CIRILO GONÇALVES JÚNIOR

Códigos do tipo Reed-Muller em interseções completas

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2015

CIRILO GONÇALVES JÚNIOR

Códigos do tipo Reed-Muller em interseções completas

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

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

Orientador: Prof. Dr. Cícero Fernandes de Carvalho.

UBERLÂNDIA - MG
2015

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

G635c 2015

Gonçalves Júnior, Cirilo, 1990-
Códigos do tipo Reed-Muller em interseções completas / Cirilo Gonçalves junior. - 2015.
57 f.

Orientador: Cícero Fernandes de Carvalho.
Dissertação (mestrado) - Universidade Federal de Uberlândia, Programa de Pós-Graduação em Matemática.
Inclui bibliografia.

1. Matemática - Teses. 2. Bases de Gröbner - Teses. 3. Álgebra comutativa - Teses. 4. Geometria algébrica - 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: Cirilo Gonçalves Júnior.

NÚMERO DE MATRÍCULA: 11312MAT004.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Códigos do tipo Reed-Muller em interseções completas.

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 20 de Fevereiro de 2015, às 14h00min, 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, 20 de Fevereiro de 2015.

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.

GONÇALVES JÚNIOR, C. *Códigos do tipo Reed-Muller em interseções completas*. 2015. 57 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Este trabalho tem como objetivo apresentar resultados sobre o comprimento e a dimensão de códigos sobre interseções completas. Também determinamos a distância mínima em um caso particular de tais códigos. As ferramentas utilizadas provêm da teoria de bases de Groebner, álgebra comutativa e geometria algébrica. Nesse trabalho recordamos os conceitos destas teorias que são necessárias para a análise dos códigos, e também apresentamos fatos da teoria de códigos lineares.

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

GONÇALVES JÚNIOR, C. *Reed Muller codes on Complete Intersections*. 2015. 57 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

This work aims at presenting results on the length and dimension of codes defined over complete intersections. We also determine the minimum distance in a particular case of such codes. The tools that we use come from Groebner bases theory, commutative algebra and algebraic geometry. The work recalls the concepts from these theories that are necessary for the analysis of the codes, and also presents facts of the theory of linear codes.

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

Sumário

Introdução

Este trabalho trata de códigos corretores de erros, em particular, dos parâmetros básicos que são: distância mínima, dimensão e comprimento. Essa teoria é um campo de pesquisa ativo em diversas áreas do conhecimento: matemática, computação, estatística, engenharia elétrica entre outras. 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. Esses códigos são utilizados quando as mensagens são transmitidas com algum tipo de ruído, ou seja, quando não transmitem a mensagem tal como foi enviada. Um código corretor de erros procura, essencialmente, acrescentar de uma forma organizada, alguns dados a cada informação que se pretende transmitir para que possa recuperar a informação detectando e corrigindo eventuais erros que possam surgir.

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 três 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 vemos as propriedades que serão mais utilizadas no desenvolvimento deste trabalho. Estes primeiros capítulos podem ser encontrados no livro de D. COX, J. LITTLE, e D. O'SHEA *Ideals, Varieties, e Algorithms* ([1]).

O capítulo 3, trata os códigos sobre interseções completas, primeiramente obtendo resultados sobre o anel $R_{\mathcal{X}} := A/I_{\mathcal{X}}$, onde $A = K[x_0, x_1, \ldots, x_n]$ e seu módulo canônico $\omega_{\mathcal{X}}$ (ver [5]). Então damos uma definição para o conceito de interseção completa (ver [3]e [4]), com isso construímos o código de avaliação de ordem j, denotado por $C_{\mathcal{X}}(j)$, sobre uma interseção completa, como sendo a imagem de uma aplicação de avaliação. Nessa altura, calculamos a dimensão e o comprimento desse código. Além disso, usamos o módulo canônico $\omega_{\mathcal{X}}$, para definirmos um código dual para o código $C_{\mathcal{X}}(a_{\mathcal{X}})$, onde $a_{\mathcal{X}}$ é o a-invariante de $R_{\mathcal{X}}$ (ver [10] e [5]). Finalmente, terminamos esse trabalho apresentando uma interseção completa particular (ver [9]), na qual utilizamos algumas ferramentas da teoria das bases de Groebner para calcular a distância mínima do código $C_{\mathcal{X}}(j)$ proveniente dessa interseção completa.

Cirilo Gonçalves Júnior
Uberlândia-MG, 20 de fevereiro de 2015.

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 o máximo* $|\alpha|$ *tal que* $a_\alpha \neq 0$*.*

Definição 1.1.3 *Uma ordem monomial* $\succeq$ *no conjunto dos monômios* $\mathcal{M}_n \subseteq K[x_1, \ldots, x_n]$ *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* $\mathrm{mdeg}(f_i) = \delta \in \mathbb{N}^n$*, para todo* i*.*

Se $\mathrm{mdeg}\left(\sum_{i=1}^{s} c_i f_i\right) < \delta$*, 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,* $\mathrm{mdeg}\,(S(f_j, f_k)) < \delta$*.*

Demonstração. Seja $d_i := \mathrm{LC}(f_i)$, assim $\mathrm{LC}(c_i f_i) = c_i d_i$. Como $\mathrm{mdeg}(f_i) = \delta, \forall i = 1, \ldots, s$ e $\mathrm{mdeg}\left(\sum_{i=1}^{s} c_i f_i\right) < \delta$, temos que $\sum_{i=1}^{s} c_i d_i = 0$ (do contrário, teríamos $\mathrm{lt}\,(\sum_{i=1}^{s} c_i f_i) = (\sum_{i=1}^{s} c_i d_i)\, x^{\delta}$, logo $\mathrm{mdeg}\,(\sum_{i=1}^{s} c_i f_i) = \delta$, 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 $\mathrm{lm}(f_i) = x^{\delta}, \forall i = 1, \ldots, s$, temos $\mathrm{lcm}(\mathrm{lm}(f_j), \mathrm{lm}(f_k)) = x^{\delta}$ para todo $i \in \{1, \ldots, s\}$.
Observe que

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

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

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

■

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 $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle$, basta mostrar que $\mathrm{lt}(I) \subseteq \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle$.
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 $\mathrm{lt}(g') = \mathrm{lt}(g)$, então $\mathrm{lt}(G') = \mathrm{lt}(G)$, logo $\langle \mathrm{lt}(G') \rangle = \langle \mathrm{lt}(G) \rangle = \langle \mathrm{lt}(I) \rangle$, 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 $\mathrm{lt}(g') \notin \langle \mathrm{lt}(G' - \{g'\}) \rangle$ e que $\mathrm{LC}(g') = 1$.
  É claro que $\mathrm{LC}(g') = 1$, pois $\mathrm{lt}(g') = \mathrm{lt}(g)$ e $\mathrm{LC}(g) = 1$.
  De $G' - \{g'\} = G - \{g\}$ vem que $\mathrm{lt}(G' - \{g'\}) = \mathrm{lt}(G - \{g\})$, assim $\langle \mathrm{lt}(G' - \{g'\}) \rangle = \langle \mathrm{lt}(G - \{g\}) \rangle$. Como G é minimal e $g \in G$, temos que $\mathrm{lt}(g') = \mathrm{lt}(g) \notin \langle \mathrm{lt}(G - \{g\}) \rangle = \langle \mathrm{lt}(G' - \{g'\}) \rangle$, 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 $\langle \mathrm{lt}(G - \{g\}) \rangle = \langle \mathrm{lt}(G' - \{g'\}) \rangle$. 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: $\mathrm{lt}(G) = \mathrm{lt}(\widetilde{G})$

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

Como G e $\widetilde{G}$ são bases minimais, temos que $\#G = \#\mathrm{lt}(G) = \#\mathrm{lt}(\widetilde{G}) = \#\widetilde{G}$.
Como $\mathrm{lt}(G) = \mathrm{lt}(\widetilde{G})$, dado $g \in G$, existe $\widetilde{g} \in \widetilde{G}$ tal que $\mathrm{lt}(g) = \mathrm{lt}(\widetilde{g})$. 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 $\langle \mathrm{lt}(G - \{g\}) \rangle$, então nenhum monômio de g, exceto $\mathrm{lm}(g)$, pertence a $\langle \mathrm{lt}(\widetilde{G}) \rangle = \langle \mathrm{lt}(G) \rangle$. 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 $\langle \mathrm{lt}(G) \rangle$. 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

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

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

Códigos de Reed-Muller sobre Interseção Completa

3.1 Códigos sobre interseções completas

Um **anel graduado** é um anel R juntamente com uma decomposição em soma direta

$$R = \bigoplus_{i \geq 0} R_i,$$

onde cada R_i é um grupo abeliano, e $R_i R_j \subset R_{i+j}$ para $i, j \geq 0$. Um **elemento homogêneo** de R é um elemento de algum R_i, e um **ideal homogêneo** de R é um ideal gerado por elementos homogêneos. Nessas condições, um **módulo graduado** sobre R é um módulo M com a decomposição

$$M = \bigoplus_{i=-\infty}^{\infty} M_i,$$

onde cada M_i é um grupo abeliano, e $R_i M_j \subset M_{i+j}$ para todos i e j. Precisaremos ainda, de uma notação que indica o deslocamento da graduação (shift) em d passos, ou seja, consideramos o módulo graduado $M(d)$ isomorfo a M com a graduação

$$M(d)_e = M_{d+e}.$$

Sejam K um corpo finito com q elementos, onde q é uma potência de um primo p e $A = K[x_0, x_1, \ldots, x_n] = \oplus_{j \geq 0} A_j$ o anel de polinômios nas variáveis $x_0, x_1, \ldots, x_n$ sobre o corpo K, com a graduação usual. Seja $\mathcal{X} = \{P_1, \ldots, P_m\} \subseteq \mathbb{P}^n(K)$ e

$$I_{\mathcal{X}} := \{f \in A \mid f(P_i) = 0, \forall i = 1, \ldots, m\} = \bigoplus_{j \geq 0} I_{\mathcal{X},j}$$

o ideal gerado pelos polinômios homogêneos que se anulam em $\mathcal{X}$ e o anel quociente

$$R_{\mathcal{X}} := A/I_{\mathcal{X}} = \oplus_{j \geq 0} A_j / I_{\mathcal{X},j}.$$

A função de Hilbert do anel $R_{\mathcal{X}}$ é definida por

$$H_{\mathcal{X}}(j) := \dim_K A_j - \dim_K I_{\mathcal{X},j}, \forall j \in \mathbb{Z}$$

a série de Hilbert correspondente é dada por

$$F_{\mathcal{X}}(t) = \sum_{j=0}^{\infty} H_{\mathcal{X}}(j) t^j.$$

Seja $I_{\mathcal{X}} = \oplus_{r=\gamma}^{\infty} I_{\mathcal{X},r}$ com $I_{\mathcal{X},\gamma} \neq 0$, onde γ é o menor grau de uma componente homogênea não trivial do ideal $I_{\mathcal{X}}$. Existe um inteiro $a_{\mathcal{X}}$ chamado de **a-invariante** de $R_{\mathcal{X}}$ tal que:

(1) $H_{\mathcal{X}}(j) = \dim_K A_j = \binom{j+n}{n}$ se, e somente se, $j < \gamma$;

(2) $H_{\mathcal{X}}(j) < H_{\mathcal{X}}(j+1) < m$ para $0 \leq j < a_{\mathcal{X}}$;

(3) $H_{\mathcal{X}}(j) = m$ para $j > a_{\mathcal{X}}$.

O número $a_{\mathcal{X}} + 1$ é chamado de **índice de regularidade** de $R_{\mathcal{X}}$.

Observação 3.1.1 *Pode-se mostrar que para* $j > a_{\mathcal{X}}$ *a função de Hilbert* $H_{\mathcal{X}}(j)$ *é um polinômio em* j*, chamado de polinômio de Hilbert e é tal que* $\deg H_{\mathcal{X}}(j) = \dim R_{\mathcal{X}} - 1$*, onde* $\dim R_{\mathcal{X}}$ *é a dimensão de Krull de* $R_{\mathcal{X}}$*, ver [4, 4.1.8]. Como mencionado acima, para* $j > a_{\mathcal{X}}$ *no nosso caso temos* $H_{\mathcal{X}}(j) = m$*, logo* $\dim R_{\mathcal{X}} = 1$.

Lema 3.1.2 *Seja* $f \in A$ *um polinômio que não se anula em nenhum ponto de* $\mathcal{X}$*. Então,* $\overline{f} \in R_{\mathcal{X}}$ *não é um divisor de zero em* $R_{\mathcal{X}}$.

Demonstração. Por hipótese $f(P_i) \neq 0$ para todo $i = 1, \ldots, m$. Seja $\overline{g} \in R_{\mathcal{X}} \backslash \{\overline{0}\}$, ou seja, $g \in A \backslash I_{\mathcal{X}}$, logo existe $i \in \{1, \ldots, m\}$ tal que $g(P_i) \neq 0$, então $(f \cdot g)(P_i) = f(P_i) \cdot g(P_i) \neq 0$, implicando $f \cdot g \in A \backslash I_{\mathcal{X}}$, logo $\overline{f \cdot g} \neq \overline{0}$ portanto f não é um divisor de zero em $R_{\mathcal{X}}$. ■

No que se segue gostaríamos que $\overline{x_0} \in R_{\mathcal{X}}$ não fosse um divisor de zero em $R_{\mathcal{X}}$, mas isso nem sempre é verdade, como mostra o exemplo abaixo.

Exemplo 3.1.3 *Sejam* $K = \mathbb{F}_2$*,* $A = K[x_0, x_1, x_2]$*,* $f = x_0$ *e*

$$\mathcal{X} = \{[1,0,0], [0,1,0], [0,0,1], [1,1,1]\} \subset \mathbb{P}^2(K).$$

Se $g = x_1 + x_2$*, temos* $g(0,1,0) = 1 \neq 0$*, logo* $g \notin I_{\mathcal{X}}$*, consequentemente* $\overline{g} = \overline{0}$ *em* $R_{\mathcal{X}}$*. Mas* $fg = x_0x_1 + x_0x_2 \in I_{\mathcal{X}}$*, e assim* $\overline{fg} = \overline{0}$ *em* $R_{\mathcal{X}}$*, portanto* f *é um divisor de zero em* $R_{\mathcal{X}}$.

Uma maneira de resolver esse problema é a seguinte.

