NICOLÁS FITZGERALD MUÑOZ HERRERA

Máximo número de zeros de uma família de polinômios em um produto cartesiano finito

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2020

NICOLÁS FITZGERALD MUÑOZ HERRERA

Máximo número de zeros de uma família de polinômios em um produto cartesiano finito

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: Álgebra.

Orientador(a): Prof. Dr. Victor Gonzalo Lopez Neumann.

UBERLÂNDIA - MG
2020

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

H565 Herrera, Nicolás Fitzgerald Muñoz, 1996-
2020 Máximo número de zeros de uma família de polinômios em um produto cartesiano finito. [recurso eletrônico] / Nicolás Fitzgerald Muñoz Herrera. - 2020.

Orientador: Victor Gonzalo Lopez Neumann.
Coorientador: Cicero Carvalho.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2020.357
Inclui bibliografia.

1. Matemática. I. Neumann, Victor Gonzalo Lopez,1974-, (Orient.). II. Carvalho, Cicero,1960-, (Coorient.). III. Universidade Federal de Uberlândia. Pós-graduação em Matemática. IV. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:
Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

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(A): Nicolás Fitzgerald Muñoz Herrera.

NÚMERO DE MATRÍCULA: 11812MAT007.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Álgebra.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Máximo número de zeros de uma família de polinômios em um produto cartesiano finito.

ORIENTADOR(A): Prof. Dr. Victor Gonzalo Lopez Neumann.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 20 de fevereiro de 2010, às 10h00min, pela seguinte Banca Examinadora:

NOME	ASSINATURA
Prof. Dr. Victor Gonzalo Lopez Neumann UFU - Universidade Federal de Uberlândia	Victor Neumann
Prof. Dr.Herivelto Martins Borges Filho USP- Universidade de São Paulo campus São Carlos	
Prof. Dr. Cícero Fernandes de Carvalho UFU - Universidade Federal de Uberlândia	

Uberlândia-MG, 20 de fevereiro de 2020.

MUNOZ, N. *Máximo número de zeros de uma família de polinômios em um produto cartesiano finito.* 2020. (33) p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho apresentamos uma cota para o número de zeros de uma família de polinômios em um produto cartesiano finito e adicionalmente mostramos um exemplo que atinge aquela cota transformando aquela cota em um máximo. Estes resultados foram provados usando ferramentas algébricas e combinatórias. Os principais elementos usados para provar este resultado é o Teorema da base de Hilbert, as bases de Groebner, a função de Hilbert, a generalização do teorema de Macaulay e a generalização do teorema de Wei. Este trabalho foi principalmente baseado nos artigos [3] e [2].

Palavras-chave: Zeros de polinômios, Função de Hilbert, Teorema de Macaulay, Teorema de Wei.

MUNOZ, N. *Maximum number of zeros of a polynomial family in a finite cartesian product.* 2020. (# 33) p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work, we present an upper bound for the number of zeros of a family of polynomials in a finite cartesian product and additionally we show an example that takes that upper bound turning that upper bound in a maximum. These results have been proven using algebraic and combinatorial tools. The main elements used to prove this result are the Hilbert's base theorem, the Groebner's bases, the Hilber's function, the generalization of Macaulay's theorem and the generalization of Wei's theorem. This work was mainly based on the articles [3] and [2].

Keywords: Zeros of polynomials, Hilbert's function, Macaulay's theorem, Wei's theorem.

Sumário

Introdução

Encontrar zeros de polinômios tem sido um dos problemas mais estudados na matemática, desde a escola aprendemos como achar raízes de alguns polinômios numa variável, começando no caso linear com as operações básicas, logo no caso quadrático usando alguns casos de fatorizarão ou a conhecida 'formula quadrática"e posteriormente em casos de grau maior vemos que achar as raízes de polinômios pode ser uma tarefa bastante difícil. No caso geral, achar os zeros de polinômios em varias variáveis pode ser estudado desde o ponto de vista algébrico, geométrico, analítico ou computacional, mas em geral não é um problema tao simples. O objetivo deste texto é estudar o número de zeros de uma família de polinômios em um produto cartesiano finito. Mais especificamente nosso objetivo é resolver o seguinte problema:

Sejam $n \in \mathbb{N}$, $k_1, \ldots, k_n$ inteiros, tais que $1 \leq k_1 \leq \cdots \leq k_n$, $\mathbb{F}$ um corpo e $A_1, \ldots, A_n$ subconjuntos finitos não vazios de $\mathbb{F}$, tais que $|A_1| = k_1, \ldots, |A_n| = k_n$. define-se $\mathcal{A} = A_1 \times \cdots \times A_n \subseteq \mathbb{F}^n$.

Seja $S = \mathbb{F}[x_1, \ldots, x_n]$ o anel de polinômios nas variáveis $x_1, \ldots, x_n$ e coeficientes em $\mathbb{F}$. Dado um inteiro $d \geq 1$, denota-se $S_{\leq d}(\mathcal{A})$ o subespaço de S que contem exatamente os polinômios f com $\deg(f) \leq d$ e $\deg_i(f) < k_i$, para todo $i = 1, \ldots, n$. O objetivo deste trabalho é responder a seguinte pregunta:

Pergunta 0.1. *Dados um inteiro $r \leq \dim_{\mathbb{F}}(S_{\leq d}(\mathcal{A}))$ e $f_1, \ldots, f_r$ polinômios linearmente independentes de $S_{\leq d}(\mathcal{A})$, qual é a quantidade máxima de zeros comuns que $f_1, \ldots, f_r$ podem ter em $\mathcal{A}$?*

Para resolver esta pergunta vamos estudar principalmente resultados algébricos e combinatórios segundo o trabalho de Peter Beelen e Mrinmoy Datta em [1], além de referencias adicionais que permitiram ter um entendimento mais detalhado da teoria necessária para estudar este problema. O texto está dividido em três capítulos como segue.

No primeiro capitulo vamos estudar ferramentas algébricas que ajudam no estudo de zeros de polinômios e permitiram traduzir a Pergunta 0.1 num problema combinatório. Aqui vamos estudar alguns conceitos básicos como o algoritmo da divisão em varias variáveis, o Teorema da base de Hilbert, as bases de Groebner e a função de Hilbert. Estes resultados permitem fazer uma conexão entre os zeros de polinômios e pontos no espaço base. Ao final do capitulo apresentamos uma cota para a quantidade de zeros de uma família de polinômios em um produto cartesiano finito que independe da forma explicita dos polinômios e reduz o problema em achar o mínimo cardinal de um conjunto concreto. A maioria da teoria estudada neste capitulo esta baseada nos textos [1], [3] e [4].

No segundo capitulo vamos desenvolver ferramentas combinatórias para achar uma cara explicita do conjunto cujo cardinal atinge o valor mínimo que encontramos no capitulo anterior e assim chegar perto de responder a Pergunta 0.1. Neste capitulo focaremos nossa atenção em provar dois resultados importantes, o Teorema de Macaulay e o Teorema de Weil. Começamos definindo as estruturas onde vamos trabalhar e estudamos algumas propriedades básicas destes conjuntos. Posteriormente apresentamos alguns exemplos e algumas aplicações básicas dos teoremas. Finalmente achamos o conjunto desejado e o relacionamos com o resultado principal

do primeiro capitulo. A maioria da teoria estudada neste capitulo esta baseada nos textos [1], [2] e [5].

No terceiro capitulo relacionamos a cota achada no primeiro capitulo junto com o conjunto explicito cujo cardinal atinge aquela cota para dar resposta à Pergunta 0.1. Começamos este capitulo apresentando uma bijeção que permitira achar de maneira explicita a cara do cardinal procurado e relacionar este valor com a cota achada no primeiro capitulo. Posteriormente relacionamos o conjunto obtido no segundo capitulo com o valor explicito de cardinal procurado e respondemos finalmente a pergunta inicial.

Nicolás Fitzgerald Muñoz Herrera
Uberlândia-MG, 20 de janeiro de 2020.

Capítulo 1

Preliminares

O objetivo desde capitulo é apresentar resultados clássicos de álgebra comutativa e geometria algébrica com o objetivo de estudar e responder a Pergunta 0.1. A maioria destes resultados podem ser achados no livro de Cox, Little e O'Shea [3].

1.1 Teorema da base de Hilbert e bases de Groebner

Nesta seção apresentamos os conceitos preliminares necessários para provar o Teorema da base de Hilbert e desenvolver a teoria de bases de Groebner, como ordens monomiais, o algoritmo da divisão e o Lema de Dickson.

Denotamos por $\mathbb{F}$ um corpo qualquer, $\mathbb{Z}_{\geq 0}$ como o conjunto dos inteiros maiores ou iguais que zero, $\mathbb{Z}_{\geq 0}^n$ como as n-tuplas com coordenadas inteiras maiores ou iguais que zero e dados $i, j \in \mathbb{Z}$, com $i < j$, escrevemos $[i, j] = \{m \in \mathbb{Z} : i \leq m \leq j\}$.

Definição 1.1. *Seja $a \in \mathbb{Z}_{\geq 0}^n$, com $a = (a[1], \ldots, a[n])$, chamamos de monômios nas variáveis $x_1, \ldots, x_n$ (ou simplesmente monômios) aos termos $x^a = x_1^{a[1]} \cdots x_n^{a[n]} \in \mathbb{F}[x_1, \ldots, x_n]$ e consideramos o conjunto de todos os monômios como*

$$\mathcal{M} = \{x^a = x_1^{a[1]} \cdots x_n^{a[n]} \in \mathbb{F}[x_1, \ldots, x_n] : a = (a[1], \ldots, a[n]) \in \mathbb{Z}_{\geq 0}^n\}.$$

Exemplo 1.2. *O conjunto dos monômios depende da quantidade de variáveis que consideramos.*

- *Se $n = 1$, $\mathcal{M} = \{x^a \in \mathbb{F}[x] : a \in \mathbb{Z}_{\geq 0}\}$.*
- *Se $n = 2$, $\mathcal{M} = \{x^{(a,b)} = x^a y^b \in \mathbb{F}[x, y] : a, b \in \mathbb{Z}_{\geq 0}\}$.*
- *Se $n = 3$, $\mathcal{M} = \{x^{(a,b,c)} = x^a y^b z^c \in \mathbb{F}[x, y, z] : a, b, c \in \mathbb{Z}_{\geq 0}\}$.*

Definição 1.3. *Se $>$ é uma relação em $\mathbb{Z}_{\geq 0}^n$ que satisfaz:*

1. *$>$ é uma ordem total em $\mathbb{Z}_{\geq 0}^n$, ou seja, todos os elementos são comparáveis, isto é, para todos $a, b \in \mathbb{Z}_{\geq 0}^n$ tem-se que $a > b$, $a = b$ ou $a < b$.*

2. *$>$ é uma boa ordem em $\mathbb{Z}_{\geq 0}^n$, ou seja, todo subconjunto não vazio de $\mathbb{Z}_{\geq 0}$ tem menor elemento em relação à $>$, isto é, se $S \subseteq \mathbb{Z}_{\geq 0}$ com $S \neq \emptyset$, então existe $a_0 \in S$ tal que $a_0 < a$, para todo $a \in S$ com $a \neq a_0$.*

3. *$>$ respeita a soma em $\mathbb{Z}_{\geq 0}^n$, ou seja, dados $a, b, c \in \mathbb{Z}_{\geq 0}^n$, com $a > b$, temos que $a+c > b+c$.*

Então $>$ é chamada de ordem monomial em $\mathbb{Z}_{\geq 0}^n$.

Sejam $x^a, x^b \in \mathcal{M}$, com $a, b \in \mathbb{Z}_{\geq 0}^n$, escrevemos $x^a \succ x^b$ se $a > b$, $x^a = x^b$ se $a = b$ e $x^a \prec x^b$ se $a < b$. Se $>$ é uma ordem monomial em $\mathbb{Z}_{\geq 0}^n$ dizemos que $\succ$ é ordem monomial em $\mathcal{M}$.

Dado $a \in \mathbb{Z}_{\geq 0}^n$, com $a = (a[1], \ldots, a[n])$, definimos o grau de a como $|a| = a[1] + \cdots + a[n]$ e dizemos que $>$ é uma ordem monomial graduada em $\mathbb{Z}_{\geq 0}^n$ se para todos $a, b \in \mathbb{Z}_{\geq 0}^n$ tais que $|a| > |b|$ segue que $a > b$. Analogamente, dizemos que $\succ$ é uma ordem monomial graduada em $\mathcal{M}$ se $>$ é uma ordem monomial graduada em $\mathbb{Z}_{\geq 0}^n$.

Vamos agora apresentar alguns exemplos de. ordens monomiais verificando que satisfazem a definição anterior, ou equivalentemente que satisfazem o seguinte resultado.

Lema 1.4. *Uma ordem $>$ em $\mathbb{Z}_{\geq 0}^n$ é uma boa ordem se, e somente se, toda sequencia decrescente $(a_n)_{n\in\mathbb{N}} \subseteq \mathbb{Z}_{\geq 0}^n$ $(a_1 > a_2 > \cdots)$ se estabiliza eventualmente.*

Demonstração. Vamos provar por contra-positiva, ou seja, vamos provar que $>$ não é uma boa ordem se, e somente se, existe uma sequencia estritamente decrescente em $\mathbb{Z}_{\geq 0}^n$.

Se $>$ não é uma boa ordem, dado $S \subseteq \mathbb{Z}_{\geq 0}^n$ não tem elemento mínimo, isto é, dado $a_1 \in S$, existe $a_2 \in S$ tal que $a_1 > a_2$. Analogamente, para todo $a_m \in S$ existe $a_{m+1} \in S$ tal que $a_m > a_{m+1}$. Portanto, a sequência $(a_m)_{m\in\mathbb{N}}$ é estritamente decrescente em $\mathbb{Z}_{\geq 0}^n$.

Se existe $S = (a_m)_{m\in\mathbb{N}} \subseteq \mathbb{Z}_{\geq 0}^n$ uma sequência estritamente decrescente, o conjunto S não tem elemento mínimo e portanto $>$ não é uma boa ordem. □

Exemplo 1.5 (Ordem lexicográfica)**.** *Dados $a, b \in \mathbb{Z}_{\geq 0}^n$ com $a = (a[1], \ldots, a[n])$ e $b = (b[1], \ldots, b[n])$, dizemos que $a >_{lex} b$ se para o vetor $a - b \in \mathbb{Z}^n$ a entrada não nula mais à esquerda é positiva. Neste caso, se $a >_{lex} b$ escrevemos $x^a \succ_{lex} x^b$. Vamos provar que $>_{lex}$ é uma ordem monomial em $\mathbb{Z}_{\geq 0}^n$ e portanto $\succ_{lex}$ é uma ordem monomial em $\mathcal{M}$.*

1. *Dados $a, b \in \mathbb{Z}_{\geq 0}^n$ consideramos o vetor $a - b$ e vemos que temos três opções: todas suas entradas são nulas (neste caso $a = b$), sua primeira entrada não nula mais à esquerda é positiva (neste caso $a >_{lex} b$) ou é negativa (neste caso $b >_{lex} a$).*

2. *Suponha que $>_{lex}$ não é uma boa ordem, pelo Lema 1.4, existe uma sequencia $(a_m)_{m\in\mathbb{N}} \subseteq \mathbb{Z}_{\geq 0}^n$ estritamente decrescente $(a_1 >_{lex} a_2 >_{lex} \cdots)$. Tome $(a_m[1])_{m\in\mathbb{N}}$ e veja que é uma sequencia não crescente em $\mathbb{Z}_{\geq 0}$, logo, como $>$ é uma boa ordem em $\mathbb{Z}_{\geq 0}$, existe $N_1 \in \mathbb{N}$ tal que $a_m[1] = a_{m+1}[1]$, para todo $m \geq N_1$. Agora, veja que $(a_m[2])_{m\geq N_1}$ é uma sequencia não crescente em $\mathbb{Z}_{\geq 0}$ e pelo argumento anterior, exite um N_2 tal que $a_m[2] = a_{m+1}[2]$ para todo $m \geq N_2$. Iterativamente, existe $N_n \in \mathbb{Z}_{\geq 0}$ tal que $a_m[1] = a_{m+1}[1], \ldots, a_m[n] = a_{m+1}[n]$ para todo $m \geq N_n$, isto significa que a sequencia $(a_m)_{m\geq N_n}$ é constante. Absurdo, portanto $>_{lex}$ é uma boa ordem.*

3. *Dados $a, b, c \in \mathbb{Z}_{\geq 0}^n$ com $a >_{lex} b$, tem-se que a primeira entrada não nula do vetor $a - b$ é positiva e como $(a + c) - (b + c) = a - b$, segue que a primeira entrada não nula do vetor $(a + c) - (b + c)$ também é positiva, logo $a + c >_{lex} b + c$.*

Observação 1.6. *Dados $a \in \mathbb{Z}_{\geq 0}^n$ e $\sigma \in S_n$ (uma permutação de n elementos), escrevemos $\sigma(a) = (a[\sigma(1)], \ldots, a[\sigma(n)])$. Dados $a, b \in \mathbb{Z}_{\geq 0}^n$ dizemos que $a >_{lex(\sigma)} b$ se $\sigma(a) >_{lex} \sigma(b)$. Podemos verificar que $>_{lex(\sigma)}$ é de fato uma ordem monomial. Isto significa que permutando a ordem das variáveis e usando a ideia da ordem lexicográfica conseguimos $n!$ exemplos de ordens monomiais.*

Exemplo 1.7 (Ordem lexicográfica graduada)**.** *Dados $a, b \in \mathbb{Z}_{\geq 0}^n$, com $a = (a[1], \ldots, a[n])$ e $b = (b[1], \ldots, b[n])$, dizemos que $a >_{grlex} b$ se*

$$|a| > |b| \quad ou \quad |a| = |b| \text{ e } a >_{lex} b.$$

Neste caso, se $a >_{grlex} b$ escrevemos $x^a \succ_{grlex} x^b$. Vamos provar que $>_{grlex}$ é uma ordem monomial graduada em $\mathbb{Z}_{\geq 0}^n$ e portanto $\succ_{grlex}$ é uma ordem monomial graduada em $\mathcal{M}$.

