

Alef Alves Fidelis

Códigos cartesianos afins e seus duais

Uberlândia - Minas Gerais, Brasil

2025

Alef Alves Fidelis

Códigos cartesianos afins e seus duais

Dissertação apresentada ao Instituto de Matemática e Estatística como requisito parcial para obtenção do título de Mestre em Matemática.

Universidade Federal de Uberlândia – UFU

Instituto de Matemática e Estatística – IME

Programa de Pós-Graduação em Matemática - PPGMAT

Mestrado em Matemática

Orientador: Cícero Fernandes de Carvalho

Uberlândia - Minas Gerais, Brasil

2025

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

F451 2025	Fidelis, Alef Alves, 2000- Códigos afins e seus duais [recurso eletrônico] / Alef Alves Fidelis. - 2025. 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.2025.132 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

Alef Alves Fidelis

Códigos cartesianos afins e seus duais

Dissertação apresentada ao Instituto de Matemática e Estatística como requisito parcial para obtenção do título de Mestre em Matemática.

Trabalho _____. Uberlândia, _____ de _____ de _____:

Cícero Fernandes de Carvalho
Orientador

Victor Gonzalo Lopez Neumann
Examinador 1

Pietro Speziali
Examinador 2

Uberlândia - Minas Gerais, Brasil
2025



UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Coordenação do Programa de Pós-Graduação em Matemática

Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 158 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902

Telefone: (34) 3239-4209/4154 - www.ppmat.ime.ufu.br - ppmat@ime.ufu.br



ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, 122, PPGMAT				
Data:	26 de fevereiro de 2025	Hora de início:	10:00	Hora de encerramento:	12:00
Matrícula do Discente:	12312MAT001				
Nome do Discente:	Alef Alves Fidelis				
Título do Trabalho:	Códigos cartesianos afins e seus duais				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Códigos monomiais generalizados e seus duais				

Reuniu-se na Sala 1F 119 (Sala Multiuso do Instituto de Matemática e Estatística) - Bloco 1F (Campus Santa Mônica) da Universidade Federal de Uberlândia, e também por videoconferência, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Pietro Speziali - IMECC-Unicamp ; Victor Neumann - IME/ UFU; e Cícero Fernandes de Carvalho- IME/UFU, orientador do candidato.

Iniciando os trabalhos o presidente da mesa, Dr. Cícero Fernandes de Carvalho , apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao Discente a palavra para a exposição do seu trabalho.

A duração da apresentação do Discente e o tempo de arguição e resposta foram conforme as normas do Programa. A seguir o senhor presidente concedeu a palavra, pela ordem sucessivamente, aos examinadores, que passaram a arguir o candidato. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o candidato:

Aprovado.

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.



Documento assinado eletronicamente por **Cícero Fernandes de Carvalho, Professor(a) do Magistério Superior**, em 26/02/2025, às 12:18, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann, Professor(a) do Magistério Superior**, em 26/02/2025, às 15:03, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Pietro Speziali, Usuário Externo**, em 26/02/2025, às 15:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5999492** e o código CRC **27F0C3D8**.

*Aos matemáticos que vieram antes de mim, cuja dedicação tornou este trabalho possível.
Aos que virão depois, que ele sirva como alicerce para o contínuo desenvolvimento da
Matemática.*

Agradecimentos

Agradeço, primeiramente, a todo e qualquer brasileiro que já existiu, seja natural ou assimilado. Graças à força e ao sacrifício de milhões de pessoas ao longo da história, tive a oportunidade de estar presente neste tempo e espaço. Pude ter acesso à alimentação, transporte, educação, saúde, segurança e tantas outras condições essenciais. Fui contemplado com uma graduação gratuita e de qualidade, que pude concluir e, assim, exercer a profissão para a qual fui formado.

Expresso também minha gratidão a todos os professores que contribuíram para minha formação, desde a infância até este momento. Agora, ao concluir meu mestrado, tenho a certeza de que fiz a escolha certa ao trilhar os caminhos da Matemática.

Agradeço ao meu orientador, Cícero Fernandes de Carvalho, por enxergar potencial no meu trabalho, me convidar para o programa e aceitar me orientar. Foram dois anos (ou três, para ser mais exato) de aprendizado e discussões valiosas — não apenas sobre Matemática, mas também sobre docência, gestão, possibilidades e futuro.

Sou grato à CAPES pelo fomento à pesquisa que desenvolvi durante o último ano do mestrado.

Por fim, mas não menos importante, agradeço aos colegas e amigos que fiz durante esse período. No mestrado, construí amizades que levarei para a vida, afinal, continuaremos trabalhando juntos. No ambiente profissional, tive a oportunidade de enxergar antigos professores como pares — em especial, Raquel Bodart e Leandro Martins, meus ex-professores de Matemática e hoje colegas de trabalho, que sempre me incentivaram a seguir esse percurso.

“Matemática não é sobre números, equações,
cálculos ou algoritmos: é sobre compreensão.”
(William Paul Thurston)

Resumo

Neste trabalho, abordamos conceitos e exploramos resultados sobre Códigos Corretores de Erro, com foco nos códigos afins e seus códigos duais. O estudo de códigos corretores é uma área fundamental da Teoria da Informação e desempenha um papel crucial na detecção e correção de erros em transmissões de dados, sendo amplamente utilizado em comunicações digitais e armazenamento de informações. Para embasar nosso estudo, realizamos uma revisão detalhada de conceitos fundamentais, essenciais para a compreensão dos resultados apresentados. Entre eles, destacamos as Bases de Gröbner de um ideal, o Critério de Buchberger para um subconjunto de polinômios de múltiplas variáveis e o Algoritmo de Buchberger, que é uma ferramenta central na manipulação algébrica de polinômios. Além disso, abordamos o conceito de Pegada, a noção de Variedade Afim e propriedades fundamentais de corpos finitos, que desempenham um papel importante na construção e análise dos códigos considerados. Em seguida, introduzimos os conceitos básicos da Teoria dos Códigos, identificamos seus principais parâmetros e discutimos sua relevância no contexto da codificação da informação. Posteriormente, apresentamos a construção de códigos afins por meio da função avaliação, exploramos técnicas para identificar uma base para esses códigos utilizando a Pegada e realizamos o cálculo de sua dimensão. Por fim, focamos na caracterização do dual de um código afim, utilizando a função resíduo para determinar suas propriedades estruturais e identificar uma base correspondente. Esse estudo permite compreender melhor a relação entre um código e seu dual, além de fornecer ferramentas importantes para a análise de suas aplicações. Ao longo do texto, optamos por incluir diversos exemplos práticos para ilustrar e facilitar a compreensão dos conceitos apresentados. Acreditamos que a combinação de fundamentação teórica e exemplos concretos contribui significativamente para a assimilação do conteúdo, tornando o trabalho mais acessível e didático para o leitor.

Palavras-chaves: Bases de Gröbner. Pegadas. Variedades afins. Corpos finitos. Códigos corretores de erro. Códigos afins. Dual de um código afim.

Abstract

In this work, we discuss concepts and explore results on Error-Correcting Codes, focusing on affine codes and their dual codes. The study of error-correcting codes is a fundamental area of Information Theory and plays a crucial role in detecting and correcting errors in data transmission, being widely used in digital communications and data storage. To support our study, we conduct a detailed review of fundamental concepts essential for understanding the presented results. Among these, we highlight Gröbner bases of an ideal, Buchberger's criterion for a subset of multivariate polynomials, and Buchberger's algorithm, which is a central tool in the algebraic manipulation of polynomials. Additionally, we discuss the concept of footprint, the notion of affine variety, and fundamental properties of finite fields, which play an important role in the construction and analysis of the considered codes. Next, we introduce the basic concepts of Coding Theory, identify its key parameters, and discuss its relevance in the context of information encoding. Subsequently, we present the construction of affine codes through the evaluation function, explore techniques for identifying a basis for these codes using the footprint, and calculate their dimension. Finally, we focus on characterizing the dual of an affine code, using the residue function to determine its structural properties and identify a corresponding basis. This study provides a better understanding of the relationship between a code and its dual and offers important tools for analyzing its applications. Throughout the text, we have included several practical examples to illustrate and facilitate the understanding of the presented concepts. We believe that combining theoretical foundations with concrete examples significantly contributes to content assimilation, making the work more accessible and didactic for the reader.

Key-words: Gröbner bases. Footprints. Affine varieties. Finite fields. Error-correcting codes. Affine codes. Dual of an affine code.

Résumé

Dans ce travail, nous abordons des concepts et explorons des résultats sur les codes correcteurs d'erreurs, en nous concentrant sur les codes affines et leurs codes duaux. L'étude des codes correcteurs d'erreurs est un domaine fondamental de la théorie de l'information et joue un rôle crucial dans la détection et la correction des erreurs lors de la transmission des données, étant largement utilisée dans les communications numériques et le stockage de l'information. Pour soutenir notre étude, nous réalisons une revue détaillée des concepts fondamentaux essentiels à la compréhension des résultats présentés. Parmi eux, nous mettons en avant les bases de Gröbner d'un idéal, le critère de Buchberger pour un sous-ensemble de polynômes à plusieurs variables et l'algorithme de Buchberger, qui est un outil central dans la manipulation algébrique des polynômes. De plus, nous abordons le concept d'empreinte, la notion de variété affine et les propriétés fondamentales des corps finis, qui jouent un rôle important dans la construction et l'analyse des codes étudiés. Ensuite, nous introduisons les concepts de base de la théorie des codes, identifions leurs paramètres fondamentaux et discutons de leur importance dans le contexte de l'encodage de l'information. Par la suite, nous présentons la construction des codes affines à l'aide de la fonction d'évaluation, explorons des techniques pour identifier une base pour ces codes en utilisant l'empreinte et calculons leur dimension. Enfin, nous nous concentrons sur la caractérisation du dual d'un code affine, en utilisant la fonction résidu pour déterminer ses propriétés structurelles et identifier une base correspondante. Cette étude permet une meilleure compréhension de la relation entre un code et son dual et fournit des outils importants pour analyser leurs applications. Tout au long du texte, nous avons inclus plusieurs exemples pratiques pour illustrer et faciliter la compréhension des concepts présentés. Nous pensons que la combinaison des fondements théoriques et des exemples concrets contribue de manière significative à l'assimilation du contenu, rendant ce travail plus accessible et didactique pour le lecteur.

Mots-clés : Bases de Gröbner. Empreintes. Variétés affines. Corps finis. Codes correcteurs d'erreurs. Codes affines. Dual d'un code affine.

Lista de ilustrações

Figura 1	– Em azul, temos os monômios líderes da base de Gröbner de I e, em vermelho, temos os monômios que pertencem a pegada $\Delta(I)$	42
Figura 2	– Em azul a variedade afim de $I = \langle Y - X^2 \rangle \subseteq \mathbb{R}[X, Y]$	45
Figura 3	– Em azul a variedade afim de $J = \langle X^2 + Y^2 - 9 \rangle$. Em vermelho a variedade afim de $K = \langle Y^2 - X \rangle$. Em verde a variedade afim de $I = \langle X^2 + Y^2 - 9, Y^2 - X \rangle$	45
Figura 4	– Em azul, os monômios líderes de f_1 e f_2 e, em vermelho, os monômios de $\Delta(I)$	67

Sumário

	Introdução	23
I	PRELIMINARES	27
1	BASES DE GRÖBNER, PEGADAS E VARIEDADES AFINS	29
1.1	Monômios e ordens monomiais	29
1.2	Bases de Gröbner	32
1.3	Pegada de um ideal	40
1.4	Variedades afins	44
2	CORPOS FINITOS	49
2.1	Característica de um corpo	49
II	CÓDIGOS CORRETORES DE ERRO AFINS	59
3	CÓDIGOS CORRETORES DE ERRO	61
3.1	Conceitos básicos	61
3.2	Construção dos códigos afins	64
3.3	Duais de códigos afins	76
	Conclusão	85
	REFERÊNCIAS	87
	ÍNDICE REMISSIVO	87

Introdução

Através da colaboração da matemática pura, engenharia e necessidades práticas, a origem da história dos Códigos Corretores de Erro remontam à Segunda Guerra Mundial impulsionada, principalmente, por desafios militares e tecnológicos. Nesta época os sistemas de comunicação e computação eram primitivos, compostos primariamente por radares e relés mecânicos. Por isso esses dispositivos falhavam devido a interferências ou ruídos, ou seja, a correção de erros tornou-se uma prioridade para garantir a confiabilidade de transmissões críticas, como ordens militares ou dados de mísseis.

O primeiro registro dessa nova teoria matemática foi em (SHANNON, 1948), artigo em que o autor estabeleceu os fundamentos teóricos para a correção de erros, mostrando que é possível transmitir informações através de canais com presença de ruídos, desde que certa redundância seja acrescentada nas mensagens. E, dando continuidade ao trabalho estabelecido, em (HAMMING, 1950), o autor desenvolveu os Códigos de Hamming, capazes de detectar e corrigir um erro em conjuntos de dados binários. Esses códigos foram rapidamente adotados em memórias de computadores, marcando a primeira aplicação prática da Teoria de Códigos Corretores de Erro.

Já de forma paralela, em (GOLAY, 1949), o autor propôs Código de Golay, um código perfeito (veja 3.1.5) que corrigia até três erros em blocos de 23 bits. Apesar de sua elegância e robustez matemática, inicialmente seu uso prático foi limitado devido sua complexidade.

Na década de 1950, os matemáticos Irving S. Reed e David Muller escreveram diversos artigos em que desenvolviam os Códigos de Reed-Muller. Baseados em polinômios sobre o corpo finito $\mathbb{F}_2$, esses códigos usavam “lógica majoritária” para decodificação, permitindo corrigir múltiplos erros. Sua aplicação inicial foi em sistemas militares, como o míssil SNARK, cujos frequentes desvios de rota motivaram a busca por soluções robustas.

Por sua vez, na década de 1960, David Muller trabalhou em conjunto com o matemático Gustave Solomon para desenvolver os Códigos de Reed-Solomon. Utilizando corpos finitos $\mathbb{F}_q$, com $q \geq 2$, em que os símbolos não binários (como bytes) substituíam bits, esses códigos permitiam corrigir erros em conjuntos maiores de dados. Apesar de revolucionários, foram inicialmente considerados impraticáveis devido à exigência computacional. Somente na década de 1970, com o algoritmo de Elwyn Berlekamp e James Massey para decodificação eficiente, os Códigos de Reed-Solomon ganharam adoção massiva.

A Administração Nacional da Aeronáutica e Espaço (NASA) foi pioneira na aplicação desses códigos em missões espaciais, como podemos destacar nos seguintes trechos:

Em 1965, a nave espacial *Mariner 4* transmitiu 22 fotos em preto e branco de Marte usando o seguinte sistema: cada foto foi decomposta em 200×200 elementos de imagem e, a cada elemento da imagem, foi atribuído um dos 64 tons de cinza pré-escolhidos e codificados como elementos de $\{0, 1\}^6$, correspondendo ao código da fonte. Esses vetores eram transmitidos sem nenhuma codificação de canal, pois o transmissor era tão lento que levava oito horas para complementar a transmissão de uma foto. (HEFEZ; VILLELA, 2017, p.3).

No qual segue:

Em 1972, a nave espacial *Mariner 9* transmitiu novas imagens de Marte. Dessa vez cada imagem foi decomposta em 700×832 elementos, aumentando consideravelmente a resolução. O código fonte foi mantido; mas, tirando-se partido do aumento da velocidade de transmissão de dados alcançada, foi possível recodificar o código através de uma aplicação injetora ϕ de $\{0, 1\}^6$ em $\{0, 1\}^{32}$ de modo que o código de canal resultante fosse capaz de detectar e corrigir até sete erros [...] (HEFEZ; VILLELA, 2017, p.3).

E por fim:

Em 1979, a nave espacial *Voyager* transmitiu imagens coloridas de Júpiter. A transmissão de imagens coloridas é na realidade uma sequência de imagens em preto e branco tiradas através de vários filtros. Cada elemento de imagem foi representado por uma das 4096 ($= 2^{12}$) tonalidades de cinza previamente escolhidas, aumentando consideravelmente a precisão de cada imagem. O codificador da fonte usava, portanto, 12 bits binários e o codificador de canal usava 24 bits. Esse código, chamado Código de Golay, era capaz de corrigir até três erros cometidos nos 24 bits de informações transmitidos. (HEFEZ; VILLELA, 2017, p.4).

A partir da década de 1980, essas tecnologias foram aplicadas para fins comerciais: CDs e DVDs usavam Códigos de Reed-Solomon para corrigir riscos e poeira, enquanto sistemas de transmissão digital (TV, Wi-Fi) e padrões como QR Code os incorporaram para garantir confiabilidade. Além disso, a teoria evoluiu com contribuições como os Códigos Turbo (1993) e Códigos Polares (2008), que hoje sustentam redes 5G e comunicações quânticas.

Nesta dissertação, buscamos definir e explorar resultados sobre os Códigos Afins, um caso particular dos Códigos Cartesianos Afins, amplamente utilizados em aplicações como comunicações por satélite, criptografia e computação quântica, cujos primeiros trabalhos advêm do matemático David Slepian. Para isso, estruturamos o trabalho em duas partes: I - Preliminares; II - Códigos Corretores de Erro Afins.

Parte I - Preliminares: Nesta seção, apresentamos os conceitos fundamentais necessários para a compreensão da Teoria dos Códigos Corretores de Erro, bem como das ferramentas utilizadas na construção dos Códigos Afins. Iniciamos com definições e resultados sobre monômios e ordens monomiais, com ênfase no algoritmo de divisão de um

polinômio de múltiplas variáveis por uma lista de polinômios. Em seguida, introduzimos o conceito de Base de Gröbner e estabelecemos sua relação com a Pegada, demonstrando que esses conceitos são equivalentes. Além disso, apresentamos resultados pontuais sobre variedades afins e corpos finitos, elementos essenciais para a construção dos Códigos Afins.

Parte II - Códigos Corretores de Erro Afins: Nesta parte, abordamos os conceitos fundamentais dos Códigos Corretores de Erro, incluindo seus principais parâmetros: comprimento, dimensão e distância mínima. Em seguida, considerando um ideal $I \subseteq \mathbb{F}_q[\mathbf{X}]$, construímos a função avaliação ϕ e definimos um Código de Variedade Afim como sendo a imagem de ϕ . A partir disso, tomando um subconjunto não vazio $\mathcal{S} \subseteq \mathbb{F}_q^n$ e um inteiro $d \geq 0$, construímos um Código Afim sobre esse conjunto. Exploramos diversas propriedades desses códigos, incluindo a descrição de uma base e o cálculo de sua dimensão. Por fim, analisamos o dual de um Código Afim e, por meio da função resíduo $\text{Res}_{\mathcal{S}}$, mostramos como identificá-lo e construir uma base para ele.

