,\ldots,x_n)1^{d-i}=g(x_1,\ldots,x_n).$$

(iv) Seja $d=\deg F$. Digamos que $F=a_1x_0^{p_1}x^{\alpha_1}+\cdots+a_tx_0^{p_t}x^{\alpha_t}$, onde $a_i\in K$ e x^{α_i} é um monômio em $K[x_1,\ldots,x_n]$.
Como F é homogêneo de grau d, temos que $p_i+|\alpha_i|=d, \forall i=1,\ldots,t$. Como $f=F(1,x_1,\ldots,x_n)$, temos que

$$f=a_1x^{\alpha_1}+\cdots+a_tx^{\alpha_t}.$$

Observe que $\deg f=d-e$, pois x_0^e é a maior potência de x_0 que divide F. Agora, digamos que

$$f^h=a_1x_0^{q_1}x^{\alpha_i}+\cdots+a_tx_0^{q_t}x^{\alpha_t}.$$

Assim, $q_i+|\alpha_i|=d-e, \forall i=1,\ldots,t$. Logo, $q_i+e=d-|\alpha_i|=p_i, \forall i=1,\ldots,t$. Portanto,

$$\begin{aligned} x_0^e f^h &= a_1x_0^{q_1+e}x^{\alpha_i}+\cdots+a_tx_0^{q_t+e}x^{\alpha_t}\\ &= a_1x_0^{p_1}x^{\alpha_1}+\cdots+a_tx_0^{p_t}x^{\alpha_t}\\ &= F. \end{aligned}$$

■

Observação: A homogeneização e a desomogeneização de um polinômio pode ser feita de forma análoga com respeito a qualquer outra variável.

Exemplo 2.2.9 *Seja* $g=y-x^3+x\in K[x,y]$ *e considere a variedade afim* $V(g)\subseteq U_2=\mathbb{A}^2(K)$. *Temos que* $g^h=yz^2-x^3+xz^2$. *Logo,* $V(g)$ *é identificada com* $V\cap U_2$ *em* $\mathbb{P}^2(K)$ *onde* $V=V(g^h)$.

Definição 2.2.10 *Seja* I *um ideal em* $K[x_0,\ldots,x_n]$. *Dizemos que* I *é um ideal homogêneo se para cada* $f\in I$, *as componentes homogêneas* f_i *de* f *também pertencem a* I.

Exemplo 2.2.11 *Seja* $I=\langle y-x^2\rangle\subseteq K[x,y]$. *As componentes homogêneas de* $f=y-x^2$ *são* $f_1=y$ *e* $f_2=-x^2$. *Nenhum desses polinômios pertencem a* I *pois nenhum é múltiplo de* $y-x^2$. *Portanto,* I *não é ideal homogêneo.*

Lema 2.2.12 *Sejam* $f,f_1,\ldots,f_s\in K[x_1,\ldots,x_n]$ *polinômios homogêneos. Dividindo* f *por* $f_1,\ldots,f_s$ *(com respeito a qualquer ordem monomial) escrevemos*

$$f=a_1f_1+\cdots+a_sf_s+r,$$

onde $a_1,\ldots,a_s,r\in K[x_1,\ldots,x_n]$ *e nenhum termo de* r *é divisível por nenhum dos termos líderes dos* $f_i's$. *Então,* $a_1,\ldots,a_s,r$ *também são polinômios homogêneos. Mais precisamente,* $\deg(r)=\deg(f)$ *e* $\deg(a_i)=\deg(f)-\deg(f_i)$, $1\le i\le s$.

Demonstração. Sejam $d=\deg f$ e $d_i=\deg f_i$ para $i=1,\ldots,s$.
Dividindo f por $f_1,\ldots,f_s$, olhamos para $\mathrm{lt}(f)$ e digamos que seja divisível por $\mathrm{lt}(f_j)$, assim a_j recebe um termo p de grau $d-d_j$ para que haja o cancelamento. Assim, temos que $f'=f-pf_j$ é o novo polinômio a ser dividido por $f_1,\ldots,f_s$. Agora, observe que pf_j é homogêneo de grau d. Logo, f' é homogêneo de grau d. Caso haja necessidade de retirar o $\mathrm{lt}(f')$ e adicioná-lo ao resto, temos que r já começa como um polinômio homogêneo de grau d.

Prosseguindo, vamos dividir f' por $f_1, \ldots, f_s$. Digamos que $\mathrm{lt}(f')$ seja divisível por $\mathrm{lt}(f_i)$, assim a_i recebe um termo q de grau $d - d_i$ para que ocorra o cancelamento. Assim, temos que $f'' = f' - qf_i$ é o novo polinômio a ser divido por $f_1, \ldots, f_s$. Observe que qf_i é homogêneo de grau d, logo f'' é homogêneo de grau d. Caso haja necessidade de retirar o $\mathrm{lt}(f'')$ e adicioná-lo ao resto, temos que r continua sendo um polinômio homogêneo de grau d. Observe também que se $i = j$, temos que $a_j = p + q$ continua sendo um polinômio homogêneo de grau $d - d_j$. Prosseguindo com o algoritmo da divisão, terminaremos com cada a_j homogêneo de grau $d - d_j$ e o resto homogêneo de grau d. ■

Lema 2.2.13 *Se* $f, g \in K[x_1, \ldots, x_n]$ *são polinômios homogêneos, então o* S*-polinômio* $S(f, g)$ *é homogêneo.*

Demonstração. Seja $x^\gamma = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$ e digamos que $\deg x^\gamma = d$.
Temos que

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

Sejam $d_1 = \deg f$ e $d_2 = \deg g$. Assim, $\deg\left(\frac{x^\gamma}{\mathrm{lt}(f)}\right) = d - d_1$ e $\deg\left(\frac{x^\gamma}{\mathrm{lt}(g)}\right) = d - d_2$.

Como f é homogêneo cada termo de f tem grau d_1, logo cada termo de $\frac{x^\gamma}{\mathrm{lt}(f)} f$ tem grau $(d - d_1) + d_1 = d$. Portanto, $\frac{x^\gamma}{\mathrm{lt}(f)} f$ é um polinômio homogêneo de grau d.

Como g é homogêneo cada termo de g tem grau d_2, logo cada termo de $\frac{x^\gamma}{\mathrm{lt}(g)} g$ tem grau $(d - d_2) + d_2 = d$. Portanto, $\frac{x^\gamma}{\mathrm{lt}(g)} g$ é um polinômio homogêneo de grau d.
Logo, $S(f, g)$ é um polinômio homogêneo de grau d. ■

Teorema 2.2.14 *Seja* I *um ideal em* $K[x_0, \ldots, x_n]$. *São equivalentes:*

(i) I *é ideal homogêneo.*

(ii) $I = \langle f_1, \ldots, f_s \rangle$, *onde* $f_1, \ldots, f_s$ *são polinômios homogêneos.*

(iii) *Uma base de Groebner reduzida para* I *(com respeito a qualquer ordem monomial) consiste de polinômios homogêneos.*

Demonstração.

(i) $\Rightarrow$ (ii) Suponha que I é um ideal homogêneo. Pelo Teorema da Base de Hilbert, temos que $I = \langle F_1, \ldots, F_t \rangle$, para alguns $F_1, \ldots, F_t \in K[x_0, \ldots, x_n]$. Escreva cada F_j como soma de suas componentes homogêneas

$$F_j = \sum_i F_{ji}.$$

Como I é homogêneo, temos que todos F_{ji} pertencem a I.
Seja I' o ideal gerado pelos polinômios homogêneos F_{ji}. Assim, cada $F_j = \sum_i F_{ji}$ pertencem a I'. Logo, $I \subseteq I'$. Como $F_{ji} \in I$ para todos i, j temos que $I' \subseteq I$. Portanto, $I = I'$.

(ii) $\Rightarrow$ (i) Se $f = \sum_i f_i$ e $g = \sum_i g_i$ são as expansões de dois polinômios como a soma de suas componentes homogêneas, então as componentes homogêneas h_k do produto $h = fg$ são dadas por

$$h_k = \sum_{i+j=k} f_i g_j,$$

de fato, observe que

$$fg = \sum_{i+j=0} f_i g_j + \sum_{i+j=1} f_i g_j + \cdots$$

é expansão de fg como soma de componentes homogêneas. Por hipótese, $I = \langle f_1, \ldots, f_s \rangle$ onde $f_1, \ldots, f_s$ são polinômios homogêneos.
Seja $f \in I$, então $f = a_1 f_1 + \cdots + a_s f_s$, para alguns $a_1, \ldots a_s \in K[x_0, \ldots, x_n]$. Escrevendo a_1 como a soma de suas componentes homogêneas temos

$$a_1 = \sum_i a_{1i}.$$

Como f_1 é homogêneo, digamos de grau d, temos que $f_1 = f_d$ é a expansão de f_1 como soma de suas componentes homogêneas. Logo, a expansão de $a_1 f_1$ como soma de suas componentes homogêneas é

$$a_1 f_1 = \sum_{i+d=0} a_{1i} f_d + \sum_{i+d=1} a_{1i} f_d + \cdots$$

Como $f_d = f_1 \in I$ temos que cada componente homogênea de $a_1 f_1$ pertence a I.
Esse processo pode ser feito para cada $a_i f_i$. Logo, cada componente homogênea de $a_i f_i$ pertence a I. Assim, cada componente homogênea de f pertence a I. Portanto, I é um ideal homogêneo.

(ii) $\Rightarrow$ (iii) Por hipótese, $I = \langle f_1, \ldots, f_s \rangle$, onde $f_1, \ldots, f_s$ são polinômios homogêneos. Pelo Lema 2.2.13 os S-polinômios $S(f_i, f_j)$ são homogêneos.
Utilizando o Algoritmo de Buchberger obtemos uma base de Groebner

$$G = \{f_1, \ldots, f_s, f_{s+1}, \ldots, f_m\}$$

para I, onde $f_{s+1}, \ldots, f_m$ são obtidos como restos nas divisões dos S-polinômios por uma lista de $f_i's$, e logo $f_{s+1}, \ldots, f_m$ são polinômios homogêneos pelo Lema 2.2.12. Assim, temos uma base de Groebner G para I formada por polinômios homogêneos.
Como a base de Groebner reduzida $\widetilde{G}$ para I é tal que seus elementos são alguns dos elementos de G multiplicados por uma constante (para que tenham coeficiente líder igual a 1), segue que $\widetilde{G}$ é uma base de Groebner reduzida para I formada por polinômios homogêneos.

(iii) $\Rightarrow$ (ii) É imediato.

■

Seja I um ideal homogêneo em $K[x_0, \ldots, x_n]$. Vejamos que

$$V(I) = \{p \in \mathbb{P}^n(K) : f(p) = 0, \forall f \in I\},$$

está bem definido como um conjunto.
Seja $[a_0, \ldots, a_n] = [b_0, \ldots, b_n] \in \mathbb{P}^n(K)$ e suponha que $f(a_0, \ldots, a_n) = 0, \forall f \in I$. Vamos mostrar que $f(b_0, \ldots, b_n) = 0, \forall f \in I$.
Seja $f \in I$. Como $[a_0, \ldots, a_n] = [b_0, \ldots, b_n]$, existe $\lambda \in K^*$ tal que $(b_0, \ldots, b_n) = \lambda(a_0, \ldots, a_n)$. Como I é um ideal homogêneo, existem polinômios homogêneos $f_1, \ldots, f_s \in K[x_0, \ldots, x_n]$, digamos que $\deg(f_i) = d_i$, tais que $I = \langle f_1, \ldots, f_s \rangle$. Como $f \in I$, temos que

$$f = g_1 f_1 + \cdots + g_s f_s,$$

para alguns $g_1, \ldots, g_s \in K[x_0, \ldots, x_n]$. Temos que $f_i(a_0, \ldots, a_n) = 0, \forall i = 1, \ldots, s$, logo

$$\begin{aligned} f(b_0, \ldots, b_n) &= \sum_{i=1}^{s} g_i(b_0, \ldots, b_n) f_i(b_0, \ldots, b_n) \\ &= \sum_{i=1}^{s} g_i(\lambda a_0, \ldots, \lambda a_n) f_i(\lambda a_0, \ldots, \lambda a_n) \\ &= \sum_{i=1}^{s} g_i(\lambda a_0, \ldots, \lambda a_n) \lambda^{d_i} f_i(a_0, \ldots, a_n) \\ &= 0. \end{aligned}$$

Proposição 2.2.15 *Seja* I *um ideal homogêneo em* $K[x_0, \ldots, x_n]$ *e suponha que* $I = \langle f_1, \ldots, f_s \rangle$*, onde* $f_1, \ldots, f_s$ *são homogêneos. Então*

$$V(I) = V(f_1, \ldots, f_s).$$

Demonstração. Seja $p \in V(I)$. Como $f_1, \ldots, f_s \in I$, temos que $f_i(p) = 0, \forall i = 1, \ldots, s$. Logo, $p \in V(f_1, \ldots, f_s)$.
Agora, seja $q \in V(f_1, \ldots, f_s)$. Dado $f \in I$, temos que

$$f = g_1 f_1 + \cdots + g_s f_s,$$

para alguns $g_1, \ldots, g_s \in K[x_0, \ldots, x_n]$. Assim, temos que

$$f(q) = g_1(q) f_1(q) + \cdots + g_s(q) f_s(q) = 0.$$

Portanto, $q \in V(I)$. ■

Proposição 2.2.16 *Seja* $V \subseteq \mathbb{P}^n(K)$ *uma variedade projetiva e seja*

$$I(V) = \{f \in K[x_0, \ldots, x_n] : f(a_0, \ldots, a_n) = 0, \forall [a_0, \ldots, a_n] \in V\}$$

(isto significa que f *precisa zerar todas as coordenadas homogêneas de todos os pontos em* V*). Se* K *é infinito, então* $I(V)$ *é um ideal homogêneo em* $K[x_0, \ldots, x_n]$*.*

Demonstração. Como $I(V)$ é fechado para a soma e fechado para produtos com elementos de $K[x_0, \ldots, x_n]$, temos que $I(V)$ é um ideal.
Seja $f \in I(V)$, digamos que $\deg f = d$, e seja $a = [a_0, \ldots, a_n] \in V$. Escreva

$$f = \sum_{i=0}^{d} f_i,$$

onde $f_0, \ldots, f_d$ são as componentes homogêneas de f. Vamos mostrar que $f_i \in I(V)$, para todo $i \in \{0, \ldots, d\}$.
Como $f \in I(V)$ e $[a_0, \ldots, a_n] \in V$ temos que $f(\lambda a_0, \ldots, \lambda a_n) = 0, \forall \lambda \in K^*$.
Observe que

$$f(\lambda a_0, \ldots, \lambda a_n) = \sum_{i=0}^{d} f_i(\lambda a_0, \ldots, \lambda a_n) = \sum_{i=0}^{d} \lambda^i f_i(a_0, \ldots, a_n),$$

logo $\sum_{i=0}^{d} \lambda^i f_i(a_0, \ldots, a_n) = 0$, para todo $\lambda \in K^*$.
Defina

$$p(x) = \sum_{i=0}^{d} x^i f_i(a_0, \ldots, a_n) \in K[x].$$

Como $p(\lambda) = 0, \forall \lambda \in K^*$ e K^* é infinito, temos que $p = 0$, ou seja, todos os coeficientes de p são iguais a zero, isto é, $f_i(a_0, \ldots, a_n) = 0, \forall i = 0, \ldots, d$.
Como f_i é homogêneo temos que f_i se anula em todas as coordenadas homogêneas de a. Portanto, para cada $i \in \{0, \ldots, d\}$ temos que $f_i(a) = 0, \forall a \in V$, ou seja, $f_i \in I(V)$. Isso prova que $I(V)$ é um ideal homogêneo. ■

Proposição 2.2.17 *Seja $W \subseteq \mathbb{P}^n(K)$ uma variedade projetiva e suponha que $I(W)$ é um ideal homogêneo. Então $V(I(W)) = W$.*

Demonstração. Dado $p \in W$ temos que $f(p) = 0$ para todo $f \in I(W)$, logo $p \in V(I(W))$. Portanto, $W \subseteq V(I(W))$.
Por outro lado, como W é uma variedade projetiva, temos que $W = V(f_1, \ldots, f_s)$ para alguns polinômios homogêneos $f_1, \ldots, f_s$. Seja $J = \langle f_1, \ldots, f_s \rangle$, temos que $W = V(J)$. Assim, $I(W) = I(V(J))$.
É claro que $J \subseteq I(V(J)) = I(W)$, e logo $V(J) \supseteq V(I(W))$, ou seja, $W \supseteq V(I(W))$. ■

Capítulo 3

Corpos Finitos

Seja p um número primo positivo em $\mathbb{Z}$. Vamos denotar por $\mathbb{Z}_p$ o corpo $\mathbb{Z}/p\mathbb{Z}$.
Seja F um corpo com elemento unidade 1. Vamos denotar $\underbrace{1+\cdots+1}_{n \text{ parcelas}}$ por $n \cdot 1$.