1. *Dados $a, b \in \mathbb{Z}_{\geq 0}^n$ temos duas opções: se $|a| \neq |b|$ então $|a| > |b|$ ($a >_{grlex} b$) ou $|a| < |b|$ ($b >_{grlex} a$), mas se $|a| = |b|$ tem-se outros três casos, $a >_{lex} b$ ($a >_{grlex} b$), $b >_{lex} a$ ($b >_{grlex} a$) ou $a = b$.*

2. *Suponha que $>_{grlex}$ não é uma boa ordem, pelo Lema 1.4, existe uma sequencia $(a_m)_{m\in\mathbb{N}} \subseteq \mathbb{Z}_{\geq 0}^n$ estritamente decrescente ($a_1 >_{grlex} a_2 >_{grlex} \cdots$). Veja que $|a_1| \geq |a_2| \geq \cdots$ em $\mathbb{Z}_{\geq 0}$, mas como $>$ é uma boa ordem em $\mathbb{Z}_{\geq 0}$, existe $n_0 \in \mathbb{Z}_{\geq 0}$ tal que $|a_{m_1}| = |a_{m_2}|$ para todo $m_1, m_2 \geq n_0$. Assim, $a_m >_{lex} a_{m+1}$ para todo $m \geq n_0$, mas como $>_{lex}$ é uma boa ordem em $\mathbb{Z}_{\geq 0}^n$, a sequencia $a_m >_{lex} a_{m+1} >_{lex} \cdots$ estabiliza eventualmente e de esta forma $a_1 >_{grlex} a_2 >_{grlex} \cdots$ estabiliza eventualmente.*

3. *Dados $a, b, c \in \mathbb{Z}_{\geq 0}^n$, com $a >_{grlex} b$, tem-se $|a + c| = \sum_{i=1}^n a[i] + c[i] = \sum_{i=1}^n a[i] + \sum_{i=1}^n c[i] = |a| + |c|$. Agora, se $|a| > |b|$, então $|a + c| = |a| + |c| > |b| + |c| = |b + c|$. Mas, se $|a| = |b|$ e $a >_{lex} b$, segue que $a + c >_{lex} b + c$. Portanto, nos dois casos segue que $a + c >_{grlex} b + c$.*

Exemplo 1.8 (Ordem lexicográfica graduada revertida)**.** *Dados $a, b \in \mathbb{Z}_{\geq 0}^n$, com $a = (a[1], \ldots, a[n])$ e $b = (b[1], \ldots, b[n])$, dizemos que $a >_{grevlex} b$ se*

$$|a| > |b| \quad ou \quad |a| = |b| \text{ e a entrada mais à direita de } a - b \in \mathbb{Z}^n \text{ é negativa.}$$

Neste caso, se $a >_{grevlex} b$ escrevemos $x^a \succ_{grevlex} x^b$. Vamos provar que $>_{grevlex}$ é uma ordem monomial graduada em $\mathbb{Z}_{\geq 0}^n$ e portanto $\succ_{grevlex}$ é uma ordem monomial graduada em $\mathcal{M}$.

1. *Dados $a, b \in \mathbb{Z}_{\geq 0}^n$ temos duas opções: se $|a| \neq |b|$ então $|a| > |b|$ ($a >_{grevlex} b$) ou $|a| < |b|$ ($b >_{grevlex} a$), mas se $|a| = |b|$ tem-se outros três casos, a entrada mais à direita de $a - b \in \mathbb{Z}^n$ é negativa ($a >_{grevlex} b$), positiva ($b >_{grevlex} a$) ou $a = b$.*

2. *Suponha que $>_{grlex}$ não é uma boa ordem, pelo Lema 1.4, existe uma sequencia $(a_m)_{m\in\mathbb{N}} \subseteq \mathbb{Z}_{\geq 0}^n$ estritamente decrescente ($a_1 >_{grlex} a_2 >_{grlex} \cdots$). Veja que $|a_1| \geq |a_2| \geq \cdots$ em $\mathbb{Z}_{\geq 0}$, mas como $>$ é uma boa ordem em $\mathbb{Z}_{\geq 0}$, existe $n_0 \in \mathbb{Z}_{\geq 0}$ tal que $|a_{m_1}| = |a_{m_2}|$ para todo $m_1, m_2 \geq n_0$. Assim, $a_m >_{lex} a_{m+1}$ para todo $m \geq n_0$, mas como $>_{lex}$ é uma boa ordem em $\mathbb{Z}_{\geq 0}^n$, a sequencia $a_m >_{lex} a_{m+1} >_{lex} \cdots$ estabiliza eventualmente e de esta forma $a_1 >_{grlex} a_2 >_{grlex} \cdots$ estabiliza eventualmente.*

3. *Dados $a, b, c \in \mathbb{Z}_{\geq 0}^n$, com $a >_{grevlex} b$, tem-se $|a + c| = \sum_{i=1}^n a[i] + c[i] = \sum_{i=1}^n a[i] + \sum_{i=1}^n c[i] = |a| + |c|$. Agora, se $|a| > |b|$, então $|a + c| = |a| + |c| > |b| + |c| = |b + c|$. Mas, se $|a| = |b|$ e a entrada mais à direita de $a - b \in \mathbb{Z}^n$ é negativa, como $(a+c)-(b+c) = a-b$ então a entrada mais à direita de $(a + c) - (b + c) \in \mathbb{Z}^n$ é negativa. Portanto, nos dois casos segue que $a + c >_{grevlex} b + c$.*

Observação 1.9. *Vejamos que no caso de $n = 1$, ou seja, polinômios numa variável, existe somente uma ordem total em $\mathbb{Z}_{\geq 0}$ e portanto existe somente uma ordem monomial no conjunto de monômios numa variável $\mathcal{M}$, chamada de ordem usual. Esta ordem monomial permite-nos ordenar os monômios dos polinômios de maneira decrescente e nesse caso chamamos ao maior dos exponentes de aqueles monômios de grau do polinômio.*

Dado $f \in \mathbb{F}[x]$ um polinômio, o grau de f é geralmente denotado por grau(f) ou por $\deg(f)$. Podemos ver também o grau como uma aplicação da seguinte forma $\deg : \mathbb{F}[x] \to \mathbb{N}$, tal que se $f(x) \in \mathbb{F}[x]$, com $f(x) = \gamma_r x^r + \gamma_{r-1} x^{r-1} + \cdots + \gamma_0$ e $\gamma_r \neq 0$, então $\deg(f) = r$.

A ideia de estudar ordens monomiais em $\mathbb{Z}_{\geq 0}^n$ é verificar que propriedades da ordem usual em $\mathbb{Z}_{\geq 0}$ seguem sendo satisfeitas em $\mathbb{Z}_{\geq 0}^n$ e nesse caso verificar que propriedades dos polinômios numa variável podem ser estudadas nos polinômios em várias variáveis. Para isso vamos usar o conceito de multigrau, ideia semelhante ao grau de polinômios numa variável.

Definição 1.10. *Dada uma ordem monomial $\succ$ em $\mathcal{M}$ e $f \in \mathbb{F}[x_1, \ldots, x_n]$ um polinômio não nulo da forma $f = \sum_a \gamma_a x^a$, definimos:*

1. *O multigrau de f como multigrau$(f) = \max\{a \in \mathbb{Z}^n_{\geq 0} : \gamma_a \neq 0\}$. O máximo é considerado em relação à ordem monomial $>$ em $\mathbb{Z}^n_{\geq 0}$.*

2. *O grau total de f como $\deg(f) = \sum_{i=1}^n$ multigrau$(f)[i]$, onde multigrau$(f) \in \mathbb{Z}^n_{\geq 0}$ e multigrau$(f) =$ (multigrau$(f)[1], \ldots,$ multigrau$(f)[n]$).*

3. *O coeficiente líder de f como $LC(f) = \gamma_{multigrau(f)} \in \mathbb{F}$.*

4. *O monômio líder de f como $LM(f) = x^{multigrau(f)} \in \mathcal{M}$.*

5. *O termo líder de f como $LT(f) = LC(f)LM(f)$.*

Observe que o multigrau, e consequentemente as outras definições, depende explicitamente da ordem monomial escolhida pois consideramos o máximo em relação à ordem monomial $>$ em $\mathbb{Z}^n_{\geq 0}$.

Exemplo 1.11. *Seja $f(x, y, z) = 2x^3y^5z^2 - 5x^4y^3z^2 \in \mathbb{R}[x, y, z]$.*

- *Em relação à ordem lexicográfica: multigrau$(f) = (4, 3, 2)$, $LC(f) = -5$, $LM(f) = x^4y^3z^2$ e $LT(f) = -5x^4y^3z^2$.*

- *Em relação à ordem lexicográfica graduada: multigrau$(f) = (3, 5, 2)$, $LC(f) = 2$, $LM(f) = x^3y^5z^2$ e $LT(f) = 2x^3y^5z^2$.*

Veja que no caso de uma variável o multigrau coincide com o grau usual dos polinômios. Logo, no caso geral podemos verificar que algumas propriedades do grau usual são satisfeitas pelo multigrau.

Proposição 1.12. *Dados $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ polinômios não nulos, tem-se:*

1. *multigrau$(fg) =$ multigrau$(f) +$ multigrau(g).*

2. *Se $f + g \neq 0$, então multigrau$(f + g) \leq \max\{$multigrau$(f),$ multigrau$(g)\}$. Mais ainda, se multigrau$(f) \neq$ multigrau(g) tem-se a igualdade.*

Demonstração. Se $f = \sum_{a \in A} \gamma_a x^a$ e $g = \sum_{b \in B} \gamma_b x^b$, com $A, B \subseteq \mathbb{Z}^n_{\geq 0}$ finitos, podemos ordenar os elementos de A e B, de maneira decrescente, assim $a_1 > a_2 > \cdots > a_{m_1} \in A$ e $b_1 > b_2 > \cdots > b_{m_2} \in B$. Agora, se $C = \{a + b \in \mathbb{Z}^n_{\geq 0} : a \in A \text{ e } b \in B\}$ vemos que também podemos ordenar os elementos de C e verificar que $a_1 + b_1$ é o seu maior elemento, ou seja que $\text{multigrau}(fg) = a_1 + b_1 = \text{multigrau}(f) + \text{multigrau}(g)$.

Se $f + g \neq 0$ segue que $g \neq -f$, logo temos dois opções para os termos líderes de f e g. Se $\text{LT}(g) \neq -\text{LT}(f)$, segue que $\text{LM}(f + g) = \max\{\text{LM}(f), \text{LM}(g)\}$ e de fato $\text{multigrau}(f + g) = \max\{\text{multigrau}(f), \text{multigrau}(g)\}$. Agora, se $\text{LT}(g) \neq -\text{LT}(f)$, segue que $\text{LM}(f + g) \prec \min\{\text{LM}(f), \text{LM}(g)\}$ e portanto $\text{multigrau}(f + g) = \max\{\text{multigrau}(f), \text{multigrau}(g)\}$.

□

Uma das propriedades mais importantes do grau usual dos polinômios é verificar quando dados dois polinômios $f, g \in \mathbb{F}[x]$ temos que g divide f. Se $\deg(g) \leq \deg(f)$ é possível que exista $h \in \mathbb{F}[x]$ tal que $f = gh$. Mas, se $\deg(g) > \deg(f)$ temos que g não pode dividir f. No caso de varias variáveis o algoritmo da divisão pode ser generalizado usando a mesma ideia que no caso usual.

Teorema 1.13 (Algoritmo da divisão)**.** *Dada uma ordem monomial $>$ em $\mathbb{Z}^n_{\geq 0}$ e $F = (f_1, \ldots, f_s)$ uma $s-$tupla ordenada de polinômios em $\mathbb{F}[x_1, \ldots, x_n]$. Para todo $f \in \mathbb{F}[x_1, \ldots, x_n]$ existem $a_1, \ldots, a_s, r \in \mathbb{F}[x_1, \ldots, x_n]$ tal que*

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

com $r = 0$ ou r um polinômio cujos monômios não são divisíveis pelos termos lideres dos $f_1, \ldots, f_s$. Este r é chamado de ***resto*** *de f na divisão pelo F. Mais ainda, vemos que se $a_i f_i \neq 0$ então*

$$\textit{multigrau}(f) \geq \textit{multigrau}(a_i f_i).$$

Demonstração. Tome $p = f$, $a_1 = \cdots = a_s = r = 0$. Sempre revisaremos dois casos:

Caso 1. Se $\mathrm{LT}(p)$ é divisível por $\mathrm{LT}(f_i)$, modifique $a_i = a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$ e $p = p - \left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}\right) f_i$.

Caso 2. Se $\mathrm{LT}(p)$ não é divisível por $\mathrm{LT}(f_i)$, modifique $r = r + \mathrm{LT}(p)$ e $p = p - \mathrm{LT}(p)$.

Veja que em cada passo se verifica que $f = a_1 f_1 + \cdots + a_s f_s + p + r$. Para el passo inicial, quando $a_1 = \cdots = a_s = r = 0$ e $p = f$ vale a igualdade.

Agora, no *caso 1*, veja que $\left(a_i + \left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}\right)\right) f_i + \left(p - \left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}\right) f_i\right) = a_i f_i + p$ e

$$\begin{aligned} f &= a_1 f_1 + \cdots + \left(a_i + \left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}\right)\right) f_i + \cdots + a_s f_s + \left(p - \left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}\right) f_i\right) + r \\ &= a_1 f_1 + \cdots + a_i f_i + \cdots + a_s f_s + p + r. \end{aligned}$$

Analogamente no *caso 2*, veja que $(p - \mathrm{LT}(p)) + (r + \mathrm{LT}(p)) = p + r$ e

$$\begin{aligned} f &= a_1 f_1 + \cdots + a_i f_i + \cdots + a_s f_s + (p - \mathrm{LT}(p)) + (r + \mathrm{LT}(p)) \\ &= a_1 f_1 + \cdots + a_i f_i + \cdots + a_s f_s + p + r. \end{aligned}$$

Verifique agora que p eventualmente vai para 0 e nesse caso $f = a_1 f_1 + \cdots + a_i f_i + \cdots + a_s f_s + r$. No *caso 1*, como $p = p - \left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}\right) f_i$ então $\mathrm{LT}\left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i\right) = \mathrm{LT}(p)$ e assim o multigrau(p) vai descendo estritamente. Analogamente, no *caso 2*, como $p = p - \mathrm{LT}(p)$ novamente o multigrau(p) vai descendo estritamente. Mas, estamos obtendo uma cadeia decrescente de multigraus em $\mathbb{Z}^n_{\geq 0}$, pela boa ordem a cadeia tem que estabilizar para $p = 0$. □

Observação 1.14. *Note que no algoritmo da divisão usamos uma $s-$tupla ordenada, ou seja, que o algoritmo da divisão depende explicitamente da ordem usada.*

Vimos que a ordem monomial e o conjunto dos monômios são muito uteis para entender os polinômios em varias variáveis. Nosso objetivo agora é usar as propriedades antes descritas para estudar polinômios e ideais em $\mathbb{F}[x_1, \ldots, x_n]$. Para isso vamos focar nossa atenção na seguinte estrutura.

Definição 1.15. *Um ideal $I \subset \mathbb{F}[x_1, \ldots, x_n]$ é um ideal monomial se existe $A \subset \mathbb{Z}^n_{\geq 0}$ tal que*

$$I = \left\{ \sum_{i=1}^{m} h_{a_i} x^{a_i} : a_1, \ldots, a_m \in A \text{ e } h_{a_i} \in k[x_1, \ldots, x_n] \right\}.$$

Nesse caso, escrevemos $I = \langle x^a : a \in A \rangle$.

Proposição 1.16. *Seja $I = \langle x^a : a \in A \rangle$ um ideal monomial. O monômio $x^b \in I$ se, e somente se, $x^b = x^a f$ para algum $a \in A$ e $f \in \mathcal{M}$, um monômio. Mais ainda, dois ideais monomiais são iguais se, e somente se, tem os mesmos monômios.*

Demonstração. Se $x^b \in I$, $x^b = \sum_{i=1}^{s} f_i x^{a_i}$, com $f_i = \sum_{j=1}^{s_i} \gamma_{ij} x^{c_{ij}} \in \mathbb{F}[x_1, \ldots, x_n]$, para todo $i \in [1, s]$. Logo, $x^b = \sum_{i=1}^{s} \left(\sum_{j=1}^{s_i} \gamma_{ij} x^{c_{ij}} \right) x^{a_i} = \sum_{i=1}^{s} \sum_{j=1}^{s_i} \gamma_{ij} x^{c_{ij}+a_i}$.

Agora, como no lado esquerdo aparece x^b no lado direito tem que aparecer x^b, ou seja que existem $0 \leq i_0 \leq s$ e $0 \leq j_0 \leq i_0$ tais que $x^b = x^{a_{i_0}+c_{i_0 j_0}} = x^{a_{i_0}} x^{c_{i_0 j_0}}$.

Por outro lado, se $x^b = x^a f$, para algum $a \in A$ e $f \in \mathbb{F}[x_1, \ldots, x_n]$, então $x^b \in I$. □

Proposição 1.17. *Se I é um ideal monomial e $f \in \mathbb{F}[x_1, \ldots, x_n]$, são equivalentes:*

1. *$f \in I$.*
2. *Todo termo de f está em I.*
3. *f é uma combinação linear sobre $\mathbb{F}$ de monômios em I.*

Demonstração. Veja primeiro que se f é uma combinação linear sobre $\mathbb{F}$ de monômios em I segue que todo termo de f está em I e se todo termo de f está em I então $f \in I$.

Agora, se $f \in I$ podemos escrever $f = \sum_{a \in A} h_a x^a$, com $A \subseteq \mathbb{Z}_{\geq 0}^n$ finito e $x^a \in I$ para todo $a \in A$. Logo, cada $h_a x^a \in I$ para todo $a \in A$, ou seja que cada termo de f está em I.

Por último, se todo termo de f está no ideal I segue que $f \in I$. □

Observe que a proposição anterior dá uma descrição mais detalhada da estrutura dos elementos de um ideal monomial I, agora queremos obter uma descrição mais detalhada da estrutura do ideal monomial I e dos seus geradores. Vamos provar que todo ideal é finitamente gerado. De fato, esta propriedade é bastante útil e é a motivação principal para desenvolver o conceito de bases de Groebner.

Teorema 1.18 (Lema de Dickson)**.** *Um ideal monomial $I = \langle x^a : a \in A \rangle \subset \mathbb{F}[x_1, \ldots, x_n]$ pode ser escrito como $I = \langle x^{a_1}, \cdots, x^{a_s} \rangle$, com $a_1, \ldots, a_s \in A$. Em outras palavras I tem base finita.*

Demonstração. Vamos provar por indução sobre n, a quantidade de variáveis.

Para $n = 1$ e $I = \langle x^a : a \in A \subseteq \mathbb{Z}_{\geq 0} \rangle$, tome $b = \min\{a \in A\}$ e veja que dado $x^a \in I$, $a \in A$ e assim $a = b + c$, com $c \in \mathbb{Z}_{\geq 0}$, ou seja $x^a = x^b x^c$. Em outras palavras $I = \langle x^b \rangle$.

Supondo que o teorema é valido para $n - 1$. Escrevemos os monômios de $\mathbb{F}[x_1, \ldots, x_{n-1}, y]$ como $x_1^{a[1]} \cdots x_{n-1}^{a[n-1]} y^m = x^a y^m$, com $a = (a[1], \ldots, a[n-1]) \in \mathbb{Z}_{\geq 0}^{n-1}$ e $m \in \mathbb{Z}_{\geq 0}$.

Seja $I = \langle x^a y^m : a = (a[1], \ldots, a[n-1]) \in \mathbb{Z}_{\geq 0}^{n-1} \text{ e } m \in \mathbb{Z}_{\geq 0} \rangle \subseteq \mathbb{F}[x_1, \ldots, x_{n-1}, y]$ um ideal monomial. Consideramos o ideal monomial

$$J = \{x^a : x^a y^m \in I \text{ para algum } m \in \mathbb{Z}_{\geq 0}\} \subseteq \mathbb{F}[x_1, \ldots, x_{n-1}].$$

Pela hipótese de indução $J = \langle x^{a_1}, \ldots, x^{a_s} \rangle$, para alguns $a_1, \ldots, a_s \in \mathbb{Z}_{\geq 0}^{n-1}$.

Agora, para cada $i \in [1, s]$, existe $m_i \in \mathbb{Z}_{\geq 0}$ tal que $x^{a_i} y^{m_i} \in I$. Consideramos $m = \max\{m_1, \ldots, m_s\} \in \mathbb{Z}_{\geq 0}$ e $J_k = \langle x^a : a = (a[1], \ldots, a[n-1]) \in \mathbb{Z}_{\geq 0}^{n-1} \text{ e } x^a y^k \in I \rangle$, para cada $k \in [0, m-1]$. Novamente pela hipótese de indução temos que para todo $k \in [0, m-1]$

$$J_k = \langle x^{a_1^{(k)}}, \ldots, x^{a_{n_k}^{(k)}} \rangle,$$

onde $n_0, \ldots, n_{m-1} \in \mathbb{Z}_{\geq 0}$ e $a_1^{(0)}, \ldots, a_{n_0}^{(0)}, \ldots, a_1^{(m-1)}, \ldots, a_{n_{m-1}}^{(m-1)} \in \mathbb{Z}_{\geq 0}^{n-1}$.