Parte I

Preliminares

1 Bases de Gröbner, pegadas e variedades afins

Neste capítulo trazemos alguns conceitos e resultados fundamentais sobre polinômios de várias variáveis. Nosso objetivo aqui é estabelecer as bases para a construção dos Códigos afins. Para tanto, fazemos uso principalmente das referências (CARVALHO, 2017) e (COX; LITTLE; O'SHEA, 2015).

1.1 Monômios e ordens monomiais

Seja $\mathbb{K}$ um corpo e denote por $\mathbb{K}[\mathbf{X}]$ o anel de polinômios $\mathbb{K}[X_1, X_2, \dots, X_{n-1}, X_n]$, isto é, o anel de polinômios com coeficientes no corpo $\mathbb{K}$ e variáveis $X_1, \dots, X_n$, com $n \in \mathbb{Z}_+^*$.

Definição 1.1.1 (Termos e monômios). *Um produto do tipo*

$$aX_1^{\alpha_1}X_2^{\alpha_2}\dots X_{n-1}^{\alpha_{n-1}}X_n^{\alpha_n},$$

com $a \in \mathbb{K}^*$ e $\alpha_1, \dots, \alpha_n \in \mathbb{Z}_+$ é chamado de termo, enquanto que

$$X_1^{\alpha_1}X_2^{\alpha_2}\dots X_{n-1}^{\alpha_{n-1}}X_n^{\alpha_n},$$

é chamado de monômio.

Um monômio $X_1^{\alpha_1}X_2^{\alpha_2}\dots X_{n-1}^{\alpha_{n-1}}X_n^{\alpha_n}$ também pode ser denotado por $\mathbf{X}^\alpha$, em que $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_+^n$. Além disso, denotaremos por $\mathcal{M}$ o conjunto de todos os monômios de $\mathbb{K}[\mathbf{X}]$.

Dado um polinômio $f \in \mathbb{K}[\mathbf{X}]$, diremos que um monômio M aparece em f se o coeficiente de M em f é não nulo.

Definição 1.1.2 (Ordem monomial). *Uma ordem monomial em $\mathcal{M}$ é uma ordem total $\preceq$ definida sobre $\mathcal{M}$ tal que:*

1. se $\mathbf{X}^\alpha \preceq \mathbf{X}^\beta$, então $\mathbf{X}^{\alpha+\gamma} \preceq \mathbf{X}^{\beta+\gamma}$, para todos os $\alpha, \beta, \gamma \in \mathbb{Z}_+^n$;
2. qualquer subconjunto não vazio $\mathcal{A} \subset \mathcal{M}$ possui um menor elemento.

Agora, apresentaremos algumas ordens monomiais.

Exemplo 1.1.3 (Ordem lexicográfica). *A ordem lexicográfica é definida como $\mathbf{X}^\alpha \preceq_{lex} \mathbf{X}^\beta$ se $\alpha = \beta$ ou se a primeira entrada não nula da esquerda para a direita em $\beta - \alpha$ é positiva. Assim, $X_n \preceq_{lex} \dots \preceq_{lex} X_1$.*

Exemplo 1.1.4 (Ordem lexicográfica graduada). A ordem lexicográfica graduada é definida como $\mathbf{X}^\alpha \preceq \mathbf{X}^\beta$ se $\alpha = \beta$ ou $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$, ou se $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$, então $\mathbf{X}^\alpha \preceq_{lex} \mathbf{X}^\beta$.

Exemplo 1.1.5 (Ordem lexicográfica graduada inversa). A ordem lexicográfica graduada inversa é definida como $\mathbf{X}^\alpha \preceq \mathbf{X}^\beta$ se $\alpha = \beta$ ou $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$, ou se $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$, então a primeira entrada não nula da direita para a esquerda em $\beta - \alpha$ é negativa.

Definição 1.1.6 (Monômios, coeficientes e termos líderes). Seja $f = \sum_{i=1}^m a_i M_i \in \mathbb{K}[\mathbf{X}]$ um polinômio não nulo com $a_i \in \mathbb{K}$, em que $a_i \neq 0$, e $M_i \in \mathcal{M}$, para todo $i = 1, \dots, m$, e considere $\preceq$ uma ordem monomial definida em $\mathcal{M}$. Então, o monômio líder de f (com respeito a $\preceq$) é

$$M_l = \max\{M_i \in \mathcal{M} \mid i = 1, \dots, m\},$$

o coeficiente líder de f é a_l e o termo líder de f é $a_l M_l$.

Denotaremos esses três elementos por $M_l = \text{ml}(f)$, $a_l = \text{cl}(f)$ e $a_l M_l = \text{tl}(f)$.

Exemplo 1.1.7. Se tomarmos $f = 4X_1^3X_2^4 + 5X_1X_3^8 + 6X_1^2X_3^7 + 2 \in \mathbb{R}[X_1, X_2, X_3]$ com o conjunto dos monômios munida da:

1. ordem lexicográfica, então:

- $\text{ml}(f) = X_1^3X_2^4$;
- $\text{cl}(f) = 4$;
- $\text{tl}(f) = 4X_1^3X_2^4$;

2. ordem lexicográfica graduada, então:

- $\text{ml}(f) = X_1^2X_3^7$;
- $\text{cl}(f) = 5$;
- $\text{tl}(f) = 5X_1X_3^8$;

3. ordem lexicográfica graduada inversa, então:

- $\text{ml}(f) = X_1^2X_3^7$;
- $\text{cl}(f) = 6$;
- $\text{tl}(f) = 6X_1^2X_3^7$.

Definição 1.1.8 (Divisão de um polinômio por uma lista de polinômios não nulos). Dividir $f \in \mathbb{K}[\mathbf{X}]$ por $\{g_1, \dots, g_t\} \subset \mathbb{K}[\mathbf{X}] \setminus \{0\}$, com respeito à uma ordem monomial $\preceq$, significa encontrar quocientes $q_1, \dots, q_t \in \mathbb{K}[\mathbf{X}]$ e um resto $r \in \mathbb{K}[\mathbf{X}]$ tais que

$$f = q_1g_1 + \dots + q_tg_t + r,$$

com $r = 0$ ou nenhum monômio que aparece em r sendo múltiplo de $\text{ml}(g_i)$, para todo $i = 1, \dots, t$.

Exemplo 1.1.9. Consideremos o anel de polinômios $\mathbb{R}[X, Y]$ cujo conjunto de monômios está munido com a ordem lexicográfica. Na divisão de $f = X^2Y + XY^2 + Y^2 \in \mathbb{R}[X, Y]$ por $\{g_1 = XY - 1, g_2 = Y^2 - 1\} \subset \mathbb{R}[X, Y]$ temos $q_1 = X + Y$, $q_2 = 1$ e $r = X + Y + 1$, ou seja,

$$f = (X + Y)(XY - 1) + 1(Y^2 - 1) + X + Y + 1.$$

De fato, faremos essa divisão passo-a-passo:

- (i) Note que $\text{ml}(f) = X^2Y$ é um múltiplo de $\text{ml}(g_1) = XY$. Temos $\text{ml}(f) = X \text{ml}(g_1)$. Então escrevemos

$$\begin{aligned} f &= X^2Y + XY^2 + Y^2 \\ &= Xg_1 + X + XY^2 + Y^2. \end{aligned}$$

- (ii) Agora, note que $\text{ml}(X + XY^2 + Y^2) = XY^2$ também é um múltiplo de $\text{ml}(g_1) = XY$. Temos $XY^2 = Y \text{ml}(g_1)$. Então escrevemos

$$\begin{aligned} f &= Xg_1 + X + XY^2 + Y^2 \\ &= Xg_1 + Yg_1 + X + Y + Y^2 \\ &= (X + Y)g_1 + X + Y + Y^2. \end{aligned}$$

- (iii) Observe que $\text{ml}(X + Y + Y^2) = X$, o qual não é múltiplo de $\text{ml}(g_1) = XY$ nem de $\text{ml}(g_2) = Y^2$. Neste caso, consideraremos X como parte do resto dessa divisão. Então escrevemos

$$\begin{aligned} f &= (X + Y)g_1 + X + Y + Y^2 \\ &= (X + Y)g_1 + Y + Y^2 + r_1, \end{aligned}$$

em que $r_1 = X$.

- (iv) Por sua vez, $\text{ml}(Y + Y^2) = Y^2$ não é múltiplo de $\text{ml}(g_1) = XY$, porém é múltiplo de $\text{ml}(g_2) = Y^2$. Temos $Y^2 = 1 \text{ml}(g_2)$. Então escrevemos

$$\begin{aligned} f &= (X + Y)g_1 + Y + Y^2 + r_1 \\ &= (X + Y)g_1 + 1g_2 + Y + 1 + r_1. \end{aligned}$$

- (v) Como os termos em $Y + 1$ não são múltiplos de $\text{ml}(g_1) = XY$ nem de $\text{ml}(g_2) = Y^2$, os consideraremos parte do resto. Então escrevemos

$$\begin{aligned} f &= (X + Y)g_1 + 1g_2 + Y + 1 + r_1 \\ &= (X + Y)g_1 + 1g_2 + r, \end{aligned}$$

em que $r = Y + 1 + r_1$.

Assim, temos que

$$\begin{aligned} f &= (X + Y)g_1 + 1g_2 + r \\ &= (X + Y)(XY - 1) + 1(Y^2 - 1) + X + Y + 1. \end{aligned}$$

Ainda é possível escrever esse processo de divisão no algoritmo da divisão “convencional”. Na sequência escrevemos ele relacionando com os passos que foram feitos.

	$X^2Y + XY^2 + Y^2$	$XY - 1$	$Y^2 - 1$	Resto
(i)	$- \frac{X^2Y - X}{X + XY^2 + Y^2}$	$X + Y$	1	$X + Y + 1$
(ii)	$- \frac{XY^2 - Y}{X + Y + Y^2}$			
(iii)	$- \frac{X}{Y + Y^2}$			
(iv)	$- \frac{Y^2 - 1}{Y + 1}$			
(v)	$- \frac{Y + 1}{0}$			

O que fizemos nessa divisão foi similar ao que se faz na divisão de dois polinômios de uma única variável. Utilizamos os termos líderes de g_1 e g_2 para eliminar o termo líder de f e os termos líderes dos subsequentes polinômios que apareceram no processo intermediário da divisão. Isso poderia ter sido feito para qualquer lista finita de polinômios não nulos. É importante observar que do algoritmo da divisão obtemos um resto que, se não for nulo, tem um monômio líder que é menor ou igual ao monômio líder de f .

Além disso, na divisão que fizemos levamos em consideração a ordem de divisores, isto é, dividimos f por g_1, g_2 (de fato, dividimos f pela sequência (g_1, g_2)). Se invertemos a ordem da divisão, isto é, se dividirmos f por g_2, g_1 , teremos $q_2 = X + 1, q_1 = X$ e $r = 2X + 1$, ou seja,

$$f = (X + 1)(Y^2 - 1) + X(XY - 1) + 2X + 1.$$

1.2 Bases de Gröbner

Definição 1.2.1 (Bases de Gröbner). *Seja $I \subset \mathbb{K}[\mathbf{X}]$ um ideal não nulo e considere $\mathcal{M}$ com uma ordem monomial $\preceq$. Um conjunto $\{g_1, \dots, g_t\} \subset I$ é uma base de Gröbner para I , com respeito a ordem monomial $\preceq$, se para todo $f \in I$, com $f \neq 0$, temos que $\text{ml}(f)$ é um múltiplo de $\text{ml}(g_i)$, para algum $i = 1, \dots, t$.*

Exemplo 1.2.2. *Seja $I = \langle XY - 1, Y^2 - 1 \rangle \subset \mathbb{R}[X, Y]$ e considere $\mathcal{M}$ com a ordem lexicográfica, em que $Y \preceq_{lex} X$. Então $\{XY - 1, Y^2 - 1\}$ não é uma base de Gröbner para I .*

De fato, se considerarmos o polinômio $-Y + X$ temos que

$$-Y + X = Y(XY - 1) - X(Y^2 - 1) \in I,$$

mas $\text{ml}(-Y + X) = X$ não é múltiplo de $\text{ml}(XY - 1) = XY$ nem de $\text{ml}(Y^2 - 1) = Y^2$. Portanto, $\{XY - 1, Y^2 - 1\}$ não pode ser uma base de Gröbner para I , com respeito à $\preceq_{lex}$.

Agora, assumiremos que $\mathcal{M}$ sempre está munido de uma ordem monomial fixa e que $I \neq \langle 0 \rangle$. Mostraremos em seguida que uma base de Gröbner para I é de fato uma base para I .

Lema 1.2.3. *Seja $\{g_1, \dots, g_t\} \subset I$ uma base de Gröbner para I . Então $f \in I$ se, e somente se, o resto da divisão de f por $\{g_1, \dots, g_t\}$ é zero. Como consequência, $I = \langle g_1, \dots, g_t \rangle$.*

Demonstração. Mostremos a suficiência. Se o resto da divisão de f por $\{g_1, \dots, g_t\}$ é zero, temos que

$$f = q_1 g_1 + \dots + q_t g_t,$$

em que $q_i \in \mathbb{K}[\mathbf{X}]$, para todo $i = 1, \dots, t$. Portanto, por definição de ideal de um anel, temos que $f \in I$.

Agora, mostremos a necessidade. Sejam $f \in I$ e

$$f = q_1 g_1 + \dots + q_t g_t + r$$

a divisão de f por $\{g_1, \dots, g_t\}$. Então,

$$r = f - q_1 g_1 - \dots - q_t g_t \in I.$$

Portanto, devemos ter $r = 0$ pois, caso contrário, r seria um polinômio não nulo em I cujo monômio líder não é múltiplo de $\text{ml}(g_i)$, para qualquer $i = 1, \dots, t$, contrariando a hipótese de $\{g_1, \dots, g_t\}$ ser uma base de Gröbner para I . Além disso, isso mostra que $I \subset \langle g_1, \dots, g_t \rangle$ e a fortiori $I = \langle g_1, \dots, g_t \rangle$. ■

Uma importante propriedade para uma base de Gröbner é a seguinte:

Proposição 1.2.4. *Seja $\{g_1, \dots, g_t\} \subset I$ uma base de Gröbner para I . Na divisão de $f \in \mathbb{K}[\mathbf{X}]$ por $\{g_1, \dots, g_t\}$ o resto é sempre o mesmo, independentemente da ordem que tomarmos para $g_1, \dots, g_t$ no algoritmo da divisão.*

Demonstração. Assuma que

$$\begin{aligned} f &= q_1 g_1 + \cdots + q_t g_t + r \\ &= \tilde{q}_1 g_1 + \cdots + \tilde{q}_t g_t + \tilde{r}, \end{aligned}$$

em que $q_i, \tilde{q}_i \in \mathbb{K}[\mathbf{X}]$, para todo $i = 1, \dots, t$, e $r, \tilde{r} \in \mathbb{K}[\mathbf{X}]$ com nenhum monômio aparecendo em r ou em $\tilde{r}$ sendo múltiplo de $\text{ml}(g_i)$, para qualquer $i = 1, \dots, t$. Como

$$r - \tilde{r} = (q_1 - \tilde{q}_1)g_1 + \cdots + (q_t - \tilde{q}_t)g_t \in I,$$

devemos ter $r - \tilde{r} = 0$ pois, caso contrário, $r - \tilde{r}$ seria um polinômio não nulo em I cujo monômio líder não é múltiplo de $\text{ml}(g_i)$, para qualquer $i = 1, \dots, t$, contradizendo o fato de $\{g_1, \dots, g_t\}$ ser uma base de Gröbner para I . ■

Até agora não está claro se todo ideal $I \subset \mathbb{K}[\mathbf{X}]$ admite uma base de Gröbner. Buchberger desenvolveu um algoritmo que, começando de qualquer base finita para I e aumentando-a, se necessário, em uma sequência finita de etapas, acaba em uma base “aumentada” que é uma base de Gröbner. Esse algoritmo recebe o nome de algoritmo de Buchberger, e usa o seguinte conceito:

Definição 1.2.5 (*S*-polinômio). *Sejam $f, g \in \mathbb{K}[\mathbf{X}] \setminus \{0\}$ com $\text{tl}(f) = a\mathbf{X}^\alpha$ e $\text{tl}(g) = b\mathbf{X}^\beta$. Considerando $\gamma_i = \max\{\alpha_i, \beta_i\}$, para todo $i = 1, \dots, n$, defina $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_n) \in \mathbb{Z}_+^n$. O *S*-polinômio de f e g é definido como*

$$S(f, g) = \frac{1}{a}\mathbf{X}^{\boldsymbol{\gamma}-\alpha}f - \frac{1}{b}\mathbf{X}^{\boldsymbol{\gamma}-\beta}g.$$

Exemplo 1.2.6. *Sejam $f, g \in \mathbb{R}[X, Y]$, em que $f = X^3Y^2 - X^2Y^3 + X$ e $g = 3X^4Y + Y^2$, com a ordem lexicográfica graduada, com $Y \preceq_{\text{lex}} X$. Então,*

$$S(f, g) = -X^3Y^3 + X^2 - \frac{1}{3}Y^3.$$

De fato, temos $\text{tl}(f) = X^3Y^2$ e $\text{tl}(g) = 3X^4Y$. Logo, $\boldsymbol{\gamma} = (4, 2)$ e, o *S*-polinômio de f e g é

$$\begin{aligned} S(f, g) &= Xf - \frac{1}{3}Yg \\ &= X(X^3Y^2 - X^2Y^3 + X) - \frac{1}{3}Y(3X^4Y + Y^2) \\ &= X^4Y^2 - X^3Y^3 - X^4Y^2 - \frac{1}{3}Y^3 \\ &= -X^3Y^3 + X^2 - \frac{1}{3}Y^3. \end{aligned}$$

Lema 1.2.7. *Sejam $g_1, \dots, g_t \in \mathbb{K}[\mathbf{X}] \setminus \{0\}$ tais que $\text{ml}(g_i) = \mathbf{X}^\alpha$, para todo $i = 1, \dots, t$, e considere $f = \sum_{i=1}^t a_i g_i$, com $a_i \in \mathbb{K}$ para todo $i = 1, \dots, t$. Se $\text{ml}(f) < \mathbf{X}^\alpha$, então f é uma combinação linear de $S(g_i, g_j)$, com $1 \leq i < j \leq t$, em que seus coeficientes estão em $\mathbb{K}$. Além disso, $\text{ml}(S(g_i, g_j)) < \mathbf{X}^\alpha$, com $1 \leq i < j \leq t$.*

Demonstração. Seja $\text{cl}(g_i) = b_i$, com $b_i \in \mathbb{K}$, para cada $i = 1, \dots, t$. Logo, $\text{tl}(g_i) = b_i \mathbf{X}^\alpha$, para cada $i = 1, \dots, t$. Como

$$\begin{aligned} \text{ml}(a_i g_i) &= \text{ml}(g_i) \\ &= \mathbf{X}^\alpha \end{aligned}$$

para todo $i = 1, \dots, t$, e $\text{ml}(f) < \mathbf{X}^\alpha$, temos que

$$\sum_{i=1}^t a_i b_i = 0.$$

Agora, por definição,

$$S(g_i, g_j) = \frac{1}{b_i} g_i - \frac{1}{b_j} g_j,$$

para todos $i, j = 1, \dots, t$ com $i \neq j$, pois $\text{ml}(g_i) = \mathbf{X}^\alpha = \text{ml}(g_j)$. Portanto,

$$\begin{aligned} f &= a_1 g_1 + \dots + a_t g_t \\ &= a_1 b_1 \left(\frac{1}{b_1} g_1 \right) + \dots + a_t b_t \left(\frac{1}{b_t} g_t \right) \\ &= a_1 b_1 \left(\frac{1}{b_1} g_1 - \frac{1}{b_2} g_2 \right) + (a_1 b_1 + a_2 b_2) \left(\frac{1}{b_2} g_2 - \frac{1}{b_3} g_3 \right) + \dots \\ &\quad \dots + (a_1 b_1 + \dots + a_{t-1} b_{t-1}) \left(\frac{1}{b_{t-2}} g_{t-2} - \frac{1}{b_{t-1}} g_{t-1} \right) + (a_1 b_1 + \dots + a_t b_t) \left(\frac{1}{b_t} g_t \right) \\ &= a_1 b_1 S(g_1, g_2) + (a_1 b_1 + a_2 b_2) S(g_2, g_3) + \dots + (a_1 b_1 + \dots + a_{t-1} b_{t-1}) S(g_{t-2}, g_{t-1}), \end{aligned}$$

pois $\sum_{i=1}^t a_i b_i = 0$, ou seja, f é uma combinação linear de $S(g_i, g_j)$, com $1 \leq i < j \leq t$, em que seus coeficientes estão em $\mathbb{K}$.