3.1 A característica de um corpo finito

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

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

Observe que $\{n \cdot 1 : n \in \mathbb{N}\} \subseteq F$. 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, $n_2 - n_1 \in \Lambda_F$. Portanto, $\Lambda_F \neq \emptyset$.

Definição 3.1.1 *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 $\text{char}(K) = \text{char}(F)$.

Proposição 3.1.2 *Se* F *é um corpo finito, então* $\text{char}(F)$ *é um número primo.*

Demonstração. Seja $m = \text{char}(F)$ e suponha que m não seja primo. Logo, $m = m_1 \cdot m_2$, onde $1 < m_1, m_2 < m$. Então

$$0 = m \cdot 1 = (m_1 \cdot m_2) \cdot 1 = m_1 \cdot (m_2 \cdot 1) = (m_1 \cdot 1) \cdot (m_2 \cdot 1).$$

Como F é domínio, temos que $m_1 \cdot 1 = 0$ ou $m_2 \cdot 1 = 0$, o que contradiz a minimalidade de m. ■

Proposição 3.1.3 *Seja* F *um corpo finito com* $\text{char}(F) = p$. *Sejam* $m \in \mathbb{Z}$ *e* $a \in F$ *tais que* $m \cdot a = 0$. *Então,* m *é um múltiplo de* p *ou* $a = 0$.

Demonstração. Como $m \cdot a = 0$, temos que $(m \cdot 1) \cdot a = 0$, logo $m \cdot 1 = 0$ ou $a = 0$.
Suponha que $m \cdot 1 = 0$. Dividindo m por p, obtemos q e r inteiros tais que $m = q \cdot p + r$, onde $0 \leq r < p$. Logo,

$$0 = m \cdot 1 = (q \cdot p + r) \cdot 1 = q \cdot (p \cdot 1) + r \cdot 1 = 0 + r \cdot 1 = r \cdot 1.$$

Pela minimalidade de p temos que $r = 0$. ■

Teorema 3.1.4 *Seja* F *um corpo finito com* $\mathrm{char}(F) = p$*, onde* p *é um número primo. então* F *contém um subcorpo isomorfo a* $\mathbb{Z}_p$ *(que ainda denotaremos por* $\mathbb{Z}_p$*). Em particular,* F *tem* p^n *elementos para algum natural* n*.*

Demonstração. Considere o homomorfismo

$$\begin{aligned} \varphi : \mathbb{Z}_p &\longrightarrow F \\ \overline{m} &\longmapsto m \cdot 1 \end{aligned}$$

Vejamos que esta aplicação está bem definida:
Sejam $\overline{m} = \overline{k}$ em $\mathbb{Z}_p$, então $m \equiv k (\mathrm{mod}\, p)$, ou seja, existe $\lambda \in \mathbb{Z}$ tal que $m = k + \lambda p$. Logo,

$$m \cdot 1 = (k + \lambda p) \cdot 1 = k \cdot 1 + (\lambda p) \cdot 1 = k \cdot 1 + \lambda \cdot (p \cdot 1) = k \cdot 1 + 0 = k \cdot 1.$$

Seja $\overline{m} \in \ker \varphi$, então $m \cdot 1 = 0$. Logo, $p \mid m$, ou seja, $\overline{m} = \overline{0}$. Portanto, $\ker \varphi = \{0\}$.
Assim, $\mathbb{Z}_p \simeq \mathbb{Z}_p / \ker \varphi \simeq \varphi(\mathbb{Z}_p)$. Portanto, $\mathbb{Z}_p$ é isomorfo ao subcorpo $\varphi(\mathbb{Z}_p)$ de F.
Observe que F é um $\mathbb{Z}_p$-espaço vetorial de dimensão finita, pois F é finito. Digamos que $\dim_{\mathbb{Z}_p} F = n$ e seja $\{v_1, \ldots, v_n\}$ uma base para F. Então, todo elemento de F se escreve de modo único na forma

$$a_1 v_1 + \cdots + a_n v_n,$$

com $a_i \in \mathbb{Z}_p, i = 1, \ldots, n$. Portanto, $|F| = p^n$ elementos. ∎

Proposição 3.1.5 *Seja* F *um corpo finito de característica* p *e seja* $q = p^r$ *para algum* $r \in \mathbb{N}$*. Se* $a, b \in F$*, temos que*

$$(a + b)^q = a^q + b^q \text{ e } (a - b)^q = a^q - b^q.$$

Demonstração. Faremos uma indução sobre r. Para $r = 1$, utilizando o binômio de Newton, temos que

$$(a + b)^p = \binom{p}{0} a^p b^0 + \binom{p}{1} a^{p-1} b^1 + \cdots + \binom{p}{p-1} a^1 b^{p-1} + \binom{p}{p} a^0 b^p.$$

Como $p \mid \binom{p}{i}$, para todo $i = 1, \ldots, p-1$. Temos que $(a + b)^p = a^p + b^p$.
Também temos que

$$(a - b)^p = \binom{p}{0} a^p b^0 - \binom{p}{1} a^{p-1} b^1 + \cdots + (-1)^p \binom{p}{p} a^0 b^p.$$

Logo, $(a - b)^p = a^p + (-1)^p b^p = a^p - b^p$ (pois, para $p = 2$, temos que $1 \equiv -1 \pmod 2$).
Suponha o resultado verdadeiro para $r - 1$.
Observe que

$$(a + b)^{p^r} = ((a + b)^{p^{r-1}})^p \overset{\text{h.i.}}{=} (a^{p^{r-1}} + b^{p^{r-1}})^p = a^{p^r} + b^{p^r}.$$

E também

$$(a - b)^{p^r} = ((a - b)^{p^{r-1}})^p \overset{\text{h.i.}}{=} (a^{p^{r-1}} - b^{p^{r-1}})^p = a^{p^r} - b^{p^r}.$$

Portanto, $(a + b)^q = a^q + b^q$ e $(a - b)^q = a^q - b^q$. ∎

Observação: Se $a_1, \ldots, a_n$ são elementos de um corpo finito F de característica p, e se q é uma potência de p, então:

(i) $(a_1 + \cdots + a_n)^q = a_1^q + \cdots + a_n^q$
De fato: faremos uma indução sobre n. Para $n = 1, 2$ já sabemos ser verdade.
Suponha que este fato seja verdadeiro para $n - 1$. Assim,

$$(a_1 + \cdots + a_n)^q = (a_1 + \cdots + a_{n-1})^q + a_n^q \overset{\text{h.i.}}{=} a_1^q + \cdots + a_n^q.$$

(ii) Se $p(x) = a_0 + a_1x + \cdots + a_nX^n \in F[x]$, então

$$p(x)^q = a_0^q + a_1^qX^q + \cdots + a_n^qX^{nq}.$$

Corolário 3.1.6 *Seja* F *um corpo finito com* $\mathrm{char}(F) = p$. *Se* $q = p^r$ *para algum* $r \in \mathbb{N}$, *então*

$$\begin{aligned} f_q : F &\longrightarrow F \\ x &\longmapsto x^q \end{aligned}$$

é um isomorfismo de corpos (conhecido como isomorfismo de Frobenius).

Demonstração. Temos que $f_q(ab) = (ab)^q = a^qb^q = f_q(a)f_q(b)$.
Pela proposição anterior temos $f_q(a + b) = (a + b)^q = a^q + b^q = f_q(a) + f_q(b)$ e como $f_q(1) = 1^q = 1$, segue que f_q é um homomorfismo.
Seja $a \in \ker f$, então $a^q = 0$, logo $a = 0$. Portanto, f é injetora.
Como F é finito, temos que f é sobrejetora. ■

Corolário 3.1.7 *Seja* F *um corpo com* $\mathrm{char}(F) = p$ *e seja* q *uma potência inteira de* p. *Então*

$$K = \{a \in F : a^q - a = 0\},$$

é um subcorpo de F.

Demonstração. Observe que $K \neq \emptyset$, pois $1, 0 \in K$.
Sejam $a, b \in K$, com $b \neq 0$. Como

$$(a - b)^q - (a - b) = a^q - b^q - a + b = (a^q - a) - (b^q - b) = 0 - 0 = 0,$$

temos que $a - b \in K$.
Como

$$\left(\frac{a}{b}\right)^q - \frac{a}{b} = \frac{a^q}{b^q} - \frac{a}{b} = \frac{a}{b} - \frac{a}{b} = 0,$$

temos que $\dfrac{a}{b} \in K$.
Portanto, K é um subcorpo de F. ■

Proposição 3.1.8 *Sejam* F *um corpo finito de característica* p *e* $f(x) \in F[x]$. *Temos que* $f'(x) = 0$ *se, e somente se, existe* $g(x) \in F[x]$ *tal que* $f(x) = g(x)^p$.

Demonstração. ($\Rightarrow$) Suponha que $f(x) = a_0 + a_1x + \cdots + a_nX^n$. Por hipótese, $f'(x) = 0$, ou seja,

$$a_1 + 2a_2x + 3a_3x^2 + \cdots + na_nX^{n-1} = 0.$$

Assim, $ia_i = 0$, para todo $i = 1, \ldots, n$. Então, $p \mid i$ sempre que $a_i \neq 0$. Logo,

$$f(x) = a_0 + a_pX^p + a_{2p}x^{2p} + \cdots .$$

Como $f_p : F \longrightarrow F$, dada por $x \mapsto x^p$, é um isomorfismo, podemos escolher $b_i \in F$ tal que $b_i^p = a_{ip}$.
Tome $g(x) = b_0 + b_1x + b_2x^2 + \cdots$. Assim,

$$g(x)^p = b_0^p + b_1^pX^p + b_2^pX^{2p} + \cdots = f(x).$$

($\Leftarrow$) Por hipótese, existe $g(x) \in F[x]$ tal que $f(x) = g(x)^p$.
Digamos que

$$g(x) = b_0 + b_1x + \cdots + b_nx^n.$$

Então,

$$g(x)^p = b_0^p + b_1^pX^p + \cdots + b_n^px^{np}.$$

Logo,

$$f'(x) = (g(x)^p)' = pb_1^pX^{p-1} + 2pb_2^pX^{2p-1} + \cdots + npb_n^pX^{np-1} = 0.$$

■

Proposição 3.1.9 *Seja* F *um corpo finito de característica* p *e seja* $q = p^r$ *para algum* $r \in \mathbb{N}$. *O polinômio* $f(x) = x^q - x$ *não possui fatores irredutíveis múltiplos em* $F[x]$.

Demonstração. Como $f'(x) = qX^{q-1}-1 = -1$ é invertível em $F[x]$, temos que $\text{mdc}(f(x), f'(x)) = 1$.
Suponha, por absurdo, que $f(x)$ possui um fator irredutível múltiplo em $F[x]$, ou seja, existe $g(x)$ irredutível em $F[x]$ tal que $f(x) = g(x)^sh(x)$, para algum $h(x) \in F[x]$ e $s \geq 2$.
Assim,

$$f'(x) = sg(x)^{s-1}g'(x)h(x) + g(x)^sh'(x).$$

Como $s - 1 \geq 1$, temos que $g(x)$ divide $f'(x)$. Logo, $g(x)$ divide $\text{mdc}(f(x), f'(x)) = 1$, ou seja, $g(x)$ é invertível, absurdo! ■

Lema 3.1.10 *Seja* F *um corpo finito com* q *elementos. Para todo* $a \in F^* = F \setminus \{0\}$ *temos que* $a^{q-1} = 1$.

Demonstração. Seja $a \in F^*$ e considere a aplicação

$$\begin{aligned} \varphi_a : F^* &\longrightarrow F^* \\ x &\longmapsto ax \end{aligned}$$

Sejam $x, y \in F^*$ tais que $\varphi_a(x) = \varphi_a(y)$, assim $ax = ay$. Como $a \in F^*$, temos que $x = y$. Logo, φ_a é injetora.
Como F^* é finito, temos que φ_a é bijetora.
Se $F^* = \{x_1, \ldots, x_{q-1}\}$, então $\{ax_1, \ldots, ax_{q-1}\} = \{x_1, \ldots, x_{q-1}\}$.
Assim, $(ax_1)(ax_2)\cdots(ax_{q-1}) = x_1x_2\cdots x_{q-1}$, ou seja, $a^{q-1}x = x$, onde $x = x_1x_2\cdots x_{q-1}$ é invertível em F. Portanto, $a^{q-1} = 1$. ■

Corolário 3.1.11 *Seja* F *um corpo finito com* q *elementos. Para todo* $a \in F$ *e para todo* $n \in \mathbb{N}$, *temos que* $a^{q^n} = a$.

Demonstração. Faremos uma indução sobre n.
Para $n = 1$, se $a \neq 0$ temos $a^{q-1} = 1$, e portanto $a^q = a$. Para $a = 0$, é claro que $a^q = a$.
Seja $n > 1$ e suponha que $a^{q^{n-1}} = a$. Assim,

$$a^{q^n} = (a^{q^{n-1}})^q \overset{h.i}{=} a^q = a.$$

Portanto, $a^{q^n} = a$, para todo $n \in \mathbb{N}$. ■

Corolário 3.1.12 *Seja* K *um corpo finito de característica* p *com* q *elementos. Seja* F *uma extensão de* K. *Então os elementos de* K *são os elementos de* F *que são raízes do polinômio* $x^q - x$, *enquanto que os elementos do subcorpo* $\mathbb{Z}_p$ *de* F *são as raízes do polinômio* $x^p - x$.

Demonstração. Como K tem q elementos, $a^q - a = 0$, para todo $a \in K$. Logo, todos os q elementos de K são raízes de $x^q - x$.
Como $x^q - x$ tem no máximo q raízes, segue que todas as raízes de $x^q - x$ são elementos de K.
Como $\mathbb{Z}_p$ tem p elementos, o argumento acima prova que os elementos de $\mathbb{Z}_p$ são as raízes de $x^p - x$. ■

Seja F um corpo finito e seja $a \in F^*$. Como $a^{q-1} = 1$, onde $|F| = q$, temos que

$$\{n \in \mathbb{N} : a^n = 1\} \neq \emptyset.$$

3.2 Existência e Unicidade de Corpos Finitos

Proposição 3.2.1 *Seja* K *um corpo finito com* q *elementos e seja* $f(x)$ *um polinômio mônico irredutível em* $K[x]$ *de grau* d. *Considere o corpo* $F = \dfrac{K[x]}{(f(x))}$. *Então:*

(i) $1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{d-1}$ *formam uma base para* F *como um* K*-espaço vetorial, onde* $\overline{x}$ *é a classe de* x.

(ii) $\overline{x}^{q^d} = \overline{x}$ *em* F

(iii) $f(x)$ *divide* $x^{q^d} - x$ *em* $K[x]$

(iv) *Os elementos* $\overline{x}, \overline{x}^q, \ldots, \overline{x}^{q^{d-1}}$ *de* F *são distintos e são as raízes de* $f(x)$.

Demonstração.