Vejamos que $I = \langle x^{a_1} y^m, \ldots, x^{a_s} y^m, x^{a_1^{(0)}}, \ldots, x^{a_{n_0}^{(0)}}, \ldots, x^{a_1^{(m-1)}} y^{m-1}, \ldots, x^{a_{n_{m-1}}^{(m-1)}} y^{m-1} \rangle$.

Seja $x^a y^p \in I$, se $p \geq m$ temos que $x^a y^m$ divide $x^a y^p$ e pela construção de J existe $x^{a_i} \in J$, com $i \in [1, s]$, tal que $x^{a_i} y^m$ divide $x^a y^m$ e portanto divide $x^a y^p$. Agora, se $p \leq m$, $x^a \in J_p$ e existe $x^{a_i^{(p)}} \in J_p$, com $i \in [1, n_p]$, tal que divide x^a, assim $x^{a_i^{(p)}} y^p$ divide $x^a y^p$. Por último, todo ideal monomial é finitamente gerado. □

Em outras palavras, podemos dizer que todo ideal monomial é finitamente gerado. Agora, vamos tentar estender este resultado para ideais quaisquer, para isso usaremos a seguinte definição.

Definição 1.19. *Dado $I \subset \mathbb{F}[x_1, \ldots, x_n]$ um ideal diferente de $\{0\}$. Dizemos que LT(I) é o conjunto de termos lideres de elementos de I, isto é,*

$$LT(I) = \{\lambda x^a : \text{ existe } f \in I \text{ tal que } LT(f) = \lambda x^a\}.$$

Também dizemos que $\langle LT(I)\rangle$ é o ideal gerado pelos elementos de LT(I) e será chamado de ideal de termos líderes de I.

Observação 1.20. *Dado $f \in \mathbb{F}[x_1, \ldots, x_n]$ observe que o termo líder de f e o monômio líder de f diferem por uma constante, logo o ideal gerado pelo termo líder de f coincide com o ideal gerado pelo monômio líder de f. Em consequência, dado um ideal monomial $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ vemos que o ideal gerado pelos termos líderes de elementos de I coincide com o ideal gerado pelos monômios líderes de elementos de I.*

Proposição 1.21. *Se $I \subset \mathbb{F}[x_1, \ldots, x_n]$ é um ideal, então segue que $\langle LT(I)\rangle$ é um ideal monomial e $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle$, para alguns $g_1, \ldots, g_s \in I \setminus \{0\}$.*

Demonstração. Considere o ideal monomial $\mathcal{I} = \langle \mathrm{LM}(g) : g \in I \setminus \{0\}\rangle$ gerado pelos monômios líderes LM(g) de $I \setminus \{0\}$. Como LM(g) e LT(g) diferem por uma constante não nula geram os mesmos ideais $\mathcal{I} = \langle \mathrm{LT}(g) : g \in I \setminus \{0\}\rangle = \langle \mathrm{LT}(I)\rangle$.

Agora, como $\langle \mathrm{LT}(I)\rangle$ é gerado pelos monômios LM(g), com $g \in I \setminus \{0\}$, pelo Teorema 1.18 (Lema de Dickson) $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)\rangle$, para alguns $g_1, \ldots, g_s \in I \setminus \{0\}$. Agora, como $\mathrm{LM}(g_i) = \mathrm{LT}(g_i)$ diferem por uma constante não nula, para todo $i \in [1, s]$, segue que $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$. □

Teorema 1.22 (Teorema da base de Hilbert)**.** *Qualquer ideal $I \subset \mathbb{F}[x_1, \ldots, x_n]$ tem um conjunto gerador finito, isto é,*

$$I = \left\{ \sum_{i=1}^{m} h_{a_i} g_i : g_1, \ldots, g_m \in I \text{ e } h_{a_i} \in k[x_1, \ldots, x_n] \right\}.$$

Nesse caso, escrevemos $I = \langle g_1, \ldots, g_s\rangle$, para alguns $g_1, \ldots, g_s \in I$.

Demonstração. Se $I = \{0\}$, o conjunto gerador é $\{0\}$. Se $I \neq \{0\}$, existe $g \in I \setminus \{0\}$ e assim, vamos construir o conjunto gerador como segue.

Escolhemos uma ordem monomial e usando o algoritmo da divisão achamos os termos líderes e $\langle \mathrm{LT}(I)\rangle$ o ideal de termos líderes de I. Pela Proposição 1.21 existem $g_1, \ldots, g_s \in I \setminus \{0\}$ tais que $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)\rangle$. Vamos provar agora que $I = \langle g_1, \ldots, g_s\rangle$.

Por construção $\langle g_1, \ldots, g_r\rangle \subseteq I$, pois cada $g_i \in I$. Agora, dado $g \in I$ aplicamos o algoritmo da divisão pela tupla $(g_1, \ldots, g_s)$ e escrevemos

$$g = q_1 g_1 + \cdots + q_s g_s + r$$

onde nenhum termo de r é divisível por nenhum $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$. Vamos provar que $r = 0$, para isso escrevemos

$$r = g - q_1 g_1 - \cdots - q_s g_s.$$

Se $r \neq 0$ temos que $\mathrm{LT}(r) \in \langle \mathrm{I}\rangle = \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)\rangle$. Pela Proposição 1.16 LT(r) tem que ser divisível por algum $\mathrm{LT}(g_i)$, contradizendo o fato de r ser o resto da divisão, portanto r tem que ser zero.

Por último, $g = q_1 g_1 + \cdots + q_s g_s \in \langle g_1, \ldots, g_s\rangle$ e $I \subseteq \langle g_1, \ldots, g_s\rangle$ completando a prova. □

Definição 1.23. *Um conjunto $\mathfrak{B} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ linearmente independente sobre o corpo base $\mathbb{F}$ que gera o ideal I é chamado de base de I.*

Definição 1.24. *Dado um ordem monomial, um subconjunto $G = \{g_1, \ldots, g_s\}$ do ideal I é chamado de base de Groebner (ou base estândar) se $\langle LT(g_1), \ldots, LT(g_s)\rangle = \langle LT(I)\rangle$.*

Corolário 1.25. *Dado um ordem monomial, qualquer ideal $I \subset \mathbb{F}[x_1, \ldots, x_n]$ tem base de Groebner. Mais ainda, qualquer base de Groebner para um ideal I é uma base de I.*

Demonstração. Dado um ideal não nulo, o conjunto $G = \{g_1, \ldots, g_s\}$ construído na demostração do Teorema 1.22 (Teorema da base de Hilbert) é base de Groebner por definição. Além disso, se $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle$, o argumento usado no Teorema 1.22 mostra que $I = \langle g_1, \ldots, g_s\rangle$, portanto G é base de I. □

Concluímos esta seção provando que todo ideal de $\mathbb{F}[x_1, \ldots, x_n]$ tem base de Groebner, mas não apresentamos a forma de achar ela. Em geral não é um processo fácil e as vezes fazer na mão poder ser tedioso. O método mais famoso para calcular bases de Groebner é o Algoritmo de Buchberger e para estudar a detalhe pode-se basear em [3].

1.2 Função de Hilbert

Nesta seção apresentamos os conceitos necessários para definir a função de Hilbert junto com algumas propriedades úteis para nosso estudo. Muitos dos resultados aqui apresentados foram tomados de [3] e [4].

Definição 1.26. *Dado V espaço vetorial e W subespaço vetorial de V, dados $v_1, v_2 \in V$ dizemos que $v_1 \sim v_2$ se $v_1 - v_2 \in W$ e escrevemos as classes de equivalência por $V/W = \{\overline{v} : v \in V\}$.*

Proposição 1.27. *Dado V espaço vetorial de dimensão finita e W subespaço de V, W e V/W são espaços vetoriais de dimensão finita e*

$$\dim V = \dim W + \dim V/W.$$

Demonstração. Tome $\{v_1, \ldots, v_m\}$ base de W e estenda a $\{v_1, \ldots, v_m, v_{m+1}, \ldots, v_{m+n}\}$ base de V, vejamos agora que $\{\overline{v_{m+1}}, \ldots, \overline{v_{m+n}}\}$ é base de V/W.

Dado $\overline{v} \in V/W$, existe $v \in V$ com $v = \lambda_1 v_1 + \cdots + \lambda_{m+n} v_{m+n}$, com λ_i no corpo base para todo $i \in [1, m+n]$. Veja que $v \sim (\lambda_{m+1} v_{m+1} \cdots + \lambda_{m+n} v_{m+n})$ pois,

$$v - (\lambda_{m+1} v_{m+1} \cdots + \lambda_{m+n} v_{m+n}) = \lambda_1 v_1 \cdots + \lambda_m v_m \in W.$$

Portanto $\overline{v} = \overline{\lambda_1 v_1 \cdots + \lambda_m v_m} = \lambda_1 \overline{v_1} \cdots + \lambda_m \overline{v_m}$.
Se $\lambda_{m+1}\overline{v_{m+1}} \cdots + \lambda_{m+n}\overline{v_{m+n}} = 0 \in W$, existem $\gamma_1, \ldots, \gamma_n \in W$ tais que

$$\gamma_1 v_1 + \cdots + \gamma_m v_m + \lambda_{m+1} v_{m+1} + \cdots + \lambda_{m+n} v_{m+n} = 0 \in W.$$

Mas como $v_1, \ldots, v_{m+n}$ é base de V então $\gamma_1 = \cdots = \gamma_m = \lambda_{m+1} = \cdots = \lambda_{m+n} = 0$ e portanto $\{\overline{v_{m+1}}, \ldots, \overline{v_{m+n}}\}$ é base de V/W. □

Definição 1.28. *Sejam $d \in \mathbb{N}$ e $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ ideal, definimos $\mathbb{F}[x_1, \ldots, x_n]_{\leq d}$ como o conjunto de polinômios de grau menor o igual que d juntamente com o polinômio nulo e $I_{\leq d} = I \cap \mathbb{F}[x_1, \ldots, x_n]_{\leq d}$. Observe que $\mathbb{F}[x_1, \ldots, x_n]_{\leq d}$ e $I_{\leq d}$ são espaços vetoriais sobre $\mathbb{F}$.*

Definimos a função de Hilbert de I como segue:

$$\begin{aligned} HF_I :&\mathbb{N} \longrightarrow \mathbb{N} \\ &d \longmapsto HF_I(d) = \dim(\mathbb{F}[x_1, \ldots, x_n]_{\leq d}) - \dim(I_{\leq d}). \end{aligned}$$

Dado $X \subseteq \mathbb{F}^n$, definimos a função de Hilbert de X como $HF_X(d) = HF_{I(X)}(d)$, para todo $d \in \mathbb{N}$.

Neste caso vamos estudar a função de Hilbert no caso afim, porem, a função de Hilbert pode ser definida também no caso projetivo considerando os polinômios homogêneos de grau d. Este caso pode ser estudado mais detalhadamente no capitulo 9 de [3].

Observação 1.29. *Se $I, J \subseteq \mathbb{F}[x_1, \ldots, x_n]$ são ideais tais que $I \subseteq J$, então $HF_I(d) \geq HF_J(d)$, para todo $d \in \mathbb{N}$.*

Lembrando que dados $X, Y \subseteq \mathbb{F}^n$ com $X \subseteq Y$ temos que $I(X) \supseteq I(Y)$, para todo $d \in \mathbb{N}$ segue que $(I(X))_{\leq d} \supseteq (I(Y))_{\leq d}$. Portanto, $HF_X(d) \leq HF_Y(d)$, para todo $d \in \mathbb{N}$.

Proposição 1.30. *Seja $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ um ideal e seja $\succ$ uma ordem monomial graduada em $\mathcal{M}$, então o ideal monomial $\langle LT(I)\rangle$ tem a mesma função de Hilbert que I, ou seja, para todo $d \in \mathbb{N}$ temos que $HF_{\langle LT(I)\rangle}(d) = HF_I(d)$.*

Demonstração. Fixado $d \in \mathbb{N}$, tome os monômios lideres de todos os elementos de $I_{\leq d} \subseteq \mathbb{F}[x_1, \ldots, x_n]_{\leq d}$, que são uma quantidade finita, digamos $\mathrm{LM}(I_{\leq d}) = \{\mathrm{LM}(f) : f \in I_{\leq d}\} = \{\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_m)\}$, reordenando e tirando os elementos repetidos obtemos $\mathrm{LM}(f_1) \succ \cdots \succ \mathrm{LM}(f_m)$. Provemos agora que $\{f_1, \ldots, f_m\}$ é base de $I_{\leq d}$.

Por contra-positiva, dados $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$ não todos nulos, tomamos $j = \min\{i \in [1, m] : \lambda_i \neq 0\}$. O termo $\lambda_j \mathrm{LM}(f_j)$ é o maior monômio da combinação lineal $\lambda_1 f_1 + \cdots + \lambda_m f_m$ e portanto não é cancelado por nenhum outro monômio. Assim $\lambda_1 f_1 + \cdots + \lambda_m f_m \neq 0$.

Considere $W = \langle f_1 \ldots, f_m\rangle \subseteq I_{\leq d}$. Se $W \neq I_{\leq d}$, então existe $f \in I_{\leq d} \setminus W$, podemos escolher f de tal forma que $\mathrm{LM}(f)$ seja minimal. Por definição temos que $\mathrm{LM}(f) \in \mathrm{LM}(I_{\leq d})$, logo $\mathrm{LM}(f) = \lambda \mathrm{LM}(f_i)$, para algum $i \in [1, m]$ e $\lambda \in \mathbb{F}^*$. Assim, $f - \lambda f_i \neq 0$, $f - \lambda f_i \in I_{\leq d} \setminus W$ e $\mathrm{LM}(f) \succ \mathrm{LM}(f - \lambda f_i)$ o que contradiz a minimalidade de $\mathrm{LT}(f)$. Por último, $f \in W$, $W = I_{\leq d}$ e $\{f_1, \ldots, f_m\}$ é base de $I_{\leq d}$.

Provamos também que $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_m)\rangle$.

Pelo argumento anterior, $\mathrm{LM}(f_1) \succ \cdots \succ \mathrm{LM}(f_m)$ são linearmente independentes, pela Proposição 1.16 basta provar que $\{\mathrm{LM}(f_1), \cdots, \mathrm{LM}(f_m)\} = \{\mathrm{LM}(f) : f \in I \text{ e grau total}(\mathrm{LM}(f)) \leq d\}$. Nesse caso, $\langle \mathrm{LT}(I)\rangle_{\leq d} = \langle \mathrm{LM}(f_1), \cdots, \mathrm{LM}(f_m)\rangle$.

Como $\succ$ é uma ordem graduada, para toda $f \in \mathbb{F}[x_1, \ldots, x_n]$, $\mathrm{LM}(f)$ tem o mesmo grau total de f, em particular, como $I_{\leq d}$ é finitamente gerado pelos f_i com grau total menor que d, então o grau total de f também é menor que d.

Logo, $I_{\leq d}$ e $\langle \mathrm{LT}(I)\rangle_{\leq d}$ têm a mesma base e portanto a mesma dimensão, assim,

$$\begin{aligned} HF_I(d) &= \dim(\mathbb{F}[x_1, \ldots, x_n]_{\leq d}/I_{\leq d}), \\ &= \dim(\mathbb{F}[x_1, \ldots, x_n]_{\leq d}) - \dim(I_{\leq d}), \\ &= \dim(\mathbb{F}[x_1, \ldots, x_n]_{\leq d}) - \dim(\langle \mathrm{LT}(I)\rangle_{\leq d}), \\ &= \dim(\mathbb{F}[x_1, \ldots, x_n]_{\leq d}/\langle \mathrm{LT}(I)\rangle_{\leq d}), \\ &= HF_{\langle \mathrm{LT}(I)\rangle}(d). \end{aligned}$$

Por último, para todo $d \in \mathbb{N}$ temos que $HF_I(d) = HF_{\langle \mathrm{LT}(I)\rangle}(d)$ e portanto $\langle LT(I)\rangle$ tem a mesma função de Hilbert que I. □

O anterior resultado nos permite estudar a função de Hilbert de qualquer ideal tomando somente o ideal gerado pelos termos líderes, esta ideia facilita as contas e o uso da função de Hilbert.

Proposição 1.31. *Se $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ é um ideal monomial e $d \in \mathbb{N}$, então $HF_I(d)$ é o número de monômios de grau menor ou igual que d fora de I.*

Demonstração. Observe primeiro que $\mathfrak{B} = \{x^a : |a| \leq d\}$ é base de $\mathbb{F}[x_1, \ldots, x_n]_{\leq d}$ e $\mathfrak{B}_1 = \{x^a : |a| \leq d, x^a \in I\}$ é base de $I_{\leq d}$. Assim, se $\mathfrak{B}_2 = \{x^a : |a| \leq d, x^a \notin I\}$ segue que $\mathfrak{B}_1 \cap \mathfrak{B}_2 = \emptyset$ e $\mathfrak{B} = \mathfrak{B}_1 \sqcup \mathfrak{B}_2$ é base de $\mathbb{F}[x_1, \ldots, x_n]_{\leq d}$.

Por último, $\mathfrak{B}_2' = \{[x^a] : |a| \leq d, x^a \notin I\}$ é base do espaço quociente $\mathbb{F}[x_1, \ldots, x_n]_{\leq d}/I_{\leq d}$ e

$$|\mathfrak{B}_2'| = |\mathfrak{B}_2| = \dim(\mathbb{F}[x_1, \ldots, x_n]_{\leq d}/I_{\leq d}) = HF_I(d).$$

□

Corolário 1.32. *Se $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ é um ideal monomial e $d \in \mathbb{N}$, então $HF_I(d)$ é o número de monômios de grau menor ou igual que d que não são divisíveis por nenhum dos geradores de I.*

Demonstração. Pela Proposição 1.31 $HF_I(d)$ é o número de monômios de grau menor ou igual que d fora de I e pela Proposição 1.16 um monômio está em I se, e somente se, é divisível por um dos geradores. Por último, $HF_I(d)$ é o número de monômios de grau menor ou igual que d que não são divisíveis por nenhum dos geradores de I. □

Agora, vimos estreita relação que tem a função de Hilbert de um ideal com a quantidade de monômios fora de ele. Por outra parte, vamos estudar a relação da função de Hilbert com a descrição de conjuntos finitos de $\mathbb{F}^n$.