Além disso, como

$$\text{tl}(g_i) = b_i \mathbf{X}^\alpha \quad \text{e} \quad \text{tl}(g_j) = b_j \mathbf{X}^\alpha,$$

temos que

$$\begin{aligned} \text{ml}(S(g_i, g_j)) &= \text{ml} \left(\frac{1}{b_i} g_i - \frac{1}{b_j} g_j \right) \\ &< \mathbf{X}^\alpha, \end{aligned}$$

com $1 \leq i < j \leq t$. ■

Teorema 1.2.8 (Critério de Buchberger). *Seja $\{g_1, \dots, g_t\} \subset I$ tal que $I = \langle g_1, \dots, g_t \rangle$. Então, $\{g_1, \dots, g_t\}$ é uma base de Gröbner para I se, e somente se, para todos $i, j = 1, \dots, t$, com $i \neq j$, o resto da divisão de $S(g_i, g_j)$ por $\{g_1, \dots, g_t\}$ é zero, independentemente da ordem que tomarmos para $g_1, \dots, g_t$ no algoritmo da divisão.*

Demonstração. Mostremos a necessidade. Se $\{g_1, \dots, g_t\}$ é uma base de Gröbner para I , então pelo Lema 1.2.3, temos que o resto da divisão de $S(g_i, g_j)$ por $\{g_1, \dots, g_t\}$ é zero, pois $S(g_i, g_j) \in I$, para todos os $i, j = 1, \dots, t$, com $i \neq j$.

Agora, mostremos a suficiência. Assuma que para todos $i, j = 1, \dots, t$, com $i \neq j$, o resto da divisão de $S(g_i, g_j)$ por $\{g_1, \dots, g_t\}$ é zero. Seja $f \in I$, então existem polinômios $h_i \in \mathbb{K}[\mathbf{X}]$, com $i = 1, \dots, t$, tais que

$$f = \sum_{i=1}^t h_i g_i.$$

Além disso, considere

$$\mathbf{X}^\alpha = \max_{1 \leq i \leq t} (\text{ml}(h_i) \text{ml}(g_i)), \quad (1.1)$$

temos então que

$$\text{ml}(f) \leq \mathbf{X}^\alpha.$$

Suponha que $\mathbf{X}^\alpha$ seja o menor monômio que aparece na equação (1.1) quando consideramos todas as expressões de f como combinação linear de $\{g_1, \dots, g_t\}$. Vamos mostrar agora que não podemos ter $\text{ml}(f) < \mathbf{X}^\alpha$, e logo devemos ter $\text{ml}(f) = \mathbf{X}^\alpha$, o que implica que $\{g_1, \dots, g_t\}$ é uma base de Gröbner para I . Para ver que não acontece $\text{ml}(f) < \mathbf{X}^\alpha$, seja

$$S = \{i \in \mathbb{Z}_+^* \mid \text{ml}(h_i) \text{ml}(g_i) = \mathbf{X}^\alpha \text{ e } i = 1, \dots, t\}.$$

Para cada $i \in S$, seja $\text{tl}(h_i) = c_i \mathbf{X}_i^{\gamma_i}$, com $c_i \in \mathbb{K}$. Defina

$$g = \sum_{i \in S} c_i \mathbf{X}_i^{\gamma_i} g_i$$

e observe que $f = g + \sum_{i=1}^t \tilde{h}_i g_i$, em que $\text{ml}\left(\sum_{i=1}^t \tilde{h}_i g_i\right) < \mathbf{X}^\alpha$.

Então, $\text{ml}(\mathbf{X}_i^{\gamma_i} g_i) = \mathbf{X}^\alpha$, para todo $i \in S$, porém $\text{ml}(g) \leq \mathbf{X}^\alpha$, pois g é um polinômio formado somente pelos termos de f que possuem o coeficiente líder igual a $\mathbf{X}^\alpha$. Logo, pelo Lema 1.2.7, para todos $i, j \in S$, com $i \neq j$, existem $d_{ij} \in \mathbb{K}$ tais que

$$g = \sum_{\substack{i, j \in S \\ i \neq j}} d_{ij} S(\mathbf{X}_i^{\gamma_i} g_i, \mathbf{X}_j^{\gamma_j} g_j). \quad (1.2)$$

Agora, considerando

$$\text{tl}(g_i) = b_i \mathbf{X}^{\beta_i} \quad \text{e} \quad \text{tl}(g_j) = b_j \mathbf{X}^{\beta_j},$$

temos

$$\text{tl}(\mathbf{X}_i^{\gamma_i} g_i) = b_i \mathbf{X}_i^{\gamma_i} \mathbf{X}^{\beta_i} \quad \text{e} \quad \text{tl}(\mathbf{X}_j^{\gamma_j} g_j) = b_j \mathbf{X}_j^{\gamma_j} \mathbf{X}^{\beta_j},$$

para todos $i, j \in S$, com $i \neq j$. Assim, tomando $\beta_\ell = \max(\beta_{i_\ell}, \beta_{j_\ell})$, para $\ell = 1, \dots, n$, e $\beta = (\beta_1, \dots, \beta_n)$, temos

$$\begin{aligned}
 S(\mathbf{X}_i^{\gamma_i} g_i, \mathbf{X}_j^{\gamma_j} g_j) &= \frac{1}{b_i \mathbf{X}_i^{\gamma_i}} \mathbf{X}^{\alpha - \beta_i} \mathbf{X}_i^{\gamma_i} g_i - \frac{1}{b_j \mathbf{X}_j^{\gamma_j}} \mathbf{X}^{\alpha - \beta_j} \mathbf{X}_j^{\gamma_j} g_j \\
 &= \frac{1}{b_i} \mathbf{X}^{\alpha - \beta_i} g_i - \frac{1}{b_j} \mathbf{X}^{\alpha - \beta_j} g_j \\
 &= \frac{1}{b_i} \mathbf{X}^{\alpha - \beta + \beta - \beta_i} g_i - \frac{1}{b_j} \mathbf{X}^{\alpha - \beta + \beta - \beta_j} g_j \\
 &= \frac{1}{b_i} \mathbf{X}^{\alpha - \beta} \mathbf{X}^{\beta - \beta_i} g_i - \frac{1}{b_j} \mathbf{X}^{\alpha - \beta} \mathbf{X}^{\beta - \beta_j} g_j \\
 &= \mathbf{X}^{\alpha - \beta} \left(\frac{1}{b_i} \mathbf{X}^{\beta - \beta_i} g_i - \frac{1}{b_j} \mathbf{X}^{\beta - \beta_j} g_j \right) \\
 &= \mathbf{X}^{\alpha - \beta} S(g_i, g_j),
 \end{aligned}$$

para todos $i, j \in S$, com $i \neq j$.

Por hipótese, para todos os $i, j = 1, \dots, t$, com $i \neq j$, o resto da divisão de $S(g_i, g_j)$ por $\{g_1, \dots, g_t\}$ é zero, e logo o resto da divisão de $S(\mathbf{X}_i^{\gamma_i} g_i, \mathbf{X}_j^{\gamma_j} g_j) = \mathbf{X}^{\alpha - \beta} S(g_i, g_j)$ por $\{g_1, \dots, g_t\}$ também será zero, para todos $i, j \in S$, com $i \neq j$. Isto implica que

$$S(\mathbf{X}_i^{\gamma_i} g_i, \mathbf{X}_j^{\gamma_j} g_j) = \sum_{v=1}^t h_{ij_v} g_v, \quad (1.3)$$

em que

$$\begin{aligned}
 \max_{1 \leq v \leq t} (\text{ml}(h_{ij_v}) \text{ml}(g_v)) &= \text{ml}(S(\mathbf{X}_i^{\gamma_i} g_i, \mathbf{X}_j^{\gamma_j} g_j)) \\
 &< \max(\text{ml}(\mathbf{X}_i^{\gamma_i} g_i), \text{ml}(\mathbf{X}_j^{\gamma_j} g_j)) \\
 &= \mathbf{X}^\alpha.
 \end{aligned}$$

Lembramos que $f = g + \sum_{i=1}^t \tilde{h}_i g_i$, e das equações (1.2) e (1.3) temos

$$f = \left(\sum_{\substack{i,j \in S \\ i \neq j}} d_{ij} \sum_{v=1}^t h_{ij_v} g_v \right) + \sum_{i=1}^t \tilde{h}_i g_i$$

ou seja,

$$f = \sum_{i=1}^t h'_i g_i,$$

em que $h'_i \in \mathbb{K}$, para todo $i = 1, \dots, t$, isto é, f possui uma outra representação, com

$$\max_{1 \leq i \leq t} (\text{ml}(h'_i) \text{ml}(g_i)) < \mathbf{X}^\alpha$$

contradizendo a minimalidade de $\mathbf{X}^\alpha$. Portanto, não podemos ter $\text{ml}(f) < \mathbf{X}^\alpha$. ■

Note que o Teorema 1.2.8 nos dá uma ideia de como será o algoritmo para determinar uma base de Gröbner para um ideal I . Se $I = \langle g_1, \dots, g_t \rangle$, então verificaremos se para algum par de inteiros distintos $i, j = 1, \dots, t$ o resto da divisão de $S(g_i, g_j)$ por $\{g_1, \dots, g_t\}$ não é zero. Se não existir tal par, então $\{g_1, \dots, g_t\}$ é uma base de Gröbner para I . Porém caso exista, seja r_{ij} o resto dessa divisão, então fazemos $g_{t+1} = r_{ij}$ e consideramos agora o conjunto $\{g_1, \dots, g_t, g_{t+1}\}$. Claramente $I = \langle g_1, \dots, g_t, g_{t+1} \rangle$ pois $g_{t+1} \in I$. Repetimos o processo quantas vezes for necessário até obter uma base de Gröbner para I . Esse é o algoritmo de Buchberger, que apresentamos a seguir, e que após um número finito de passos sempre retornará uma base de Gröbner para um ideal I dado.

Teorema 1.2.9 (Algoritmo de Buchberger). *Dado um ideal $I = \langle g_1, \dots, g_t \rangle$ não nulo, o seguinte algoritmo produzirá uma base de Gröbner para I :*

Entrada: $\{g_1, \dots, g_t\}$
Saída : Uma base de Gröbner para I

Início

$G = \{g_1, \dots, g_t\};$
 $G' = \{\{g_i, g_j\} \mid g_i \neq g_j \text{ e } g_i, g_j \in G\};$
Enquanto $G' \neq \emptyset$ **faça**

Escolha $\{g_i, g_j\} \in G';$
 $G' = G' \setminus \{\{g_i, g_j\}\};$
 Dividir $S(g_i, g_j)$ por G obtendo resto r ;
Se $r \neq 0$ **então**

$G' = G' \cup \{\{g, r\} \mid g \in G\};$
 $G = G \cup \{r\};$

Fim

Fim

Fim

Demonstração. Primeiro, mostraremos que esse algoritmo terá um fim, em algum momento. Suponha o contrário, isto é, que ele nunca terá um fim. Então, assim que esse algoritmo é feito (e refeito), ele constrói um conjunto G_i estritamente maior que G_{i-1} , obtendo a seguinte sequência infinita estritamente crescente

$$G_1 \subset G_2 \subset G_3 \subset \dots$$

Cada G_i é obtido de G_{i-1} adicionando algum $r \in I$ a G_{i-1} , em que r é o resto não nulo da divisão de $S(f, g)$ por G_{i-1} , em que $f, g \in G_{i-1}$. Além disso, temos

$$\text{tl}(r) \notin \langle \text{tl}(g) \in \mathbb{K}[\mathbf{X}] \mid g \in G_{i-1} \rangle.$$

Logo, temos

$$\langle \text{tl}(g) \in \mathbb{K}[\mathbf{X}] \mid g \in G_1 \rangle \subset \langle \text{tl}(g) \in \mathbb{K}[\mathbf{X}] \mid g \in G_2 \rangle \subset \langle \text{tl}(g) \in \mathbb{K}[\mathbf{X}] \mid g \in G_3 \rangle \subset \dots$$

uma sequência estritamente crescente de ideais, o que contradiz o Teorema da Base de Hilbert.

Já sabemos, então, que o algoritmo para depois de um número finito de passos. Se chamarmos de $F = \{f_1, \dots, f_s\}$ o conjunto de polinômios que o algoritmo retornou, então temos $G \subset F \subset I$ e, portanto,

$$\begin{aligned} I &= \langle g_1, \dots, g_t \rangle \\ &\subset \langle f_1, \dots, f_s \rangle \\ &\subset I. \end{aligned}$$

Logo, F é um conjunto gerador para o ideal I . Além disso, se $f_i, f_j \in F$, então o resto da divisão de $S(f_i, f_j)$ por $\{f_1, \dots, f_s\}$ é zero, para todos os $i, j = 1, \dots, s$, com $i \neq j$. Segue do Teorema 1.2.8 que F é uma base de Gröbner para I . ■

Exemplo 1.2.10. Considere o Exemplo 1.2.2, isto é o ideal $I = \langle XY - 1, Y^2 - 1 \rangle$ e $\mathcal{M}$ munido com a ordem lexicográfica, com $Y \preceq X$. Então $\{XY - 1, Y^2 - 1, X - Y\}$ é uma base de Gröbner para I .

Já vimos que $\{XY - 1, Y^2 - 1\}$ não é uma base de Gröbner para I , então vamos aplicar o algoritmo de Buchberger. Chamando $g_1 = XY - 1$ e $g_2 = Y^2 - 1$, temos

$$\text{tl}(g_1) = XY \quad \text{e} \quad \text{tl}(g_2) = Y^2.$$

Logo,

$$\begin{aligned} S(g_1, g_2) &= Yg_1 - Xg_2 \\ &= X - Y. \end{aligned}$$

Como os termos em $X - Y$ não são múltiplos de $\text{ml}(g_1) = XY$ nem de $\text{ml}(g_2) = Y^2$, temos que $X - Y$ é o resto da divisão de $S(g_1, g_2)$ por $\{g_1, g_2\}$. Então, seja $g_3 = X - Y$ e consideremos agora o conjunto $\{g_1, g_2, g_3\}$. Verifiquemos:

- O resto da divisão de $S(g_1, g_2)$ por $\{g_1, g_2, g_3\}$ é zero, já que $S(g_1, g_2) = g_3$.
- O resto da divisão de $S(g_1, g_3)$ por $\{g_1, g_2, g_3\}$ também é zero. De fato, como

$$\text{tl}(g_1) = XY \quad \text{e} \quad \text{tl}(g_3) = X,$$

temos

$$\begin{aligned} S(g_1, g_3) &= g_1 - Yg_3 \\ &= Y^2 - 1. \end{aligned}$$

Como $S(g_1, g_3) = g_2$, o resto da divisão de $S(g_1, g_3)$ por $\{g_1, g_2, g_3\}$ é zero.

- Por fim, o resto da divisão de $S(g_2, g_3)$ por $\{g_1, g_2, g_3\}$ também é zero. Com efeito, como

$$\text{tl}(g_2) = Y^2 \quad \text{e} \quad \text{tl}(g_3) = X,$$

temos

$$\begin{aligned} S(g_1, g_3) &= Xg_2 - Y^2g_3 \\ &= Y^3 - X. \end{aligned}$$

Assim, efetuando o algoritmo da divisão:

$Y^3 - X$	$XY - 1$	$Y^2 - 1$	$Y - X$	Resto
$- \quad Y - X$	0	Y	1	0
$\hline Y^3 - Y$				
$- \quad Y^3 - Y$				
$\hline 0$				

Ou seja, o resto da divisão de $S(g_2, g_3)$ por $\{g_1, g_2, g_3\}$ é zero.

Portanto, $\{XY - 1, Y^2 - 1, X - Y\}$ é uma base de Gröbner para I .

1.3 Pegada de um ideal

Definição 1.3.1 (Pegada). *Seja $I \subset \mathbb{K}[\mathbf{X}]$ um ideal e considere $\mathcal{M}$ munido de uma ordem monomial. A pegada de I é o conjunto*

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

A pegada de um ideal I possui uma relação íntima com as bases de Gröbner desse mesmo ideal I . Ela é dada pelo seguinte resultado.