Exemplo 3.1.4 *Considere o exemplo 3.1.3. Seja* $\tilde{K}$ *uma extensão de* K *tal que* $[\tilde{K} : K] = 3$*, logo existem* $u_1, u_2 \in \tilde{K}$ *tal que* $\{1, u_1, u_2\}$ *é uma base para* $\tilde{K}$ *como um* K*-espaço vetorial. Desse modo,* $a_0 + u_1a_1 + u_2a_2 \neq 0$ *tomando* $a_0, a_1, a_2 \in K$ *não todos nulos. Defina* $g := x_0 + u_1x_1 + u_2x_2$*, então* g *não se anula em nenhum ponto de* $\mathbb{P}^2(K)$*, e portanto* $\overline{g}$ *não é um divisor de zero em* $R_{\mathcal{X}}$*. Agora considere a aplicação linear:*

$$\begin{array}{rcl} T : \mathbb{P}^2(\tilde{K}) & \longrightarrow & \mathbb{P}^2(\tilde{K}) \\ [a_0, a_1, a_2] & \longmapsto & [a_0 + u_1a_1 + u_2a_2, a_1, a_2] \end{array}$$

que é um isomorfismo, pois sua matriz

$$[T] = \begin{pmatrix} 1 & u_1 & u_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

é claramente invertível. Temos que

$$\begin{array}{rcl} T(1,0,0) & = & (1,0,0) \\ T(0,1,0) & = & (u_1,1,0) \\ T(0,0,1) & = & (u_2,0,1) \\ T(1,1,0) & = & (1+u_1,1,0) \\ T(1,0,1) & = & (1+u_2,0,1) \\ T(0,1,1) & = & (u_1+u_2,1,1) \\ T(1,1,1) & = & (1+u_1+u_2,1,1). \end{array}$$

Além disso, $f = x_0$ *não se anula em* $T(\mathcal{X})$*, logo* $\overline{f}$ *não é um divisor de zero em* $\tilde{R_{\mathcal{X}}} = \tilde{A}/I_{T(\mathcal{X})}$*, onde* $\tilde{A} = \tilde{K}[x_0, x_1, x_2]$*.*

No caso geral, Seja $\tilde{K}$ uma extensão de K tal que $[\tilde{K} : K] = n+1$, logo existem $u_1, \ldots, u_n \in \tilde{K}$ tal que $\{1, u_1, \ldots, u_n\}$ é uma base para $\tilde{K}$ como um K-espaço vetorial. Desse modo,

$$x_0 + u_1x_1 + \ldots + u_nx_n \neq 0 \text{ tomando } x_0, x_1, \ldots, x_n \in K \text{ não todos nulos.}$$

Defina $g := x_0 + u_1x_1 + \ldots + u_nx_n$, então g não se anula em nenhum ponto de $\mathbb{P}^n(K)$, logo não se anula em nenhum ponto de $\mathcal{X}$, e portanto $\overline{g}$ não é um divisor de zero em $R_{\mathcal{X}}$. Agora considere a aplicação linear:

$$\begin{array}{rcl} T : \mathbb{P}^n(\tilde{K}) & \longrightarrow & \mathbb{P}^n(\tilde{K}) \\ [x_0, x_1, \ldots, x_n] & \longmapsto & [x_0 + u_1x_1 + \ldots + u_nx_n, x_1, \ldots, x_n] \end{array}$$

que é um isomorfismo, pois sua matriz

$$[T] = \begin{pmatrix} 1 & u_1 & u_2 & \cdots & u_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

é claramente invertível. Agora vejamos que:

$P \in \mathbb{P}^n(\tilde{K})$ anula g se, e somente se, $T(P) \in \mathbb{P}^n(\tilde{K})$ anula $f := x_0$. De fato, se $P = (a_0, a_1, \ldots, a_n)$ anula g temos que $a_0 + u_1a_1 + \ldots + u_na_n = 0$, logo $T(P) = (0, a_1, \ldots, a_n)$, e portando $f(T(P)) = 0$. Reciprocamente, se $f(T(P)) = 0$ então $T(P) = (0, a_1, \ldots, a_n)$, logo existe $a_0 \in \tilde{K}$ tal que $P = (a_0, a_1, \ldots, a_n)$ e $a_0 + u_1a_1 + \ldots + u_na_n = 0$, portanto $g(P) = 0$.

Assim como g não se anula em nenhum ponto de $\mathcal{X}$, temos que $f = x_0$ não se anula em nenhum ponto de $T(\mathcal{X})$, e portanto $\overline{f}$ não é um divisor de zero em $\tilde{R_{\mathcal{X}}} = \tilde{A}/I_{T(\mathcal{X})}$, onde $\tilde{A} = \tilde{K}[x_0, x_1, \ldots, x_n]$.

Observação 3.1.5 *A aplicação* T *acima é chamada de* **mudança de coordenada projetiva***, tal aplicação induz um* $\tilde{K}$*-isomorfismo*

$$T_* : \tilde{K}[x_0, x_1, \ldots, x_n] \longrightarrow \tilde{K}[x_0, x_1, \ldots, x_n]$$

tal que, para todo $[a_0, \ldots, a_n] \in \mathbb{P}^n(\tilde{K})$ *e todo polinômio* f

$$T_*(f)(a_0, \ldots, a_n) = f(T^{-1}(a_0, \ldots, a_n)) = f\left(a_0 - \sum_{i=1}^{n} u_ia_i, a_1, \ldots, a_n\right),$$

ver [6]. Observe que

$$T_*(f)(T(b)) = f(b), \text{ para todo } b \in \mathbb{P}^n(\tilde{K}).$$

Observação 3.1.6 *Assim vamos assumir a partir de agora, passando possivelmente a uma extensão finita* $\tilde{K}$ *de* K *e aplicando a* $\tilde{K}[x_0, x_1, \ldots, x_n]$ *um isomorfismo linear, que a primeira componente de cada ponto de* $\mathcal{X}$ *é não nula. Nesse caso,* x_0 *não se anula em* $\mathcal{X}$*, então* $x_0 := \overline{x_0}$ *não é um divisor de zero em* $R_{\mathcal{X}}$*. Assim* $R_{\mathcal{X}}$ *contém um subanel isomorfo a* $K[x_0]$*, e vamos escrever* $K[x_0] \subset R_{\mathcal{X}}$*. Como consequência, vemos que* $R_{\mathcal{X}}$ *tem uma estrutura natural de* $K[x_0]$*-módulo.*

Definição 3.1.7 *Sejam* $M = \oplus_{j\in\mathbb{Z}} M_j$ *e* $M' = \oplus_{j\in\mathbb{Z}} M'_j$ *módulos graduados sobre um anel* R. *Dizemos que um homomorfismo* $\varphi : M \longrightarrow M'$ *é* **graduado de grau** d *se*

$$\varphi(M_j) \subseteq M'_{j+d}, \quad \textit{para todo } j \in \mathbb{Z}.$$

Considere o número $h_j := H_{\mathcal{X}}(j) - H_{\mathcal{X}}(j-1)$, para cada $j \geq 1$ e $h_0 = 1$.

Proposição 3.1.8 *Existe um isomorfismo graduado, de grau zero, de* $K[x_0]$*-módulos, entre* $R_{\mathcal{X}}$ *e* $\bigoplus_{j=0}^{a_{\mathcal{X}}+1} K[x_0](-j)^{h_j}$.

Demonstração.

Temos $R_{\mathcal{X}} = \bigoplus_{j\geq 0} R_{\mathcal{X},j}$, onde $R_{\mathcal{X},0} = K$ e seja $h_j = \dim_K R_{\mathcal{X},j} - \dim_K R_{\mathcal{X},j-1}$, para $j \geq 1$ com $h_0 = 1$.

Comecemos pela construção de bases de $R_{\mathcal{X},j}$, como K-espaço vetorial, por indução. Para $R_{\mathcal{X},0}$, temos a base $A_0 = B_0 = \{f_{01} = 1\}$. Como x_0 não é um divisor de zero, então $R_{\mathcal{X},j} \xrightarrow{\cdot x_0} R_{\mathcal{X},j+1}$ é uma aplicação linear injetora. Seja B_j a K-base de $R_{\mathcal{X},j}$, então x_0B_j é linearmente independente em $R_{\mathcal{X},j+1}$. Para $0 \leq j \leq a_{\mathcal{X}}$, temos que $h_{j+1} = \dim_K R_{\mathcal{X},j+1} - \dim_K R_{\mathcal{X},j} > 0$ e portanto existe um conjunto $A_{j+1} = \{f_{j+1,1}, \ldots, f_{j+1,h_{j+1}}\} \subset R_{\mathcal{X},j+1}$, tal que $B_{j+1} = x_0B_j \cup A_{j+1}$ é base de $R_{\mathcal{X},j+1}$ como K-espaço vetorial. Para $j \geq a_{\mathcal{X}} + 1$, x_0B_j é base de $R_{\mathcal{X},j+1}$.

Em outras palavras:

$$\begin{array}{lll}
B_0 = A_0 & \text{base de} & R_{\mathcal{X},0} \\
B_1 = x_0B_0 \cup A_1 = x_0A_0 \cup A_1 & \text{base de} & R_{\mathcal{X},1} \\
B_2 = x_0B_1 \cup A_2 = x_0^2A_0 \cup x_0A_1 \cup A_2 & \text{base de} & R_{\mathcal{X},2} \\
\cdots & \cdots & \\
B_{a_{\mathcal{X}}} = x_0B_{a_{\mathcal{X}}-1} \cup A_{a_{\mathcal{X}}} = x_0^{a_{\mathcal{X}}}A_0 \cup \cdots \cup x_0A_{a_{\mathcal{X}}-1} \cup A_{a_{\mathcal{X}}} & \text{base de} & R_{\mathcal{X},a_{\mathcal{X}}} \\
B_{a_{\mathcal{X}}+1} = x_0B_{a_{\mathcal{X}}} \cup A_{a_{\mathcal{X}}+1} = x_0^{a_{\mathcal{X}}+1}A_0 \cup \cdots \cup x_0A_{a_{\mathcal{X}}} \cup A_{a_{\mathcal{X}}+1} & \text{base de} & R_{\mathcal{X},a_{\mathcal{X}}+1} \\
\cdots & \cdots & \\
B_{j+1} = x_0B_j = x_0^{j+1}A_0 \cup \cdots \cup x_0^{j-a_{\mathcal{X}}}A_{a_{\mathcal{X}}+1} & \text{base de} & R_{\mathcal{X},j+1}
\end{array} \tag{3.1}$$

para $j \geq a_{\mathcal{X}} + 1$.

Temos que

$$\bigcup_{i\geq 0} x_0^iA_0 \cup \bigcup_{i\geq 0} x_0^iA_1 \cup \ldots \cup \bigcup_{i\geq 0} x_0^iA_{a_{\mathcal{X}}+1},$$

é uma K-base para $R_{\mathcal{X}}$ e denotando por $A_jK[x_0]$ o $K[x_0]$-módulo gerado por A_j temos

$$R_{\mathcal{X}} = \bigoplus_{j=0}^{a_{\mathcal{X}}+1} A_jK[x_0]\,,$$

Finalmente

$$\begin{array}{rccl}
\Psi_j : & (K[x_0](-j))^{h_j} & \longrightarrow & A_jK[x_0] \\
& (p_1(x_0), \ldots, p_{h_j}(x_0)) & \longmapsto & p_1(x_0)f_{j,1} + \cdots + p_{h_j}(x_0)f_{j,h_j}
\end{array}$$

é um isomorfismo graduado de grau zero de $K[x_0]$-módulos graduados. De fato, se

$\Psi_j((p_1(x_0),\ldots,p_{h_j}(x_0)))=0$ temos que

$$\begin{aligned}\sum_{i=1}^{h_j} p_i(x_0)f_{j,i} &= \sum_{i=1}^{h_j}\left(\sum_{l=0}^{t} a_{i,l}x_0^l\right)f_{j,i}\\ &= \sum_{l=0}^{t}\sum_{i=1}^{h_j} a_{i,l}x_0^l f_{j,i}\\ &= \underbrace{\sum_{i=1}^{h_j} a_{i,0}f_{j,i}}_{\in R_{\mathcal{X},j}} + \underbrace{\sum_{i=1}^{h_j} a_{i,1}x_0 f_{j,i}}_{\in R_{\mathcal{X},j+1}} + \ldots + \underbrace{\sum_{i=1}^{h_j} a_{i,t}x_0^t f_{j,i}}_{\in R_{\mathcal{X},j+t}}\\ &= 0\end{aligned}$$

como a soma $R_{\mathcal{X},j}+R_{\mathcal{X},j+1}+\ldots+R_{\mathcal{X},j+t}=R_{\mathcal{X},j}\oplus R_{\mathcal{X},j+1}\oplus\ldots\oplus R_{\mathcal{X},j+t}$ é direta, temos que

$$\sum_{i=1}^{h_j} a_{i,l}x_0^l f_{j,i}=0 \text{ para cada } l=1,\ldots,t$$

Como $\{x_0^l f_{j,1},\ldots,x_0^l f_{j,h_j}\}$ é um conjunto K-linearmente independente, temos que $a_{i,l}=0$ para todo $1\le i\le h_j$ e $0\le l\le t$, logo $p_i(x_0)=0$ para todo $1\le i\le h_j$. Portanto Ψ_j é injetor.

Veja que a imagem do elemento $(0,\ldots,1,\ldots,0)$, que é de grau j em $(K[x_0](-j))^{h_j}$, é enviado em $f_{j,i}$ que é de grau j em $A_jK[x_0]$. Por outro lado, por (3.1), os elementos $x_0^l f_{j,i}$, onde $0\le l\le t$ e $1\le i\le h_j$, são todos K-linearmente independentes.

Dessa forma temos

$$R_{\mathcal{X}}\simeq\bigoplus_{j=0}^{a_{\mathcal{X}}+1}(k[x_0](-j))^{h_j}\,. \tag{3.2}$$

■

Observação 3.1.9 *Para $j\ge a_{\mathcal{X}}+1$ temos que $R_{\mathcal{X},j}\simeq R_{\mathcal{X},a_{\mathcal{X}}+1}$, na verdade*

$$R_{\mathcal{X},j}=x_0^{j-(a_{\mathcal{X}}+1)}R_{\mathcal{X},a_{\mathcal{X}}+1}.$$

Agora como $R_{\mathcal{X}}$ e $K[x_0]$ são $K[x_0]$-módulos, temos que

$$N:=\mathrm{Hom}_{K[x_0]}(R_{\mathcal{X}},K[x_0])=\{\varphi:R_{\mathcal{X}}\longrightarrow K[x_0]\mid \varphi \text{ é um } K[x_0]\text{-homomorfismo}\}$$

é um $R_{\mathcal{X}}$-módulo graduado com as operações

$$\begin{aligned}&+:N\times N\longrightarrow N \quad \text{dada por} \quad (\varphi+\psi)(\overline{g})=\varphi(\overline{g})+\psi(\overline{g}),\ \text{e}\\ &\cdot:R_{\mathcal{X}}\times N\longrightarrow N \quad \text{dada por} \quad (\overline{h}\cdot\psi)(\overline{g})=\psi(\overline{hg}).\end{aligned}$$

De fato, $(N,+)$ é um grupo abeliano e

- $((\overline{h_1}+\overline{h_2})\cdot\varphi)(\overline{g})=\varphi(\overline{(h_1+h_2)g})=\varphi(\overline{h_1g}+\overline{h_2g})=\varphi(\overline{h_1g})+\varphi(\overline{h_2g})=(\overline{h_1}\cdot\varphi)(\overline{g})+(\overline{h_2}\cdot\varphi)(\overline{g})$;
- $(\overline{h}\cdot(\varphi+\psi))(\overline{g})=(\varphi+\psi)(\overline{hg})=\varphi(\overline{hg})+\psi(\overline{hg})=(\overline{h}\cdot\varphi)(\overline{g})+(\overline{h}\cdot\psi)(\overline{g})$;
- $((\overline{h_1}\cdot\overline{h_2})\cdot\varphi)(\overline{g})=\varphi(\overline{h_1h_2g})=\varphi(\overline{h_2h_1g})=(\overline{h_2}\cdot\varphi)(\overline{h_1g})=(\overline{h_1}\cdot(\overline{h_2}\cdot\varphi))(\overline{g})$;

- $(\overline{1}\cdot\varphi)(\overline{g}) = \varphi(\overline{1\cdot g}) = \varphi(\overline{g})$,

para todos $\overline{h_1}, \overline{h_2}, \overline{g} \in R_{\mathcal{X}}$ e todos $\varphi, \psi \in N$. Além disso,

$$N_d := \{\varphi \in N \mid \varphi(R_{\mathcal{X},j}) \subseteq K[x_0]_{j+d} \text{ para todo } j \geq 0\}$$

é a componente d-homogênea de N. De fato,

- Sejam $\varphi, \psi \in N_d$ e $\overline{g} \in R_{\mathcal{X},j}$, temos que $(\varphi+\psi)(\overline{g}) = \varphi(\overline{g}) + \psi(\overline{g}) \in K[x_0]_{j+d}$ e $(-\varphi)(\overline{g}) = \varphi(\overline{-g}) \in K[x_0]_{j+d}$, logo $(\varphi+\psi), (-\varphi) \in N_d$. Portanto, N_d é um subgrupo abeliano de N.