Lema 1.33. *Se $\gamma_1, \ldots, \gamma_r \in \mathbb{F}^n$ são pontos distintos, então existem $f_1, \ldots, f_r \in \mathbb{F}[x_1, \ldots, x_n]$ tais que $f_i(\gamma_i) = f_i(\gamma_i[1], \ldots, \gamma_i[n]) = 1$ e $f_i(\gamma_j) = f_i(\gamma_j[1], \ldots, \gamma_j[n]) = 0$, para todo $i, j \in [1, r]$, com $i \neq j$.*

Demonstração. Se $\gamma_i = (\gamma_i[1], \ldots, \gamma_i[n])$, para todo $i \in [1, r]$, como todos os pontos são distintos, para $i \geq 2$, existe $j \in [1, n]$ tal que $\gamma_1[j] \neq \gamma_i[j]$. Considere

$$h_i(x_1, \ldots, x_n) = \frac{x_j - \gamma_i[j]}{\gamma_1[j] - \gamma_i[j]}.$$

Assim, $h_i(\gamma_1) = h_i(\gamma_1[1], \ldots, \gamma_1[n]) = 1$ e $h_i(\gamma_i) = h_i(\gamma_i[1], \ldots, \gamma_i[n]) = 0$, para todo $i \in [2, n]$. Por último, tomamos

$$f_1(x_1, \ldots, x_n) = \prod_{i=2}^{r} h_i(x_1, \ldots, x_n).$$

Note que $f_1(\gamma_1) = 1$ e $f_1(\gamma_i) = 0$, para todo $i \in [2, n]$, obtendo o f_1 do lema. Analogamente, construímos $f_2, \ldots, f_r$. □

Lema 1.34. *Seja $X \subseteq \mathbb{F}^n$ finito, então para d suficientemente grande temos que $|X| \leq HF_X(d)$.*

Demonstração. Seja $X = \{\gamma_1, \ldots, \gamma_r\} \subseteq \mathbb{F}^n$, pelo Lema 1.33 existem $f_1, \ldots, f_r \in \mathbb{F}[x_1, \ldots, x_n]$, tais que $f_i(\gamma_i) = 1$ e $f_i(\gamma_j) = 0$, para todo $i, j \in [1, r]$, com $i \neq j$.

Observe que $f_1, \ldots, f_r \notin I(X)$, pois para cada $i \in [1, r]$ temos que, por construção, f_i não anula ao elemento γ_i. Por outra parte, existe $d \in \mathbb{N}$ tal que $\deg(f_i) \geq d$, para todo $i \in [1, r]$, ou seja que $f_1, \ldots, f_r \in \mathbb{F}[x_1, \ldots, x_n]_{\leq d}/I(X)_{\leq d}$

Vamos provar que $f_1, \ldots, f_r$ são linearmente independentes em $\mathbb{F}[x_1, \ldots, x_n]_{\leq d}/I(X)_{\leq d}$.

Suponha que existem constantes $\lambda_1, \ldots, \lambda_r \in \mathbb{F}$, não todas nulas, tais que

$$\lambda_1(f_1 + I(X)) + \cdots + \lambda_r(f_r + I(X)) = (0 + I(X)).$$

Ou equivalentemente $\lambda_1 f_1 + \cdots + \lambda_r f_r \in I(X)$. Agora, para cada $i \in [1, r]$ temos que avaliando em γ_i segue que $0 = \lambda_1 f_1(\gamma_i) + \cdots + \lambda_r f_r(\gamma_i) = \lambda_i f_i(\gamma_i) = \lambda_i$, logo $\lambda_i = 0$, para todo $i \in [1, r]$. Ou seja, que $(f_1 + I(X)), \ldots, (f_r + I(X))$ são linearmente independentes em $\mathbb{F}[x_1, \ldots, x_n]_{\leq d}/I(X)_{\leq d}$. Por último, para d suficientemente grande temos que

$$|X| = r = \dim(\langle (f_1 + I(X)), \ldots, (f_r + I(X)) \rangle) \leq \dim(\mathbb{F}[x_1, \ldots, x_n]_{\leq d}/I(X)_{\leq d}) = HF_X(d).$$

□

Observação 1.35. *Veja que na demonstração do Lema 1.33 temos que* $\deg(f_i) = r$*, para todo* $i \in [1, r]$*. Logo o* $d \in \mathbb{N}$ *achado na demonstração do Lema 1.34 é* $d = r$ *e vemos explicitamente um* d *para o qual funciona o resultado.*

1.3 Zeros de polinômios e função de Hilbert

O objetivo desta seção é aplicar os resultados anteriormente estudados para apresentar uma relação da função de Hilbert com os zeros de uma família de polinômios em varias variáveis em um produto cartesiano finito. Lembrando sempre que o objetivo do trabalho completo é responder a Pergunta 0.1.

Começamos primeiro definindo o nosso objeto de estudo desta seção.

Definição 1.36. *Dada* $\mathcal{F} = \{f_\alpha\}_{\alpha \in \Lambda} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ *uma família de polinômios, definimos o conjunto de zeros de* $\mathcal{F}$ *como*

$$Z(\mathcal{F}) = \{(x_1, \ldots, x_n) \in \mathbb{F}^n : f_\alpha(x_1, \ldots, x_n) = 0 \text{ para todo } \alpha \in \Lambda\}.$$

Em particular, se $\mathcal{F} = \{f_1, \ldots, f_r\}$ *escrevemos* $Z(\mathcal{F}) = Z(f_1, \ldots, f_r)$*.*

Como no enunciado da Pergunta 0.1, consideramos $A_1, \ldots, A_n \subseteq \mathbb{F}$ subconjuntos finitos de $\mathbb{F}$ com cardinalidades $k_1, \ldots, k_n$ respectivamente, $\mathcal{A} = A_1 \times \cdots \times A_n$, $S = \mathbb{F}[x_1, \ldots, x_n]$ e dado $d \in \mathbb{N}$ escrevemos $S_{\leq d}(\mathcal{A}) = \{f \in S : \deg(f) \leq d \text{ e } f \in I(\mathcal{A})\}$.

Dados $r \leq \dim(S_{\leq d}(\mathcal{A}))$ e $f_1, \ldots, f_r \in S_{\leq d}(\mathcal{A})$ linearmente independentes, nosso objetivo é achar o máximo valor possível de $|Z(f_1, \ldots, f_r) \cap \mathcal{A}|$.

Vamos primeiro estudar o ideal gerado pelos termos líderes de $I(Z(f_1, \ldots, f_r) \cap \mathcal{A})$, como vimos antes o fato de ser um ideal monomial ajuda na hora de fazer contas.

Lema 1.37. *Dados* $r \leq \dim(S_{\leq d}(\mathcal{A}))$ *e* $f_1, \ldots, f_r \in S_{\leq d}(\mathcal{A})$ *linearmente independentes, segue que*

$$\langle LT(f_1), \ldots, LT(f_r), x_1^{k_1}, \ldots, x_n^{k_n} \rangle \subseteq \langle LT(I(Z(f_1, \ldots, f_r) \cap \mathcal{A})) \rangle.$$

Demonstração. Suponha que cada $A_i = \{\gamma_1^{(i)}, \ldots, \gamma_{k_i}^{(i)}\}$, para todo $i \in [1, n]$. Vamos reescrever $\mathcal{A} = A_1 \times \cdots \times A_n$ como $\mathcal{A} = \{(\gamma_{j_1}^{(1)}, \ldots, \gamma_{j_n}^{(n)}) : i \in [1, n] \text{ e } j_i \in [1, k_i]\}$.

Observe que para todo $i \in [1, n]$ temos que o seguinte polinômio está em $I(\mathcal{A})$,

$$g_i = g_i(x_1, \ldots, x_n) = \prod_{j=1}^{k_i} (x_i - \gamma_j^{(i)}) \in I(\mathcal{A}).$$

Assim, $x_i^{k_i} = \mathrm{LT}(g_i) \in \mathrm{LT}(I(\mathcal{A}))$, para todo $i \in [1, n]$. Além disso, como $Z(f_1, \ldots, f_r) \cap \mathcal{A} \subseteq \mathcal{A}$, temos que $I(\mathcal{A}) \subseteq I(Z(f_1, \ldots, f_r) \cap \mathcal{A})$ e portanto

$$\langle x_1^{k_1}, \ldots, x_n^{k_n} \rangle \subseteq \langle \mathrm{LT}(I(\mathcal{A})) \rangle \subseteq \langle \mathrm{LT}(I(Z(f_1, \ldots, f_r) \cap \mathcal{A})) \rangle.$$

Analogamente, como $f_1, \ldots, f_r \in I(Z(f_1, \ldots, f_r) \cap \mathcal{A})$ segue que

$$\langle LT(f_1), \ldots, LT(f_r) \rangle \subseteq \langle \mathrm{LT}(I(Z(f_1, \ldots, f_r) \cap \mathcal{A})) \rangle.$$

Por último,

$$\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_r), x_1^{k_1}, \ldots, x_n^{k_n} \rangle \subseteq \langle \mathrm{LT}(I(Z(f_1, \ldots, f_r) \cap \mathcal{A})) \rangle.$$

□

Proposição 1.38. *Dados $r \leq \dim(S_{\leq d}(\mathcal{A}))$ e $f_1, \ldots, f_r \in S_{\leq d}(\mathcal{A})$ linearmente independentes, segue que para $d \in \mathbb{N}$ suficientemente grande*

$$|Z(f_1, \ldots, f_r) \cap \mathcal{A}| \leq HF_{\mathcal{J}}(d) \leq HF_{\mathcal{I}}(d),$$

onde $\mathcal{I} = \langle LT(f_1), \ldots, LT(f_r), x_1^{k_1}, \ldots, x_n^{k_n} \rangle$ e $\mathcal{J} = \langle LT(I(Z(f_1, \ldots, f_r) \cap \mathcal{A})) \rangle$.

Demonstração. Primeiro, como $Z(f_1, \ldots, f_r) \cap \mathcal{A} \subseteq \mathcal{A}$ segue que $|Z(f_1, \ldots, f_r) \cap \mathcal{A}| \leq |\mathcal{A}|$, ou seja que $Z(f_1, \ldots, f_r) \cap \mathcal{A}$ é um conjunto finito. Portanto, pelas Proposições 1.34 e 1.30 temos que para $d \in \mathbb{N}$ suficientemente grande

$$|Z(f_1, \ldots, f_r) \cap \mathcal{A}| \leq HF_{I(Z(f_1, \ldots, f_r) \cap \mathcal{A})}(d) = HF_{\langle \mathrm{LT}(I(Z(f_1, \ldots, f_r) \cap \mathcal{A})) \rangle}(d).$$

Agora, pelo Lema 1.37

$$\mathcal{I} = \langle LT(f_1), \ldots, LT(f_r), x_1^{k_1}, \ldots, x_n^{k_n} \rangle \subseteq \langle LT(I(Z(f_1, \ldots, f_r) \cap \mathcal{A})) \rangle = \mathcal{J}.$$

Pela Observação 1.29, para todo $d \in \mathbb{N}$ temos que $HF_{\mathcal{J}}(d) \leq HF_{\mathcal{I}}(d)$. Finalmente, para $d \in \mathbb{N}$ suficientemente grande, segue que

$$|Z(f_1, \ldots, f_r) \cap \mathcal{A}| \leq HF_{\mathcal{J}}(d) \leq HF_{\mathcal{I}}(d).$$

□

Agora, para achar uma cota para a quantidade de zeros de $f_1, \ldots, f_r \in \mathbb{F}[x_1, \ldots, x_n]$ no conjunto $\mathcal{A}$ vamos usar o Corolário 1.32 e contaremos a quantidade de monômios de grau menor ou igual que d fora de $\mathcal{I}$, para todo $d \in \mathbb{N}$. Assim, traduzimos um problema de achar zeros de polinômios em contar monômios fora de um ideal monomial.

Sejam $\mathcal{M}$ conjunto dos monômios de $\mathbb{F}[x_1, \ldots, x_n]$ e φ a seguinte aplicação

$$\begin{aligned} \varphi : \mathcal{M} &\longrightarrow \mathbb{Z}_{\geq 0}^n \\ x^a = x_1^{a[1]} \cdots x_n^{a[n]} &\longmapsto (a[1], \ldots, a[n]) = a. \end{aligned}$$

Note que φ é uma bijeção e portanto $|\varphi(\mathcal{M} \setminus \mathcal{I})| = |\mathcal{M} \setminus \mathcal{I}|$ é a quantidade de monômios fora de $\mathcal{I}$. Agora, como $\mathcal{I} = \langle LT(f_1), \ldots, LT(f_r), x_1^{k_1}, \ldots, x_n^{k_n} \rangle$, consideramos $\mathcal{I}_1 = \langle x_1^{k_1}, \ldots, x_n^{k_n} \rangle$ e $\mathcal{I}_2 = \langle LT(f_1), \ldots, LT(f_r) \rangle$ para escrever $\mathcal{I} = \mathcal{I}_1 + \mathcal{I}_2$.

Agora o problema de achar zeros de polinômios pode ser estudado desde o ponto de vista de contar pontos num reticulado. Portanto podemos usar algumas ferramentas combinatórias para fazer esta contagem.

Dado $x^a = x_1^{a[1]} \cdots x_n^{a[n]} \in \mathcal{M}$, pela Proposição 1.16 tem-se que $x^a \in \mathcal{I}_1$ se, e somente se, $a[i] \geq k_i$ para algum $i \in [1, n]$. Equivalentemente, se $\mathcal{M}_1 = \mathcal{M} \setminus \mathcal{I}_1$ é o conjunto dos monômios que estão fora de $\mathcal{I}_1$, temos que $x^a \in \mathcal{M}_1$ se, e somente se, $a[i] < k_i$ para todo $i \in [1, n]$.

Por outra parte, se $F = \{a = (a[1], \ldots, a[n]) \in \mathbb{Z}_{\geq 0}^n : a[i] \in [0, k_i - 1] \text{ para todo } i \in [1, n]\}$ podemos escrever $\mathcal{M}_1 = \{x^a \in \mathcal{M} : a \in F\}$ e verificar que a seguinte restrição é uma bijeção:

$$\begin{aligned} \varphi_1 = \varphi|_{\mathcal{M}_1} : \mathcal{M}_1 &\longrightarrow F \\ x^a = x_1^{a[1]} \cdots x_n^{a[n]} &\longmapsto (a[1], \ldots, a[n]) = a. \end{aligned}$$

Logo, como $\mathcal{M} \setminus \mathcal{I} = \mathcal{M}_1 \setminus \mathcal{I}_2$ podemos usar a bijeção φ_1 para achar $|\mathcal{M} \setminus \mathcal{I}|$, o número de monômios fora de $\mathcal{I}$, calculando $|\varphi_1(\mathcal{M}_1 \setminus \mathcal{I}_2)|$. Para isso estudaremos o conjunto $\varphi(\mathcal{M}_1 \setminus \mathcal{I}_2)$ como subconjunto de F.

Observe que podemos reescrever $F = [0, k_1 - 1] \times \cdots \times [0, k_n - 1]$ e como em $\mathbb{Z}_{\geq 0}^n$ escrevemos o grau de $a \in F$, com $a = (a[1], \ldots, a[n])$, como $|a| = a[1] + \cdots + a[n]$. Assim, dado $d \in [0, k]$ podemos considerar os seguintes conjuntos $F_d = \{a \in F : |a| = d\}$, $F_{\leq d} = \{a \in F : |a| \leq d\}$ e $F_{\geq d} = \{a \in F : |a| \geq d\}$.

Definição 1.39. *Dados $a, b \in F$, com $a = (a[1], \ldots, a[n])$ e $b = (b[1], \ldots, b[n])$, definimos a ordem parcial em F como $a \leq_P b$ se, e somente se, $a[i] \leq b[i]$ para todo $i \in [1, n]$.*

Dado $S \subseteq F$, definimos a sombra de S como sendo o conjunto

$$\nabla(S) = \{a \in F : b \leq_P a \text{ para todo } b \in S\}.$$

Além disso, se $S = \{a_1, \ldots, a_r\}$ escrevemos $\nabla(a_1, \ldots, a_r) = \nabla(S)$.

Proposição 1.40. *Dados $r \leq \dim(S_{\leq d}(\mathcal{A}))$ e $f_1, \ldots, f_r \in S_{\leq d}(\mathcal{A})$ linearmente independentes, segue que*

$$|Z(f_1, \ldots, f_r) \cap \mathcal{A}| \leq |F \setminus \varphi(LT(f_1), \ldots, LT(f_r))|.$$

Demonstração. Primeiro, dados $x^a, x^b \in \mathcal{M}_1$ veja que $x^a | x^b$ se, e somente se, $\varphi(x^a) \leq_P \varphi(x^b)$. Agora, pela Proposição 1.16 vemos que dado $x^a \in \mathcal{M}_1$, $x^a \in \mathcal{I}_2$ se, e somente se, $\mathrm{LT}(f_i) | x^a$ para algum $i \in [1, r]$. Portanto, $x^a \in \mathcal{I}_2$ se, e somente se, $\varphi(\mathrm{LT}(f_i)) \leq \varphi(x^a)$ para algum $i \in [1, r]$.

Por outra parte, pela Proposição 1.31 para $d \geq k$ segue que

$$HF_{\mathcal{I}}(d) = |F \setminus \nabla(\varphi(\mathrm{LT}(f_1)), \ldots, \varphi(\mathrm{LT}(f_r)))|,$$

onde $\nabla(\varphi(\mathrm{LT}(f_1)), \ldots, \varphi(\mathrm{LT}(f_r)))$ é a sombra do conjunto $\{\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_r)\}$.

Por último, substituindo o anterior resultado na desigualdade da Proposição 1.38 temos que

$$|Z(f_1, \ldots, f_r) \cap \mathcal{A}| \leq |F \setminus \varphi(\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_r))|.$$

□

Corolário 1.41. *Dados $r \leq \dim(S_{\leq d}(\mathcal{A}))$ e $f_1, \ldots, f_r \in S_{\leq d}(\mathcal{A})$ linearmente independentes, segue que*

$$|Z(f_1, \ldots, f_r) \cap \mathcal{A}| \leq \max\{|F \setminus \nabla(a_1, \ldots, a_r)| : a_1, \ldots, a_r \in F_{\leq d}\}.$$

Observação 1.42. *O problema de achar o número máximo de zeros de r polinômios linearmente independentes em $S_{\leq d}(\mathcal{A})$ pode ser traduzido no problema combinatório de achar o máximo valor do conjunto*

$$\{|F \setminus \nabla(a_1, \ldots, a_r)| : a_1, \ldots, a_r \in F_{\leq d}\}.$$

Ou equivalentemente, achar o valor mínimo do conjunto

$$\{|\nabla(a_1, \ldots, a_r)| : a_1, \ldots, a_r \in F_{\leq d}\}.$$

Este último será o objetivo do seguinte capitulo.

Capítulo 2

Teorema de Macaulay e Teorema de Wei

O objetivo deste capitulo é desenvolver a teoria necessária para provar o Teorema de Macaulay e o Teorema de Wei, resultados combinatórios que permitem achar explicitamente o conjunto cujo cardinal atinge o $\min\{|\nabla(a_1,\ldots,a_r)| : a_1,\ldots,a_r \in F_{\leq d}\}$.

Pela Observação 1.42 vimos que achar aquele mínimo equivale achar uma cota superior para a quantidade de zeros de uma família de polinômios em um produto cartesiano finito. Estos resultados buscam sempre responder a Pergunta 0.1.

2.1 Generalização Combinatória do Teorema de Macaulay

Nesta secção vamos apresentar e estudar os conceitos e as ferramentas necessárias para provar a Generalização Combinatória do Teorema de Macaulay desenvolvida por Clements e Lindström em [2]. Resultado fundamental para posteriormente provar a Generalização Combinatória do Teorema de Wei.