Proposição 1.3.2. *Sejam $I \subset \mathbb{K}[\mathbf{X}]$ um ideal e $\{g_1, \dots, g_t\}$ uma base de Gröbner para I . Então um monômio $M \in \Delta(I)$ se, e somente se, M não é múltiplo de $\text{ml}(g_i)$, para todo $i = 1, \dots, t$.*

Demonstração. Mostremos a necessidade. Seja $M \in \mathcal{M}$. Se $M \in \Delta(I)$, então, por definição, não existe $f \in I$ tal que $\text{ml}(f) = M$. Em particular, como $\{g_1, \dots, g_t\} \subset I$, temos que $Tg_i \in I$, em que $T \in \mathcal{M}$, e daí $\text{ml}(Tg_i) = T \cdot \text{ml}(g_i) \neq M$, para todo $T \in \mathcal{M}$ e todo $i = 1, \dots, t$. Em outras palavras, M não é múltiplo de $\text{ml}(g_i)$, para todo $i = 1, \dots, t$.

Agora, mostremos a suficiência. Pela definição de base de Gröbner, sabemos que se $M \in \mathcal{M}$ não é múltiplo de $\text{ml}(g_i)$, para todo $i = 1, \dots, t$, então M não é monômio líder de nenhum polinômio de I . ■

Exemplo 1.3.3. Seja $I = \langle X^3 - X, Y^3 - Y, X^2Y - Y \rangle \subset \mathbb{R}[X, Y]$ e considere $\mathcal{M}$ munido com a ordem lexicográfica, com $Y \preceq X$. Então,

$$\Delta(I) = \{1, X, X^2, Y, XY, Y^2, XY^2\}.$$

Primeiramente, note que $\{X^3 - X, Y^3 - Y, X^2Y - Y\}$ é uma base de Gröbner para I . De fato, chamando $g_1 = X^3 - X$, $g_2 = Y^3 - Y$ e $g_3 = X^2Y - Y$ temos que:

- A divisão de $S(g_1, g_2)$ por $\{g_1, g_2, g_3\}$ é zero. Com efeito, como

$$\text{tl}(g_1) = X^3 \quad \text{e} \quad \text{tl}(g_2) = Y^3,$$

temos

$$\begin{aligned} S(g_1, g_2) &= Y^3g_1 - X^3g_2 \\ &= X^3Y - XY^3. \end{aligned}$$

Assim, efetuando o algoritmo da divisão:

$X^3Y - XY^3$	$X^3 - X$	$Y^3 - Y$	$X^2Y - Y$	Resto
$- \frac{X^3Y - XY^3}{XY - XY^3}$	Y	$-X$	0	0
$- \frac{XY - XY^3}{XY - XY^3}$				
0				

Ou seja, o resto da divisão de $S(g_1, g_2)$ por $\{g_1, g_2, g_3\}$ é zero.

- A divisão de $S(g_1, g_3)$ por $\{g_1, g_2, g_3\}$ também é zero. De fato, como

$$\text{tl}(g_1) = X^3 \quad \text{e} \quad \text{tl}(g_3) = X^2Y,$$

temos

$$\begin{aligned} S(g_1, g_3) &= Yg_1 - Xg_3 \\ &= 0. \end{aligned}$$

Logo, o resto da divisão de $S(g_1, g_3)$ por $\{g_1, g_2, g_3\}$ é zero.

- Por fim, a divisão de $S(g_2, g_3)$ por $\{g_1, g_2, g_3\}$ também é zero. Como

$$\text{tl}(g_2) = Y^3 \quad \text{e} \quad \text{tl}(g_3) = X^2Y,$$

temos

$$\begin{aligned} S(g_2, g_3) &= X^2g_2 - Y^2g_3 \\ &= Y^3 - YX^2. \end{aligned}$$

Assim, efetuando o algoritmo da divisão:

$$\begin{array}{r|c|c|c|c}
 Y^3 - YX^2 & X^3 - X & Y^3 - Y & X^2Y - Y & \text{Resto} \\
 - \frac{Y - X^2Y}{Y^3 - Y} & 0 & 1 & -1 & 0 \\
 - \frac{Y^3 - Y}{0} & & & & \\
 \hline
 0 & & & &
 \end{array}$$

Ou seja, o resto da divisão de $S(g_2, g_3)$ por $\{g_1, g_2, g_3\}$ é zero.

Portanto, $\{X^3 - X, Y^3 - Y, X^2Y - Y\}$ é uma base de Gröbner para I .

Agora, pela Proposição 1.3.2, temos que os elementos de $\Delta(I)$ são os monômios que não são múltiplos de $\text{ml}(X^3 - X) = X^3$, $\text{ml}(Y^3 - Y) = Y^3$ ou $\text{ml}(X^2Y - Y) = X^2Y$. Podemos identificar $\mathcal{M}$ com $\{(\alpha, \beta) \in \mathbb{Z}^2 \mid \alpha \geq 0 \text{ e } \beta \geq 0\}$ associando o monômio $X^\alpha Y^\beta$ com o par ordenado (α, β) de inteiros não negativos. Assim, temos:

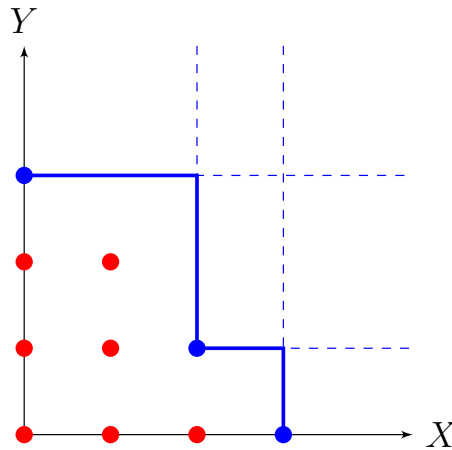


Figura 1 – Em azul, temos os monômios líderes da base de Gröbner de I e, em vermelho, temos os monômios que pertencem a pegada $\Delta(I)$.

Os pontos $(3, 0)$, $(0, 3)$ e $(2, 1)$ correspondem, respectivamente aos monômios líderes dos polinômios $X^3 - X$, $Y^3 - Y$ e $X^2Y - Y$, pertencentes à base de Gröbner de I . Desta forma, podemos determinar visualmente quais são os monômios que são múltiplos de pelo menos um desses monômios líderes e, conseqüentemente, determinar quais não são múltiplos de nenhum deles. Logo, concluímos que os monômios que não são múltiplos de $\text{ml}(X^3 - X) = X^3$, $\text{ml}(Y^3 - Y) = Y^3$ e $\text{ml}(X^2Y - Y) = X^2Y$ correspondem aos pontos $(0, 0)$, $(1, 0)$, $(2, 0)$, $(0, 1)$, $(1, 1)$, $(0, 2)$ e $(1, 2)$, ou seja,

$$\Delta(I) = \{1, X, X^2, Y, XY, Y^2, XY^2\}.$$

Teorema 1.3.4. *Seja $I \subset \mathbb{K}[\mathbf{X}]$ um ideal. Então,*

$$\mathcal{B} = \{M + I \in \mathbb{K}[\mathbf{X}]/I \mid M \in \Delta(I)\}$$

é uma base para $\mathbb{K}[\mathbf{X}]/I$ como um espaço vetorial sobre $\mathbb{K}$.

Demonstração. Sejam G uma base de Gröbner para I , com respeito à mesma ordem monomial utilizada para determinar $\Delta(I)$, e $f \in \mathbb{K}[\mathbf{X}]$. Dividindo f por G , temos que o resto é da forma

$$r = \sum_{i=1}^t a_i M_i,$$

em que $a_i \in \mathbb{K}$ e $M_i \in \Delta(I)$, para todo $i = 1, \dots, t$. Como $f + I = r + I$, segue que $\mathcal{B}$ gera $\mathbb{K}[\mathbf{X}]/I$.

Agora, assumamos que

$$\sum_{i=1}^s b_i (M_i + I) = 0 + I,$$

em que $b_i \in \mathbb{K}$ e $M_i \in \Delta(I)$, para todo $i = 1, \dots, s$. Então, $\sum_{i=1}^s b_i M_i \in I$ implica que $b_i = 0$, para todo $i = 1, \dots, s$, pois caso contrário teríamos que $\sum_{i=1}^s b_i M_i$ seria um elemento não nulo de I , no qual o monômio líder não é o monômio líder de algum polinômio de I . Isso mostra que $\mathcal{B}$ é linearmente independente.

Como $\mathcal{B}$ gera $\mathbb{K}[\mathbf{X}]/I$ e é linearmente independente, segue que ele é uma base para $\mathbb{K}[\mathbf{X}]/I$. ■

Exemplo 1.3.5. Considere o Exemplo 1.3.3, isto é o ideal $I = \langle X^3 - X, Y^3 - Y, X^2Y - Y \rangle$ e $\mathcal{M}$ munido com a ordem lexicográfica, com $Y \preceq X$. Então uma base para $\mathbb{R}[X, Y]/I$ é

$$\{1 + I, X + I, X^2 + I, Y + I, XY + I, Y^2 + I, XY^2 + I\}.$$

De fato, já vimos que $\{X^3 - X, Y^3 - Y, X^2Y - Y\}$ forma uma base de Gröbner para I , e que

$$\Delta(I) = \{1, X, X^2, Y, XY, Y^2, XY^2\}.$$

Logo, pelo Teorema 1.3.4,

$$\{1 + I, X + I, X^2 + I, Y + I, XY + I, Y^2 + I, XY^2 + I\}$$

é uma base para $\mathbb{R}[X, Y]/I$ como um espaço vetorial sobre $\mathbb{R}$. Consequentemente $\mathbb{R}[X, Y]/I$ é um espaço vetorial sobre $\mathbb{R}$ com dimensão 7.

Agora, sejam $I \subset \mathbb{K}[\mathbf{X}]$ um ideal e $\{g_1, \dots, g_t\}$ uma base para I . Defina o conjunto

$$\begin{aligned} \Delta(\text{ml}(g_1), \dots, \text{ml}(g_t)) = \{M \in \mathcal{M} \mid M \text{ não é múltiplo} \\ \text{de } \text{ml}(g_i), \text{ para todo } i = 1, \dots, t\}. \end{aligned}$$

Note que sempre é verdade que

$$\Delta(I) \subset \Delta(\text{ml}(g_1), \dots, \text{ml}(g_t))$$

pois se $M \in \Delta(I)$ então M não é monômio líder de nenhum polinômio em I e, em particular, não é múltiplo de nenhum $\text{ml}(g_i)$, com $i = 1, \dots, t$.

Observe que, pela Proposição 1.3.2, temos que

$$\Delta(I) = \Delta(\text{ml}(g_1), \dots, \text{ml}(g_t))$$

se, e somente se, $\{g_1, \dots, g_t\}$ é uma base de Gröbner para I .

1.4 Variedades afins

Um dos conceitos mais importantes da geometria algébrica é o de variedade. Esse conceito conecta as áreas de álgebra e de geometria. Além disso, será fundamental no trabalho que se apresenta.

Definição 1.4.1 (Variedade afim). *Seja $I \subseteq \mathbb{K}[\mathbf{X}]$ um ideal. Uma variedade afim associada a I é o conjunto*

$$V(I) = \{(a_1, \dots, a_n) \in \mathbb{K}^n \mid f(a_1, \dots, a_n) = 0, \text{ para todo } f \in I\}.$$

Note que se $I = \langle g_1, \dots, g_t \rangle$, com $g_1, \dots, g_t \in \mathbb{K}[\mathbf{X}]$, então $(a_1, \dots, a_n) \in V(I)$ se, e somente se, $g_i(a_1, \dots, a_n) = 0$, para todo $i = 1, \dots, t$. De fato, temos que

$$\begin{aligned} (a_1, \dots, a_n) \in V(I) &\iff f(a_1, \dots, a_n) = 0, \text{ para todo } f \in I, \\ &\iff \left(\sum_{i=1}^t h_i g_i \right) (a_1, \dots, a_n) = 0, \text{ para todo } h_i \in \mathbb{K}[\mathbf{X}], \\ &\iff g_i(a_1, \dots, a_n) = 0, \text{ para todo } i = 1, \dots, t. \end{aligned}$$

Dado uma variedade afim de um ideal I , a saber, $V(I)$ podemos nos perguntar sobre o conjunto de polinômios que se anulam nos pontos de $V(I)$. Esse conjunto é denotado por $\mathcal{I}(V(I))$ e é um ideal.

Definição 1.4.2 (O ideal de uma variedade afim). *Sejam $I \subseteq \mathbb{K}[\mathbf{X}]$ um ideal e $V(I)$ a variedade afim associada a esse ideal. O conjunto de polinômios que se anulam nos pontos de $V(I)$ é chamado de ideal da variedade $V(I)$.*

Por vezes, denotaremos $\mathcal{I}(V(I))$ simplesmente por $\mathcal{I}(V)$. Verifiquemos que esse conjunto é de fato um ideal. Com efeito, dados $f, g \in \mathcal{I}(V(I))$ temos

$$\begin{aligned} (f + g)(a_1, \dots, a_n) &= f(a_1, \dots, a_n) + g(a_1, \dots, a_n) \\ &= 0, \end{aligned}$$

para todo $(a_1, \dots, a_n) \in V(I)$. E ainda, dado $h \in \mathbb{K}[X]$, temos que

$$\begin{aligned} (hf)(a_1, \dots, a_n) &= h(a_1, \dots, a_n) \cdot f(a_1, \dots, a_n) \\ &= 0, \end{aligned}$$

para todo $(a_1, \dots, a_n) \in V(I)$. Portanto, $\mathcal{I}(V(I))$ é um ideal. E, além disso, é fácil verificar que $I \subseteq \mathcal{I}(V(I))$.

Uma variedade afim pode ter uma quantidade infinita ou finita de pontos. Isso depende, inicialmente, do corpo no qual estamos trabalhando e de quantos polinômios formam a base do ideal. Por exemplo, se considerarmos:

- $I = \langle Y - X^2 \rangle \subseteq \mathbb{R}[X, Y]$, $V(I)$ tem uma quantidade infinita de pontos;

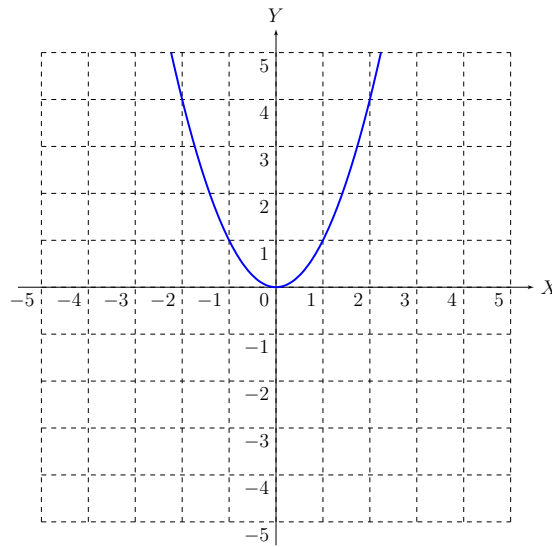


Figura 2 – Em azul a variedade afim de $I = \langle Y - X^2 \rangle \subseteq \mathbb{R}[X, Y]$.

- $I = \langle X^2 + Y^2 - 9, Y^2 - X \rangle \subseteq \mathbb{R}[X, Y]$, $V(I)$ tem uma quantidade finita de pontos.

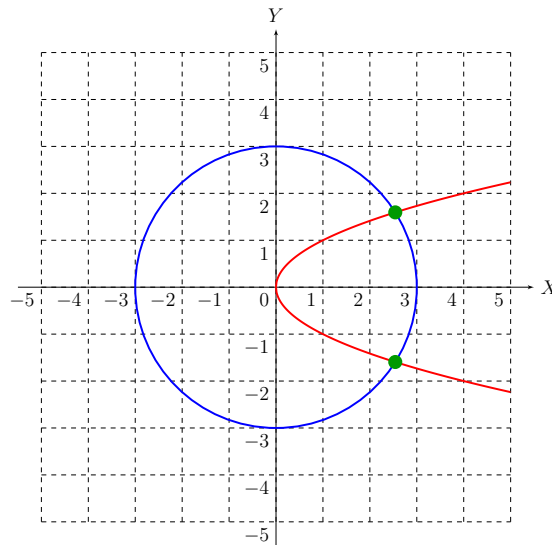


Figura 3 – Em azul a variedade afim de $J = \langle X^2 + Y^2 - 9 \rangle$. Em vermelho a variedade afim de $K = \langle Y^2 - X \rangle$. Em verde a variedade afim de $I = \langle X^2 + Y^2 - 9, Y^2 - X \rangle$.

Mostraremos agora uma importante relação entre a variedade de um ideal I e a pegada desse ideal, quando $\Delta(I)$ é um conjunto finito. Antes disso, temos o seguinte resultado auxiliar:

Lema 1.4.3. *Sejam $I \subseteq \mathbb{K}[\mathbf{X}]$ um ideal e $\mathbf{P}_1, \dots, \mathbf{P}_r \in V(I)$ pontos distintos. Então, existem polinômios $f_1, \dots, f_r \in \mathbb{K}[\mathbf{X}]$ tais que $f_i(\mathbf{P}_j) = \delta_{ij}$, para todos $i, j = 1, \dots, r$.*

Demonstração. Tome $i \in \{1, \dots, r\}$ e considere $\mathbf{P}_i = (a_{i1}, \dots, a_{in}) \in \mathbb{K}^n$ um ponto fixado. Como todos os pontos tomados são distintos, para todo $j \in \{1, \dots, r\} \setminus \{i\}$, existe $k_j \in \{1, \dots, n\}$ tal que

$$a_{ik_j} \neq a_{jk_j}.$$

Seja

$$h_j = \frac{X_{k_j} - a_{jk_j}}{a_{ik_j} - a_{jk_j}}.$$

Então,

$$h_j(\mathbf{P}_i) = 1 \quad \text{e} \quad h_j(\mathbf{P}_j) = 0,$$

para todo $j \in \{1, \dots, r\} \setminus \{i\}$. Logo, tomando

$$f_i = \prod_{\substack{j \in \{1, \dots, r\} \\ j \neq i}} h_j,$$

temos

$$f_i(\mathbf{P}_i) = 1 \quad \text{e} \quad f_i(\mathbf{P}_j) = 0,$$

para todo $j \in \{1, \dots, r\} \setminus \{i\}$. Como $i = 1, \dots, r$ foi tomado de forma arbitrária, segue que todos os polinômios $f_1, \dots, f_r$ são construídos da mesma forma. ■

Proposição 1.4.4. *Seja $I \subseteq \mathbb{K}[X]$ um ideal tal que $\Delta(I)$ é um conjunto finito. Então $V(I)$ também é um conjunto finito e $|V(I)| \leq |\Delta(I)|$.*

Demonstração. Sejam $\mathbf{P}_1, \dots, \mathbf{P}_r \in V(I)$ pontos distintos. Vamos determinar um conjunto em $\mathbb{K}[\mathbf{X}]/I$ que é linearmente independente e possui r elementos.

