MATHEUS MANOEL DANTAS

Sobre funções distância mínima de códigos do tipo Reed-Muller

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2020

MATHEUS MANOEL DANTAS

Sobre funções distância mínima de códigos do tipo Reed-Muller

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: Teoria de códigos algébricos geométricos.

Orientador(a): Prof. Dr. Cícero Fernandes de Carvalho.

UBERLÂNDIA - MG
2020

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

D192 Dantas, Matheus Manoel, 1995-
2020 Sobre funções distância mínima de códigos do tipo Reed-Muller [recurso eletrônico] / Matheus Manoel Dantas. - 2020.

Orientador: Cícero Fernandes de Carvalho.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2020.233
Inclui bibliografia.
Inclui ilustrações.

1. Matemática. I. Carvalho, Cícero Fernandes de,1960-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. 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): Matheus Manoel Dantas.

NÚMERO DE MATRÍCULA: 11812MAT006.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Teoria de códigos algébricos geométricos.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Sobre funções distância mínima de códigos do tipo Reed-Muller.

ORIENTADOR(A): Prof. Dr. Cícero Fernandes de Carvalho.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 20 de fevereiro de 2020, às 8h30min, pela seguinte Banca Examinadora:

Prof. Dr. Cícero Fernandes de Carvalho
UFU - Universidade Federal de Uberlândia

Prof. Dr. Herivelto Martins Borges Filho
USP - Universidade de São Paulo campus São Carlos

Prof. Dr. Victor Gonzalo Lopez Neumann
UFU - Universidade Federal de Uberlândia

Uberlândia-MG, 20 de fevereiro de 2020.

Dedico esta conquista e batalha a Deus e à minha noiva Elis Coimbra de Moura, que é um presente e um instrumento de meu Pai em minha vida.

"Estude e aprenda sempre que puder meu filho porque o conhecimento é a única coisa que ninguém pode te tirar."
Rosalina Maria de Jesus Dantas.

"É nosso dever e salvação dar-Vos graça sempre e em todo lugar [...]"
Igreja Católica.

"[...] Nem sempre se pode ter fé, mas nem sempre a fraqueza que se sente quer dizer que a gente não é forte."
Palavras Repetidas, Gabriel o pensador.

Agradecimentos

Passarei minha vida inteira agradecendo a Deus e a Jesus Cristo e mesmo assim continuarei sendo um filho ingrato. As vezes me pego pensando no quanto Eles cuidam de mim e nem sequer tomo conhecimento. Muito obrigado Jesus por ouvir minhas preces, por dar saúde e proteção pra minha família, por me proteger nesses seis anos sobre duas rodas. Agradeço a ti meu Deus maravilhoso por me ouvir e aconselhar nos momentos em que lhe pedi ajuda (embora as vezes seja um pouco difícil entender o que o Senhor está dizendo).

Alguns amigos me perguntaram como eu sei que estou no caminho certo cursando Matemática e a resposta é a minha noiva Elis Coimbra de Moura. Eu acredito que existe apenas uma alma gêmea em todo o mundo, e o fato de encontrar a minha metade na Matemática é uma prova definitiva que meus passos estão bem direcionados. Agradeço a Deus por tê-la encontrado meu amor e agradeço a você minha Lis por ser uma companheira muito melhor do que eu jamais poderia ter imaginado.

Uma conquista não é apenas do protagonista, uma conquista pertence a todos aqueles que lutaram direta ou indiretamente para obtê-la, inclusive à aqueles que deram suporte e apoio para a linha de frente. Tenho tantas pessoas para a agradecer que tenho medo de esquecer de alguém. Agradeço especialmente pelo apoio da melhor família do mundo: meus pais, meu irmão, minha irmã, minha tia Eliete e minhas madrinhas. Registro aqui meu Muito Obrigado ao meu orientador Cícero Fernandes de Carvalho pelos conselhos, dicas e ensinamentos. Muito Obrigado também pela paciência, incentivo e direcionamento.

Agradeço aos meus amigos e companheiros, essa galera gente boa e divertida: Siqueira, Fabim, Stefani, Gonzalo, Japa, Luís, Gabriel, Sharingan, Ervilha, Aline, Fernando, JP, Paulo Victor, PV, Shadow, Léo, Gabi, Rejiane, Jefferson e Giovanny (e se eu esqueci de alguém por favor me perdoe!). Eventualmente nossos caminhos irão se separar, mas espero de coração conseguir manter contato com todos vocês.

Agradeço aos professores Victor Gonzalo Lopez Neumann e Herivelto Martins Borges Filho por aceitarem o convite para compor a banca examinadora da minha dissertação. Agradeço a Capes, ao CNPq e ao IMPA pela bolsa de estudos durante o mestrado. Encerro agradecendo por todas as dificuldades e montanhas que surgiram no meu caminho em 2019, algumas vezes o caminho é pesado e doloroso, mas o caminho é o professor e o valor da chegada é uma função crescente proporcional à dificuldade do caminho.

DANTAS, M. M. *Sobre funções distância mínima de códigos do tipo Reed-Muller.* 2020. 60p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Nesta dissertação introduzimos os códigos projetivos do tipo Reed-Muller sobre corpos finitos e exploramos suas propriedades. Depois definimos as chamadas funções distância mínima de um ideal, pois em alguns casos tais funções fornecem uma formulação algébrica para o parâmetro distância mínima deste tipo de código e utilizando-as em conjunto com a teoria das bases de Gröbner, a teoria das funções de Hilbert e a técnica da pegada de um ideal, obtemos cotas inferiores para a distância mínima dos códigos projetivos do tipo Reed-Muller.

Palavras-chave: Decomposição Primária, Espaço Projetivo, Bases de Gröbner e Pegada.

DANTAS, M. M. *On minimum distance functions of Reed-Muller-type codes.* 2020. 60 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this essay we introduce the projective Reed-Muller-type codes over finite fields and explore its properties. Then we define the so called minimum distance functions of an ideal, because in some cases these functions give an algebraic formulation for the minimum distance parameter of this type of codes and by using them together with the theory of Gröbner basis, the theory of Hilbert functions and the footprint techniques we obtain lower bounds for the minimum distance of projective Reed-Muller-type codes.

Keywords: Primary Decomposition, Projective Space, Gröbner basis and Footprint.

Sumário

Introdução

Neste texto vamos trabalhar com os códigos projetivos de tipo Reed-Muller. Graças a estrutura destes códigos conseguiremos, em alguns casos particulares, encontrar uma formulação algébrica para o parâmetro distância mínima utilizando as chamadas funções distância mínima. Este trabalho foi realizado tendo como base o artigo *Minimum distance functions of graded ideals and Reed-Muller-type codes* cujos autores são José Martínez-Bernal, Yuriko Pitones e Rafael H. Villareal [8]. Entretanto, o conteúdo foi selecionado e reorganizado no que pensamos ser uma ordem que facilita a compreensão e fluidez da teoria.

No primeiro capítulo trabalharemos os pré-requisitos necessários para desenvolver a teoria presente no artigo, em especial na teoria das bases de Gröbner e na decomposição primária de ideais pois estas teorias exercerão um papel crucial nos resultados dos capítulos dois e três. Alguns tópicos dos pré-requisitos serão discutidos de maneira sucinta, porque caso contrário esta dissertação ficaria extensa demais. No entanto, direcionamos o leitor para as referências necessárias para o aprofundamento em cada assunto.

No capítulo dois vamos partir da teoria das funções de Hilbert para definir o que é o grau de um ideal. Depois definimos as funções distância mínima e seguimos caminhando com a teoria em direção a demonstrar que, em alguns casos especiais, estas funções distância mínima descrevem o parâmetro distância mínima dos códigos projetivos do tipo Reed-Muller. Ou seja, obtemos uma formulação puramente algébrica para este parâmetro.

No terceiro capítulo introduzimos a pegada de um ideal e demonstramos suas propriedades necessárias para definir a função pegada de um ideal, e é com estas funções que iremos obter cotas inferiores para as funções distância mínima e consequentemente obtemos também cotas inferiores para o parâmetro distância mínima de alguns casos especiais dos códigos projetivos do tipo Reed-Muller.

Neste trabalho $\mathbb{K}$ denota um corpo qualquer e $x_0, x_1, \ldots, x_n$ denotam variáveis distintas. Durante o desenvolvimento da teoria em algumas seções estaremos trabalhando no espaço afim e em outras no espaço projetivo, por este motivo chamamos a atenção para a notação $\mathbb{K}[\mathbf{X}]$ que pode representar tanto o anel dos polinômios com coeficientes em $\mathbb{K}$ e n variáveis $\mathbb{K}[x_1, \ldots, x_n]$ quanto o anel com $n+1$ variáveis $\mathbb{K}[x_0, x_1, \ldots, x_n]$. No início de cada seção deixamos explicito qual anel a notação $\mathbb{K}[\mathbf{X}]$ representa. Além disso, utilizaremos a notação $\mathbb{K}[\mathbf{X}]_d$ como sendo o conjunto de todos os polinômios homogêneos de grau d de $\mathbb{K}[\mathbf{X}]$ adicionado o polinômio nulo.

Matheus Manoel Dantas
Uberlândia-MG, 20 de fevereiro de 2020.

Capítulo 1

Alguns Tópicos de Álgebra

1.1 Anéis Noetherianos

Há muito conteúdo sobre os anéis noetherianos nos livros de Algébra. Tais anéis possuem excelentes propriedades e são pontos de partida para várias teorias. Neste trabalho não iremos precisar utilizar muitos resultados a respeito destes anéis, apenas duas definições e dois teoremas serão o suficiente.

Definição 1.1 *Seja R um anel. Dizemos que R é* ***noetheriano*** *se todos os seus ideais são finitamente gerados. Isto é, dado um ideal $I \subset R$ existem elementos $a_1, \ldots, a_m \in R$ tais que $I = \langle a_1, \ldots, a_m \rangle$ onde $0 < m \in \mathbb{N}$.*

Chamamos de **cadeia ascendente de ideais** um conjunto de ideais $\{I_j\}_{j\in\mathbb{N}}$ de R organizados de forma $I_0 \subset I_1 \subset \cdots \subset I_m \subset \cdots$.

Teorema 1.1 *Um anel R é noetheriano se, e somente se, toda cadeia ascendente de ideais de R*

$$I_0 \subset I_1 \subset \cdots \subset I_m \subset \cdots$$

estaciona, isto é, existe um natural $N \in \mathbb{N}$ tal que $I_N = I_{N+j}$ para todo $j \in \mathbb{N}$.

Demonstração.
[⇒] Suponha que R seja um anel noetheriano. Seja $I_0 \subset I_1 \subset \cdots \subset I_n \subset \cdots$ uma cadeia ascendente de ideais de R. Pela relação de continência dos elementos da cadeia temos que $I = \bigcup_{j=0}^{\infty} I_j$ é um ideal de R e portanto existem elementos $a_1, \ldots, a_m \in R$ tais que $I = \langle a_1, \ldots, a_m \rangle$. Como I é uma união, existem índices $i_1, \ldots, i_m$ tais que $a_j \in I_{i_j}$ para todo $j \in \{1, \ldots, m\}$. Tomando $N = \max\{i_1, \ldots, i_r\}$ obtemos que $I = \bigcup_{j=1}^{\infty} I_j = I_N$, pois os ideais são encaixados. Consequentemente, para todo $l \in \mathbb{N}$ temos que

$$I_N \subset I_{N+l} \subset I = \bigcup_{j=1}^{\infty} I_j = I_N$$

donde $I_N = I_{N+l}$.

[⇐] Suponha que R seja um anel onde toda cadeia ascendente de ideais estaciona. Seja $I \subset R$ um ideal qualquer. Vamos construir uma cadeia ascendente de ideais da seguinte forma: seja $0 \neq a_1 \in I$ um elemento, definimos $I_0 = \langle a_1 \rangle$. Se $I = I_0$, então I é finitamente gerado e concluímos a demonstração, se não, considere $a_2 \in I \backslash I_0$ e defina $I_1 = \langle a_1, a_2 \rangle$. Novamente, se

$I = I_1$ acabou, se não, podemos tomar um elemento $a_3 \in I \backslash I_1$ e definir o ideal $I_2 = \langle a_1, a_2, a_3 \rangle$. Continuando com este processo iremos obter uma cadeia de ideais

$$I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots \text{ tal que } I_j \subset I \ \forall j \in \mathbb{N}.$$

Então, por hipótese, existe $N \in \mathbb{N}$ tal que $I_N = I_{N+l}$ para todo $l \in \mathbb{N}$. Pela maneira como construímos a cadeia isto significa que $I = I_N = \langle a_1, \ldots, a_{N-1} \rangle$ é finitamente gerado. Portanto R é noetheriano.

■

Com relação a estrutura de anéis, o foco deste texto é trabalhar sobre anéis de polinômios com coeficientes sobre um corpo. Por este motivo, o seguinte teorema é fundamental para o nosso desenvolvimento teórico:

Teorema 1.2 (Teorema da Base de Hilbert) *Se $\mathbb{K}$ é um corpo, então o anel $\mathbb{K}[x_1, \ldots, x_n]$ dos polinômios em n variáveis com coefientes em $\mathbb{K}$ é noetheriano.*

Demonstração.

Para uma demonstração clássica consulte [7]. Para uma demonstração utilizando a teoria de ordens monomiais, que discutiremos adiante, consultar [3].

■

1.2 Dicionário Álgebra-Geometria

O dicionário Álgebra-Geometria faz a ligação entre duas grandes áreas da matemática via duas pontes, uma delas associa polinômios e ideais a conjunto de pontos e a outra associa conjunto de pontos a ideais. É importante perceber que a conexão entre a Álgebra e a Geometria não é uma ponte de sentido duplo, são duas pontes distintas cada uma com suas propriedades. Este detalhe ficará evidente no decorrer deste texto.

Seja $0 < n \in \mathbb{N}$ um número natural. Chamamos de **espaço afim n dimensional** o produto cartesiano $\mathbb{K}^n$ que também pode ser denotado por $\mathbb{A}^n(\mathbb{K})$. Esta segunda notação é geralmente utilizada para não criar confusão com o espaço projetivo sobre $\mathbb{K}$, o qual discutiremos no final deste capítulo.

Definição 1.2 *Seja $f \in \mathbb{K}[x_1, \ldots, x_n]$ um polinômio. Definimos a **variedade afim** de f pela igualdade*

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

ou seja, $V(f)$ é o conjunto de zeros do polinômio f.

*Dado um ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ definimos a **variedade afim** de I como sendo o conjunto*

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

Segue da definição que: se $I = \langle f_1, \ldots, f_n \rangle$, então $V(I) = V(f_1, \ldots, f_n) = \bigcap_{i=1}^{n} V(f_i)$. Mas e o caminho inverso? Se possuímos um conjunto de pontos $X \subset \mathbb{K}^n$ como procedemos para encontrar um ideal I tal que $X = V(I)$?

Definição 1.3 *Seja $X \subset \mathbb{K}^n$ um conjunto de pontos. O conjunto*

$$I(X) = \{f \in \mathbb{K}[x_1, \ldots, x_n] : f(P) = 0, \forall P \in X\}$$

*é chamado de **ideal de** X.*

Não é difícil demonstrar que $I(X)$ é de fato um ideal. Deixamos a cargo do leitor demonstrar as relações entre a variedade de um ideal e o ideal de uma variedade dadas abaixo. Observe que estas relações justificam a discussão sobre as pontes entre a Álgebra e a Geometria.

i) $I(V(J)) \supseteq J$ para todo ideal $J \subset \mathbb{K}[\mathbf{X}]$.

ii) $V(I(X)) \supseteq X$ para todo subconjunto $X \subset \mathbb{K}^n$.

iii) $V(I(V(J))) = V(J)$ para todo ideal $J \subset \mathbb{K}[\mathbf{X}]$.

Agora vamos caminhar em direção a enunciar um dos teoremas principais do dicionário Álgebra-Geometria. Para isto precisamos da seguinte definição:

Definição 1.4 *O* ***radical de um ideal*** $I \subset \mathbb{K}[\boldsymbol{X}]$ *é o conjunto:*

$$\sqrt{I} = rad(I) := \{f \in \mathbb{K}[\boldsymbol{X}] : f^n \in I \text{ para algum } n \in \mathbb{Z}_+\}.$$

E dizemos que I *é um* ***ideal radical*** *se* $I = \sqrt{I}$.

Temos que o radical de um ideal I também é um ideal que satisfaz as propriedades $I \subseteq \sqrt{I}$ e $\sqrt{\sqrt{I}} = \sqrt{I}$. Como $\mathbb{K}$ é um corpo e todo corpo é um domínio de integridade, obtemos que o ideal $I(X)$ é radical para todo subconjunto $X \subset \mathbb{K}^n$. Vamos enunciar o famoso teorema de Hilbert:

Teorema 1.3 (Nullstelensatz.) *Seja* $\mathbb{K}$ *um corpo algebricamente fechado. Então para todo ideal* $J \subset \mathbb{K}[x_1, \ldots, x_n]$ *temos que* $I(V(J)) = \sqrt{J}$.

Demonstração. Veja [4] cap. 1, seção 1.7.

■

As definições desta seção e o teorema de Hilbert constituem a porta de entrada para a Geometria Algébrica clássica. Na seção seguinte veremos uma outra teoria que possui diversas aplicações na Geometria Algébrica e também na Álgebra Comutativa.

1.3 Bases de Gröbner

As chamadas bases de Gröbner surgiram na tese de Doutorado do matemático Alemão Bruno Buchberger, ver [1], cujo assunto foi resolver o problema que seu orientador de doutorado, Gröbner, estudava a mais de vinte anos. O problema era o seguinte: dado um ideal não nulo $I \subset \mathbb{K}[x_1, \ldots, x_n]$ encontrar uma base para o quociente $\mathbb{K}[x_1, \ldots, x_n]/I$ como um K-espaço vetorial. Durante o caminho Burchberger definiu as bases de Gröbner que possui as mais diversas aplicações, e inclusive foi um avanço científico significativo no ramo da ciência da computação. Nesta seção discutiremos brevemente tal teoria, para mais detalhes indicamos o capítulo 2 do livro [3].

1.3.1 Ordens Monomiais

Se observarmos com cuidado o algoritmo da divisão entre polinômios do anel $\mathbb{K}[x]$ vamos perceber que é crucial escrever os polinômios da maior potência de x para a menor. Ou seja, é crucial ordenar os termos dos polinômios de $\mathbb{K}[x]$ e fazemos tal ordenação pelo expoente de x. Para anéis de polinômios em geral não é tão simples, de fato, qual monômio é maior, x_1^3 ou x_2^3 em $\mathbb{K}[x_1, x_2]$? Por este motivo começamos com a seguinte definição:

Definição 1.5 *Uma ordem monomial em $\mathbb{K}[x_1, \cdots, x_n]$ é uma relação $\prec$ em $\mathbb{N}^n$ (ou equivalentemente, uma relação sobre o conjunto dos monômios X^α onde $\alpha \in \mathbb{N}^n$), satisfazendo:*

i) $\prec$ *é uma relação de ordem total em* $\mathbb{N}^n$.

ii) Se $\alpha \prec \beta$, *então* $\alpha + \gamma \prec \beta + \gamma$, *para todos* $\alpha,\ \beta$ *e* $\gamma \in \mathbb{N}^n$.

iii) $\prec$ *é uma boa ordem, isto é, todo subconjunto não vazio de* $\mathbb{N}^n$ *tem elemento mínimo com relação a ordem* $\prec$.

Como vamos trabalhar muito no conjunto $\mathbb{N}^n$, definimos o **grau** de um elemento $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, denotado por $|\alpha|$, pela equação $|\alpha| = \alpha_1 + \cdots + \alpha_n$. Definimos também o **grau** de um monômio $X^\alpha \in \mathbb{K}[x_1, \ldots, x_n]$ como sendo o natural $\deg(X^\alpha) = |\alpha|$.

Há três ordens monomiais que são bem conhecidas:

Definição 1.6 (Ordem Lexicográfica) *Sejam $\alpha = (\alpha_1, \cdots, \alpha_n)$ e $\beta = (\beta_1, \cdots, \beta_n) \in \mathbb{N}^n$. Dizemos que $\alpha >_{lex} \beta$ se na diferença vetorial $\alpha - \beta \in \mathbb{Z}^n$, a primeira coordenada não nula lendo da esquerda para a direita é positiva. Essa é a* ***ordem lexicográfica clássica*** *onde consideramos as variáveis ordenadas da forma $x_1 >_{lex} x_2 >_{lex} \cdots >_{lex} x_n$. Podemos trocar a ordem das variáveis e obter outras ordens lexicográficas.*

Definição 1.7 (Ordem Lexicográfica Graduada) *Sejam $\alpha,\ \beta \in \mathbb{N}^n$. Dizemos que $\alpha >_{glex} \beta$ se $|\alpha| > |\beta|$ ou $|\alpha| = |\beta|$ e $\alpha >_{lex} \beta$. Ou seja, primeiro olhamos para o grau dos monômios e, caso os dois possuam o mesmo grau, utilizamos a ordem lexicográfica para "desempatar".*

Definição 1.8 (Ordem Lexicográfica Graduada Reversa) *Sejam $\alpha,\ \beta \in \mathbb{N}^n$. Dizemos que $\alpha >_{grevlex} \beta$ se $|\alpha| > |\beta|$ ou $|\alpha| = |\beta|$ e a primeira coordenada não nula de $\alpha - \beta$ lendo da direita para a esquerda é negativa.*

Não demonstraremos que estas três definições satisfazem as condições para serem ordens monomiais. Tais provas podem ser encontradas na referência [3]. Vamos denotar uma ordem monomial qualquer por $\prec$ e caso haja necessidade de alguma ordem monomial específica diremos no enunciado do resultado.

Uma grande vantagem de utilizar ordens monomiais é o fato de existir um algoritmo da divisão. Para enunciar tal algoritmo precisamos de mais uma definição.

Definição 1.9 *Seja $f = \sum_\alpha a_\alpha X^\alpha \neq 0$ um polinômio em $\mathbb{K}[\boldsymbol{X}]$ e seja $\prec$ uma ordem monomial. Definimos*

i) O ***multigrau*** *de f como sendo a n-upla $mdeg(f) = \max_\prec\{\alpha \in \mathbb{N}^n : a_\alpha \neq 0\}$ com relação a ordem monomial $\prec$.*

ii) O ***coeficiente líder*** *de f como sendo a constante $LC(f) = a_{mdeg(f)} \in \mathbb{K}$.*

iii) O ***monômio líder*** *de f como sendo o monômio $LM(f) = X^{mdeg(f)}$.*

iv) O ***termo líder*** *de f como sendo o termo $LT(f) = LC(f) \cdot LM(f)$.*

O maior problema na hora de estabelecer um algoritmo da divisão em $\mathbb{K}[x_1, \ldots, x_n]$ é saber como definir o resto da divisão. Em $\mathbb{K}[x]$, a divisão termina quando o termo líder do divisor possui grau maior que o dividendo. Seguindo por este caminho obtemos:

Teorema 1.4 (Algoritmo da divisão em $\mathbb{K}[\mathbf{X}]$) *Sejam $f_1, \cdots, f_s$ polinômios ordenados em $\mathbb{K}[x_1, \cdots, x_n]$. Então, todo polinômio $f \in \mathbb{K}[x_1, \cdots, x_n]$ pode ser escrito como*

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

*onde $a_1, \ldots, a_s, r \in \mathbb{K}[x_1, \cdots, x_n]$ e $r = 0$ ou r é uma combinação linear de monômios de tal forma que nenhum dos termos de r é divisível por $LT(f_1), \cdots, LT(f_s)$. Seja $F = \{f_i : i = 1, \ldots s\}$, chamaremos r de **resto** da divisão de f por F. Além disso, se $a_i f_i \neq 0$, então $mdeg(f) \succ mdeg(a_i f_i)$.*

Demonstração.

A demonstração deste teorema é longa e a explicação de como utilizar o algoritmo também, por este motivo não faremos neste trabalho. Para ler a demonstração e obter mais detalhes sobre o algoritmo veja teorema 2.3.3 de [3].

■

Uma pergunta que surge naturalmente é: quais propriedades o algoritmo da divisão em $\mathbb{K}[x_1, \cdots, x_n]$ possui? Por exemplo, em $\mathbb{K}[x]$ o resto é único, mas infelizmente o resto em $\mathbb{K}[\mathbf{X}]$ não possui esta propriedade.

Exemplo: Dividindo o polinômio $f = x^2y + xy^2 + y^2 \in \mathbb{R}[x, y]$ por $f_1 = xy - 1$ e $f_2 = y^2 - 1$ obtemos que

$$f = (x + y)(xy - 1) + (y^2 - 1) + (x + y + 1),$$

logo $r_1 = x + y + 1$. Por outro lado, invertendo a ordem dos divisores e refazendo a divisão obtemos que

$$f = (x + 1)(y^2 - 1) + x(xy - 1) + (2x + 1)$$

onde $r_2 = 2x + 1 \neq x + y + 1 = r_1$.

Portanto concluímos que a ordem dos divisores pode alterar o resto, e também que normalmente o resto não é único. As bases de Gröbner resolvem este problema como veremos adiante.