(i) Suponha que $a_0 + a_1\overline{x} + a_2\overline{x}^2 + \cdots + a_{d-1}\overline{x}^{d-1} = 0$. Então,

$$a_0 + a_1x + a_2x^2 + \cdots + a_{d-1}x^{d-1} \in (f(x)).$$

Como $d - 1 < \deg(f(x))$, segue que $a_0 + a_1x + a_2x^2 + \cdots + a_{d-1}x^{d-1} = 0$. Portanto, $a_i = 0$, para todo $i = 0, \ldots, d-1$.
Isso prova que $1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{d-1}$ é l.i.
Seja $\overline{g(x)} \in F$. Dividindo $g(x)$ por $f(x)$, obtemos que $q(x)$ e $r(x)$ em $K[x]$ tais que $g(x) = q(x)f(x) + r(x)$, onde $r(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{d-1}x^{d-1}$.
Como $\overline{g(x)} = \overline{r(x)} = a_0 + a_1\overline{x} + a_2\overline{x}^2 + \cdots + a_{d-1}\overline{x}^{d-1}$, temos que $1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{d-1}$ geram F.

(ii) Observe que F é um corpo finito com q^d elementos. Sabemos que $\overline{x}^{q^d} = \overline{x}$.

(iii) Como $\overline{x}^{q^d} = \overline{x}$, temos que $\overline{x^{q^d} - x} = \overline{0}$, logo $x^{q^d} - x \in (f(x))$.

(iv) Considere o polinômio

$$g(y) = (y - \overline{x})(y - \overline{x}^q) \cdots (y - \overline{x}^{q^{d-1}}) \in F[y].$$

Temos que

$$\begin{aligned} g(y^q) &= (y^q - \overline{x})(y^q - \overline{x}^q) \cdots (y^q - \overline{x}^{q^{d-1}}) \\ &= (y^q - \overline{x}^{q^d})(y^q - \overline{x}^q) \cdots (y^q - \overline{x}^{q^{d-1}}) \\ &= ((y - \overline{x}^{q^{d-1}})(y - \overline{x}) \cdots (y - \overline{x}^{q^{d-2}}))^q = g(y)^q. \end{aligned}$$

Assim, $g(y^q) = g(y)^q$. Se $g(y) = b_0 + b_1y + \cdots + b_{d-1}y^{d-1} + y^d$, temos que

$$b_0 + b_1y^q + \cdots + b_{d-1}y^{(d-1)q} + y^{dq} = g(y^q) = g(y)^q = b_0^q + b_1^qY^q + \cdots + b_{d-1}^qY^{(d-1)q} + y^{dq},$$

então $b_i = b_i^q$, para todo $i = 0, \ldots, d-1$.
Como b_i é raiz de $x^q - x$, para todo $i = 0, \ldots, d-1$, temos que $b_i \in K$, para todo $i = 0, \ldots, d-1$. Logo, $g(y) \in K[y]$.
Como $f(y), g(y) \in K[y]$ possuem uma raiz comum numa extensão F de K (tal raiz é $\overline{x} \in F$), segue que o $\mathrm{mdc}(f(y), g(y))$ é não constante em $F[y]$ e pertence a $K[y]$.
Como $f(y)$ é irredutível e mônico, temos que $f(y) = \mathrm{mdc}(f(y), g(y))$. Logo, $f(y)$ divide $g(y)$. Como $f(y)$ e $g(y)$ são mônicos e de mesmo grau, temos que $f(y) = g(y)$.
Por (iii) sabemos que $g(y)$ divide $y^{q^d} - y$. Como $y^{q^d} - y$ não possui fatores irredutíveis múltiplos em $F[y]$, segue que $g(y)$ não possui fatores irredutíveis múltiplos em $F[y]$.
Logo, as raízes $\overline{x}, \overline{x}^q, \ldots, \overline{x}^{q^{d-1}}$ de $g(y)$ são duas a duas distintas.

■

Seguindo a notação da proposição anterior, temos que se $\overline{x} \in K[x]/(f(x))$ com $f(x) \in K[x]$ irredutível de grau d, então

$$d = \min\{j \in \mathbb{N} : \overline{x}^{q^j} = \overline{x}\}.$$

Lema 3.2.2 *Sejam $q \geq 2, m$ e n inteiros positivos. Então*

$$\mathrm{mdc}(x^{q^n} - x, x^{q^m} - x) = x^{q^e} - x,$$

onde $e = \mathrm{mdc}(n, m)$.

Demonstração. Dados m e n inteiros positivos, vamos primeiramente provar que

$$\mathrm{mdc}(x^n - 1, x^m - 1) = x^{\mathrm{mdc}(n,m)} - 1.$$

É claro que isto é verdade quando $n = m$.
Suponhamos que $n > m$. Pelo algoritmo da divisão em $\mathbb{Z}$, temos que $n = mq + r$, com $0 \leq r < m$. Observe que

$$x^n - 1 = (x^m - 1)(x^{n-m} + x^{n-2m} + \cdots + x^{n-qm}) + x^r - 1 \tag{3.1}$$

Considere agora o algoritmo de Euclides para o cálculo do mdc de n e m:

$$\begin{aligned} n &= mq_1 + r_1 \\ m &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{s-1} &= r_sq_{s+1} + r_{s+1} \end{aligned}$$

onde $r_{s+1} = 0$. Logo, $\mathrm{mdc}(n, m) = r_s$.
Usando as igualdades acima e por (3.1), temos que

$$\begin{aligned} x^n - 1 &= (x^m - 1)Q_1(x) + x^{r_1} - 1 \\ x^m - 1 &= (x^{r_1} - 1)Q_2(x) + x^{r_2} - 1 \\ x^{r_1} - 1 &= (x^{r_2} - 1)Q_3(x) + x^{r_3} - 1 \\ &\vdots \\ x^{r_{s-1}} - 1 &= (x^{r_s} - 1)Q_{s+1}(x) + x^{r_{s+1}} - 1 \end{aligned}$$

onde $x^{r_{s+1}} - 1 = x^0 - 1 = 0$.
Portanto,

$$\mathrm{mdc}(x^n - 1, x^m - 1) = x^{r_s} - 1 = x^{\mathrm{mdc}(n,m)} - 1.$$

Seja $a \geq 2$ um inteiro. Então, temos que

$$\mathrm{mdc}(a^n - 1, a^m - 1) = a^{\mathrm{mdc}(n,m)} - 1.$$

Finalmente,

$$\begin{aligned} \mathrm{mdc}(x^{q^n} - x, x^{q^m} - x) &= x\mathrm{mdc}(x^{q^{n-1}} - 1, x^{q^{m-1}} - 1) \\ &= x(x^{\mathrm{mdc}(q^n-1, q^m-1)} - 1) \\ &= x(x^{q^e-1} - 1) \\ &= x^{q^e} - x, \end{aligned}$$

onde $e = \mathrm{mdc}(n, m)$. ■

Proposição 3.2.3 *Seja* F *um corpo finito com* q *elementos e seja* n *um inteiro positivo. Em* $F[x]$ *temos a igualdade:*

$$x^{q^n} - x = \prod_{d|n} G_d(x),$$

onde $G_d(x)$ *é o produto de todos os polinômios mônicos irredutíveis de grau* d *em* $F[x]$.

Demonstração. Seja $f \in F[x]$ um polinômio mônico irredutível de grau d. Como $x^{q^n} - x$ não possui fatores irredutíveis múltiplos, basta provar a seguinte afirmação:

$$f \text{ divide } x^{q^n} - x \iff d \text{ divide } n.$$

($\Rightarrow$) Como F tem q elementos e $\deg(f) = d$ temos que $f \mid x^{q^d} - x$.
Como f divide $x^{q^n} - x$ e $x^{q^d} - x$ temos que f divide $\mathrm{mdc}(x^{q^n} - x, x^{q^d} - x)$. Pelo Lema 3.2.2 temos que

$$\mathrm{mdc}(x^{q^n} - x, x^{q^d} - x) = x^{q^e} - x,$$

onde $e = \mathrm{mdc}(n, d)$. Logo, f divide $x^{q^e} - x$.
Em $\dfrac{F[x]}{(f)}$ temos que $\overline{x^{q^e} - x} = \overline{0}$, logo $\overline{x}^{q^e} = \overline{x}$. Como

$$d = \min\{j \in \mathbb{N} : \overline{x}^{q^j} = \overline{x}\},$$

segue que $d \leq e$. Como $e = \mathrm{mdc}(n, d)$, temos que $e \leq d$. Logo, $d = e = \mathrm{mdc}(n, d)$. Portanto, $d \mid n$.

($\Leftarrow$) Do Lema 3.2.2 e de $d \mid n$ vem que

$$\mathrm{mdc}(x^{q^d} - x, x^{q^n} - x) = x^{q^{\mathrm{mdc}(d,n)}} - 1 = x^{q^d} - x.$$

Logo, $x^{q^d} - x \mid x^{q^n} - x$.
Como F tem q elementos e $\deg(f) = d$, segue que $f \mid x^{q^d} - x$. Portanto, $f \mid x^{q^n} - x$. ■

Corolário 3.2.4 *Seja* $I(n)$ *o número de polinômios mônicos irredutíveis de grau* n *em* $K[x]$, *onde* K *é um corpo finito com* q *elementos. Então,*

$$q^n = \sum_{d|n} dI(d).$$

Demonstração. Sabemos que $x^{q^n} - x = \prod_{d|n} G_d(x)$.

Como $\deg G_d(x) = dI(d)$, temos que $\deg\left(\prod_{d|n} G_d(x)\right) = \sum_{d|n} dI(d)$.

Logo, $q^n = \deg(x^{q^n} - x) = \deg\left(\prod_{d|n} G_d(x)\right) = \sum_{d|n} dI(d)$. ■

Exemplo 3.2.5 *Vamos calcular* $I(n)$ *para alguns valores de* n *em* $\mathbb{Z}_2[x]$.
Como os únicos polinômios mônicos irredutíveis de $\mathbb{Z}_2[x]$ *de grau* 1 *são* x *e* $x+1$*, temos que* $I(1) = 2$.
Usando a fórmula do corolário, temos que

$$2^2 = I(1) + 2I(2) = 2 + 2I(2) \Longrightarrow I(2) = 1.$$

O único polinômio mônico irredutível de grau 2 *em* $\mathbb{Z}_2[x]$ *é* $x^2 + x + 1$.
Novamente pelo corolário anterior, temos que

$$2^3 = I(1) + 3I(3) = 2 + 3I(3) \Longrightarrow I(3) = 2.$$

Os únicos polinômios mônicos irredutíveis de grau 3 *em* $\mathbb{Z}_2[x]$ *são* $x^3 + x + 1$ *e* $x^3 + x^2 + 1$.
Do mesmo modo, podemos obter $I(4) = 3, I(5) = 6$*, etc.*

Teorema 3.2.6 *Seja* F *um corpo finito. Para cada inteiro positivo* n*, existe pelo menos um polinômio irredutível de grau* n *em* $F[x]$.

Demonstração. Para $n = 1$, basta considerar o polinômio x.
Suponha $n \geq 2$. Sejam $1 = d_1 < \cdots < d_s < n$ os divisores de n. Digamos que $q = |F|$. Pelo corolário acima, temos que

$$\begin{aligned}
q^n &= \sum_{d|n} dI(d) \\
&= d_1 I(d_1) + \cdots + d_s I(d_s) + nI(n) \\
&\leq \sum_{d|d_1} dI(d) + \cdots + \sum_{d|d_s} dI(d) + nI(n) \\
&= q^{d_1} + \cdots + q^{d_s} + nI(n) \\
&\leq q + q^2 + \cdots + q^{d_s} + nI(n) \\
&= \frac{q^{d_s+1} - 1}{q - 1} + nI(n) \\
&< q^{d_s+1} + nI(n).
\end{aligned}$$

Portanto, $nI(n) > q^n - q^{d_s+1}$.
Como $d_s \mid n$ e $d_s < n$, temos que $n = \lambda d_s$, para algum $\lambda \geq 2$. Assim,

$$d_s = \frac{n}{\lambda} \leq \frac{n}{2} \text{ e } q^{d_s+1} \leq q^{\frac{n}{2}+1}.$$

Logo,

$$nI(n) > q^n - q^{d_s+1} \geq q^n - q^{\frac{n}{2}+1} = q^n(1 - q^{-\frac{n}{2}+1}). \tag{3.2}$$

Observe que

$$n \geq 2 \Rightarrow \frac{n}{2} \geq 1 \Rightarrow 0 \geq 1 - \frac{n}{2} \Rightarrow 1 = q^0 \geq q^{1-\frac{n}{2}} \Rightarrow 1 - q^{1-\frac{n}{2}} \geq 0.$$

Caso $n \geq 2$, temos que $nI(n) > 0$. Portanto, $I(n) > 0$. ■

Teorema 3.2.7 *(Existência de Corpos Finitos) Se p e n são inteiros positivos com p primo, então existe um corpo com p^n elementos.*

Demonstração. Sabemos que existe $f(x) \in \mathbb{Z}_p[x]$ tal que $f(x)$ é irredutível de grau n. Logo, $\mathbb{Z}_p[x]/f(x)$ é um corpo com p^n elementos. ■

Teorema 3.2.8 *(Unicidade dos Corpos Finitos) Dois corpos finitos com o mesmo número de elementos são isomorfos.*

Demonstração. Seja L um corpo finito com p^n elementos, logo a característica de L é p e ele contém um corpo isomorfo a $\mathbb{Z}_p$. Assim, L é um $\mathbb{Z}_p$-espaço vetorial de dimensão n.
Como L tem p^n elementos, todas as raízes de $x^{p^n} - x$ são exatamente todos os elementos de L.
Seja $f \in \mathbb{Z}_p[x]$ um polinômio mônico irredutível de grau n. Sabemos que f divide $x^{p^n} - x$ em $\mathbb{Z}_p[x]$. Logo, existe $u \in L$ tal que $f(u) = 0$.

Afirmação: $B = \{1, u, \ldots, u^{n-1}\}$ é uma base para L.

Como $\dim L = n$, basta provar que B é l.i.
Suponha, por absurdo, que existam $a_0, \ldots, a_{n-1} \in \mathbb{Z}_p$, não todos nulos, tais que

$$a_0 + a_1 u + \cdots + a_{n-1} u^{n-1} = 0.$$

Então, $r(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathbb{Z}_p[x]$ é um polinômio não nulo de grau $< n$ tal que $r(u) = 0$. Assim, $\text{mdc}(f, r) \neq 1$ em L, e como $f, r \in \mathbb{Z}_p[x]$ temos que $\text{mdc}(f, r) \neq 1$ em $\mathbb{Z}_p$.
Como f é irredutível, temos que $f \mid r$, o que é impossível, pois $\deg(r) < \deg(f)$.
Portanto, B é uma base para L como um $\mathbb{Z}_p$-espaço vetorial.

Seja $F = \dfrac{\mathbb{Z}_p[x]}{(f)}$. Sabemos que F é um $\mathbb{Z}_p$-espaço vetorial e uma base para F é $B' = \left\{1, \overline{x}, \ldots, \overline{x}^{n-1}\right\}$.
Considere a aplicação

$$\begin{array}{ccc} \varphi : F & \longrightarrow & L \\ \displaystyle\sum_{i=0}^{n-1} a_i \overline{x}^i & \longmapsto & \displaystyle\sum_{i=0}^{n-1} a_i u^i \end{array}$$

(i) φ está bem definida:

Suponha que $\displaystyle\sum_{i=0}^{n-1} a_i \overline{x}^i = \sum_{i=0}^{n-1} b_i \overline{x}^i$. Assim, $\displaystyle\sum_{i=0}^{n-1} a_i X^i - \sum_{i=0}^{n-1} b_i X^i \in (f)$, ou seja, existe $g \in \mathbb{Z}_p[x]$ tal que $\displaystyle\sum_{i=0}^{n-1} a_i X^i - \sum_{i=0}^{n-1} b_i X^i = fg$. Logo, $\displaystyle\sum_{i=0}^{n-1} a_i u^i - \sum_{i=0}^{n-1} b_i u^i = f(u)g(u) = 0$.
Portanto, $\displaystyle\sum_{i=0}^{n-1} a_i u^i = \sum_{i=0}^{n-1} b_i u^i$.