Definição 2.1. *Sejam $v \in [0,k]$ e $H \subseteq F$, escrevemos $H_v = H \cap F_v$ e definimos $L(H_v)$ como o conjunto dos $|H_v|$ maiores elementos de F_v, em relação à ordem lexicográfica, e $C(H_v)$ como o conjunto dos $|H_v|$ menores elementos de F_v, em relação à ordem lexicográfica. Neste caso, $C(H_v)$ é chamado de compressão de H_v. Em geral, dado $H \subseteq F$, definimos*

$$C(H) = \bigcup_{v=0}^{k} C(H_v).$$

Se $a = (a[1],\ldots,a[n]) \in F$, para cada $i \in [1,n]$ definimos $\Gamma_i(a)$ e $P_i(a)$ como segue

$$\Gamma_i(a) = (a[1],\ldots,a[i-1],a[i]-1,a[i+1],\ldots,a[n]) \text{ e}$$
$$P_i(a) = (a[1],\ldots,a[i-1],a[i]+1,a[i+1],\ldots,a[n]).$$

Além dos conjuntos $\Gamma(a) = \{\Gamma_1(a),\ldots,\Gamma_n(a)\}\cap F$ e $P(a) = \{P_1(a),\ldots,P_n(a)\}\cap F$. De maneira geral, se $H \subseteq F$, definimos

$$\Gamma(H) = \bigcup_{a\in H} \Gamma(a) \qquad\qquad P(H) = \bigcup_{a\in H} P(a).$$

Com estas definições podemos enunciar o resultado principal desta seção, chamado de generalização do teorema combinatório de Macaulay, estudada e desenvolvida por Clements e Lidnström em [2].

Teorema 2.2. *Dado $H \subseteq F$, se $H_v \subseteq= H \cap F_v$, então $\Gamma(C(H_v)) \subseteq C(\Gamma(H_v))$, para todo $v \in [1,k]$.*

Uma forma simples de entender este resultado pode ser vista no seguinte exemplo.

Exemplo 2.3. *Sejam $k_1 = k_2 = k_3 = k_4 = 10$ e $F = \{(a_1,a_2,a_3,a_4) : a_1,a_2,a_3,a_4 \in [0,10]\}$. Para $H_7 = \{(0,0,0,7),(0,0,1,6),(2,0,0,5),(3,0,0,4),(4,0,0,3),(4,0,1,2)\} \subseteq F_7$, temos que:*

$$C(H_7) = \{(0,0,0,7),(0,0,1,6),(0,0,2,5),(0,0,3,4),(0,0,4,3),(0,0,5,2)\},$$
$$\Gamma(C(H_7)) = \{(0,0,0,6),(0,0,1,5),(0,0,2,4),(0,0,3,3),(0,0,4,2),(0,0,5,1)\}.$$

Por outro lado,

$$\Gamma(H_7) = \{(0,0,0,6),(0,0,1,5),(1,0,0,5),(2,0,0,4),(3,0,0,3),(4,0,0,2),(3,0,1,2),(4,0,1,1)\},$$
$$C(\Gamma(H_7)) = \{(0,0,0,6),(0,0,1,5),(0,0,2,4),(0,0,3,3),(0,0,4,2),(0,0,5,1),(0,0,6,0),(0,1,0,5)\}.$$

Claramente, $\Gamma(C(H_7)) \subseteq C(\Gamma(H_7))$.

Para provar o teorema vamos provar primeiro algumas propriedades dos conjuntos do tipo $H_v = H \cap F_v$, para $v \in [1,k]$, e veremos alguns exemplos interessantes.

Definição 2.4. *Sejam $H \subseteq F$, $i \in [1,n]$ e $d \in [0,k]$, definimos*

$$F_{i:d} := \{(a[1],\ldots,a[n]) \in F : a[i] = d\} \text{ e } H_{i:d} := F_{i:d} \cap H.$$

Se $H_v = H \cap F_v$, definimos $(C(H_v))_{i:d}$ como o conjunto dos $|(H_v)_{i:d}|$ menores elementos de $(F_v)_{i:d}$. Dizemos que H_v está $i-$comprimido se $(C(H_v))_{i:d} = (H_v)_{i:d}$ para todo $d \in [0,k_i]$.

Exemplo 2.5. *Considere $H_7 = \{(0,0,0,7),(0,0,1,6),(2,0,0,5),(3,0,0,4),(4,0,0,3),(4,0,1,2)\}$ como no Exemplo 2.3. Vejamos que:*

$$(C(H_7))_{1:0} = \{(0,0,0,7),(0,0,1,6)\},$$
$$(C(H_7))_{1:1} = \emptyset,$$
$$(C(H_7))_{1:2} = \{(2,0,0,5)\},$$
$$(C(H_7))_{1:3} = \{(3,0,0,4)\},$$
$$(C(H_7))_{1:4} = \{(4,0,0,3),(4,0,1,2)\}.$$

Portanto, H_7 está $1-$ comprimido, mas não está $i-$comprimido para $i = 2,3,4$.

Observação 2.6. *Veja que $(C(H_v))_{i:d}$ denota o conjunto dos menores $|(H_v)_{i:d}|$ elementos de $(F_v)_{i:d}$. Mas, $C((H_v)_{i:d})$ denota o conjunto dos menores $|(H_v)_{i:d}|$ elementos de F_v, sem fixar as $i-$ésima coordenada igual a d.*

Definição 2.7. *Dado $H_v \subseteq F_v$ definimos a sequência de subconjuntos $H_v^1, H_v^2, \ldots, H_v^j, \ldots$ como $H_v^1 = H_v$ e $H_v^{j+1} = \bigcup_{d=0}^{k_i} (C(H_v^j))_{i:d}$, onde $i \equiv j (mod\ n)$ e $i \in [1,n]$.*

Observação 2.8. *Dado $H_v \subseteq F_v$, provemos que $|H_v^{j+1}| = |H_v|$, para todo $j \in \mathbb{N}$.*

Se $j = 1$, $H_v^2 = H_v^{1+1} = \bigcup_{d=0}^{k_1} (C(H_v))_{1:d}$, onde $(C(H_v))_{1:d_1} \cap (C(H_v))_{1:d_2} = \emptyset$, para todos $d_1, d_2 \in [0,k_1]$ e $d_1 \neq d_2$. Logo, $|H_v^2| = \sum_{d=0}^{k_1} |(C(H_v))_{1:d}| = \sum_{d=0}^{k_1} |(H_v)_{1:d}| = |H_v|$.

Suponhamos a igualdade válida para $j-1$, ou seja, que $|H_v^j| = |H_v|$.

Seja $H_v^{j+1} = \bigcup_{d=0}^{k_i} (C(H_v^j))_{i:d}$ como na Definição 2.7. Como $(C(H_v^j))_{i:d_1} \cap (C(H_v^j))_{i:d_2} = \emptyset$, para $d_1, d_2 \in [0, k_i]$ e $d_1 \neq d_2$. Logo, $|H_v^{j+1}| = \sum_{d=0}^{k_i} |(C(H_v^j))_{i:d}| = \sum_{d=0}^{k_i} |(H_v^j)_{i:d}| = |H_v^j| = |H_v|$.

A igualdade segue por indução.

Lema 2.9. *Existe $p \in \mathbb{N}$, tal que H_v^p está $i-$comprimido, para todo $i \in [1, n]$.*

Demonstração. Enumeramos os elementos de F_v em relação à ordem lexicográfica, se $a \in F_v$, $n(a)$ denota a posição de a em F_v em relação à ordem lexicográfica, por exemplo para o menor elemento $a \in F_v$, temos que $n(a) = 1$. Além disso, para $H_v \subseteq F_v$, $n(H_v)$ denota a soma das posições dos elementos de H_v, isto é, $n(H_v) = \sum_{a \in H_v} n(a)$.

Por outro lado, dado $j \in \mathbb{N}$ e $i \in [1, n]$, com $i \equiv j (\text{mod } n)$, vemos que $H_v^j = \bigcup_{d=0}^{k_i} (H_v^j)_{i:d}$ é uma união disjunta e como $(C(H_v))_{i:d}$ denota os $|(H_v)_{i:d}|$ menores elementos de $(F_v)_{i:d}$ temos que $n((C(H_v))_{i:d}) \leq n((H_v)_{i:d})$. Portanto,

$$n(H_v^j) = n\left(\bigcup_{d=0}^{k_i} (H_v^j)_{i:d}\right) = \sum_{d=0}^{k_i} n((H_v^j)_{i:d}) \geq \sum_{d=0}^{k_i} n((C(H_v^j)_{i:d})) = n(H_v^{j+1}).$$

Agora, para $i \in [1, n]$ e $d \in [0, k_i]$ temos que $n((C(H_v))_{i:d}) = n((H_v)_{i:d})$ se, e somente se, $(C(H_v))_{i:d} = (H_v)_{i:d}$. Assim, $n(H_v^j) = n(H_v^{j+1})$ se, e somente se, $H_v^j = H_v^{j+1}$.

Pelo principio da boa ordem, a sequência $\{n(H_v^j)\}_{j \in \mathbb{N}} \subseteq \mathbb{N}$ não pode ser infinitamente decrescente, ou seja, existe $p \in \mathbb{N}$ tal que $H_v^p = H_v^{p+m}$, para todo $m \in \mathbb{N}$. Isto prova que H_v^p está $i-$comprimido, para todo $i \in [1, n]$. □

Exemplo 2.10. *Seja $H_7 = \{(0,0,0,7), (0,0,1,6), (2,0,0,5), (3,0,0,4), (4,0,0,3), (4,0,1,2)\}$ como no Exemplo 2.3.*

Por definição, $H_7^1 = H_7$. Agora, para achar H_7^2 vemos que

$$H_7^2 = H_7^{1+1} = \bigcup_{d=0}^{10} (C(H_7^1))_{1:d} = \bigcup_{d=0}^{10} (C(H_7))_{1:d} = \bigcup_{d=0}^{10} (H_7)_{1:d} = \bigcup_{d=0}^{10} (H_7^1)_{1:d} = H_7^1 = H_7,$$

pois H_7 está $1-$comprimido.

Para achar H_7^3 lembramos que $H_7^3 = H_7^{2+1} = \bigcup_{d=0}^{10} (C(H_7^2))_{2:d} = \bigcup_{d=0}^{10} (C(H_7))_{2:d}$.

Se $d = 0$ temos que $|(H_7)_{2:0}| = 6$, logo $(C(H_7))_{2:0} = \{(0,0,0,7), (0,0,1,6), (0,0,2,5), (0,0,3,4), (0,0,4,3), (0,0,5,1)\}$. Mas, se $d \in [1, 10]$ temos que $|(H_7)_{2:d}| = 0$, então $(C(H_7))_{2:d} = \emptyset$, para $d \in [1, 10]$. Assim,

$$H_7^3 = \bigcup_{d=0}^{10} (C(H_7))_{2:d} = \{(0,0,0,7), (0,0,1,6), (0,0,2,5), (0,0,3,4), (0,0,4,3), (0,0,5,2)\}.$$

Para achar $H_7^4 = H_7^{3+1} = \bigcup_{d=0}^{10} (C(H_7^3))_{3:d}$ olhamos as terceiras componentes de cada vetor:

$$(C(H_7^2))_{3:0} = \{(0,0,0,7)\}, \quad (C(H_7^2))_{3:1} = \{(0,0,1,6)\}, \quad (C(H_7^2))_{3:2} = \{(0,0,2,5)\},$$
$$(C(H_7^2))_{3:3} = \{(0,0,3,4)\}, \quad (C(H_7^2))_{3:4} = \{(0,0,4,3)\}, \quad (C(H_7^2))_{3:5} = \{(0,0,5,2)\},$$
$$(C(H_7^2))_{3:6} = (C(H_7^2))_{3:7} = \emptyset.$$

Portanto,

$$H_7^4 = \bigcup_{d=0}^{10}(C(H_7^3))_{3:d} = \{(0,0,0,7),(0,0,1,6),(0,0,2,5),(0,0,3,4),(0,0,4,3),(0,0,5,2)\} = H_7^3.$$

Por último, $H_7^p = H_7^3$ *para todo* $p \geq 3$.

Lema 2.11. *Suponha que o Teorema 2.2 é verdade em* $n-1$ *dimensões. Seja* $v \in [1,k]$ *e* $H \subseteq F$ *tal que* $\Gamma(H_v) \subseteq H_{v-1}$ *(em n dimensões), então* $\Gamma(H_v^j) \subseteq H_{v-1}^j$*, para todo* $j \geq 1$.

Demonstração. A prova vai ser por indução. Se $j = 1$, temos que $\Gamma(H_v^1) = \Gamma(H_v) \subseteq H_{v-1} = H_{v-1}^1$.

Suponhamos o caso de j vamos provar para $j+1$.

Provemos primeiro que $\Gamma((H_v^j)_{i:d}) \cap (F_{v-1})_{i:d} \subseteq (H_{v-1}^j)_{i:d}$. Seja $a \in \Gamma((H_v^j)_{i:d}) \cap (F_{v-1})_{i:d}$, com $a = (a[1],\ldots,a[n])$, isto é, $a[i] = d$, $|a| = v-1$ e existe $b \in (H_v^j)_{i:d}$, tal que $a \in \Gamma(b) \subseteq \Gamma(H_v^j)$, com $b = (b[1],\ldots,b[n])$ e $b[i] = d$. Assim, como $a \in \Gamma(H_v^j) \subseteq H_{v-1}^j$ e $a[i] = d$, segue que $a \in (H_{v-1}^j)_{i:d}$.

Agora, considere $(H_v^j)_{i:d} \subseteq (F_v)_{i:d}$. A compressão de $(H_v)_{i:d}$ fixando a coordenada i igual a d é $(C(H_v^j))_{i:d}$, pois são os $|(H_v^j)_{i:d}|$ elementos de F_v com a coordenada i fixa i igual a d. Logo, a sombra de $(C(H_v^j))_{i:d}$ fixando a coordenada i igual a d é $\Gamma((C(H_v^j))_{i:d}) \cap (F_{v-1})_{i:d}$.

Por outro lado, a sombra de H_v^j fixando a coordenada i igual a d é $\Gamma(H_v^j) \cap (F_{v-1})_{i:d} = (\Gamma(H_v^j))_{i:d}$. Logo, a compressão deste conjunto fixando a coordenada i igual d é $(C(\Gamma(H_v^j)))_{i:d}$.

Pelo teorema em $n-1$ dimensões temos que $\Gamma((C(H_v^j))_{i:d}) \cap (F_{v-1})_{i:d} = \Gamma(C((H_v^j)_{i:d})) \subseteq C(\Gamma((H_v^j)_{i:d}))$. Além disso, como $\Gamma(H_v^j) \subseteq H_{v-1}^j$, então $(\Gamma(H_v^j))_{i:d} \subseteq (H_{v-1}^j)_{i:d}$ e fixando a coordenada i igual a d temos que $(C(\Gamma(H_v^j)))_{i:d} \subseteq (C(H_{v-1}^j))_{i:d}$. Portanto,

$$\Gamma((C(H_v^j))_{i:d}) \cap (F_{v-1})_{i:d} \subseteq (C(H_{v-1}^j))_{i:d}. \tag{2.1}$$

Provemos agora que $|(H_v^j)_{i:d}| \leq |(H_{v-1}^j)_{i:d-1}|$, para $d \geq 1$. Seja $d \geq 1$, como $\Gamma(H_v^j) \subseteq H_{v-1}^j$, provemos que $\Gamma_i((H_v^j)_{i:d}) \subseteq (H_{v-1}^j)_{i:d}$. Dado $a \in (H_v^j)_{i:d}$, com $a = (a_1,\ldots,a_{i-1},d,a_{i+1},\ldots,a_n)$, segue que $\Gamma_i(a) = (a_1,\ldots,a_{i-1},d-1,a_{i+1},\ldots,a_n) \in \Gamma(H_v^j) \subseteq H_{v-1}^j$ com a coordenada i igual a $d-1$, logo $\Gamma_i(a) \in (H_{v-1}^j)_{i:d-1}$. Assim, como a função Γ_i é injetiva no conjunto $(H_v^j)_{i:d}$, por cardinalidades obtemos $|(H_v^j)_{i:d}| = |\Gamma_i((H_v^j)_{i:d})| \leq |(H_{v-1}^j)_{i:d-1}|$.

Seja $d \geq 1$, observe que $(C(H_v^j))_{i:d}$ é o conjunto dos $|(H_v^j)_{i:d}|$ menores elementos de $(F_v)_{i:d}$ e $\Gamma_i((C(H_v^j))_{i:d})$ é o conjunto dos $|(H_v^j)_{i:d}|$ menores elementos de $(F_{v-1})_{i:d-1}$. Agora, $(C(H_{v-1}^j))_{i:d}$ é o conjunto dos $|(H_{v-1}^j)_{i:d}|$ menores elementos de $(F_{v-1})_{i:d-1}$, e como $|(H_v^j)_{i:d}| \leq |(H_{v-1}^j)_{i:d-1}|$, para $d \geq 1$, temos que

$$\Gamma((C(H_v^j))_{i:d}) \cap (F_{v-1})_{i:d-1} = \Gamma_i((C(H_v^j))_{i:d}) \subseteq C(H_{v-1}^j))_{i:d-1}. \tag{2.2}$$

Portanto, para $d \geq 1$ juntamos 2.1 e 2.2 obtendo

$$\begin{aligned}\Gamma((C(H_v^j))_{i:d}) &= (\Gamma((C(H_v^j))_{i:d}) \cap (F_{v-1})_{i:d-1}) \cup (\Gamma((C(H_v^j))_{i:d}) \cap (F_{v-1})_{i:d}),\\ &\subseteq (C(H_{v-1}^j))_{i:d-1}) \cup (C(H_{v-1}^j))_{i:d}).\end{aligned}$$

No caso $d = 0$, aplicamos o teorema em $n-1$ dimensões e temos

$$\Gamma((C(H_v^j))_{i:0}) \subseteq (C(\Gamma(H_v^j)))_{i:0} \subseteq (C(H_{v-1}^j))_{i:0}.$$

Por último,

$$\begin{aligned}\Gamma(H_v^{j+1}) &= \Gamma\left(\bigcup_{d=0}^{k_i}(C(H_v^j))_{i:d}\right),\\ &= \bigcup_{d=0}^{k_i}\Gamma((C(H_v^j))_{i:d}),\\ &\subseteq (C(H_{v-1}^j))_{i:0} \cup \bigcup_{d=1}^{k_i}\left((C(H_{v-1}^j))_{i:d-1} \cup (C(H_{v-1}^j))_{i:d}\right),\\ &= \bigcup_{d=0}^{k_i}\left((C(H_{v-1}^j))_{i:d}\right) = H_{v-1}^{j+1}.\end{aligned}$$

O que prova o lema.

□

Definição 2.12. *Seja $H_v \subseteq F_v$, dizemos que H_v está comprimido se $C(H_v) = H_v$.*

Lema 2.13. *Se H_v está comprimido, então $\Gamma(H_v)$ também está comprimido.*

Demonstração. Sejam $a, b \in F_{v-1}$, com $a = (a[1], \ldots, a[n]), b = (b[1], \ldots, b[n])$ e $a <_{lex} b$. Suponha que H_v está comprimido, vamos provar que se para todo $j \in [1, n]$, temos que $P_j(b) \in H_v$, então $a \in \Gamma(H_v)$, isto é, que $\Gamma(H_v)$ está comprimido.

Seja $j \in [1, n]$, defina $i = \min\{t \in [1, n] : a[t] < b[t]\}$, isto é, $a[1] = b[1], \ldots a[i-1] = b[i-1]$ e $a[i] < b[i]$, pois $a <_{lex} b$. Se $j \leq i$ temos que $P_j(a) < P_j(b) \in H_v$, logo $P_j(a) \in H_v$, pois H_v está comprimido. Portanto $a \in \Gamma(H_v)$.

Vejamos agora o caso quando $j > i$.

Suponha que existe $s \in [i+1, n]$ tal que $a[s] < k_s$, assim $P_s(a) \in F_v$. Como $i < s$, então $P_s(a) = (a[1], \ldots, a[i], \ldots, a[s]+1, \ldots, a[n]) < (b[1], \ldots, b[i], \ldots, b[j]+1, \ldots, b[n]) = P_j(b)$, pois $a[i] < b[i]$. Assim, como $P_j(b) \in H_v$ e H_v está comprimido, então $P_s(a) \in H_v$ e como antes $a \in \Gamma(H_v)$.