1.3.2 Ideais Monomiais

Definição 1.10 *Um ideal $I \subset \mathbb{K}[\boldsymbol{X}]$ é chamado de **ideal monomial** se I possui um conjunto gerador de monômios. Em outras palavras, existe um conjunto de expoentes $A \subset \mathbb{N}^n$ (não necessariamente finito) tal que*

$$I = \langle \{X^\alpha : \alpha \in A\} \rangle.$$

Os ideais monomiais tem uma propriedade muito boa: seja $I = \langle X^\alpha : \alpha \in A \subset \mathbb{N}^n \rangle$ um ideal monomial. Então o monômio $X^\beta \in I$ se, e só se, $X^\alpha \mid X^\beta$ para algum $\alpha \in A$.

Definição 1.11 *Seja $\{0\} \neq I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal.*

i) Definimos o conjunto $LT(I) := \{cX^\alpha \in \mathbb{K}[\boldsymbol{X}] : \exists f \in I \text{ e } LT(f) = cX^\alpha\}$.

*ii) Denotamos por $\langle LT(I) \rangle$ o ideal gerado pelos elementos de $LT(I)$ chamado de **ideal de termos líderes** de I.*

Por definição temos que $\langle LT(I) \rangle$ é um ideal monomial. Além disso, se $I = \langle f_1, \cdots, f_r \rangle \subset \mathbb{K}[\mathbf{X}]$, então temos que $\langle LT(f_1), \cdots, LT(f_r) \rangle \subset \langle LT(I) \rangle$ pois cada $LT(f_i) \in LT(I)$ mas em geral não é uma igualdade. Vejamos o exemplo abaixo.

Exemplo: Considere $I = \langle f_1, f_2 \rangle$ onde $f_1 = x^3 - 2xy$ e $f_2 = x^2y - 2y^2 + x$. Vamos utilizar a ordem lexicográfica graduada em $K[x, y]$. Veja que $x \cdot (x^2y - 2y^2 + x) - y(x^3 - 2xy) = x^2 \in I$, logo $LT(x^2) = x^2 \in \langle LT(I) \rangle$ mas x^2 não é divisível por $LT(f_1) = x^3$ tão pouco por $LT(f_2) = x^2y$, ou seja, $x^2 \notin \langle LT(f_1), LT(f_2) \rangle$.

Definição 1.12 *Seja $0 \subsetneqq I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal. Um subconjunto finito $G = \{g_1, \cdots, g_r\} \subset I$ é chamado de **base de Gröbner** de I (ou base padrão) se satisfaz a igualdade*

$$\langle LT(I) \rangle = \langle LT(g_1), \cdots, LT(g_r) \rangle.$$

Segue da definição que um subconjunto $\{g_1, \cdots, g_r\} \subset I$ é uma base de Gröbner se, e somente se, para qualquer $f \in I$, existe $1 \leq i \leq r$ tal que $LT(g_i) \mid LT(f)$. E segue diretamente do teorema da base de Hilbert e do algoritmo da divisão a seguinte proposição:

Proposição 1.1 *Todo ideal $I \subset K[X]$ não nulo possui uma base de Gröbner quando fixada uma ordem monomial. Além disso, qualquer base de Gröbner de um ideal I é um conjunto gerador de I.*

Demonstração .

Do teorema da base de Hilbert segue que o ideal $\langle LT(I) \rangle$ possui um conjunto finito de geradores. Pela definição de $LT(I)$ encontramos elementos cujos termos líderes geram $\langle LT(I) \rangle$ e aplicando o algoritmo da divisão mostramos que estes elementos geram I.

■

A força da teoria das bases de Gröbner está nas suas propriedades extremamente úteis. As bases de Gröbner possuem diversas aplicações, principalmente na Álgebra Comutativa, na Geometria Algébrica e na Ciência da Computação. Vejamos algumas destas propriedades:

Proposição 1.2 *Seja $G = \{g_1, \cdots, g_m\}$ uma base de Gröbner para o ideal $I \subset \mathbb{K}[\boldsymbol{X}]$ e seja $f \in \mathbb{K}[\boldsymbol{X}]$ um polinômio qualquer. Então existe um único polinômio $r \in \mathbb{K}[\boldsymbol{X}]$ com as seguintes propriedades:*

i) Nenhum termo de r é divisível por $LT(g_i)$ para todo $i = 1, \cdots, m$.

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

Em particular, r é o resto na divisão de f por G não importando a ordem dos elementos $g_i \in G$ na divisão. Ou seja, o resto é único.

Demonstração.

Pelo algoritmo da divisão obtemos que $f = a_1g_1 + \cdots + a_mg_m + r$ onde r satisfaz a condição [i]. Tomando $g = a_1g_1 + \cdots a_mg_m$ temos que $g \in I$ e $f = g + r$. Logo existe um resto r satisfazendo [i] e [ii], resta provar que tal resto é único. Suponha que existem $g' \in I$ e $r' \in \mathbb{K}[\mathbf{X}]$ tais que $f = g + r = g' + r'$, então $r - r' = g' - g \in I$. Como G é base de Gröbner, segue que $LT(r - r') \in \langle LT(g_i) : i = 1, \cdots, m \rangle$ o que acontece se, e somente se, $r - r' = 0$ uma vez que vale a propriedade [i] para r e r'. Portanto $r = r'$.

■

O resto r também é chamado de **forma normal** de f com relação a I e, além disso, uma base de Gröbner também pode ser caracterizada pela propriedade do resto único. No entanto, mesmo que o resto r seja único, os coeficientes a_i da divisão podem ser diferentes quando mudamos a ordem dos divisores g_i. Terminamos esta seção com uma das melhores propriedades das bases de Gröbner:

Corolário 1.1 *Seja $G = \{g_1, \cdots, g_m\}$ uma base de Gröbner para o ideal $I \subset K[X]$. Então $f \in I$ se, e somente se, o resto de f na divisão por G é zero.*

Demonstração.
Consequência direta da proposição anterior.

■

1.4 Decomposição Primária

Primeiramente vamos definir o que é uma variedade algébrica irredutível e um ideal irredutível. Em seguida demonstraremos que todo ideal em $\mathbb{K}[x_1, \ldots, x_n]$, onde $\mathbb{K}$ é um corpo, possui decomposição em irredutíveis não necessariamente única. Além disso, toda variedade também possui decomposição em irredutíveis, a qual é única a menos de permutação. Em busca de unicidade para a decomposição de ideais, vamos demonstrar que todo ideal possui uma decomposição primária não redundante que é única. Concluímos a seção explorando a relação entre a decomposição primária não redundante de um ideal e a decomposição irredutível de uma variedade.

1.4.1 Ideais e Variedades Irredutíveis

A decomposição primária de ideais aparece naturalmente em anéis bem conhecidos! Para dar um bom exemplo precisamos primeiro definir o produto de ideais:

Definição 1.13 *Sejam R um anel e $I, J \subset R$ ideais de R. Definimos o **ideal produto** de I e J por*

$$IJ = \left\{ \sum_{i=1}^{m} a_i b_i \in R : 0 < m \in \mathbb{N} \text{ e } a_i \in I, b_i \in J \ \forall i \in \{1, \ldots, m\} \right\}.$$

Não é difícil ver que IJ é um ideal de R. Além disso, fixamos a notação $I^k = \underbrace{II \cdots I}_{k produtos}$.

Vamos começar com um exemplo pra motivar a decomposição primária. Nos inteiros sabemos que, como $360 = 2^3 \cdot 5 \cdot 3^2$, então

$$\langle 360 \rangle = (\langle 2 \rangle)^3 \cap \langle 5 \rangle \cap (\langle 3 \rangle)^2.$$

Outro caso onde uma decomposição similar ocorre é o seguinte: seja $I = \langle f \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ onde a decomposição de f em irredutíveis é $f = f_1^{r_1} \cdots f_m^{r_m}$. Então

$$I = (\langle f_1 \rangle)^{r_1} \cap \cdots \cap (\langle f_m \rangle)^{r_m}.$$

As decomposições acima são muito práticas e são utilizadas de várias maneiras e em várias teorias. Infelizmente a decomposição utilizando os elementos irredutíveis nem sempre é possível. Por esta razão precisamos de uma teoria mais geral para decompor ideais.

Definição 1.14 *Um ideal $I \subset R$ é **redutível** se pode ser escrito como interseção de dois ideais maiores de R. Isto é, $I = J_1 \cap J_2$ tais que $I \subsetneq J_1,\ J_2$. Se I não é redutível, dizemos que I é **irredutível**.*

Para obter exemplos temos a seguinte proposição (é muito bom quando a teoria funciona como nos inteiros):

Proposição 1.3 *Todo ideal primo é irredutível.*

Demonstração.
Seja $I \subset R$ um ideal primo. Sejam $J_1,\ J_2 \subset R$ ideais tais que $I = J_1 \cap J_2$. Suponha que $I \neq J_1$, então existe $f \in J_1 \backslash I$ tal que para todo $g \in J_2$ temos que $fg \in J_1 \cap J_2 = I$. Como I é primo e $f \notin I$, $g \in I$ para todo $g \in J_2$. Portanto $I = J_2$.

■

Definição 1.15 *Seja $V \subset \mathbb{A}^n(\mathbb{K})$ uma variedade algébrica. Se existem subvariedades $V_1,\ V_2 \subsetneqq V$ tais que $V = V_1 \cup V_2$, então dizemos que V é uma variedade* ***redutível****. Caso contrário, dizemos que V é* ***irredutível****.*

Será que há uma relação entre a irredutibilidade de uma variedade e a irredutibilidade de um ideal ? A resposta é sim, e para demonstrar esta relação precisamos do seguinte lema:

Lema 1.1 *Seja $V = V_1 \cup V_2 \subset \mathbb{A}^n(\mathbb{K})$ uma união de variedades. Então*

$$I(V) = I(V_1 \cup V_2) = I(V_1) \cap I(V_2).$$

Demonstração.
Se $f \in I(V)$, então $f(P) = 0$ para todo $P \in V$, em particular, como $V_1, V_2 \subset V$, temos que $f \in I(V_1) \cap I(V_2)$. Por outro lado, se $f \in I(V_1) \cap I(V_2)$, então para todo $P \in V_1 \cup V_2$ temos que $f(P) = 0$, ou seja, $f \in I(V)$.

■

Teorema 1.5 (Relação entre Variedades e Ideais Irredutíveis.) *i) Se $V \subset \mathbb{A}^n(\mathbb{K})$ é uma variedade algébrica irredutível, então $I(V)$ é um ideal primo.*

ii) Se $V \subset \mathbb{A}^n(\mathbb{K})$ é uma variedade irredutível, então o ideal $I(V)$ é irredutível.

iii) Se $I \subset \mathbb{K}[x_1, \ldots, x_n]$ é irredutível, então $V(I)$ é irredutível.

Demonstração.
[i)] Suponha que $I(V)$ não seja um ideal primo, então existem $f_1, f_2 \in \mathbb{K}[\mathbf{X}] \backslash I(V)$ tais que $f_1 f_2 \in I(V)$. Considere as variedades $V(f_1), V(f_2) \subset \mathbb{A}^n(\mathbb{K})$. Temos que $V \cap V(f_i) \subsetneqq V$ para $i = 1, 2$. De fato, se $V \cap V(f_i) = V$, então $V \subset V(f_i)$ donde $f_i(P) = 0$ para todo $P \in V$, ou seja, $f_i \in I(V)$ o que é um absurdo. Agora vejamos que

$$V = (V \cap V(f_1)) \cup (V \cap V(f_2)).$$

É claro que $(V \cap V(f_1)) \cup (V \cap V(f_2)) \subset V$. Seja $P \in V$, então $f_1 f_2(P) = 0$ já que $f_1 f_2 \in I(V)$. Como $\mathbb{K}$ é um corpo, temos que $f_1(P) = 0$ ou $f_2(P) = 0$, ou seja $P \in V(f_1)$ ou $P \in V(f_2)$ o que implica que $P \in (V \cap V(f_1)) \cup (V \cap V(f_2))$. Portanto V é redutível.

[ii)] Se $V \subset \mathbb{A}^n(\mathbb{K})$ irredutível, então $I(V)$ é um ideal primo e, pela proposição anterior, todo ideal primo é irredutível.

[iii)] Seja $I \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal e suponha que $V(I) \subset \mathbb{A}^n(\mathbb{K})$ seja redutível, isto é, existem variedades $V_1,\ V_2 \subsetneqq V$ tais que $V(I) = V_1 \cup V_2$. Daí,

$$I \subset I(V(I)) = I(V_1) \cap I(V_2).$$

Como $\mathbb{K}[x_1,\ldots,x_n]$ é noetheriano, temos que $\langle (I(V_1)\cap I(V_2))\backslash I\rangle = \langle y_1,\ldots,y_m\rangle$ onde $m\in\mathbb{N}$ e $y_j\in\mathbb{K}[x_1,\ldots,x_n]$ para todo $j\in\{1,\ldots,m\}$. Completando os geradores podemos escrever

$$I(V_1)=\langle y_1,\ldots,y_m,\ w_{m+1},\ldots,w_r\rangle \text{ e } I(V_2)=\langle y_1,\ldots,y_m,z_{m+1},\ldots,z_s\rangle$$

onde $r,\ s\in\mathbb{N}$ e $w_{m+1},\ldots,w_r,\ z_{m+1},\ldots,\ z_s\in\mathbb{K}[x_1,\ldots,x_n]$. Definindo os ideais $J_1=\langle w_{m+1},\ldots,w_r\rangle$ e $J_2=\langle z_{m+1},\ldots,z_s\rangle$ obtemos que $I=J_1\cap J_2$ onde $I\subsetneqq J_1,\ J_2$ e $J_1\neq J_2$ pois $V_1\neq V_2$. Portanto I é redutível.

■

Agora vejamos alguns exemplos não triviais!

Exemplo: Vejamos que $I=\langle xy,y^2\rangle\subset\mathbb{K}[x,y]$ é redutível.

De fato, vamos provar que $I=\langle y\rangle\cap\langle x,y^2\rangle$. Primeiramente, pelos geradores de I é claro que $I\subset\langle y\rangle\cap\langle x,y^2\rangle$. Por outro lado, se $z\in\langle y\rangle\cap\langle x,y^2\rangle$, então existem $h,\ g\in\mathbb{K}[x,y]$ tais que $z=hx+gy^2$ e como $z\in\langle y\rangle$ temos que $y\mid h$. Logo existe $h_2\in\mathbb{K}[x,y]$ tal que $h=h_2y$ e daí $z=h_2(xy)+gy^2\in I$.

Vejamos que $\langle y\rangle$ e $\langle x,y^2\rangle$ são irredutíveis. Como y é irredutível, $\langle y\rangle$ é um ideal primo e portanto irredutível. A irredutibilidade de $\langle x,y^2\rangle$, que não é primo, não será tão simples. Suponha que existam $J_1,\ J_2\in\mathbb{K}[x,y]$ ideais tais que $\langle x,y^2\rangle=J_1\cap J_2$ onde $\langle x,y^2\rangle\subsetneqq J_1,\ J_2$. Então, para $i=1,2$, vale $\dim(\mathbb{K}[x,y]/J_i)<\dim(\mathbb{K}[x,y]/\langle x,y^2\rangle)=2$ como $\mathbb{K}$-espaços vetoriais. Portanto devemos ter que $\dim(\mathbb{K}[x,y]/J_1)=\dim(\mathbb{K}[x,y]/J_2)=1$, ou seja, J_1 e J_2 são ideais maximais que contém $\langle x,y^2\rangle$. Agora observe que a única possibilidade é $J_1=\langle x,y\rangle=J_2$ o que é uma contradição. Portanto $\langle x,y^2\rangle$ é um ideal irredutível.

Exemplo: A decomposição em irredutíveis não é única. Seja $I=\langle x^2,xy,y^2\rangle\subset\mathbb{K}[x,y]$. Deixamos a cargo do leitor demonstrar que

$$I=\langle x^2,y\rangle\cap\langle x,y^2\rangle=\langle x+y,x^2\rangle\cap\langle x,y^2\rangle$$

onde $\langle x^2,y\rangle,\langle x,y^2\rangle,\langle y+x,x^2\rangle,\langle x,y^2\rangle$ são irredutíveis.

Nem sempre um ideal possui decomposição em irredutíveis. A condição que necessitamos para que exista tal decomposição é o anel ser noetheriano.

Proposição 1.4 *Seja R um anel noetheriano. Todo ideal $I\subset R$ pode ser escrito como $I=I_1\cap I_2\cap\cdots\cap I_m$. onde $m\in\mathbb{N}$ e cada I_j é irredutível. Dizemos que a decomposição é* ***fracamente não redundante*** *se nenhum dos I_j pode ser removido, isto é, $I_j\not\supseteq I_1\cap\cdots\cap I_{j-1}\cap I_{j+1}\cap\cdots\cap I_m$.*

Demonstração.

Se $I\subset R$ é um ideal irredutível, então fazemos $m=1$ e $I=I_1$ e problema resolvido. Se $I\subset R$ é um ideal redutível, então existem ideais $I_1,J_1\subset R$ tais que $I\subsetneqq I_1,\ I\subsetneqq J_1$ e $I=I_1\cap J_1$. Se I_1 e J_1 são irredutíveis terminamos a demonstração, se não, suponha sem perda de generalidade que I_1 é redutível, então existem ideais $I_2,J_2\subset R$ tais que $I_1\subsetneqq I_2,\ I_1\subsetneqq J_2$ e $I_1=I_2\cap J_2$. Se nunca obtemos uma escrita como interseção de irredutíveis para I, então continuando com este processo iremos obter uma cadeia ascendente de ideais

$$I\subsetneqq I_1\subsetneqq I_2\subsetneqq\cdots\subsetneqq I_n\subsetneqq\cdots$$

onde $I=I_1\cap J_1,\ I\subsetneqq I_1,\ J_1$ e $I_j=I_{j+1}\cap J_{j+1}$ com $I_J\subsetneqq I_{j+1},\ J_{j+1}$. Dessa forma obtemos uma cadeia ascendente de ideais que não estaciona. Portanto, R não é noetheriano.

■

Temos um resultado semelhante para variedades:

Teorema 1.6 *Seja $V \subset \mathbb{A}^n(\mathbb{K})$ uma variedade. Então podemos escrever $V = V_1 \cup V_2 \cup \cdots \cup V_r$ onde $r \in \mathbb{N}$ e cada V_j é uma variedade irredutível. Se essa escrita é não redundante, isto é, $V_i \nsubseteq V_j$ para todo $i \neq j$, então a decomposição é única a menos de permutação. Os V_j com $j \in \{1, \ldots, r\}$ são chamados de componentes irredutíveis de V.*

Demonstração.

[Existência] De modo semelhante a proposição anterior, suponha que $V \subset \mathbb{A}^n(\mathbb{K})$ é uma variedade redutível que não pode ser escrita como no enunciado, então obtemos uma cadeia descendente de variedades

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq \cdots \supsetneq V_n \supsetneq \cdots .$$

que nunca termina. Tomando os ideais de tais variedades obtemos uma cadeia de ideais

$$I(V) \subsetneqq I(V_1) \subsetneqq I(V_2) \subsetneqq \cdots \subsetneqq I(V_n) \subsetneqq \cdots$$

que nunca estaciona, o que significa que $\mathbb{K}[x_1, \ldots, x_n]$ não é noetheriano. Absurdo. Portanto existem variedades irredutíveis $V_1, \ldots, V_r \subset \mathbb{K}^n$ tais que $V = V_1 \cup \cdots \cup V_r$.

[Unicidade] Suponha que temos duas representações

$$V = V_1 \cup \cdots \cup V_r = V_1' \cup \cdots \cup V_s'$$

onde $V_i \nsubseteq V_j$ e $V_i' \nsubseteq V_j'$ para todo $i \neq j$. Daí,

$$V_1 = V \cap V_1 = \bigcup_{i=1}^{s} (V_1 \cap V_i')$$

e como V_1 é irredutível temos que $V_1 = V_1 \cap V_m'$ donde $V_1 \subset V_m'$ para algum $m \in \{1, \ldots, s\}$. Por outro lado, $V_m' = V \cap V_m'$ e repetindo o argumento obtemos que existe um $l \in \{1, \ldots, r\}$ tal que $V_m' \subset V_l$. Por hipótese, $V_i \nsubseteq V_l$ se $i \neq l$, portanto $V_1 \subset V_m' \subset V_1$, ou seja, $V_1 = V_m'$. Reproduzindo o argumento um número finito de vezes obtemos a unicidade da decomposição em irredutíveis de uma variedade.

■

Mesmo que a decomposição para variedades em irredutíveis seja única, infelizmente já vimos que para ideais essa decomposição em irredutíveis não é necessariamente única. Nosso objetivo nesta seção será encontrar condições para que haja unicidade na decomposição de ideais.

1.4.2 Ideais Quociente

Definição 1.16 *Dados ideais $I, J \subset R$, definimos o **ideal quociente** de I por J pela igualdade*

$$(I : J) := \{r \in R : rJ \subset I\}.$$

É fácil verificar que $(I : J)$ é de fato um ideal. Observe ainda que para quaisquer ideais $I, J, K \subset R$ vale $IJ \subset K$ se, e somente se, $I \subset (K : J)$. Esta propriedade justifica a escolha do nome.

Agora vejamos algumas relações entre ideais quociente e o dicionário Álgebra-Geometria.

Proposição 1.5 *Dados dois ideais $I,\ J \subset \mathbb{K}[x_1,\ldots,x_n]$ e duas variedades $V,\ W$ temos que:*

i) $(I:J) \subset I(V(I)\backslash V(J))$.

ii) $(I(V):I(W)) = I(V\backslash W)$.

Demonstração.

[i] Sejam $r \in (I:J)$ e $P \in V(I)\backslash V(J)$. Então existe $f \in J$ tal que $f(P) \neq 0$. Temos que $rf \in I$ e $f(P) \neq 0$. Então $rf(P) = r(P)f(P) = 0$, pois $P \in V(I)$. Logo $r(P) = 0$ donde $r \in I(V(I)\backslash V(J))$.

[ii] Seja $r \in (I(V) : I(W))$. Para cada $P \in V\backslash W$ existe um polinômio $g \in I(W)$ tal que $g(P) \neq 0$ (caso não existisse tal polinômio g, então $P \in V(I(W)) = W$ o que é uma contradição). Por hipótese, $rg \in I(V)$, então $rg(P) = 0$ e portanto $r(P) = 0$. Logo $r \in I(V\backslash W)$.

Por outro lado, dado $r \in I(V\backslash W)$ e $f \in I(W)$ temos dois casos possíveis para $P \in V$:

$$\begin{cases} P \in V\backslash W \ \Rightarrow r(P) = 0 \Rightarrow rf(P) = 0, \\ P \in V \cap W \Rightarrow f(P) = 0 \Rightarrow rf(P) = 0. \end{cases}$$

Consequentemente $rf \in I(V)$ para todo $f \in I(W)$, ou seja, $r \in (I(V) : I(W))$.

■

Vejamos agora uma maneira de calcular o ideal quociente $(I:J)$ a partir dos geradores da interseção $I \cap J$.

Proposição 1.6 *Sejam $I \subset \mathbb{K}[x_1,\ldots,x_n]$ um ideal e $g \in \mathbb{K}[x_1,\ldots,x_n]$ um polinômio. Se $I \cap \langle g\rangle = \langle h_1,\ldots,h_s\rangle$, então*

$$(I:\langle g\rangle) = \left\langle \frac{h_1}{g}, \cdots, \frac{h_s}{g} \right\rangle.$$

Em geral, se $J = \langle g_1,\ldots,g_r\rangle \subset \mathbb{K}[x_1,\ldots,x_n]$ é um ideal, temos que

$$(I:J) = (I:\langle g_1\rangle) \cap \cdots \cap (I:\langle g_r\rangle).$$

Demonstração.

Como cada $h_i/g \in (I:\langle g\rangle)$ a inclusão contrária é direta. Agora dado $f \in (I:\langle g\rangle)$, temos por definição que $fg \in I$, logo $fg \in I \cap \langle g\rangle$. Então existem $a_1,\ldots,a_s \in \mathbb{K}[\mathbf{X}]$ tais que $fg = a_1h_1 + \cdots + a_sh_s$. Como g divide cada h_i, segue que $f = \frac{a_1h_1}{g} + \cdots + \frac{a_sh_s}{g} \in \langle h_1/g,\ldots,h_s/g\rangle$.

Para o caso geral em que $J = \langle g_1,\ldots,g_r\rangle$, a inclusão $(I:\langle g_1\rangle) \cap \cdots \cap (I:\langle g_r\rangle) \subset (I:J)$ é direta e a inclusão contraria segue de

$$\begin{aligned} f \in (I:J) \ &\Rightarrow fg \in I,\ \forall g \in J \\ &\Rightarrow fg_i \in I,\ \forall i \in \{1,\ldots,r\} \\ &\Rightarrow f \in (I:\langle g_i\rangle),\ \forall i \in \{1,\ldots,r\} \\ &\Rightarrow f \in (I:\langle g_1\rangle) \cap \cdots \cap (I:\langle g_r\rangle). \end{aligned}$$

■

1.4.3 Decomposição Primária

Definição 1.17 *Um ideal I em um anel R é chamado de **primário** se, para todo par de elementos $f, g \in R$ tais que $fg \in I$ vale $f \in I$ ou $g^m \in I$ para algum inteiro positivo m.*

Da definição obtemos que se $Q \subset R$ é um ideal primário, então seu radical $\sqrt{Q}$ é um ideal primo, chamado de **primo associado** a Q. Façamos alguns exemplos!