Pelo Lema 1.4.3, existem polinômios $f_1, \dots, f_r \in \mathbb{K}[\mathbf{X}]$ tais que $f_i(\mathbf{P}_j) = \delta_{ij}$, para todos $i, j = 1, \dots, r$. Assuma que

$$\sum_{i=1}^r a_i(f_i + I) = 0 + I,$$

em que $a_i \in \mathbb{K}$, para todo $i = 1, \dots, r$. Então,

$$\begin{aligned} a_j &= \sum_{i=1}^r a_i f_i(\mathbf{P}_j) \\ &= 0, \end{aligned}$$

para todo $j \in 1, \dots, r$. Assim, $\{f_1 + I, \dots, f_r + I\}$ é um conjunto linearmente independente de $\mathbb{K}[\mathbf{X}]/I$.

Pelo Teorema 1.3.4, sabemos que $|\Delta(I)|$ é a dimensão de $\mathbb{K}[\mathbf{X}]/I$ como um $\mathbb{K}$ -espaço vetorial. Portanto, sendo $\Delta(I)$ um conjunto finito, temos que $V(I)$ também é um conjunto finito e $|V(I)| \leq |\Delta(I)|$. ■

Na verdade, existe um resultado mais refinado. Para isso, precisamos da definição de radical de um ideal, que é um conceito mais amplo do que utilizado no escopo desta dissertação.

Definição 1.4.5 (Radical de um ideal). *Seja I um ideal de um anel R . O radical do ideal é o conjunto*

$$\{a \in R \mid a^n \in I, \text{ para algum } n \in \mathbb{Z}_+\}.$$

O radical de um ideal será denotado por $\sqrt{I}$.

Definição 1.4.6 (Ideal radical). *Seja I um ideal de um anel R . Um ideal é dito radical se $I = \sqrt{I}$.*

Naturalmente, temos $I \subseteq \sqrt{I}$. Mas o contrário nem sempre é verdade. Além disso, estamos interessados quando $I \subseteq \mathbb{K}[\mathbf{X}]$.

Teorema 1.4.7 (Theorem 8.32 (BECKER; WEISPFENNING, 1993)). *Sejam $I \subseteq \mathbb{K}[\mathbf{X}]$ um ideal tal que $\Delta(I)$ é um conjunto finito e $\mathbb{L}$ uma extensão algebricamente fechada de $\mathbb{K}$. Então*

$$V_{\mathbb{L}}(I) = \{(a_1, \dots, a_n) \in \mathbb{L}^n \mid f(a_1, \dots, a_n) = 0, \text{ para todo } f \in I\}$$

é um conjunto finito e $|V_{\mathbb{L}}(I)| \leq |\Delta(I)|$. Além disso, se $\mathbb{K}$ é um corpo perfeito (isto é, um corpo finito ou de característica zero) e I um ideal radical, então $|V_{\mathbb{L}}(I)| = |\Delta(I)|$.

2 Corpos finitos

Neste capítulo trazemos alguns conceitos triviais, porém fundamentais, sobre corpos finitos. Nosso objetivo aqui é apresentar os corpos onde os Códigos afins estarão definidos. Para tanto, fazemos uso principalmente da referência (HEFEZ; VILLELA, 2017).

2.1 Característica de um corpo

Definição 2.1.1 (Homomorfismos entre corpos). *Sejam $\mathbb{K}_1$ e $\mathbb{K}_2$ corpos. Diremos que uma função $f: \mathbb{K}_1 \rightarrow \mathbb{K}_2$ é um homomorfismo se ela satisfaz:*

- i. $f(x + y) = f(x) + f(y)$;
- ii. $f(x \cdot y) = f(x) \cdot f(y)$;
- iii. $f(1) = 1$;

para todos $x, y \in \mathbb{K}_1$.

Caso esse homomorfismo f seja injetor, diremos que ele é um monomorfismo. Caso ele seja sobrejetor, diremos que ele é um epimorfismo. E, caso ele seja bijetor, diremos que ele é um isomorfismo. Além disso, dados dois corpos, $\mathbb{K}_1$ e $\mathbb{K}_2$, diremos que $\mathbb{K}_1$ é isomorfo a $\mathbb{K}_2$ (ou vice-versa) caso exista um isomorfismo entre eles.

Proposição 2.1.2. *Sejam $\mathbb{K}_1$ e $\mathbb{K}_2$ corpos, $f: \mathbb{K}_1 \rightarrow \mathbb{K}_2$ um homomorfismo e $x, y \in \mathbb{K}_1$. Então:*

1. $f(0) = 0$;
2. $f(-x) = -f(x)$;
3. $f(x - y) = f(x) - f(y)$;
4. $f(x^{-1}) = f(x)^{-1}$, com $x \in \mathbb{K}_1$ invertível;
5. Se f é um isomorfismo, então f^{-1} é um homomorfismo;
6. f é um monomorfismo e $f(\mathbb{K}_1)$ é um subcorpo de $\mathbb{K}_2$.

Demonstração. Mostremos cada item da proposição.

1. Temos que

$$\begin{aligned} f(0) &= f(0 + 0) \\ &= f(0) + f(0). \end{aligned}$$

Daí,

$$\begin{aligned} f(0) &= f(0) + f(0) \iff 0 = f(0) + f(0) - f(0) \\ &\iff 0 = f(0). \end{aligned}$$

Portanto, $f(0) = 0$.

2. Note que

$$\begin{aligned} f(0) &= f(x - x) \\ &= f(x) + f(-x). \end{aligned}$$

Como $f(0) = 0$ pelo item 1, segue que

$$0 = f(x) + f(-x) \iff -f(x) = f(-x).$$

Portanto, $f(-x) = -f(x)$.

3. Pelo item 2, segue que

$$\begin{aligned} f(x - y) &= f(x + (-y)) \\ &= f(x) + f(-y) \\ &= f(x) - f(y). \end{aligned}$$

Portanto, $f(x - y) = f(x) - f(y)$.

4. Como $x \in \mathbb{K}_1$ é invertível, temos

$$\begin{aligned} f(1) &= f(x \cdot x^{-1}) \\ &= f(x) \cdot f(x^{-1}). \end{aligned}$$

Como $f(1) = 1$, segue que

$$1 = f(x) \cdot f(x^{-1}) \iff f(x)^{-1} = f(x^{-1}).$$

Portanto, $f(x^{-1}) = f(x)^{-1}$, com $x \in \mathbb{K}_1$ invertível.

5. Pela teoria de funções, como f é bijetora, faz sentido falarmos em f^{-1} e $f^{-1}(f(t)) = t$, para todo $t \in \mathbb{K}_1$.

Sejam $u, v \in \mathbb{K}_2$. Pela bijeção de f , existem $x, y \in \mathbb{K}_1$ tais que

$$x = f^{-1}(u) \quad \text{e} \quad y = f^{-1}(v).$$

Daí:

i. Segue que

$$\begin{aligned} f^{-1}(u + v) &= f^{-1}(f(x) + f(y)) \\ &= f^{-1}(f(x + y)) \\ &= x + y \\ &= f^{-1}(u) + f^{-1}(v). \end{aligned}$$

Portanto, $f^{-1}(u + v) = f^{-1}(u) + f^{-1}(v)$.

ii. Note que

$$\begin{aligned} f^{-1}(u \cdot v) &= f^{-1}(f(x) \cdot f(y)) \\ &= f^{-1}(f(x \cdot y)) \\ &= x \cdot y \\ &= f^{-1}(u) \cdot f^{-1}(v). \end{aligned}$$

Portanto, $f^{-1}(u \cdot v) = f^{-1}(u) \cdot f^{-1}(v)$.

iii. Como $f(1) = 1$, temos

$$\begin{aligned} f(1) = 1 &\iff f^{-1}(f(1)) = f^{-1}(1) \\ &\iff 1 = f^{-1}(1). \end{aligned}$$

Portanto, $f^{-1}(1) = 1$.

Como $u, v \in \mathbb{K}_2$ foram tomados arbitrariamente, segue que f^{-1} é um homomorfismo.

6. Sejam $x, y \in \mathbb{K}_1$ e suponha que $f(x) = f(y)$. Então, pelo item 3,

$$\begin{aligned} f(x) = f(y) &\iff f(x) - f(y) = 0 \\ &\iff f(x - y) = 0. \end{aligned}$$

Se $x \neq y$, então $x - y \neq 0$ e, portanto, é invertível. Então, pelo item 4, $f(x - y)$ é invertível e não poderia ser nulo. Portanto, a única possibilidade é $x = y$, ou seja, f é um homomorfismo injetor, ou ainda, um monomorfismo.

Para mostrar que $f(\mathbb{K}_1)$ é um corpo, basta verificarmos que se $u, v \in f(\mathbb{K}_1)$, com $v \neq 0$, então $u - v \in f(\mathbb{K}_1)$ e $u \cdot v^{-1} \in f(\mathbb{K}_1)$. Como $u, v \in f(\mathbb{K}_1)$, sejam $x, y \in \mathbb{K}_1$ tais que

$$u = f(x) \quad \text{e} \quad v = f(y).$$

Então,

$$\begin{aligned} u - v &= f(x) - f(y) \\ &= f(x - y) \in f(\mathbb{K}_1), \end{aligned}$$

e

$$\begin{aligned} u \cdot v^{-1} &= f(x) \cdot f(y)^{-1} \\ &= f(x) \cdot f(y^{-1}) \\ &= f(x \cdot y^{-1}) \in f(\mathbb{K}_1). \end{aligned}$$

Portanto, $f(\mathbb{K}_1)$ é um subcorpo de $\mathbb{K}_2$.

Sendo todos os itens verdadeiros, segue a proposição. ■

Para simplificar a notação, o produto $x \cdot y$ será simplesmente denotado por xy . Desta forma, por exemplo, o produto $x \cdot y^{-1}$ será denotado por xy^{-1} .

Agora, seja $\mathbb{K}$ um corpo finito (um corpo com uma quantidade finita de elementos) com unidade 1. Considere o conjunto

$$\Lambda_{\mathbb{K}} = \{n \in \mathbb{Z}_+ \mid n1 = 0\},$$

onde $\mathbb{Z}_+$ denota o conjunto dos inteiros positivos. Pelo fato de $\mathbb{K}$ ser finito, existem dois inteiros n_1 e n_2 , com $n_1 < n_2$, tais que

$$n_1 1 = 0 \quad \text{e} \quad n_2 1 = 0.$$

Segue então que $(n_2 - n_1)1 = 0$, com $n_2 - n_1 > 0$ e, portanto, $\Lambda_{\mathbb{K}} \neq \emptyset$.

Definição 2.1.3 (Característica de um corpo). *Seja $\mathbb{K}$ um corpo finito. A característica de $\mathbb{K}$ será o inteiro não negativo $\text{car}(\mathbb{K})$ definido como*

$$\text{car}(\mathbb{K}) = \min(\Lambda_{\mathbb{K}}).$$

Note que se $\mathbb{F}$ é um subcorpo de $\mathbb{K}$ então $\text{car}(\mathbb{F}) = \text{car}(\mathbb{K})$, pois $\Lambda_{\mathbb{K}} = \Lambda_{\mathbb{F}}$.

Proposição 2.1.4. *Seja $\mathbb{K}$ um corpo finito, então $\text{car}(\mathbb{K})$ é um número primo.*

Demonstração. Seja $p = \text{car}(\mathbb{K})$ e suponhamos que p não seja primo. Logo, $p = p_1 p_2$, com $p_1, p_2 \in \mathbb{Z}_+$ e $1 < p_1, p_2 < p$. Então,

$$\begin{aligned} 0 &= p1 \\ &= (p_1 p_2)1 \\ &= p_1(p_2 1) \\ &= (p_1 1)(p_2 1). \end{aligned}$$

Como $\mathbb{K}$ é um corpo (e, em particular, um domínio de integridade), temos que $p_1 1 = 0$ ou $p_2 1 = 0$. Isso contradiz a minimalidade de p . Portanto, p é primo. ■

Proposição 2.1.5. *Seja $\mathbb{K}$ um corpo finito com $\text{car}(\mathbb{K}) = p$. Se para $m \in \mathbb{Z}$ e $a \in \mathbb{K}$ tem-se $ma = 0$, então m é múltiplo de p ou $a = 0$.*

Demonstração. Suponhamos que $ma = 0$. Então, $(m1)a = 0$. Como $\mathbb{K}$ é um corpo (e, em particular, um domínio de integridade), temos

$$m1 = 0 \quad \text{ou} \quad a = 0.$$

Se $a = 0$, o resultado segue. Então, suponhamos que $m1 = 0$ e mostremos que m é múltiplo de p . Pelo algoritmo da divisão euclidiana, existem únicos $q, r \in \mathbb{Z}_+$ tais que $m = qp + r$, com $r < p$. Logo,

$$\begin{aligned} 0 &= p1 \\ &= (qp + r)1 \\ &= q(p1) + r1 \\ &= q0 + r1 \\ &= r1, \end{aligned}$$

e, pela minimalidade de p , segue que $r = 0$. Portanto, m é múltiplo de p . ■

Teorema 2.1.6. *Seja $\mathbb{K}$ um corpo finito com $\text{car}(\mathbb{K}) = p$. Então, $\mathbb{K}$ contém um subcorpo isomorfo a $\mathbb{Z}_p$.*

Demonstração. Considere a função $\phi: \mathbb{Z}_p \rightarrow \mathbb{K}$ dada por

$$\phi([n]) = n1.$$

Primeiramente, mostremos que essa função está bem definida. Com efeito, se $[m] = [n]$, com $m, n \in \mathbb{Z}$, então existe $\lambda \in \mathbb{Z}$ tal que

$$n = m + \lambda p.$$

Logo,

$$\begin{aligned} n1 &= (m + \lambda p)1 \\ &= m1 + \lambda(p1) \\ &= m1 + \lambda 0 \\ &= m1. \end{aligned}$$

Agora, vejamos que ϕ é um monomorfismo. Note que

$$\begin{aligned} \phi([n] + [m]) &= \phi([n + m]) \\ &= (n + m)1 \\ &= n1 + m1 \\ &= \phi([n]) + \phi([m]), \end{aligned}$$

e

$$\begin{aligned}
 \phi([n] \cdot [m]) &= \phi([nm]) \\
 &= nm1 \\
 &= n(m1) \\
 &= (n1)(m1) \\
 &= \phi([n])\phi([m]),
 \end{aligned}$$

e

$$\phi([1]) = 1.$$

Assim, ϕ é um homomorfismo entre $\mathbb{Z}_p$ e $\mathbb{K}$. Pela Proposição 2.1.2, ϕ é um monomorfismo e $\phi(\mathbb{Z}_p)$ é um subcorpo de $\mathbb{K}$. Portanto,

$$\phi: \mathbb{Z}_p \longrightarrow \phi(\mathbb{Z}_p) \subseteq \mathbb{K}$$

é um isomorfismo e, conseqüentemente, $\mathbb{K}$ contém um subcorpo isomorfo a $\mathbb{Z}_p$. ■

Como $\mathbb{K}$ contém um subcorpo isomorfo a $\mathbb{Z}_p$ pela função ϕ definida no Teorema 2.1.6, identificaremos $\phi(\mathbb{Z}_p)$ com $\mathbb{Z}_p$ e, simplificando a notação, consideraremos $\mathbb{Z}_p \subseteq \mathbb{K}$.

Corolário 2.1.7. *Seja $\mathbb{K}$ um corpo finito com $\text{car}(\mathbb{K}) = p$. Então $\mathbb{K}$ tem p^n elementos para algum número inteiro positivo n .*

Demonstração. Note que $\mathbb{K}$ é um espaço vetorial sobre $\mathbb{Z}_p$. Além disso, como $\mathbb{K}$ é finito, segue que $\mathbb{K}$ tem dimensão finita sobre $\mathbb{Z}_p$.

Sejam $x_1, \dots, x_n \in \mathbb{K}$ os elementos de uma base de $\mathbb{K}$ sobre $\mathbb{Z}_p$. Então, todo elemento $x \in \mathbb{K}$ pode ser escrito de maneira única como

$$x = \lambda_1 x_1 + \dots + \lambda_n x_n$$

com $\lambda_i \in \mathbb{Z}_p$, para todo $i = 1, \dots, n$. Contando as possibilidades para os λ 's, obtemos $|\mathbb{K}| = p^n$. Portanto, $\mathbb{K}$ tem p^n elementos para algum número inteiro positivo n . ■

Proposição 2.1.8. *Sejam $\mathbb{K}$ um corpo finito com $\text{car}(\mathbb{K}) = p$, então*

$$(x_1 + \dots + x_n)^p = x_1^p + \dots + x_n^p.$$

Demonstração. Mostremos esse resultado por indução sobre n .

Primeiramente, note que para $n = 1$ temos

$$(x_1)^p = x_1^p.$$

Suponha agora que $n \geq 2$. Utilizando a expansão do Binômio de Newton, temos

$$((x_1 + \dots + x_{n-1}) + x_n)^p = \sum_{i=0}^p \binom{p}{i} (x_1 + \dots + x_{n-1})^i x_n^{p-i}.$$

Por definição, os coeficientes binomiais são da forma

$$\binom{p}{i} = \frac{p!}{(p-i)!i!}.$$

Logo, $\binom{p}{0} = 1$, $\binom{p}{p} = 1$ e $p \mid \binom{p}{i}$, para todo $i = 1, \dots, p-1$. Assim,

$$\begin{aligned} (x_1 + \dots + x_n)^p &= ((x_1 + \dots + x_{n-1}) + x_n)^p \\ &= \sum_{i=0}^p \binom{p}{i} (x_1 + \dots + x_{n-1})^i x_n^{p-i} \\ &= (x_1 + \dots + x_{n-1})^p + x_n^p. \end{aligned}$$

Utilizando a hipótese de indução,

$$(x_1 + \dots + x_{n-1})^p = x_1^p + \dots + x_{n-1}^p.$$

Daí,

$$\begin{aligned} (x_1 + \dots + x_n)^p &= (x_1 + \dots + x_{n-1})^p + x_n^p \\ &= x_1^p + \dots + x_{n-1}^p + x_n^p \\ &= x_1^p + \dots + x_n^p. \end{aligned}$$

■

Corolário 2.1.9. *Sejam $\mathbb{K}$ um corpo finito com $\text{car}(\mathbb{K}) = p$, e seja $q = p^r$, com $r \in \mathbb{Z}_+^*$. Então*

$$(x_1 + \dots + x_n)^q = x_1^q + \dots + x_n^q.$$

Demonstração. Faremos uma indução sobre r . Para $r = 1$, o resultado é a Proposição 2.1.8.