- Seja $\psi = \overline{g}\cdot\varphi$, com $\overline{g} \in R_{\mathcal{X},j}$ e $\varphi \in N_d$, como $\psi(\overline{h}) = (\overline{g}\cdot\varphi)(\overline{h}) = \varphi(\underbrace{\overline{gh}}_{j+s}) \in K[x_0]_{s+j+d}$ para todo $\overline{h} \in R_{\mathcal{X},s}$, isso mostra que $N_d \cdot R_{\mathcal{X},j} \subseteq N_{j+d}$.

- Seja $\varphi \in N$. Com a mesma notação da prova de 3.1.8 temos que $R_{\mathcal{X}} = \bigoplus_{j=0}^{a_{\mathcal{X}}+1} A_j K[x_0]$, onde $A_j = \{f_{j,1}, \ldots, f_{j,h_j}\} \subset R_{\mathcal{X}}$ é um conjunto linearmente independente sobre K, para todo $j = 0, \ldots, a_{\mathcal{X}}+1$. Observe que

  $$\varphi(f_{j,i}) = a_{j,i,0} + a_{j,i,1}x_0 + \ldots a_{j,i,t}x_0^t, \text{ para todo } j = 0, \ldots, a_{\mathcal{X}}+1 \text{ e todo } i = 1, \ldots, h_j,$$

  (completando com zeros se necessário, para que x_0^t apareça na expressão de todos os $\varphi(f_{j,i})$). Definimos

  $$\varphi_{j,i,l}(f_{j,i}) = a_{j,i,l}x_0^l, \text{ para todo } j = 0, \ldots, a_{\mathcal{X}}+1, \text{ todo } i = 1, \ldots, h_j \text{ e todo } l = 0, \ldots, t$$

  e

  $$\varphi_{j,i,l}(f_{m,n}) = 0, \text{ se } m \neq j \text{ ou } n \neq i.$$

  Então

  $$\varphi = \sum_{j=0}^{a_{\mathcal{X}}+1}\sum_{i=1}^{h_j}\sum_{l=1}^{t}\varphi_{j,i,l}.$$

  Agora seja $p \in R_{\mathcal{X},s}$, então

  $$p = \sum_{m=0}^{a_{\mathcal{X}}+1}\sum_{n=0}^{h_m}\underbrace{q_{m,n}(x_0)f_{m,n}}_{\text{grau } s},$$

  como o grau de $q_{m,n}(x_0)$ é $s-m$ temos

  $$\begin{aligned}
  \varphi_{j,i,l}(p) &= \varphi_{j,i,l}\left(\sum_{m=0}^{a_{\mathcal{X}}+1}\sum_{n=0}^{h_m} q_{m,n}(x_0)f_{m,n}\right)\\
  &= \sum_{m=0}^{a_{\mathcal{X}}+1}\sum_{n=0}^{h_m} q_{m,n}(x_0)\varphi_{j,i,l}(f_{m,n})\\
  &= q_{j,i}(x_0)\varphi_{j,i,l}(f_{j,i})\\
  &= \underbrace{q_{j,i}(x_0)a_{j,i,l}x_0^l}_{\text{grau } s-j+l} \in K[x_0]_{s+(l-j)}
  \end{aligned}$$

  Desse modo, tomando $d = l-j$ temos que $\varphi_{j,i,l}(R_{\mathcal{X},s}) \subseteq K[x_0]_{s+d}$, logo $\varphi_{j,i,l} \in N_d$.

Portanto,

$$N = \bigoplus_{d\in\mathbb{Z}} N_d$$

O módulo canônico de $R_{\mathcal{X}}$ é definido por

$$\omega_{\mathcal{X}} := N(-1) = \mathrm{Hom}_{K[x_0]}(R_{\mathcal{X}}, K[x_0])(-1) \tag{3.3}$$

é um $R_{\mathcal{X}}$-módulo finitamente gerado, ver [11].

Lema 3.1.10 *Sejam* $M = \oplus_{i=0}^{s} M_i$ *e* M' *módulos sobre um anel* R. *Então*

(a)
$$M = \bigoplus_{i=0}^{s} M_i \simeq \prod_{i=0}^{s} M_i.$$

(b)
$$\mathrm{Hom}_R\left(\bigoplus_{i=0}^{s} M_i, M'\right) \simeq \bigoplus_{i=0}^{s} \mathrm{Hom}_R(M_i, M').$$

(c)
$$\mathrm{Hom}_R(R, R) \simeq R.$$

Demonstração.

(a) Defina

$$\Gamma : M \longrightarrow \prod_{i=0}^{s} M_i$$

dado por $\Gamma(a) = \Gamma(a_0 + \ldots + a_s) = (a_0, \ldots, a_s)$ para todo $a = a_0 + \ldots + a_s \in M$, com $a_i \in M_i$ para todo $i = 0, \ldots, s$. Temos que

$$\begin{aligned}
\Gamma(ra + b) &= \Gamma((ra_0 + b_0) + \ldots + (ra_s + b_s)) \\
&= (ra_0 + b_0, \ldots, ra_s + b_s) \\
&= r \cdot (a_0, \ldots, a_s) + (b_0, \ldots, b_s) \\
&= r \cdot \Gamma(a) + \Gamma(b)
\end{aligned}$$

para todo $r \in R$ e todos $a = a_0 + \ldots + a_s, b = b_0 + \ldots + b_s \in M$, com $a_i, b_i \in M_i$ para todo $i = 0, \ldots, s$, logo Γ é um R-homomorfismo. Dado $a = a_0 + \ldots + a_s \in M$ com $a_i \in M_i$ para todo $i = 0, \ldots, s$, temos que $\Gamma(a) = 0$ se, e somente se, $(a_0, \ldots, a_s) = 0$ se, e somente se, $a_i = 0$ para todo $i = 0, \ldots, s$ se, e somente se, $a = 0$, logo Γ é injetor. Se $(a_0, \ldots, a_s) \in \prod_{i=0}^{s} M_i$ então $\Gamma(a_0 + \ldots + a_s) = (a_0, \ldots, a_s)$, logo Γ é sobrejetor.

(b) Defina

$$\begin{aligned}
\Gamma : \mathrm{Hom}_R(M, M') &\longrightarrow \prod_{i=0}^{s} \mathrm{Hom}_R(M_i, M'). \\
\varphi &\longmapsto (\varphi_{|M_0}, \ldots, \varphi_{|M_s})
\end{aligned}$$

Sejam $\varphi, \psi \in \mathrm{Hom}_R(M, M')$ e $r \in R$, como

$$(r \cdot \varphi + \psi)_{|M_i}(a_i) = (r \cdot \varphi + \psi)(a_i) = r \cdot \varphi(a_i) + \psi(a_i) = r \cdot \varphi_{|M_i}(a_i) + \psi_{|M_i}(a_i)$$

para todo $a_i \in M_i$ e todo $i = 0, \ldots, s$ temos que

$$\begin{aligned}\Gamma(r \cdot \varphi + \psi) &= ((r \cdot \varphi + \psi)_{|M_0}, \ldots, (r \cdot \varphi + \psi)_{|M_s}) \\ &= (r \cdot \varphi_{|M_0} + \psi_{|M_0}, \ldots, r \cdot \varphi_{|M_s} + \psi_{|M_s}) \\ &= r \cdot (\varphi_{|M_0}, \ldots, \varphi_{|M_s}) + (\psi_{|M_0}, \ldots, \psi_{|M_s}) \\ &= r \cdot \Gamma(\varphi) + \Gamma(\psi),\end{aligned}$$

logo Γ é um R-homomorfismo. Dado $\varphi \in \mathrm{Hom}_R(M, M')$ temos que $\Gamma(\varphi) = 0$ se, e somente se, $\varphi_{|M_i} = 0$ para todo $i = 0, \ldots, s$, se, e somente se,

$$\varphi(a) = \varphi(a_0 + \ldots + a_s) = \varphi(a_0) + \ldots + \varphi(a_s) = \varphi_{|M_0}(a_0) + \ldots + \varphi_{|M_s}(a_s) = 0$$

para todo $a = a_0 + \ldots + a_s \in M$, com $a_i \in M_i$ para todo $i = 0, \ldots, s$ se, e somente se, $\varphi = 0$, logo Γ é injetor. Dado $(\psi_0, \ldots, \psi_s) \in \prod_{i=0}^{s} \mathrm{Hom}_R(M_i, M')$, tome

$$\psi : M = \bigoplus_{i=0}^{s} M_i \longrightarrow M'$$

definida por $\psi(a) = \psi_0(a_0) + \ldots + \psi_s(a_s)$ para todo $a = a_0 + \ldots + a_s \in M$, com $a_i \in M_i$ para todo $i = 0, \ldots, s$. Temos que

$$\begin{aligned}\psi(ra + b) &= \psi_0(ra_0 + b_0) + \ldots + \psi_s(ra_s + b_s) \\ &= r \cdot \psi_0(a_0) + \psi_0(b_0) + \ldots + r \cdot \psi_s(a_s) + \psi_s(b_s) \\ &= r \cdot (\psi_0(a_0) + \ldots + \psi_s(a_s)) + (\psi_0(b_0) + \ldots + \psi_s(b_s)) \\ &= r \cdot \psi(a) + \psi(b)\end{aligned}$$

para todo $r \in R$ e todos $a = a_0 + \ldots + a_s, b = b_0 + \ldots + b_s \in M$, com $a_i, b_i \in M_i$ para todo $i = 0, \ldots, s$, portanto ψ é um R-homomorfismo. Além disso, $\Gamma(\psi) = (\psi_{|M_0}, \ldots, \psi_{|M_s}) = (\psi_0, \ldots, \psi_s)$, logo Γ é sobrejetor. Portanto Γ é um isomorfismo.

Assim, pelo item (a) temos que

$$\mathrm{Hom}_R\left(\bigoplus_{i=0}^{s} M_i, M'\right) \simeq \prod_{i=0}^{s} \mathrm{Hom}_R(M_i, M') \simeq \bigoplus_{i=0}^{s} \mathrm{Hom}_R(M_i, M').$$

(c) Defina

$$\begin{aligned}\Gamma : \mathrm{Hom}_R(R, R) &\longrightarrow R \\ \varphi &\longmapsto \varphi(1)\end{aligned}$$

Temos que $\Gamma(r \cdot \varphi + \psi) = (r \cdot \varphi + \psi)(1) = r\varphi(1) + \psi(1) = r \cdot \Gamma(\varphi) + \Gamma(\psi)$ para todo $r \in R$ e todos $\varphi, \psi \in \mathrm{Hom}_R(R, R)$, logo Γ é um R-homomorfismo. Dado $\varphi \in \mathrm{Hom}_R(R, R)$ temos que $\Gamma(\varphi) = 0$ se, e somente se, $\varphi(1) = 0$ se, somente se, $\varphi(r) = r\varphi(1) = 0$ para todo $r \in R$, isto é, $\varphi = 0$, logo Γ é injetor. Dado $r \in R$, defina

$$\begin{aligned}\varphi : R &\longrightarrow R \\ r_1 &\longmapsto r_1 r\end{aligned}$$

temos que $\varphi(r_1 r_2 + r_3) = (r_1 r_2 + r_3)r = r_1(r_2 r) + r_3 r = r_1\varphi(r_2) + \varphi(r_3)$ para todos $r_1, r_2, r_3 \in R$, logo φ é um R-homomorfismo. Além disso, $\Gamma(\varphi) = \varphi(1) = r$, logo Γ é sobrejetor. Portanto Γ é um isomorfismo.

■

Lema 3.1.11 *Sejam* M, M_1, M_2 *módulos sobre o anel* R. *Se* $M_1 \simeq M_2$, *então* $\mathrm{Hom}_R(M_1, M) \simeq \mathrm{Hom}_R(M_2, M)$.

Demonstração. Seja $\Phi : M_1 \longrightarrow M_2$ um isomorfismo. Para cada $\varphi \in \mathrm{Hom}_R(M_1, M)$, defina $\hat{\varphi} : M_2 \longrightarrow M$, dado por $\hat{\varphi}(m) = \varphi(\Phi^{-1}(m))$ para todo $m \in M_2$. Temos que $\hat{\varphi}$ é um R-homomorfismo, pois $\hat{\varphi} = \varphi \circ \Phi^{-1}$, logo $\hat{\varphi} \in \mathrm{Hom}_R(M_2, M)$. defina

$$\begin{array}{rcl} \Gamma : \mathrm{Hom}_R(M_1, M) & \longrightarrow & \mathrm{Hom}_R(M_2, M) \\ \varphi & \longmapsto & \hat{\varphi} \end{array}$$

Dados $\varphi, \psi \in \mathrm{Hom}_R(M_1, M)$ e $a \in R$ temos

$$\begin{array}{rcl} \Gamma(a \cdot \varphi + \psi)(m) & = & \widehat{(a \cdot \varphi + \psi)}(m) \\ & = & (a \cdot \varphi + \psi)(\Phi^{-1}(m)) \\ & = & a\varphi(\Phi^{-1}(m)) + \psi(\Phi^{-1}(m)) \\ & = & a\hat{\varphi}(m) + \hat{\psi}(m) \\ & = & (a \cdot \Gamma(\varphi) + \Gamma(\psi))(m)), \end{array}$$

para todo $m \in M_2$, logo Γ é um R-homomorfismo. Dado $\varphi \in \mathrm{Hom}_R(M_1, M)$ temos que

$$\begin{array}{rcl} \Gamma(\varphi) = 0 & \Leftrightarrow & \Gamma(\varphi)(m) = 0, \text{ para todo } m \in M_2 \\ & \Leftrightarrow & \hat{\varphi}(m) = 0, \text{ para todo } m \in M_2 \\ & \Leftrightarrow & \varphi(\Phi^{-1}(m)) = 0, \text{ para todo } m \in M_2 \\ & \Leftrightarrow & \Phi^{-1}(m) \in \ker(\varphi), \text{ para todo } m \in M_2 \\ & \Leftrightarrow & \mathrm{Im}(\Phi^{-1}) \in \ker(\varphi) \\ & \Leftrightarrow & M_1 \in \ker(\varphi) \\ & \Leftrightarrow & \varphi = 0, \end{array}$$

logo Γ é injetor. Seja $\psi \in \mathrm{Hom}_R(M_2, M)$, defina $\tilde{\psi} : M_1 \longrightarrow M$ dado por $\tilde{\psi}(n) = \psi(\Phi(n))$ para todo $n \in M_1$. Temos que $\tilde{\psi}$ é um R-homomorfismo, pois $\tilde{\psi} = \psi \circ \Phi$, logo $\tilde{\psi} \in \mathrm{Hom}_R(M_1, M)$. Além disso,

$$\Gamma(\tilde{\psi})(m) = \hat{\tilde{\psi}}(m) = \tilde{\psi}(\Phi^{-1}(m)) = \psi(\Phi(\Phi^{-1}(m))) = \psi(m)$$

para todo $m \in M_2$, logo $\Gamma(\tilde{\psi}) = \psi$. Portanto, Γ é um isomorfismo. ■

O próximo resultado segue da aplicação da proposição 3.1.8 e dos lemas 3.1.11 e 3.1.10 no módulo canônico $\omega_{\mathcal{X}}$ de $R_{\mathcal{X}}$.