Exemplo: Seja $f \in \mathbb{K}[\mathbf{X}]$ um irredutível. Então $P = \langle f \rangle$ é um ideal primo e para todo $0 < m \in \mathbb{N}$ o ideal P^m é primário.

Proposição 1.7 *Sejam $\mathcal{M} = \langle x_1, \ldots, x_n \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ e $I \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal tal que $\mathcal{M}^k \subset I$ para algum $0 < k \in \mathbb{N}$. Então I é primário.*

Demonstração.

Suponha que existam $f,\ g \in \mathbb{K}[\mathbf{X}]$ tais que $fg \in I$ e $g^m \notin I$ para todo $0 < m \in \mathbb{N}$. Então $g^m \notin \mathcal{M}$ para todo $0 < m \in \mathbb{N}$ pois caso contrário $g^{mk} \in I$. Devemos provar que $f \in I$. Com este intuito primeiro definimos:

$$\begin{array}{rccc} \mu_g : & \frac{\mathbb{K}[\mathbf{X}]}{\mathcal{M}^k} & \longrightarrow & \frac{\mathbb{K}[\mathbf{X}]}{\mathcal{M}^k} \\ & h + \mathcal{M}^k & \longmapsto & hg + \mathcal{M}^k \end{array}.$$

Deixamos a cargo do leitor demonstrar que μ_g está bem definida e é um homomorfismo de $\mathbb{K}$-espaços vetoriais. Provemos que μ_g é injetor. Como $g \notin \mathcal{M}$, $g(0, \ldots, 0) \neq 0$ e assim, dado $h \in \mathbb{K}[\mathbf{X}] \backslash \mathcal{M}^k$ temos que $h(0, \ldots, 0) \neq 0$ e a expansão de Taylor de h ao redor da origem é da forma

$$h = h_d + \texttt{ termos de ordem maior},\ h_d \neq 0$$

consequentemente a expansão de gh é da foma

$$gh = g(0, \ldots, 0)h_d + \texttt{ termos de ordem maior},$$

onde o primeiro termo $g(0, \ldots, 0)h_d \neq 0$. Portanto $hg \notin \mathcal{M}^k$, ou seja, μ_g é injetora. E como dimensão de $\mathbb{K}[\mathbf{X}] \backslash \mathcal{M}^k$ é finita, μ_g também é sobrejetora.

Seja $\overline{I} = \{h + \mathcal{M}^k : h \in I\}$. Veja que se $h + \mathcal{M}^k \in \overline{I}$, então $hg + \mathcal{M}^k \in \overline{I}$, pois $hg \in I$. Logo $\mu_g(\overline{I}) \subset \overline{I}$. Como μ_g é sobrejetora, devemos ter que $\mu_g(\overline{I}) = \overline{I}$. Assim, se $h + \mathcal{M}^k \notin \overline{I}$, então $hg + \mathcal{M}^k \notin \overline{I}$. Portanto $fg \in I$ implica que $\mu_g(f + \mathcal{M}^k) \in \overline{I}$, ou seja, $f + \mathcal{M}^k \in \overline{I}$. Mas por hipótese $\mathcal{M}^k \subset I$, então $f \in I$.

■

Exemplo: Em $\mathbb{Z}$ é fácil perceber que os ideais $\{0\}$ e $\langle p^m \rangle$ são primários onde $p \in \mathbb{Z}$ é um número primo e m um inteiro positivo. Mas nem sempre os ideais primários são potências de primos. De fato, o ideal $Q = \langle x,\ y^2 \rangle \subset \mathbb{K}[x, y]$ é primário e temos que $\sqrt{Q} = \langle x,\ y \rangle = P$ que é um ideal primo. No entanto, $P^2 \neq Q$ e ainda vale $P^2 \subsetneq Q \subsetneq P$. Logo Q não pode ser potência de P.

Exemplo: E também nem toda potência de um ideal primo é primária. Considere o ideal

$$P = \langle AD - B^2, AF - C^2, DF - E^2, AE - BC, BE - CD, BF - CE \rangle \subset \mathbb{K}[A, B, C, D, E, F].$$

O ideal P^2 não é primário. Para uma demonstração deste fato ver capítulo de decomposição primária de [6].

Agora veremos uma caracterização dos ideais primários e uma aplicação do primo associado! Para isto definimos:

Definição 1.18 *Sejam $I \subset R$ um ideal e $a \in R$ um elemento qualquer. Dizemos que a é um* ***divisor de zero*** *em R se existe um elemento $0 \neq b \in R$ tal que $a \cdot b = 0$. Caso contrário, dizemos que a é um elemento* ***regular****.*

Agora observe que se $I \subset \mathbb{K}[\mathbf{X}]$ é um ideal e $f \in \mathbb{K}[\mathbf{X}]$ um polinômio. Por abuso de notação, diremos que f é um **divisor de zero** em $\mathbb{K}[\mathbf{X}]/I$ se existe um elemento $g \in \mathbb{K}[\mathbf{X}]\backslash I$ $(I \neq \overline{g})$ tal que $fg \in I$ $(\overline{fg} = I)$.

Proposição 1.8 *Um ideal $I \subset R$ é primário se, e somente se, cada divisor de zero do quociente é nilpotente. Além disso, quando I é primário, um elemento de R/I é divisor de zero se, e somente se, é a imagem de um elemento do ideal primo associado $P = \sqrt{I}$ pelo homomorfismo canônico e tal elemento não está em I.*

Demonstração.

Suponha que I seja um ideal primário. Dado um divisor de zero $\overline{f} \in R/I$, temos que $f \notin I$ e existe um elemento $g \in R\backslash I$ tal que $gf \in I$. Como $g \notin I$ e I é primário, temos que $f^m \in I$ para algum $1 < m \in \mathbb{N}$, ou seja, $\overline{f}$ é nilpotente em R/I. Suponha agora que todo divisor de zero de R/I seja nilpotente. Seja $f \in R\backslash I$ um divisor de zero, então existe $g \in R\backslash I$ tal que $fg \in I$. Assim g também é um divisor de zero em R/I, o que implica que $\overline{g}$ é nilpotente em R/I, ou seja, existe $1 < m \in \mathbb{N}$ tal que $g^m \in I$. Portanto I é primário.

Vejamos a segunda equivalência. Sejam $I \subset R$ um ideal primário e $\pi : R \longrightarrow R/I$ o homomorfismo canônico. Seja $\overline{f}$ um divisor de zero em R/I, então pela equivalência anterior existe $1 < m \notin \mathbb{N}$ tal que $f^m \in I$. Segue que $f \in P = \sqrt{I}$ e $\pi(f) = \overline{f}$. Por outro lado, suponha que $I \neq \overline{f} = \pi(f)$ para algum elemento $f \in P\backslash I$. Como $P = \sqrt{I}$, existe $1 < m \in \mathbb{N}$ tal que $f^m \in I$, consequentemente $\pi(f^m) = \overline{f}^m = I$, ou seja, $\overline{f}$ é nilpotente. Pela primeira equivalência que demonstramos, $\overline{f}$ é um divisor de zero em R/I.

■

Daqui em diante estaremos considerando que o anel R é noetheriano, comutativo e com unidade.

Proposição 1.9 *Todo ideal irredutível de R é primário.*

Demonstração.

Suponha que $I \subset R$ seja um ideal irredutível e tome elementos $f,\ g \in R$ tais que $fg \in I$. Começamos considerando a sequência de ideais

$$I \subset (I : \langle g \rangle) \subset (I : \langle g^2 \rangle) \subset \cdots \subset (I : \langle g^m \rangle) \subset \cdots .$$

Como R é noetheriano, existe $N \in \mathbb{N}$ tal que $(I : \langle g^N \rangle) = (I : \langle g^{N+k} \rangle)$ para todo $k \in \mathbb{N}$. Vamos provar que

$$(I + \langle g^N \rangle) \cap (I + \langle f \rangle) = I.$$

É fácil ver que I está contido nesta interseção. Por outro lado, seja $h \in (I+\langle g^N \rangle) \cap (I+\langle f \rangle)$, então existem $y,\ z \in I$ e $a,\ b \in R$ tais que $h = y + ag^N = z + bf$. Multiplicando esta igualdade por g obtemos que

$$hg = yg + ag^{N+1} = \underbrace{zg}_{\in I} + \underbrace{b(fg)}_{\in I},$$

ou seja, $hg \in I$. Além disso, da igualdade segue que $ag^{N+1} = zg + b(fg) - yg \in I$. E como $(I : \langle g^N \rangle) = (I : \langle g^{N+1} \rangle)$, segue que

$$\begin{cases} r \in (I : \langle g^N \rangle) \Longleftrightarrow rg^N \in I \\ r \in (I : \langle g^{N+1} \rangle) \Longleftrightarrow rg^{N+1} \in I \end{cases} \overbrace{\Longrightarrow}^{(I:\langle g^N \rangle)=(I:\langle g^{N+1} \rangle)} (rg^N \in I \Longleftrightarrow rg^{N+1} \in I).$$

Assim, $ag^{N+1} \in I$ implica que $ag^N \in I$ e consequentemente $h = y + ag^N \in I$. Portanto $(I + \langle g^N \rangle) \cap (I + \langle f \rangle) = I$. No entanto, I é irredutível por hipótese, então devemos ter que $I = I + \langle g^N \rangle$ ou $I = I + \langle f \rangle$. Em outras palavras, I é primário.

■

Finalmente com esta proposição obtemos que:

Teorema 1.7 (Teorema da Decomposição Primária:) *Dado um ideal $I \subset R$ podemos escrever I da forma $I = Q_1 \cap \cdots \cap Q_r$ onde cada Q_j é um ideal primário. Esta escrita é chamada de* ***decomposição primária*** *de I.*

Demonstração.
É uma combinação das proposições 1.4 e 1.9.

■

Da mesma maneira como fizemos para os irredutíveis no início desta seção temos que: se nenhum dos Q_j é desnecessário na decomposição de I, então diremos que a decomposição primária é **fracamente não redundante**. Nessas condições, os ideais primos do conjunto $Ass(I) = \{\sqrt{Q_1}, \ldots, \sqrt{Q_r}\}$ são chamados de primos associados de I. No caso em que I é primário, temos que $Ass(I) = \{\sqrt{I}\}$. Infelizmente nem mesmo essa decomposição é única.

Exemplo: Considere $I = \langle x^2,\ xy \rangle \subset \mathbb{R}[x, y]$. Temos que I pode ser escrito como interseção de ideais primários de duas maneiras diferentes:

$$I = \langle x \rangle \cap \langle y,\ x^2 \rangle = Q_1 \cap Q_2 \text{ e } I = \langle x \rangle \cap \langle y^2,\ x^2,\ xy \rangle = Q_1 \cap Q_2'.$$

Note que $Q_1 = P_1$ é um ideal primo, Q_2 e Q_2' são primários pela proposição 1.7 e observe também que $Q_2' \nsubseteq Q_2$ e $Q_2' \not\supseteq Q_2$. No entanto, temos que $P_2 = \sqrt{Q_2} = \sqrt{Q_2'} = \langle x, y \rangle$. Isto é, Q_2 e Q_2' possuem o mesmo primo associado. Portanto investigar os primos associados pode nos levar à tão desejada unicidade.

Uma boa aplicação da decomposição primária de um ideal é a seguinte:

Exemplo: Vamos dar uma aplicação da relação ideal-variedade utilizando as decomposições. Seja $I = \langle xz - y^2,\ z - xy \rangle \subset \mathbb{R}[x, y, z]$ um ideal, vamos determinar $V(I)$ utilizando a decomposição primária de I. Observe que :

$$I = \langle xz - y^2,\ z - xy,\ y - x^2 \rangle \cap \langle y,\ z \rangle = \langle z - xy,\ y - x^2 \rangle \cap \langle y,\ z \rangle = Q_1 \cap Q_2.$$

Note que Q_1 e Q_2 são primos. De fato, Q_1 consiste nas equações que se anulam na imagem do morfismo $\phi : \mathbb{R} \longrightarrow \mathbb{R}^3$ dado por $\phi(t) = (t, t^2, t^3) = V(Q)$ que é irredutível e portanto Q_1 é primo. Dessa forma, $V(I)$ é exatamente $V(Q_1) \cup V(Q_2)$, ou seja $V(I) = Img(\phi) \cup \{(x, 0, 0) \in \mathbb{R}^3 : x \in \mathbb{R}\}$.

1.4.4 Unicidade da Decomposição Primária

Em busca da unicidade vamos primeiramente determinar a natureza dos primos associados de um ideal I. Para isto precisamos do seguinte lema:

Lema 1.2 *Sejam $P \subset R$ um ideal primo e $I_1, \ldots, I_m \subset R$ ideais.*

i) Se $\bigcap_{j=1}^m I_j \subset P$, então existe $i \in \{1, \ldots, m\}$ tal que $I_i \subset P$.

ii) Em particular, se $P = \bigcap_{j=1}^{m} I_j$, *então* $P = I_i$ *para algum* $i \in \{1, \ldots, s\}$.

Demonstração.

[i)] Suponha que $I_j \nsubseteq P$ para todo $1 \leq j \leq m$. Então é possível escolher elementos $g_j \in I_j \backslash P$ tais que $g = g_1 \cdots g_m \in P$ e nenhum elemento deste produto está em P, logo P não é primo o que é uma contradição. Portanto existe $i \in \{1, \ldots, m\}$ tal que $I_i \subset P$.

[ii)] Primeiramente observe que, como $P = \bigcap_{j=1}^{m} I_j$, então $P \subset I_j$ para todo j. Por outro lado, pelo item i), existe um $i \in \{1, \ldots, m\}$ tal que $I_i \subset P$. Portanto $P = I_i$.

■

Teorema 1.8 *Seja* $I \subset R$ *um ideal com decomposição primária fracamente não redundante* $I = Q_1 \cap \cdots \cap Q_r$. *Então os primos associados de* I *são exatamente aqueles ideais primos que podem ser escritos da forma*

$$P = \sqrt{(I : \langle f \rangle)}$$

para algum elemento $f \in R$. *Em particular, os primos associados são unicamente determinados por* I.

Demonstração.

Já demonstramos que

$$(I : \langle f \rangle) = (Q_1 : \langle f \rangle) \cap \cdots \cap (Q_r : \langle f \rangle).$$

Vamos demonstrar agora que

$$\sqrt{(I : \langle f \rangle)} = \sqrt{(Q_1 : \langle f \rangle)} \cap \cdots \cap \sqrt{(Q_r : \langle f \rangle)}.$$

Seja $g \in \sqrt{(I : \langle f \rangle)}$. Então $g^m \in (I : \langle f \rangle)$ para algum $0 < m \in \mathbb{N}$, consequentemente $g^m \in (Q_i : \langle f \rangle)$ para todo $i \in \{1, \ldots, r\}$, ou seja, $g \in \sqrt{(Q_i : \langle f \rangle)}$ para todo i. Portanto $g \in \sqrt{(Q_1 : \langle f \rangle)} \cap \cdots \cap \sqrt{(Q_r : \langle f \rangle)}$. Por outro lado, dado $g \in \sqrt{(Q_1 : \langle f \rangle)} \cap \cdots \cap \sqrt{(Q_r : \langle f \rangle)}$ existem inteiros positivos $m_1, \ldots, m_r$ tais que $g^{m_i} \in (Q_i : \langle f \rangle)$ para todo $i \in \{1, \ldots, r\}$. Tomando $m = \max\{m_1, \ldots, m_r\}$ obtemos que $g^m \in (Q_i : \langle f \rangle)$ para todo i, ou seja, $(g^m \in I : \langle f \rangle)$ e portanto $g \in \sqrt{(I : \langle f \rangle)}$.

Agora observe que: caso $f \in Q_i$, então $(Q_i : \langle f \rangle) = \sqrt{(Q_i : \langle f \rangle)} = R$, entretanto, se $f \notin Q_i$, então $(Q_i : \langle f \rangle) = \{r \in R : rf \in Q_i\}$ é o conjunto dos divisores de zero em R/Q_i unido com Q_i. Pela caracterização dos ideais primários (proposição 1.8) temos que $\sqrt{(Q_i : \langle f \rangle)} = P_i$.

Assim, como a decomposição primária $I = \bigcap_{i=1}^{r} Q_i$ é fracamente não redundante, existe $f_j \notin Q_j$ tal que $f_j \in \bigcap_{i \neq j} Q_i$. Logo $f_j \notin I$ e pela observação acima segue que

$$\sqrt{(I : \langle f_j \rangle)} = R \cap \cdots R \cap P_j \cap R \cap \cdots \cap R = P_j.$$

Portanto os primos associados de I são escrito da maneira que queríamos.

Resta provar que se um ideal primo pode ser escrito como o radical do quociente de I por algum elemento f de R, então este ideal é um primo associado de I. Seja $P = \sqrt{(I : \langle f \rangle)}$ um ideal primo para algum elemento $f \in R$. Segue que $P = \sqrt{(Q_i : \langle f \rangle)} \cap \cdots \cap \sqrt{(Q_r : \langle f \rangle)}$, então existem índices $i_1, \ldots, i_s \in \{1, \ldots, r\}$ tais que $P = P_{i_1} \cap \cdots \cap P_{i_s}$. Como P é primo, pelo lema anterior $P = P_{i_l}$ para algum $i_l \in \{i_i, \ldots, i_s\}$, ou seja, P é um primo associado de I.

■

É um fato relativamente bem conhecido que o radical de um ideal I é a interseção de todos os ideais primos que contém I. Vamos demonstrar que não precisam ser todos os ideais primos, é suficiente fazer a interseção dos primos associados de uma decomposição primária fracamente não redundante.

Corolário 1.2 *Seja $I \subset R$ um ideal com decomposição primária fracamente redundante $I = Q_1 \cap \cdots \cap Q_r$. Sejam $P_j = \sqrt{Q_j}$ os primos associados de I, $j = 1, \ldots, r$. Então $\sqrt{I} = \bigcap_{j=1}^{r} P_j$.*

Demonstração.

Na demonstração do teorema anterior, provamos que dado $f \in R$ temos que

$$\sqrt{(I : \langle f \rangle)} = \sqrt{(Q_1 : \langle f \rangle)} \cap \cdots \cap \sqrt{(Q_r : \langle f \rangle)}.$$

Em particular, como R é um anel noetheriano, comutativo e com unidade, escolhemos $f = 1$ e como $(J : R) = (J : \langle 1 \rangle) = \{g \in R : g \cdot 1 \in J\} = J$ obtemos que

$$\sqrt{I} = \sqrt{(I : \langle 1 \rangle)} = \sqrt{(Q_1 : \langle 1 \rangle)} \cap \cdots \cap \sqrt{(Q_r : \langle 1 \rangle)} = \bigcap_{i=1}^{r} \sqrt{Q_i} = \bigcap_{i=1}^{r} P_i.$$

■

Estamos quase conseguindo nossa querida unicidade. Precisamos ainda melhorar nosso conhecimento sobre os ideais primários na decomposição de I.

Definição 1.19 *Seja $I \subset R$ um ideal. Um ideal primo P associado a I é chamado de* ***minimal*** *se não contém nenhum dos outros primos associados de I. Caso contrário, dizemos que P é* ***mergulhado****.*

A importância desta definição fica evidente com o seguinte resultado:

Proposição 1.10 *Sejam $Q_1,\ Q_2 \subset R$ ideais primários tais que $\sqrt{Q_1} = P_1 \subset \sqrt{Q_2} = P_2$. Então $Q_1 \cap Q_2$ é um ideal primário e $\sqrt{Q_1 \cap Q_2} = P_1$.*

Demonstração.

Sejam $f,\ g \in R$ tais que $fg \in Q_1 \cap Q_2$. Se $f \in Q_1 \cap Q_2$ não precisamos fazer nada, se não, então $f \notin Q_1 \cap Q_2$ implica que $f \notin Q_1$ ou $f \notin Q_2$. Suponha, sem perda de generalidade, que $f \notin Q_1$. Nesse caso, como Q_1 é primário e $fg \in Q_1$, então $g^m \in Q_1$ para algum $0 < m \in \mathbb{N}$ e daí $g \in P_1$, mas $P_1 \subset P_2 = \sqrt{Q_2}$, logo existe $0 < k \in \mathbb{N}$ tal que $g^k \in Q_2$. Tomando $M = \max\{m, k\}$ temos que $g^M \in Q_1 \cap Q_2$ e portanto $Q_1 \cap Q_2$ é primário.

Vejamos que $\sqrt{Q_1 \cap Q_2} = P_1$. Como $Q_1 \cap Q_2 \subset Q_1$, temos que $\sqrt{Q_1 \cap Q_2} \subset \sqrt{Q_1} = P_1$. Por outro lado, dado $f \in P_1$, como $P_1 \subset P_2$, existem inteiros positivos m_1 e m_2 tais que $g^{m_1} \in Q_1$ e $g^{m_2} \in Q_2$, logo $g^M \in Q_1 \cap Q_2$ onde $M = \max\{m_1,\ m_2\}$. Portanto $g \in \sqrt{Q_1 \cap Q_2}$.

■

Esta proposição nos fornece o caminho para a tão sonhada unicidade. Primeiramente observe que, se $I \subset R$ é um ideal com decomposição primária fracamente não redundante dada por $I = Q_1 \cap \cdots \cap Q_r$ onde Q_1 e Q_2 satisfazem $P_1 = \sqrt{Q_1} \subset \sqrt{Q_2} = P_2$, então tomamos $Q' = Q_1 \cap Q_2$ e temos que $I = Q' \cap Q_3 \cap \cdots \cap Q_r$ também é uma decomposição primária fracamente não redundante de I mas nesta decomposição temos um primo mergulhado de I a menos que na decomposição anterior. Esta propriedade é o que nos permite fazer a seguinte definição:

Definição 1.20 *Uma decomposição primária de um ideal é* ***(fortemente) não redundante*** *se é fracamente não redundante e nenhum dos primos associados está contido em outro (em outras palavras, minimais). Isto é, $P_i \nsubseteq P_j$ para todo $i \neq j$.*

Nós já demonstramos que os primos associados de I são unicamente determinados por I. Agora vamos demonstrar que os ideais primários de uma decomposição não redundante são determinados pelos primos associados.

Teorema 1.9 *Seja $I \subset R$ um ideal com decomposição primária não redundante $I = Q_1 \cap \cdots \cap Q_r$. Para todo $j \in \{1, \ldots, r\}$ temos que se P_j é um primo associado minimal, então existe um elemento $a \in \bigcap_{i \neq j} P_i$ tal que $a \notin P_j$ e*

$$Q_j = \bigcup_{m=1}^{\infty} (I : \langle a^m \rangle).$$

Este resultado irá implicar que a decomposição primária não redundante é única.

Demonstração.

Primeiramente observe que se $\bigcap_{i \neq j} P_i \subset P_j$, então pelo lema anterior segue que $P_i \subset P_j$ para algum $i \neq j$ o que não ocorre porque a decomposição primária é não redundante. Além disso, é claro que $P_j \nsubseteq \bigcap_{i \neq j} P_i$. Então podemos tomar um elemento $a \in \bigcap_{i \neq j} P_i$ tal que $a \notin P_j$. Provemos que

$$Q_j = \bigcup_{m=1}^{\infty} (I : \langle a^m \rangle).$$

Dado $x \in Q_j$, como $a \in \bigcap_{i \neq j} P_i$, existem inteiros positivos $m_1, \ldots, m_{j-1}, m_{j+1}, \ldots, m_r$ tais que $a^{m_i} \in Q_i$ para todo $i \neq j$. Tomando $M = max\{m_i : i \neq j\}$ temos que $xa^M \in Q_i$ para todo $i \in \{1, \ldots, r\}$, ou seja, $xa^M \in I$ o que significa que $x \in (I : \langle a^M \rangle)$.

Por outro lado, se $x \in \bigcup_{m=1}^{\infty} (I : \langle a^m \rangle)$, então existe $m \in \mathbb{Z}$ tal que $x \in (I : \langle a^m \rangle)$, logo $xa^m \in I$ e portanto $xa^m \in Q_j$. Mas Q_j é primário e $a \notin P_j$ o que significa que $a^k \notin Q_j$ para todo inteiro positivo k, assim devemos ter que $x \in Q_j$.

■

Pela proposição anterior a decomposição primária não redundante de um ideal existe e, além disso, possui a propriedade que desejamos, a nossa tão sonhada unicidade:

Teorema 1.10 *Seja $I \subset R$ um ideal. A decomposição primária não redundante de I existe e é única.*

Demonstração.