Agora, supondo que o resultado vale para $r-1$, mostremos que vale para r . Sabemos que $p^r = p^{r-1}p$, daí,

$$\begin{aligned} (x_1 + \dots + x_n)^q &= (x_1 + \dots + x_n)^{p^r} \\ &= \left((x_1 + \dots + x_n)^{p^{r-1}} \right)^p \\ &= \left(x_1^{p^{r-1}} + \dots + x_n^{p^{r-1}} \right)^p \\ &= \left(x_1^{p^{r-1}} \right)^p + \dots + \left(x_n^{p^{r-1}} \right)^p \\ &= x_1^{p^r} + \dots + x_n^{p^r} \\ &= x_1^q + \dots + x_n^q. \end{aligned}$$

Portanto, o resultado segue. ■

Note que se $\mathbb{K}$ é um corpo finito de característica p e q é uma potência de p , então se

$$P(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{K}[X],$$

então

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

Corolário 2.1.10. *Seja $\mathbb{K}$ um corpo finito de característica p . Se $q = p^r$, com $r \in \mathbb{Z}_+^*$, então a função $f_q: \mathbb{K} \rightarrow \mathbb{K}$ dada por*

$$f_q(x) = x^q$$

é um isomorfismo de corpos.

Demonstração. De fato, note que, pela Proposição 2.1.8,

$$\begin{aligned} f_q(x+y) &= (x+y)^q \\ &= x^q + y^q \\ &= f_q(x) + f_q(y), \end{aligned}$$

para todos $x, y \in \mathbb{K}$. Além disso,

$$\begin{aligned} f_q(xy) &= (xy)^q \\ &= x^q y^q \\ &= f_q(x) f_q(y), \end{aligned}$$

para todos $x, y \in \mathbb{K}$. E,

$$\begin{aligned} f_q(1) &= 1^q \\ &= 1. \end{aligned}$$

Logo, f_q é um homomorfismo entre corpos. Observe que f_q é claramente homomorfismo injetor, e como o domínio e o contradomínio têm a mesma cardinalidade, temos que f_q é uma bijeção. Portanto, f_q é um isomorfismo de corpos. ■

Corolário 2.1.11. *Sejam $\mathbb{F}$ um corpo de característica $p > 0$ e q uma potência inteira de p . Então o conjunto $\mathbb{K} = \{\alpha \in \mathbb{F} \mid \alpha^q - \alpha = 0\}$ é um subcorpo de $\mathbb{F}$.*

Demonstração. Basta mostrarmos que se $\alpha, \beta \in \mathbb{K}$, com $\beta \neq 0$, então $\alpha - \beta \in \mathbb{K}$, $\alpha\beta^{-1} \in \mathbb{K}$ e $\beta^{-1} \in \mathbb{K}$.

Sejam $\alpha, \beta \in \mathbb{K}$. Como $\alpha^q - \alpha = 0$ e $\beta^q - \beta = 0$, segue que, pela Proposição 2.1.8,

$$\begin{aligned} (\alpha - \beta)^q - (\alpha - \beta) &= (\alpha^q - \beta^q) - (\alpha - \beta) \\ &= (\alpha^q - \alpha) - (\beta^q - \beta) \\ &= 0. \end{aligned}$$

Logo, $\alpha - \beta \in \mathbb{K}$.

Observe que

$$\begin{aligned} 1 &= 1^q \\ &= (\beta\beta^{-1})^q \\ &= \beta^q(\beta^{-1})^q \\ &= \beta(\beta^{-1})^q, \end{aligned}$$

logo $(\beta^{-1})^q = \beta^{-1}$. Assim,

$$\begin{aligned} (\alpha\beta^{-1})^q - \alpha\beta^{-1} &= \alpha^q(\beta^{-1})^q - \alpha\beta^{-1} \\ &= \alpha\beta^{-1} - \alpha\beta^{-1} \\ &= 0. \end{aligned}$$

Portanto, $\mathbb{K}$ é um subcorpo de $\mathbb{F}$. ■

É possível mostrar os seguintes resultados importantes.

Teorema 2.1.12 (Existência de corpos finitos). *Para todos os inteiros positivos p e n , com p primo, existe um corpo com p^n elementos.*

Demonstração. Veja (HEFEZ; VILLELA, 2017), página 75. ■

Teorema 2.1.13 (Unicidade dos corpos finitos). *Dois corpos finitos com o mesmo número de elementos são isomorfos.*

Demonstração. Veja (HEFEZ; VILLELA, 2017), página 76. ■

Parte II

Códigos Corretores de Erro Afins

3 Códigos corretores de erro

Neste capítulo trazemos os principais resultados dessa dissertação. Aqui nosso foco é construir e explorar ferramentas sobre os Códigos Afins e seus duais. Para isso fazemos uso das referências (CARVALHO, 2017), (LOPEZ; MANGANIELLO; MATTHEWS, 2019) e (LOPEZ; MATTHEWS; SOPRUNOV, 2020).

3.1 Conceitos básicos

O corpo sobre o qual estarão definidos nossos objetos agora será sempre finito, isto é, consideremos $\mathbb{F}_q$ um corpo finito com q elementos.

Definição 3.1.1 (Código linear). *Um código linear $\mathcal{C}$ definido sobre um alfabeto $\mathbb{F}_q$ de tamanho n é um $\mathbb{F}_q$ -espaço vetorial de $\mathbb{F}_q^n$.*

Os elementos desse código $\mathcal{C}$ são chamados de palavras.

Sejam $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$, em que $\mathbf{a} = (a_1, \dots, a_n)$ e $\mathbf{b} = (b_1, \dots, b_n)$. A distância de Hamming entre $\mathbf{a}$ e $\mathbf{b}$ é definida como

$$d(\mathbf{a}, \mathbf{b}) = |\{i \mid a_i \neq b_i, \text{ com } i = 1, \dots, n\}|.$$

De fato, a palavra distância está bem empregada pois a função $d: \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{R}$ define uma métrica em $\mathbb{F}_q^n$. Com efeito, dados $\mathbf{a} = (a_1, \dots, a_n), \mathbf{b} = (b_1, \dots, b_n), \mathbf{c} = (c_1, \dots, c_n) \in \mathbb{F}_q^n$:

- Não negatividade: Temos que

$$\begin{aligned} d(\mathbf{a}, \mathbf{b}) &= |\{i \mid a_i \neq b_i, \text{ com } i = 1, \dots, n\}| \\ &\geq 0, \end{aligned}$$

valendo a igualdade se, e somente se, $a_i = b_i$, para todo $i = 1, \dots, n$, ou seja, se, e somente se, $\mathbf{a} = \mathbf{b}$.

- Simetria: Temos que

$$\begin{aligned} d(\mathbf{a}, \mathbf{b}) &= |\{i \mid a_i \neq b_i, \text{ com } i = 1, \dots, n\}| \\ &= |\{i \mid b_i \neq a_i, \text{ com } i = 1, \dots, n\}| \\ &= d(\mathbf{b}, \mathbf{a}). \end{aligned}$$

- Desigualdade triangular: Temos que

$$\begin{aligned}
d(\mathbf{a}, \mathbf{c}) + d(\mathbf{c}, \mathbf{b}) &= |\{i \mid a_i \neq c_i, \text{ com } i = 1, \dots, n\}| \\
&\quad + |\{i \mid c_i \neq b_i, \text{ com } i = 1, \dots, n\}| \\
&= |\{i \mid a_i \neq c_i \text{ ou } c_i \neq b_i, \text{ com } i = 1, \dots, n\}| \\
&\quad + |\{i \mid a_i \neq c_i \text{ e } c_i \neq b_i, \text{ com } i = 1, \dots, n\}| \\
&= |\{i \mid (a_i \neq c_i \text{ e } c_i = b_i) \text{ ou } (a_i = c_i \text{ e } c_i \neq b_i) \\
&\quad \text{ou } (a_i \neq c_i \text{ e } c_i \neq b_i), \text{ com } i = 1, \dots, n\}| \\
&\quad + |\{i \mid a_i \neq c_i \text{ e } c_i \neq b_i, \text{ com } i = 1, \dots, n\}| \\
&= |\{i \mid a_i \neq b_i, \text{ com } i = 1, \dots, n\}| \\
&\quad + |\{i \mid a_i \neq c_i \text{ e } c_i \neq b_i, \text{ com } i = 1, \dots, n\}| \\
&\quad - |\{i \mid a_i \neq b_i \text{ e } a_i \neq c_i \text{ e } c_i \neq b_i, \text{ com } i = 1, \dots, n\}| \\
&\quad + |\{i \mid a_i \neq c_i \text{ e } c_i \neq b_i, \text{ com } i = 1, \dots, n\}| \\
&\geq d(\mathbf{a}, \mathbf{b}) + |\{i \mid a_i \neq c_i \text{ e } c_i \neq b_i, \text{ com } i = 1, \dots, n\}| \\
&\geq d(\mathbf{a}, \mathbf{b}),
\end{aligned}$$

pois

$$\begin{aligned}
\{i \mid a_i \neq b_i, \text{ com } i = 1, \dots, n\} &= \{i \mid (a_i \neq c_i \text{ e } c_i = b_i) \text{ ou } (a_i = c_i \text{ e } c_i \neq b_i) \\
&\quad \text{ou } (a_i \neq c_i \text{ e } c_i \neq b_i \text{ e } a_i \neq b_i), \\
&\quad \text{com } i = 1, \dots, n\},
\end{aligned}$$

e

$$\{i \mid a_i \neq b_i \text{ e } a_i \neq c_i \text{ e } c_i \neq b_i, \text{ com } i = 1, \dots, n\} \subseteq \{i \mid a_i \neq c_i \text{ e } c_i \neq b_i, \text{ com } i = 1, \dots, n\}.$$

Então, segue que a distância de Hamming é de fato uma distância, pois é uma métrica. Logo, sendo uma métrica, ela define um espaço métrico em $\mathbb{F}_q^n$. Então, por exemplo, podemos considerar as bolas abertas (e fechadas) desse espaço:

- a bola aberta de centro $\mathbf{a} \in \mathbb{F}_q^n$ e raio $r > 0$ é

$$B(\mathbf{a}, r) = \{\mathbf{x} \in \mathbb{F}_q^n \mid d(\mathbf{x}, \mathbf{a}) < r\};$$

- a bola fechada de centro $\mathbf{a} \in \mathbb{F}_q^n$ e raio $r > 0$ é

$$B[\mathbf{a}, r] = \{\mathbf{x} \in \mathbb{F}_q^n \mid d(\mathbf{x}, \mathbf{a}) \leq r\}.$$

Além disso, se $\mathcal{C} \subseteq \mathbb{F}_q^n$ é um código e $\mathbf{a}, \mathbf{b} \in \mathcal{C}$, então $\mathbf{a} - \mathbf{b} \in \mathcal{C}$ e

$$d(\mathbf{a}, \mathbf{b}) = d(\mathbf{a} - \mathbf{b}, \mathbf{0}),$$

onde $\mathbf{0} \in \mathbb{F}_q^n$ é o vetor nulo. Desta forma, podemos definir:

Definição 3.1.2 (Distância mínima de um código). *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear. A distância mínima em $\mathcal{C}$ é definida como*

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

Agora, seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear. Se definirmos

$$\kappa = \frac{d_{\min} - 1}{2},$$

obtemos o seguinte resultado:

Lema 3.1.3. *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear com distância mínima $d_{\min}$. Então, se $\mathbf{a}, \mathbf{a}' \in \mathcal{C}$ são palavras distintas, então*

$$B[\mathbf{a}, \kappa] \cap B[\mathbf{a}', \kappa] = \emptyset.$$

Demonstração. De fato, suponha que exista $\mathbf{x} \in \mathbb{F}_q^n$ tal que

$$\mathbf{x} \in B[\mathbf{a}, \kappa] \cap B[\mathbf{a}', \kappa].$$

Então, $d(\mathbf{x}, \mathbf{a}) \leq \kappa$ e $d(\mathbf{x}, \mathbf{a}') \leq \kappa$. Logo,

$$\begin{aligned} d(\mathbf{a}, \mathbf{a}') &\leq d(\mathbf{x}, \mathbf{a}) + d(\mathbf{x}, \mathbf{a}') \\ &\leq 2\kappa \\ &\leq d_{\min} - 1 \\ &< d_{\min}. \end{aligned}$$

Isso é um absurdo, pois devemos ter $d(\mathbf{a}, \mathbf{a}') \geq d_{\min}$, para quaisquer duas palavras distintas do código. ■

Esse lema tem a seguinte consequência importante.

Teorema 3.1.4. *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear com distância mínima $d_{\min}$. Então $\mathcal{C}$ pode corrigir até κ erros e detectar até $d_{\min} - 1$ erros.*

Demonstração. Se ao transmitirmos uma palavra $\mathbf{a} \in \mathcal{C}$ cometemos t erros, com $t \leq \kappa$, recebemos a palavra $\mathbf{a}'$, então

$$d(\mathbf{a}, \mathbf{a}') = t \leq \kappa.$$

Pelo Lema 3.1.3, a distância de $\mathbf{a}'$ até qualquer outra palavra do código é maior que κ . Assim, a palavra enviada originalmente só pode ser $\mathbf{a} \in \mathcal{C}$, isto é, $\mathbf{a}$ está completamente determinado por $\mathbf{a}'$.

Por outro lado, podemos introduzir até $d_{\min} - 1$ erros na palavra $\mathbf{a} \in \mathcal{C}$ sem encontrar outra palavra do código. Assim a detecção do erro será de até $d_{\min} - 1$ erros. ■

Em um código temos três parâmetros fundamentais:

- Comprimento (n): o comprimento de um código se refere ao tamanho das palavras que serão transmitidas;
- Dimensão (k): a dimensão de um código se refere a capacidade de transmissão das palavras, já que o número de palavras em um código será q^k ;
- Distância mínima ($d_{\min}$): a distância mínima de um código está relacionada ao máximo de entradas erradas que um código poderá detectar e corrigir, como já visto.

Um código ideal seria aquele com uma grande dimensão (capaz de transmitir muita informação), uma grande distância mínima (o que significaria que seríamos capazes de determinar um maior número de erros e corrigi-los) e um comprimento pequeno (quanto maior o comprimento de um código, mais custoso é para transmitir cada palavra). Porém, esses parâmetros estão relacionados entre si e não é possível realizar todas essas otimizações simultaneamente.

Teorema 3.1.5 (A desigualdade de Singleton). *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear com comprimento n , dimensão k e distância mínima $d_{\min}$. Então,*

$$k + d_{\min} \leq n + 1.$$

Demonstração. Veja (MACWILLIAMS; SLOANE, 1977), página 33. ■

No caso que a desigualdade é uma igualdade, o código $\mathcal{C}$ é dito perfeito. A título de curiosidade, os únicos exemplos não triviais de códigos perfeitos são os Códigos de Hamming e o Código de Golay.

3.2 Construção dos códigos afins

Seja $I \subseteq \mathbb{F}_q[X_1, \dots, X_n]$ um ideal tal que $I = \langle g_1, \dots, g_t \rangle$. Para simplificar a escrita, escreveremos $\mathbb{F}_q[X_1, \dots, X_n]$ simplesmente como $\mathbb{F}_q[\mathbf{X}]$.

É fato que, para todo $i = 1, \dots, n$,

$$\prod_{a \in \mathbb{F}_q} (X_i - a) = X_i^q - X_i.$$

Isso ocorre pois $\prod_{a \in \mathbb{F}_q} (X_i - a)$ é um polinômio de grau q que se anula em todos os elementos de $\mathbb{F}_q$, isto é, ele possui q raízes, sendo elas os próprios elementos de $\mathbb{F}_q$. Por outro lado, $X_i^q - X_i$ também é um polinômio de grau q que se anula em todos os elementos de $\mathbb{F}_q$, pois

$$\begin{aligned} a^q - a &= a - a \\ &= 0, \end{aligned}$$

para todo $a \in \mathbb{F}_q$. Como ambos os polinômios são mônicos, necessariamente temos $\prod_{a \in \mathbb{F}_q} (X_i - a) = X_i^q - X_i$, para todo $i = 1, \dots, n$.

Defina $I_q = \langle g_1, \dots, g_t, X_1^q - X_1, \dots, X_n^q - X_n \rangle$. Assim, trivialmente,

$$V(I) = V(I_q).$$

Consideremos agora a ordem lexicográfica $\preceq_{lex}$, com $X_n \preceq_{lex} \dots \preceq_{lex} X_1$, no conjunto dos monômios $\mathcal{M} \subseteq \mathbb{F}_q[\mathbf{X}]$.

Como já vimos,

$$\begin{aligned} |\Delta(I_q)| &\leq |\Delta(\text{ml}(g_1), \dots, \text{ml}(g_t), X_1^q, \dots, X_n^q)| \\ &\leq q^n. \end{aligned}$$

Logo, pela Proposição 1.4.4, $|V(I_q)| \leq |\Delta(I_q)|$. Seja $V(I_q) = \{\mathbf{P}_1, \dots, \mathbf{P}_m\}$ e defina $\phi: \mathbb{F}_q[\mathbf{X}]/I_q \rightarrow \mathbb{F}_q^m$ como

$$\phi(f + I_q) = (f(\mathbf{P}_1), \dots, f(\mathbf{P}_m)).$$

Proposição 3.2.1. *A função ϕ é um isomorfismo entre $\mathbb{F}_q$ -espaços vetoriais.*

Demonstração. Note que ϕ é uma transformação linear. De fato, para todos $f, g \in \mathbb{F}_q[\mathbf{X}]$ e todo $\alpha \in \mathbb{F}_q$, segue que

$$\begin{aligned} \phi((f + I_q) + \alpha(g + I_q)) &= \phi((f + \alpha g) + I_q) \\ &= ((f + \alpha g)(\mathbf{P}_1), \dots, (f + \alpha g)(\mathbf{P}_m)) \\ &= (f(\mathbf{P}_1), \dots, f(\mathbf{P}_m)) + \alpha(g(\mathbf{P}_1), \dots, g(\mathbf{P}_m)) \\ &= \phi(f + I_q) + \alpha\phi(g + I_q). \end{aligned}$$

Agora, $X_i^q - X_i \in I_q$, para todo $i = 1, \dots, n$, e portanto I_q é ideal radical (v. (BECKER; WEISPFENNING, 1993, Prop. 8.14)). Assim, se $\mathbb{L}$ é um corpo algebricamente fechado contendo $\mathbb{F}_q$, do Teorema 1.4.7 temos que

$$|V_{\mathbb{L}}(I_q)| = |\Delta(I_q)|.$$

Por outro lado, do Teorema 1.3.4 temos que $\dim_{\mathbb{F}_q}(\mathbb{F}_q[\mathbf{X}]/I_q) = |\Delta(I_q)|$, e é claro que $V_{\mathbb{L}}(I_q) = V_{\mathbb{F}_q}(I_q) = m$. Isso mostra que o domínio e o contradomínio de ϕ têm a mesma dimensão.