(ii) φ é um homomorfismo de corpos:

Sejam $\overline{g} = \displaystyle\sum_{i=0}^{n-1} a_i \overline{x}^i$ e $\overline{h} = \sum_{i=0}^{n-1} b_i \overline{x}^i$ em F. Então,

$$\varphi(\overline{g} + \overline{h}) = \sum_{i=0}^{n-1} (a_i + b_i) u^i = \sum_{i=0}^{n-1} a_i u^i + \sum_{i=0}^{n-1} b_i u^i = \varphi(\overline{g}) + \varphi(\overline{h}).$$

Dividindo gh por f obtemos $q, r \in \mathbb{Z}_p[x]$ tais que $gh = fq + r$, onde r é zero ou é um polinômio de grau $\leq n - 1$. Logo,

$$\overline{g}\,\overline{h} = \overline{f}\,\overline{g} + \overline{r} = \overline{r} \text{ e } g(u)h(u) = f(u)q(u) + r(u) = r(u).$$

Assim, $\varphi(\overline{g}\,\overline{h}) = \varphi(\overline{r}) = r(u) = g(u)h(u) = \varphi(\overline{g})\varphi(\overline{h})$.

(iii) φ é sobrejetora:

Seja $\sum_{i=0}^{n-1} a_i u^i$ um elemento de L. Defina $g = \sum_{i=0}^{n-1} a_i X^i$. Então $\overline{g} \in F$ e $\varphi(\overline{g}) = g(u) = \sum_{i=0}^{n-1} a_i u^i$, o que prova que φ é sobrejetora.

(iv) φ é injetora:

Como $\ker(\varphi)$ é um ideal de F e φ não é o homomorfismo nulo, segue que $\ker(\varphi) = \{0\}$.

■

Capítulo 4

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, cujo os elementos são n-uplas $a = (a_1, \ldots, a_n)$ com $a_i \in K, i = 1, \ldots, n$.

Definição 4.0.9 *Um subespaço vetorial $C \subset K^n$ é chamado código linear.*

Assim, todo código linear tem dimensão dimensão finita.
De maneira usual, denotaremos por $|A|$ o número de elementos de um conjunto A.

Definição 4.0.10

(i) *Dados $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_n)$ em 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 $a = (a_1, \ldots, a_n) \in K^n$ é definido como*

$$w(a) := |\{i : \ a_i \neq 0\}|.$$

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

Observação 4.0.11 *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 4.0.12 *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*

$$\delta = \min\{d(a,b) : a,b \in C \text{ e } a \neq b\} = \min\{w(a) = d(a,0) : a \in C, a \neq 0\}.$$

O comprimento, a dimensão e a distância mínima constituem os *parâmetros básicos* de um código linear. 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 4.0.13 *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* $d = n - k + 1$.

Capítulo 5

A distância mínima de códigos parametrizados no toro projetivo

A partir de agora vamos considerar:

- $K = \mathbb{F}_q$ um corpo finito com q elementos
- $m_1, \ldots, m_s$ monômios em $K[y_1, \ldots, y_n]$, onde

$$\begin{aligned} m_1 &= y^{v_1} = y_1^{v_{11}} \cdots y_n^{v_{1n}} \\ &\vdots \\ m_s &= y^{v_s} = y_1^{v_{s1}} \cdots y_n^{v_{sn}} \end{aligned}$$

- $S = K[t_1, \ldots, t_s]$
- $S_d = K[t_1, \ldots, t_s]_d = \{f \in K[t_1, \ldots, t_s] : f \text{ é homogêneo de grau } d \text{ ou } f = 0\}$
- $\mathbb{M}$ é o conjunto de todos os monômios de $K[t_1, \ldots, t_s]$.

Definição 5.0.14 *Seja* I *um ideal em* $K[t_1, \ldots, t_s]$. *Definimos a Pegada de* I *como sendo o conjunto*

$$\Delta(I) = \{m \in \mathbb{M} : m \notin \langle \mathrm{lm}(I) \rangle\}.$$

Também definimos

$$\Delta(I)_d = \Delta(I) \cap S_d.$$

Proposição 5.0.15 *Seja* I *um ideal em* $K[t_1, \ldots, t_s]$ *e sejam* $f_1, \ldots, f_t \in I$. *Então,*

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

(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 $m \in \Delta(I)$. Como $m \notin \langle \mathrm{lm}(I) \rangle$ e $\langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t) \rangle \subseteq \langle \mathrm{lm}(I) \rangle$ temos que $m \notin \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t) \rangle$. Portanto, $m \in \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$.

(ii) ($\Rightarrow$) Seja $f \in I$. Vamos mostrar que $\mathrm{lm}(f) \in \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t) \rangle$. Suponha por absurdo que $\mathrm{lm}(f) \notin \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t) \rangle$. Assim, $\mathrm{lm}(f) \in \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t)) = \Delta(I)$, ou seja, $\mathrm{lm}(f) \notin \langle \mathrm{lm}(I) \rangle$. Portanto, $\mathrm{lm}(f) \notin \mathrm{lm}(I)$, absurdo, pois $f \in I$.

($\Leftarrow$) Seja $m \in \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$. Temos que, $m \notin \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t) \rangle = \langle \mathrm{lm}(I) \rangle$. Portanto, $m \in \Delta(I)$.

■

Proposição 5.0.16 *Seja* I *um ideal homogêneo em* $K[t_1,\ldots,t_s]$. *Então,* $B=\{\overline{m} : m \in \Delta(I)_d\}$ *é uma base para* $K[t_1,\ldots,t_s]_d/I_d$ *como um* K*-espaço vetorial.*

Demonstração. Seja $f \in K[t_1,\ldots,t_s]_d$, isto é, f é homogêneo de grau d. Como I é um ideal homogêneo, existem $g_1,\ldots,g_n \in K[t_1,\ldots,t_s]$ homogêneos tais que $G=\{g_1,\ldots,g_n\}$ é uma base de Groebner para I. Dividindo f por $\{g_1,\ldots,g_n\}$ obtemos $f_1,\ldots,f_n, r \in K[t_1,\ldots,t_s]$ tais que $f=f_1g_1+\cdots+f_ng_n+r$ e r é uma K-combinação linear de monômios de $\Delta(I)_d$. Como $f-r \in I_d$, temos que $\overline{f}=\overline{r}$. Portanto, $\overline{f}$ é uma K-combinação linear de elementos de B.

Para provar que B é linearmente independente, sejam $\overline{m_1},\ldots,\overline{m_l} \in B$ e $c_1,\ldots,c_l \in K$ tais que $c_1\overline{m_1}+\cdots+c_l\overline{m_l}=\overline{0}$. Suponha por absurdo que algum $c_j \neq 0$. Como $r := c_1m_1+\cdots+c_lm_l \in I_d$ temos que $lm(r) \in lm(I_d) \subseteq lm(I)$. Logo, $lm(r) \in \langle lm(I)\rangle$, ou seja, $lm(r) \notin \Delta(I)$. Como $lm(r) = m_i$ para algum $i \in \{1,\ldots,l\}$ temos $m_i \notin \Delta(I)$, logo $m_i \notin \Delta(I)_d$. Portanto, B é linearmente independente. ■

5.1 O Código Parametrizado de ordem d

Definição 5.1.1 *O conjunto*

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

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

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

$$X=\{[p_1],\ldots,[p_m]\}, \text{ onde } m=|X|.$$

Dado $d \in \mathbb{N}$, seja $f_0(t_1,\ldots,t_s)=t_1^d$ e considere a aplicação

$$\begin{aligned} \phi_d : S_d &\longrightarrow K^m \\ f &\longmapsto \left(\frac{f(p_1)}{f_0(p_1)},\ldots,\frac{f(p_m)}{f_0(p_m)}\right). \end{aligned}$$

Vejamos que ϕ_d é uma transformação linear:
Para provar que ϕ_d está bem definida, sejam $f \in S_d$ e $[a]=[b] \in X$. Digamos que $a=(a_1,\ldots,a_s)$ e $b=(b_1,\ldots,b_s)$. Temos que $a=\lambda b$, para algum $\lambda \in K^*$. Vamos provar que

$$\frac{f(a)}{f_0(a)}=\frac{f(b)}{f_0(b)}.$$

Observe que $f_0(a)=f_0(\lambda b)=(\lambda b_1)^d=\lambda^d f_0(b)$.
Como f é homogêneo de grau d, temos que $f(a)=f(\lambda b)=\lambda^d f(b)$. Portanto,

$$\frac{f(a)}{f_0(a)}=\frac{\lambda^d f(b)}{\lambda^d f_0(b)}=\frac{f(b)}{f_0(b)}.$$

Vamos provar que ϕ_d é uma transformação linear. Sejam $f,g \in S_d$ e $\lambda \in K$. Temos que

$$\begin{aligned} \phi_d(f+\lambda g) &= \left(\frac{(f+\lambda g)(p_1)}{f_0(p_1)},\ldots,\frac{(f+\lambda g)(p_m)}{f_0(p_m)}\right)=\left(\frac{f(p_1)+\lambda g(p_1)}{f_0(p_1)},\ldots,\frac{f(p_m)+\lambda g(p_m)}{f_0(p_m)}\right) \\ &= \left(\frac{f(p_1)}{f_0(p_1)},\ldots,\frac{f(p_m)}{f_0(p_m)}\right)+\lambda\left(\frac{g(p_1)}{f_0(p_1)},\ldots,\frac{g(p_m)}{f_0(p_m)}\right)=\phi_d(f)+\lambda\phi_d(g). \end{aligned}$$

Definição 5.1.2 *A imagem da transformação linear* ϕ_d *é chamada de código parametrizado de ordem* d *e denotamos por*

$$\phi_d(S_d) = C_X(d).$$

Definição 5.1.3 *O ideal anulador de* X*, denotado por* $I(X)$*, é o ideal de* S *gerado pelos polinômios homogêneos de* S *que se anulam em* X*.*

Observe que $I(X)$ é um ideal homogêneo.

Considere $I(X)_d := I(X) \cap S_d$. Assim, $I(X)_d$ é um subgrupo normal de S_d. Logo, $S_d/I(X)_d$ é um grupo com as operações usuais de classes. Portanto, $S_d/I(X)_d$ é um $K-$espaço vetorial.

Observe que $\ker(\phi_d) = I(X)_d$:
Dado $f \in \ker(\phi_d)$ temos que $f \in S_d$ e $\phi_d(f) = 0$. Assim,

$$\left(\frac{f(p_1)}{f_0(p_1)}, \ldots, \frac{f(p_m)}{f_0(p_m)}\right) = (0, \ldots, 0), \text{ ou seja, } f(p_1) = \cdots = f(p_m) = 0.$$

Portanto, f é homogêneo de grau d e se anula em X. Isso mostra que $f \in I(X) \cap S_d = I(X)_d$. Para provar a outra inclusão, seja $g \in I(X)_d$, logo $g \in S_d$ e $g \in I(X)$. Assim,

$$g(p_1) = \cdots = g(p_m) = 0.$$

Logo, $\phi_d(g) = 0$.

Proposição 5.1.4 *A aplicação*

$$\begin{array}{rcl} T : S_d/I(X)_d & \longrightarrow & C_X(d) \\ \overline{f} & \longmapsto & \phi_d(f) \end{array}$$

é um isomorfismo de $K-$*espaços vetoriais.*

Demonstração. Vamos provar que T é um isomorfismo. De fato:

(i) T é uma transformação linear:
Sejam $\overline{f}, \overline{g} \in S_d/I(X)_d$ e $\lambda \in K$. Assim, temos que

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

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

(iii) $\mathrm{Im}T = C_X(d)$:
Seja $a \in C_X(d) = \mathrm{Im}(\phi_d)$, então existe $f \in S_d$ tal que $a = \phi_d(f)$, ou seja, $a = T(\overline{f}) \in \mathrm{Im}T$.

■

Dado um ideal homogêneo I em $K[t_1, \ldots, t_s]$ vamos denotar por $H_I : \mathbb{N} \longrightarrow \mathbb{N}$ a função de Hilbert de I. Assim, temos que

$$H_{I(X)}(d) = \dim_K (S_d/I(X)_d) = \dim_K C_X(d).$$

Observação 5.1.5 *Como* $B = \{\overline{m} : m \in \Delta(I(X))_d\}$ *é uma base para* $S_d/I(X)_d$ *como* K*-espaço vetorial, temos que*

$$\dim_K C_X(d) = \dim_K (S_d/I(X)_d) = |\Delta(I(X))_d|.$$

Teorema 5.1.6 $H_{I(X)}(d) = |X|$ *para todo* $d \geq |X| - 1$.

Demonstração. Seja $d \geq |X| - 1$. Vamos construir um polinômio $f_1 \in S_d$ tal que $\phi_d(f_1) = e_1 \in K^m$. Denotaremos os pontos de X por

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

tais que $p_{11} = \cdots = p_{m1} = 1$. Como $p_1 \neq p_2$, podemos escolher $k \in \{1, \ldots, s\}$ tal que $p_{1k} \neq p_{2k}$. Defina

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

Observe 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

$$h_i(p_j) = \begin{cases} 0, & \text{se } i = j \\ 1, & \text{se } j = 1. \end{cases}$$

Considere

$$f_1 := t_1^{d-m+1} h_2 \cdots h_m.$$

Observe que f_1 é um polinômio homogêneo de grau $(d-m+1)+(m-1) = d$, ou seja, $f_1 \in S_d$. Mais ainda, $f_1(p_1) = 1$ e $f_1(p_j) = 0$, para $2 \leq j \leq m$. Portanto, $\phi_d(f_1) = e_1 \in K^m$.

Analogamente, construímos $f_2, \ldots, f_m \in S_d$ tais que $\phi_d(f_j) = e_j$ para $1 \leq j \leq m$. Isso prova que ϕ_d é sobrejetora para todo $d \geq |X| - 1$. Portanto,

$$H_{I(X)}(d) = \dim S_d / I(X)_d = \dim \phi_d(S_d) = \dim K^m = m = |X|,$$

para todo $d \geq |X| - 1$. ∎

Dado um ideal homogêneo I em $K[t_1, \ldots, t_s]$ vamos denotar por $h_I(t) \in \mathbb{Q}[t]$ o polinômio de Hilbert de I. Observe que $\deg(h_{I(X)}(t)) = \dim X = 0$. Assim, temos que $h_{I(X)}(t)$ é o polinômio constante c_0.

Definição 5.1.7 *O índice de regularidade de um ideal* I*, denotado por* $\mathrm{reg}(I)$*, é o menor inteiro* $p \geq 0$ *tal que*

$$h_I(d) = H_I(d), \quad \textit{para } d \geq p.$$

Observe que $h_{I(X)}(t) = |X|$ e $H_{I(X)}(d) = |X|$ para todo $d \geq \mathrm{reg}(I(X))$. De fato, seja $d = \max\{\mathrm{reg}(I(X)), |X| - 1\}$. Assim, $c_0 = h_{I(X)}(d) = H_{I(X)}(d) = |X|$. Portanto, $c_0 = |X|$.

5.2 Os parâmetros do Código do Toro Projetivo

Considere

$$\mathbb{T} = \{[x_1, \ldots, x_s] \in \mathbb{P}^{s-1} : (x_1, \ldots, x_s) \in (K^*)^s\}$$

um toro projetivo em $\mathbb{P}^{s-1}$. Vamos ver que o ideal $I(\mathbb{T})$ é gerado pelos polinômios $f_2, \ldots, f_s$, onde $f_i = t_i^{q-1} - t_1^{q-1}$, com $2 \leq i \leq s$.

Proposição 5.2.1 $I(\mathbb{T}) = \langle f_2, \ldots, f_s \rangle$.

Demonstração. Vamos considerar a ordem lexicográfica com $t_1 < \cdots < t_s$. Como K é um corpo finito com q elementos, temos que $a^{q-1} = 1$ para todo $a \in K^*$. Logo, $f_i(x_1, \ldots, x_s) = 0$ para todo $[x_1, \ldots, x_s] \in \mathbb{T}$ e para todo $i \in \{2, \ldots, s\}$. Portanto, $\langle f_2, \ldots, f_s \rangle \subseteq I(\mathbb{T})$.