Falta apenas demonstrar que a decomposição primária não redundante de I é única. O primeiro passo é provar que os primos associados são finitos e nenhum deles é desnecessário. Sejam $I = Q_1 \cap \cdots \cap Q_m$ e $I = Q'_1 \cap \cdots \cap Q'_r$ duas decomposições primárias não redundantes de I. Pelo corolário 1.2 segue que

$$\sqrt{I} = P_1 \cap \cdots \cap P_m = P'_1 \cap \cdots \cap P'_r$$

onde $P_i = \sqrt{Q_i}$ para todo $i \in \{1, \ldots, m\}$ e $P'_j = \sqrt{Q'_j}$ para todo $j \in \{1, \ldots, r\}$. Em particular, $\bigcap_{i=1}^{m} P_i \subset P'_1$, então pelo lema 1.2 existe um $l \in \{1, \ldots, m\}$ tal que $P_l \subset P'_1$. Mas P'_1 é um primo associado minimal, portanto devemos ter que $P'_1 = P_l$. Retirando P_l e P'_1 obtemos que

$$P_1 \cap \cdots \cap P_{l-1} \cap P_{l+1} \cap \cdots \cap P_m = \bigcap_{j=2}^{r} P'_j.$$

Podemos repetir o processo que fizemos e demonstrar que $P_2' = P_k$ para algum $k \in \{1, \ldots, l-1, l+1, \ldots, m\}$. Como as interseções são finitas, repetindo este processo obteremos que $m = r$ e para todo $j \in \{1, \ldots, r\}$ existe $i \in \{1, \ldots, m\}$ tal que $P_i = P_j'$, ou seja, os primos associados minimais são únicos.

No segundo passo vamos demonstrar que os ideais primários são únicos. De fato, dado $k_1 \in \{1, \ldots, m\}$ existe $k_2 \in \{1, \ldots, r\}$ tais que $P_{k_1} = P_{k_2}'$. Pelo teorema anterior, existe um elemento $a \in \bigcap_{i \neq k_1} P_i = \bigcap_{j \neq k_2} P_j'$ tal que $a \notin P_{k_1} = P_{k_2}'$ e valem

$$Q_{k_1} = \bigcup_{i=1}^{\infty} (I : \langle a^i \rangle) \text{ e } Q_{k_2}' = \bigcup_{i=1}^{\infty} (I : \langle a^i \rangle).$$

Portanto $Q_{k_1} = Q_{k_2}'$ e a decomposição primária não redundante é única.

■

A primeira aplicação que faremos da decomposição primária não redundante de um dado ideal $I \subset R$ é continuar com o trabalho de identificar os divisores de zero do quociente R/I. Generalizando o que fizemos na proposição 1.8 obtemos o teorema:

Teorema 1.11 *Se $I \subset \mathbb{K}[\boldsymbol{X}]$ é um ideal com decomposição primária não redundante $I = Q_1 \cap \cdots \cap Q_m$, sabemos que os primos associados de I são os ideais $P_i = \sqrt{Q_i}$. Nessas condições,*

$$\bigcup_{i=1}^{m} (P_i + I).$$

é o conjunto dos divisores de zero de $\mathbb{K}[\boldsymbol{X}]/I$.

Demonstração.

Seja x um divisor de zero de $\mathbb{K}[\mathbf{X}]/I$, então existe $0 \neq \overline{y} \in \mathbb{K}[\mathbf{X}]/I$ tal que $\overline{y} \cdot \overline{x} = 0$, ou seja, $yx \in I = \bigcap_{i=1}^{m} Q_i$. Daí, como $y \notin I$, existe pelo menos um natural $j \in \{1, \ldots, m\}$ tal que $y \notin Q_j$ donde $x^\alpha \in Q_j$ para algum $\alpha \in \mathbb{N}$, pois Q_j é um ideal primário. Consequentemente, $x \in \sqrt{Q_j} = P_j$.

Por outro lado, dado $\overline{x} \in \bigcup_{i=1}^{m} (P_i + I)$, $x \in P_j$ para algum $j \in \{1, \ldots, m\}$. Seja β o menor natural tal que $x^\beta \in Q_j$. Como a decomposição é não redundante, $Q_j \not\supseteq \bigcap_{i \neq j} Q_i$ e os primos associados são minimais, então existe $y \in \bigcap_{i \neq j} Q_i$ tal que $y \notin P_j \supset Q_j$. Segue que $y \notin I$ e $x^\beta y \in Q_i$ para todo $i \in \{1, \ldots, m\}$ e daí $\overline{x} \cdot (\overline{x^{\beta-1} y}) = 0$ onde $\overline{x^{\beta-1} y} \neq 0$. De fato, como β é a menor potência tal que $x^\beta \in Q_j$, temos que $x^{\beta-1} \notin Q_j$ e como $y \notin P_j$ segue que $y^\gamma \notin Q_j$ para todo $\gamma \in \mathbb{N}$ o que significa que $x^{\beta-1} y \notin Q_j$, ou seja, $x^{\beta-1} y \notin I$. Portanto x é um divisor de zero em $\mathbb{K}[\mathbf{X}]/I$.

■

Finalmente, podemos explorar a relação entre a decomposição primária de um ideal e a decomposição em irredutíveis de uma variedade. Seja $V = V_1 \cup \cdots \cup V_r \subset \mathbb{A}^n(\mathbb{K})$ uma variedade escrita na sua decomposição em irredutíveis. Então, $I(V) = I(V_1) \cap \cdots \cap I(V_r)$ onde cada $I(V_j)$ é um ideal primo e irredutível, além disso, $I(V_i) \neq I(V_j)$ se $i \neq j$. Em outras palavras, o ideal de cada componente irredutível de V é um primo associado de $I(V)$.

Por outro lado, se $I = Q_1 \cap \cdots \cap Q_r \subset \mathbb{K}[x_1, \ldots, x_n]$ é um ideal na sua decomposição primária não redundante, então a decomposição em irredutíveis de sua variedade associada é $V(I) = V(Q_1) \cup \cdots \cup V(Q_r)$ e temos que $I \subset I(V(I)) = I(V(Q_1)) \cap \cdots \cap I(V(Q_r))$ onde cada $I(V(Q_j))$ é um ideal primo e irredutível. Além disso, $\sqrt{Q_i} \subset I(V(Q_i))$, ou seja, o primo associado minimal $P_i = \sqrt{Q_i}$ está contido em $I(V(Q_i))$ e, caso $\mathbb{K}$ seja um corpo algebricamente

fechado, então pelo Nullstelensatz, vale a igualdade $P_i = \sqrt{Q_i} = I(V(Q_i))$, em outras palavras, os ideais $I(V(Q_i))$ são os primos minimais de I.

Para finalizar, ainda no caso em que $\mathbb{K}$ é algebricamente fechado, temos que $I(V(I)) = \sqrt{I} = \sqrt{Q_1} \cap \cdots \cap \sqrt{Q_r}$, isto é, já temos a decomposição primária de $I(V(I))$ a partir da decomposição primária de I.

Exemplo: Seja $I = \langle x^2, xy \rangle \subset \mathbb{R}[x, y]$, vamos determinar as componentes irredutíveis de $V(I)$. Temos que $I = \langle x \rangle \cap \langle x^2,\ y \rangle = Q_1 \cap Q_2$. Temos que Q_1 é um ideal primo e Q_2 é um ideal primário. Os primos associados de I são $P_1 = Q_1$ e $P_2 = \langle x,\ y \rangle$ e, como $P_1 \subsetneqq P_2$, o único primo minimal de I é P_1. Portanto, $V(I) = V(x) = \{(0, y) \in \mathbb{R}^2 : y \in \mathbb{R}\}$.

1.5 A Dimensão de Krull e a Altura de um Ideal

1.5.1 Dimensão de Krull

Seja M um conjunto de conjuntos. Uma **cadeia** em M é um subconjunto $\mathcal{C} \subset M$ que é totalmente ordenado com a inclusão. O **comprimento** de $\mathcal{C}$ é definido como

$$length(\mathcal{C}) := |\mathcal{C}| - 1 \in \mathbb{N} \cup \{-1, \infty\}.$$

E denotaremos uma cadeia de comprimento n por $\mathcal{C} = \{X_0 \subsetneqq X_1 \subsetneqq \cdots \subsetneqq X_n\}$. Definimos também o comprimento de M como

$$length(M) := \sup\{length(\mathcal{C}) : \mathcal{C} \subset M \text{ é uma cadeia}\}.$$

Definição 1.21 *Sejam X um espaço topológico e $F \subset X$ um subconjunto fechado. Dizemos que F é **irredutível** se F não pode ser escrito como união de dois fechados próprios. Isto é, se $F_1,\ F_2 \subset F$ são fechados tais que $F = F_1 \cup F_2$, então $F = F_1$ ou $F = F_2$.*

Vejamos um exemplo que motivará nossa definição de dimensão de Krull:

Exemplo: Sejam V um $\mathbb{K}$-espaço vetorial e M o subconjunto de todos os $\mathbb{K}$-subespaços vetoriais de V. Então podemos escrever:

$$\begin{aligned} \dim_{\mathbb{K}}(V) &= \sup\{\dim_{\mathbb{K}}(H) : H \text{ é } \mathbb{K}\text{-subespaço vetorial de } V\} \\ &= \sup\{length(\mathcal{C}) : \mathcal{C} \text{ é uma cadeia em } M\} \\ &= length(M). \end{aligned}$$

Definição 1.22 (Dimensão de Krull.) *a) Sejam X um espaço topológico e M o conjunto de todos os fechados irredutíveis de X. A **dimensão de Krull** de X é definida por $\dim(X) := length(M)$. Se $F \subset X$ é um fechado, então a dimensão de Krull de F é o comprimento da maior cadeia de fechados irredutíveis contida em F.*

b) Seja R um anel. Como os fechados irredutíveis de R na topologia de Zariski são os ideais primos, então definimos a dimensão de Krull de R como sendo o valor $\dim(R) = length(Spec(R))$. Em particular, dado um ideal $I \subset R$, definimos a dimensão de Krull de I como sendo o comprimento da maior cadeia de ideais primos contida em I.

c) Seja $\mathbb{K}$ um corpo. A dimensão de um subconjunto fechado $X \subset \mathbb{K}^n$ pela topologia de Zariski é o comprimento da maior cadeia de variedades irredutíveis contida em X. Como toda variedade $V \subset \mathbb{K}^n$ é um conjunto fechado, definimos a dimensão de Krull de V como sendo a maior cadeia de variedades irredutíveis contida em V.

Caso não haja possibilidade de confusão iremos nos referir a dimensão de Krull simplesmente por dimensão.

Exemplos:

1) Todo corpo tem dimensão de Krull zero.

2) Como as cadeias de ideais primos de $\mathbb{Z}$ são da forma $\{0\} \subsetneqq \langle p \rangle \subsetneqq \mathbb{Z}$ para algum número primo $p \in \mathbb{Z}$, então $\dim(\mathbb{Z}) = 2 - 1 = 1$.

3) Seja R um anel noetheriano. Não é difícil demonstrar que $\dim(R[x_1, \ldots, x_n]) = \dim(R) + n$.

4) Seja $R = \mathbb{K}[x_1, \ldots, x_n, \ldots]$ o anel dos polinômios em infinitas variáveis sobre $\mathbb{K}$. Como

$$\{0\} \subsetneqq \langle x_1 \rangle \subsetneqq \langle x_1, x_2 \rangle \subsetneqq \cdots \subsetneqq \langle x_1, \ldots, x_n \rangle \subsetneqq \cdots$$

é uma cadeia em R, então $\dim(R) = \infty$.

Pela definição poderiamos pensar que dado um anel R temos que R é noetheriano se, e somente se, $\dim(R) < \infty$. No entanto, ambas as implicações são falsas! O fato de trabalharmos apenas com cadeias de ideais primos não é o suficiente para garantir tal equivalência. Para encontrar os contra-exemplos das implicações consulte exemplo 2.3 e exercício 5.3 de [7].

1.5.2 Altura de um Ideal

Um outro conceito que está relacionado com comprimento de cadeias é a ideia de altura de um ideal. Não entraremos em muitos detalhes sobre o assunto, para mais informações consultar [7] e [9].

Definição 1.23 *Sejam R um anel e $P \subset R$ um ideal primo. Definimos a* ***altura*** *de P como sendo o comprimento da maior cadeia de ideais primos contida em P que termina em P. Isto é,*

$$ht(P) := sup\{length(\mathcal{C}) : \mathcal{C} = \{P_0 \subsetneqq P_1 \subsetneqq \cdots \subsetneqq P_n = P\} \text{ é uma cadeia de ideais primos}\}$$

Se o ideal $I \subset R$ não é primo, como definiremos a altura de I? Definiremos como sendo a altura do primo "mais próximo"de I.

Definição 1.24 *Seja $I \subset R$ um ideal. A* ***altura*** *de I é definida como sendo o valor*

$$ht(I) = \min\{ht(P) : I \subset P,\ P \in Spec(R)\}.$$

Em geral, $\dim(R/I) + ht(I) \leq \dim(R)$ valendo a igualdade em diversos casos. A diferença $\dim(R) - \dim(R/I) := codim(I)$ é chamada de **codimensão** de I. Para mais detalhes sobre este assunto consultar Capítulo 6 de [7]. Além disso, utilizaremos o seguinte resultado:

Proposição 1.11 *Seja $P \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal primo. Então vale a igualdade*

$$ht(P) + \dim(\mathbb{K}[\boldsymbol{X}]/P) = n = dim(\mathbb{K}[\boldsymbol{X}]).$$

Demonstração.
Corolário 1 página 218 de [9].

■

Com esta proposição iremos concluir a seção com a prova de um resultado que utilizaremos em algumas demonstrações adiante.

Teorema 1.12 *Seja $\mathbb{K}$ um corpo. Para todo ideal $I \subset \mathbb{K}[x_1, \dots x_n]$ vale a igualdade*

$$ht(I) + \dim(\mathbb{K}[\boldsymbol{X}]/I) = n.$$

Demonstração.

Seja $P \subset \mathbb{K}[\mathbf{X}]$ um ideal primo minimal de I tal que $ht(I) = ht(P)$. Então existem ideais primos $P_1, \dots, P_{ht(P)} = P$, $Q_0 = P, Q_1, \dots, Q_{\dim(\mathbb{K}[\mathbf{X}]/P)} \subset \mathbb{K}[\mathbf{X}]$ tais que

$$\langle 0 \rangle \subsetneqq P_1 \subsetneqq \cdots \subsetneqq P_{ht(P)} = P = Q_0 \subsetneqq Q_1 \subsetneqq \cdots \subsetneqq Q_{\dim(\mathbb{K}[\mathbf{X}]/P)} = \mathbb{K}[\mathbf{X}].$$

Em particular, $P_{ht(P)-1} \subsetneqq I \subsetneqq P$ pois caso contrário teríamos $ht(I) = ht(P_{ht(P)-1})$. Daí, pela proposição anterior a cadeia de ideais primos

$$\langle 0 \rangle \subsetneqq P_1 \subsetneqq \cdots \subsetneqq P_{ht(I)-1} \subsetneqq I \subsetneqq P \subsetneqq Q_1 \subsetneqq \cdots \subsetneqq Q_{\dim(\mathbb{K}[\mathbf{X}]/P)} = \mathbb{K}[\mathbf{X}].$$

possui comprimento máximo. Logo

$$ht(P) + \dim(\mathbb{K}[\mathbf{X}]/P) = n.$$

Precisamos demonstrar ainda que $\dim(\mathbb{K}[\mathbf{X}]/I) = \dim(\mathbb{K}[\mathbf{X}]/P)$. Por um lado, como $ht(I) = ht(P)$ temos que

$$\dim(\mathbb{K}[\mathbf{X}]/I) + ht(I) \leq n \Rightarrow \dim(\mathbb{K}[\mathbf{X}]/I) \leq n - ht(P) = \dim(\mathbb{K}[\mathbf{X}]/P).$$

Por outro lado, sabemos que $I \subset P$, então no quociente obtemos que $\dim(\mathbb{K}[\mathbf{X}]/I) \geq \dim(\mathbb{K}[\mathbf{X}]/P)$. Portanto $\dim(\mathbb{K}[\mathbf{X}]/I) = \dim(\mathbb{K}[\mathbf{X}]/P)$ e

$$\dim(\mathbb{K}[\mathbf{X}]/I) + ht(I) = n.$$

■

1.6 Ideais Não Misturados

Precisaremos do conceito de ideais não misturados para obter boas cotas inferiores para as funções distância mínima. No entanto, não iremos nos aprofundar nesta teoria.

Definição 1.25 *Um ideal $I \subset R$ é **não misturado** se $ht(I) = ht(P)$ para todos os primos associados minimais P de I.*

1.7 Espaço Projetivo

O espaço projetivo é obtido através do espaço afim adicionando pontos chamados de pontos no infinito. Nesta dissertação não utilizaremos muito da geometria projetiva em si, utilizaremos apenas a definição, a transição entre o espaço afim e o espaço projetivo e dois resultados particulares. Para um estudo aprofundado do espaço projetivo recomendamos os livros [6] e [3].

Para definir o espaço projetivo n dimensional sobre $\mathbb{K}$ precisamos da seguinte relação de equivalência sobre os pontos de $\mathbb{K}^{n+1}$. Sejam $P = (x_0, \dots, x_n)$ e $P' = (x'_0, \dots, x'_n) \in \mathbb{K}^{n+1}$ dois pontos com $n+1$ coordenadas. Dizemos que P e P' estão relacionados, e denotamos $P \sim P'$, se, e somente se, existe uma constante não nula $\lambda \in \mathbb{K}$ tal que $P' = \lambda P$, isto é, $(x'_0, \dots, x'_n) = (\lambda x_0, \dots, \lambda x_n)$. Deixamos a cargo do leitor demonstrar que $\sim$ é uma relação de equivalência.

Definição 1.26 *O **espaço projetivo** n **dimensional sobre** $\mathbb{K}$, denotado por $\mathbb{P}^n(\mathbb{K})$, é o conjunto das classes de equivalência da relação $\sim$. Ou seja,*

$$\mathbb{P}^n(\mathbb{K}) = (\mathbb{K}^{n+1}\backslash\{0\})/\sim$$

*onde 0 denota o vetor nulo em $\mathbb{K}^{n+1}$. Seja $P \neq 0$ uma $(n+1)$-upla de $\mathbb{K}^{n+1}$, então P representa um ponto do espaço projetivo cuja notação é $P = (x_0 : x_1 : \cdots : x_n)$ e dizemos que $(x_0 : \ldots : x_n)$ são **coordenadas homogêneas** de P.*

Por causa da definição acima, sempre precisamos trabalhar com os chamados polinômios homogêneos quando utilizamos o espaço projetivo. Vejamos o motivo.

Definição 1.27 *Um polinômio $f \in \mathbb{K}[x_1, \cdots, x_n]$ é chamado de **polinômio homogêneo** de grau d se todos os seus termos tem grau exatamente d.*

Um exemplo simples é o polinômio $f = x^2 + xy + y^2 \in \mathbb{K}[x, y]$ homogêneo de grau dois. O motivo pelo qual precisamos trabalhar com polinômios homogêneos é o seguinte: considere o polinômio não homogêneo $f = xyz - r \in \mathbb{R}[x, y, z]$, temos que $f(r, 1, 1) = 0$ mas $f(\lambda r, \lambda, \lambda) = \lambda^3 r - r$ que é diferente de zero se $\lambda \neq 1$. No entanto, $(r, 1, 1)$ e $(\lambda r, \lambda, \lambda)$ com $\lambda \neq 0$ representam o mesmo ponto espaço projetivo $\mathbb{P}^2(\mathbb{K})$. Isto não ocorre se f for homogêneo.

Proposição 1.12 *Seja $f \in \mathbb{K}[x_0, \ldots, x_n]$ um polinômio homogêneo de grau d onde $1 \leq d \in \mathbb{N}$. Se f se anula em um representante do ponto $P \in \mathbb{P}^n(\mathbb{K})$, então f se anula em qualquer representante de P.*

Demonstração.
De fato, seja $(a_0 : \ldots : a_n) = P$ um representante de P tal que $f(a_0, \ldots, a_n) = 0$. Dado um escalar $0 \neq \lambda \in \mathbb{K}[\mathbf{X}]$ poderemos colocar λ^d em evidência na escrita de $f(\lambda a_0, \ldots, \lambda a_n)$ pois cada termo de f tem grau d e cada variável x_i será substituída por λa_i. Em outras palavras,

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

Portanto f se anula em qualquer representante do ponto $P \in \mathbb{P}^n(\mathbb{K})$.

■

Do mesmo modo que temos o dicionário Álgebra-Geometria para o espaço afim, podemos construir um dicionário Álgebra-Geometria para o espaço projetivo. Não é tão simples como no caso afim mas também não é muito complicado. Primeiro definimos um caso particular de variedades projetivas:

Definição 1.28 *Sejam $f_1, \cdots, f_m \in \mathbb{K}[x_0, \ldots, x_n]$ polinômios homogêneos. Definimos o conjunto*

$$V(f_1, \ldots, f_m) = \{(a_0 : \ldots : a_n) \in \mathbb{P}^n(\mathbb{K}) : f_i(a_0, \ldots, a_n) = 0 \ \forall 1 \leq i \leq m\}$$

*chamado de **variedade projetiva** definida por $f_1, \ldots, f_m$.*

Note que não definimos a variedade projetiva de um ideal. Isto ocorre porque não é natural, temos o problema devido aos vários representantes de um mesmo ponto. Para chegar às definições que queremos vamos definir uma passagem de $\mathbb{K}[x_1, \ldots, x_n]$ para $\mathbb{K}[x_0, x_1, \ldots, x_n]$ de modo que o resultado serão ideais apropriados.

Definição 1.29 *Seja $g \in \mathbb{K}[x_1, \ldots, x_n]$ um polinômio de grau d.*

i) Reorganizando os termos de g como polinômios homogêneos podemos escrever $g = g_d + \cdots + g_1 + g_0$ onde cada g_i é composto pelos termos de grau i de g. Estes polinômios g_i são chamados de ***componentes homogêneas*** *de g. Então*

$$g^h := g_d + g_{d-1}x_0 + g_{d-2}x_0^2 + \cdots + g_1x_0^{d-1} + g_0x_0^d$$

é um polinômio homogêneo de grau d em $\mathbb{K}[x_0, \ldots, x_n]$ chamado de ***homogeneização*** *de g.*

ii) A homogeneização de g pode ser calculada pela expressão

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

iii) A ***desomogeneização*** *de g^h é g que é obtida pela expressão $g = g^h(1, x_1, \ldots, x_n)$. Observe que o processo de desomogeneização pode ser aplicado a qualquer polinômio homogêneo de $\mathbb{K}[x_0, \ldots, x_n]$.*

iv) Seja $F \in \mathbb{K}[x_0, \ldots, x_n]$ um polinômio homogêneo e seja x_0^k a maior potência de x_0 que divide F. Se $f = F(1, x_1, \ldots, x_n)$ é a desomogeneização de F, então $F = x_0^k f^h$.

Deixamos a cargo do leitor demonstrar os detalhes das afirmações presentes na definição anterior. Uma consequência direta da definição anterior é a seguinte: seja $W = V(f_1, \ldots, f_m) \subset \mathbb{A}^n(\mathbb{K})$ uma variedade afim, então $V = V(f_1^h, \ldots, f_m^h) \subset \mathbb{P}^n(\mathbb{K})$ é uma variedade projetiva obtida através de W.

Precisamos resolver um problema sério. Um ideal gerado por polinômios homogêneos não contém apenas polinômios homogêneos porque a soma de dois polinômios homogêneos de grau diferente nunca será um polinômio homogêneo. Estes elementos de I que são polinômios não homogêneos são um problema na hora de definir $V(I)$. A solução deste problema está nas componentes homogêneas de um polinômio não homogêneo.

Definição 1.30 *Um ideal I em $\mathbb{K}[x_0, \ldots, x_n]$ é dito* ***homogêneo*** *se para cada $f \in I$, as componentes homogêneas f_i de f estão em I.*

A vantagem de se trabalhar com ideais homogêneos é o fato que estes são finitamente gerados por polinômios homogêneos (teorema 8.3.2 de [3]). Podemos então definir:

Definição 1.31 *Seja $I \subset \mathbb{K}[x_0, \ldots, x_n]$ um ideal homogêneo. Definimos a variedade projetiva de I como sendo o conjunto*

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

A variedade projetiva de I está bem definida. De fato, se $I = \langle f_1, \ldots f_m \rangle$ onde cada f_i é homogêneo, então $V(I) = V(f_1, \ldots, f_m)$ e mantemos nossa primeira definição. Para terminar o que discutiremos sobre o dicionário Álgebra-Geometria temos a seguinte proposição:

Proposição 1.13 *Seja $V \subset \mathbb{P}^n(\mathbb{K})$ uma variedade projetiva. Então o conjunto*

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

é um ideal homogêneo em $\mathbb{K}[x_0, \ldots, x_n]$. (Note que, pela escrita $(a_0 : \ldots : a_n) \in V$, f tem que anular todos os pontos P de V independente da escolha das coordenadas homogêneas de P).

Demonstração.
Proposição 8.3.4 de [3].

■

Além do que já fizemos até aqui, durante esta dissertação utilizaremos ainda mais dois resultados sobre as características do espaço projetivo.

Proposição 1.14 (Propriedades do Espaço Projetivo.) *Seja $Y = \{[\alpha], [\beta]\} \subset \mathbb{P}^n$. Então:*

i) Existe um polinômio $h \in \mathbb{K}[\boldsymbol{X}]_1$ tal que $h([\alpha]) \neq 0$ e $h([\beta]) = 0$.

ii) Para todo $1 \leq d \in \mathbb{Z}$ existe um polinômio $f \in \mathbb{K}[\boldsymbol{X}]_d$ tal que $f([\alpha]) \neq 0$ e $f([\beta]) = 0$.

iii) Se $X \subset \mathbb{P}^n$ é um subconjunto finito com $|X| \geq 2$, então para todo $1 \leq d \in \mathbb{Z}$ existe $f \in \mathbb{K}[\boldsymbol{X}]_d$ tal que $f \notin I(X)$ e $(I(X) : f) \neq I(X)$.