Proposição 3.1.12 *Temos que*

$$\omega_{\mathcal{X}} \simeq \bigoplus_{i=0}^{a_{\mathcal{X}}+1} K[x_0](i-1)^{h_i}.$$

Demonstração. Combinando os resultados 3.1.8 e 3.1.11 com (3.3) obtemos

$$\omega_{\mathcal{X}} = \mathrm{Hom}_{K[x_0]}(R_{\mathcal{X}}, K[x_0])(-1) \simeq \mathrm{Hom}_{K[x_0]}\left(\bigoplus_{i=0}^{a_{\mathcal{X}}+1} K[x_0](-i)^{h_i}, K[x_0]\right)(-1).$$

Assim, por 3.1.10 temos que

$$\omega_{\mathcal{X}} \simeq \bigoplus_{i=0}^{a_{\mathcal{X}}+1} (\mathrm{Hom}_{K[x_0]}(K[x_0](-i), K[x_0]))^{h_i}(-1).$$

Para cada $i = 1, \ldots, a_{\mathcal{X}} + 1$ temos que $\varphi \in \mathrm{Hom}_{K[x_0]}(K[x_0](-i), K[x_0])_d$ se, e somente se, para todo $p \in K[x_0](-i)_t$ tem-se $\varphi(p) \in K[x_0]_{d+t}$, isto é, para todo $p \in K[x_0]_{t-i}$ tem-se $\varphi(p) \in K[x_0]_{d+t}$, onde $d + t = d + i + (t - i)$, ou seja, φ é homogênea de grau $d + i$ em $\mathrm{Hom}_{K[x_0]}(K[x_0], K[x_0])$, isto é, $\varphi \in \mathrm{Hom}_{K[x_0]}(K[x_0], K[x_0])(i)_d$.

Agora, por 3.1.10 temos que $\mathrm{Hom}_{K[x_0]}(K[x_0](-i), K[x_0]) = \mathrm{Hom}_{K[x_0]}(K[x_0], K[x_0])(i) \simeq k[x_0](i)$, logo

$$(\mathrm{Hom}_{K[x_0]}(K[x_0](-i), K[x_0])^{h_i})(-1) \simeq (K[x_0](i)^{h_i})(-1) \simeq K[x_0](i-1)^{h_i}.$$

Portanto

$$\omega_{\mathcal{X}} \simeq \bigoplus_{i=0}^{a_{\mathcal{X}}+1} K[x_0](i-1)^{h_i}.$$

■

Agora combinamos as proposições 3.1.8 e 3.1.12 para obtermos uma relação entre a função de Hilbert de $R_{\mathcal{X}}$ e a função de Hilbert de $\omega_{\mathcal{X}}$.

Proposição 3.1.13 *Sejam $H_{\mathcal{X}}$ a função de Hilbert de $R_{\mathcal{X}}$ e $H_{\omega_{\mathcal{X}}}$ a função de Hilbert do módulo canônico de $R_{\mathcal{X}}$. Então*

$$H_{\mathcal{X}}(d) + H_{\omega_{\mathcal{X}}}(-d) = m \qquad \textit{para todo } \ d \in \mathbb{Z}.$$

Demonstração. De (3.2) temos que $R_{\mathcal{X}} \simeq \bigoplus_{i=0}^{a_{\mathcal{X}}+1} K[x_0](-i)^{h_i}$, logo

$$H_{\mathcal{X}}(d) = \dim_K R_{\mathcal{X},d} = \dim_K \left(\bigoplus_{i=0}^{a_{\mathcal{X}}+1} K[x_0](-i)^{h_i} \right)_d = \sum_{i=0}^{a_{\mathcal{X}}+1} h_i \dim_K K[x_0]_{d-i}.$$

De 3.1.12 temos que $\omega_{\mathcal{X}} \simeq \bigoplus_{i=0}^{a_{\mathcal{X}}+1} K[x_0](i-1)^{h_i}$, logo

$$H_{\omega_{\mathcal{X}}}(-d) = \dim_K \omega_{\mathcal{X},-d} = \dim_K \left(\bigoplus_{i=0}^{a_{\mathcal{X}}+1} K[x_0](i-1)^{h_i} \right)_{-d} = \sum_{i=0}^{a_{\mathcal{X}}+1} h_i \dim_K K[x_0]_{i-1-d}.$$

Se $i, d \in \mathbb{Z}$ temos que

$$i - 1 - d \geq 0 \Leftrightarrow i - 1 - d > -1 \Leftrightarrow d - i + 1 < 1 \Leftrightarrow d - i < 0$$

Observe que para $l \geq 0$ temos que $\{x_0^l\}$ é uma base para $K[x_0]_l$ com um K-espaço vetorial, então

temos que

$$\begin{aligned}
H_{\mathcal{X}}(d) + H_{\omega_{\mathcal{X}}}(-d) &= \sum_{i=0}^{a_{\mathcal{X}}+1} h_i \dim_K K[x_0]_{d-i} + \sum_{i=0}^{a_{\mathcal{X}}+1} h_i \dim_K K[x_0]_{i-1-d} \\
&= \sum_{i=0}^{a_{\mathcal{X}}+1} h_i \left(\dim_K K[x_0]_{d-i} + \dim_K K[x_0]_{i-1-d}\right) \\
&= \sum_{i=0}^{a_{\mathcal{X}}+1} h_i \\
&= \sum_{i=0}^{a_{\mathcal{X}}+1} (H_{\mathcal{X}}(i) - H_{\mathcal{X}}(i-1)) \\
&= H_{\mathcal{X}}(0) - H_{\mathcal{X}}(-1) + H_{\mathcal{X}}(1) - H_{\mathcal{X}}(0) + \ldots + H_{\mathcal{X}}(a_{\mathcal{X}}+1) - H_{\mathcal{X}}(a_{\mathcal{X}}) \\
&= H_{\mathcal{X}}(a_{\mathcal{X}}+1) - H_{\mathcal{X}}(-1) \\
&= H_{\mathcal{X}}(a_{\mathcal{X}}+1) \\
&= m.
\end{aligned}$$

■

3.2 Interseção Completa

O nosso objetivo agora é estudar o anel quociente $R_{\mathcal{X}}$, onde $\mathcal{X}$ é uma interseção completa.

Definição 3.2.1

(1) *Um conjunto* $\mathcal{Y} \subseteq \mathbb{P}^n(K)$ *é chamado de* **interseção completa** *se*

$$I_{\mathcal{Y}} := \{f \in A \mid f(P) = 0, \forall P \in \mathcal{Y}\}$$

for gerado por uma sequência regular de n *elementos, ou seja, existem* $f_1, \ldots, f_n \in A$ *tais que* $I_{\mathcal{Y}} = \langle f_1, \ldots, f_n \rangle$*, onde* f_i *não é divisor de zero em* $A/\langle f_1, \ldots, f_{i-1} \rangle$ *para todo* $i = 1, \ldots, n$*.*

(2) *Se* $\mathcal{Y} \subseteq \mathbb{P}^n(K)$ *é interseção completa gerado pela sequência regular* $f_1, \ldots, f_n \in A$*, dizemos que* $\mathcal{Y}$ *é uma interseção completa de multigrau* $\mathcal{D} = (d_1, \ldots, d_n)$*, se* f_i *for homogêneo de grau* d_i *para cada* $i = 1, \ldots, n$*.*

Lema 3.2.2 *Sejam* $f_1, \ldots, f_r \in A$ *sequência regular e* $I = \langle f_1, \ldots, f_r \rangle$*. Se* f_i *for homogêneo de grau* a_i *para todo* $i = 1, \ldots, r$*, então a série de Hilbert de* A/I *é dado por*

$$F(t) = \frac{\prod_{i=1}^{n}(1 - t^{a_i})}{(1-t)^{n+1}}.$$

Ver [4].

Lema 3.2.3 *Sejam* $f_1, \ldots, f_r \in A$ *sequência regular e* $I = \langle f_1, \ldots, f_n \rangle$*. Se* f_i *for homogêneo de grau* a_i *para todo* $i = 1, \ldots, r$*, então o módulo canônico de* $M = A/I$ *é dado por*

$$\omega_M = M((a_1 + \ldots + a_r) - (n+1)).$$

Ver [3, pag. 546].

Observação 3.2.4 *Temos que para todo inteiro* d*, a componente homogênea*

$$(\omega_M)_{-d} = M((a_1 + \ldots + a_r) - (n+1))_{-d} = M_{(a_1+\ldots+a_r)-(n+1)-d},$$

em particular, a função de hilbert de M *é dada por*

$$H_{\omega_M}(-d) = \dim_K M_{(a_1+\ldots+a_r)-(n+1)-d}.$$

Proposição 3.2.5 *Seja* $\mathcal{X} = \{P_1, \ldots, P_m\} \subseteq \mathbb{P}^n(K)$ *uma interseção completa gerado pela sequência regular* $f_1, \ldots, f_n \in A$ *de multigrau* $\mathcal{D} = (d_1, \ldots, d_n)$*. Então:*

(1) *O* a*-invariante de* $R_{\mathcal{X}}$ *é dado por*

$$a_{\mathcal{X}} = (d_1 + \ldots + d_n) - (n+1);$$

(2) $H_{\omega_{\mathcal{X}}}(-d) = H_{\mathcal{X}}(a_{\mathcal{X}} - d)$ *para todo* $d \in \mathbb{Z}$*, em particular* $H_{\mathcal{X}}(d) + H_{\mathcal{X}}(a_{\mathcal{X}} - d) = m$*;*

(3) *A série de Hilbert de* $R_{\mathcal{X}}$ *é dada por*

$$F_{\mathcal{X}}(t) = \frac{1}{(1-t)^{n+1}}\left[1 - \sum_{i=1}^{n} t^{d_i} + \sum_{1\leq i_1<i_2\leq n} t^{d_{i_1}+d_{i_2}} - \ldots + (-1)^n t^{d_1+\ldots+d_n}\right];$$

(4) *A função de Hilbert de* $R_{\mathcal{X}}$ *é dada por*

$$H_{\mathcal{X}}(d) = \binom{n+d}{d} - \sum_{i=1}^{n}\binom{n+d-d_i}{d-d_i} + \sum_{1\leq i_1<i_2\leq n}\binom{n+d-(d_{i_1}+d_{i_2})}{d-(d_{i_1}+d_{i_2})} -$$

$$- \sum_{1\leq i_1<i_2<i_3\leq n}\binom{n+d-(d_{i_1}+d_{i_2}+d_{i_3})}{d-(d_{i_1}+d_{i_2}+d_{i_3})} + \ldots + (-1)^n\binom{n+d-(d_1+\ldots+d_n)}{d-(d_1+\ldots+d_n)}.$$

Demonstração.

(1) Temos que

$$\begin{aligned}
F_{\mathcal{X}}(t) &= \sum_{j=0}^{\infty} H_{\mathcal{X}} t^j \\
&= \sum_{j=0}^{a_{\mathcal{X}}} H_{\mathcal{X}} t^j + \sum_{j=a_{\mathcal{X}}+1}^{\infty} H_{\mathcal{X}} t^j \\
&= \sum_{j=0}^{a_{\mathcal{X}}} H_{\mathcal{X}} t^j + \sum_{j=a_{\mathcal{X}}+1}^{\infty} m t^j \\
&= \sum_{j=0}^{a_{\mathcal{X}}} H_{\mathcal{X}} t^j + m\sum_{j=0}^{\infty} t^{(a_{\mathcal{X}}+1)+j} \\
&= \sum_{j=0}^{a_{\mathcal{X}}} H_{\mathcal{X}} t^j + m t^{a_{\mathcal{X}}+1}\sum_{j=0}^{\infty} t^j \\
&= \sum_{j=0}^{a_{\mathcal{X}}} H_{\mathcal{X}} t^j + \frac{m t^{a_{\mathcal{X}}+1}}{1-t}.
\end{aligned}$$

Sabemos de 3.2.2 que $F_{\mathcal{X}}(t) = \dfrac{p(t)}{(1-t)^{n+1}}$, onde $p(t) = \prod_{i=1}^{n}(1-t^{d_i})$, logo

$$\frac{p(t)}{(1-t)^{n+1}} = \sum_{j=0}^{a_{\mathcal{X}}} H_{\mathcal{X}} t^j + \frac{m t^{a_{\mathcal{X}}+1}}{1-t}$$

então

$$p(t) = (1-t)^{n+1} \sum_{j=0}^{a_{\mathcal{X}}} H_{\mathcal{X}} t^j + m t^{a_{\mathcal{X}}+1}(1-t)^n,$$

logo $\deg(p(t)) = a_{\mathcal{X}} + (n+1)$. Observe que $\deg(p(t)) = d_1 + \ldots + d_n$, portanto

$$a_{\mathcal{X}} = (d_1 + \ldots + d_n) - (n+1).$$

(2) De 3.2.4 temos que

$$\begin{aligned} H_{\omega_{\mathcal{X}}}(-d) &= \dim_K R_{\mathcal{X},(d_1+\ldots+d_n)-(n+1)-d} \\ &= \dim_K R_{\mathcal{X},\underbrace{(d_1+\ldots+d_n)-(n+1)}_{a_{\mathcal{X}}}-d} \\ &= \dim_K R_{\mathcal{X},a_{\mathcal{X}}-d} \\ &= H_{\mathcal{X}}(a_{\mathcal{X}} - d) \end{aligned}$$

para todo $d \in \mathbb{Z}$. De 3.1.13 temos que $H_{\mathcal{X}}(d)+H_{\omega_{\mathcal{X}}}(-d) = m$, logo $H_{\mathcal{X}}(d)+H_{\mathcal{X}}(a_{\mathcal{X}}-d) = m$ para todo $d \in \mathbb{Z}$.