Para mostrar que $I(\mathbb{T}) \subseteq \langle f_2, \ldots, f_s \rangle$ faremos uma indução sobre s. Usaremos a notação

$$\mathbb{T}_s = \{[x_1, \ldots, x_s] \in \mathbb{P}^{s-1} : (x_1, \ldots, x_s) \in (K^*)^s\}.$$

Suponha $s = 2$ e seja $f \in I(\mathbb{T}_2)$. Dividindo f por $t_2^{q-1} - t_1^{q-1}$ obtemos

$$f = g(t_2^{q-1} - t_1^{q-1}) + r$$

para alguns $g, r \in K[t_1, t_2]$ com

$$r = \sum_{j=0}^{q-2} a_j t_1^{n-j} t_2^j,$$

onde $n = \deg(f)$ e $a_j \in K$ para todo j. Dado $x_2 \in K^*$, como f e $t_2^{q-1} - t_1^{q-1}$ se anulam em $(1, x_2)$, temos que $r(1, x_2) = 0$. Assim, $r(1, t_2) \in K[t_2]$ se anula em K^*. Portanto $t_2^{q-1} - 1$ divide $r(1, t_2)$ e $\deg(r(1, t_2)) \leq q - 2$. Isso mostra que $r(1, t_2) = 0$, ou seja,

$$\sum_{j=0}^{q-2} a_j t_2^j = 0.$$

Logo, $a_j = 0$ para todo j, o que prova que $r = 0$ e consequentemente que $f \in \langle f_2 \rangle$. Portanto, $I(\mathbb{T}_2) = \langle f_2 \rangle$.

Agora, suponha que $I(\mathbb{T}_{s-1}) = \langle f_2, \ldots, f_{s-1} \rangle$. Vamos provar que $I(\mathbb{T}_s) \subseteq \langle f_2, \ldots, f_s \rangle$. Seja $f \in I(\mathbb{T}_s)$. Dividindo f por $\{f_2, \ldots, f_s\}$ obtemos

$$f = g_2 f_2 + \cdots + g_s f_s + r,$$

onde $g_1, \ldots, g_s, r \in K[t_1, \ldots, t_s]$ e

$$r = \sum_{j=0}^{q-2} p_j(t_1, \ldots, t_{s-1}) t_2^j.$$

Como $f, f_2, \ldots, f_s \in I(\mathbb{T}_s)$, temos que $r \in I(\mathbb{T}_s)$. Dado $[x_1, \ldots, x_{s-1}] \in \mathbb{T}_{s-1}$ temos que $r(x_1, \ldots, x_{s-1}, t_s)$ é um polinômio em $K[t_s]$ que se anula em todo $x_s \in K^*$. Assim, $t_s^{q-1} - 1$ divide $r(x_1, \ldots, x_{s-1}, t_s)$ e $\deg(r(x_1, \ldots, x_{s-1}, t_s)) \leq q - 2$. Logo, $r(x_1, \ldots, x_{s-1}, t_s) = 0$, ou seja,

$$\sum_{j=0}^{q-2} p_j(x_1, \ldots, x_{s-1}) t_2^j = 0.$$

Portanto, $p_j(x_1, \ldots, x_{s-1}) = 0$ para todo j e para todo $[x_1, \ldots, x_{s-1}] \in \mathbb{T}_{s-1}$. Por hipótese de indução, para cada j temos

$$p_j(t_1, \ldots, t_{s-1}) \in I(\mathbb{T}_{s-1}) = \langle f_2, \ldots, f_{s-1} \rangle \subseteq \langle f_2, \ldots, f_s \rangle.$$

Observe que $p_j(t_1, \ldots, t_{s-1}) t_s^j \in \langle f_2, \ldots, f_s \rangle$, para todo j. Logo, $r \in \langle f_2, \ldots, f_s \rangle$. Isso prova que $f \in \langle f_2, \ldots, f_s \rangle$. Portanto, $I(\mathbb{T}_s) = \langle f_2, \ldots, f_s \rangle$. ■

A partir de agora vamos denotar $I = I(\mathbb{T})$.

Teorema 5.2.2 *O índice de regularidade de* I *é* $(s-1)(q-2)$.

Demonstração. Considere a aplicação injetora

$$\begin{array}{rccc} \psi_d: & \Delta(I)_d & \longrightarrow & \Delta(I)_{d+1} \\ & t_1^{\alpha_1}\cdots t_s^{\alpha_s} & \longmapsto & t_1^{\alpha_1+1}t_2^{\alpha_2}\cdots t_s^{\alpha_s} \end{array}$$

e observe que vale a seguinte afirmação:

$$\psi_d \text{ é sobrejetora} \iff d \geq (s-1)(q-2).$$

($\Longrightarrow$) Suponha que $d < (s-1)(q-2)$, ou seja, $d+1 \leq (s-1)(q-2)$. Dividindo $d+1$ por $q-2$ obtemos $d+1 = r(q-2)+l$ onde

$$(i)\ r = s-1 \text{ e } l = 0 \text{ ou } (ii)\ r < s-1 \text{ e } 0 \leq l < q-2.$$

Caso ocorra (i), defina $\beta_1 = 0$ e $\beta_i = q-2$, para $2 \leq i \leq s$. Como $\sum_{j=1}^{s} \beta_j = r(q-2) = d+1$ e $\beta_j \leq q-2$ para todo j, temos que $t_1^{\beta_1}\cdots t_s^{\beta_s} \in \Delta(I)_{d+1}$ mas $t_1^{\beta_1}\cdots t_s^{\beta_s} \notin \psi_d(\Delta(I)_d)$, pois $\beta_1 = 0$.

Caso ocorra (ii), defina

$$\beta_i = \begin{cases} 0, & \text{se } i = 1 \\ q-2, & \text{se } 2 \leq i \leq r+1 \\ l, & \text{se } i = r+2 \\ 0, & \text{se } r+3 \leq i \leq s \end{cases}.$$

Como $\sum_{j=1}^{s} \beta_j = r(q-2)+l = d+1$ e $\beta_j \leq q-2$ para todo j, temos que $t_1^{\beta_1}\cdots t_s^{\beta_s} \in \Delta(I)_{d+1}$ mas $t_1^{\beta_1}\cdots t_s^{\beta_s} \notin \psi_d(\Delta(I)_d)$, pois $\beta_1 = 0$. Portanto, ψ_d não é sobrejetora.

($\Longleftarrow$) Suponha que $d \geq (s-1)(q-2)$. Dado $t_1^{\beta_1}\cdots t_s^{\beta_s} \in \Delta(I)_{d+1}$ temos que $\sum_{j=1}^{s} \beta_j = d+1$ e $\beta_j \leq q-2$ para todo $j \in \{1,\ldots,s\}$. Temos que ter $\beta_1 \geq 1$, pois do contrário teríamos que $\beta_1 = 0$ e assim $\beta_1 + \cdots + \beta_s \leq (s-1)(q-2)$, ou seja, $d+1 \leq (s-1)(q-2) \leq d$, que é um absurdo. Logo

$$t_1^{\beta_1}\cdots t_s^{\beta_s} = \psi_d(t_1^{\beta_1-1}\cdots t_s^{\beta_s}) \in \psi_d(\Delta(I)_d).$$

Portanto, ψ_d é sobrejetora.

Agora, observe que

$$\begin{cases} |\Delta(I)_d| < |\Delta(I)_{d+1}|, & \text{se } d < (s-1)(q-2) \\ |\Delta(I)_d| = |\Delta(I)_{d+1}|, & \text{se } d \geq (s-1)(q-2) \end{cases}.$$

Ou seja,

$$\begin{cases} H_I(d) < H_I(d+1), & \text{se } d < (s-1)(q-2) \\ H_I(d) = H_I(d+1), & \text{se } d \geq (s-1)(q-2) \end{cases}.$$

Portanto, o índice de regularidade de I é $(s-1)(q-2)$. ■

Observe que $H_I(d) = |\mathbb{T}|$ para todo $d \geq (s-1)(q-2)$.

Proposição 5.2.3 *Se* $d \geq (s-1)(q-2)$*, então a distância mínima de* $C_{\mathbb{T}}(d)$ *é* $\delta_d = 1$.

Demonstração. Como $d \geq (s-1)(q-2)$, temos que $H_I(d) = |\mathbb{T}|$. Observe que

$$\dim C_{\mathbb{T}}(d) = H_I(d) = |\mathbb{T}| = \dim K^{|\mathbb{T}|}.$$

Logo, $C_{\mathbb{T}}(d) = K^{|\mathbb{T}|}$. Portanto, $\delta_d = 1$. ■

Teorema 5.2.4 *O comprimento de* $C_{\mathbb{T}}(d)$ *é* $(q-1)^{s-1}$ *e*

$$\dim_K C_{\mathbb{T}}(d) = \sum_{j=0}^{\lfloor \frac{d}{q-1} \rfloor} (-1)^j \binom{s-1}{j} \binom{s-1+d-j(q-1)}{s-1}.$$

Demonstração. Observe que $|\mathbb{T}| = (q-1)^{s-1}$, pois dado um ponto $[1, a_2, \ldots, a_s] \in \mathbb{T}$ temos $q-1$ possibilidades para cada entrada $a_2, \ldots, a_s$.

Para cada $j \in \{2, \ldots, s\}$ defina $M(j) = \{m \in \mathbb{M} : \mathrm{lm}(f_j) \mid m\}$. Assim, temos que

$$\Delta(I)_d = \mathbb{M}_d - \bigcup_{j=2}^{s} M(j)_d.$$

Portanto, temos que

$$|\Delta(I)_d| = |\mathbb{M}_d| - \left(\sum_{j=2}^{s} |M(j)_d| - \sum_{2 \leq j_1 < j_2 \leq s} |M(j_1)_d \cap M(j_2)_d| + \cdots + (-1)^s \Big| \bigcap_{j=2}^{s} M(j)_d \Big| \right) =$$

$$\binom{d+s-1}{d} - \left[\binom{s-1}{1} \binom{s-1+d-(q-1)}{s-1} - \binom{s-1}{2} \binom{s-1+d-2(q-1)}{s-1} + \right.$$

$$\left. \binom{s-1}{3} \binom{s-1+d-3(q-1)}{s-1} + \cdots + (-1)^s \binom{s-1}{s-1} \binom{s-1+d-(s-1)(q-1)}{s-1} \right] =$$

$$\binom{s-1}{0} \binom{s-1+d-0\cdot(q-1)}{s-1} - \binom{s-1}{1} \binom{s-1+d-1\cdot(q-1)}{s-1} +$$

$$\binom{s-1}{2} \binom{s-1+d-2(q-1)}{s-1} + \cdots + (-1)^{s-1} \binom{s-1}{s-1} \binom{s-1+d-(s-1)(q-1)}{s-1} =$$

$$\sum_{j=0}^{s-1} (-1)^j \binom{s-1}{j} \binom{s-1+d-j(q-1)}{s-1},$$

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

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

$$\frac{d}{q-1} - 1 < j \leq \frac{d}{q-1}.$$

Logo, $j = \left\lfloor \frac{d}{q-1} \right\rfloor$. Portanto,

$$\dim_K C_{\mathbb{T}}(d) = |\Delta(I)_d| = \sum_{j=0}^{\lfloor \frac{d}{q-1} \rfloor} (-1)^j \binom{s-1}{j} \binom{s-1+d-j(q-1)}{s-1}.$$

■

5.3 A Distância Mínima

Agora vamos encontrar a distância mínima do código $C_{\mathbb{T}}(d)$ quando $d < (s-1)(q-2)$.

Vamos considerar a ordem lexicográfica com $t_1 < \cdots < t_s$. Digamos que $\mathbb{T} = \{[p_1], \ldots, [p_m]\}$, onde a primeira entrada à esquerda de p_i é 1, para todo $i = 1, \ldots, m$. Observe que $\{f_2, \ldots, f_s\}$ é uma base de Groebner para I, pois $\mathrm{lm}(f_i)$ e $\mathrm{lm}(f_j)$ são primos entre si, pra todos $i \neq j$. A distância mínima de $C_{\mathbb{T}}(d)$ é dada por

$$\delta_d = \min\{w(\phi_d(f)) : f \in S_d \text{ e } f \notin I_d\}.$$

onde $w(a_1, \ldots, a_m) = |\{i : a_i \neq 0\}|$.

Definição 5.3.1 *Seja* J *um ideal em* $K[t_1, \ldots, t_s]$ *e seja* $f \in K[t_1, \ldots, t_s]$. *Definimos o seguinte conjunto*

$$\nabla(J, f) = \{m \in \Delta(J) : \mathrm{lm}(f) \mid m\}.$$

Vamos considerar $\nabla(J, f)_e = \nabla(J, f) \cap S_e$.

Teorema 5.3.2 *Seja* $d < (s-1)(q-2)$ *e seja* $e \geq |\mathbb{T}| - 1$. *Então,*

$$\min\{|\nabla(I, m)_e| : m \in \Delta(I)_d\} \leq \delta_d \leq w(\phi_d(f)),$$

para todo $f \in S_d \backslash I_d$.

Demonstração. Dado $f \in S_d \backslash I_d$, é claro que $\delta_d \leq w(\phi_d(f))$. Para provar a outra desigualdade, considere

$$\mathbb{T}_f = \{[p] \in \mathbb{T} : f(p) = 0\}.$$

Observe que

$$w(\phi_d(f)) = |\{[p] \in \mathbb{T} : f(p) \neq 0\}| = |\mathbb{T}| - |\mathbb{T}_f|. \tag{5.1}$$

Como $I(\mathbb{T}_f) \supseteq I + \langle f \rangle$, temos

$$\begin{array}{ccc} S_e & \twoheadrightarrow & S_e/I(\mathbb{T}_f)_e \\ \downarrow & \nearrow & \\ S_e/(I + \langle f \rangle)_e & & \end{array}$$

Logo,

$$\dim S_e/(I + \langle f \rangle)_e \geq \dim S_e/I(\mathbb{T}_f)_e. \tag{5.2}$$

Dividindo f por $\{f_2, \ldots, f_s\}$ obtemos um resto não nulo que continuaremos a denotar por f. Como $I + \langle f \rangle = \langle f_2, \ldots, f_s, f \rangle$, temos que

$$\langle \mathrm{lm}(I + \langle f \rangle) \rangle \supseteq \langle \mathrm{lm}(f_2), \ldots, \mathrm{lm}(f_s), \mathrm{lm}(f) \rangle.$$

Logo,

$$\Delta(I + \langle f \rangle) \subseteq \Delta(\mathrm{lm}(f_2), \ldots, \mathrm{lm}(f_s), \mathrm{lm}(f)). \tag{5.3}$$

Por 5.2 temos que

$$\dim S_e/I(\mathbb{T}_f)_e \leq \dim S_e/(I + \langle f \rangle)_e = |\Delta(I + \langle f \rangle)_e| \overset{5.3}{\leq} |\Delta(\mathrm{lm}(f_2), \ldots, \mathrm{lm}(f_s), \mathrm{lm}(f))_e|.$$

Como

$$\begin{cases} \nabla(I,f) \cap \Delta(\mathrm{lm}(f_2),\ldots,\mathrm{lm}(f_s),\mathrm{lm}(f)) = \emptyset \\ \nabla(I,f) \cup \Delta(\mathrm{lm}(f_2),\ldots,\mathrm{lm}(f_s),\mathrm{lm}(f)) = \Delta(I) \end{cases}$$

temos que

$$|\Delta(\mathrm{lm}(f_2),\ldots,\mathrm{lm}(f_s),\mathrm{lm}(f))_e| = |\Delta(I)_e| - |\nabla(I,f)_e|,$$

logo

$$|\Delta(I(\mathbb{T}_f))_e| = \dim S_e/I(\mathbb{T}_f)_e \leq |\Delta(I)_e| - |\nabla(I,f)_e|. \tag{5.4}$$

Como $e \geq |\mathbb{T}| - 1 \geq |\mathbb{T}_f| - 1$ temos que $|\mathbb{T}| = |\Delta(I)_e|$ e $|\mathbb{T}_f| = |\Delta(I(\mathbb{T}_f))_e|$. Assim,

$$w(\phi_d(f)) \overset{5.1}{=} |\mathbb{T}| - |\mathbb{T}_f| = |\Delta(I)_e| - |\Delta(I(\mathbb{T}_f))_e| \overset{5.4}{\geq} |\Delta(I)_e| - (|\Delta(I)_e| - |\nabla(I,f)_e|) = |\nabla(I,f)_e|.$$

Portanto,

$$\delta_d = \min\{w(\phi_d(f)) : f \in S_d \text{ e } f \notin I_d\} \geq \min\{|\nabla(I,f)_e| : f \in \Delta(I)_d\} = \min\{|\nabla(I,m)_e| : m \in \Delta(I)_d\}.$$

■

Agora, vamos trabalhar no sentido de encontrar o $\min\{|\nabla(I,m)_e| : m \in \Delta(I)_d\}$.
Seja $d < (s-1)(q-2)$. Considere o conjunto

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

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

Lema 5.3.3 *Temos que* $\mu_d = \min\{m(\alpha) : \alpha \in N_d \text{ e } s(\alpha) = d\}$.