Demonstração.
[*i*] Como $[\alpha]$ e $[\beta]$ são distintos, temos que existem pelo menos duas variáveis dentre $x_0, x_1, \ldots, x_n$ que não anulam $[\alpha]$ e $[\beta]$ simultaneamente, ou seja, $\dim(\mathbb{K}[\mathbf{X}]_1/I(Y)_1) \geq 2$, então existem dois polinômios distintos linearmente independentes de grau 1 que não estão em $I(Y)$, logo a transformação linear de avaliação

$$\begin{array}{rccc} T: & \mathbb{K}[\mathbf{X}]_1 & \longrightarrow & \mathbb{K}^2 \\ & f & \longmapsto & (f([\alpha]), f([\beta])) \end{array}$$

satisfaz $\dim_{\mathbb{K}}(Im(T)) \geq 2$ e como $\dim(\mathbb{K}^2) = 2$ obtemos que T é uma transformação linear sobrejetora. Então existe um polinômio homogêneo $h \in \mathbb{K}[\mathbf{X}]_1$ tal que $T(h) = (1, 0)$, ou seja, $h([\alpha]) = 1 \neq 0$ e $h([\beta]) = 0$.

[*ii*] Seja h o polinômio homogêneo do item anterior. Então $h^d \in \mathbb{K}[\mathbf{X}]_d$ e $h^d([\alpha]) = 1 \neq 0$ e $h^d([\beta]) = 0$.

[*iii*] Sejam $m, d \in \mathbb{N}$ dois naturais tais que $d \geq 1$ e $m \geq 2$. Digamos que $X = \{[\alpha_1], \ldots, [\alpha_m]\}$. Pelo item anterior, existem polinômios $f_1, f_2, \ldots, f_m \in \mathbb{K}[\mathbf{X}]_d$ tais que $f_1([\alpha_1]) = 0, f_1([\alpha_2]) \neq 0$ e para todo $i \in \{2, \ldots, m\}$ valem $f_i([\alpha_1]) \neq 0$ e $f_i([\alpha_i]) = 0$. Dessa forma $f_i \notin I(X)$ para todo $1 \leq i \leq m$ mas $f_1(f_2 \cdots f_m) \in I(X)$. Então $g = f_2 \cdots f_m \in (I(X) : f)$ e $g \notin I(X)$.

■

Proposição 1.15 *Seja $X \subset \mathbb{P}^n$ um subconjunto finito do espaço projetivo. Seja $[\alpha] = (\alpha_0 : \ldots : \alpha_n) \in X$ com $\alpha_k \neq 0$ para algum $k \in \{1, \ldots, n\}$. Seja $I_{[\alpha]} \subset \mathbb{K}[x_0, \ldots, x_n]$ o ideal dos polinômios homogêneos que se anulam em $[\alpha]$. Então $I_{[\alpha]}$ é primo e valem*

$$I_{[\alpha]} = \langle \{\alpha_k x_i - \alpha_i x_k : k \neq i \in \{0, \ldots, n\}\} \rangle,$$

$\dim(\mathbb{K}[\boldsymbol{X}]/I_{[\alpha]}) = 1$, $ht(I_{[\alpha]}) = n$ *e* $I(X) = \bigcap_{[\alpha] \in X} I_{[\alpha]}$ *é uma decomposição primária do ideal de X.*

Demonstração.
Primeiramente, como $\{[\alpha]\} \subset \mathbb{P}^n$ é irredutível, então $I_{[\alpha]}$ é um ideal primo. Por um lado, como para cada $k \neq i \in \{0, \ldots, n\}$ temos que $\alpha_k x_i - \alpha_i x_k$ anula $[\alpha]$, então $\langle \{\alpha_k x_i - \alpha_i x_k : k \neq$

$i \in \{0, \ldots, n\}\}\rangle \subset I_{[\alpha]}$. Por outro lado, seja $f \in I_{[\alpha]}$. Definimos em $\mathbb{K}[\mathbf{X}]$ a ordem lexicográfica $<$ com a seguinte ordem de variáveis:

$$x_k < x_0 < x_1 < \cdots < x_{k-1} < x_{k+1} < \cdots < x_n.$$

Dessa forma, ao dividir f por $\alpha_k x_0 - \alpha_0 x_k$, obtemos dois polinômios $g_0, h \in \mathbb{K}[\mathbf{X}]$ tais que

$$f = g_0(\alpha_k x_0 - \alpha_0 x_k) + h.$$

Além disso, como $\deg(\alpha_k x_0 - \alpha_0 x_k) = 1$ e $LT(\alpha_k x_0 - \alpha_0 x_k) = \alpha_k x_0$ temos que a variável x_0 não aparece em h, isto é, $h \in \mathbb{K}[x_1, \ldots, x_n]$. Repetindo o processo para os outros geradores $\alpha_k x_i - \alpha_i x_k$ obtemos polinômios $g_1, \ldots, g_{k-1}, g_{k+1}, \ldots, g_n \in \mathbb{K}[\mathbf{X}]$ e uma constante $c \in \mathbb{K}$ tais que

$$f = g_0(\alpha_k x_0 - \alpha_0 x_k) + \cdots + g_{k-1}(\alpha_k x_{k-1} - \alpha_{k-1} x_k) + g_{k+1}(\alpha_k x_{k+1} - \alpha_{k+1} x_k) + \cdots + g_n(\alpha_k x_n - \alpha_n x_k) + c.$$

Daí,

$$0 = f([\alpha]) = g_0([\alpha]) \cdot 0 + \cdots + g_{k-1}([\alpha]) \cdot 0 + g_{k+1}([\alpha]) \cdot 0 + \cdots + g_n([\alpha]) \cdot 0 + c,$$

ou seja, $c = 0$. Portanto $f \in \langle \{\alpha_k x_i - \alpha_i x_k : k \neq i \in \{0, \ldots, n\}\}\rangle$.

Vejamos os demais detalhes. Pelos geradores de $I_{[\alpha]}$ temos que o complementar do ideal de termos líderes de $I_{[\alpha]}$ é um conjunto de constantes, logo $\dim(\mathbb{K}[\mathbf{X}]/I_{[\alpha]}) = 1$. Pelo teorema 1.12, segue que $ht(I_{[\alpha]}) = \dim(\mathbb{K}[x_0, \ldots, x_n]) - \dim(\mathbb{K}[\mathbf{X}]/I_{[\alpha]}) = n + 1 - 1 = n$.

■

Capítulo 2

Códigos Projetivos de Tipo Reed-Muller e Função Distância Mínima

Neste capítulo vamos definir os códigos projetivos de tipo Reed-Muller e estudar o seu parâmetro distância mínima. Depois vamos trabalhar as teorias de funções de Hilbert e de grau de um ideal para encontrar uma formulação algébrica para a distância mínima destes códigos.

Primeiramente vamos definir o que é um código corretor de erros. A ideia básica é construir maneiras de preparar uma mensagem de modo que ao envia-la conseguiremos obter a mensagem correta mesmo se houver erros de transmissão.

Definição 2.1 *Seja $0 \neq n \in \mathbb{N}$. Um **código corretor de erros** é um subconjunto $C \subset A^n$ onde A é um conjunto finito qualquer chamado de **alfabeto**. Os elementos de A^n são chamados de **palavras**.*

O natural n presente na definição anterior é chamado de **comprimento** do código C, isto é, o tamanho de cada palavra. E a quantidade de palavras que o código possui é chamado de **dimensão**. Há ainda um terceiro parâmetro importante em um código corretor de erros mas para explicá-lo precisamos de uma definição.

Na teoria de códigos conseguimos medir a distância entre duas palavras utilizando a métrica de Hamming:

Definição 2.2 *Sejam $u, v \in A^n$, definimos a **distância** entre u e v denotada por $d(u, v)$ como sendo o número de coordenadas não nulas do vetor $u - v$.*

Visto que C é um conjunto finito munido com uma métrica definimos o terceiro parâmetro importante de um código, a distância mínima

$$\delta(C) := \min\{d(u, v) : u, v \in C,\ u \neq v\}$$

Estamos interessados nos casos em que $A = \mathbb{K}$ é um corpo e $C \subset \mathbb{K}^n$ é um subespaço vetorial. Nesses casos, a dimensão do código C é a dimensão de C como um $\mathbb{K}$-espaço vetorial e dado $u \in C$ podemos definir a **norma de Hamming**

$$||u|| := d(u, 0)$$

como sendo o número de coordenadas não nulas do vetor. Daí

$$\delta(C) = \min\{d(u, v) : u, v \in C,\ u \neq v\} = \min\{||u-v|| : 0 \neq u-v \in C\} = \min\{||u|| : 0 \neq u \in C\}.$$

O parâmetro distância mínima está intimamente ligado à quantidade de erros por palavra que o código consegue corrigir e por definição temos que $\delta(C) \geq 1$.

2.1 Códigos Projetivos de Tipo Reed-Muller

Sejam $\mathbb{K} = \mathbb{F}_q$ um corpo finito com q elementos, $\mathbb{P}^n$ o espaço projetivo sobre $\mathbb{K}$, $Y \subset \mathbb{P}^n$ um subconjunto finito do espaço projetivo e $\{P_1, \ldots, P_m\}$ um conjunto de representantes de Y. Fixando $0 \leq d \in \mathbb{Z}$, temos que, pela proposição 1.14, existem polinômios homogêneos $f_1, \ldots, f_m \in \mathbb{K}[\mathbf{X}]_d$ tais que $f_i(P_i) \neq 0$ para todo $i \in \{1, \ldots, m\}$ (a rigor, pela proposição, $f_i(P_j) = 0$ para algum $j \neq i$, mas não utilizaremos esta informação). Podemos então definir a função:

$$\begin{array}{rccc} ev_d: & \mathbb{K}[x_0, x_1, \ldots, x_n]_d & \longrightarrow & \mathbb{K}^m \\ & f & \longmapsto & \left(\frac{f(P_1)}{f_1(P_1)}, \frac{f(P_2)}{f_2(P_2)}, \cdots, \frac{f(P_m)}{f_m(P_m)}\right) \end{array}$$

Temos que ev_d é uma transformação linear o que nos permite definir:

Definição 2.3 *$C_Y(d) := Im(ev_d)$ é um subespaço vetorial de $\mathbb{K}^m$ chamado de **código projetivo de tipo Reed-Muller** de grau d em Y.*

Além disso, ev_d não depende da escolha dos representantes de Y. De fato, temos o resultado:

Lema 2.1 (Independência dos Representantes.) *a) A função ev_d está bem definida, isto é, não depende da escolha dos representantes de Y.*

b) Os parâmetros básicos do código projetivo de tipo Reed-Muller associado a ev_d são independentes da escolha de $f_1, \ldots, f_m$.

Demonstração.

[a)] Seja $\{P'_1, \ldots, P'_m\}$ um outro conjunto de representantes de Y. Então existem constantes $\lambda_1, \ldots, \lambda_m \in \mathbb{K}^*$ tais que $P'_i = \lambda_i P_i$ para todo $i \in \{1, \ldots, m\}$. Então

$$\frac{f(P'_i)}{f_i(P'_i)} = \frac{f(\lambda_i P_i)}{f_i(\lambda_i P_i)} = \frac{\lambda_i^d f(P_i)}{\lambda_i^d f_i(P_i)} = \frac{f(P_i)}{f_i(P_i)}.$$

[b)] Sejam $f'_1, \ldots, f'_m \in \mathbb{K}[\mathbf{X}]_d$ polinômios homogêneos tais que $f'_i(P_i) \neq 0$ para todo $i \in \{1, \ldots, m\}$. Definimos

$$\begin{array}{rccc} ev'_d: & \mathbb{K}[x_0, x_1, \ldots, x_n]_d & \longrightarrow & \mathbb{K}^m \\ & f & \longmapsto & \left(\frac{f(P_1)}{f'_1(P_1)}, \frac{f(P_2)}{f'_2(P_2)}, \cdots, \frac{f(P_m)}{f'_m(P_m)}\right) \end{array}$$

a função avaliação relativa a $f'_1, \ldots, f'_m$. Pela definição de ev_d e ev'_d temos que $\ker(ev_d) = \ker(ev'_d)$ e $||ev_d(f)|| = ||ev'_d(f)||$ para todo $f \in \mathbb{K}[\mathbf{X}]_d$. Então os parâmetros de ev_d e ev'_d são os mesmos.

■

Esse tipo de código tem comprimento $|Y|$, dimensão $\dim_{\mathbb{K}} C_Y(d)$ e distância mínima denotada por $\delta_Y(d) := \delta(C_Y(d))$.

Os códigos projetivos de Reed-Muller possuem uma propriedade interessante que se relaciona com a teoria que iremos desenvolver. A proposição a seguir nos diz que à medida que aumentamos o grau dos polinômios que avaliamos, a distância mínima do Código Projetivo de Reed-Muller estaciona em $\delta_Y(d) = 1$.

Proposição 2.1 *Existe um inteiro $r \geq 0$ tal que*

$$|Y| = \delta_Y(0) > \delta_Y(1) > \cdots > \delta_Y(d) = \delta_Y(r) = 1$$

para todo inteiro $d \geq r$.

Demonstração.

Primeiramente fixamos a notação $V_Y(f)$ como sendo os pontos de Y nos quais o polinômio f se anula. Além disso, observe que o número mínimo de entradas não nulas é igual ao total de entrada menos o máximo de entradas nulas. Isto é,

$$\delta_Y(d) = \min\{||ev_d(f)|| : f \in \mathbb{K}[\mathbf{X}]_d \backslash I(Y)\} = |Y| - \max\{|V_Y(f)| : ev_d(f) \neq 0,\ f \in \mathbb{K}[\mathbf{X}]_d\}.$$

Note que para o caso $d = 0$, como $\mathbb{K}[\mathbf{X}]_0 = \mathbb{K}$ são as constantes, o máximo da igualdade anterior é zero e portanto $\delta_Y(0) = |Y|$. Segundo, se $\delta_Y(d) = 1$ para todo $d \geq 0$, então não há nada para provar.

Suponha que $\delta_Y(d) > 1$. Vamos provar que $\delta_Y(d+1) < \delta_Y(d)$. Seja $g \in \mathbb{K}[\mathbf{X}]_d$ tal que $g \notin I(Y)$ e vale

$$|V_Y(g)| = \max\{|V_Y(f)| : ev_d(f) \neq 0, f \in \mathbb{K}[\mathbf{X}]_d\}.$$

Então, como $\delta_Y(d) > 1$, temos que $\delta_Y(d) = |Y| - |V_Y(g)| \geq 2$. Então existem α e $\beta \in Y$ tais que $g(\alpha) \neq 0$ e $g(\beta) \neq 0$.

Agora vamos construir um polinômio de grau $d+1$ com ao menos uma entrada nula a mais que g. Primeiramente, pela proposição 1.14, existe $h \in \mathbb{K}[\mathbf{X}]_1$ tal que $h(\alpha) \neq 0$ e $h(\beta) = 0$. Assim, $hg(\alpha) \neq 0$ porque $\mathbb{K}$ é um corpo e $hg(\beta) = 0$. Além disso, $deg(hg) = d+1$ e vale $|V_Y(hg)| \geq |V_Y(g)| + 1$ donde

$$\max\{|V_Y(f)| : ev_{d+1}(f) \neq 0, f \in \mathbb{K}[\mathbf{X}]_{d+1}\} > \max\{|V_Y(f)| : ev_d(f) \neq 0, f \in \mathbb{K}[\mathbf{X}]_d\}$$

e portanto

$$\begin{aligned} \delta_Y(d+1) &= |Y| - \max\{|V_Y(f)| : ev_{d+1}(f) \neq 0, f \in \mathbb{K}[\mathbf{X}]_{d+1}\} \\ &< |Y| - \max\{|V_Y(f)| : ev_d(f) \neq 0, f \in \mathbb{K}[\mathbf{X}]_d\} = \delta_Y(d). \end{aligned}$$

Para concluir a demonstração observe que, como $ev_d(f) \neq 0$ na definição da distância mínima, temos que $\max\{|V_Y(f)| : ev_d(f) \neq 0, f \in \mathbb{K}[\mathbf{X}]_d\} \leq |Y| - 1$ o que significa que $\delta_Y(d) \geq 1$ para todo $d \geq 1$.

■

Para procurar de maneira mais eficiente quanto vale a distância mínima de um código projetivo de tipo Reed-Muller, uma boa estratégia é diminuir o conjunto $\mathbb{K}[\mathbf{X}]_d$. Em outras palavras, precisamos encontrar as características dos polinômios homogêneos de grau d nos quais a distância mínima será atingida.

Como ev_d é uma função de avaliação, fica fácil encontrar com quais polinômios de $\mathbb{K}[\mathbf{X}]_d$ devemos nos preocupar. Seja $Y \subset \mathbb{P}^n$ finito e $I(Y)$ o ideal da variedade. Temos:

- Se $f \in I(Y)$, então $f(P) = 0$ para todo $P \in Y$ o que implica que $ev_d(f) = 0$. Ou seja, a distância mínima não será atingida nestes polinômios.
- Agora, se $f \notin I(Y)$ e para todo $g \notin I(Y)$ temos que $fg \notin I(Y)$, então $f(P) \neq 0$ para todo $P \in Y$. Isto porque caso $f \notin I$ mas anule algum ponto P, podemos utilizar a proposição 1.14 para construir um outro polinômio $g \notin I$ tal que $fg \in I$. Concluímos então que a distância mínima também não será atingida nos polinômios deste caso.
- E o último caso, se $f \notin I(Y)$ e existe $g \notin I(Y)$ tal que $fg \in I(Y)$. Nesse caso, f se anula em alguns pontos de Y mas não em todos.

Sendo assim, sabemos que nossa distância mínima vão ocorrer nos polinômios do último item. Estes polinômios são especiais. Com efeito, note que o último item corresponde aos divisores de zero no anel $\mathbb{K}[\mathbf{X}]/I(Y)$. Utilizando os ideais quociente podemos escrever de maneira equivalente:

- Se $f \in I(Y)$, então $(I(Y) : f) = \mathbb{K}[\mathbf{X}]$.
- Se $f \notin I(Y)$ e para todo $g \notin I(Y)$ temos que $fg \notin I(Y)$, então $(I(Y) : f) = I(Y)$.
- Se $f \notin I(Y)$ e existe $g \notin I(Y)$ tal que $fg \in I(Y)$, então $I(Y) \subsetneqq (I(Y) : f) \subsetneqq \mathbb{K}[\mathbf{X}]$.

Por este motivo vamos reduzir o nosso trabalho e nos concentrar em avaliar os polinômios do conjunto

$$\mathcal{F}_d := \{f \in \mathbb{K}[\mathbf{X}]_d \backslash I : (I : f) \neq I\}$$

onde $I \subset \mathbb{K}[\mathbf{X}]$ é um ideal.

2.2 Funções de Hilbert

Nesta seção vamos definir as funções de Hilbert e introduzir uma técnica de trabalhar os ideais pelos elementos do complementar do seu ideal de termos líderes. Tal técnica foi desenvolvida primeiramente por Hilbert para determinar a dimensão de uma variedade. Vamos partir de uma motivação geométrica que é o estudo da dimensão de uma variedade. Embora já tenhamos estudado dimensão de Krull de uma variedade, podemos também definir a dimensão de variedades utilizando as funções de Hilbert que é uma abordagem diferente que será apresentada ao longo desta seção como uma curiosidade. Além disso, vamos trabalhar de maneira que o conceito de grau de um ideal fique claro.

2.2.1 A Variedade de um Ideal Monomial

Começaremos a trabalhar com as variedades de um ideal monomial porque dessa forma ficará mais fácil de entender o significado das definições e objetos que veremos adiante.

Seja $I = \langle x^2y, x^3\rangle \subset \mathbb{R}[x, y]$ um ideal monomial. Denotando os eixos coordenados como H_x e H_y, temos que

$$V(I) = V(x^2y) \cap V(x^3) = (H_x \cup H_y) \cap H_x = H_x.$$

Lembrando que H_x também é um espaço vetorial faz sentido pensar que $\dim_{\mathbb{K}}(V(I)) = \dim_{\mathbb{K}}(H_x) = 1$. Com este exemplo surgem várias perguntas. Dentre elas, há uma que devemos destacar: sempre é possível associar uma variedade a subespaços vetoriais ? Se estivermos trabalhando com ideais monomiais, então a resposta é sim.

Estendendo a notação dos eixos coordenados, definimos os espaços vetoriais

$$H_{x_{i_1}x_{i_2}\ldots x_{i_r}} := \{(a_1, \ldots, a_n) \in \mathbb{A}(\mathbb{K})^n : a_{i_1} = \cdots = a_{i_r} = 0\}$$

onde $r \neq n$ é um número natural. Quando um subespaço de $\mathbb{K}^n$ é determinado definindo coordenadas iguais a zero, como é o caso dos espaços acima, atribui-se a eles o nome de **espaços de coordenadas**. Em particular,

$$H_{x_{i_1}x_{i_2}\ldots x_{i_r}} = V(x_{i_1}, x_{i_2}, ..., x_{i_r}).$$

Agora vejamos um problema que pode ocorrer quando vamos associar variedades de ideais monomiais a subespaços vetoriais. Seja $I = \langle y^2z^3, x^5z^4, x^2yz^2\rangle \subset \mathbb{R}[x, y, z]$. Nesse caso,

$$\begin{aligned} V(I) &= V(y^2x^3) \cap V(x^5z^4) \cap V(x^2yz^2) = (H_y \cup H_x) \cap (H_x \cup H_z) \cap (H_x \cup H_y \cup H_z) \\ &= [(H_y \cap H_z) \cup H_x] = H_{yz} \cup H_x. \end{aligned}$$

Qual a dimensão de $V(I)$? Como união de espaços vetoriais não é um espaço vetorial, não podemos calcular a dimensão de $V(I)$ como fizemos anteriormente. No entanto, estamos falando

de espaços vetoriais de dimensão finita, e mais que isso, pela estrutura destes espaços sabemos que aquele de maior dimensão irá conter cópias dos outros. No exemplo acima, $\dim(H_x) = 2$ (plano $x = 0$) e $\dim(H_{yz}) = 1$ (eixo x) onde H_x contém vários subespaços isomorfos a H_{yz}. Por este motivo, definimos:

Definição 2.4 *Seja $W = W_1 \cup \cdots \cup W_r \subset \mathbb{K}^n$ uma união finita de subespaços vetoriais de $\mathbb{K}^n$ onde $\mathbb{K}$ é um corpo. Definimos a* ***dimensão*** *de W como*

$$\dim_{\mathbb{K}}(W) = \max\{\dim(W_1), \ldots, \dim(W_r)\}.$$

Com esta definição, a dimensão da variedade no exemplo anterior é dois. Repetindo as contas que fizemos nos dois exemplos anteriores podemos entender como é a variedade de um ideal monomial.

Proposição 2.2 *A variedade de um ideal monomial em $\mathbb{K}[x_1, \ldots, x_n]$ é uma união finita de subespaços de coordenadas.*

Demonstração.

Vamos começar com o caso em que I é gerado por um único monômio. Seja $I = \langle x_{i_1}^{\alpha_1} \cdots x_{i_r}^{\alpha_r} \rangle \subset \mathbb{K}[\mathbf{X}]$ onde $\alpha_j \geq 1$ para todo $1 \leq j \leq r$. Nesse caso,

$$V(I) = V(x_{i_1}^{\alpha_1} \cdots x_{i_r}^{\alpha_r}) = H_{x_{i_1}} \cup \cdots \cup H_{x_{i_r}},$$

ou seja, $V(I)$ é uma união finita de supespaços de coordenadas.

Agora, como $\mathbb{K}[\mathbf{X}]$ é noetheriano, dado um ideal monomial $I \subset \mathbb{K}[\mathbf{X}]$ sabemos que I é gerado por uma quantidade finita de monômios, digamos que $I = \langle X^{\alpha_1}, \ldots, X^{\alpha_r} \rangle$. Então $V(I) = V(X^{\alpha_1}) \cap \cdots \cap V(X^{\alpha_r})$ é uma interseção finita. Pela primeira etapa, cada $V(X^{\alpha_i})$ é uma união finita de subespaços de coordenadas. Pelas fórmulas de De Moivre e pelo fato que interseção de subespaço de coordenadas também é um subespaço de coordenadas, podemos reescrever $V(I)$ como uma união finita de subespaços de coordenadas.

■

Dado um ideal monomial $I \subset \mathbb{K}[\mathbf{X}]$, se escrevermos a decomposição de $V(I)$ como subespaços de coordendas omitindo os subespaços que estão contidos em outros maiores, então $V(I) = V_1 \cup \cdots \cup V_r$ onde $V_i \nsubseteq V_j$ se $i \neq j$. É fácil ver que esta escrita é única. Isto significa que a dimensão de uma variedade de um ideal monomial está bem definida, em outras palavras, podemos utilizar a definição anterior sem preocupações.