(3) De 3.2.2 temos que

$$F_{\mathcal{X}}(t) = \frac{\prod_{i=1}^{n}(1-t^{d_i})}{(1-t)^{n+1}} = \frac{1}{(1-t)^{n+1}}\left[1 - \sum_{i=1}^{n} t^{d_i} + \sum_{1\le i_1<i_2\le n} t^{d_{i_1}+d_{i_2}} - \ldots + (-1)^n t^{d_1+\ldots+d_n}\right].$$

(4) De 3.2.2 temos que

$$F_{\mathcal{X}}(t) = \frac{\prod_{i=1}^{n}(1-t^{d_i})}{(1-t)^{n+1}},$$

como

$$\frac{1}{(i-t)^{n+1}} = \sum_{j=0}^{\infty} \binom{n+j}{j} t^j$$

temos

$$\begin{aligned} F_{\mathcal{X}}(t) &= \sum_{j=0}^{\infty} \binom{n+j}{j} t^j \left[\prod_{i=1}^{n}(1-t^{d_i})\right] \\ &= \sum_{j=0}^{\infty} \binom{n+j}{j} t^j \left[1 - \sum_{i=1}^{n} t^{d_i} + \sum_{1\le i_1<i_2\le n} t^{d_{i_1}+d_{i_2}} - \ldots + (-1)^n t^{d_1+\ldots+d_n}\right] \\ &= \sum_{j=0}^{\infty} H_{\mathcal{X}}(j) t^j \end{aligned}$$

Observe que, se $j + (d_{i_1} + \ldots + d_{i_l}) = d$ então $j = d - (d_{i_1} + \ldots + d_{i_l})$ para $1 \le i_1 < \ldots < i_l \le n$ com $l = 1, \ldots, n$. Assim

$$H_{\mathcal{X}}(d) = \binom{n+d}{d} - \sum_{i=1}^{n} \binom{n+d-d_i}{d-d_i} + \sum_{1\le i_1<i_2\le n} \binom{n+d-(d_{i_1}+d_{i_2})}{d-(d_{i_1}+d_{i_2})} - \ldots +$$

$$+(-1)^n \binom{n+d-(d_1+\ldots+d_n)}{d-(d_1+\ldots+d_n)}.$$

■

3.3 Códigos de Reed-Muller sobre Interseção Completa

De maneira usual, denotaremos por $|Z|$ o número de elementos de um conjunto Z.

Definição 3.3.1 *Um* **código** *(linear)* C *de comprimento* m *é um subespaço de* K^m.

Definição 3.3.2 *Seja* $C \subseteq K^m$ *um código, definimos:*

(1) *A* **dimensão** *do código* C *é a dimensão de* C *como um* K*-espaço vetorial, e será denotada por* $\dim C$*;*

(2) *Dados* $a = (a_1, \ldots, a_m)$ *e* $b = (b_1, \ldots, b_m)$ *em* K^m *definimos a* **distância de Hamming** *entre* a *e* b *como sendo o número de coordenadas que estes elementos diferem, ou seja,*

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

(3) *O peso de um elemento* $a = (a_1, \ldots, a_m) \in K^m$ *é definido como*

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

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

Observação 3.3.3 *A distância de Hamming é uma métrica sobre* K^m. *Mais especificamente, dados* a, b *e* c *em* K^m*, 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 3.3.4 *Seja* $C \subseteq K^m$ *um código. A* **distância mínima** *de* C *é o número*

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

Comprimento, dimensão e distância mínima constituem os **parâmetros básicos** do código. No caso em que $C \subseteq K^m$ é um código de comprimento m, dimensão k e distância mínima δ, dizemos que C é um $[m, k, \delta]$-*código linear*. Os parâmetros do código estão relacionados pela cota de Singleton

$$k + \delta \leq m + 1.$$

Seja $\mathcal{X} = \{P_1, \ldots, P_m\} \subseteq \mathbb{P}^n(K)$. Usaremos a representação padrão para os pontos de $\mathbb{P}^n(K)$, isto é, a primeira entrada não nula a partir da esquerda de cada ponto é 1. Da observação 3.1.6 temos que a primeira entrada a partir da esquerda de cada ponto é 1, além disso, a observação 3.1.5 nos diz que os parâmetros básicos do código não são alterados quando consideramos a

observação 3.1.6. Seja $\mathcal{L}$ um K-espaço vetorial de dimensão finita formado por funções definidas em $\mathcal{X}$ tomando valores em K. Então, a aplicação de avaliação

$$\begin{aligned} ev : \mathcal{L} &\longrightarrow K^m \\ f &\longmapsto (f(P_1), \ldots, f(P_m)) \end{aligned}$$

é um homomorfismo, pois

$$\begin{aligned} ev(a \cdot f + g) &= ((a \cdot f + g)(P_1), \ldots, (a \cdot f + g)(P_m)) \\ &= ((af(P_1) + g(P_1), \ldots, af(P_m) + g(P_m)) \\ &= a \cdot (f(P_1), \ldots, f(P_m)) + (g(P_1), \ldots, g(P_m)) \end{aligned}$$

para todo $a \in K$ e todos $f, g \in \mathcal{L}$. Portanto, $C_{\mathcal{X}} := ev(\mathcal{L})$ define um código linear. Tomemos $\mathcal{L} = A$ e seja $ev_j = ev_{|A_j}$

Definição 3.3.5 *Para cada $j \geq 0$, o código $C_{\mathcal{X}}(j) := ev_j(A_j)$ é chamado de* **código de avaliação** *de ordem j proveniente de $\mathcal{X}$.*

Observação 3.3.6 *Temos que $\ker(ev_j) = I_{\mathcal{X},j}$. De fato,*

$$f \in \ker(ev_j) \Leftrightarrow ev_j(f) = 0 \Leftrightarrow (f(P_1), \ldots, f(P_m)) = 0 \Leftrightarrow f(P_i) = 0, \forall i = 1, \ldots, m \Leftrightarrow f \in I_{\mathcal{X},j}.$$

Então, pelo teorema do homomorfismo temos que

$$C_{\mathcal{X}}(j) \simeq A_j / \ker(ev_j) = A_j / I_{\mathcal{X},j} \simeq R_{\mathcal{X},j}$$

e portanto a dimensão de $C_{\mathcal{X}}(j)$ é dada pela função de Hilbert $H_{\mathcal{X}}$ de $R_{\mathcal{X},j}$, isto é,

$$\dim C_{\mathcal{X}}(j) = H_{\mathcal{X}}(j).$$

Assim, de 3.2.5 temos o seguinte resultado.

Corolário 3.3.7 *Seja $\mathcal{X} = \{P_1, \ldots, P_m\} \subseteq \mathbb{P}^n(K)$ uma interseção completa de multigrau $\mathcal{D} = (d_1, \ldots, d_n)$. Então*

$$\dim C_{\mathcal{X}}(d) = \binom{n+d}{d} - \sum_{i=1}^{n} \binom{n+d-d_i}{d-d_i} + \sum_{1 \leq i_1 < i_2 \leq n} \binom{n+d-(d_{i_1}+d_{i_2})}{d-(d_{i_1}+d_{i_2})} -$$

$$- \sum_{1 \leq i_1 < i_2 < i_3 \leq n} \binom{n+d-(d_{i_1}+d_{i_2}+d_{i_3})}{d-(d_{i_1}+d_{i_2}+d_{i_3})} + \ldots + (-1)^n \binom{n+d-(d_1+\ldots+d_n)}{d-(d_1+\ldots+d_n)}.$$

Definição 3.3.8 *Seja R um anel. Uma sequência de homomorfismos de R-módulos*

$$\ldots \longrightarrow M_{j+1} \xrightarrow{\varphi_{j+1}} M_j \xrightarrow{\varphi_j} M_{j-1} \longrightarrow \ldots$$

é chamada de **complexo** *se $\ker(\varphi_j) \supseteq Im(\varphi_{j+1})$ para todo j. Dizemos que a sequência é* **exata** *em M_j se $\ker(\varphi_j) = Im(\varphi_{j+1})$, dizemos simplesmente que a sequência é* **exata** *se for exata em todo M_j. Uma sequência exata da forma*

$$0 \longrightarrow M_{j+1} \longrightarrow M_j \longrightarrow M_{j-1} \longrightarrow 0$$

é chamada de **sequência exata curta**.

Exemplo 3.3.9 *Sejam R um anel e M, M' módulos sobre R. Temos que*

(1) $0 \xrightarrow{\psi} M \xrightarrow{\varphi} M'$ *é exata se, e somente se,* $Im(\psi) = \{0\} = \ker(\varphi)$*, e logo,* φ *é injetor.*

(2) $M \xrightarrow{\varphi} M' \xrightarrow{\psi} 0$ *é exata se, e somente se,* $\ker(\psi) = M' = Im(\varphi)$*, e logo,* φ *é sobrejetor.*

Exemplo 3.3.10 *Sejam* V, V_1 *e* V_2 *espaços vetoriais de dimensão finita sobre o corpo* K *e*

$$0 \longrightarrow V_1 \xrightarrow{\varphi} V \xrightarrow{\psi} V_2 \longrightarrow 0$$

uma sequência exata curta. Temos que $\ker(\psi) = Im(\varphi)$*,* $Im(\psi) = V_2$ *e* $\ker(\varphi) = \{0\}$*. Pelo teorema do núcleo e imagem temos que*

$$\begin{aligned} \dim_k V &= \dim_K \ker(\psi) + \dim_K Im(\psi) \\ &= \dim_K Im(\varphi) + \dim_K V_2 \\ &= (\dim_k \ker(\varphi) + \dim_K Im(\varphi)) + \dim_K V_2 \\ &= \dim_K V_1 + \dim_K V_2. \end{aligned}$$

Observação 3.3.11 *Sejam* R *um anel e* I *um ideal de* R*, a aplicação* $\psi : R \longrightarrow R/I$ *dada por* $\psi(g) = \overline{g}$ *é um* R*-homomorfismo sobrejetor. A aplicação* ψ *é chamada de* **homomorfismo canônico**.

Teorema 3.3.12 *Sejam* $f_1, \ldots, f_r \in A$ *uma sequência regular e* $I_r = \langle f_1, \ldots, f_r \rangle$*. Se* f_i *for homogêneo de grau* a_i *para todo* $i = 1, \ldots, r$*, então o polinômio de Hilbert de* $M_r := A/I_r$ *é dado por*

$$H_{M_r}(z) = \frac{a_1 \cdot \ldots \cdot a_r}{(n-r)!} \cdot z^{n-r} + \quad \textit{termos de grau menor em } z.$$

Demonstração. Faremos indução sobre r. Para $r = 1$ considere a sequência

$$0 \longrightarrow A(-a_1) \xrightarrow{\varphi} A \xrightarrow{\psi} M_1 \longrightarrow 0,$$

onde $\varphi(g) = gf_1$ para todo $g \in A(-a_1)$ e ψ é o homomorfismo canônico. Temos que a sequência acima é exata, de fato, seja $g \in A(-a_1)$, temos que $\varphi(g) = 0$ se, e somente se, $\varphi(g) = gf_1 = 0$ se, e somente se, $g = 0$ pois f_1 não é um divisor de zero em A. Além disso, é claro que $\mathrm{Im}(\varphi) = I_1 = \ker(\psi)$ e que ψ é sobrejetor.
Temos de 3.3.10 que

$$\begin{aligned} H_{M_1}(z) &= \dim_K M_1(z) \\ &= \dim_K A_z - \dim_K A(-a_1)_z \\ &= \binom{n+z}{z} - \binom{n+z-a_1}{z-a_1} \\ &= \frac{(n+z)!}{n!z!} - \frac{(n+z-a_1)!}{n!(z-a_1)!} \\ &= \frac{(z+n)(z+(n-1)) \cdot \ldots \cdot (z+1) - (z+n-a_1)(z+(n-1)-a_1) \cdot \ldots \cdot (z+1-a_1)}{n!} \\ &= \frac{z^n - z^n}{n!} + \frac{(\sum_{i=1}^{n} i - \sum_{i=1}^{n}(i-a_1))}{n!} \cdot z^{n-1} + \quad \text{termos de grau menor em } z \\ &= \frac{na_1}{n!} \cdot z^{n-1} + \quad \text{termos de grau menor em } z \\ &= \frac{a_1}{(n-1)!} \cdot z^{n-1} + \quad \text{termos de grau menor em } z. \end{aligned}$$

Suponha que o resultado seja verdadeiro para $r-1$. Considere a sequência

$$0 \longrightarrow M_{r-1}(-a_r) \xrightarrow{\varphi} M_{r-1} \xrightarrow{\psi} M_r \longrightarrow 0,$$

onde $\varphi(\overline{g}) = \overline{gf_r}$ e $\psi(\overline{h}) = \overline{h}$. Temos que a sequência acima é exata, de fato

- Temos que $\varphi(p\overline{g}+\overline{h}) = \varphi(\overline{pg+h}) = \overline{(pg+h)f_r} = \overline{pgf_r+hf_r} = p\overline{gf_r}+\overline{hf_r} = p\varphi(\overline{g})+\varphi(\overline{h})$ para todo $p \in A$ e todos $\overline{g},\overline{h} \in M_{r-1}(-a_r)$. E que $\psi(p\overline{g}+\overline{h}) = \psi(\overline{pg+h}) = \overline{pg+h} = p\overline{g}+\overline{h} = p\psi(\overline{g})+\psi(\overline{h})$ para todo $p \in A$ e todos $\overline{g},\overline{h} \in M_{r-1}$. Portanto, φ e ψ são homomorfismos.