Suponha agora que $a[s] = k_s$ para todo $s \in [i+1, n]$. Se $a[i] + 1 < b[i]$, então $P_i(a) < P_j(b) \in H_v$ e de novo, como H_v está comprimido, então $P_i(a) \in H_v$ e assim, $a \in \Gamma(H_v)$.

O único caso que falta é quando $a[1] = b[1], \ldots, a[i-1] = b[i-1]$, $a[i]+1 = b[i]$ e $a[s] = k_s$, para todo $s \in [i+1, n]$.

Como $P_j(b) \in H_v$, então $b[j] + 1 \leq k_j$. Por outro lado, como $a, b \in F_{v-1}$ temos que $|a| = |b| = v - 1$ e como $a[1] = b[1], \ldots, a[i-1] = b[i-1], a[i]+1 = b[i]$ e $a[s] = k_s$, para todo $s \in [i+1, n]$, segue que $k_{i+1} + \cdots + k_n = 1 + b[i+1] + \cdots + b[n]$.

Agora, como $b[i+1] \leq k_{i+1}, \ldots, b[n] \leq k_n$ e $b[j] \leq k_j - 1$, então $1 + b[i+1] + \cdots + b[n] \leq 1 + k_{i+1} + \cdots + (k_j - 1) + \cdots + k_n$. Isso implica, $b[i+1] = k_{i+1}, \ldots, b[n] = k_n$ e $b[j] = k_j - 1$. Logo, temos que

$$\begin{aligned}P_j(b) &= (b[1], \ldots, b[i-1], b[i], \ldots, b[j]+1, \ldots, b[n]),\\ &= (a[1], \ldots, a[i-1], a[i]+1, \ldots, (k_j-1)+1, \ldots, k_n),\\ &= (a[1], \ldots, a[i-1], a[i]+1, \ldots, k_j, \ldots, k_n) = P_i(a) \in H_v,\end{aligned}$$

e nesse caso segue que $a \in \Gamma(H_v)$. Portanto, $\Gamma(H_v)$ está comprimido. □

Observação 2.14. *Considere a seguinte aplicação*

$$\begin{aligned}\phi : F &\longrightarrow F\\ (a[1], \ldots, a[n]) &\longmapsto (k_1 - a[1], \ldots, k_n - a[n]).\end{aligned}$$

Observe que dados $a, b \in F$, com $a = (a[1], \ldots, a[n]), b = (b[1], \ldots, b[n])$. Se $\phi(a) = \phi(b)$, segue que $(k_1 - a[1], \ldots, k_n - a[n]) = (k_1 - b[1], \ldots, k_n - b[n])$, ou seja, $a[1] = b[1], \ldots, a[n] = b[n]$. Logo, $a = b$ e portanto ϕ é injetiva. Por outro lado, se tomamos $a' = \phi(a) = (k_1 - a[1], \ldots, k_n - a[n])$, temos que $\phi(a') = (k_1 - (k_1 - a[1]), \ldots, k_n - (k_n - a[n])) = (a[1], \ldots, a[n]) = a$, ou seja, $(\phi \circ \phi)(a) = a$, para todo $a \in F$. Portanto, ϕ é bijetora e ela é sua própria inversa, $\phi \circ \phi = id_F$.

Observe também que $\phi(F_v) = F_{k-v}$ e que ϕ é uma aplicação que inverte a ordem, isto é, dados $a, b \in F$ e $a' = \phi(a), b' = \phi(b) \in F$, segue que $a <_{lex} b$ se, e somente se, $b' <_{lex} a'$. De fato, $\min\{t \in [1, n] : a[t] < b[t]\} = \min\{t \in [1, n] : k_t - b[t] < k_t - a[t]\}$.

Por último, dado $S \subseteq F$, definimos $S' = \phi(S)$. Neste caso $b \in S$ se, e somente se, $b' = \phi(b) \in S'$. Sejam $a, b \in F_v$, com $a = (a[1], \ldots, a[n]), b = (b[1], \ldots, b[n])$, $a < b$ e $i = \min\{t \in [1, n] : a[t] < b[t]\}$. Se S está $i-$comprimido, são equivalentes:

1. *Se $b \in S$, então $a \in S$.*
2. *Se $b' \in S'$, então $a' \in S'$.*

Lema 2.15. *Seja $n \geq 3$, $S \subseteq F_v$ e $a, b \in F_v$, com $a = (a[1], \ldots, a[n]), b = (b[1], \ldots, b[n])$, $a <_{lex} b$ e $b[n] = 0$ ou $a[n] = k_n$. Se $b \in S$ e S está $i-$comprimido, para todo $i \in 1, 2, n$, então $a \in S$.*

Demonstração. Vamos provar o caso que $a[n] = k_n$. Para isso comparamos as primeiras coordenadas de a e b.

1. Se $a[1] = b[1]$, como $a <_{lex} b$, então $a[2] \leq b[2]$. Portanto, reescrevendo a e b segue que $a = (b[1], a[2], \ldots, a[n]) <_{lex} (b[1], b[2], \ldots, b[n]) = b$ e como S está $1-$comprimido, segue que $a \in S$. Observe que isto acontece independentemente que $a[n] = k_n$ ou $b[n] = 0$.

2. Se $a[1] < b[1]$ e $a[i] > 0$, para algum $i \in [2, n-1]$, temos que

   $$a = (a[1], a[2], \ldots, a[n]) <_{lex} (b[1], a[2]', \ldots, a[n-1]', a[n]) <_{lex} (b[1], b[2], \ldots, b[n]) = b,$$

   onde $(a[2]', \ldots, a[n-1]')$ é o menor elemento (em $n-2$ dimensões), em relação à ordem lexicográfica, tal que $b[1] + a[2]' + \cdots + a[n-1]' + a[n] = a[1] + \cdots + a[n] = v$, isto é, $a[2]' + \cdots + a[n-1]' = v - k_n - b[1]$. Assim, tomando $c = (b[1], a[2]', \ldots, a[n-1]', a[n])$, como S está $1-$comprimido, $c \in S$, e como S está $n-$comprimido, então $a \in S$.

3. Se $a[1] <_{lex} b[1]$ e $a[2] = \cdots = a[n-1] = 0$ obtemos as desigualdades

   $$a = (a[1], \ldots, a[n]) <_{lex} (b[1], a[2], \ldots, a[n-1], a[n] - b[1] + a[1]) \leq_{lex} (b[1], \ldots, b[n]) = b.$$

   Nesse caso $c = (b[1], a[2], \ldots, a[n-1], a[n] - b[1] + a[1]) \in F_v$, pois $b[1] - a[1] \leq k_1 \leq k_n = a[n]$. Assim, como S está $1-$comprimido, $c \in S$, e como S está $2-$comprimido, então $a \in S$.

Provamos no caso $a[n] = k_n$ que, se $a[1] < b_[1]$, então existe $c \in F_v$, tal que $a <_{lex} c <_{lex} b$ e a primeira, a segunda ou a última coordenada de c é igual às respectivas coordenadas de a e b. Logo, como $b \in S$ e S está $i-$comprimido, para $i = 1, 2, n$, então $c \in S$ e analogamente $a \in S$.

Por outra parte, para o caso $b[n] = 0$, considere S' como na observação 2.14. Veja que se $b[n] = 0$, a última coordenada do vetor $b' = (k_1 - b[1], \ldots, k_n - b[n])$ é igual a k_n. Assim, se $a[1] < b[1]$, segue que $k_1 - b[1] < k_1 - a[1]$ e portanto podemos usar o resultado anterior para $b' <_{lex} a'$.

Existe $c' \in F_{k-v}$, com a primeira, a segunda ou a última coordenada igual às respectivas coordenadas de b' e a', tal que $b' = (k_1 - b[1], \ldots, k_n - b[n]) <_{lex} c' <_{lex} (k_1 - a[1], \ldots, k_n - a[n]) = a'$. Logo, pelo fato que ϕ inverte a ordem temos que $a <_{lex} c <_{lex} b$, onde $c = \phi(c')$ e a primeira, a segunda ou a última coordenada de c é igual às respectivas coordenadas de a e b. Por último, como $b \in S$ e S está $i-$comprimido, para $i = 1, 2, n$, então $c \in S$ e analogamente $a \in S$. □

A prova do Teorema 2.2 será feita por indução sobre n, o número de variáveis. Por tal razão podemos focar nossa atenção no caso $n = 2$, o caso base, para entender a motivação no caso de $\mathbb{Z}^2_{\geq 0}$ e tentar generalizar esta ideia para mais variáveis. Este caso base será estudado mais detalhadamente a continuação.

Observação 2.16. *Sejam $v \in [0, k]$ e $B = \{(a[1], a[2]), (a[1]+1, a[2]-1), \ldots, (a[1]+m, a[2]-m)\} \subsetneq F_v$ um subconjunto próprio de F_v, dizemos que B é um bloco de F_v de tamanho $m+1$, para $m \in \mathbb{N}$.*

Um bloco B_0 que contem exatamente os menores $m+1$ elementos de F_v, em relação à ordem lexicográfica, é chamado um bloco inicial de F_v de tamanho $m+1$, com $m \in \mathbb{N}$.

Veja que se B é um bloco de tamanho $m+1$ e $(a[1], a[2]), (a[1]+1, a[2]-1) \in B$, então $\Gamma_2((a[1], a[2])) = (a[1], a[2]-1) = \Gamma_1((a[1]+1, a[2]-1)) \in \Gamma(B)$. De este modo simplificamos a forma de achar $\Gamma(B)$. Em geral, é possível classificar os blocos iniciais de F_v dependendo do $v \in [0, k]$.

Seja B_0 um bloco inicial de F_v de tamanho $m+1$, para $m \in \mathbb{N}$.

Se $v \in [0, k_2]$, $B_0 = \{(0, v), (1, v-1), \ldots, (m, v-m)\}$ e a sombra de B_0 é da forma

$$\Gamma(B_0) = \{\Gamma_2((0, v)), \Gamma_2((1, v)), \ldots, \Gamma_2((m-1, v-(m-1))), \Gamma_2((m, v-m))\},$$
$$\Gamma(B_0) = \{(0, v-1), (1, v-2), \ldots, (m-1, v-m), (m, v-m-1)\}.$$

Neste caso, como $|B_0| = m+1$, então $|\Gamma(B_0)| = m+1$ e $|\Gamma(B_0)| - |B_0| = 0$.

Se $v \in [k_2+1, k_1+k_2]$, $B_0 = \{(a, k_2), (a+1, k_2-1), \ldots, (a+m, k_2-m)\}$, com $a \in [1, k_1]$ e neste casso:

$$\Gamma(B_0) = \{\Gamma_1((a, k_2)), \Gamma_1((a+1, k_2-1)), \ldots, \Gamma_1((a+m, k_2-m)), \Gamma_2((a+m, k_2-m))\}$$
$$\Gamma(B_0) = \{(a-1, k_2), (a, k_2-1), \ldots, (a+m-1, k_2-m), (a+m, k_2-m-1)\}$$

Neste caso, como $|B_0| = m+1$, então $|\Gamma(B_0)| = m+2$ e $|\Gamma(B_0)| - |B_0| = 1$.

Analogamente, seja B é um bloco final de tamanho $m+1$, isto é, um bloco que contem exatamente os maiores $m+1$ elementos de F_v. Se $v \in [0, k_1]$, temos que $|\Gamma(B)| = m+1$ e $|\Gamma(B)| - |B| = 0$. Se $v \in [k_1+1, k_1+k_2]$, temos que $|\Gamma(B)| = m+2$ e $|\Gamma(B)| - |B| = 1$.

Em geral, se B é um bloco tal que $(0, v) \notin B$ e $(v, 0) \notin B$, então $|\Gamma(B)| = |B| + 1$, isto é, $|\Gamma(B)| - |B| = 1$. Caso contrario, se $(0, v) \in B$ ou $(v, 0) \in B$, então $|\Gamma(B)| = |B|$. Observe que, como $B \neq F_v$ não é possível que $(0, v) \in B$ e $(v, 0) \in B$.

Sejam B bloco de F_v e B_0 bloco inicial de F_v. Se $v \in [0, k_2]$, então $|\Gamma(B)| - |B| = 0$ ou 1 e $|\Gamma(B_0)| - |B_0| = 0$. Se $v \in [k_2+1, k_1+k_2]$, então $|\Gamma(B)| - |B| = 1$ e $|\Gamma(B_0)| - |B_0| = 1$.

Por último, para todo $v \in [0, k]$, B bloco de F_v e B_0 bloco inicial de F_v, segue que

$$|\Gamma(B)| - |B| \geq |\Gamma(B_0)| - |B_0|. \tag{2.3}$$

Definição 2.17. *Seja $H \subseteq F$ e $H_v \subsetneq F_v$. Se existem $B_1, \ldots, B_r$ blocos de F_v tais que $H_v = \bigcup_{i=1}^{r} B_i$, dizemos que $\mathcal{B} = \{B_1, \ldots, B_r\}$ é uma decomposição de H_v.*

Se $\mathcal{B} = \{B_1, \ldots, B_r\}$ é uma decomposição de H_v, tal que $B_i \cap B_j = \emptyset$ e $\Gamma(B_i) \cap \Gamma(B_j) = \emptyset$, para $i, j \in [1, r]$ com $i \neq j$, dizemos que $B_1, \ldots, B_n$ são os blocos maximais de H_v e que $\mathcal{B}$ é a decomposição de H_v em blocos maximais.

Proposição 2.18. *Dado $H_v \subsetneq F_v$ sempre é possível achar a decomposição de H_v em blocos maximais.*

Demonstração. Se H_v é um bloco de F_v, ele já é uma decomposição em blocos maximais.

Se $\mathcal{B} = \{B_1, \ldots, B_r\}$ é uma decomposição de H_v, tal que $B_i \cap B_j \neq \emptyset$, para alguns $i, j \in [1, r]$ com $i \neq j$, consideramos $B'_i = B_i \cup B_j$ e reescrevemos $\mathcal{B}' = (\mathcal{B} \setminus \{B_i, B_j\}) \cup B'_i$. Repare que $\mathcal{B}'$

continua sendo uma decomposição de H_v. Repetindo este processo uma quantidade finita de vezes conseguimos uma decomposição $\mathcal{B}$ de H_V tal que todos seus blocos são disjuntos.

Agora, seja $\mathcal{B}$ é uma decomposição de H_v tal que todos os seus blocos são disjuntos. Se $\Gamma(B_i) \cap \Gamma(B_j) \neq \emptyset$, para alguns $i, j \in [1, r]$ com $i \neq j$, consideramos $B_i' = B_i \cup B_j$ e reescrevemos $\mathcal{B}' = (\mathcal{B} \setminus \{B_i, B_j\}) \cup B_i'$. Repare que $\mathcal{B}'$ continua sendo uma decomposição de H_v de blocos disjuntos. Repetindo este processo uma quantidade finita de vezes conseguimos uma decomposição $\mathcal{B}$ de H_V de blocos disjuntos com sombra disjunta, ou seja, uma uma decomposição $\mathcal{B}$ de H_V em blocos maximais.

Finalmente, se $\mathcal{B} = \{B_1, \ldots, B_r\}$ é a decomposição de H_v em blocos maximais, segue que $|H_v| = |B_1| + \cdots + |B_r|$. □

Com estos resultados já podemos proceder a provar o Teorema 2.2 no caso $n = 2$ no seguinte lema.

Lema 2.19. *Sejam k_1, k_2 inteiros tais que $1 \leq k_1 \leq k_2$ e $v \in [1, k]$, definimos $k = k_1 + k_2$ e $F = \{(a[1], a[2]) : a[1] \in [0, k_1]$ e $a[2] \in [0, k_2]\}$, com a ordem lexicográfica. Dado $H \subseteq F$, se para todo $v \in [1, k]$ $H_v \subseteq F_v$, então $\Gamma(C(H_v)) \subseteq C(\Gamma(H_v))$.*

Demonstração. Se $H_v = F_v$, então $C(H_v) = C(F_v) = F_v$ e $\Gamma(C(H_v)) = \Gamma(F_v) = F_{v-1}$. Por outra parte, $\Gamma(H_v) = \Gamma(F_v) = F_{v-1}$ e $C(\Gamma(H_v)) = C(F_{v-1}) = F_{v-1}$, obtendo a igualdade desejada.

Se $H_v \subsetneq F_v$ e $\mathcal{B} = \{B_1, \ldots, B_r\}$ é a decomposição de H_v em blocos maximais, por (2.3) temos que

$$|\Gamma(H_v)| - |H_v| = \sum_{i=1}^{r} (|\Gamma(B_i)| - |B_i|) \geq |\Gamma(B_0)| - |B_0|,$$

para B_0 qualquer bloco inicial de F_v. Em particular, para B_0 o bloco inicial de tamanho $|H_v|$, ou seja, para $B_0 = C(H_v)$. Assim, segue que

$$|\Gamma(H_v)| \geq |\Gamma(C(H_v))|. \tag{2.4}$$

Por último, como $C(H_v)$ está comprimido, pelo Lema 2.13, $\Gamma(C(H_v))$ também está comprimido, isto é, $C(\Gamma(C(H_v))) = \Gamma(C(H_v))$. Logo, como $C(\Gamma(C(H_v))) = \Gamma(C(H_v))$ são os $|\Gamma(C(H_v))|$ menores elementos de F_{v-1} e $C(\Gamma(H_v))$ são os $|\Gamma(H_v)|$ menores elementos de F_{v-1}, pela desigualdade (2.4) segue que $\Gamma(C(H_v)) \subseteq C(\Gamma(H_v))$, provando o lema. □

Segue agora a prova geral do teorema 2.2.

Teorema 2.1. *Dado $H \subseteq F$, se $H_v \subseteq F_v$, então $\Gamma(C(H_v)) \subseteq C(\Gamma(H_v))$, para todo $v \in [1, k]$.*

Demonstração. A prova é por indução. O caso $n = 2$ já foi feito no Lema 2.19.

Agora, vamos supor o teorema válido para $n-1$ dimensões e vamos provar para n dimensões.

Sejam $v \in [1, k]$ e $H_v \subseteq F_v$. Considere as sequências $\{H_v^j\}_{j \in \mathbb{N}}$ e $\{(\Gamma(H_v))^j\}_{j \in \mathbb{N}}$ como na Definição 2.7. Pelo Lema 2.9, sabemos que existem $p_1, p_2 \in \mathbb{N}$, tais que $H_v^{p_1}$ e $(\Gamma(H_v))^{p_2}$ estão $i-$comprimidos, para todo $i \in [1, n]$. Tomando $p = \max\{p_1, p_2\}$ segue que H_v^p e $(\Gamma(H_v))^p$ estão $i-$comprimidos, para todo $i \in [1, n]$.

Por outra parte, se tomamos $H_{v-1} = \Gamma(H_v)$ a hipótese do Lema 2.11 é satisfeita e portanto temos que $\Gamma(H_v^j) \subseteq (H_{v-1})^j = (\Gamma(H_v))^j$, para todo $j \geq 2$. Em particular, se $S = H_v^p$ e $T = (\Gamma(H_v))^p$ segue que

$$\Gamma(S) \subseteq T. \tag{2.5}$$

Para completar a prova vamos modificar S e T até obter $S = C(H_v)$ e $T = C(\Gamma(H_v))$, verificando que a inclusão (2.5) seja satisfeita. Logo, seguiria que $\Gamma(C(H_v)) \subseteq C(\Gamma(H_v))$ e provaríamos o teorema.