Demonstração. 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 $s(\alpha) < d < (s-1)(q-2)$. Observe que existe $i \in \{1,\ldots,s-1\}$ tal que $\alpha_i < q-2$, pois do contrário, $\alpha_i = q-2$, para todo i, logo, $s(\alpha) = (s-1)(q-2)$, que é um absurdo. Considere $\widetilde{\alpha} = (\widetilde{\alpha}_1,\ldots,\widetilde{\alpha}_{s-1})$ 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, $s(\widetilde{\alpha}) = s(\alpha)+1 \leq d$. Portanto, $\widetilde{\alpha} \in N_d$. 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,

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

■

Proposição 5.3.4 *Sejam* k *e* ℓ *os únicos inteiros não negativos tais que* $1 \leq \ell \leq q-2$ *e* $d = k(q-2)+\ell$. *Então,*

$$\mu_d = (q-1-\ell)(q-1)^{s-k-2}.$$

Demonstração. Observe que $k < s-1$, pois do contrário teríamos $d > (s-1)(q-2)$. Veja que $d = k(q-2)+\ell < k(q-2) < (s-1)(q-2)$. Seja $\alpha \in N_d$ com $s(\alpha) = d$. Como $s(\alpha) < (s-1)(q-2)$, existe $i \in \{1,\ldots,s-1\}$ 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 $\beta = (\beta_1,\ldots,\beta_{s-1}) \in \mathbb{N}^{s-1}$ 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,

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

(I.2) Suponha que $\alpha_j + \alpha_{j'} > q-2$. Considere $\beta = (\beta_1,\ldots,\beta_{s-1}) \in \mathbb{N}^{s-1}$ 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 $\alpha_{k+2} = \cdots = \alpha_{s-1} = 0$. Tomamos $\beta = \alpha$, que teremos $m(\alpha) = m(\beta)$. Seja $\gamma = (\gamma_1, \ldots, \gamma_{s-1}) \in \mathbb{N}^{s-1}$ tal que

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

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,

$$\mu_d = m(\gamma) = (q-1-\ell)(q-1)^{s-k-2}.$$

■

Teorema 5.3.5 *Seja* $d < (s-1)(q-2)$ *e seja* $e \geq |\mathbb{T}| - 1$. *Então,*

$$\min\{|\nabla(I, m)_e| : m \in \Delta(I)_d\} = (q-1-l)(q-1)^{s-k-2},$$

onde k *e* l *são os únicos inteiros não negativos tais que* $1 \leq l \leq q-2$ *e* $d = k(q-2)+l$.

Demonstração. Observe que $\Delta(I)_d = \{t_1^{\alpha_1} \cdots t_s^{\alpha_s} : \alpha_1 + \cdots + \alpha_s = d \text{ e } \alpha_j \leq q-2, \forall j \geq 2\}$. Seja $m = t_1^{\alpha_1} \cdots t_s^{\alpha_s} \in \Delta(I)_d$. Temos que

$$\nabla(I, m)_e = \{N \in \Delta(I)_e : m \mid N\}.$$

Seja $N = t_1^{\beta_1} \cdots t_s^{\beta_s} \in \nabla(I, m)_e$. Assim, $\beta_1 + \cdots + \beta_s = e$ e $\beta_j \leq q-2$, para todo $j \geq 2$. Como $m \mid N$ temos que $\alpha_j \leq \beta_j$, para todo $j \geq 1$. Logo, $\alpha_j \leq \beta_j \leq q-2$, para todo $j \geq 2$, e $\alpha_1 \leq \beta_1 = e - (\beta_2 + \cdots + \beta_s) \geq e - (q-2)(s-1)$.
Podemos escolher $e \geq (s-1)(q-2) + \alpha_1$. Assim, β_1 sempre existe para toda escolha de $\beta_2, \ldots, \beta_s$, portanto,

$$|\nabla(I, m)_e| = \prod_{j=2}^{s} (q-1-\alpha_j).$$

Pela Proposição 5.3.4, temos que

$$\min\{|\nabla(I, m)_e| : m \in \Delta(I)_d\} = (q-1-l)(q-1)^{s-k-2}.$$

■

Teorema 5.3.6 *Se* k *e* l *os únicos inteiros não negativos tais que* $1 \leq l \leq q-2$ *e* $d = k(q-2)+l$*, então existe* $f \in S_d \backslash I_d$ *tal que*

$$w(\phi_d(f)) = (q-1-l)(q-1)^{s-k-2}.$$

Demonstração. Digamos que $K^* = \{a_1, \ldots, a_{q-1}\}$. Para cada $j \in \{2, \ldots, k+1\}$ defina

$$h_j = (t_j - a_1) \cdots (t_j - a_{q-2}).$$

Observe que cada h_j tem grau $q-2$ e se anula em $\{a_1, \ldots, a_{q-2}\}$. Agora, considere

$$g = \left(\prod_{j=2}^{k+1} h_j \right) (t_{k+2} - a_1)(t_{k+2} - a_2) \cdots (t_{k+2} - a_l).$$

Seja f a homogeneização de g com respeito a t_1. Assim, temos que

$$\deg(f) = \deg(g) = k(q-2)+l = d.$$

Seja $p = [1, b_2, \ldots, b_s] \in \mathbb{T}$ tal que $f(p) \neq 0$, ou seja, $g(p) \neq 0$. Veja que

$$\begin{cases} b_2, \ldots, b_{k+1} \in \{a_{q-1}\} \\ b_{k+2} \in \{a_{l+1}, \ldots, a_{q-1}\} \\ b_{k+3}, \ldots, b_s \in \{a_1, \ldots, a_{q-1}\}. \end{cases}$$

Portanto, temos $(q-1-l)(q-1)^{s-k-2}$ possibilidades para a escolha de p. Isso mostra que $w(\phi_d(f)) = (q-1-l)(q-1)^{s-k-2}$. ∎

Mostramos assim que,

$$(q-1-l)(q-1)^{s-k-2} \leq \delta_d \leq (q-1-l)(q-1)^{s-k-2}.$$

Teorema 5.3.7 *Se* $d < (s-1)(q-2)$*, então a distância mínima do código* $C_{\mathbb{T}}(d)$ *é*

$$\delta_d = (q-1-l)(q-1)^{s-k-2},$$

onde k *e* l *são os únicos inteiros não negativos tais que* $1 \leq l \leq q-2$ *e* $d = k(q-2)+l$*.*

Proposição 5.3.8 *Se* $\mathbb{T}$ *é um toro projetivo em* $\mathbb{P}^1$*, então* $C_{\mathbb{T}}(d)$ *é um código MDS e sua distância mínima é dada por*

$$\delta_d = \begin{cases} q-1-d & \text{se} \quad 1 \leq d \leq q-3, \\ 1 & \text{se} \quad d \geq q-2. \end{cases}$$

Se $\mathbb{T}$ *é um toro projetivo em* $\mathbb{P}^2$*, então a distância mínima de* $C_{\mathbb{T}}(d)$ *é dada por*

$$\delta_d = \begin{cases} (q-1)^2 - d(q-1) & \text{se} \quad 1 \leq d \leq q-2, \\ 2q-d-3 & \text{se} \quad q-1 \leq d \leq 2q-5, \\ 1 & \text{se} \quad d \geq 2q-4. \end{cases}$$

Demonstração. Seja $\mathbb{T}$ um toro projetivo em $\mathbb{P}^1$. Observe que $\operatorname{reg}(I(\mathbb{T})) = q-2$. Se $d \geq q-2$ temos que $\delta_d = 1$ e $\dim_K C_{\mathbb{T}}(d) = |\mathbb{T}| = q-1$, portanto, $\delta_d = |\mathbb{T}| - \dim_K C_{\mathbb{T}}(d) + 1$, isto é, $C_{\mathbb{T}}(d)$ é um código MDS.

Se $d \leq q-3$, temos que

$$\delta_d = (q-1-l)(q-1)^{s-k-2},$$

onde k e l são os únicos inteiros não negativos tais que $1 \leq l \leq q-2$ e $d = k(q-2)+l$. Observe que $s = 2$ e como $d \leq q-3$, temos que $k = 0$ e $l = d$. Isso mostra que $\delta_d = q-1-d$. Note que $|\mathbb{T}| = q-1$ e

$$\dim_K C_{\mathbb{T}}(d) = \sum_{j=0}^{1} (-1)^j \binom{1}{j} \binom{1+d-j(q-1)}{1} =$$

$$\binom{1}{0}\binom{1+d}{1} - \binom{1}{1}\binom{1+d-(q-1)}{1} = \binom{1}{0}\binom{1+d}{1} = d+1.$$

Portanto, $\delta_d = |\mathbb{T}| - \dim_K C_{\mathbb{T}}(d) + 1$, ou seja, $C_{\mathbb{T}}(d)$ é um código MDS.

Agora, seja $\mathbb{T}$ um toro projetivo em $\mathbb{P}^2$. Nesse caso, $s = 3$ e $\mathrm{reg}(I(\mathbb{T})) = 2(q-2) = 2q-4$. Seja $d < \mathrm{reg}(I(\mathbb{T}))$. Assim,

$$\delta_d = (q-1)^{1-k}(q-1-l)$$

onde k e l são os únicos inteiros não negativos tais que $1 \leq l \leq q-2$ e $d = k(q-2)+l$.

Se $d < q-2$ temos que $k = 0$ e $l = d$, logo

$$\delta_d = (q-1)(q-1-d) = (q-1)^2 - d(q-1).$$

Se $d = q-2$ temos que $k = 1$ e $l = 0$, logo

$$\delta_d = (q-1)^0(q-1-0) = q-1 = (q-1)^2 - d(q-1).$$

Se $d > q-2$, como $d < 2(q-2)$ temos que $k = 1$ e $l = d-(q-2)$, logo

$$\delta_d = (q-1)^0(q-1-d+q-2) = 2q-d-3.$$

Portanto,

$$\delta_d = \begin{cases} (q-1)^2 - d(q-1) & \text{se} \quad 1 \leq d \leq q-2, \\ 2q-d-3 & \text{se} \quad q-1 \leq d \leq 2q-5, \\ 1 & \text{se} \quad d \geq 2q-4. \end{cases}$$

■

Observe que se $\mathbb{T}$ é um toro projetivo em $\mathbb{P}^2$, então $C_{\mathbb{T}}(d)$ pode não ser um código MDS. De fato, considere F um corpo com 5 elementos e $d = 2$. Assim, temos que $|\mathbb{T}| = 16$, $\delta_d = 10$ e $\dim_F C_{\mathbb{T}}(d) = 6$. Nesse caso,

$$\delta_d < |\mathbb{T}| - \dim_F C_{\mathbb{T}}(d) + 1.$$

5.4 Toros Projetivos Parametrizados por Clutters

Proposição 5.4.1 *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* $G = 0$.

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 $G = 0$.
Suponha que a proposição é verdadeira para $n-1$ (com $n \geq 2$) e vamos prová-la 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 $G_j = 0$, para todo $j = 1, \ldots, s$ e, portanto $G = 0$. ■

Proposição 5.4.2 *Sejam* $B = K[t_1, \ldots, t_s, y_1, \ldots, y_n, z], S = K[t_1, \ldots, t_s]$ *e* $I \subset B$ *um ideal. Se* G *é uma base de Groebner para* I *com respeito a ordem lexicográfica (com* $z > y_1 > y_2 > \cdots > y_n > t_1 > \cdots > t_s$*), 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 $\mathrm{lt}(g)$, 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 $\mathrm{lt}(g)$, para algum $g \in G$. Como $f \in I'$, isso nos diz que $\mathrm{lt}(g)$ envolve apenas as variáveis $t_1, \ldots, t_s$. Agora, observe que, como estamos utilizando a ordem lexicográfica com $z > y_1 > \cdots > y_n > t_1 > \cdots > t_s$, qualquer monômio envolvendo $y_1, \ldots, y_n, z$ 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 5.4.3 *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 5.4.4 *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:

- 1^o 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 $t^{\theta+\delta} - t^\beta$.

- 2^o 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 5.4.5 *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* $\mathrm{lt}(f) = t^\alpha, \mathrm{lt}(g) = t^\gamma$ *e* $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g)) = t^\theta$*, então:*

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

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

Lema 5.4.6 *Sejam* $B = K[t_1, \ldots, t_s, y_1, \ldots, y_n, z]$ *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 a ordem lexicográfica com $z > y_1 > \cdots > y_n > t_1 > \cdots > t_s$. Utilizando o algoritmo de Buchberger podemos a partir de $\{g_1, \ldots, g_t\}$ obter uma base de Groebner G para I formada por binômios. Assim, temos que $G \cap S$ é uma base (de Groebner) para $I \cap S$, portanto, $I \cap S$ é um ideal binomial. ■

Teorema 5.4.7 *Sejam* $B = K[t_1, \ldots, t_s, y_1, \ldots, y_n, z]$ *e* $S = K[t_1, \ldots, t_s]$*. Temos que*

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

e $I(X)$ *é um ideal binomial.*

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

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

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

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

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

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

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

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

onde p_i é um polinômio do ideal $\langle t_1 - y^{v_1}z, \ldots, t_s - y^{v_s}z\rangle$. Assim,

$$F = \lambda_1 p_1 + \cdots + \lambda_r p_r + F(y^{v_1}z, \ldots, y^{v_s}z) = \lambda_1 p_1 + \cdots + \lambda_r p_r + z^d F(y^{v_1}, \ldots, y^{v_s}).$$

Como $\lambda_1 p_1 + \cdots + \lambda_r p_r \in \langle t_1 - y^{v_1}z, \ldots, t_s - y^{v_s}z\rangle$, temos que

$$F = \sum_{i=1}^{s} g_i(t_i - y^{v_i}z) + z^d F(y^{v_1}, \ldots, y^{v_s}),$$

para alguns $g_1, \ldots, g_s$ em B. Considere a ordem lexicográfica com

$$z > y_1 > \cdots > y_n > t_1 > \cdots > t_s.$$

Pelo algoritmo da divisão em $K[y_1, \ldots, y_n]$ temos que

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

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 $k = 1, \ldots, n$. Assim,

$$F = \sum_{j=1}^{s} g_j \cdot (t_j - y^{v_j}z) + z^d \left(\sum_{k=1}^{n} h_k \cdot (y_k^{q-1} - 1)\right) + z^d G(y_1, \ldots, y_n). \tag{5.5}$$

Para mostrar que $F \in I' \cap S$, devemos mostrar que $G = 0$. Vejamos que G se anula em $(K^*)^n$. Seja $x = (x_1, \ldots, x_n) \in (K^*)^n$. Substituindo t_j por x^{v_j}, para todo $j \in \{1, \ldots, s\}$ em (5.5) e usando o fato de que F se anula em X, temos que

$$0 = F(x^{v_1}, \ldots, x^{v_s}) = \sum_{j=1}^{s} g_j' \cdot (x^{v_j} - y^{v_j}z) + z^d \left(\sum_{k=1}^{n} h_k \cdot (y_k^{q-1} - 1)\right) + z^d G(y_1, \ldots, y_n), \tag{5.6}$$

onde $g'_j = g_j(x^{v_1}, \ldots, x^{v_s}, y_1, \ldots, y_n, z)$, ou seja,

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

é igual ao polinômio nulo para todos os valores de $y_1, \ldots, y_n, z$. Assim, tomando $z = 1$ e $y_k = x_k$, para todo k, na equação (5.6) segue que G se anula em $x = (x_1, \ldots, x_n)$. Portanto, $G = 0$.