Pelo Lema 1.4.3, existem polinômios $f_1, \dots, f_m \in \mathbb{F}_q[\mathbf{X}]$ tais que $f_i(\mathbf{P}_j) = \delta_{ij}$, para todos $i, j = 1, \dots, m$. Logo,

$$\phi(f_i + I_q) = \mathbf{e}_i,$$

onde $\mathbf{e}_i \in \mathbb{F}_q^m$ é o i -ésimo vetor canônico de $\mathbb{F}_q^m$, para todo $i = 1, \dots, m$. Portanto, ϕ é sobrejetora e, *a fortiori*, um isomorfismo. ■

Definição 3.2.2 (Código de variedade afim). *Seja $L \subseteq \mathbb{F}_q[\mathbf{X}]/I_q$ um $\mathbb{F}_q$ -espaço vetorial. A imagem $\phi(L) = \mathcal{C}(L)$ é chamado de código de variedade afim associado a L .*

Nosso objetivo nesse trabalho é apresentar resultados particulares sobre esses códigos e estudar seus duais. Para isso, sejam $S_1, \dots, S_n \subseteq \mathbb{F}_q$ subconjuntos não vazios e defina

$$\mathcal{S} = S_1 \times \dots \times S_n. \quad (3.1)$$

Seja $f_i \in \mathbb{F}_q[\mathbf{X}]$ o polinômio

$$f_i = \prod_{a \in S_i} (X_i - a),$$

para todo $i = 1, \dots, n$, e defina

$$I = \langle f_1, \dots, f_n \rangle.$$

Claramente, pela própria construção, $V(I) = \mathcal{S}$. Neste caso, tomamos

$$I_q = \langle f_1, \dots, f_n, X_1^q - X_1, \dots, X_n^q - X_n \rangle$$

e observamos que $I_q = I$, pois f_i é um fator de $X_i^q - X_i$, para todo $i = 1, \dots, n$.

Considere para todo inteiro $d \geq 0$, o $\mathbb{F}_q$ -subespaço vetorial de $\mathbb{F}_q[\mathbf{X}]$ dado por

$$L_d = \{f + I \in \mathbb{F}_q[\mathbf{X}]/I \mid f = 0 \text{ ou } \text{grau}(f) \leq d\},$$

onde $\text{grau}(f)$ se refere ao grau total do polinômio $f \in \mathbb{F}_q[\mathbf{X}]$, isto é,

$$\text{grau}(f) = \max(\text{grau}(M)),$$

com M sendo um monômio de f .

Definição 3.2.3 (Código afim). *O código afim $\mathcal{C}(d)$ é a imagem $\phi(L_d)$.*

Exemplo 3.2.4. *Seja $\mathbb{F}_4[X, Y]$ um anel de polinômios de duas variáveis, em que no conjunto de monômios $\mathcal{M} \subseteq \mathbb{F}_4[X, Y]$ está estabelecida a ordem lexicográfica, com $Y \preceq X$, e sejam $S_1, S_2 \in \mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$, com $\alpha^2 + (\alpha + 1) = 0$, dados por $S_1 = \{0, 1\}$ e $S_2 = \{\alpha, \alpha + 1\}$. Desta forma, temos $\mathcal{S} = \{(0, \alpha), (0, \alpha + 1), (1, \alpha), (1, \alpha + 1)\}$.*

Primeiramente, lembre-se que as operações de adição e produto definidas em $\mathbb{F}_4$ são dadas pelas seguintes tabelas:

+	0	1	α	$\alpha + 1$	·	0	1	α	$\alpha + 1$
0	0	1	α	$\alpha + 1$	0	0	0	0	0
1	1	0	$\alpha + 1$	α	1	0	1	α	$\alpha + 1$
α	α	$\alpha + 1$	0	1	α	0	α	$\alpha + 1$	1
$\alpha + 1$	$\alpha + 1$	α	1	0	$\alpha + 1$	0	$\alpha + 1$	1	α

Além disso,

$$f_1 = \prod_{a \in S_1} (X - a) = X^2 - X \quad e \quad f_2 = \prod_{b \in S_2} (Y - b) = Y^2 - Y + 1.$$

Logo, $I = \langle f_1, f_2 \rangle$, com $\{f_1, f_2\}$ sendo uma base de Gröbner para I . Assim, podemos identificar a pegada pela Figura 4.

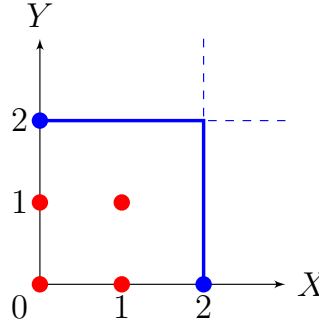


Figura 4 – Em azul, os monômios líderes de f_1 e f_2 e, em vermelho, os monômios de $\Delta(I)$.

A pegada é formada pelos monômios $X^\delta Y^\gamma$ com $(\delta, \gamma) \in \{(0, 0), (0, 1), (1, 0), (1, 1)\}$, ou seja, $\Delta(I) = \{1, Y, X, XY\}$. Portanto

$$\mathcal{B} = \{1 + I, Y + I, X + I, XY + I\}$$

é uma base para $\mathbb{F}_4[X, Y]/I$. Para simplificar a escrita e manter a harmonia estética, optaremos por representar $\alpha + 1$ por β . Assim:

(i) Para $d = 0$,

$$L_d = \{0 + I, 1 + I, \alpha + I, \beta + I\}.$$

Logo,

$$\begin{aligned} \phi(0 + I) &= (0, 0, 0, 0) & e & \quad \phi(1 + I) = (1, 1, 1, 1), \\ \phi(\alpha + I) &= (\alpha, \alpha, \alpha, \alpha) & e & \quad \phi(\beta + I) = (\beta, \beta, \beta, \beta). \end{aligned}$$

Portanto, $\mathcal{C}(d) = \{(0, 0, 0, 0), (1, 1, 1, 1), (\alpha, \alpha, \alpha, \alpha), (\beta, \beta, \beta, \beta)\}$.

(ii) Para $d = 1$,

$$L_d = \{aX + bY + c + I \in \mathbb{F}_4[X, Y]/I \mid a, b, c \in \mathbb{F}_4\}.$$

Note que isso implica que $|L_d| = 64$.

Agora, já sabemos que

$$\begin{aligned} \phi(0 + I) &= (0, 0, 0, 0) & e & \quad \phi(1 + I) = (1, 1, 1, 1), \\ \phi(\alpha + I) &= (\alpha, \alpha, \alpha, \alpha) & e & \quad \phi(\beta + I) = (\beta, \beta, \beta, \beta). \end{aligned}$$

Assim,

$$\begin{array}{llll}
 \phi(X + I) & = & (0, 0, 1, 1) & e \quad \phi(X + 1 + I) = (1, 1, 0, 0), \\
 \phi(X + \alpha + I) & = & (\alpha, \alpha, \beta, \beta) & e \quad \phi(X + \beta + I) = (\beta, \beta, \alpha, \alpha), \\
 \phi(\alpha X + I) & = & (0, 0, \alpha, \alpha) & e \quad \phi(\alpha X + 1 + I) = (1, 1, \beta, \beta), \\
 \phi(\alpha X + \alpha + I) & = & (\alpha, \alpha, 0, 0) & e \quad \phi(\alpha X + \beta + I) = (\beta, \beta, 1, 1), \\
 \phi(\beta X + I) & = & (0, 0, \beta, \beta) & e \quad \phi(\beta X + 1 + I) = (1, 1, \alpha, \alpha), \\
 \phi(\beta X + \alpha + I) & = & (\alpha, \alpha, 1, 1) & e \quad \phi(\beta X + \beta + I) = (\beta, \beta, 0, 0),
 \end{array}$$

e

$$\begin{array}{llll}
 \phi(Y + I) & = & (\alpha, \beta, \alpha, \beta) & e \quad \phi(Y + 1 + I) = (\beta, \alpha, \beta, \alpha), \\
 \phi(Y + \alpha + I) & = & (0, 1, 0, 1) & e \quad \phi(Y + \beta + I) = (1, 0, 1, 0), \\
 \phi(\alpha Y + I) & = & (\beta, 1, \beta, 1) & e \quad \phi(\alpha Y + 1 + I) = (\alpha, 0, \alpha, 0), \\
 \phi(\alpha Y + \alpha + I) & = & (1, \beta, 1, \beta) & e \quad \phi(\alpha Y + \beta + I) = (0, \alpha, 0, \alpha), \\
 \phi(\beta Y + I) & = & (1, \alpha, 1, \alpha) & e \quad \phi(\beta Y + 1 + I) = (0, \beta, 0, \beta), \\
 \phi(\beta Y + \alpha + I) & = & (\beta, 0, \beta, 0) & e \quad \phi(\beta Y + \beta + I) = (\alpha, 1, \alpha, 1),
 \end{array}$$

e

$$\begin{array}{llll}
 \phi(X + Y + I) & = & (\alpha, \beta, \beta, \alpha) & e \quad \phi(X + Y + 1 + I) = (\beta, \alpha, \alpha, \beta), \\
 \phi(X + Y + \alpha + I) & = & (0, 1, 1, 0) & e \quad \phi(X + Y + \beta + I) = (1, 0, 0, 1), \\
 \phi(X + \alpha Y + I) & = & (\beta, 1, \alpha, 0) & e \quad \phi(X + \alpha Y + 1 + I) = (\alpha, 0, \beta, 1), \\
 \phi(X + \alpha Y + \alpha + I) & = & (1, \beta, 0, \alpha) & e \quad \phi(X + \alpha Y + \beta + I) = (0, \alpha, 1, \beta), \\
 \phi(X + \beta Y + I) & = & (1, \alpha, 0, \beta) & e \quad \phi(X + \beta Y + 1 + I) = (0, \beta, 1, \alpha), \\
 \phi(X + \beta Y + \alpha + I) & = & (\beta, 0, \alpha, 1) & e \quad \phi(X + \beta Y + \beta + I) = (\alpha, 1, \beta, 0),
 \end{array}$$

e

$$\begin{array}{llll}
 \phi(\alpha X + Y + I) & = & (\alpha, \beta, 0, 1) & e \quad \phi(\alpha X + Y + 1 + I) = (\beta, \alpha, 1, 0), \\
 \phi(\alpha X + Y + \alpha + I) & = & (0, 1, \alpha, \beta) & e \quad \phi(\alpha X + Y + \beta + I) = (1, 0, \beta, \alpha), \\
 \phi(\alpha X + \alpha Y + I) & = & (\beta, 1, 1, \beta) & e \quad \phi(\alpha X + \alpha Y + 1 + I) = (\alpha, 0, 0, \alpha), \\
 \phi(\alpha X + \alpha Y + \alpha + I) & = & (1, \beta, \beta, 1) & e \quad \phi(\alpha X + \alpha Y + \beta + I) = (0, \alpha, \alpha, 0), \\
 \phi(\alpha X + \beta Y + I) & = & (1, \alpha, \beta, 0) & e \quad \phi(\alpha X + \beta Y + 1 + I) = (0, \beta, \alpha, 1), \\
 \phi(\alpha X + \beta Y + \alpha + I) & = & (\beta, 0, 1, \alpha) & e \quad \phi(\alpha X + \beta Y + \beta + I) = (\alpha, 1, 0, \beta),
 \end{array}$$

e

$$\begin{array}{llll}
 \phi(\beta X + Y + I) & = & (\alpha, \beta, 1, 0) & e \quad \phi(\beta X + Y + 1 + I) = (\beta, \alpha, 0, 1), \\
 \phi(\beta X + Y + \alpha + I) & = & (0, 1, \beta, \alpha) & e \quad \phi(\beta X + Y + \beta + I) = (1, 0, \alpha, \beta), \\
 \phi(\beta X + \alpha Y + I) & = & (\beta, 1, 0, \alpha) & e \quad \phi(\beta X + \alpha Y + 1 + I) = (\alpha, 0, 1, \beta), \\
 \phi(\beta X + \alpha Y + \alpha + I) & = & (1, \beta, \alpha, 0) & e \quad \phi(\beta X + \alpha Y + \beta + I) = (0, \alpha, \beta, 1), \\
 \phi(\beta X + \beta Y + I) & = & (1, \alpha, \alpha, 1) & e \quad \phi(\beta X + \beta Y + 1 + I) = (0, \beta, \beta, 0), \\
 \phi(\beta X + \beta Y + \alpha + I) & = & (\beta, 0, 0, \beta) & e \quad \phi(\beta X + \beta Y + \beta + I) = (\alpha, 1, 1, \alpha).
 \end{array}$$

Portanto,

$$\begin{aligned} \mathcal{C}(d) = \{ & (0, 0, 0, 0), (0, 0, 1, 1), (0, 0, \alpha, \alpha), (0, 0, \beta, \beta), (0, 1, 0, 1), (0, 1, 1, 0), \\ & (0, 1, \alpha, \beta), (0, 1, \beta, \alpha), (0, \alpha, 0, \alpha), (0, \alpha, 1, \beta), (0, \alpha, \alpha, 0), (0, \alpha, \beta, 1), \\ & (0, \beta, 0, \beta), (0, \beta, 1, \alpha), (0, \beta, \alpha, 1), (0, \beta, \beta, 0), (1, 0, 0, 1), (1, 0, 1, 0), \\ & (1, 0, \alpha, \beta), (1, 0, \beta, \alpha), (1, 1, 0, 0), (1, 1, 1, 1), (1, 1, \alpha, \alpha), (1, 1, \beta, \beta), \\ & (1, \alpha, 0, \beta), (1, \alpha, 1, \alpha), (1, \alpha, \alpha, 1), (1, \alpha, \beta, 0), (1, \beta, 0, \alpha), (1, \beta, 1, \beta), \\ & (1, \beta, \alpha, 0), (1, \beta, \beta, 1), (\alpha, 0, 0, \alpha), (\alpha, 0, 1, \beta), (\alpha, 0, \alpha, 0), (\alpha, 0, \beta, 1), \\ & (\alpha, 1, 0, \beta), (\alpha, 1, 1, \alpha), (\alpha, 1, \alpha, 1), (\alpha, 1, \beta, 0), (\alpha, \alpha, 0, 0), (\alpha, \alpha, 1, 1), \\ & (\alpha, \alpha, \alpha, \alpha), (\alpha, \alpha, \beta, \beta), (\alpha, \beta, 0, 1), (\alpha, \beta, 1, 0), (\alpha, \beta, \alpha, \beta), (\alpha, \beta, \beta, \alpha), \\ & (\beta, 0, 0, \beta), (\beta, 0, 1, \alpha), (\beta, 0, \alpha, 1), (\beta, 0, \beta, 0), (\beta, 1, 0, \alpha), (\beta, 1, 1, \beta), \\ & (\beta, 1, \alpha, 0), (\beta, 1, \beta, 1), (\beta, \alpha, 0, 1), (\beta, \alpha, 1, 0), (\beta, \alpha, \alpha, \beta), (\beta, \alpha, \beta, \alpha), \\ & (\beta, \beta, 0, 0), (\beta, \beta, 1, 1), (\beta, \beta, \alpha, \alpha), (\beta, \beta, \beta, \beta) \}; \end{aligned}$$

(iii) Para $d = 2$,

$$L_d = \{aXY + bX + cY + d + I \in \mathbb{F}_4[X, Y]/I \mid a, b, c, d \in \mathbb{F}_4\}.$$

Note que isso implica que $|L_d| = 256$. Como $\phi(L_d) \subseteq \mathbb{F}_4^4$ e $|\mathbb{F}_4^4| = 256$, segue que

$$\mathcal{C}(d) = \mathbb{F}_4^4.$$

(iv) Note que, para todo número inteiro $d \geq 1$,

$$L_{d-1} \subseteq L_d.$$

Desta forma, para todo $d \geq 3$, temos

$$L_2 \subseteq L_3 \subseteq \cdots \subseteq L_{d-1} \subseteq L_d,$$

o que implica

$$\mathcal{C}(2) \subseteq \mathcal{C}(3) \subseteq \cdots \subseteq \mathcal{C}(d-1) \subseteq \mathcal{C}(d).$$

Como $\mathcal{C}(d) \subseteq \mathbb{F}_4^4$ e, por (iii), $\mathcal{C}(2) = \mathbb{F}_4^4$, segue que

$$\mathcal{C}(d) = \mathbb{F}_4^4,$$

para todo $d \geq 3$. No Teorema 3.2.10, item (i), veremos que esse fenômeno sempre acontece.

Exemplo 3.2.5. No caso que $S_i = \mathbb{F}_q$, para todo $i = 1, \dots, n$, temos que $\mathcal{C}(d)$ é chamado de código generalizado de Reed-Muller, para todo inteiro $d \geq 0$ (v. e.g. (MACWILLIAMS; SLOANE, 1977, Cap. 13)).

Os códigos generalizados de Reed-Muller são amplamente estudados na Teoria de Códigos Corretores de Erro e, por tal motivo, não serão objeto de discussão aprofundada nesse trabalho.

Seja $d_i = |S_i|$, para todo $i = 1, \dots, n$. Então,

$$|V(I)| = d_1 \cdots d_n,$$

e esse é o comprimento de $\mathcal{C}(d)$, para todo inteiro $d \geq 0$. Sem perda de generalidade, podemos assumir $d_1 \leq \cdots \leq d_n$ e mais ainda, podemos assumir que $2 \leq d_1$ (veja (LOPEZ; RENTERIA-MARQUEZ; VILLARREAL, 2012, Prop. 3.2)).