- Seja $\overline{g} \in M_{r-1}(-a_r)$, temos que $\varphi(\overline{g}) = 0$ se, e somente se, $\overline{gf_r} = 0$ se, e somente se, $\overline{g} = 0$ pois $\overline{f_r}$ não é um divisor de zero em M_{r-1};

- Temos que

$$\begin{aligned}
\overline{h} \in \mathrm{Im}(\varphi) \subseteq M_{r-1} &\Leftrightarrow \text{ existe } g \in A(-a_r) \text{ tal que } \overline{h} = \varphi(\overline{g}) = \overline{gf_r} \\
&\Leftrightarrow \overline{h} - \overline{gf_r} = \overline{0} \text{ em } M_{r-1} \\
&\Leftrightarrow \overline{h - gf_r} = \overline{0} \text{ em } M_{r-1} \\
&\Leftrightarrow h - gf_r \in I_{r-1} \\
&\Leftrightarrow \text{existem } h_1,\ldots,h_{r-1} \in A \text{ tal que } h - gf_r = h_1f_1 + \ldots + h_{r-1}f_{r-1} \\
&\Leftrightarrow h = h_1f_1 + \ldots + h_{r-1}f_{r-1} + gf_r \\
&\Leftrightarrow h \in I_r \\
&\Leftrightarrow \overline{h} = \overline{0} \text{ em } M_r \\
&\Leftrightarrow \psi(\overline{h}) = \overline{0} \text{ em } M_r \\
&\Leftrightarrow \overline{h} \in \ker(\psi) \subseteq M_{r-1};
\end{aligned}$$

Com isso, de 3.3.10 temos que

$$\dim_K(M_{r-1})_z = \dim_K(M_{r-1}(-a_r))_z + \dim_K(M_r)_z,$$

logo

$$H_{M_r}(z) = H_{M_{r-1}}(z) - H_{M_{r-1}}(z-a_r)$$

pela hipótese de indução temos que existem $b_0, b_1, \ldots, b_{n-r} \in K$ tais que

$$\begin{aligned}
H_{M_r}(z) &= \frac{a_1 \cdot \ldots \cdot a_{r-1}}{(n-r+1)!} \cdot z^{n-r+1} + b_{n-r}z^{n-r} + \ldots + b_1z + b_0 - \\
&- \left(\frac{a_1 \cdot \ldots \cdot a_{r-1}}{(n-r+1)!} \cdot (z-a_r)^{n-r+1} + b_{n-r}(z-a_r)^{n-r} + \ldots + b_1(z-a_r) + b_0 \right),
\end{aligned}$$

logo

$$\begin{aligned}
H_{M_r}(z) &= \frac{a_1 \cdot \ldots \cdot a_{r-1}}{(n-r+1)!} \cdot z^{n-r+1} - \frac{a_1 \cdot \ldots \cdot a_{r-1}}{(n-r+1)!} \cdot z^{n-r+1} + \\
&+ \frac{a_1 \cdot \ldots \cdot a_{r-1}}{(n-r+1)!} \cdot a_r(n-r+1)z^{n-r} + \ldots + b_{n-r}z^{n-r} - b_{n-r}z^{n-r} + \\
&+ \text{ termos de grau menor em } z.
\end{aligned}$$

Portanto,

$$H_{M_r}(z) = \frac{a_1 \cdot \ldots \cdot a_r}{(n-r)!} \cdot z^{n-r} + \text{ termos de grau menor em } z.$$

■

Corolário 3.3.13 *Seja $\mathcal{X} = \{P_1,\ldots,P_m\} \subseteq \mathbb{P}^n(K)$ uma interseção completa de multigrau $\mathcal{D} = (d_1,\ldots,d_n)$. Então o código $C_{\mathcal{X}}(j)$ tem comprimento $|\mathcal{X}| = d_1 \cdot \ldots \cdot d_n$ para todo $j \in \mathbb{Z}$.*

Demonstração. Segue de 3.3.12 que $|\mathcal{X}| = H_{\mathcal{X}}(a_{\mathcal{X}} + 1) = d_1 \cdot \ldots \cdot d_n$. ■

Nosso objetivo agora é estudar o código dual do código $C_{\mathcal{X}}(a_{\mathcal{X}})$.

Definição 3.3.14 *Se C é um código linear em K^m, então o complemento ortogonal de C, segundo o produto interno usual, é chamado de* **código dual** *de C.*

Consideremos o conjunto

$$\mathcal{G} = \{\varphi : R_{\mathcal{X},a_{\mathcal{X}}+1} \longrightarrow K \mid \varphi \text{ é um } K\text{-homomorfismo e } \varphi(x_0 R_{\mathcal{X},a_{\mathcal{X}}}) = 0\}.$$

Lema 3.3.15

1. *Temos que $\omega_{\mathcal{X},-a_{\mathcal{X}}}$ é isomorfo a $\mathcal{G}$.*
2. *Sejam $j \geq 0$, $g \in R_{\mathcal{X},j}$ e $\varphi \in \omega_{\mathcal{X},-a_{\mathcal{X}}}$. Então,*

$$g\varphi = 0 \text{ se, e somente se, } g\varphi_{|R_{\mathcal{X},a_{\mathcal{X}}+1}} = 0.$$

Demonstração.

1. Considere a aplicação

$$\begin{array}{ccccccc} \sigma : \omega_{\mathcal{X},-a_{\mathcal{X}}} & \longrightarrow & \mathcal{G} & & & & \\ \varphi & \longmapsto & \sigma(\varphi) := \varphi_{|R_{\mathcal{X},a_{\mathcal{X}}+1}} : & R_{\mathcal{X},a_{\mathcal{X}}+1} & \longrightarrow & K \\ & & & g & \longmapsto & \varphi(g) \end{array}$$

Primeiramente vejamos que σ está bem definida, para isso usaremos (3.3). Seja

$$\varphi \in \omega_{\mathcal{X},-a_{\mathcal{X}}} = (\mathrm{Hom}_{K[x_0]}(R_{\mathcal{X}}, K[x_0])(-1))_{-a_{\mathcal{X}}} = \mathrm{Hom}_{K[x_0]}(R_{\mathcal{X}}, K[x_0])_{-a_{\mathcal{X}}-1},$$

vejamos que $\sigma(\varphi) \in \mathcal{G}$. Temos que $\varphi : R_{\mathcal{X}} \longrightarrow K[x_0]$ é um $K[x_0]$-homomorfismo homogêneo de grau $-a_{\mathcal{X}}-1$. Para cada $j = 1, \ldots, a_{\mathcal{X}}$ e cada $g \in R_{\mathcal{X},j}$ temos que $j - a_{\mathcal{X}} - 1 < 0$ e $\varphi(g) \in K[x_0]_{j-a_{\mathcal{X}}-1}$, logo $\varphi(g) = 0$, logo $\varphi(R_{\mathcal{X},j}) = 0$. Restringindo φ a $R_{\mathcal{X},a_{\mathcal{X}}+1}$ temos que

$$\sigma(\varphi) = \varphi_{|R_{\mathcal{X},a_{\mathcal{X}}+1}} : R_{\mathcal{X},a_{\mathcal{X}}+1} \longrightarrow K$$

pois $K[x_0]_{(a_{\mathcal{X}}+1)-a_{\mathcal{X}}-1} = K$, e $\sigma(\varphi)$ é um K-homomorfismo. Agora para $g \in x_0 R_{\mathcal{X},a_{\mathcal{X}}} \subset R_{\mathcal{X},a_{\mathcal{X}}+1}$, temos que $g = x_0 h$ para algum $h \in R_{\mathcal{X},a_{\mathcal{X}}}$, logo

$$\sigma(\varphi)(g) = \sigma(\varphi)(x_0 h) = \varphi(x_0 h) = x_0 \varphi(h) = 0.$$

Assim, $\sigma(\varphi)(x_0 R_{\mathcal{X},a_{\mathcal{X}}}) = 0$, portanto, $\sigma(\varphi) \in \mathcal{G}$.
Vejamos agora que σ é um K-homomorfismo. Dados $\varphi, \psi \in \omega_{\mathcal{X},-a_{\mathcal{X}}}$ e $a \in K$ temos $a\varphi + \psi \in \omega_{\mathcal{X},-a_{\mathcal{X}}}$, pois $\omega_{\mathcal{X},-a_{\mathcal{X}}}$ é um $K[x_0]$-módulo. Assim,

$$\begin{aligned} \sigma(a\varphi + \psi)(g) &= (a\varphi + \psi)_{|R_{\mathcal{X},a_{\mathcal{X}}+1}}(g) \\ &= (a\varphi + \psi)(g) \\ &= a\varphi(g) + \psi(g) \\ &= a\varphi_{|R_{\mathcal{X},a_{\mathcal{X}}+1}}(g) + \psi_{|R_{\mathcal{X},a_{\mathcal{X}}+1}}(g) \\ &= a\sigma(\varphi)(g) + \sigma(\psi)(g), \end{aligned}$$

para todo $g \in R_{\mathcal{X},a_{\mathcal{X}}+1}$.
Além disso, se $\varphi \in \ker(\sigma)$ temos que

$$\begin{aligned}\sigma(\varphi) = 0 &\Leftrightarrow \varphi_{|R_{\mathcal{X},a_{\mathcal{X}}+1}} = 0\\ &\Leftrightarrow \varphi(g) = 0 \text{ para todo } g \in R_{\mathcal{X},a_{\mathcal{X}}+1}\\ &\Leftrightarrow \varphi(g) = 0 \text{ para todo } g \in R_{\mathcal{X},j} \text{ com } j = 1,\ldots,a_{\mathcal{X}}+1\\ &\Leftrightarrow \varphi = 0,\end{aligned}$$

pois $R_{\mathcal{X},j} = x_0^{j-(a_{\mathcal{X}}+1)}R_{\mathcal{X},a_{\mathcal{X}}+1}$ para todo $j \geq a_{\mathcal{X}}+1$, ver observação 3.1.9, portanto σ é injetor.
Agora, seja $\psi \in \mathcal{G}$. Se $j \geq a_{\mathcal{X}}+1$ e $g \in R_{\mathcal{X},j}$, então $g = x_0^{j-(a_{\mathcal{X}}+1)}h$ para algum $h \in R_{\mathcal{X},a_{\mathcal{X}}+1}$. Dessa forma podemos estender ψ a aplicação $\tilde{\psi} : R_{\mathcal{X}} \longrightarrow K[x_0]$,

$$\tilde{\psi}(g) = \begin{cases} 0 & , \text{ se } \quad g \in R_{\mathcal{X},j} \text{ com } j \leq a_{\mathcal{X}} \\ x_0^{j-(a_{\mathcal{X}}+1)}\psi(h) & , \text{ se } \quad g \in R_{\mathcal{X},j} \text{ com } j > a_{\mathcal{X}} \end{cases}$$

que é um $K[x_0]$-homomorfismo. Por outro lado, $\tilde{\psi}(g) \in K[x_0]_{j-(a_{\mathcal{X}}+1)}$, para todo $g \in R_{\mathcal{X},j}$, logo $\tilde{\psi} \in \mathrm{Hom}_{K[x_0]}(R_{\mathcal{X}}, K[x_0])_{-a_{\mathcal{X}}-1} = \omega_{\mathcal{X},-a_{\mathcal{X}}}$. Então,

$$\sigma(\tilde{\psi})(g) = \tilde{\psi}_{|R_{\mathcal{X}}(a_{\mathcal{X}}+1)}(g) = \tilde{\psi}(g) = \psi(g),$$

para todo $g \in R_{\mathcal{X},a_{\mathcal{X}}+1}$, logo $\sigma(\tilde{\psi}) = \psi$.
Portanto, σ é um isomorfismo.

2. Suponha que $g\varphi_{|R_{\mathcal{X},a_{\mathcal{X}}+1}} = 0$. Seja $h \in R_{\mathcal{X},s}$.

   - Se $s \leq a_{\mathcal{X}}$ temos que $x_0^{a_{\mathcal{X}}+1-s}(g\varphi)(h) = g\varphi(\underbrace{x_0^{a_{\mathcal{X}}+1-s}h}_{\in R_{\mathcal{X},a_{\mathcal{X}}+1}}) = 0$, logo $(g\varphi)(h) = 0$.

   - Se $s > a_{\mathcal{X}}$, temos que $h = x_0^{s-(a_{\mathcal{X}}+1)}p$ para algum $p \in R_{\mathcal{X},a_{\mathcal{X}}+1}$, logo

     $$(g\varphi)(h) = (g\varphi)(x_0^{s-(a_{\mathcal{X}}+1)}p) = x_0^{s-(a_{\mathcal{X}}+1)}(g\varphi)(p) = 0.$$

     Portanto, $g\varphi = 0$.

■

Agora construiremos uma base B para $R_{\mathcal{X},a_{\mathcal{X}}+1}$ como K-espaço vetorial, então da observação 3.1.9 temos que $x_0^{j-(a_{\mathcal{X}}+1)}B$ é uma base para $R_{\mathcal{X},j}$, para $j \geq a_{\mathcal{X}}+1$, logo podemos escrever $g \in R_{\mathcal{X},j}$ como $K[x_0]$-combinação linear dos elementos de B.

Proposição 3.3.16

1. *Existe uma* K*-base* $f_1,\ldots,f_m$ *para* $R_{\mathcal{X},a_{\mathcal{X}}+1}$ *tal que*

   $$f_i(P_j) = \begin{cases} 1 & , \ se \quad i = j \\ 0 & , \ se \quad i \neq j \end{cases},$$

   para todo $i,j = 1,\ldots,m$.

2. *Seja* $g \in R_{\mathcal{X},j}$ *para* $j \geq a_{\mathcal{X}}+1$*, então* g *se escreve de maneira única como*

   $$g = g(P_1)x_0^{j-(a_{\mathcal{X}}+1)}f_1 + \ldots + g(P_m)x_0^{j-(a_{\mathcal{X}}+1)}f_m.$$

Demonstração.

1. Seja $d = \max\{a_{\mathcal{X}} + 1, m\}$. Para cada $i = 1, \ldots, m$, escrevemos $P_i = [1, p_{i2}, p_{i3}, \ldots, p_{in}]$. Como $P_1 \neq P_2$, podemos escolher $l \in \{1, \ldots, n\}$ tal que $p_{1l} \neq p_{2l}$. Defina

$$h_2 = \frac{x_l - p_{2l}x_0}{p_{1l} - p_{2l}},$$

observe que $h_2(P_1) = 1$ e $h_2(P_2) = 0$. Da mesma forma definimos $h_3, \ldots, h_m$ tais que

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

Considere

$$g_1 = x_0^{d-m+1} h_2 \cdot \ldots \cdot h_m,$$

temos que g_1 é homogêneo de grau $d - m + 1 + (m - 1) = d$, ou seja, $g_1 \in A_d$. Mais ainda, $g_1(P_1) = 1$ e $g_1(P_j) = 0$ para $2 \leq j \leq m$,
Analogamente, construímos $g_2, \ldots, g_m \in A_d$ tais que

$$g_i(P_j) = \begin{cases} 1 & , \text{ se } \quad i = j \\ 0 & , \text{ se } \quad i \neq j \end{cases},$$

para todos $i, j = 1, \ldots, m$, dessa forma logo $g_i \neq 0$ em $R_{\mathcal{X},d}$ para todo $i = 1, \ldots, m$.
Observe que $g_1, \ldots, g_m$ são linearmente independentes em $R_{\mathcal{X},d}$, pois se $a_1 g_1 + \ldots + a_m g_m = 0$, com $a_1, \ldots, a_m \in K$, temos para cada $i = 1, \ldots, m$ que $a_i = a_i g_i(P_i) = 0$. Assim como $\dim_K R_{\mathcal{X},d} = m$ temos que $g_1, \ldots, g_m$ é uma K-base para $R_{\mathcal{X},d}$.
Agora como $d \geq a_{\mathcal{X}} + 1$ e $R_{\mathcal{X},d} = x_0^{d-(a_{\mathcal{X}}+1)} R_{\mathcal{X},a_{\mathcal{X}}+1}$, obtemos K-base $f_1, \ldots, f_m$ para $R_{\mathcal{X},a_{\mathcal{X}}+1}$ onde $g_i = x_0^{d-(a_{\mathcal{X}}+1)} f_i$ para todo $1, \ldots, m$. Além disso,

$$f_i(P_j) = \begin{cases} 1 & , \text{ se } \quad i = j \\ 0 & , \text{ se } \quad i \neq j \end{cases},$$

para todo $i, j = 1, \ldots, m$, pois

$$f_i(P_j) = \underbrace{x_0^{d-(a_{\mathcal{X}}+1)}(P_j)}_{=1} f_i(P_j) = (x_0^{d-(a_{\mathcal{X}}+1)} f_i)(P_j) = g_i(P_j),$$

para todo $i, j = 1, \ldots, m$.