Pela proposição acima, significa que existe um subespaço de coordenadas $H_{x_{i_1} x_{i_2} \ldots x_{i_r}}$ tal que

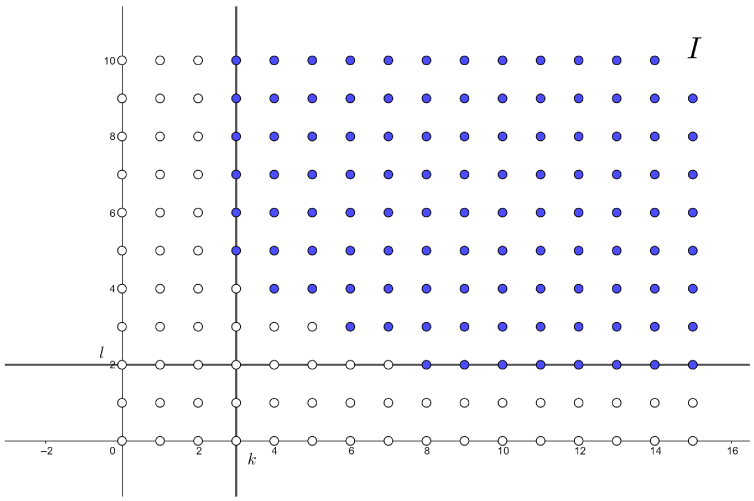
$$\dim_{\mathbb{K}}(V(I)) = \dim_{\mathbb{K}}(H_{x_{i_1} x_{i_2} \ldots x_{i_r}}) = n - r.$$

Ou seja, a dimensão da variedade de um ideal monomial é a quantidade total de variáveis menos o número mínimo delas que precisamos zerar para anular todos os monômios geradores de I.

2.2.2 O Complementar de um Ideal Monomial

Em um de seus artigos, Hilbert teve a ideia de estudar um ideal pelos elementos do seu complementar. Com isto Hilbert demonstrou que é possível determinar a dimensão de uma variedade calculando o crescimento do número de elementos no complementar de I à medida que o grau máximo permitido para estes elementos também aumenta.

Uma maneira de organizar os monômios que não estão em I é a seguinte: seja $I \subset \mathbb{K}[x, y]$ um ideal monomial. Então fazendo a associação $x^\alpha y^\beta \in \mathbb{K}[x, y] \longleftrightarrow (\alpha, \beta) \in \mathbb{N}^2$ e representando por bolas fechadas os monômios que estão em I e por bolas abertas os monômios que não estão em I, temos a seguinte representação gráfica onde k é o menor grau de x que aparece em algum monômio de I e l é o menor grau de y que aparece em algum monômio de I.



Os monômios no complementar de I consistem em k linhas verticais descritas no conjunto

$$\{x^\alpha y^\beta : 0 \leq \alpha \leq k-1,\ \beta \in \mathbb{N}\},$$

l linhas horizontais dadas por

$$\{x^\alpha y^\beta : \alpha \in \mathbb{N},\ 0 \leq \beta \leq l-1\}$$

mais uma quantidade finita de monômios.

Agora vamos contar quantos monômios não estão em I de grau menor ou igual a um natural s, e se s for suficientemente grande, então demonstraremos adiante que podemos obter uma fórmula polinomial para contar esses monômios.

Definição 2.5 *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal monomial. Vamos denotar o conjunto dos expoentes dos monômios que não estão em I por:*

$$C(I) = \{\alpha \in \mathbb{N}^n : X^\alpha \notin I\}.$$

Sejam $e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{N}$ os vetores clássicos. O motivo pelo qual conseguimos determinar a dimensão de uma variedade de um ideal monomial utilizando os elementos de $C(I)$ é a seguinte proposição:

Proposição 2.3 *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal monomial. Então:*

i) O subespaço vetorial $H_{x_{i_1} x_{i_2} \ldots x_{i_r}} \subset V(I)$ se, e somente se, $\langle e_j : j \notin \{i_1, i_2, \ldots, i_r\}\rangle \subset C(I)$.

ii) A dimensão da variedade $V(I)$ é igual a dimensão do maior subespaços de coordenadas de $C(I)$.

Demonstração.

Para simplificar a demonstração vamos supor, sem perda de generalidade, que os índices $i_j = j$ para todo $j \in \{1, \ldots, r\}$.

[(i), $\Rightarrow$] Suponha que $H_{x_1 \ldots x_r} = V(x_1, \ldots, x_r) \subset V(I)$. Então, dado $\alpha \in \langle e_{r+1}, \ldots, e_n\rangle$, podemos escrever $\alpha = (0, \ldots, 0, \alpha_{r+1}, \ldots, \alpha_n) \in \mathbb{N}^n$. Agora considere o ponto

$$P = (\underbrace{0, \ldots, 0}_{r\ zeros}, 1, \ldots, 1) \in H_{x_1 \ldots x_r},$$

temos que

$$X^\alpha(P) = 1^{\alpha_{r+1}} \cdots 1^{\alpha_n} = 1 \neq 0.$$

Assim $X^\alpha \notin I$ o que significa que $\alpha \in C(I)$.

[(i), $\Leftarrow$] Suponha que $\langle e_{r+1}, \ldots, e_n \rangle \subset C(I)$. Seja X^α um monômio de I, então, pela definição de $C(I)$, existe uma variável x_j onde $j \in \{1, \ldots, r\}$ tal que x_j divide o monômio X^α, digamos que $X^\alpha = x_j \cdot X^{\alpha'}$. Seja $P \in V(x_1, \ldots, x_r)$, então $P = (0, \ldots, 0, a_{r+1}, \ldots, a_n)$. Daí,

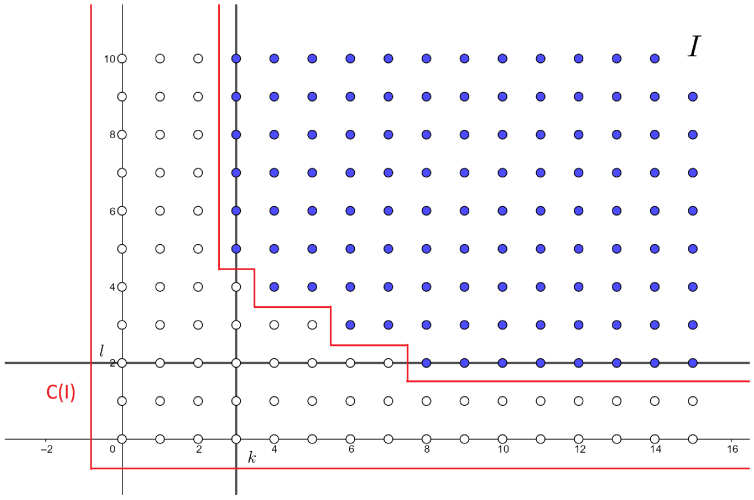
$$X^\alpha(P) = (0) \cdot X^{\alpha'}(P) = 0,$$

ou seja, $P \in V(I)$.

[ii] Pelo item anterior, cada subespaços de coordedadas de $V(I)$ corresponde a um subespaço de coordenadas de $C(I)$ e, além disso, os subespaços associados tem a mesma dimensão. De fato, dimensão de $\dim(V(x_{i_1}, \ldots, x_{i_r}) = n - r$ e $\dim(\langle e_{r+1}, \ldots, e_n \rangle) = n - r$.

■

Podemos então determinar exatamente a natureza do complementar de um ideal monomial. Em outras palavras, podemos entender quem é o conjunto $C(I)$. Observe o seguinte exemplo: seja $I = \langle x^3y^5, x^4y^4, x^6y^3, x^8y^2 \rangle \subset \mathbb{R}[x, y]$. Então $C(I)$ é o conjunto dado na imagem abaixo:



Perceba que $C(I)$ é uma união finita de translações de subespaços de coordenadas. De fato,

$$\begin{aligned} C(I) = \; & \langle e_1 \rangle \cup (e_2 + \langle e_1 \rangle) \cup \langle e_2 \rangle \cup (e_1 + \langle e_2 \rangle) \cup (2e_1 + \langle e_2 \rangle) \cup \{(3,2)\} \cup \cdots \cup \{(7,2)\} \cup \\ & \cup \{(3,3)\} \cup \{(4,3)\} \cup \{(5,3)\} \cup \{(3,4)\}. \end{aligned}$$

onde cada ponto é uma translação do subespaço de coordenadas 0-dimensional que é a origem em $\mathbb{N}^2$.

Teorema 2.1 *Se $I \subset \mathbb{K}[X]$ é um ideal monomial próprio, então o conjunto $C(I) \subset \mathbb{N}^n$ de expoentes dos monômios que não estão em I pode ser escrito como uma união finita, não necessariamente disjunta, de translações de subespaços de coordenadas de $\mathbb{N}^n$.*

Demonstração.

Se $I = \langle 0 \rangle$, então $C(I) = \mathbb{N}^n$ e pronto. Suponha então que $I \neq \langle 0 \rangle$. Vamos demonstrar por indução sobre o número de variáveis. Primeiramente, se $n = 1$, então $I = \langle x^k \rangle \subsetneq \mathbb{K}[x]$ para algum $k \in \mathbb{N}$ e nesse caso os únicos monômios que não estão em I são $1, x, x^2, \ldots, x^{k-1}$. Ou seja, $C(I)$ é uma união de $k - 1$ subespaços de coordenadas 0-dimensionais.

Suponha então que o resultado seja verdadeiro para $n-1$ coordenadas. Seja $I \subsetneq \mathbb{K}[x_1, \ldots, x_n]$ um ideal monomial. Para cada $j \in \mathbb{N}$ definimos o ideal $I_j \subset \mathbb{K}[x_1, \ldots, x_{n-1}]$ dado por

$I_j = \{y \in \mathbb{K}[x_1, \ldots, x_{n-1}] : y \cdot x_n^j \in I\}$. Deixamos a demonstração que I_j é um ideal a cargo do leitor. Então $C(I_j)$ é o conjunto dos expoentes $\alpha \in \mathbb{N}^{n-1}$ tais que $X^\alpha x_n^j \notin I$.

Como I é um ideal, $I_j \subset I_i$ se $j < i$. Assim, $I_0 \subset I_1 \subset I_2 \subset \cdots$ é uma cadeia ascendente de ideais em um anel noetheriano, ou seja, existe um $j_0 \in \mathbb{N}$ tal que $I_j = I_{j_0}$ para todo $j \geq j_0$. Vamos demonstrar que

$$C(I) = (C(I_{j_0} \times \mathbb{N}) \cup \bigcup_{j=0}^{j_0-1} (C(I_j) \times \{j\})). \tag{2.1}$$

Primeiramente note que por definição $C(I_j) \times \{j\} \subset C(I)$. Vejamos que $C(I_{j_0}) \times \mathbb{N} \subset C(I)$. Como $I_{j_0} = I_j$ para $j \geq j_0$ temos que $C(I_{j_0}) \times \{j\} \subset C(I)$ donde $C(I_{j_0}) \times \mathbb{N}_{\geq j_0} \subset C(I)$. Por outro lado, se $j < j_0$, então dado $\alpha \in C(I_{j_0})$ temos que $X^\alpha x_n^{j_0} \notin I$ e como I é um ideal $X^\alpha x_n^j \notin I$ pois caso contrário $X^\alpha x_n^j \cdot x_n^{j_0-j} = X^\alpha x_n^{j_0} \in I$ o que é um absurdo. Ou seja, $(\alpha, j) \in C(I)$. Isso significa que $C(I_{j_0}) \times \{j\} \subset C(I)$ o que conclui a primeira inclusão.

Agora seja $\alpha = (\alpha_1, \ldots, \alpha_n) \in C(I)$, então por construção $\alpha \in C(I_{\alpha_n}) \times \{\alpha_n\}$. Temos dois casos possíveis: ou $\alpha_n < j_0$ o que implica que $\alpha \in \bigcup_{j=0}^{j_0-1} C(I_j) \times \{j\}$ ou $\alpha_n \geq j_0$ e neste caso $\alpha \in C(I_{j_0}) \times \{\alpha_n\} \subset C(I_{j_0}) \times \mathbb{N}$. Portanto vale a igualdade (2.1).

Pela hipótese de indução cada um dos complementares $C(I_0), \ldots, C(I_{j_0})$ é uma união finita de translações de subespaços de coordenadas. Tomando estas uniões e substituindo no lado direito da equação (2.1) demonstramos que $C(I)$ é uma união finita de translações de subespaços de coordenadas.

■

Para obter conclusões a respeito de I a partir de seu complementar precisamos contar quantos monômios não estão em I quando estipulamos uma cota superior para o grau destes monômios. O primeiro resultado nesta direção é o seguinte:

Lema 2.2 *O número de monômios de grau menor ou igual a s em $\mathbb{K}[x_1, \ldots, x_n]$ é o coeficiente binomial $\binom{n+s}{s}$.*

Demonstração.

Basta observar que um monômio X^α tem grau menor ou igual a s se $\alpha_1 + \cdots + \alpha_n \leq s$ onde $\alpha = (\alpha_1, \ldots, \alpha_n)$. Isto significa que o número de monômios de grau menor ou igual a s em $\mathbb{K}[\mathbf{X}]$ é igual ao número de soluções inteiras positivas da equação

$$\alpha_1 + \cdots + \alpha_n \leq s.$$

Por combinatória obtemos que este número é $\binom{n+s}{s}$.

■

Lembre da notação $|\alpha| = \alpha_1 + \cdots + \alpha_n$ para o grau de $\alpha \in \mathbb{N}^n$. É claro que $\deg(X^\alpha) = |\alpha|$. Com esta notação e utilizando o lema anterior obtemos que o número de pontos de grau menor ou igual a s em um subespaço de coordenadas n dimensional é $\binom{n+s}{s}$. Agora observe que se fixarmos n, então obtemos a expressão

$$\binom{n+s}{s} = \binom{n+s}{n} = \frac{1}{n!}(s+n)(s+n-1)\cdots(s+1)$$

que é um polinômio em s de grau n cujo coeficiente líder é $1/n!$.

E quantos pontos de grau $\leq s$ há em uma translação de um subespaço de coordenadas? Considere a translação $T = (0, \ldots, 0, a_{m+1}, \ldots, a_n) + \langle e_1, \ldots, e_m \rangle \in \mathbb{N}^n$. Uma vez que $a_{m+1}, \ldots, a_n$ são naturais fixos e $|\alpha| = \alpha_1 + \cdots + \alpha_m + a_{m+1} + \cdots + a_n$ para todo $\alpha \in T$, o número de pontos de T de grau menor ou igual a s é igual o número de pontos de $\langle e_1, \ldots, e_m \rangle$ de grau menor ou igual a $s - a_{m+1} - \cdots - a_n$. De modo geral temos o seguinte resultado:

Lema 2.3 *Seja $\alpha + \langle e_{i_1}, \ldots, e_{i_m}\rangle \subset \mathbb{N}^n$ uma translação de um subespaço de coordenadas onde $\alpha = \sum_{i\notin\{i_1,\ldots,i_m\}} a_i e_i$. Então:*

i) O número de pontos em $\alpha + \langle e_{i_1}, \ldots, e_{i_m}\rangle$ de grau menor ou igual a s é igual a $\binom{m+s-|\alpha|}{s-|\alpha|}$.

ii) Para $s > |\alpha|$ o número de pontos de grau menor ou igual a s em $\alpha + \langle e_{i_1}, \ldots, e_{i_m}\rangle$ é uma função polinomial de s de grau m e o coeficiente de s^m é $1/m!$.

Demonstração.

Combinação do lema anterior com a observação acima.

■

Teorema 2.2 *Se $I \subset \mathbb{K}[\boldsymbol{X}]$ é um ideal monomial com $\dim V(I) = d$, então para todo s suficientemente grande o número de monômios de grau menor ou igual a s que não estão em I é expresso por um polinômio de grau d em s. Além disso, o coeficiente de s^d é positivo.*

Demonstração.

Pelo teorema 2.1 sabemos que $C(I) = T_1 \cup \cdots \cup T_r$ onde cada T_i é uma translação de um subespaço de coordenadas e $T_i \neq T_j$ para todo $i \neq j$. O problema é que estes conjuntos podem ter interseção. Como a dimensão de cada T_i é a dimensão do subespaço associado e a dimensão de $V(I)$ é d, então $\dim T_i \leq d$ para todo $i \in \{1, \ldots, r\}$, e além disso, existe $l \in \{1, \ldots, r\}$ tal que $\dim T_l = d$.

Vamos denotar por $C(I)_{\leq s}$ os elementos de $C(I)$ com grau menor ou igual a s. Seguindo esta notação temos que

$$C(I)_{\leq s} = (T_1)_{\leq s} \cup \cdots \cup (T_r)_{\leq s}.$$

Pelo princípio da inclusão-exclusão obtemos que

$$\begin{aligned} |C(I)_{\leq s}| = \; & \sum_{i=1}^{r} |(T_i)_{\leq s}| - \sum_{i<j} |(T_i)_{\leq s} \cap (T_j)_{\leq s}| \; + \sum_{i<j<k} |(T_i)_{\leq s} \cap (T_j)_{\leq s} \cap (T_k)_{\leq s}| + \\ & + \cdots + (-1)^r |(T_1)_{\leq s} \cap \cdots \cap (T_r)_{\leq s}|. \end{aligned} \tag{2.2}$$

Pelo lema anterior, $|(T_i)_{\leq s}|$ é um polinômio de grau $m_i = \dim T_i$ em s para s suficientemente grande e o coeficiente é $1/m_i!$. Daí, da equação (2.2) segue que $\deg |C(I)_{\leq s}| \leq d$. Basta demonstrar então que o grau do lado direito da equação é d. Observando que a interseção de duas translações de subespaços de coordenadas é uma translação de um subespaço de coordenadas e lembrando que $m_l = \dim T_l = d$, temos que existe pelo menos um monômio de grau d no lado direito de (2.2). No entanto, como $m_i \leq d$ para todo i e os coeficientes líderes de cada um destes polinômios é positivo, segue que todos os monômios de grau d no lado direito de (2.2) possuem coeficiente positivo. Portanto $\deg |C(I)_{\leq s}| = d$ e seu coeficiente líder é positivo.

■

Observe que o teorema acima nos fornece uma outra maneira puramente algébrica de definir a dimensão de uma variedade. Vamos entrar em mais detalhes adiante. Além disso, pela demonstração do teorema obtemos que:

Proposição 2.4 *Se $I \subset \mathbb{K}[\boldsymbol{X}]$ é um ideal monomial e $dim V(I) = d$, então para todo s suficientemente grande o número de pontos de $C(I)$ com grau menor ou igual a s é um polinômio de grau d em s que pode ser escrito da forma*

$$\sum_{i=0}^{d} a_i \binom{s}{d-i}$$

onde $a_i \in \mathbb{Z}$ para todo $i > 0$ e $a_0 > 0$.

Agora já podemos começar a teoria das funções de Hilbert!

2.2.3 A Função de Hilbert Afim

Primeiramente, para definir a função de Hilbert precisamos obter subespaços vetoriais de $\mathbb{K}[\mathbf{X}]$ de dimensão finita. Observe que: como $\dim_{\mathbb{K}}(\mathbb{K}[\mathbf{X}]) = \infty$, uma das maneiras de obter espaços vetoriais de dimensão finita devemos restringir o grau dos polinômios, isto é, dado $d \in \mathbb{N}$ definimos o conjunto

$$\mathbb{K}[\mathbf{X}]_{\leq d} = \mathbb{K}[x_1, \ldots, x_n]_{\leq d} = \{f \in \mathbb{K}[x_1, \ldots, x_n] : deg(f) \leq d\}$$

que é um $\mathbb{K}$-espaço vetorial satisfazendo

$$\dim_{\mathbb{K}}(\mathbb{K}[\mathbf{X}]_{\leq d}) = \binom{n+d}{d}.$$

Além disso, se $I \subset \mathbb{K}[\mathbf{X}]$ é um ideal, denotamos $I_{\leq d} = I \cap \mathbb{K}[\mathbf{X}]_{\leq d}$.

Definição 2.6 *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal. A função de Hilbert afim de I é a seguinte função:*

$$\begin{array}{rccc} {}^{a}HF_I: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & d & \longmapsto & {}^{a}HF_I(d) = \dim_{\mathbb{K}}\left(\mathbb{K}[\boldsymbol{X}]_{\leq d}/I_{\leq d}\right) \end{array}$$

Note que ${}^{a}HF_I$ está bem definida pois a dimensão de um espaço vetorial é única. Além disso, da álgebra linear sabemos que

$${}^{a}HF_I(d) = \dim(\mathbb{K}[\mathbf{X}]_{\leq d}/I_{\leq d}) = \dim(\mathbb{K}[\mathbf{X}]_{\leq d}) - \dim(I_{\leq d}).$$

Sabemos também que nem sempre é fácil calcular a dimensão de um espaço vetorial. Felizmente o nosso interesse nas funções de Hilbert é dado pela proposição abaixo:

Proposição 2.5 *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal monomial. São válidas:*

i) Para todo $s \in \mathbb{N}$, ${}^{a}HF_I(s)$ é o número de monômios que não estão em I cujo grau é menor ou igual a s.

ii) Para s suficientemente grande, existem inteiros $d, a_0, \ldots, a_d$ com $d \geq 0$ e $a_0 > 0$ tais que

$${}^{a}HF_I(s) = \sum_{i=0}^{d} a_i \binom{s}{d-i}.$$

iii) O inteiro d no item anterior é a dimensão de $V(I)$.

Demonstração.

[i] Primeiramente observe que $\{x^\alpha \in \mathbb{K}[\mathbf{X}] : |\alpha| \leq s\}$ é uma base de $\mathbb{K}[\mathbf{X}]_{\leq s}$ como espaço vetorial. Além disso, o conjunto $\{x^\alpha \in I : |\alpha| \leq s\}$ é uma base de $I_{\leq s}$ como $\mathbb{K}$-espaço vetorial, e portanto, o conjunto $\{[x^\alpha] : |\alpha| \leq s,\ x^\alpha \notin I\}$ é uma base de $\mathbb{K}[\mathbf{X}]_{\leq s}/I_{\leq s}$ o que completa a prova do item [i].

Utilizando o item [i] e os resultados anteriores obtemos os itens [ii] e [iii].

■

A priori pode parecer que esta proposição não é tão boa pois é válida apenas para ideais monomiais enquanto a função de Hilbert afim está definida para qualquer ideal. Mas tem muitas coisas na vida que são flores! Para contornar este empecilho vamos fixar $<$ como sendo a ordem lexicográfica graduada no conjunto $\mathbb{K}[\mathbf{X}]$ e demonstrar o seguinte teorema:

Teorema 2.3 *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal. Então o ideal monomial $\langle LT(I)\rangle$ possui a mesma função de Hilbert afim que o ideal I. Em outras palavras, ${}^aHF_I(s) = {}^aHF_{\langle LT(I)\rangle}(s)$ para todo $s \in \mathbb{N}$.*

Demonstração.

Fixe um natural s e considere os monômios líderes dos elementos de $I_{\leq s}$. Então o conjunto destes elementos é finito e podemos obter elementos $f_1, \ldots, f_m \in I_{\leq s}$ tais que

$$LM(I)_{\leq s} = \{LM(f_1), \ldots, LM(f_m)\}$$

como um $\mathbb{K}$-espaço vetorial. Além disso, retirando elementos duplicados e reordenando se necessário podemos supor, sem perda de generalidade, que $LM(f_1) \succ LM(f_2) \succ \cdots \succ LM(f_m)$. Vamos provar que $I_{\leq s} = \langle f_1, \ldots, f_m\rangle$ como um $\mathbb{K}$-espaço vetorial.

De fato, considere uma combinação linear não trivial $c_1f_1 + \cdots + c_mf_m$ e seja c_j a primeira constante não nula da combinação. Como os líderes monomiais de $f_1, \ldots, f_m$ são distintos e estão ordenados de maneira decrescente, é impossível a combinação linear cancelar o elemento $c_jLT(f_j)$, portanto o conjunto $\{f_1, \ldots, f_m\}$ é linearmente independente sobre $\mathbb{K}$. Por construção obtemos também que $W = \langle f_1, \ldots, f_m\rangle \subset I_{\leq s}$. Por outro lado, suponha por absurdo que existe $f \in I_{\leq s}\backslash W$ de grau mínimo. Observe que $f \neq 0$ porque $0 \in W$. Então existe um inteiro $i \in \{1, \ldots, m\}$ tal que $LM(f) = LM(f_i)$, ou seja, $LT(f) = c \cdot LM(f_i)$ para algum $c \in \mathbb{K}$. Assim $f - c \cdot f_i \in I_{\leq s}$ e $\deg(f - c \cdot f_i) \leq \deg(f)$ e pela minimalidade do grau de f devemos ter que $f - c \cdot f_i = 0$, donde $f \in W$. Contradição!

$$\therefore I_{\leq s} = W = \langle f_1, \ldots, f_m\rangle.$$

Por construção $LM(I)_{\leq s}$ representa todos os líderes monomiais de I de grau menor igual a s, além disso, pela escolha dos elementos $f_1, \ldots, f_m$, segue que $\langle LT(I)_{\leq s}\rangle = \langle LM(f_1), \ldots, LM(f_m)\rangle$ como um K-espaço vetorial. Portanto $\dim_{\mathbb{K}}(I_{\leq s}) = \dim_{\mathbb{K}}(LT(I)_{\leq s})$ e daí concluímos que

$${}^aHF_I(s) = \dim_{\mathbb{K}}(\mathbb{K}[\mathbf{X}]_{\leq s}) - \dim_{\mathbb{K}}(I_{\leq s}) = \dim_{\mathbb{K}}(\mathbb{K}[\mathbf{X}]_{\leq s}) - \dim_{\mathbb{K}}(LT(I)_{\leq s}) = {}^aHF_{LT(I)}(s).$$

■

Assim, pela proposição anterior, dado um ideal $I \subset \mathbb{K}[\mathbf{X}]$, se s é suficientemente grande, então podemos escrever a função de Hilbert afim de I como um polinômio

$${}^aHF_I(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i}$$

chamado de **Polinômio de Hilbert de** I denotado por ${}^ahp_I(s)$.