Se $S = F_v$, pela Observação 2.8 temos que $|S| = |(H_v)^p| = |H_v|$ e como $H_v \subseteq F_v$, então $H_v = F_v$. Neste caso $\Gamma(C(F_v)) = \Gamma(F_v) = F_{v-1}$ e $C(\Gamma(F_v)) = C(F_{v-1}) = F_{v-1}$. Portanto $\Gamma(C(H_v)) \subseteq C(\Gamma(H_v))$ é satisfeita.

Agora, vamos supor que $S \subsetneq F_v$. Como $F_v \setminus S \neq \emptyset$, chamamos $a = (a[1], \ldots, a[n])$ ao menor elemento de F_v fora de S e $b = (b[1], \ldots, b[n]) \in S$ o maior elemento de S. Assim, obtemos dois casos $b <_{lex} a$ ou $b >_{lex} a$.

Se $b <_{lex} a$, então $S = \{x \in F_v : x \leq_{lex} b\}$. Agora, como $S = H_v^p$ e $|H_v^p| = |H_v|$, segue que $S = C(H_v)$ e portanto, $\Gamma(S) = \Gamma(C(H_v)) \subseteq T = (\Gamma(H_v))^p$. Em particular, por cardinalidades $|\Gamma(C(H_v))| \leq |(\Gamma(H_v))^p| = |\Gamma(H_v)| = |C(\Gamma(H_v))|$.

Observe que, pelo Lema 2.13 $\Gamma(C(H_v))$ está comprimido, isto significa que $\Gamma(C(H_v))$ é o conjunto dos $|\Gamma(C(H_v))|$ menores elementos de F_{v-1} e como $|\Gamma(C(H_v))| \leq |C(\Gamma(H_v))|$, segue que $\Gamma(C(H_v)) \subseteq C(\Gamma(H_v))$. Provando o teorema para o caso quando $b <_{lex} a$.

Vamos supor agora que $b >_{lex} a$.

Se $b[n] = 0$, pelo Lema 2.15, como $b >_{lex} a$, $b \in S$ e S está $i-$comprimido, para $i = 1, 2, n$, então $a \in S$, absurdo, pois $a \in F_v \setminus S$. Portanto $b[n] > 0$ e $\Gamma_n(b) \in F_{v-1}$. Logo, como $b \in S$, segue que $\Gamma_n(b) \in \Gamma(S) \subseteq T$.

Por outra parte, veja que se $x \in S \setminus \{b\}$, temos que $y <_{lex} x <_{lex} b$, para todo $y \in \Gamma(x)$. Assim, não existe $x \in S \setminus \{b\}$, tal que $\Gamma_n(b) \in \Gamma(x)$. Consideramos agora, $S' = (S \setminus \{b\}) \cup \{a\}$ e $T' = (T \setminus \{\Gamma_n(b)\}) \cup \{\Gamma_n(a)\}$, se $a[n] > 0$, e $T' = T$, se $a[n] = 0$. Veja que $\Gamma_n(a) \in F_{v-1}$, se $a[n] > 0$.

Vamos mostrar agora que $\Gamma(S') \subseteq T'$. Já provamos que não existe nenhum $x \in S \setminus \{b\}$, tal que $\Gamma_n(b) \in \Gamma(x)$. Logo, $\Gamma(S \setminus \{b\}) \subseteq (T \setminus \{\Gamma_n(b)\})$ e portanto é suficiente mostrar que $\Gamma(a) \subseteq T'$.

Observe primeiro que, se $a[n] = k_n$, pelo Lema 2.15, como $b >_{lex} a$, $b \in S$ e S está $i-$comprimido, para $i = 1, 2, n$, segue que $a \in S$, absurdo, pois $a \in F_v \setminus S$. Portanto, $a[n] < k_n$.

Se $a[n] > 0$, então $\Gamma_n(a) \in \Gamma(a) \subseteq T'$, por definição. Agora, se $a[n] = 0$ e $a[i] > 0$, para algum $i \in [1, n-1]$, então $\Gamma_i(a) \in \Gamma(a)$. Mas, $\Gamma_i(a) \in \Gamma(a')$, com $a' = P_n(\Gamma_i(a)) \in S$, pois $a' <_{lex} a$ e a é o menor elemento de F_v fora de S. Logo, como $\Gamma(a') \subseteq \Gamma(S) \subseteq T$, segue que $\Gamma_i(a) \in T$.

Por outra parte, como $b >_{lex} a$, segue que $b[1] \geq a[1]$. Mas, se $b[1] = a[1]$, como S está $1-$comprimido, então $a \in (C(S))_{1:b[1]} = S_{1:b[1]}$ e $a \in S$, absurdo, logo $b[1] > a[1]$. Assim, $\Gamma_n(b) \neq \Gamma_i(a)$ e $\Gamma_i(a) \in T'$. Logo, $\Gamma(a) \subseteq T'$. Além disso, temos por construção que S' segue estando $i-$comprimido.

Por último, trocamos S por S' e T por T'. Repare que depois de aplicar um número finito de vezes o procedimento anterior temos que $S' = C(H_v)$ e $\Gamma(C(H_v)) \subseteq T'$.

Agora, $C(\Gamma(H_v))$ é o conjunto dos $|\Gamma(H_v)|$ menores elementos de F_{v-1} e pelo Lema 2.13 $\Gamma(C(H_v))$ é o conjunto dos $|\Gamma(C(H_v))|$ menores elementos de F_{v-1}. Mas $|\Gamma(C(H_v))| \leq |T'| = |T| = |\Gamma(H_v)|$, portanto $\Gamma(C(H_v)) \subseteq C(\Gamma(H_v))$, provando o teorema. □

Corolário 2.20. *Sejam $H \subseteq F$ e $v \in [0, k]$, se $H_v \subseteq F_v$ então $P(L(H_v)) \subseteq L(P(H_v))$.*

Demonstração. Consideremos $\phi : F \to F$ como na Observação 2.14. Se tomamos $H'_{k-v} = \phi(H_v)$, então, como ϕ é uma bijeção que reverte a ordem, segue que $L(H'_{k-v}) = \phi(C(H_v))$ e $P(H'_{k-v}) = \phi(\Gamma(H_v))$. Por último, como $\Gamma(C(H_v)) \subseteq C(\Gamma(H_v))$, para todo $v \in [0, k]$, aplicando ϕ obtemos $P(L(H_v)) \subseteq L(PH_v)$, para todo $v \in [0, k]$. □

2.2 Teorema de Wei

O objetivo desta secção é estudar os conceitos e as ferramentas necessárias para provar a generalização do Teorema de Wei desenvolvida por Beelen e Datta em [1]. O teorema de Wei

foi estudado inicialmente em [5] mas teve alguns erros que foram corregidos posteriormente e generalizados em [1], texto onde esta baseada esta secção.

Para provar a generalização do Teorema de Wei usaremos a notação introduzida na Secção 1.3 e os resultados antes estudados neste capitulo.

Proposição 2.21. *Seja $H_v \subseteq F_v$, segue que $\nabla_{v+m}(\nabla_{v+(m-1)}(H_v)) = \nabla_{v+m}(H_v)$, para todo $m \in [1, k-v]$.*

Demonstração. Se $a \in \nabla_{v+m}(\nabla_{v+(m-1)}(H_v))$, existe $b \in \nabla_{v+(m-1)}(H_v)$, tal que $b \leq_P a$ e para o qual existe $c \in H_v$, tal que $c \leq_P b \leq_P a$. Portanto, $a \in \nabla_{v+m}(H_v)$.

Se $a \in \nabla_{v+m}(H_v)$, existe $c \in H_v$, tal que $c \leq_P a$. Como $|c| = v$, existe $i \in [1, n]$, tal que $c[i] < a[i]$, isto implica que $b_1 = P_i(c) \in F_{v+1}$ e $c \leq_P b_1 \leq_P a$. Seguindo esta construção achamos uma cadeia crescente $c \leq_P b_1 \leq_P \cdots \leq_P b_{m-1} \leq_P a$, com $b_j \in \nabla_{v+j}(H_v)$, para cada $j \in [1, m-1]$. Portanto, $a \in \nabla_{v+m}(\nabla_{v+(m-1)}(H_v))$.

Por último, $\nabla_{v+m}(\nabla_{v+(m-1)}(H_v)) = \nabla_{v+m}(H_v)$ para todo $m \in [1, k-v]$. □

Proposição 2.22. *Sejam $H \subseteq F$ e $v \in [0, k]$, se $H_v \subseteq F_v$, então $\nabla_{v+m}(L(H_v)) \subseteq L(\nabla_{v+m}(H_v))$, para todo $m \in [0, k-v]$. Em particular, $|\nabla_{v+m}(L(H_v))| \leq |L(\nabla_{v+m}(H_v))|$.*

Demonstração. A prova é por indução sobre m. Vamos primeiro provar para $m = 0, 1, 2$.

Se $m = 0$ e $v \in [0, k-1]$, temos que $\nabla_v(L(H_v)) = L(H_v) \cap F_v = L(H_v)$ e $\nabla_v(H_v) = H_v \cap F_v = H_v$, logo, $\nabla_v(L(H_v)) = L(H_v) = L(\nabla_v(H_v))$.

Se $m = 1$ e $v \in [0, k-1]$, queremos $\nabla_{v+1}(L(H_v)) = P(L(H_v)) \subseteq L(P(H_v)) = L(\nabla_{v+1}(H_v))$. A prova segue pelo Corolário 2.20.

Se $m = 2$ e $v \in [0, k-2]$, consideremos $S = \nabla_{v+1}(H_v) \subseteq F_{v+1}$, pelo Corolário 2.20 para $v+1$ segue que $\nabla_{(v+1)+1}(L(S)) \subseteq L(\nabla_{(v+1)+1}(S))$, isto é, $\nabla_{v+2}(L(\nabla_{v+1}(H_v))) \subseteq L(\nabla_{v+2}(\nabla_{v+1}(H_v)))$. Por último, pela Proposição 2.21 segue que

$$\begin{aligned}\nabla_{v+2}(L(H_v)) &= \nabla_{v+2}(\nabla_{v+1}(L(H_v))) \\ &\subseteq \nabla_{v+2}(L(\nabla_{v+1}(H_v))) \\ &\subseteq L(\nabla_{v+2}(\nabla_{v+1}(H_v))) = L(\nabla_{v+2}(H_v)).\end{aligned}$$

Agora, vamos supor o teorema válido para $m-1$ e $v \in [0, k-(m-1)]$, isto é,

$$\nabla_{v+(m-1)}(L(H_v)) \subseteq L(\nabla_{v+(m-1)}(H_v)).$$

Vamos provar o caso m e $v \in [0, k-m]$. Como no caso $m = 2$, pelo Corolário 2.20 para $v + (m-1) \in [0, k-1]$ temos que $\nabla_{v+m}(L(\nabla_{v+(m-1)}(H_v))) \subseteq L(\nabla_{v+m}(\nabla_{v+(m-1)}(H_v)))$ e pela Proposição 2.21, segue que

$$\begin{aligned}\nabla_{v+m}(L(H_v)) &= \nabla_{v+m}(\nabla_{v+(m-1)}(L(H_v))) \\ &\subseteq \nabla_{v+m}(L(\nabla_{v+(m-1)}(H_v))) \\ &\subseteq L(\nabla_{v+m}(\nabla_{v+(m-1)}(H_v))) = L(\nabla_{v+m}(H_v)).\end{aligned}$$

Provando a inclusão desejada.

□

Corolário 2.23. *Sejam $H \subseteq F$ e $v \in [0, k]$, se $H_v \subseteq F_v$, então $|\nabla(L(H_v))| \leq |\nabla(H_v)|$.*

Demonstração. Pela Proposição 2.22, como $|\nabla_{v+m}(L(H_v))| \leq |L(\nabla_{v+m}(H_v))| = |\nabla_{v+m}(H_v)|$, para todo $m \in [0, k-v]$, então

$$|\nabla(H_v)| = \sum_{m=0}^{k-v} |\nabla_{v+m}(H_v)| \geq \sum_{m=0}^{k-v} |\nabla_{v+m}(L(H_v))| = |\nabla(L(H_v))|.$$

□

Lema 2.24. *Sejam $v \in [1,k]$, $b \in F_v$ e $a = \max_{lex}\{x \in F_{v-1} : x \leq_{lex} b\}$, então $a \leq_P b$.*

Demonstração. Seja $c = b - a = (0, \ldots, 0, c[i], \ldots, c[n])$, como $a \leq_{lex} b$ temos que $c[i] \geq 0$. Vamos provar que $c[j] \geq 0$, para todo $j > i$, e portanto $a \leq_P b$.

Vamos provar por contradição, suponha que existe $l > i$, tal que $c[l] < 0$. Neste caso, tomamos $j = \min\{l \in [1,n] : c[l] < 0\} = \min\{l > i : c[l] < 0\}$.

1. Se $c[i] > 1$, definimos $a' = a + e_i - e_j \in F_{v-1}$, onde e_i é o vetor com 1 na $i-$ésima coordenada e 0 nas outras. Veja que $0 \leq a[i] < a[i]+1 = b[i]-c[i]+1 < b[i] \leq k_i$ e como $c[j] < 0$, segue que $k_j \geq a[j] > a[j] - 1 = b[j] - c[j] - 1 \geq b[j] \geq 0$. Logo, $a' \in F$.

   Por outro lado, veja que $a = (a[1], \ldots, a[n]) <_{lex} (a[1], \ldots, a[i]+1, \ldots, a[j]-1, \ldots, a[n]) = a'$. Mais ainda, a primeira coordenada não nula de $c' = b - a'$ é $c[i] - 1 > 0$. Isto implica que $a' <_{lex} b$ e portanto $a <_{lex} a' <_{lex} b$, contradizendo a maximalidade de a.

2. Se $c[i] = 1$ e $c[l] > 0$, para algum $i < l < j$, definimos $a' = a + e_i - e_j \in F_{v-1}$, como no caso anterior e vemos que $a' \in F$ e que $a <_{lex} a' <_{lex} b$, contradizendo a maximalidade de a.

3. Se $c[i] = 1$ e $c[l] = 0$, para todo $i < l < j$. Como $c[j] < 0$ e $|c| = |b| - |a| = v - (v-1) = 1$, existe $h > j$, tal que $c[h] > 0$. Definimos $a' = b - e_h \in F_{v-1}$ e vemos que a primeira coordenada não nula de $a' - a$ é $c[i] = 1 > 0$, contradizendo a maximalidade de a.

Assim, não existe $l > i$, tal que $c[l] < 0$, isto é, $c[j] \geq 0$, para todo $j > i$, e portanto $a \leq_P b$. □

Observação 2.25. *Sejam $u, v \in [1,k]$ com $u \leq v$, aplicando o lema iterativamente obtemos que se $b \in F_v$ e $a = \max_{lex}\{x \in F_u : x \leq_{lex} b\}$, então $a \leq_P b$.*

Proposição 2.26. *Sejam $r \in \mathbb{N}$ e $u, v \in [1,k]$ com $u \leq v$, definimos $M(r)$ como o conjunto dos r maiores elementos de $F_{\leq v}$, em relação à ordem lexicográfica, e $M_u = M(r) \cap F_u$. Se $r_u = |M_u|$, definimos M_u* como o conjunto dos $r_u + 1$ maiores elementos de F_u, em relação à ordem lexicográfica. Segue que:*

1. $\nabla_v(M_u) \subseteq M_v \subseteq \nabla_v(M_u*)$.
2. $|\nabla(M(r))| = r - |M_v| + |\nabla(M_v)|$.

Demonstração. 1. Se $a \in \nabla_v(M_u)$, existe $b \in M_u$ e $c \in F_{v-u}$, tais que $a = b + c$. Logo, $b \leq_P a$ e, em particular, $b \geq_{lex} a$. Agora, como $b \in M(r)$, segue que $a \in M(r)$ e como $a \in F_v$, então $a \in M_v = M(r) \cap F_v$. Provamos assim a primeira inclusão.

Por outro lado, se $a \in M_v$, consideramos $c = \max_{lex}\{x \in F_u : x \leq_{lex} a\}$ e pela Observação 2.25, temos que $c \leq_P a$. Se $c \in M_u$, segue a segunda inclusão. Suponhamos agora que $c \notin M_u$, como M_u é o conjunto dos r_u maiores elementos de F_u, em relação à ordem lexicográfica, então $c \leq_{lex} a_{r_u+1}$, onde $a_1, \ldots, a_{r_u 1+}$ são os $r_u + 1$ maiores elementos de F_u, em relação à ordem lexicográfica.

Se $c = a_{r_u+1}$, então $c \in M_u*$ e portanto, $a \in \nabla_v(M_u*)$. Agora, se $c <_{lex} a_{r_u+1}$. Pela maximalidade de c temos que $a \leq_{lex} c <_{lex} a_{r_u+1}$, mas como $a \in M(r)$, então $a_{r_u+1} \in M(r)$ e assim, $a_{r_u+1} \in M_u$. Absurdo, pois $|M_u| = r_u$. Portanto, $c = a_{r_u+1}$ e a segunda inclusão segue.

2. Vejamos primeiro que $|\nabla(M(r))| = |\nabla(M(r)) \cap F_{<v}| + |\nabla(M(r)) \cap F_{\geq v}|$.

Primeiro, vamos provar que $\nabla(M(r)) \cap F_{<v} = \nabla(M(r) \setminus M_v) \cap F_{<v}$. Se $a \in \nabla(M(r)) \cap F_{<v}$, existe $b \in M(r)$, tal que $b \leq_P a$. Mas, como $a \in F_{<v}$, aquele $b \in M(r) \cap F_{<v} = M(r) \setminus M_v$. Assim, $a \in \nabla(M(r) \setminus M_v) \cap F_{<v}$. Agora, se $a \in \nabla(M(r) \setminus M_v) \cap F_{<v}$, existe $b \in M(r) \setminus M_v \subset M(r)$, tal que $b \leq_P a$. Portanto, $a \in \nabla(M(r)) \cap F_{<v}$.

Por outro lado, vejamos que $M(r) \setminus M_v$ é o conjunto dos $r - |M_v|$ maiores elementos de $F_{\leq v-1}$, em relação à ordem lexicográfica. De fato, provemos que $\nabla_u(M(r) \setminus M_v) = M_u$, para todo $u \in [1, v-1]$. Se $a \in \nabla_u(M(r) \setminus M_v) = \nabla(M(r) \setminus M_v) \cap F_u$, existe $b \in M(r) \setminus M_v$, tal que $b \leq_P a$. Mas, como $a \in F_u$ e $u < v$, então $a \in M(r) \cap F_u = M_u$. Obviamente, $M_u \subseteq \nabla_u(M(r) \setminus M_v)$.

Desta primeira parte obtemos que $|\nabla(M(r)) \cap F_{<v}| = |\nabla(M(r) \setminus M_v) \cap F_{<v}| = r - |M_v|$.

Agora, provaremos que $\nabla(M(r)) \cap F_{\geq v} = \nabla(M_v)$. Se $a \in \nabla(M(r)) \cap F_{\geq v}$, existe $b \in M(r)$, tal que $b \leq_P a$. Se $b \in F_v$, segue que $b \in M_v = M(r) \cap F_v$ e $a \in \nabla(M_v)$. Se $b \notin F_v$, existe $u < v$, tal que $b \in F_u$, logo existem $b_1, \ldots, b_{v-u} \in F_{u+j}$, tais que $b \leq_P b_1 \leq_P \cdots \leq_P b_{v-u} \leq_P a$. Portanto, $a \in \nabla(M_v)$.