Agora, vamos mostrar a inclusão $I(X) \supseteq I' \cap S$. Como I' é um ideal binomial em B, temos que $I' \cap S$ é um ideal binomial em S. Assim, basta mostrar que todo binômio em $I' \cap S$ é homogêneo e se anula em X. Seja $f = t^a - t^b$ um binômio em $I' \cap S$, onde $a = (a_1, \ldots, a_s)$ e $b = (b_1, \ldots, b_s)$. Como $f \in I'$, podemos escrever

$$f = \sum_{i=1}^{s} g_i \cdot (t_i - y^{v_i} z) + \sum_{j=1}^{n} h_j \cdot (y_j^{q-1} - 1), \tag{5.7}$$

para alguns polinômios $g_1, \ldots, g_s, h_1, \ldots, h_n$ em B. Substituindo $t_i = y^{v_i} z$, para $i = 1, \ldots, s$, obtemos

$$f(y^{v_1} z, \ldots, y^{v_s} z) = \sum_{j=1}^{n} h'_j \cdot (y_j^{q-1} - 1),$$

onde $h'_j = h_j(y^{v_1} z, \ldots, y^{v_s} z, y_1, \ldots, y_n, z)$. Substituindo $y_i = 1$, para $i = 1, \ldots, n$, vemos que $f(z, \ldots, z) = 0$, ou seja,

$$z^{a_1} \cdots z^{a_s} - z^{b_1} \cdots z^{b_s} = 0.$$

Assim, temos que $a_1 + \cdots + a_s = b_1 + \cdots + b_s$, logo f é homogêneo.
Seja $[p] = [x^{v_1}, \ldots, x^{v_s}] \in X$. Tomando $t_i = x^{v_i}$ em (5.7), obtemos

$$f(x^{v_1}, \ldots, x^{v_s}) = \sum_{i=1}^{s} \tilde{g}_i \cdot (x^{v_i} - y^{v_i} z) + \sum_{j=1}^{n} \tilde{h}_j \cdot (y_j^{q-1} - 1).$$

Substituindo $z = 1$ e $y_i = x_i$ para todo i, vemos que $f(p) = 0$. Isso mostra que $I(X) \supseteq I' \cap S$.
■

Definição 5.4.8 *Um clutter $\mathcal{C}$ é uma família de subconjuntos de um conjunto base finito $V_{\mathcal{C}} = \{y_1, \ldots, y_n\}$ tal que se $A, B \in \mathcal{C}$, $A \neq B$, então $A \not\subset B$. O conjunto base $V_{\mathcal{C}}$ é chamado conjunto de vértices de $\mathcal{C}$. Os elementos de $\mathcal{C}$ são chamados de arestas.*

Definição 5.4.9 *Seja $\mathcal{C}$ um clutter com conjunto de vértices $V_{\mathcal{C}} = \{y_1, \ldots, y_n\}$ e seja A uma aresta de $\mathcal{C}$. O vetor característico de A é o vetor*

$$v = \sum_{y_i \in A} e_i,$$

onde e_i é o i-ésimo vetor unitário do $\mathbb{R}^n$.

Em toda esta seção vamos assumir que $\{v_1, \ldots, v_s\}$ é o conjunto de todos os vetores característicos das arestas de $\mathcal{C}$.
Relembre que o conjunto tórico algébrico parametrizado por $m_1, \ldots, m_s$ é o conjunto

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

onde

$$\begin{aligned} m_1 &= y^{v_1} = y_1^{v_{11}} \cdots y_n^{v_{1n}} \\ &\vdots \\ m_s &= y^{v_s} = y_1^{v_{s1}} \cdots y_n^{v_{sn}} \end{aligned}$$

são monômios em $K[x_1, \ldots, x_n]$.

Definição 5.4.10 *Se* $a = (a_1, \ldots, a_s) \in \mathbb{R}^s$*, seu suporte é definido como sendo o conjunto*

$$\operatorname{supp}(a) = \{i : a_i \neq 0\}.$$

Observe que se $V_{\mathcal{C}} = \{y_1, y_2, y_3, y_4, y_5\}$ e $A = \{y_2, y_5\}$, temos que o vetor característico de A é

$$v = e_2 + e_5 = (0, 1, 0, 0, 1)$$

e o suporte de v é dado por $\operatorname{supp}(v) = \{2, 5\}$.

Observe que num clutter não podemos ter dois vetores característicos $v_1 \neq v_2$ tais que $\operatorname{supp}(v_1) \subset \operatorname{supp}(v_2)$.

Lema 5.4.11 *Seja* $\mathcal{C}$ *um clutter e seja* $f \neq 0$ *um polinômio homogêneo de* $I(X)$ *da forma* $t_i^b - t^c$ *com* $b \in \mathbb{N}$*,* $c \in \mathbb{N}^s$ *e* $i \notin \operatorname{supp}(c)$*, então,*

(i) $\deg(f) \geq q - 1$.

(ii) *Se* $\deg(f) = q - 1$*, então* $f = t_i^{q-1} - t_j^{q-1}$ *para algum* $j \neq i$.

Demonstração. (i) Suponha por absurdo que $b < q - 1$. Seja β o gerador do grupo cíclico $(K^*, \cdot)$. Vamos assumir que

$$f = t_1^b - t_2^{c_2} \cdots t_r^{c_r},$$

onde $c_j \geq 1$ para $2 \leq j \leq r$ e $b = c_2 + \cdots + c_r$. Dado $x = (x_1, \ldots, x_n) \in (K^*)^n$, como f se anula em X temos que $f(m_1(x), \ldots, m_s(x)) = 0$, ou seja, $m_1(x)^b - m_2(x)^{c_2} \cdots m_r(x)^{c_r} = 0$, assim

$$(x_1^{v_{11}} \cdots x_n^{v_{1n}})^b = (x_1^{v_{21}} \cdots x_n^{v_{2n}})^{c_2} \cdots (x_1^{v_{r1}} \cdots x_n^{v_{rn}})^{c_r}. \tag{5.8}$$

Afirmação: Se $v_{1k} = 1$ para algum $k \in \{1, \ldots, n\}$, então $v_{jk} = 1$ para todo $j = 2, \ldots, r$.

De fato, suponha que $v_{jk} = 0$ para algum $j \in \{2, \ldots, r\}$. Escolhendo $x_i = 1$ para todo $i \neq k$ em (5.8) obtemos

$$(x_k^{v_{1k}})^b = (x_k^{v_{2k}})^{c_2} \cdots (x_k^{v_{rk}})^{c_r}.$$

Como $v_{1k} = 1$ temos que $x_k^b = x_k^m$, onde $m = v_{2k}c_2 + \cdots + v_{rk}c_r$. Veja que $m < b$, pois $v_{jk} = 0$. Assim, $x_k^{b-m} = 1$ para todo $x_k \in K^*$. Em particular, $\beta^{b-m} = 1$. Com isso, temos que $b - m$ é um múltiplo de $q - 1$ e portanto $b \geq q - 1$, contradição. Isso prova a afirmação.

Assim, temos que $\operatorname{supp}(v_1) \subseteq \operatorname{supp}(v_i)$ para $i = 2, \ldots, r$, absurdo, pois $\mathcal{C}$ é um clutter. Portanto, $b \geq q - 1$.

(ii) Basta mostrar que $r = 2$. Suponha por absurdo que $r \geq 3$.
Afirmação: Se $v_{2k} = 1$ para algum $k \in \{1, \ldots, n\}$, então $v_{jk} = 1$ para todo $j \geq 3$.

De fato, suponha que $v_{jk} = 0$ para algum $j \geq 3$. Substituindo $x_i = 1$, para todo $i \neq k$, e $b = q - 1$ em (5.8) temos que $1 = x_k^b = x_k^m$, onde $m < b = q - 1$. Assim, $x_k^m = 1$ para todo $x_k \in K^*$, contradição, pois $\beta^m \neq 1$.

Isso mostra que $\text{supp}(v_2) \subseteq \text{supp}(v_i)$ para todo $i \geq 3$. Absurdo, pois $\mathcal{C}$ é um clutter. Portanto, $r = 2$.

■

Se $f_1, \ldots, f_r$ são polinômios homogêneos em $K[t_1, \ldots, t_s]$, temos que $\dim V(f_1, \ldots, f_r) \geq s-1-r$, veja em [4].

Se $V \subseteq \mathbb{P}^{s-1}$ é uma variedade projetiva de dimensão k, temos que $I(V)$ é gerado por no mínimo $s - 1 - k$ polinômios. De fato, digamos que $I(V) = \langle f_1, \ldots, f_r \rangle$. Como $V = V(I(V)) = V(f_1, \ldots, f_r)$, temos que

$$k = \dim V = \dim V(f_1, \ldots, f_r) \geq s - 1 - r,$$

logo, $r \geq s - 1 - k$.

Definição 5.4.12 *Uma variedade $V \subseteq \mathbb{P}^{s-1}$ é uma interseção completa se $I(V)$ é gerado por $(s-1) - \dim V$ elementos.*

Sabemos que $I(\mathbb{T}) = \langle t_1^{q-1} - t_s^{q-1}, \ldots, t_{s-1}^{q-1} - t_s^{q-1} \rangle$, logo, $\mathbb{T}$ é uma interseção completa.

Lema 5.4.13 *Seja $B = \{h_1, \ldots, h_{s-1}\} \subset S$ um conjunto minimal de binômios homogêneos que gera $I(X)$, isto é, $\langle B \backslash \{h_j\} \rangle \subsetneq \langle B \rangle$ para todo $1 \leq j \leq s - 1$. Então, t_i não divide h_j para todos $1 \leq i \leq s$ e $1 \leq j \leq s - 1$.*

Demonstração. Suponha por absurdo que t_i divide h_j para alguns $i \in \{1, \ldots, s\}$ e $j \in \{1, \ldots, s-1\}$. Assim, $h_j = t_i(t^a - t^b)$, onde $\deg(t^a - t^b) = \deg(h_j) - 1$. Como h_j se anula em X e t_i não se anula em nenhum elemento de X, temos que $t^a - t^b$ é homogêneo e se anula em X, ou seja $t^a - t^b \in I(X)$. Como $I(X) = \langle B \rangle$, temos que

$$t^a - t^b = \sum_{l=1}^{s-1} \lambda_l h_l,$$

onde $\lambda_l \in S$. Como $\deg(t^a - t^b) < \deg(h_j)$, temos que

$$t^a - t^b = \sum_{\substack{l=1 \\ l \neq j}}^{s-1} \lambda_l' h_l \in \langle B \backslash \{h_j\} \rangle.$$

Daí, temos que $h_j \in \langle B \backslash \{h_j\} \rangle$ e logo, $\langle B \backslash \{h_j\} \rangle = \langle B \rangle$, absurdo. ■

Teorema 5.4.14 *Seja $\mathcal{C}$ um clutter. Se X é uma interseção completa, então*

$$I(X) = \langle t_1^{q-1} - t_s^{q-1}, \ldots, t_{s-1}^{q-1} - t_s^{q-1} \rangle.$$

Demonstração. Como $X \subset \mathbb{P}^{s-1}$ é uma interseção completa, temos que o ideal binomial $I(X)$ é gerado por $s-1$ binômios homogêneos, digamos $B = \{h_1, \ldots, h_{s-1}\}$, e temos que $\langle B \backslash \{h_i\} \rangle \subsetneq I(X)$, para todo $1 \leq i \leq s - 1$. Vamos assumir que $h_1, \ldots, h_m$ são os binômios de B que contém um termo da forma $t_i^{c_i}$, ou seja, são da forma $t_i^{c_i} - t^c$ e $i \notin \text{supp}(c)$. Pelo lema 5.4.11, temos que $\deg(h_i) \geq q - 1$ para $1 \leq i \leq m$.

Assumindo que $h_1, \ldots, h_k$ são os binômios de B de grau $q-1$ que contém um termo da forma $t_i^{c_i}$, temos que $h_{k+1}, \ldots, h_m$ tem grau maior que $q-1$. Pelo lema 5.4.11, os binômios $h_1, \ldots, h_k$ são da forma $t_i^{q-1} - t_j^{q-1}$. Observe que os termos dos binômios $h_{m+1}, \ldots, h_{s-1}$ não pertencem ao conjunto $\{t_1^{a_1}, \ldots, t_s^{a_s} : a_i \geq 1,\ 1 \leq i \leq s\}$. Dado $i \in \{1, \ldots, s-1\}$, temos que $t_i^{q-1} - t_s^{q-1} \in I(X)$, assim

$$t_i^{q-1} - t_s^{q-1} = \sum_{l=1}^{k} \lambda_l h_l + \sum_{l=k+1}^{m} \mu_l h_l + \sum_{l=m+1}^{s-1} \theta_l h_l,$$

para $\lambda_l, \mu_l, \theta_l \in S$. Como $h_1, \ldots, h_{s-1}$ são binômios homogêneos, podemos reescrever esta igualdade como

$$t_i^{q-1} - t_s^{q-1} = \sum_{l=1}^{k} \lambda_l' h_l + \sum_{l=m+1}^{s-1} \theta_l' h_l,$$

onde $\lambda_l' \in K$ para $1 \leq l \leq k$ e para cada $m+1 \leq l \leq s-1$ ou ocorre $\deg(h_l) > q-1$ e $\theta_l' = 0$ ou ocorre $\deg(h_l) \leq q-1$ e $\deg(h_l) + \deg(\theta_l') = q-1$. Assim, temos

$$t_i^{q-1} - t_s^{q-1} - \sum_{l=1}^{k} \lambda_l' h_l = \sum_{l=m+1}^{s-1} \theta_l' h_l.$$

Temos que ter o lado esquerdo igual ao polinômio nulo, pois do contrário temos que os monômios do lado esquerdo tem que aparecer do lado direito, mas isto é impossível pois os monômios do lado esquerdo tem a forma t_j^{q-1}. Isso mostra que

$$t_i^{q-1} - t_s^{q-1} = \sum_{l=1}^{k} \lambda_l' h_l \in \langle h_1, \ldots, h_k \rangle.$$

Agora, seja $h_l \in \{h_1, \ldots, h_k\}$, digamos que $h_l = t_i^{q-1} - t_j^{q-1}$. Como

$$h_l = (t_i^{q-1} - t_s^{q-1}) - (t_j^{q-1} - t_s^{q-1}),$$

temos que $h_l \in \langle t_1^{q-1} - t_s^{q-1}, \ldots, t_{s-1}^{q-1} - t_s^{q-1} \rangle$. Assim,

$$\langle t_1^{q-1} - t_s^{q-1}, \ldots, t_{s-1}^{q-1} - t_s^{q-1} \rangle = \langle h_1, \ldots, h_k \rangle.$$

Como $I(\mathbb{T}) = \langle h_1, \ldots, h_k \rangle$ temos que $\mathbb{T} = V(I(\mathbb{T})) = V(h_1, \ldots, h_k)$. Como

$$0 = \dim \mathbb{T} = \dim V(h_1, \ldots, h_k) \geq s - 1 - k,$$

temos que $k \geq s-1$ e logo $k = s-1$. Portanto,

$$\langle t_1^{q-1} - t_s^{q-1}, \ldots, t_{s-1}^{q-1} - t_s^{q-1} \rangle = \langle h_1, \ldots, h_{s-1} \rangle = I(X).$$

■

Corolário 5.4.15 *Seja $\mathcal{C}$ um clutter. São equivalentes:*

(i) X *é uma interseção completa.*

(ii) $I(X) = \langle t_1^{q-1} - t_s^{q-1}, \ldots, t_{s-1}^{q-1} - t_s^{q-1} \rangle$.

(iii) $X = \mathbb{T}$.