2. Se $g \in R_{\mathcal{X},j}$ para $j \geq a_{\mathcal{X}} + 1$, temos que $g = x_0^{j-(a_{\mathcal{X}}+1)} h$ para algum $h \in R_{\mathcal{X},a_{\mathcal{X}}+1}$. Pelo item anterior temos que existem $a_1, \ldots, a_m \in K$ tais que $h = a_1 f_1 + \ldots + a_m f_m$. Logo

$$g = x_0^{j-(a_{\mathcal{X}}+1)} a_1 f_1 + \ldots + x_0^{j-(a_{\mathcal{X}}+1)} a_m f_m$$

onde $a_i = (x_0^{j-(a_{\mathcal{X}}+1)} a_1 f_1 + \ldots + x_0^{j-(a_{\mathcal{X}}+1)} a_m f_m)(P_i) = g(P_i)$, portanto

$$g = g(P_1) x_0^{j-(a_{\mathcal{X}}+1)} f_1 + \ldots + g(P_m) x_0^{j-(a_{\mathcal{X}}+1)} f_m.$$

■

Seja $f_1, \ldots, f_m$ a K-base para $R_{\mathcal{X},a_{\mathcal{X}}+1}$ da proposição 3.3.16. Com a mesma notação de 3.3.15, sejam $\tilde{\varphi} \in \mathcal{G}$ e $\varphi \in \omega_{\mathcal{X},-a_{\mathcal{X}}}$ tal que $\sigma(\varphi) = \tilde{\varphi}$. Então a aplicação

$$\begin{aligned} \pi : \omega_{\mathcal{X},-a_{\mathcal{X}}} &\longrightarrow K^m \\ \varphi &\longmapsto (\tilde{\varphi}(f_1), \ldots, \tilde{\varphi}(f_m)) \end{aligned}$$

é um K-homomorfismo e sua imagem em K^m define o código $C_{\omega_{\mathcal{X}}}$.

Proposição 3.3.17

$$\dim_K C_{\omega_\mathcal{X}} = m - \dim_K C_\mathcal{X}(a_\mathcal{X}).$$

Demonstração. Vejamos que o homomorfismo π é injetivo. de fato, se $\pi(\varphi) = 0$, temos que $\tilde{\varphi}(f_i) = 0$, para todo $i = 1, \ldots, m$, então $\sigma(\varphi)(f_i) = 0$, para todo $i = 1, \ldots, m$, logo $\varphi_{|R_{\mathcal{X},a_\mathcal{X}+1}}(f_i) = 0$, para todo $i = 1, \ldots, m$, daí que $\varphi_{|R_{\mathcal{X},a_\mathcal{X}+1}} = 0$ pois se anula em uma base de $R_{\mathcal{X},a_\mathcal{X}+1}$, então de 3.3.15(2) temos que $\varphi = 0$. Portanto, π é injetor. Assim, de 3.1.13 temos

$$\begin{aligned}
\dim_K C_{\omega_\mathcal{X}} &= \dim_K \omega_{\mathcal{X},-a_\mathcal{X}} \\
&= H_{\omega_\mathcal{X}}(-a_\mathcal{X}) \\
&= m - H_\mathcal{X}(a_\mathcal{X}) \\
&= m - \dim_K C_\mathcal{X}(a_\mathcal{X}).
\end{aligned}$$

■

Da proposição 3.3.17 temos que $\dim_K C_{\omega_\mathcal{X}} + \dim_K C_\mathcal{X}(a_\mathcal{X}) = m = \dim_K K^m$, logo para que código $C_{\omega_\mathcal{X}}$ seja o dual do código $C_\mathcal{X}(a_\mathcal{X})$, falta mostrar que os elementos de $C_{\omega_\mathcal{X}}$ são ortogonais, segundo o produto interno usual, aos elementos de $C_\mathcal{X}(a_\mathcal{X})$.

Proposição 3.3.18 *O código $C_{\omega_\mathcal{X}}$ é o dual do código $C_\mathcal{X}(a_\mathcal{X})$.*

Demonstração. Sejam

$$ev_{a_\mathcal{X}}(f) = (f(P_1), \ldots, f(P_m)) \in C_\mathcal{X}(a_\mathcal{X}) \text{ e } \pi(\varphi) = (\tilde{\varphi}(f_1), \ldots, \tilde{\varphi}(f_m)) \in C_{\omega_\mathcal{X}}.$$

Como $x_0(P_i) = 1$ para todo $i = 1, \ldots, m$ e olhando para f em $R_{\mathcal{X},a_\mathcal{X}}$ temos que $x_0 f \in R_{\mathcal{X},a_\mathcal{X}+1}$ e de 3.3.16(2) temos que

$$x_0 f = (x_0 f)(P_1) f_1 + \ldots + (x_0 f)(P_m) f_m.$$

Assim, como $\tilde{\varphi} \in \mathcal{G}$ temos que

$$\begin{aligned}
ev_{a_\mathcal{X}}(f) \cdot \pi(\varphi) &= f(P_1)\tilde{\varphi}(f_1) + \ldots + f(P_m)\tilde{\varphi}(f_m) \\
&= x_0(P_1)f(P_1)\tilde{\varphi}(f_1) + \ldots + x_0(P_m)f(P_m)\tilde{\varphi}(f_m) \\
&= \underbrace{(x_0 f)(P_1)}_{\in K}\tilde{\varphi}(f_1) + \ldots + \underbrace{(x_0 f)(P_m)}_{\in K}\tilde{\varphi}(f_m) \\
&= \tilde{\varphi}((x_0 f)(P_1) f_1 + \ldots + (x_0 f)(P_m) f_m) \\
&= \tilde{\varphi}(x_0 f) \\
&= 0.
\end{aligned}$$

■

Observação 3.3.19 *Pela proposição 3.2.5 temos que*

$$H_\mathcal{X}(a_\mathcal{X}) + H_\mathcal{X}(0) = m \Rightarrow H_\mathcal{X}(a_\mathcal{X}) + 1 = m \Rightarrow H_\mathcal{X}(a_\mathcal{X}) = m - 1.$$

e da proposição 3.3.17 temos que

$$\dim_K C_{\omega_\mathcal{X}} = m - \dim_K C_\mathcal{X}(a_\mathcal{X}) = m - H_\mathcal{X}(a_\mathcal{X}) = m - (m-1) = 1.$$

3.4 Parâmetros de um código de avaliação

Na seção anterior, calculamos a dimensão e o comprimento de um código do tipo Reed-Muller em uma interseção completa qualquer. No entanto, não é possível fazer o mesmo para distância mínima, assim sendo, no que se segue calculamos a distância mínima de um código sobre uma interseção completa particular.

A partir de agora trabalharemos com o seguinte conjunto

$$\mathcal{X} = \{[1, t_1^{m_1}, t_2^{m_2}, \ldots, t_n^{m_n}] : t_i \in K^* \text{ para todo } i = 1, \ldots, n\} \subseteq \mathbb{P}^n(K), \tag{3.4}$$

onde $K^* = K\backslash\{0\}$ e m_i é um inteiro positivo para todo $i = 1, \ldots, m$. É importante ressaltar que a ordem em que os números $m_1, \ldots, m_n$ aparecem não é importante pois obteremos códigos equivalentes (ver [9]).

Teorema 3.4.1 *O conjunto $\mathcal{X} \subseteq \mathbb{P}^n(K)$ definido em (3.4) é uma interseção completa, onde*

$$I_{\mathcal{X}} = \langle x_1^{s_1} - x_0^{s_1}, \ldots, x_n^{s_n} - x_0^{s_n} \rangle$$

onde $s_i = \frac{q-1}{\gcd(q-1, m_i)}$ para todo $i = 1, \ldots, n$.

Demonstração. Usaremos a ordem lexicográfica $x_n > x_{n-1} > \ldots > x_0$. Faremos a prova por indução sobre n.
Se $n = 1$, seja $f \in I_{\mathcal{X}}$, onde $\mathcal{X} = \{[1, t^{m_1}] : t \in K^*\} \subseteq \mathbb{P}^1$. Podemos escrever $f(x_0, x_1) = x_0^r \cdot g(x_0, x_1)$ onde $r \geq 0$ e x_0 não divide $g(x_0, x_1)$. Logo, $0 = f(1, t^{m_1}) = g(1, t^{m_1})$, para todo $t \in K^*$. defina $g(1, x_1) \in K[x_1]$, então $g(1, x_1) \in I_U$ onde $U = \{t^{m_1} : t \in K^*\}$ e $|U| = \frac{q-1}{\gcd(q-1, m_1)} = s_1$, temos que existe $p(x_1) \in K[x_1]$ tal que

$$g(1, x_1) = p(x_1) \cdot \prod_{a \in U} (X_1 - a) = p(x_1) \cdot (x_1^{s_1} - 1).$$

Homogeneizando com relação a x_0 temos

$$g(x_0, x_1) = p^h(x_1) \cdot (x_1^{s_1} - x_0^{s_1}),$$

logo

$$f(x_0, x_1) = x_0^r \cdot p^h(x_1) \cdot (x_1^{s_1} - x_0^{s_1}).$$

Portanto, $I(X) = \langle x_1^{s_1} - x_0^{s_1} \rangle$.
Agora suponha que o resultado seja válido para $n - 1$. Seja $f \in I_{\mathcal{X}}$, onde
$\mathcal{X} = \{[1, t_1^{m_1}, t_2^{m_2}, \ldots, t_n^{m_n}] : t_i \in K^* \text{ para todo } i = 1, \ldots, n\} \subseteq \mathbb{P}^n$. Pelo algoritmo da divisão obtemos $q_1, r_1 \in S$ tal que

$$f = (x_n - t^{m_n} x_0) q_1 + r_1, \text{ para } t \in K^*$$

e nenhum dos monômios de r_1 é divisível por x_n. Logo, $r_1 \in K[x_0, \ldots, x_{n-1}]$, além disso, se $P' \in \mathcal{Y} = \{[1, t_1^{m_1}, t_2^{m_2}, \ldots, t_{n-1}^{m_{n-1}}] : t_i \in K^* \text{ para todo } i = 1, \ldots, n-1\} \subseteq \mathbb{P}^{n-1}$, então $P = [P', t_n^{m_n}] \in \mathcal{X}$ e consequentemente

$$0 = f(P) = (t^{m_n} - t^{m_n}) \cdot q_1(P) + r_1(P) = r_1(P) = r_1(P'), \text{ logo, } r_1 \in I_{\mathcal{Y}} \overset{\text{(H.I.)}}{=} \langle x_1^{s_1} - x_0^{s_1}, \ldots, x_{n-1}^{s_{n-1}} - x_0^{s_{n-1}} \rangle.$$

Seja $z \in K^*$, com $z^{m_n} \neq t^{m_n}$, aplicando novamente o algoritmo da divisão obtemos $q_2, r_2 \in S$ tais que

$$q_1 = (x_n - z^{m_n} x_0) q_2 + r_2,$$

da mesma forma, temos que $r_2 \in K[x_0, \ldots, x_{n-1}]$, além disso, tomando $P_1 = [P', z^{m_n}] \in \mathfrak{X}$ temos

$$0 = q_1(P_1) = (z^{m_n} - z^{m_n}) \cdot q_2(P_1) + r_2(P_1) = r_2(P_1) = r_2(P'), \text{ logo, } r_2 \in I_{\mathcal{Y}}.$$

Assim, temos

$$\begin{aligned} f &= (x_n - t^{m_n} x_0) q_1 + r_1 \\ &= (x_n - t^{m_n} x_0)\left[(x_n - z^{m_n} x_0) q_2 + r_2\right] + r_1 \\ &= (x_n - t^{m_n} x_0)(x_n - z^{m_n} x_0) q_2 + \underbrace{(x_n - t^{m_n} x_0) r_2 + r_1}_{\in I_{\mathcal{Y}}}. \end{aligned}$$

Continuando com esse processo obtemos $q \in S$, $r \in I_{\mathcal{Y}}$ e $W = \{t^{m_n} : t \in K^*\}$, com $|W| = \frac{q-1}{\gcd(q-1, m_n)} = s_n$ tais que

$$f = \left[\prod_{a \in W} (x_n - a x_0)\right] \cdot q + r = (x_n^{s_n} - x_0^{s_n}) \cdot q + r$$

como $r \in I_{\mathcal{Y}} \overset{\text{(H.I.)}}{=} \langle x_1^{s_1} - x_0^{s_1}, \ldots, x_{n-1}^{s_{n-1}} - x_0^{s_{n-1}} \rangle$ temos que $f \in \langle x_1^{s_1} - x_0^{s_1}, \ldots, x_n^{s_n} - x_0^{s_n} \rangle$. Portanto, $I_{\mathcal{X}} = \langle x_1^{s_1} - x_0^{s_1}, \ldots, x_n^{s_n} - x_0^{s_n} \rangle$. ■

Assim, de 3.3.7 e 3.3.13 temos a dimensão e o comprimento de código $C_{\mathcal{X}}(d)$ são dados por

$$\dim C_{\mathcal{X}}(d) = \binom{n+d}{d} - \sum_{i=1}^{n} \binom{n+d-s_i}{d-s_i} + \sum_{1 \le i_1 < i_2 \le n} \binom{n+d-(s_{i_1}+s_{i_2})}{d-(s_{i_1}+s_{i_2})} -$$

$$- \sum_{1 \le i_1 < i_2 < i_3 \le n} \binom{n+d-(s_{i_1}+s_{i_2}+s_{i_3})}{d-(s_{i_1}+s_{i_2}+s_{i_3})} + \ldots + (-1)^n \binom{n+d-(s_1+\ldots+s_n)}{d-(s_1+\ldots+s_n)}$$

e

$$|\mathcal{X}| = s_1 \cdot \ldots \cdot s_n = \prod_{i=1}^{n} s_i.$$

De 3.2.5 temos que o índice de regularidade de $R_{\mathcal{X}}$ é

$$a_{\mathcal{X}} + 1 = (s_1 + \ldots + s_n) - (n+1) + 1 = s_1 + \ldots + s_n - n = \sum_{i=1}^{n} (s_i - 1).$$

Vamos considerar a ordem lexicográfica $x_n > x_{n-1} > \ldots > x_0$. Observe que $\{f_1, \ldots, f_n\}$ onde $f_i = x_i^{s_i} - x_0^{s_i}$, para todo $i = 1, \ldots, n$ é uma base de Groebner para $I_{\mathcal{X}}$, pois $\mathrm{lm}(f_i)$ e $\mathrm{lm}(f_j)$ são primos entre si, para todo $i \neq j$. A distância mínima de $C_{\mathcal{X}}(d)$ é dada por

$$\delta_d := \delta(C_{\mathcal{X}}(d)) = \min\{w(ev_d(f) \mid f \in A_d \text{ e } f \notin I_{\mathcal{X},d}\}.$$

Agora trabalharemos para calcular a distância mínima δ_d de $C_{\mathcal{X}}(d)$, para isso considere o conjunto

$$\mathcal{M} = \{M \in A \mid M \text{ é monômio}\}.$$

Definição 3.4.2 *Seja* I *um ideal de* A. *A* **pegada** *do ideal* I *(com respeito a alguma ordem monômial) é o conjunto*

$$\Delta(I) = \{M \in \mathcal{M} \mid M \text{ não é monômio lider de nenhum polinômio de } I\}.$$

Para cada $d \in \mathbb{Z}_{\geq 0}$ considere o conjunto $\Delta(I)_d = \Delta(I) \cap A_d$.