Definição 2.7 *O menor inteiro r tal que a função de Hilbert afim de I assume comportamento polinomial é chamado de* ***índice de regularidade*** *de I, denotado por $reg(\mathbb{K}[\boldsymbol{X}]/I)$. Em outras palavras, r é o menor inteiro tal que ${}^aHF_I(s) = {}^ahp_I(s)$ para todo inteiro $s \geq r$.*

Note que o grau do polinômio de Hilbert é o mesmo grau do polinômio que encontramos na Proposição 2.4 e também exerce uma função parecida com a função daquele polinômio antigo. Utilizando o teorema anterior, obtemos que o polinômio de Hilbert afim de I conta quantos monômios não estão em $LT(I)$. Além disso, o grau do polinômio de Hilbert afim de I é igual a dimensão de $V(I)$, ou seja, temos uma maneira algébrica de definir a dimensão de uma variedade. Todas estas observações deixam evidente a importância do polinômio de Hilbert afim de I.

Note que ainda não está perfeitamente claro esta questão da dimensão de uma variedade porque estamos partindo do ideal. Dado uma variedade $V \in \mathbb{K}^n$ qual a dimensão de V? Lembre que podem existir vários ideais I distintos que satisfazem a equação $V = V(I)$. Em corpos algebricamente fechados é fácil de resolver o problema porque podemos combinar o Nullstelensatz com o seguinte fato:

Proposição 2.6 *Se $I \subset \mathbb{K}[\boldsymbol{X}]$ é um ideal, então os polinômios de Hilbert afim de I e $\sqrt{I}$ possuem o mesmo grau.*

Demonstração.

Para todo ideal monomial $I \subset \mathbb{K}[\mathbf{X}]$ temos que $V(I) = V(\sqrt{I})$ e pelos resultados anteriores segue este caso.

Agora seja $I \subset \mathbb{K}[\mathbf{X}]$ um ideal qualquer. Provemos que

$$\langle LT(I)\rangle \subset \langle LT(\sqrt{I})\rangle \subset \sqrt{\langle LT(I)\rangle}.$$

Como $I \subset \sqrt{I}$ segue a primeira inclusão. Para a segunda inclusão tome um elemento $X^\alpha \in \langle LT(\sqrt{I})\rangle$. Então existem um polinômio $f \in \sqrt{I}$ tal que $LT(f) = X^\alpha$ e um inteiro $r > 0$ de modo que $f^r \in I$. Logo $LT(f^r) = X^{r\alpha} \in \langle LT(I)\rangle$. Portanto $X^\alpha \in \sqrt{\langle LT(I)\rangle}$.

Utilizando que, se $I \subset J$ então $\deg({}^a hp_I) \geq \deg({}^a hp_J)$, das inclusões anteriores obtemos que

$$\deg\left({}^a hp_{\langle LT(I)\rangle}\right) \geq \deg\left({}^a hp_{\langle LT(\sqrt{I})\rangle}\right) \geq \deg\left({}^a hp_{\sqrt{\langle LT(I)\rangle}}\right).$$

Mas $\langle LT(I)\rangle$ é um ideal radical e portanto $\deg\left({}^a hp_{\langle LT(I)\rangle}\right) = \deg\left({}^a hp_{\sqrt{\langle LT(I)\rangle}}\right)$ donde $\deg\left({}^a hp_{\langle LT(I)\rangle}\right) = \deg\left({}^a hp_{\langle LT(\sqrt{I})\rangle}\right)$. Portanto

$$\deg({}^a hp_I) = \deg\left({}^a hp_{\langle LT(I)\rangle}\right) = \deg\left({}^a hp_{\langle LT(\sqrt{I})\rangle}\right) = \deg\left({}^a hp_{\sqrt{I}}\right).$$

■

Todas estas observações que fizemos é para que a teoria fique mais intuitiva. Tudo o que estamos fazendo está relacionado de certa forma, principalmente no caso afim. Observe que, se I é um ideal monomial ou $\mathbb{K}$ é algebricamente fechado, então $I(V(I)) = \sqrt{I}$ e dizemos que a dimensão de V é o grau do polinômio de Hilbert afim de $I(V)$. Mas se não estamos nesse caso, então temos várias complicações.

Até aqui fizemos muito trabalho no caso afim! Mas não podemos esquecer do caso projetivo, pois é nele que estamos interessados. Trabalhar no caso afim tem várias vantagens:é mais fácil entender as ideias e as demonstrações, podemos aproveitar o que fizemos para simplificar as demonstrações do caso projetivo e estamos trabalhando de maneira mais geral.

2.2.4 A Função de Hilbert Projetiva

Podemos repetir muitos resultados que já demonstramos para o caso projetivo e utilizando fatos análogos aos que demonstramos podemos definir também a dimensão de uma variedade projetiva utilizando o polinômio de Hilbert projetivo. Mas este não é o nosso foco, então vamos abreviar esta seção para seguir adiante.

Definição 2.8 *Seja $I \subset \mathbb{K}[x_0, x_1, \ldots, x_n]$ um ideal homogêneo. A função*

$$\begin{array}{rccc} HF_I: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & d & \longmapsto & \dim(\mathbb{K}[\boldsymbol{X}]_d/I_d) \end{array}$$

*é chamada de **função de Hilbert projetiva** de I.*

É possível demonstrar que I possui a mesma função de Hilbert projetiva que $\langle LT(I)\rangle$, que $HF_I(d)$ é o número de monômios de grau d que não estão em $\langle LT(I)\rangle$. Além disso, as funções de Hilbert afim e projetiva estão intimamente ligadas pela relação ${}^aHF_I(s) = HF_{I^h}(s)$ onde I^h é a homogeneização de I. Mais detalhes sobre esta teoria podem ser encontrados no capítulo 9 de [3]. Estamos interessados em um resultado particular:

Proposição 2.7 *Seja $I \subset \mathbb{K}[x_0, \ldots, x_n]$ um ideal homogêneo. Então existe um polinômio hp_I tal que para todo s suficientemente grande vale a igualdade*

$$HF_I(s) = hp_I(s).$$

Demonstração.

Como no caso projetivo trabalhamos apenas com ideais homogêneos, temos pela definição que a função de Hilbert projetiva de I conta quantos monômios de grau s não estão em $\langle LT(I)\rangle$. De fato, para s suficientemente grande temos que ${}^aHF_I(s) = {}^ahp_I(s)$ é o número de monômios de grau menor ou igual a s que não estão em $\langle LT(I)\rangle$, então

$$hp_I(s) = {}^ahp_I(s) - {}^ahp_I(s-1) = {}^aHF_I(s) - {}^aHF_I(s-1) = HF_I(s)$$

é um polinômio que conta quantos monômios de grau s não estão em I para s suficientemente grande.

■

2.3 Grau de um Quociente

Definição 2.9 *Seja $I \neq \{0\}$ um ideal homogêneo de $\mathbb{K}[x_0, \ldots, x_n]$ com dimensão de Krull k. Definimos o **grau** de $\mathbb{K}[\boldsymbol{X}]/I$ como sendo o numerador do coeficiente líder do polinômio de Hilbert hp_I quando $k \geq 1$. E caso a dimensão de I seja 0, definimos o grau de I como sendo a dimensão do quociente $\mathbb{K}[\boldsymbol{X}]/I$.*

A primeira propriedade do grau que veremos é a aditividade.

Proposição 2.8 (Aditividade do Grau de um Ideal.) *Se $I \subset \mathbb{K}[\boldsymbol{X}]$ é um ideal com decomposição primária não redundante $I = Q_1 \cap \cdots \cap Q_m$, então*

$$\deg(\mathbb{K}[\boldsymbol{X}]/I) = \sum_{ht(Q_i)=ht(I)} \deg(\mathbb{K}[\boldsymbol{X}]/Q_i).$$

Demonstração.

Proposição 2.1 de [8].

■

Lema 2.4 *Seja $I \subset \mathbb{K}[x_0, \ldots, x_n]$ um ideal radical e não misturado. Se $f \in \mathbb{K}[\boldsymbol{X}]$ é um polinômio homogêneo tal que $(I : f) \neq I$, então $ht(I) = ht(\langle I, f\rangle)$ e*

$$\deg(\mathbb{K}[\boldsymbol{X}]/\langle I, f\rangle) = \sum_{P \in A} \deg(\mathbb{K}[\boldsymbol{X}]/P)$$

onde A é o conjunto de todos os primos associados de I que contém f.

Demonstração.

Se f é um divisor de zero em $\mathbb{K}[\mathbf{X}]/I$, então f pertence a algum primo P associado de I e $ht(P) = ht(I)$, pois I é não misturado. Então, $I \subset \langle I, f\rangle \subset P$ donde $ht(I) \leq ht(\langle I, f\rangle) \leq ht(P)$, e portanto, $ht(I) = ht(\langle I, f\rangle)$. Provamos a primeira afirmação e também que $A \neq \varnothing$.

Como I é um ideal radical, sabemos que $I = \bigcap_{i=1}^{m} P_i$ onde cada P_i é um primo associado minimal de I. Denotando $A = \{P_1, \ldots, P_r\}$ podemos obter ideais primários $Q'_{r+1}, \ldots, Q'_t \subset \mathbb{K}[\mathbf{X}]$ tais que

$$\langle I, f\rangle = P_1 \cap \cdots \cap P_r \cap Q'_{r+1} \cap \cdots Q'_t$$

é uma decomposição primária não redundante onde $ht(P_i) = ht(I)$ para todo $i \in \{1, \ldots, r\}$ e $ht(Q'_j) > ht(I)$ para todo $j \in \{r+1, \ldots, t\}$ pois $I \subset \langle I, f\rangle$. Pela aditividade do grau de um ideal segue que

$$\begin{aligned} \deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle) &= \sum_{ht(P_i)=ht(\langle I,f\rangle)} \deg(\mathbb{K}[\mathbf{X}]/P_i) \\ &\overset{ht(I)=ht(\langle I,f\rangle)}{=} \sum_{ht(P_i)=ht(I), f\in P_i} \deg(\mathbb{K}[\mathbf{X}]/P_i) \\ &= \sum_{P\in A} \deg(\mathbb{K}[\mathbf{X}]/P). \end{aligned}$$

■

2.4 Funções Distância Mínima

Sejam $Y \subset \mathbb{P}^n$ um subconjunto finito e $I(Y)$ o ideal de Y. Vamos denotar a função de Hilbert de $I(Y)$ por $H_{I(Y)}(d) = H_Y(d)$ e o polinômio de Hilbert por $hp_{I(Y)} = hp_Y$. A regularidade de $\mathbb{K}[\mathbf{X}]/I(Y)$ é definida como sendo a regularidade de $H_Y(d)$ e denotada por $reg(\mathbb{K}[\mathbf{X}]/I(Y))$.

Dado um ideal $I \subset \mathbb{K}[x_0, \ldots, x_n]$, lembre que estamos interessados nos polinômios do conjunto:

$$\mathcal{F}_d := \{f \in \mathbb{K}[\mathbf{X}]_d \backslash I : (I : f) \neq I\}.$$

Pois é em $\mathcal{F}_d$ que a distância mínima será atingida. Finalmente podemos definir as chamadas funções distância mínima.

Definição 2.10 *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal. A função $\delta_I(d) : \mathbb{N} \longrightarrow \mathbb{Z}$ dada por*

$$\delta_I(d) = \begin{cases} \deg(\mathbb{K}[\boldsymbol{X}]/I) - \max\{\deg(\mathbb{K}[\boldsymbol{X}]/\langle I, f\rangle) : f \in \mathcal{F}_d\} \text{ se } \mathcal{F}_d \neq \varnothing, \\ \deg(\mathbb{K}[\boldsymbol{X}]/I) \text{ se } \mathcal{F}_d = \varnothing. \end{cases}$$

é chamada de ***função distância mínima*** *de I.*

Em geral a função distância mínima é difícil de se calcular. Discutiremos casos em que é relativamente fácil calcular a função distância mínima no próximo capítulo. Em alguns casos específicos conseguimos simplificar as contas, como é o caso a seguir:

Teorema 2.4 *Sejam $I \subset \mathbb{K}[\boldsymbol{X}]$ não misturado e $d \in \mathbb{N}$ um natural. Se $\langle x_0, x_1, \ldots, x_n\rangle^d \nsubseteq I$, então*

$$\delta_I(d) = \min\{deg(\mathbb{K}[\boldsymbol{X}]/(I : f)) : f \in \mathbb{K}[\boldsymbol{X}]_d \backslash I\}$$

Demonstração.

Não faremos esta demonstração porque precisaríamos adicionar muita teoria que seria utilizada apenas nesta prova. A demonstração pode ser encontrada na referência [8] teorema 4.4.

■

2.5 Aplicações da teoria sobre os Códigos Projetivos de Tipo Reed-Muller

Proposição 2.9 *Seja $Y \subset \mathbb{P}^n$ um subconjunto finito não vazio. As seguintes afirmações são verdadeiras:*

i) $H_Y(d) = \dim_{\mathbb{K}} C_Y(d)$, *para todo* $d \geq 0$.

ii) $ht(I(Y)) = n$

iii) $\deg(\mathbb{K}[\boldsymbol{X}]/I(Y)) = |Y|$.

iv) $\delta_Y(d) = 1$, *para todo* $d \geq reg(\mathbb{K}[\boldsymbol{X}]/I(Y))$.

v) $C_Y(d) \neq \langle 0 \rangle$ *para todo* $d \geq 1$.

Demonstração.

[i] Sabemos que $ev_d(f) = (f(P_1), \ldots, f(P_m))$. Por definição $H_Y(d) = \dim(\mathbb{K}[\mathbf{X}]_d/I(Y)_d)$ e como $\ker(ev_d) = I(Y)_d$ segue que

$$\dim(C_Y(d)) = \dim(Im(ev_d)) = \dim(\mathbb{K}[\mathbf{X}]_d) - dim(I(Y)_d) = dim(\mathbb{K}[\mathbf{X}]_d/I(Y)_d) = H_Y(d).$$

[ii] Pelo lema 1.15, $I(Y) = \bigcap_{\alpha \in Y} I_\alpha$ onde $\deg(\mathbb{K}[\mathbf{X}]/I_\alpha) = 1$ e $ht(I_\alpha) = n$ para todo $\alpha \in Y$. Como os primos minimais de $I(Y)$ são os ideais I_α que possuem altura constante, temos que $ht(I(Y)) = n$.

[iii] Seja A o conjunto dos primos minimais de $I(Y)$. Como as alturas são constantes, pelo item (ii) e pela aditividade do grau de um ideal temos que

$$\deg(\mathbb{K}[\mathbf{X}]/I(Y)) = \sum_{P \in A} \deg(\mathbb{K}[\mathbf{X}]/P) = \sum_{\alpha \in Y} \deg(\mathbb{K}[\mathbf{X}]/I_\alpha) = |Y|.$$

[iv] Proposição 2.1.

[v] Como Y é finito e não vazio, se $d \geq 1$, então $\mathbb{K}[\mathbf{X}]_d \neq I(Y)_d$ pela proposição 1.14. Do item (i) acima segue que $\dim(C_Y(d)) = \dim(\mathbb{K}[\mathbf{X}]_d/I(Y)_d) \neq 0$.

■

Lema 2.5 *Seja $Y \subset \mathbb{P}^n$ finito e $I(Y) \subset \mathbb{K}[\boldsymbol{X}]$ o ideal de Y. Se $0 \neq f \in \mathbb{K}[\boldsymbol{X}]$ é homogêneo, então o número de zeros de f em Y é dado por*

$$|V_Y(f)| = \begin{cases} \deg(\mathbb{K}[\boldsymbol{X}]/\langle I(Y), f \rangle) \text{ se } (I(Y) : f) \neq I(Y), \\ 0 \text{ se } (I(Y) : f) = I(Y). \end{cases}$$

Demonstração.

Para demonstrar esta igualdade vamos aplicar o lema 2.4 ao ideal de Y. Mas para fazer isso precisamos demonstrar primeiro que $I(Y)$ é um ideal não misturado.

Seja $P = (\alpha_0 : \alpha_1 : \ldots : \alpha_n) \in Y$ e $\alpha_j \neq 0$ para alguma coordenada j. Então, pelo lema 1.15, I_P é primo e temos que

$$I_P = \langle \{\alpha_j x_i - \alpha_i x_j : j \neq i \in \{1, \ldots, m\}\} \rangle,$$

onde $deg(\mathbb{K}[\mathbf{X}]/I_P) = 1$, $ht(I_P) = n$ e $I(Y) = \bigcap_{P\in Y} I_P$ é uma decomposição primária de $I(Y)$. Contudo, cada I_P é primo, logo $I(Y)$ é um ideal radical e como $ht(I_P) = n$ para todo $P \in Y$, $I(Y)$ é um ideal não misturado.

Vamos demonstrar a igualdade proposta no lema. Sejam $f \in \mathbb{K}[x_0, \ldots, x_n]$ homogêneo tal que $(I(Y) : f) \neq I(Y)$ e A o conjunto dos ideais I_P tais que $f \in I_P$. Como $f \in I_P$ se, e somente se, $f(P) = 0$, temos que $A = \{I_P \subset \mathbb{K}[\mathbf{X}] : f(P) = 0\} = \{I_P \subset \mathbb{K}[\mathbf{X}] : P \in V_Y(f)\}$. Assim, aplicando o lema 2.4 e utilizando que $deg(\mathbb{K}[\mathbf{X}]/I_P) = 1$, iremos obter que

$$|V_Y(f)| = |A| = \sum_{P\in V_Y(f)} deg(\mathbb{K}[\mathbf{X}]/I_P) = \sum_{I_P\in A} deg(\mathbb{K}[\mathbf{X}]/I_P) = deg\left(\frac{\mathbb{K}[\mathbf{X}]}{\langle I(Y), f\rangle}\right).$$

Se $|V_Y(f)| \neq 0$, então existe $P \in V_Y(f)$. Tomamos então o polinômio $g \in \mathbb{K}[\mathbf{X}]$ tal que $g(Q) = 0$ para todo $P \neq Q \in Y$ e $g(P) \neq 0$. Nessas condições, $g \notin I(Y)$ mas $fg \in Y$, ou seja, $g \in (I(Y : f)\backslash I(Y))$.

■

E finalmente chegamos em um dos principais resultados desta dissertação! Conseguimos uma formulação algébrica para a distância mínima dos códigos projetivos de tipo Reed-Muller.

Teorema 2.5 *Seja $Y \subset \mathbb{P}^n$ finito. Se $|Y| \geq 2$, então*

$$\delta_Y(d) = \delta_{I(Y)}(d) \geq 1, \ \forall\ d \geq 1.$$

Ou seja, as funções distância mínima descrevem o parâmetro distância mínima de códigos projetivos de tipo Reed-Muller.

Demonstração. Por definição

$$ev_d(f) = (f(P_1), \ldots, f(P_m)) \ \ e\ |V_Y(f)| = |\{P \in Y : f(P) = 0\}|.$$

Daí,

$$\begin{aligned}\delta_Y(d) &= \min\{||ev_d(f)|| : f \in \mathbb{K}[\mathbf{X}]_d,\ ev_d(f) \neq 0\}\\ &= |Y| - \max\{|V_Y(f)| : f \in \mathbb{K}[\mathbf{X}]_d,\ ev_d(f) \neq 0\}.\end{aligned}$$

Como $|Y| \geq 2$, para $I = I(Y)$ temos, pelo item (iv) da proposição 1.14 ,que $\mathcal{F}_d \neq \varnothing$ para todo $d \geq 1$. Então, pelo lema anterior,

$$\begin{aligned}&\max\{|V_Y(f)| : ev_d(f) \neq 0,\ f \in \mathbb{K}[\mathbf{X}]_d\} =\\ &= \max\{deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle) : f \in \mathcal{F}_d\}.\end{aligned}$$

Daí,

$$\delta_Y(d) = deg(\mathbb{K}[\mathbf{X}]/I) - \max\{deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle) : f \in \mathcal{F}_d\} = \delta_{I(Y)}(d).$$

■

Capítulo 3

Cotas para a Função Distância Mínima

Neste capítulo iremos desenvolver técnicas para obter cotas superiores e inferiores para a distância mínima. Não entraremos em muitos detalhes sobre as cotas superiores porque na teoria de códigos elas não são muito úteis. Por outro lado, utilizaremos as técnicas da pegada de um ideal para simplificar nosso problema e então obter cotas inferiores para a função distância mínima de I utilizando uma função auxiliar chamada função pegada de I.

3.1 A Pegada de um Ideal

A pegada de um ideal foi um conceito que surgiu na tese de doutorado do matemático alemão Bruno Buchberger como a base do $\mathbb{K}$-espaço vetorial $\mathbb{K}[\mathbf{X}]/I$, contudo a teoria das bases de Gröbner recentemente começou a ser utilizada para encontrar cotas inferiores para o parâmetro distância mínima na teoria de Códigos Corretores de Erro. Tal técnica foi introduzida por Geil [5] e amplamente trabalhada por Carvalho [2]. Neste texto vamos utilizar a pegada de um ideal para obter cotas inferiores pada a distância mínima de um tipo específico de código, os códigos projetivos de tipo Reed-Muller.

Definição 3.1 *Sejam $\mathcal{M} \subset \mathbb{K}[\boldsymbol{X}]$ o conjunto de todos os monômios e $\prec$ uma ordem monomial em $\mathbb{K}[\boldsymbol{X}]$. Definimos a **pegada** de I como sendo o conjunto*

$$\Delta_{\prec}(I) := \{f \in \mathcal{M} : \forall\ g \in I,\ LT(g) \nmid f\}.$$

Note que os expoentes dos monômios de $\Delta_{\prec}(I)$ são os elementos do conjunto $C(LT(I))$ que definimos no capítulo anterior. Um elemento da pegada de I é chamado de **monômio padrão** e um polinômio que é uma combinação linear de monômios padrões é chamado de **polinômio padrão**.

A pegada de um ideal I é um conceito que está intimamente ligado com as bases de Gröbner de I.

Proposição 3.1 *Sejam $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal e $G = \{g_1, \ldots, g_m\}$ uma base de Gröbner para I. Então $X^\alpha \in \Delta(I)$ se, e somente se, X^α não é múltiplo de $LM(g_i)$ para todo $i \in \{1, \ldots, m\}$.*

Demonstração.

[⇒] Pela definição de base de Gröbner temos que $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_m)\rangle$. Daí, se $X^\alpha \in \Delta(I)$, então $X^\alpha \notin \langle LT(I)\rangle$. Isto significa que X^α não é múltiplo de $LT(g_i)$ para todo $i = 1, \cdots, m$.

[⇐] Se X^α não é múltiplo de nenhum $LT(g_i)$, então $X^\alpha \notin \langle LT(g_1), \ldots, LT(g_m)\rangle = \langle LT(I)\rangle$. Então por definição $X^\alpha \in \Delta(I)$.

■

Assim se obtivermos uma base de Gröbner para I, facilmente determinamos $\Delta(I)$. A ligação entre os dois conceitos é tão forte que o inverso também é verdadeiro, isto é, conhecendo pegada de I podemos determinar uma base de Gröbner para I.

A pegada de um ideal tem diversas aplicações, vamos demonstrar uma propriedade que utilizaremos e citar uma outra como curiosidade.

Teorema 3.1 *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$. Então $B := \{X^\alpha + I : X^\alpha \in \Delta(I)\}$ é uma base para $\mathbb{K}[\boldsymbol{X}]/I$ como um $\mathbb{K}$-espaço vetorial.*

Demonstração.

Vejamos que B gera $\mathbb{K}[\mathbf{X}]/I$. Seja $G = \{g_1, \ldots, g_m\}$ uma base de Gröbner de I. Dado $f \in \mathbb{K}[\mathbf{X}]\backslash I$ existem polinômios $q_1, \ldots, q_m, r \in \mathbb{K}[\mathbf{X}]$ tais que $f = \sum_{i=1}^m q_i g_i + r$ onde r é único e $LT(g_i) \nmid r$ para todo i. Assim $f - r \in I$ donde $f + I = r + I$ em $\mathbb{K}[\mathbf{X}]/I$ e, como $LT(g_i) \nmid r$ para todo i, temos pela proposição anterior que $r + I \in B$.