Demonstração. (i) $\Rightarrow$ (ii) Já está provado.
(ii) $\Rightarrow$ (iii) Como $I(X) = I(\mathbb{T})$, temos que $V(I(X)) = V(I(\mathbb{T}))$, ou seja, $X = \mathbb{T}$.
(iii) $\Rightarrow$ (i) Observe que $I(X) = I(\mathbb{T}) = \langle t_1^{q-1} - t_s^{q-1}, \ldots, t_{s-1}^{q-1} - t_s^{q-1} \rangle$ é um ideal gerado por $s-1$ polinômios, logo, X é uma interseção completa. ■

Lema 5.4.16 *Seja* $i \in \mathbb{N}$ *e considere as aplicações entre* K*- espaços vetoriais*

$$\begin{aligned} \psi_{t_s} : S_{i-1}/I(X)_{i-1} &\longrightarrow S_i/I(X)_i \\ f + I(X)_{i-1} &\longmapsto t_s f + I(X)_i \end{aligned}$$

$$\begin{aligned} \phi : S_i/I(X)_i &\longrightarrow S_i/\langle I(X), t_s \rangle_i \\ f + I(X)_i &\longmapsto f + \langle I(X), t_s \rangle_i. \end{aligned}$$

Temos a seguinte sequência exata:

$$0 \longrightarrow S_{i-1}/I(X)_{i-1} \xrightarrow{\psi_{t_s}} S_i/I(X)_i \xrightarrow{\phi} S_i/\langle I(X), t_s \rangle_i \longrightarrow 0.$$

Demonstração. Inicialmente, vejamos que ψ_{t_s} e ϕ estão bem definidas. Sejam $f, g \in S_{i-1}$ tais que $f + I(X)_{i-1} = g + I(X)_{i-1}$, ou seja, $f - g \in I(X)_{i-1}$. Assim, temos que $t_s(f-g) \in I(X)_i$, ou seja, $t_s f - t_s g \in I(X)_i$, logo, $\psi_{t_s}(f) = \psi_{t_s}(g)$. Suponha $f, g \in S_i$ tais que $f + I(X)_i = g + I(X)_i$. Assim, $f - g \in I(X)_i$. Como $I(X)_i \subseteq \langle I(X), t_s \rangle_i$, temos que $f - g \in \langle I(X), t_s \rangle_i$, logo, $\phi(f) = \phi(g)$.

É fácil ver que ψ_{t_s} e ϕ são transformações lineares e que ϕ é sobrejetora, assim basta mostrar que ψ_{t_s} é injetora e que $\mathrm{Im}(\psi_{t_s}) = \ker(\phi)$. Para mostrar que ψ_{t_s} é injetora, seja $f + I(X)_{i-1} \in \ker(\psi_{t_s})$. Temos que $t_s f + I(X)_i = 0 + I(X)_i$, ou seja, $t_s f \in I(X)_i$. Como t_s não se anula em nenhum elemento de X, temos que $f \in I(X)_{i-1}$. Isso prova que $f + I(X)_{i-1} = 0 + I(X)_{i-1}$.

Agora, vejamos que $\mathrm{Im}(\psi_{t_s}) = \ker(\phi)$. Seja $f + I(X)_{i-1} \in S_{i-1}/I(X)_{i-1}$. Vamos mostrar que $\psi_{t_s}(f + I(X)_{i-1}) \in \ker(\phi)$. Observe que

$$\phi(\psi_{t_s}(f + I(X)_{i-1})) = \phi(t_s f + I(X)_i) = t_s f + \langle I(X), t_s \rangle_i.$$

Como $t_s f \in \langle I(X), t_s \rangle_i$, temos que $t_s f + \langle I(X), t_s \rangle_i = 0 + \langle I(X), t_s \rangle_i$. Assim, $\mathrm{Im}(\psi_{t_s}) \subseteq \ker(\phi)$. Para provar a outra inclusão, seja $f + I(X)_i \in \ker(\phi)$. Temos que $f + \langle I(X), t_s \rangle_i = 0 + \langle I(X), t_s \rangle_i$, ou seja, $f \in \langle I(X), t_s \rangle_i$. Podemos escrever

$$f = g + t_s h,$$

onde $g \in I(X)_i$ e $h \in S_{i-1}$. Como $f - t_s h = g \in I(X)_i$, temos que $f + I(X)_i = t_s h + I(X)_i$. Observe que,

$$\psi_{t_s}(h + I(X)_{i-1}) = t_s h + I(X)_i = f + I(X)_i.$$

Assim, $\mathrm{Im}(\psi_{t_s}) = \ker(\phi)$. ■

Lema 5.4.17 *Se* $d > (q-2)(s-1)$ *então*

$$\frac{K[t_1, \ldots, t_{s-1}]_d}{\langle t_1^{q-1}, \ldots, t_{s-1}^{q-1} \rangle_d} = \{0\}.$$

Demonstração. Seja $d > (q-2)(s-1)$ e seja $m = t_1^{\alpha_1} \cdots t_{s-1}^{\alpha_{s-1}}$ um monômio em $K[t_1, \ldots, t_{s-1}]_d$. Vamos mostrar que $\overline{m} = \overline{0}$. Como $\alpha_1 + \cdots + \alpha_{s-1} = d$ e $d > (q-2)(s-1)$, existe $j \in \{1, \ldots, s-1\}$ tal que $\alpha_j > q-2$. Assim, $t_j^{\alpha_j}$ é múltiplo de t_j^{q-1}, ou seja, $t_j^{\alpha_j} \in \langle t_1^{q-1}, \ldots, t_{s-1}^{q-1} \rangle$, logo, $m \in \langle t_1^{q-1}, \ldots, t_{s-1}^{q-1} \rangle$. Como m tem grau d segue que $m \in \langle t_1^{q-1}, \ldots, t_{s-1}^{q-1} \rangle_d$. Isso prova que $\overline{m} = \overline{0}$. ■

Lema 5.4.18 *Dado* $i \in \mathbb{N}$*, temos que* $\dfrac{S_i}{\langle I(\mathbb{T}), t_s\rangle_i}$ *é isomorfo a* $\dfrac{K[t_1,\ldots,t_{s-1}]_i}{\langle t_1^{q-1},\ldots,t_{s-1}^{q-1}\rangle_i}$ *como* K*-espaços vetoriais.*

Demonstração. Considere a aplicação

$$\begin{aligned} \psi : K[t_1,\ldots,t_{s-1}]_i &\longrightarrow S_i/\langle I(\mathbb{T}), t_s\rangle_i \\ f &\longmapsto \overline{f} \end{aligned}$$

É fácil ver que ψ é uma transformação linear. Inicialmente, vamos mostrar que

$$\ker(\psi) = \langle t_1^{q-1},\ldots,t_{s-1}^{q-1}\rangle_i.$$

Dado $j \in \{1,\ldots,s-1\}$, temos que $\overline{t_j^{q-1}} = \overline{t_j^{q-1} - t_s^{q-1}} = \overline{0}$ em $S/\langle I(\mathbb{T}), t_s\rangle$, logo, $t_j^{q-1} \in \langle I(\mathbb{T}), t_s\rangle$. Assim, temos que $\langle t_1^{q-1},\ldots,t_{s-1}^{q-1}\rangle \subseteq \langle I(\mathbb{T}), t_s\rangle$. Daí, vem que $\langle t_1^{q-1},\ldots,t_{s-1}^{q-1}\rangle_i \subseteq \langle I(\mathbb{T}), t_s\rangle_i$. Dado $f \in \langle t_1^{q-1},\ldots,t_{s-1}^{q-1}\rangle_i$, temos que $f \in \langle I(\mathbb{T}), t_s\rangle_i$, logo, $\psi(f) = \overline{f} = \overline{0}$. Isso prova que $\langle t_1^{q-1},\ldots,t_{s-1}^{q-1}\rangle_i \subseteq \ker(\psi)$.

Para provar a outra inclusão seja $f \in K[t_1,\ldots,t_{s-1}]_i$ tal que $\psi(f) = \overline{0}$, isto é,

$$f \in \langle I(\mathbb{T}), t_s\rangle_i = \langle t_1^{q-1} - t_s^{q-1},\ldots,t_{s-1}^{q-1} - t_s^{q-1}, t_s\rangle_i.$$

Podemos escrever f como

$$f = \sum_{j=1}^{s-1} g_j(t_j^{q-1} - t_s^{q-1}) + g_s t_s,$$

onde $g_1,\ldots,g_s \in S$. Para cada $j \in \{1,\ldots,s\}$, existe h_j e r_j em S tais que $g_j = h_j t_s + r_j$ onde t_s não aparece em r_j. Assim,

$$f = \sum_{j=1}^{s-1} (h_j t_s + r_j)(t_j^{q-1} - t_s^{q-1}) + (h_s t_s + r_s)t_s,$$

que podemos escrever como

$$f = \sum_{j=1}^{s-1} r_j t_j^{q-1} + t_s F,$$

onde $F \in S$. Daí,

$$t_s F = f - \sum_{j=1}^{s-1} r_j t_j^{q-1}.$$

Observe que t_s não aparece em nenhum monômio do lado direito, logo,

$$f = \sum_{j=1}^{s-1} r_j t_j^{q-1}.$$

Como f tem grau i, temos que $f \in \langle t_1^{q-1},\ldots,t_{s-1}^{q-1}\rangle_i$.

Agora, vamos mostrar que $\mathrm{Im}(\psi) = S_i/\langle I(\mathbb{T}), t_s\rangle_i$. Seja $\overline{g} \in S_i/\langle I(\mathbb{T}), t_s\rangle_i$. Dividindo g por t_s obtemos $g = t_s h + r$ onde $h \in S$ e $r \in K[t_1,\ldots,t_{s-1}]_i$. Assim,

$$\overline{g} = \overline{t_s h} + \overline{r} = \overline{r} = \psi(r) \in \mathrm{Im}(\psi).$$

Portanto, $\dfrac{K[t_1,\ldots,t_{s-1}]_i}{\langle t_1^{q-1},\ldots,t_{s-1}^{q-1}\rangle_i}$ é isomorfo a $\dfrac{S_i}{\langle I(\mathbb{T}), t_s\rangle_i}$ como K-espaços vetoriais. ∎

Teorema 5.4.19 $\operatorname{reg}(I(X)) \leq (q-2)(s-1)$ *e vale a igualdade se* X *for uma interseção completa.*

Demonstração. Para cada $i \in \mathbb{N}$ considere $h_i := \dim_K \dfrac{S_i}{\langle I(X), t_s\rangle_i}$. Como

$$0 \longrightarrow \frac{S_{i-1}}{I(X)_{i-1}} \xrightarrow{\psi_{t_s}} \frac{S_i}{I(X)_i} \xrightarrow{\phi} \frac{S_i}{\langle I(X), t_s\rangle_i} \longrightarrow 0$$

é uma sequência exata, temos que

$$\dim_K \frac{S_i}{\langle I(X), t_s\rangle_i} = \dim_K \frac{S_i}{I(X)_i} - \dim_K \frac{S_{i-1}}{I(X)_{i-1}},$$

ou seja, $h_i = H_{I(X)}(i) - H_{I(X)}(i-1)$, para $i \geq 1$. Como $X \subseteq \mathbb{T}$, temos que $I(\mathbb{T}) \subseteq I(X)$, logo, $\langle I(\mathbb{T}), t_s\rangle_i \subseteq \langle I(X), t_s\rangle_i$. Assim, existe uma transformação linear sobrejetora

$$\frac{S_i}{\langle I(\mathbb{T}), t_s\rangle_i} \longrightarrow \frac{S_i}{\langle I(X), t_s\rangle_i},$$

logo,

$$\dim_K \frac{S_i}{\langle I(\mathbb{T}), t_s\rangle_i} \geq \dim_K \frac{S_i}{\langle I(X), t_s\rangle_i} = h_i.$$

Seja

$$D_i := \frac{K[t_1, \ldots, t_{s-1}]_i}{\langle t_1^{q-1}, \ldots, t_{s-1}^{q-1}\rangle_i}.$$

Pelo Lema 5.4.18, temos que $\dfrac{S_i}{\langle I(\mathbb{T}), t_s\rangle_i}$ é isomorfo a D_i, logo, $0 \leq h_i \leq \dim_K D_i$, para todo $i \in \mathbb{N}$. Pelo Lema 5.4.17, temos que $D_i = \{0\}$ para todo $i > (q-2)(s-1)$. Assim,

$$0 \leq h_i \leq \dim_K D_i = 0, \quad \text{para } i \geq (q-2)(s-1)+1.$$

Como $h_i = H_{I(X)}(i) - H_{I(X)}(i-1)$, temos que

$$H_{I(X)}(i-1) = H_{I(X)}(i), \quad \text{para } i-1 \geq (q-2)(s-1).$$

Isso mostra que $\operatorname{reg}(I(X)) \leq (q-2)(s-1)$. Se X é uma interseção completa, então $X = \mathbb{T}$, logo, $\operatorname{reg}(I(X)) = (q-2)(s-1)$. ∎

Proposição 5.4.20 *Se* $d \geq \operatorname{reg}(I(X))$*, então* $\delta_d = 1$.

Demonstração. Dado $d \geq \operatorname{reg}(I(X))$, temos que

$$\dim_K(C_X(d)) = H_{I(X)}(d) = |X| = \dim_K K^{|X|}.$$

Assim, temos que $\delta_d = 1$. ∎

Proposição 5.4.21 *A distância mínima de* $C_X(d)$ *é decrescente, como uma função de* d*, até atingir o valor constante igual a* 1.

Demonstração. A distância mínima de $C_X(d)$ é dada por:

$$\delta_d = \min\{w(\phi_d(f)) : f \in S_d \text{ e } \phi_d(f) \neq 0\}.$$

Temos que

$$w(\phi_d(f)) = |X| - |X_f|,$$

onde $X_f = \{[p] \in X : f(p) = 0\}$. Observe que o mínimo do conjunto

$$\{w(\phi_d(f)) : f \in S_d \text{ e } \phi_d(f) \neq 0\}$$

é atingido quando $|X_f|$ for o maior possível. Suponha que $\delta_d > 1$. Vamos mostrar que $\delta_d > \delta_{d+1}$. Para isto, basta mostrar que

$$\max\{|X_f| : f \in S_d \text{ e } \phi_d(f) \neq 0\} < \max\{|X_f| : f \in S_{d+1} \text{ e } \phi_{d+1}(f) \neq 0\}. \tag{5.9}$$

Seja $f \in S_d$, com $\phi_d(f) \neq 0$, tal que $|X_f| = \max\{|X_f| : f \in S_d \text{ e } \phi_d(f) \neq 0\}$. Como $\delta_d > 1$, existem dois elementos distintos $[a], [b] \in X$, digamos que $a = (1, a_2, \ldots, a_s)$ e $b = (1, b_2, \ldots, b_s)$, tais que $f(a)$ e $f(b)$ são não nulos. Como $a \neq b$, temos que $a_k \neq b_k$ para algum $k \in \{2, \ldots, s\}$. Seja

$$g := f \cdot (a_k t_1 - t_k).$$

Observe que $g \in S_{d+1}$ e $\phi_{d+1}(g) \neq 0$, pois $g(b) = f(b) \cdot (a_k - b_k) \neq 0$. Como $g(a) = 0$ e $f(a) \neq 0$, temos que g tem mais zeros do que f. Isso prova a desigualdade (5.9), e portanto $\delta_d > \delta_{d+1}$.

Agora, suponha que $\delta_d = 1$. Vamos mostrar que $\delta_{d+1} = 1$. Como $\delta_d = 1$, temos que $w(\phi_d(f)) = 1$ para algum $f \in S_d$ com $\phi_d(f) \neq 0$. Seja

$$g := t_1 \cdot f \in S_{d+1}.$$

Como t_1 não se anula em X, temos que os zeros de f e os zeros de g coincidem. Assim, $w(\phi_{d+1}(g)) = 1$. Isso prova que $\delta_{d+1} = 1$.

■

Referências Bibliográficas

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

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

[3] E. Sarmiento, M. Vaz Pinto and R. H. Villarreal, The minimum distance of parameterized codes on projective tori, Appl. Algebra Engrg. Comm. Comput., to appear, 2011. DOI: 10.1007/s00200-011-0148-2.

[4] I. R. Shafarevich; Basic Algebraic Geometry ; vol. 1; second ed; Springer-Verlag; 1994.