Proposição 3.4.3 *Seja* $I = \bigoplus_{d \geq 0} I_d$ *um ideal homogêneo de* A. *Então,* $B = \{\bar{M} \mid M \in \Delta(I)_d\}$ *é uma base para* S_d/I_d *como um* K*-espaço vetorial.*

Demonstração. Seja $f \in A_d$, isto é, f é homogêneo de grau d. Como I é um ideal homogêneo, existem $g_1, \ldots, g_t \in A$ homogêneos tais que $G = \{g_1, \ldots, g_t\}$ é uma base de Goebner para I. Dividindo f por $\{g_1, \ldots, g_t\}$ obtemos $f_1, \ldots, f_t, r \in S$ tais que $f = f_1 + \ldots + f_t + r$ e r é uma k-combinação linear de monômios de $\Delta(I)_d$. Como $f, r \in I_d$ temos que $f - r \in I_d$, logo $\bar{f} = \bar{r}$. Portanto, $\bar{f}$ é uma k-combinação linear de elementos de B.
Para provar que B é linearmente independente, sejam $\bar{M}_1, \ldots, \bar{M}_s \in B$ e $a_1, \ldots, a_s \in K$ tais que $a_1\bar{M}_1 + \ldots + a_s\bar{M}_s = \bar{0}$. Suponha por absurdo que algum $a_j \neq 0$. Como $r := a_1\bar{M}_1 + \ldots + a_s\bar{M}_s \in I_d$ temos que $\mathrm{lm}(r) \in \mathrm{lm}(I_d) \subseteq \mathrm{lm}(I)$. Logo, $\mathrm{lm}(r) \in \langle \mathrm{lm}(I) \rangle$, ou seja, $\mathrm{lm}(r) \notin \Delta(I)$. Como $\mathrm{lm}(r) = M_i$ para algum $i \in \{1, \ldots, s\}$ temos $M_i \notin \Delta(I)$, logo $M_i \notin \Delta(I)_d$, o que é uma contradição. Portanto, B é linearmente independente. ■

Definição 3.4.4 *Seja* I *um ideal de* A *e seja* $f \in A$. *Definimos o seguinte conjunto*

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

Vamos considerar também $\nabla(I, f)_e = \nabla(I, f) \cap A_e$.

Teorema 3.4.5 *Seja* $d < \sum_{i=1}^{n}(s_i - 1)$ *e seja* $e \geq |\mathcal{X}| - 1$. *Então*

$$\min\{|\nabla(I_{\mathcal{X}}, M)_e| \mid M \in \Delta(I_{\mathcal{X}})_d\} \leq \delta_d \leq w(ev_d(f)),$$

para todo $f \in A_d \backslash I_{\mathcal{X},d}$.

Demonstração. Dado $f \in A_d \backslash I_{\mathcal{X},d}$, é claro que $\delta_d \leq w(ev_d(f))$. Para prova a outra desigualdade, considere

$$\mathcal{X}_f = \{P \in \mathcal{X} \mid f(P) = 0\}$$

observe que

$$w(ev_d(f)) = |\{P \in \mathcal{X} \mid f(P) \neq 0\}| = |\mathcal{X}| - |\mathcal{X}_f|. \tag{3.5}$$

Como $I_{\mathcal{X}_f} \supseteq I_{\mathcal{X}} + \langle f \rangle$, temos

$$\begin{array}{ccc} A_e & \twoheadrightarrow & A_e/I_{\mathcal{X}_f,e} \\ \downarrow & \nearrow & \\ A_e/(I_{\mathcal{X}} + \langle f \rangle)_e & & \end{array}$$

logo,

$$\dim_K A_e/(I_{\mathcal{X}} + \langle f \rangle)_e \geq \dim_K A_e/I_{\mathcal{X}_f,e} \tag{3.6}$$

Dividindo f por $\{f_1, \ldots, f_n\}$ obtemos um resto não nulo que continuaremos a denotar por f. Como $I_{\mathcal{X}} + \langle f \rangle = \langle f_1, \ldots, f_n, f \rangle$, temos que

$$\langle \mathrm{lm}(I_{\mathcal{X}} + \langle f \rangle) \rangle \supset \langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_n), \mathrm{lm}(f) \rangle$$

Por (3.6) temos que

$$\dim_K A_e/I_{\mathcal{X}_f,e} \leq \dim_K A_e/(I_{\mathcal{X}} + \langle f \rangle)_e = |\Delta(I_{\mathcal{X}} + \langle f \rangle))_e| \leq |\Delta(\langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_n), \mathrm{lm}(f) \rangle)_e|.$$

Como

$$\begin{cases} \nabla(I_{\mathcal{X}}, f) \cap \Delta(\langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_n), \mathrm{lm}(f) \rangle) = \emptyset \\ \nabla(I_{\mathcal{X}}, f) \cup \Delta(\langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_n), \mathrm{lm}(f) \rangle) = \Delta(I_{\mathcal{X}}) \end{cases}$$

temos que

$$|\Delta(\langle \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_n), \mathrm{lm}(f)\rangle)_e| = |\Delta(I_{\mathcal{X}})_e| - |\nabla(I_{\mathcal{X}}, f)_e|,$$

logo

$$|\Delta(I_{\mathcal{X}_f})_e| = \dim_K A_e/I_{\mathcal{X}_f,e} \leq |\Delta(I_{\mathcal{X}})_e| - |\nabla(I_{\mathcal{X}}, f)_e|. \tag{3.7}$$

Como $e \geq |\mathcal{X}| - 1 \geq |\mathcal{X}_f| - 1$ temos que $|\mathcal{X}| = |\Delta(I_{\mathcal{X}})_e|$ e $|\mathcal{X}_f| = |\Delta(I_{\mathcal{X}_f})_e|$. Assim

$$w(ev_d(f)) \overset{(3.5)}{=} |\mathcal{X}| - |\mathcal{X}_f| = |\Delta(I_{\mathcal{X}})_e| - |\Delta(I_{\mathcal{X}_f})_e| \overset{(3.7)}{\geq} |\Delta(I_{\mathcal{X}})_e| - (|\Delta(I_{\mathcal{X}})_e| - |\nabla(I_{\mathcal{X}}, f)_e|) = |\nabla(I_{\mathcal{X}}, f)_e|.$$

Portanto,

$$\begin{aligned} \delta_d &= \min\{w(ev_d(f) \mid f \in A_d \text{ e } f \notin I_{\mathcal{X},d}\} \\ &\geq \min\{|\nabla(I_{\mathcal{X}}, f)_e| \mid f \in \Delta(I_{\mathcal{X}})_d\} \\ &= \min\{|\nabla(I_{\mathcal{X}}, M)_e| \mid M \in \Delta(I_{\mathcal{X}})_d\}. \end{aligned}$$

■

vamos trabalhar no sentido de encontrar $\min\{|\nabla(I_{\mathcal{X}}, M)_e| \mid M \in \Delta(I_{\mathcal{X}})_d\}$, para isso usaremos seguinte lema ver [7].

Lema 3.4.6 *Sejam* $0 < d_1 \leq \ldots \leq d_n$ *e* $d \leq \sum_{i=1}^{n}(d_i - 1)$ *inteiros. Seja* $m(\alpha_1, \ldots, \alpha_n) = \prod_{i=1}^{n}(d_i - \alpha_i)$*, onde* $0 \leq \alpha \leq d_i$ *é um inteiro para todo* $i = 1, \ldots, n$*. Então*

$$\min\{m(\alpha_1, \ldots, \alpha_n) : \alpha_1 + \ldots + \alpha_n \leq d\} = (d_{k+1} - l) \prod_{i=k+2}^{n} d_i$$

onde k *e* l *são unicamente determinados por* $s = \sum_{i=1}^{n}(d_i - 1) + l$ *com* $0 \leq l \leq d_{k+1} - 1$*. Se* $k + 1 = n$ *então entenderemos que* $\prod_{i=k+2}^{n} d_i = 1$*, e se* $d < d_1 - 1$ *então temos* $k = 0$ *e* $l = d$*.*

Proposição 3.4.7 *Dado* $e \geq |\mathcal{X}| - 1$ *e* $d < \sum_{i=1}^{n}(s_i - 1)$ *temos que*

$$\min\{|\nabla(I_{\mathcal{X}}, M)_e| \mid M \in \Delta(I_{\mathcal{X}})_d\} = (s_{k+1} - l) \prod_{i=k+2}^{n} s_i$$

onde k *e* l *são unicamente determinados por* $d = \sum_{i=1}^{n}(s_1 - 1) + l$ *com* $0 \leq l \leq s_{k+1} - 1$*. Como anteriormente, se* $k + 1 = n$ *então entenderemos que* $\prod_{i=k+2}^{n} s_i = 1$*, e se* $d < s_1 - 1$ *então temos* $k = 0$ *e* $l = d$*.*

Demonstração. Temos que

$$\Delta(I_{\mathcal{X}})_d = \{M = x_0^{\alpha_0} \cdot \ldots \cdot x_n^{\alpha_n} \mid \alpha_0 + \ldots + \alpha_n = d,\ 0 \leq \alpha_j \leq s_{j-1} \text{ para } 1 \leq j \leq n \text{ e } 0 \leq \alpha_0\}.$$

Para $M = x_0^{\alpha_0} \cdot \ldots \cdot x_n^{\alpha_n} \in \Delta(I_{\mathcal{X}})_d$ temos que

$$\nabla(I_{\mathcal{X}}, M)_e = \{N \in \Delta(I_{\mathcal{X}})_d \mid M \mid N\}.$$

Seja $M = x_0^{\beta_0} \cdot \ldots \cdot x_n^{\beta_n} \in \nabla(I_{\mathcal{X}}, M)_e$, como $N \in \Delta(I_{\mathcal{X}})_d$ temos que $\beta_0 + \ldots + \beta_n = d$, $0 \leq \beta_j \leq s_{j-1}$ para $1 \leq j \leq n$ e $0 \leq \beta_0$, além disso, como $M \mid N$ temos $\alpha_i \leq \beta_i \leq s_{i-1}$ para todo $i = 1, \ldots, n$, então

$$\alpha_0 \leq \beta_0 = e - (\beta_1 + \ldots + \beta_n) \geq e - \sum_{i=1}^{n}(s_i - 1).$$

Assim, tomando $e \geq \sum_{i=1}^{n}(s_i - 1) + \alpha_0$ então β_0 existe para toda escolha de $\beta_1, \ldots, \beta_n$, em particular podemos tomar $\beta_0 = \beta_0$. Portanto

$$|\nabla(I_{\mathcal{X}}, M)_e| = \prod_{i=1}^{n}(s_i - 1 - \alpha_i + 1) = \prod_{i=1}^{n}(s_i - \alpha_i).$$

Então por 3.4.6 temos que

$$\min\{|\nabla(I_{\mathcal{X}}, M)_e| \mid M \in \Delta(I_{\mathcal{X}})_d\} = (s_{k+1} - l) \prod_{i=k+2}^{n} s_i.$$

■

Proposição 3.4.8 *Seja* $d < \sum_{i=1}^{n}(s_i - 1)$. *Se* k *e* l *são os únicos inteiros não negativos tais que* $0 \leq l \leq s_{k+1} - 1$ *e* $d = \sum_{i=1}^{n}(s_1 - 1) + l$, *então existe* $f \in A_d \backslash I_{\mathcal{X},d}$ *tal que*

$$w(ev_d(f)) = (s_{k+1} - l) \prod_{i=k+2}^{n} s_i.$$

Demonstração. Considere os conjuntos $D_i = \{a_{i1}, \ldots, a_{is_i}\}$ para todo $i = 1, \ldots, n$. Para cada $j = 1, \ldots, k$ defina

$$g_i = \prod_{j=1}^{s_i - 1}(x_i - a_{ij}).$$

Observe que g_i tem grau $s_i - 1$ e se anula em D_i. Agora considere

$$g = \left(\prod_{i=1}^{k} g_i\right) \prod_{j=1}^{l}(x_{k+1} - a_{k+1j}).$$

Seja f a homogeneização de g com respeito a x_0, então temos

$$\deg(f) = \deg(g) = \sum_{i=1}^{n}(s_1 - 1) + l = d.$$

Observe que f tem $\prod_{i=1}^{n} s_i - (s_{k+1} - l)\prod_{i=k+2}^{n} s_i$ zeros em $A_1 \times \ldots \times A_n$, logo

$$w(ev_d(f)) = (s_{k+1} - l) \prod_{i=k+2}^{n} s_i.$$

■

Teorema 3.4.9 *Se* $d < \sum_{i=1}^{n}(s_i - 1)$, *então a distância mínima do código* $C_{\mathcal{X}}(d)$ *é*

$$\delta_d = (s_{k+1} - l) \prod_{i=k+2}^{n} s_i,$$

onde k *e* l *são os únicos inteiros não negativos tais que* $0 \leq l \leq s_{k+1} - 1$ *e* $d = \sum_{i=1}^{n}(s_1 - 1) + l$.

Referências Bibliográficas

[1] D. COX, J. LITTLE, e D. O'SHEA *Ideals, Varieties, e Algorithms*, second ed, Springer, Berlim, 1997.

[2] A. HEFEZ, e M.L.T VILLELA, *Códigos Corretores de Erros*, Série de Computação e Matemática, 2002.

[3] D. EISENBUD, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, 1994.

[4] R. H. VILLARREAL, *Monomial Algebras*, Monographs and Textbooks in Pure and Applied Mathematics 238, Marcel Dekker, Inc., New York, 2001.

[5] I. DUURSMA, C. RENTERÍA, H. TAPIA-RECILLAS, *Reed Muller codes on Complete Intersections*, Applicable Algebra in Engineering, Communica-tion and Computing, AAECC, Springer, 11(2001), 455-462.

[6] I. VAINSENCHER, *Introdução às curvas algebricas planas*, Impa, 1979.

[7] C. CARVALHO, *Gröbner bases methods in coding theory*, Publications of CIMPA, Mexico, 2012.

[8] M. G. SARABIA, C. RENTERÍA, A. J. S. HERNÁNDEZ. *Evaluation Codes Over a Particular Complete Intersection*, Int. J. Contemp. Math. Sciences, Vol. 6, 2011, no. 30, 1497-1504.

[9] M. G. SARABIA, C. RENTERÍA, A. J. S. HERNÁNDEZ. *Minimum distance of some evaluation codes*, AAECC, Springer, (2013) 24:95-106.

[10] C. RENTERÍA, H. TAPIA-RECILLAS, *Linear codes associated to the ideal of points in* P^{d} *and its canonical module*. Commun. Algebra 24, 1083-1090 (1996).

[11] A. V. GERAMITA, M. KREUZER,L. ROBBIANO *Cayley-Bacharach Schemes and their Canonical Modules*, Trans. Am. Math. Soc. 339(1), 163-189 (1993).