Observe que se $a \in \nabla(M_v)$, existe $b \in M_v \subseteq M(r)$, tal que $b \leq_P a$. Assim, $a \in \nabla(M(r)) \cap F_{\geq v}$. Por cardinalidades segue que $|\nabla(M(r)) \cap F_{\geq v}| = |\nabla(M_v)|$.

Por último, juntando as desigualdades anteriores temos que $|\nabla(M(r))| = r - |M_v| + |\nabla(M_v)|$. □

Teorema 2.27. *Sejam $v \in [1, k]$ e $H \subseteq F_{\leq v}$, com $|H| = r$, então $|\nabla(M(r))| \leq |\nabla(H)|$, onde $M(r)$ denota os r maiores elementos de $F_{\leq v}$ em relação à ordem lexicográfica.*

Demonstração. Dado $u \in [1, v]$, definimos $H_u = H \cap F_u$, $M_u = M(r) \cap F_u$ e $r_u = |M_u|$. Dividimos a prova em dois casos:

Caso 1. Se $|H_v| \geq r_v = |M_v|$, isto é, existe $\alpha \geq 0$, tal que $|H_v| = r_v + \alpha$. Vejamos primeiro que

$$|\nabla(H)| = |\nabla(H) \cap F_{<v}| + |\nabla(H) \cap F_{\geq v}|.$$

Mais ainda, como $H \subseteq \nabla(H)$, segue que $H \cap F_{<v} \subseteq \nabla(H) \cap F_{<v}$. Além disso, provemos que $\nabla(H_v) \subseteq \nabla(H) \cap F_{\geq v}$. Se $a \in \nabla(H_v)$, existe $b \in H_v \subseteq H$, tal que $b \leq_P a$, logo $a \in \nabla(H)$ e como $b \in F_v$, então $a \in F_{\geq v}$, o que implica $a \in \nabla(H) \cap F_{\geq v}$. Por cardinalidades, segue que

$$\begin{aligned} |\nabla(H)| &= |\nabla_{<v}(H)| + |\nabla_{\geq v}(H)| \\ &\geq |H \cap F_{<v}| + |\nabla(H_v)| = r - |H_v| + |\nabla(H_v)|. \end{aligned}$$

Seja $H'_v \subseteq H_v$, tal que $|H'_v| = r_v$, vemos que $\nabla(H'_v) \subseteq \nabla(H_v)$. Por outra parte, vemos que $L(H'_v) = M_v$ e pelo Corolário 2.23, segue que $|\nabla(H_v)| \geq |\nabla(H'_v)| \geq |\nabla(M_v)|$.

$$|\nabla(H_v)| \geq |\nabla(M_v)| + \alpha.$$

Isto segue do Corolário 2.23 aplicado ao conjunto H_v que consiste de r_v elementos e da contribuição da sombra dos restantes α elementos de $H \setminus H_v$.

Por último, lembrando que $|\nabla(M(r))| = r - |M_v| + |\nabla(M_v)|$, pela Proposição 2.26, e juntado as anteriores desigualdades segue que

$$\begin{aligned} |\nabla(H)| &\geq r - |H_v| + |\nabla(H_v)| \\ &\geq r - r_v - \alpha + |\nabla(M_v)| + \alpha = |\nabla(M(r))|. \end{aligned}$$

Caso 2. Se $|H_v| < r_v = |M_v|$. Como $|H| = r = |M(r)|$, existe $u < v$, tal que $|H_u| > r_u = |M_u|$ e $|H_u| \geq r_u + 1 = |M^*_u|$. Pela Proposição 2.26, $|M_v| \leq |\nabla_v(M^*_u)|$ e pelo Corolário 2.20, $|\nabla_v(M^*_u)| \leq |\nabla_v(H_u)|$.

Por último,

$$\begin{aligned} |\nabla(H)| &\geq r - |H_v| + |\nabla_{\geq v}(H)| \\ &\geq r - |M_v| + |\nabla(\nabla_v(H_u))| \\ &\geq r - |M_v| + |\nabla(M_v)| = |\nabla(M(r))|. \end{aligned}$$

□

Este último teorema prova que o conjunto que tem sombra com menor cardinal em $F_{\leq v}$ é exatamente o conjunto dos maiores r elementos de $F_{\leq v}$ em relação à ordem lexicográfica. Portanto achamos explicitamente um conjunto que atinge o $\min\{|\nabla(a_1, \ldots, a_r)| : a_1, \ldots, a_r \in F_{\leq d}\}$.

Pela Observação 1.42 vimos que achar aquele mínimo equivale com achar uma cota superior para o número de zeros de uma família de polinômios em um produto cartesiano finito. Agora, só falta mostrar uma cara explicita deste mínimo e relacionar este resultado com a Pergunta 0.1. Este último será o objetivo do seguinte capitulo.

Capítulo 3

Zeros de polinômios em um produto cartesiano finito

O objetivo deste capitulo é responder a Pergunta 0.1 formulada no começo do texto. Para isso vamos usar os resultados obtidos nos capítulos anteriores além de algumas bijeções que aclaram a relação entre os zeros de polinômios num produto cartesiano finito com o conjunto F e com o $\min\{|\nabla(a_1,\ldots,a_r)| : a_1,\ldots,a_r \in F_{\leq d}\}$ que temos estudado ao longo do texto. A maioria dos resultados estão baseados em [1].

Observação 3.1. *Lembrando que* $F = \{(a[1],\ldots,a[n]) : a_i \in [0,k_i-1]$ *para todo* $i \in [1,n]\}$, *consideramos a aplicação:*

$$\phi : F \to [0, k_1\cdots k_n - 1]$$
$$(a[1],\ldots,a[n]) \mapsto \phi((a[1],\ldots,a[n])) = \sum_{i=1}^{n} a[i] \prod_{j=i+1}^{n} k_i.$$

Observe que dado $m \in [0, k_1\cdots k_n - 1]$, *pelo algoritmo da divisão existem únicos* $a[1] \in [0, k_1 - 1]$ *e* $r_1 \in [0, k_2\cdots k_n - 1]$, *tais que* $m = a[1](k_2\cdots k_n) + r_1$. *Analogamente, para* $r_1 \in [0, k_2\cdots k_n - 1]$ *existem únicos* $a[2] \in [0, k_2 - 1]$ *e* $r_2 \in [0, k_3\cdots k_n - 1]$, *tais que* $r_1 = a[2](k_3\cdots k_n) + r_2$.

Fazendo este processo n *vezes achamos* $a[1] \in [0, k_1 - 1], \ldots, a_n \in [0, k_n - 1]$, *tais que* $m = a[1](k_2\cdots k_n) + a[2](k_3\cdots k_n) + \cdots + a[n]k_n$. *Deste modo,* $(a[1],\ldots,a[n]) \in F$ *e* $\phi((a[1],\ldots,a[n])) = m$, *portanto* ϕ *é sobrejetora.*

Por outro lado, observe que em cada aplicação do algoritmo da divisão achamos que aqueles $a[1],\ldots,a[n]$ *são únicos. Assim, dados* $a, b \in F$, *com* $a = (a[1],\ldots,a[n])$ *e* $b = (b[1],\ldots,b[n])$, *tais que* $\phi((a[1],\ldots,a[n])) = \phi((b[1],\ldots,b[n]))$, *chamamos*

$$m = \sum_{i=1}^{n} a[i] \prod_{j=i+1}^{n} k_i = \sum_{i=1}^{n} b[i] \prod_{j=i+1}^{n} k_i.$$

Mas, pela unicidade da escritura de $m \in [0, k_1\cdots k_n - 1]$, *segue que* $a[i] = b[i]$, *para todo* $i \in [1,n]$, *isto é,* $(a[1],\ldots,a[n]) = (b[1],\ldots,b[n])$. *Portanto* ϕ *é injetora.*

Finalmente temos que ϕ *é uma bijeção. Mais ainda, vemos que*

$$(a[1],\ldots,a[n]) \leq_{lex} (b[1],\ldots,b[n]) \text{ se, e somente se, } \sum_{i=1}^{n} a[i] \prod_{j=i+1}^{n} k_i \leq \sum_{i=1}^{n} b[i] \prod_{j=i+1}^{n} k_i.$$

Neste caso, como $\phi((0,\ldots,0)) = 0$ *e* $\phi((k_1 - 1,\ldots,k_n - 1)) = k_1\cdots k_n - 1$, *vemos que o primeiro e o último elemento de* F *são enviados para o primeiro e último elemento de* $[0, k_1\cdots k_n - 1]$, *respetivamente.*

Analogamente, para cada $r \in [0, k_1 \cdots k_n - 1]$ existe $a_r = (a_r[1], \ldots, a_r[n]) \in F$, tal que $\phi((a_r[1], \ldots, a_r[n])) = k_1 \cdots k_n - r$. Isto implica que, como $k_1 \cdots k_n - r$ é o $r-$ésimo maior elemento de $[0, k_1 \cdots k_n - 1]$, então aquele a_r é o $r-$ésimo maior elemento de F, em relação à ordem lexicográfica. Aplicando esta ideia pode-se enunciar e provar o seguinte resultado.

Lema 3.2. *Se $a_1, \ldots, a_r$ são os maiores r elementos de $F_{\leq d}$, então*

$$\nabla(a_1, \ldots, a_r) = \{a \in F : a_r \leq_{lex} a\}.$$

Mais ainda, se $a_r = (a_r[1], \ldots, a_r[n])$, então

$$|\nabla(a_1, \ldots, a_r)| = k_1 \cdots k_n - \sum_{i=1}^{n} a_r[i] \prod_{j=i+1}^{n} k_j.$$

Demonstração. Dado $b \in \nabla(a_1, \ldots, a_r)$, existe $i \in [1, r]$, tal que $a_i \leq_P b$. Portanto, $a_r \leq_{lex} a_i \leq_{lex} b$, para todo $i \in [1, r]$, e assim $\nabla(a_1, \ldots, a_r) \subseteq \{b \in F : a_r \leq_{lex} b\}$.

Por outro lado, dado $b \geq_{lex} a_r$ temos dois opções. Se $b = a_r$, segue que $b \geq_P a$ e portanto $b \in \nabla(a_1, \ldots, a_r)$. Vejamos agora o caso que $b >_{lex} a_r$.

Se $b = (b[1], \ldots, b[n])$, consideramos $s = \min\{i \in [1, n] : b[i] > a_r[i]\}$ e

$$c = (a_r[1], \ldots, a_r[s-1], a_r[s] + 1, 0, \ldots, 0) \in F.$$

Por construção, temos que $b \geq_P c$, $c \geq_{lex} a_r$ e $\deg(c) \leq |a_r| + 1$.

Se $|c| = |a_r| + 1$, temos que $a_r = (a_r[1], \ldots, a_r[s], 0, \ldots, 0)$ e $a_r \leq_P c \leq_P b$, ou seja, $b \in \nabla(a_1, \ldots, a_r)$.

Se $|c| \leq |a_r| \leq d$, então $c \in F_{\leq d}$. Assim, como $c \geq_{lex} a_r$, segue que $c = a_i$, para algum $i \in [1, r]$. Portanto, $b \geq a_i$ e $b \in \nabla(a_1, \ldots, a_r)$. □

Proposição 3.3. *Se $f_1, \ldots, f_r \in S_{\leq d}(\mathcal{A})$ são polinômios linearmente independentes, então*

$$|Z(f_1, \ldots, f_r) \cap \mathcal{A}| \leq \sum_{i=1}^{n} a_r[i] \prod_{j=i+1}^{n} k_j$$

onde $a_r = (a_r[1], \ldots, a_r[n])$ é o $r-$ésimo maior elemento de $F_{\leq d}$ em relação à ordem lexicográfica.

Demonstração. Primeiro, pelo Corolário 1.41 temos que

$$|Z(f_1, \ldots, f_r) \cap \mathcal{A}| \leq \max\{|F \setminus \nabla(a_1, \ldots, a_r)| : a_1, \ldots, a_r \in F_{\leq d}\}.$$

Agora, pelo Teorema 2.27 temos que

$$|\nabla(M(r))| = \min\{|\nabla(a_1, \ldots, a_r)| : a_1, \ldots, a_r \in F_{\leq d}\},$$

onde $M(r)$ denota os r maiores elementos de $F_{\leq d}$ em relação à ordem lexicográfica.

Portanto, se $M(r) = \{a_1, \ldots, a_r\}$, com a_i o i-ésimo maior elemento de de $F_{\leq d}$ em relação à ordem lexicográfica, pelo Lema 3.2 temos que

$$|\nabla(M(r))| = |\nabla(a_1, \ldots, a_r)| = k_1 \cdots k_n - \sum_{i=1}^{n} a_r[i] \prod_{j=i+1}^{n} k_j,$$

onde $a_r = (a_r[1], \ldots, a_r[n])$. Assim, juntando os resultado anteriores obtemos que

$$\begin{aligned}\max\{|F \setminus \nabla(a_1, \ldots, a_r)| : a_1, \ldots, a_r \in F_{\leq d}\} &= |F| - \min\{|\nabla(a_1, \ldots, a_r)| : a_1, \ldots, a_r \in F_{\leq d}\} \\ &= |F| - |M(r)| \\ &= |F| - |\nabla(a_1, \ldots, a_r)| \\ &= k_1 \cdots k_n - (k_1 \cdots k_n - \sum_{i=1}^{n} a_r[i] \prod_{j=i+1}^{n} k_j) \\ &= \sum_{i=1}^{n} a_r[i] \prod_{j=i+1}^{n} k_j.\end{aligned}$$

Por último, obtemos a desigualdade desejada

$$|Z(f_1, \ldots, f_r) \cap \mathcal{A}| \leq \sum_{i=1}^{n} a_r[i] \prod_{j=i+1}^{n} k_j$$

onde $a_r = (a_r[1], \ldots, a_r[n])$ é o $r-$ésimo maior elemento de $F_{\leq d}$ em relação à ordem lexicográfica. □

A Proposição anterior dá uma cota superior para a quantidade de zeros, mas vamos provar que a cota é realmente a melhor possível. Para isso vamos construir uma família de polinômios tais que a quantidade de zeros de aquela família em um produto cartesiano finito atingem a cota achada.

Observação 3.4. *Vamos agora construir uma família de polinômios $f_1, \ldots, f_r \in \mathcal{S}_{\leq d}(\mathcal{A})$, linearmente independentes sobre F, tais que a cardinalidade de $Z(f_1, \ldots, f_r) \cap \mathcal{A}$ atinge a cota superior obtida na Proposição 3.3.*

Suponha que para cada $i \in [1, n]$, $A_i = \{\gamma_1^{(i)}, \ldots, \gamma_{k_i}^{(i)}\}$.

Dado $b = (b[1], \ldots, b[n]) \in F_{\leq d}$ definimos o polinômio $f_b \in \mathbb{F}[x_1, \ldots, x_n]$ como

$$f_b(x_1, \ldots, x_n) = \prod_{i=1}^{n} \prod_{j=1}^{b[i]} (x_i - \gamma_j^{(i)}).$$

Sejam $a_1, \ldots, a_r$ os maiores r elementos de $F_{\leq d}$, em relação à ordem lexicográfica, então

$$|Z(f_{a_1}, \ldots, f_{a_r}) \cap \mathcal{A}| = \sum_{i=1}^{n} a_r[i] \prod_{j=i+1}^{n} k_j,$$

onde $a_r = (a_r[1], \ldots, a_r[n])$. Considere a bijeção

$$\begin{aligned}\psi : \mathcal{A} &\longrightarrow F \\ (\gamma_{j_1}^{(1)}, \ldots, \gamma_{j_n}^{(n)}) &\longmapsto \psi((\gamma_{j_1}^{(1)}, \ldots, \gamma_{j_n}^{(n)})) = (j_1 - 1, \ldots, j_n - 1).\end{aligned}$$

Dado $b \in F_{\leq d}$, pela construção de f_b segue que $f_b((\gamma_{j_1}^{(1)}, \ldots, \gamma_{j_n}^{(n)})) \neq 0$ se, e somente se, $\gamma_{j_i}^{(i)} \in \{\gamma_j^{(i)} : j > b[i]\}$, para todo $i \in [1, n]$. Assim, $f_b((\gamma_{j_1}^{(1)}, \ldots, \gamma_{j_n}^{(n)})) \neq 0$ se, e somente se, $\psi((\gamma_{j_1}^{(1)}, \ldots, \gamma_{j_n}^{(n)})) \in \nabla(b)$.

Agora, se $a_1, \ldots, a_r$ são os maiores r elementos de $F_{\leq d}$, em relação à ordem lexicográfica, então $(\gamma_{j_1}^{(1)}, \ldots, \gamma_{j_n}^{(n)}) \in \mathcal{A} \setminus Z(f_{a_1}, \ldots, f_{a_r})$ se, e somente se, $\psi((\gamma_{j_1}^{(1)}, \ldots, \gamma_{j_n}^{(n)})) \in \nabla(a_1, \ldots, a_r)$.

Por último, $|\mathcal{A} \setminus Z(f_{a_1}, \ldots, f_{a_r})| = |\nabla(a_1, \ldots, a_r)| = k_1 \cdots k_n - \sum_{i=1}^{n} a_r[i] \prod_{j=i+1}^{n} k_j$ e por complemento, $|Z(f_{a_1}, \ldots, f_{a_r}) \cap \mathcal{A}| = \sum_{i=1}^{n} a_r[i] \prod_{j=i+1}^{n} k_j$. Atingindo a igualdade.

Finalmente, para responder a Pergunta 0.1 verificamos que a cota dada pela Proposição 3.3 é de fato atingida e aquela cota é a melhor possível.

Teorema 3.5. *A cota dada pela Proposição 3.3 é atingida, ou seja,*

$$\max\{|Z(f_1,\ldots,f_r)\cap\mathcal{A}|\} = \sum_{i=1}^{n} a_r[i] \prod_{i=i+1}^{n} k_j,$$

onde $a_r = (a_r[1],\ldots,a_r[n])$ *é o* $r-$*ésimo maior elemento de* $F_{\leq d}$ *em relação à ordem lexicográfica e o máximo é tomado sob todos os* $f_1,\ldots,f_r \in S_{\leq d}(\mathcal{A})$ *linearmente independentes sobre* $\mathbb{F}$*.*

Demonstração. Pela Observação 3.4 existem r polinômios em $S_{\leq d}(\mathcal{A})$ linearmente independentes sobre $\mathbb{F}$ tais que os zeros de aqueles polinômios em $\mathcal{A}$ atingem igualdade. □

Referências Bibliográficas

[1] Beelen P., Mrinmoy D.: *Generalized Hamming weights of affine cartesian codes* Finite fields and their applications, Vol. 51, 130-145, 2018. https://doi.org/10.1016/j.ffa.2018.01.006

[2] Clements G., Lindström B.: *A generalization of a combinatorial theorem of Macaulay* Journal of combinatorial theory, 230-238, 1969. https://doi.org/10.1016/S0021-9800(69)80016-5

[3] Cox D., Little J., O'Shea D.: *Ideals, Varieties and Algorithms* An Introduction to Computational Algebraic Geometry and Conmutative Algebra, Second Edition , 1996.

[4] Nie Z., Wang A.Y.: *Hilbert functions and the finite degree Zariski clousure in finite field combinatorial geometry* Journal of combinatorial theory, Vol. A134 196-220, 2015. https://doi.org/10.1016/j.jcta.2015.03.011

[5] Wei V.K.: *Generalized Hamming weights for linear codes* IEEE Transactions on Information Theory, Vol 37 1412-1418, 1991. https://doi.org/10.1109/18.133259