Provemos agora que B é um conjunto linearmente independente. Sejam $0 < k \in \mathbb{N}$, $X^{\alpha_1}, \ldots, X^{\alpha_k} \in \Delta(I)$ e $a_1, \ldots, a_k \in \mathbb{K}$ tais que

$$(a_1 X^{\alpha_1} + \cdots + a_k X^{\alpha_k}) + I = I,$$

logo $a_1 X^{\alpha_1} + \cdots + a_k X^{\alpha_k} \in I$. Se $a_j \neq 0$ para algum $j \in \{1, \ldots, k\}$, então $\sum_{l=1}^k a_l X^{\alpha_l}$ é um polinômio de I onde $LT(g_i) \nmid LT(\sum_{l=1}^k a_l X^{\alpha_l})$ para todo $i \in \{1, \ldots, m\}$, mas isso contraria o fato de G ser uma base de Gröbner para I. Portanto $a_i = 0$ para todo i.

■

Proposição 3.2 *Seja $I \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal tal que $\Delta(I)$ é um conjunto finito. Então a variedade afim de I também é um conjunto finito e $|V(I)| \leq |\Delta(I)|$.*

Demonstração.

Teorema 2.14 de [2].

■

Observe que do teorema anterior obtemos uma relação muito forte entre a pegada de um ideal e sua função de Hilbert projetiva. De fato, temos que

$$HF_I(d) = \dim(\mathbb{K}[\mathbf{X}]_d / I_d) = |\Delta(I)_d|.$$

Esta relação motiva a simplificação do problema de encontrar cotas que faremos na seção a seguir.

3.2 Simplificando o Problema

Nós já encontramos um bom conjunto onde a distância mínima será atingida por seus elementos, a saber, o conjunto $\mathcal{F}_d$. Basicamente o que faremos para encontrar cotas é encontrar subconjuntos de $\mathcal{F}_d$ com uma estrutura conveniente.

Fixando um natural $0 < d \in \mathbb{N}$ temos que $\Delta_\prec(I)_d = \{X^{a_1}, \ldots, X^{a_r}\}$ é um conjunto finito. Utilizando $\Delta_\prec(I)_d$ conseguimos identificar bons polinômios para procurar a distância mínima, tais elementos denotamos pelo conjunto

$$\mathcal{F}_{\prec,d} := \left\{ f = \sum_{i=1}^r \lambda_i X^{a_i} : f \neq 0, \lambda_i \in \mathbb{K} \text{ e } (I : f) \neq I \right\}$$

das combinações lineares dos elementos de $\Delta_\prec(I)_d$ com coeficientes em $\mathbb{K}$.

A utilidade deste conjunto é a seguinte: seja $f \in \mathcal{F}_d$, então pelo algoritmo da divisão, existe $g \in I_d$ e constantes $c_1, \ldots, c_r \in \mathbb{K}$ tais que

$$f = g + c_1 X^{a_1} + \cdots + c_r X^{a_r}$$

onde $c_j \neq 0$ para algum $j \in \{1, \ldots, r\}$. Seja $f' = \sum_{i=1}^{r} c_i X^{a_i}$. Então da igualdade anterior segue que $\langle I, f\rangle = \langle I, f'\rangle$. Consequentemente

$$\begin{aligned} \delta_I(d) &= \deg(\mathbb{K}[\mathbf{X}]/I) - \max\{deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle) : f \in \mathcal{F}_d\} \\ &= \deg(\mathbb{K}[\mathbf{X}]/I) - \max\{deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle) : f \in \mathcal{F}_{\prec,d}\}. \end{aligned}$$

Ou seja, conseguimos reduzir ainda mais os elementos onde a distância mínima será atingida. Além disso, pela propriedade do resto único das bases de Gröbner, temos também que

$$\mathcal{F}_d \neq \varnothing \Leftrightarrow \mathcal{F}_{\prec,d} \neq \varnothing.$$

Com esta simplificação, se $\mathbb{K} = \mathbb{F}_q$ é um corpo finito, então o número de polinômios padrão de grau d em $\mathbb{K}[x_0, x_1, \ldots, x_n]$ é $N^q - 1$ onde N é o número de monômios padrão de grau d. Dessa forma, para pequenos valores de N e q conseguimos calcular $\delta_I(d)$. Note que para que o valor N seja pequeno, o número de variáveis e o natural d devem ser pequenos.

3.3 Cotas Superiores

Para encontrar cotas superiores para $\delta_Y(d)$ é relativamente fácil: de fato, como estamos trabalhando com os polinômios do conjunto $\mathcal{F}_d = \{f \in \mathbb{K}[\mathbf{X}]_d : f \notin I \ e \ (I : f) \neq I\}$, um jeito natural de obter cotas superiores para $\delta_I(d)$ é restringir $\mathcal{F}_d$. Em particular, podemos restringir $\mathcal{F}_{\prec,d}$. Denotando $\mathcal{F}'_{\prec,d} \subset \mathcal{F}_{\prec,d}$ obtemos que

$$\max\{\deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle) : f \in \mathcal{F}'_{\prec,d}\} \leq \max\{\deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle) : f \in \mathcal{F}_{\prec,d}\}$$

donde

$$\begin{aligned} \delta_I(d) &= \deg(\mathbb{K}[\mathbf{X}]/I) - \max\{\deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle) : f \in \mathcal{F}_{\prec,d}\} \\ &\leq \deg(\mathbb{K}[\mathbf{X}]/I) - \max\{\deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle) : f \in \mathcal{F}'_{\prec,d}\} \quad = \delta'_I(d). \end{aligned}$$

Ou seja, $\delta_I(d)'$ é uma cota superior para $\delta_I(d)$. Em geral utiliza-se o conjunto

$$\mathcal{F}'_{\prec,d} := \left\{ f = \sum_{i=1}^{r} \lambda_i X^{a_i} : f \neq 0, \lambda_i \in \{0, 1\} \ e \ (I : f) \neq I \right\}$$

onde estamos considerando $\Delta_\prec(I)_d = \{X^{a_1}, \ldots, X^{a_r}\}$.

3.4 Cotas Inferiores com a Função Pegada de I

A simplificação do conjunto $\mathcal{F}_d$ que fizemos no início do capítulo é apenas o começo do nosso trabalho. No entanto, já deixa evidente que a pegada de um ideal é um bom caminho na procura das cotas inferiores. Adiante ficará claro o motivo pelo qual vamos definir a seguinte função auxiliar:

Definição 3.2 *A função* $fp_I(d) : \mathbb{N} \longrightarrow \mathbb{Z}$ *dada por*

$$fp_I(d) = \begin{cases} \deg(\mathbb{K}[\boldsymbol{X}]/I) - \max\left\{deg\left(\frac{\mathbb{K}[\boldsymbol{X}]}{\langle LM(I), X^a\rangle}\right) : X^a \in \Delta_\prec(I)_d\right\} & se \ \Delta_\prec(I)_d \neq \varnothing, \\ \deg(\mathbb{K}[\boldsymbol{X}]/I) \ se \ \Delta_\prec(I)_d = \varnothing. \end{cases}$$

é chamada de ***função pegada*** *de* I.

O motivo pelo qual definição a função pegada de I que é uma simplificação da função distância mínima é o seguinte lema:

Lema 3.1 *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal não misturado. Se $f \in \mathbb{K}[\boldsymbol{X}]$ é um polinômio homogêneo e $(I : f) \neq I$, então*

$$\deg(\mathbb{K}[\boldsymbol{X}]/\langle I, f\rangle) \leq \deg(\mathbb{K}[\boldsymbol{X}]/\langle LM(I), LM(f)\rangle) \leq \deg(\mathbb{K}[\boldsymbol{X}]/I)$$

e vale $\deg(\mathbb{K}[\boldsymbol{X}]/\langle I, f\rangle) < \deg(\mathbb{K}[\boldsymbol{X}]/I)$ *se I é radical e não misturado com $f \notin I$.*

Demonstração.

Para simplificar a escrita desta demonstração denotaremos $L = \langle LM(I), LM(f)\rangle$. Primeiro vamos mostrar que as dimensões de Krull de $\mathbb{K}[\mathbf{X}]/I$, $\mathbb{K}[\mathbf{X}]/\langle I, f\rangle$ e $\mathbb{K}[\mathbf{X}]/L$ são iguais.

Seja f um divisor de zero em $\mathbb{K}[\mathbf{X}]/I$. Então existe um primo associado P de I tal que $f \in P$. Como I é não misturado segue que $ht(P) = ht(I)$. Pelo teorema 1.12 sabemos que $\dim(\mathbb{K}[\mathbf{X}]/I) = \dim(\mathbb{K}[\mathbf{X}]) - ht(I)$ para todo ideal $I \subset \mathbb{K}[\mathbf{X}]$. Então $\dim(\mathbb{K}[\mathbf{X}]/P) = \dim(\mathbb{K}[\mathbf{X}]/I)$ e daí,

$$\begin{aligned} I \subset \langle I, f\rangle \subset P &\Rightarrow \mathbb{K}[\mathbf{X}]/I \supset \mathbb{K}[\mathbf{X}]/\langle I, f\rangle \supset \mathbb{K}[\mathbf{X}]/P \\ &\Rightarrow \dim\left(\frac{\mathbb{K}[\mathbf{X}]}{I}\right) \geq \dim\left(\frac{\mathbb{K}[\mathbf{X}]}{\langle I, f\rangle}\right) \geq \dim\left(\frac{\mathbb{K}[\mathbf{X}]}{P}\right) \\ &\Rightarrow \dim\left(\frac{\mathbb{K}[\mathbf{X}]}{I}\right) = \dim\left(\frac{\mathbb{K}[\mathbf{X}]}{\langle I, f\rangle}\right). \end{aligned}$$

Por outro lado, sabemos que as funções de Hilbert de I e $LM(I)$ são iguais, assim como as funções de Hilbert de P e $LM(P)$, logo

$$\dim(\mathbb{K}[\mathbf{X}]/\langle LM(I)\rangle) = \dim(\langle LM(I)\rangle) = \dim(I) = \dim(P) = \dim(\langle LM(P)\rangle) = \dim(\mathbb{K}[\mathbf{X}]/\langle LM(P)\rangle).$$

Finalmente, $\langle LM(I)\rangle \subset L \subset \langle LM(P)\rangle$ implica que $ht(I) \leq ht(L) \leq ht(P)$. No entanto, $ht(I) = ht(P)$ donde $ht(I) = ht(L)$ e daí $\dim(\mathbb{K}[\mathbf{X}]/L) = \dim(\mathbb{K}[\mathbf{X}]/I)$.

Agora observe que se a dimensão de Krull de I é zero, então como I é não misturado segue do lema 2.4 que $ht(I) = ht(\langle I, f\rangle)$ consequentemente $\dim(\mathbb{K}[\mathbf{X}]/I) = \dim(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle)$ e daí, pela definição do grau de um ideal temos que

$$\deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle) = \deg(\mathbb{K}[\mathbf{X}]/L) = \deg(\mathbb{K}[\mathbf{X}]/I).$$

Assim, se $\dim(I) > 0$, então com o primeiro passo demonstramos que os polinômios de Hilbert de I, L e $\langle I, f\rangle$ possuem o mesmo grau. Agora vamos demonstrar a desigualdade do enunciado deste lema. Seja $G = \{g_1, \ldots, g_r\}$ uma base de Gröbner de I. Então $\langle I, f\rangle = \langle G \cup \{f\}\rangle$ e daí

$$\Delta(\langle I, f\rangle) \subset \Delta(LM(g_1), \ldots, LM(g_r), LM(f)) = \Delta(LM(I), LM(f)) = \Delta(L) \subset \Delta(G) = \Delta(I),$$

ou seja, $\Delta(\langle I, f\rangle) \subset \Delta(L) \subset \Delta(I)$. Pela relação entre a função de Hilbert e a pegada de um ideal temos que $H_{\langle I,f\rangle}(d) \leq H_L(d) \leq H_I(d)$. Mas estes três polinômios possuem o mesmo grau $k = \dim(\mathbb{K}[\mathbf{X}]/I)$, portanto

$$k! \lim_{d\to\infty}\left(\frac{H_{\langle I,f\rangle}(d)}{d^k}\right) \leq k! \lim_{d\to\infty}\left(\frac{H_L(d)}{d^k}\right) \leq k! \lim_{d\to\infty}\left(\frac{H_I(d)}{d^k}\right).$$

Em outras palavras,

$$\deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle) \leq \deg(\mathbb{K}[\mathbf{X}]/L) \leq \deg(\mathbb{K}[\mathbf{X}]/I).$$

Para concluir a demonstração, note que se I é um ideal radical não misturado, então I é a interseção de seus primos associados, e nesse caso, $f \notin I$ significa que existe um primo associado de I tal que $f \notin P$. E pelo lema 2.4, segue que $\deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle) < \deg(\mathbb{K}[\mathbf{X}]/I)$.

■

Deste lema vamos obter duas informações importantes. A primeira delas é uma cota superior para o número de pontos da variedade de um polinômio em um subconjunto finito $X \subset \mathbb{P}^n$.

Corolário 3.1 *Sejam $X \subset \mathbb{P}^n$ e $I(X) \subset \mathbb{K}[\boldsymbol{X}]$ o ideal de X. Se $0 \neq f \in \mathbb{K}[\boldsymbol{X}]$ é homogêneo e $(I(X) : f) \neq I(X)$, então*

$$|V_X(f)| = \deg\left(\frac{\mathbb{K}[\boldsymbol{X}]}{\langle I(X), f\rangle}\right) \leq \deg\left(\frac{\mathbb{K}[\boldsymbol{X}]}{\langle LM(I(X)), LM(f)\rangle}\right) \leq \deg(\mathbb{K}[\boldsymbol{X}]/I(X)),$$

e $\deg(\mathbb{K}[\boldsymbol{X}]/\langle I(X), f\rangle) < \deg(\mathbb{K}[\boldsymbol{X}]/I(X))$ se $f \notin I(X)$.

Demonstração.
Basta aplicar o lema anterior ao lema 2.5.

■

A segunda é a ideia por trás da definição da função pegada de I: se $I \subset \mathbb{K}[\mathbf{X}]$ é um ideal não misturado, então dado $f \in \mathbb{K}[\mathbf{X}]_d \backslash I$ tal que $(I : f) \neq I$, temos que o líder monomial de f está em $LM(f) = X^a \in \Delta_\prec(I)_d$, e pelo lema anterior segue que

$$\deg(\mathbb{K}[\mathbf{X}]/\langle LM(I), X^a\rangle) \geq \deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle)$$

donde,

$$\begin{aligned} fp_I(d) &= \deg(\mathbb{K}[\mathbf{X}]/I) - \max\left\{\deg\left(\tfrac{\mathbb{K}[\mathbf{X}]}{\langle LM(I), X^a\rangle}\right) : X^a \in \Delta_\prec(I)_d\right\} \\ &\leq \deg(\mathbb{K}[\mathbf{X}]/I) - \max\left\{\deg\left(\tfrac{\mathbb{K}[\mathbf{X}]}{\langle I, f\rangle}\right) : f \in \mathcal{F}_{\prec,d}\right\} \\ &= \delta_I(d). \end{aligned}$$

Ou seja, a função pegada de I fornece uma boa cota inferior para a função distância mínima de I. Infelizmente sem outras condições sobre I a função pegada de I pode não fornecer uma boa cota inferior. Com efeito, fp_I pode assumir valores negativos (veja exemplo 7.3 de [8]). Vamos em busca de uma condição para melhorar esta cota inferior.

3.5 Aperfeiçoando as Cotas Inferiores

Teorema 3.2 *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal não misturado com $\dim_{\mathbb{K}}(I) \geq 1$ tal que as variáveis x_i são divisoras de zero em $\mathbb{K}[\boldsymbol{X}]/I$ para todo $i \in \{1, \ldots, n\}$. Então para todo $1 \leq d \in \mathbb{Z}$ valem:*

i) $\mathcal{F}_d = \{f \in \mathbb{K}[\boldsymbol{X}]_d : f \notin I, (I : f) \neq I\} \neq \varnothing$.

ii) $\delta_I(d) \geq fp_I(d)$.

iii) $\deg\left(\frac{\mathbb{K}[\boldsymbol{X}]}{\langle I, X^a\rangle}\right) \leq \deg\left(\frac{\mathbb{K}[\boldsymbol{X}]}{\langle LM(I), X^a\rangle}\right) \leq \deg\left(\frac{\mathbb{K}[\boldsymbol{X}]}{I}\right)$.

iv) $fp_I(d) \geq 0$.

v) $\delta_I(d) \geq \delta_I(d+1) \geq 0$.

vi) Se I é radical e seus primos associados são gerados por polinômios homogêneos de grau um, então existe um inteiro $r \geq 1$ tal que

$$\delta_I(1) > \delta_I(2) > \cdots > \delta_I(r) = \delta_I(d) = 1$$

sempre que $d \geq r$.

Demonstração.

[i] Fixado $d \in \mathbb{N}$, como $\dim(\mathbb{K}[\mathbf{X}]/I) \geq 1$, existe uma variável x_j tal que $x_j^d \notin I$ para algum $j \in \{1, \ldots, n\}$. Por hipótese, x_j^d é um divisor de zero em $\mathbb{K}[\mathbf{X}]/I$, isto é, existe $g \in \mathbb{K}[\mathbf{X}] \backslash I$ tal que $x_j^d \cdot g \in I$, ou seja, $(I : x_j^d) \neq I$. Portanto $x_j^d \in \mathcal{F}_d$.

[ii] Por hipótese I é um ideal não misturado e pelo item anterior $\mathcal{F}_d \neq \varnothing$, logo $\mathcal{F}_{\prec,d}$ é não vazio e sob estas condições já demonstramos que $\delta_I(d) \geq fp_I(d)$.

[iii] Basta observar que cada elemento $X^\alpha \in \Delta_\prec(I)_d$ satisfaz as condições do lema anterior.

[iv] Pelo item anterior, para todo $X^\alpha \in \Delta_\prec(I)_d$, temos que $\deg(\mathbb{K}[\mathbf{X}]/\langle LM(I), X^\alpha\rangle) \leq \deg(\mathbb{K}[\mathbf{X}]/I)$ donde

$$fp_I(d) = \deg(\mathbb{K}[\mathbf{X}]/I) - \max\{\deg(\mathbb{K}[\mathbf{X}]/\langle LM(I), X^\alpha\rangle) : X^\alpha \in \Delta_\prec(I)_d\} \geq 0.$$

[v] A demonstração deste item pode ser encontrada no teorema 4.5 de [8]. Não faremos a demonstração pois a mesma utiliza resultados sobre sequências exatas e sua relação com funções de Hilbert e tal teoria não foi discutida neste texto.

[vi] Suponha que I seja um ideal radical. Como I é não misturado, dado $f \in \mathcal{F}_d$ temos que $\deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle) < \deg(\mathbb{K}[\mathbf{X}]/I)$ pelo lema anterior. Daí, pelo item $[i]$ obtemos que

$$\delta_I(d) = \deg(\mathbb{K}[\mathbf{X}]/I) - \max\{\deg(\mathbb{K}[\mathbf{X}]/\langle I, f\rangle) : f \in \mathcal{F}_d\} \geq 1.$$

Se $\delta_I(d) = 1$ para todo natural d, então não há nada a fazer. Seja $0 < d \in \mathbb{N}$ um natural tal que $\delta_I(d) > 1$. Pelo item $[v]$ temos que $\delta_I(d) \geq \delta_I(d+1)$, então é suficiente demonstrar que $\delta_I(d) > \delta_I(d+1)$. Como $\mathcal{F}_d \neq \varnothing$, $\mathcal{F}_{\prec,d} \neq \varnothing$ e portanto podemos escolher $F \in \mathcal{F}_d$ tal que $f \notin I$, $(I : F) \neq I$ e

$$\deg(\mathbb{K}[\mathbf{X}]/\langle I, F\rangle) = \max\{\deg(\mathbb{K}[\mathbf{X}]/\langle I, F\rangle) : f \in \mathbb{K}[\mathbf{X}]_d \backslash I, (I : F) \neq I\}.$$

Sejam $P_1, \ldots, P_m$ os primos associados de I. Como $F \notin I \subset P_1 \cap \cdots \cap P_m$ Então, pelo lema 2.4 obtemos que

$$\begin{aligned} \delta_I(d) &= \deg(\mathbb{K}[\mathbf{X}]/I) - \deg(\mathbb{K}[\mathbf{X}]/\langle I, F\rangle) \\ &= \textstyle\sum_{i=1}^m \deg(\mathbb{K}[\mathbf{X}]/P_i) - \sum_{F \in P_i} \deg(\mathbb{K}[\mathbf{X}]/P_i) \geq 2, \end{aligned}$$

pois por hipótese $\delta_I(d) > 1$. Então existem $P_k \neq P_j$ primos associados de I tais que $F \notin P_k \cup P_j$. Utilizando a hipótese que os primos associados de I são gerados por polinômios homogêneos de grau um, podemos tomar um polinômio homogêneo $h \in P_k \backslash P_j$ de grau um. Assim, $hF \in P_k$ e $hF \notin P_j$ porque P_j é um ideal primo. Segue que $hF \notin I$ e como F é um divisor de zero de $\mathbb{K}[\mathbf{X}]/I$, segue que hF também é um divisor de zero do quociente. Portanto, novamente pelo lema 2.4, obtemos que

$$\deg(\mathbb{K}[\mathbf{X}]/\langle I, F\rangle) = \sum_{F \in P_i} \deg(\mathbb{K}[\mathbf{X}]/P_i) < \sum_{hF \in P_i} \deg(\mathbb{K}[\mathbf{X}]/P_i) = \deg(\mathbb{K}[\mathbf{X}]/\langle I, hF\rangle).$$

Por construção, $\deg(\mathbb{K}[\mathbf{X}]/\langle I, F\rangle) = \max\{\deg(\mathbb{K}[\mathbf{X}]/\langle I, F\rangle) : f \in \mathbb{K}[\mathbf{X}]_d \backslash I, (I : F) \neq I\}$, então a inequação acima implica que $\delta_I(d) > \delta_I(d+1)$.

■

Antes de concluir o capítulo com um exemplo, temos um corolário que resume o nosso objetivo ao longo de todo este trabalho.

Corolário 3.2 *Sejam $\mathbb{K}$ um corpo e X um subconjunto finito de $\mathbb{P}^n$. Se x_i é um divisor de zero de $\mathbb{K}[\boldsymbol{X}]/I(X)$ para todo $i \in \{0, \ldots, n\}$, então*

$$\delta_X(d) = \delta_{I(X)}(d) \geq fp_{I(X)}(d) \geq 1$$

para todo natural $d \geq 1$.

Demonstração.

Pelo lema 1.15 obtemos que $I(X)$ é um ideal não misturado, então basta utilizar os teoremas 2.5 e 3.2.

■

Exemplo: Seja X um subconjunto de $\mathbb{P}^3$ parametrizado por x_0x_1, x_1x_2, x_2x_3 e x_0x_3 sobre o corpo $\mathbb{F}^3$. Temos que

d	1	2	3	$\cdots$
$\|X\|$	16	16	16	$\cdots$
$H_X(d)$	4	9	16	$\cdots$
$\delta_X(d)$	9	4	1	$\cdots$
$fp_{I(X)}$	6	3	1	$\cdots$

Este exemplo foi feito computacionalmente e seu código pode ser encontrado no exemplo 7.2 de [8]. Observe que a função pegada de $I(X)$ pode fornecer uma boa cota inferior, principalmente nas condições do teorema anterior. Este exemplo também demonstra que todo o nosso trabalho e desenvolvimento teórico tem aplicações boas na teoria dos códigos projetivos de tipo Reed-Muller.

Referências Bibliográficas

[1] BUCHBERGER, B.. A theoretical basis for the reduction of polynomials to canonical forms, SIGSAM Bull. (An English Translation appeared in J. Symbolic Comput. 41 (2006) 475 - 511.

[2] CARVALHO, Cícero. Gröbner bases methods in coding theory. American Mathematical Society, v. 642, p. 73-86, 2015.

[3] COX, D.; LITTLE, J.; O'SHEA, D.. Ideals, Varieties and Algorithms, An Introduction to Computational Algebraic Geometry and Commutative Algebra, Springer, 3ª edição.

[4] FULTON, W.. Algebraic Curves - An Introduction to Algebraic Geometry. Local: http://www.math.lsa.umich.edu/∼wfulton/, 2008.

[5] GEIL, Olav. On the second weight of generalized Reed-Muller codes. Des. Codes Cryptogr. 48 (2008) 323-330.
https://doi.org/10.1007/s10623-008-9211-9

[6] HASSETT, Brendan. Introduction to Algebraic Geometry. Cambridge University Press, 2007.
https://doi.org/10.1017/CBO9780511755224

[7] KEMPER, G.. A Course in Commutative Algebra. Springer-Verlag, Berlin e Heidelberg 2011.
https://doi.org/10.1007/978-3-642-03545-6

[8] MARTÍNEZ-BERNAL, J.; PITONES, Y.; VILLAREAL, R. H.. Minimum distance functions of graded ideals and Reed-Muller-type codes. Journal of Pure and Applied Algebra 221 (2017), pág. 251 - 275.
https://doi.org/10.1016/j.jpaa.2016.06.006

[9] ZARISKI, Oscar.; SAMUEL, Pierre. Graduate Texts in Mathematics 29 - Commutative Algebra, volume II. Springer-Verlag, New York.