Lema 3.2.6. *O conjunto $\{f_1, \dots, f_n\}$ é uma base de Gröbner para I .*

Demonstração. Claramente $\text{ml}(f_i) = X_i^{d_i}$, para todo $i = 1, \dots, n$. Logo,

$$\Delta(I) \subseteq \{X_1^{\alpha_1} \cdots X_n^{\alpha_n} \mid 0 \leq \alpha_i < d_i, \text{ para todo } i = 1, \dots, n\}.$$

Agora, observe que pelo Teorema 1.4.7, temos

$$\begin{aligned} |V(I)| &= d_1 \cdots d_n \\ &\leq |\Delta(I)| \\ &\leq d_1 \cdots d_n. \end{aligned}$$

Desta forma, temos $|\Delta(I)| = d_1 \cdots d_n$. Portanto, $\{f_1, \dots, f_n\}$ é uma base de Gröbner para I , pois se não fosse, usando o algoritmo de Buchberger encontraríamos um polinômio f_{n+1} , cujo monômio líder não é múltiplo de $\text{ml}(f_i)$, para todo $i = 1, \dots, n$, o que implicaria em $|\Delta(I)| < d_1 \cdots d_n$. ■

Lema 3.2.7. *O ideal de $\mathcal{S}$ é I , isto é, $\mathcal{I}(\mathcal{S}) = I$.*

Demonstração. Primeiramente, note que $I \subseteq \mathcal{I}(\mathcal{S})$ (de fato, como $\mathcal{S} = V(I)$, então, obviamente, $I \subseteq \mathcal{I}(\mathcal{S})$). Logo,

$$\Delta(\mathcal{I}(\mathcal{S})) \subseteq \Delta(I).$$

Assim, pela Proposição 1.4.4, temos

$$\begin{aligned} d_1 \cdots d_n &= |V(\mathcal{I}(\mathcal{S}))| \\ &\leq |\Delta(\mathcal{I}(\mathcal{S}))| \\ &\leq |\Delta(I)| \\ &= d_1 \cdots d_n. \end{aligned}$$

O que implica $|\Delta(\mathcal{I}(\mathcal{S}))| = d_1 \cdots d_n$. Como

$$\{f_1, \dots, f_n\} \subseteq \mathcal{I}(\mathcal{S}),$$

pelo Lema 3.2.6, temos que $\{f_1, \dots, f_n\}$ é uma base de Gröbner para $\mathcal{I}(\mathcal{S})$ e $\mathcal{I}(\mathcal{S}) = I$. ■

Vamos obter agora a dimensão de $\mathcal{C}(d)$. Como ϕ é um isomorfismo e $\mathcal{C}(d) = \phi(L_d)$, temos

$$\dim(\mathcal{C}(d)) = \dim(L_d).$$

Seja

$$\Delta(I)_d = \{M \in \Delta(I) \mid \text{grau}(M) \leq d\}.$$

Proposição 3.2.8. *O conjunto*

$$\{M + I \in \mathbb{F}_q[\mathbf{X}]/I \mid M \in \Delta(I)_d\}$$

é uma base para L_d .

Demonstração. Pelo Teorema 1.3.4, temos que

$$\{M + I \in \mathbb{F}_q[\mathbf{X}]/I \mid M \in \Delta(I)_d\}$$

é um conjunto linearmente independente e, claramente,

$$\{M + I \in \mathbb{F}_q[\mathbf{X}]/I \mid M \in \Delta(I)_d\} \subseteq L_d.$$

Sejam $f \in \mathbb{F}_q[\mathbf{X}]$, tal que $f \neq 0$ e $\text{grau}(f) \leq d$, e $r \in \mathbb{F}_q[\mathbf{X}]$ o resto da divisão de f por $\{f_1, \dots, f_n\}$. Do algoritmo da divisão, como $\{f_1, \dots, f_n\}$ é uma base de Gröbner para I e pela Proposição 1.3.2, segue que r é uma combinação linear de monômios em $\Delta(I)_d$. Portanto, segue o resultado. ■

Lema 3.2.9. *Seja $d' = \sum_{i=1}^n (d_i - 1) - d - 1$. Então,*

$$\dim(\mathcal{C}(d)) + \dim(\mathcal{C}(d')) = d_1 \cdots d_n.$$

Demonstração. Pela Proposição 3.2.8, o valor de $\dim(\mathcal{C}(d))$ pode ser visto como o número de soluções inteiras da desigualdade

$$\alpha_1 + \cdots + \alpha_n \leq d,$$

com $0 \leq \alpha_i \leq d_i - 1$, para todo $i = 1, \dots, n$. Por sua vez, o número de soluções inteiras da desigualdade

$$\alpha_1 + \cdots + \alpha_n > d,$$

com $0 \leq \alpha_i \leq d_i - 1$, para todo $i = 1, \dots, n$, é numericamente igual ao número de soluções inteiras da desigualdade

$$\beta_1 + \cdots + \beta_n \leq \sum_{i=1}^n (d_i - 1) - d - 1,$$

com $0 \leq \beta_i \leq d_i - 1$, para todo $i = 1, \dots, n$. De fato, seja $(\alpha_1, \dots, \alpha_n)$ tal que $\alpha_1 + \dots + \alpha_n > d$, e $0 \leq \alpha_i \leq d_i - 1$, para todo $i = 1, \dots, n$. Tomando $\beta_i = d_i - 1 - \alpha_i$, para todo $i = 1, \dots, n$, temos

$$\begin{aligned} d &< \alpha_1 + \dots + \alpha_n \\ &= (d_1 - 1 - \beta_1) + \dots + (d_n - 1 - \beta_n) \\ &= \sum_{i=1}^n (d_i - 1) - (\beta_1 + \dots + \beta_n), \end{aligned}$$

ou seja, $\sum_{i=1}^n (d_i - 1) - (\beta_1 + \dots + \beta_n) > d$. Logo,

$$\begin{aligned} \beta_1 + \dots + \beta_n &\leq \sum_{i=1}^n (d_i - 1) - d - 1 \\ &= d'. \end{aligned}$$

Além disso, como $0 \leq \alpha_i \leq d_i - 1$, segue que $0 \leq \beta_i \leq d_i - 1$, para todo $i = 1, \dots, n$. Analogamente, se mostra que dada uma n -upla $(\beta_1, \dots, \beta_n)$ tal que $\beta_1 + \dots + \beta_n \leq d'$ e $0 \leq \beta_i \leq d_i - 1$, para todo $i = 1, \dots, n$, se definimos $\alpha_i = d_i - 1 - \beta_i$ para todo $i = 1, \dots, n$ temos que $\alpha_1 + \dots + \alpha_n > d$.

Pela Proposição 3.2.8, o valor de $\dim(\mathcal{C}(d'))$ pode ser visto como o número de soluções inteiras da desigualdade

$$\beta_1 + \dots + \beta_n \leq d',$$

com $0 \leq \beta_i \leq d_i - 1$, para todo $i = 1, \dots, n$.

Agora seja $M \in \Delta(I)$, digamos $M = X_1^{\alpha_1} \dots X_n^{\alpha_n}$. Então $\text{grau}(M) = \alpha_1 + \dots + \alpha_n$ com $0 \leq \alpha_i \leq d_i - 1$, para todo $i = 1, \dots, n$. Assim,

$$\alpha_1 + \dots + \alpha_n \leq d \quad \text{ou} \quad \alpha_1 + \dots + \alpha_n > d.$$

Desta forma, temos

$$\dim(\mathcal{C}(d)) + \dim(\mathcal{C}(d')) = d_1 \dots d_n,$$

como desejávamos. ■

Teorema 3.2.10. *A dimensão de um código $\mathcal{C}(d)$ é*

$$\dim(\mathcal{C}(d)) = |\Delta(I)_d|,$$

e, em particular,

$$(i) \text{ para todo } d \geq \sum_{i=1}^n (d_i - 1),$$

$$\dim(\mathcal{C}(d)) = d_1 \dots d_n;$$

(ii) para todo $0 \leq d < \sum_{i=1}^n (d_i - 1)$,

$$\begin{aligned} \dim(\mathcal{C}(d)) &= \binom{n+d}{d} - \sum_{i=1}^n \binom{n+d-d_i}{d-d_i} + \cdots + \\ &\quad + (-1)^j \sum_{1 \leq i_1 < \cdots < i_j \leq n} \binom{n+d-d_{i_1}-\cdots-d_{i_j}}{d-d_{i_1}-\cdots-d_{i_j}} + \cdots + \\ &\quad + (-1)^n \binom{n+d-d_1-\cdots-d_n}{d-d_1-\cdots-d_n}, \end{aligned}$$

com $\binom{a}{b} = 0$ se $b < 0$.

Demonstração. Pela Proposição 3.2.8, temos que

$$\{M + I \in \mathbb{F}_q[\mathbf{X}]/I \mid M \in \Delta(I)_d\}$$

é uma base para L_d . Como $\mathcal{C}(d) = \phi(L_d)$, segue que

$$\begin{aligned} \dim(\mathcal{C}(d)) &= \dim(L_d) \\ &= |\{M + I \in \mathbb{F}_q[\mathbf{X}]/I \mid M \in \Delta(I)_d\}| \\ &= |\Delta(I)_d|, \end{aligned}$$

lembrando que $\Delta(I)_d = \{M \in \Delta(I) \mid \text{grau}(M) \leq d\}$.

Agora:

(i) Suponha que $d \geq \sum_{i=1}^n (d_i - 1)$.

Como $\{f_1, \dots, f_n\}$ é uma base de Gröbner para I , temos

$$\Delta(I) = \{X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in \mathbb{F}_q[\mathbf{X}] \mid 0 \leq \alpha_i \leq d_i - 1, \text{ para todo } i = 1, \dots, n\}.$$

Desta forma, $\Delta(I)_d = \Delta(I)$, logo pelo Lema 3.2.8 temos que

$$\begin{aligned} \dim(\mathcal{C}(d)) &= |\Delta(I)| \\ &= d_1 \cdots d_n. \end{aligned}$$

(ii) Suponha $0 \leq d \leq \sum_{i=1}^n (d_i - 1)$.

Note que existe uma bijeção entre os conjuntos $\Delta(I)_d$ e

$$\begin{aligned} \nabla_d = \left\{ X_0^{\alpha_0} X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in \mathbb{F}_q[X_0, X_1, \dots, X_n] \mid \sum_{i=0}^n \alpha_i = d \text{ e} \right. \\ \left. 0 \leq \alpha_i \leq d_i - 1, \text{ para todo } i = 1, \dots, n \right\} \end{aligned}$$

dada por $\Gamma: \Delta(I)_d \longrightarrow \nabla_d$, em que

$$\Gamma(M) = X_0^d \cdot M \left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0} \right),$$

isto é, o produto de X_0^d pelo monômio M após sua avaliação em $\left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0} \right)$, e $\Gamma^{-1}: \nabla_d \longrightarrow \Delta(I)_d$, em que

$$\Gamma^{-1}(N) = N(1, X_1, \dots, X_n),$$

isto é, o monômio N avaliado em $(1, X_1, \dots, X_n)$. Com efeito, sejam $M \in \Delta(I)_d$, e $N \in \nabla_d$, em que

$$M = X_1^{\beta_1} \dots X_n^{\beta_n} \quad \text{e} \quad N = X_0^{\alpha_0} X_1^{\alpha_1} \dots X_n^{\alpha_n},$$

com $\text{grau}(M) = \sum_{i=1}^n \beta_i \leq d$, $\text{grau}(N) = \sum_{j=0}^n \alpha_j = d$ e $0 \leq \alpha_j \leq d_j - 1$, para todo $j = 1, \dots, n$, então

$$\begin{aligned} (\Gamma \circ \Gamma^{-1})(N) &= \Gamma(N(1, X_1, \dots, X_n)) \\ &= \Gamma(X_1^{\alpha_1} \dots X_n^{\alpha_n}) \\ &= X_0^d \cdot X_1^{\alpha_1} \dots X_n^{\alpha_n} \left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0} \right) \\ &= X_0^d \cdot \frac{X_1^{\alpha_1}}{X_0^{\alpha_1}} \dots \frac{X_n^{\alpha_n}}{X_0^{\alpha_n}} \\ &= \frac{X_0^d}{X_0^{\alpha_1 + \dots + \alpha_n}} X_1^{\alpha_1} \dots X_n^{\alpha_n} \\ &= X_0^{d - (\alpha_1 + \dots + \alpha_n)} X_1^{\alpha_1} \dots X_n^{\alpha_n} \\ &= X_0^{\alpha_0} X_1^{\alpha_1} \dots X_n^{\alpha_n} \\ &= N, \end{aligned}$$

e, considerando $\sum_{i=1}^n \beta_i =: \tilde{d}$,

$$\begin{aligned} (\Gamma^{-1} \circ \Gamma)(M) &= \Gamma^{-1} \left(X_0^d \cdot M \left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0} \right) \right) \\ &= \Gamma^{-1} \left(X_0^d \cdot X_1^{\beta_1} \dots X_n^{\beta_n} \left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0} \right) \right) \\ &= \Gamma^{-1} \left(X_0^d \cdot \frac{X_1^{\beta_1}}{X_0^{\beta_1}} \dots \frac{X_n^{\beta_n}}{X_0^{\beta_n}} \right) \\ &= \Gamma^{-1} \left(\frac{X_0^d}{X_0^{\beta_1 + \dots + \beta_n}} X_1^{\beta_1} \dots X_n^{\beta_n} \right) \\ &= \Gamma^{-1} \left(X_0^{d - \tilde{d}} X_1^{\beta_1} \dots X_n^{\beta_n} \right) \\ &= X_0^{d - \tilde{d}} X_1^{\beta_1} \dots X_n^{\beta_n} (1, X_1, \dots, X_n) \\ &= X_1^{\beta_1} \dots X_n^{\beta_n} \\ &= M. \end{aligned}$$

Portanto, Γ e Γ^{-1} são bijeções entre $\Delta(I)_d$ e ∇_d de fato.

Agora, defina

$$H(t) = (1 + t + t^2 + \dots) \cdot \prod_{i=1}^n (1 + t + \dots + t^{d_i-1}).$$

Observe que o coeficiente de t^d é igual a $|\nabla_d|$. Para calcular esse coeficiente, podemos enxergar H como um função real de um variável, a saber t , definida em alguma vizinhança de 0, digamos $|t| < 1$. Então, a série geométrica

$$1 + t + t^2 + \dots$$

é convergente e

$$1 + t + t^2 + \dots = \frac{1}{1-t}.$$

Além disso, para todo $i = 1, \dots, n$, a expressão

$$1 + t + \dots + t^{d_i-1}$$

é um pedaço dessa série geométrica (ou uma série geométrica truncada), assim,

$$1 + t + \dots + t^{d_i-1} = \frac{1 - t^{d_i}}{1 - t}.$$

Logo,

$$\begin{aligned} H(t) &= (1 + t + t^2 + \dots) \cdot \prod_{i=1}^n (1 + t + \dots + t^{d_i-1}) \\ &= \frac{1}{1-t} \cdot \prod_{i=1}^n \frac{1 - t^{d_i}}{1 - t} \\ &= \frac{1}{(1-t)^{n+1}} \cdot \prod_{i=1}^n (1 - t^{d_i}) \\ &= \left(\sum_{j=0}^{\infty} \binom{n+j}{j} t^j \right) \cdot \prod_{i=1}^n (1 - t^{d_i}) \\ &= \left(\sum_{j=0}^{\infty} \binom{n+j}{j} t^j \right) \cdot \left(1 - \sum_{i=0}^n t^{d_i} + \sum_{i \leq i_1 < i_2 \leq n} t^{d_{i_1} + d_{i_2}} + \dots \right. \\ &\quad \left. + (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq n} t^{d_{i_1} + \dots + d_{i_k}} + \dots + (-1)^n t^{d_{i_1} + \dots + d_{i_n}} \right) \\ &= \sum_{j=0}^{\infty} \binom{n+j}{j} t^j - \sum_{i=0}^n \left(\sum_{j=0}^{\infty} \binom{n+j}{j} t^{j+d_i} \right) + \\ &\quad + \sum_{i \leq i_1 < i_2 \leq n} \left(\sum_{j=0}^{\infty} \binom{n+j}{j} t^{j+d_{i_1}+d_{i_2}} \right) + \dots \\ &\quad + (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq n} \left(\sum_{j=0}^{\infty} \binom{n+j}{j} t^{j+d_{i_1}+\dots+d_{i_k}} \right) + \dots + \\ &\quad + (-1)^n \sum_{j=0}^{\infty} \binom{n+j}{j} t^{j+d_{i_1}+\dots+d_{i_n}}, \end{aligned}$$

pois $\frac{1}{(1-t)^{n+1}} = \sum_{j=0}^{\infty} \binom{n+j}{j} t^j$ (veja (SANTOS, 2024)). Assim, o coeficiente de t^d é igual a $|\nabla_d|$, o qual é igual a $|\Delta(I)_d|$ por Γ (ou Γ^{-1}). Portanto,

$$\begin{aligned} \dim(\mathcal{C}(d)) &= |\Delta(I)_d| \\ &= |\nabla_d| \\ &= \binom{n+d}{d} - \sum_{i=1}^n \binom{n+d-d_i}{d-d_i} + \cdots + \\ &\quad + (-1)^j \sum_{1 \leq i_1 < \cdots < i_j \leq n} \binom{n+d-d_{i_1}-\cdots-d_{i_j}}{d-d_{i_1}-\cdots-d_{i_j}} + \cdots + \\ &\quad + (-1)^n \binom{n+d-d_1-\cdots-d_n}{d-d_1-\cdots-d_n}, \end{aligned}$$

com $\binom{a}{b} = 0$ se $b < 0$.

Portanto, o resultado segue. ■

3.3 Duais de códigos afins

Definição 3.3.1 (Produto interno). *O produto interno em $\mathbb{F}_q^n$ é a função $\langle \cdot, \cdot \rangle: \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ dada por*

$$\begin{aligned} \langle \mathbf{a}, \mathbf{b} \rangle &= a_1 b_1 + \cdots + a_n b_n \\ &= \sum_{i=1}^n a_i b_i, \end{aligned}$$

para todos $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$, em que $\mathbf{a} = (a_1, \dots, a_n)$ e $\mathbf{b} = (b_1, \dots, b_n)$.

Exemplo 3.3.2. *Sejam $\mathbb{F}_5$ o corpo finito com 5 elementos e tome $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in \mathbb{F}_5^4$ com:*

$$\begin{aligned} \mathbf{a} &= (0, 0, 0, 0) & e & \quad \mathbf{b} = (1, 3, 1, 4), \\ \mathbf{c} &= (3, 2, 2, 0) & e & \quad \mathbf{d} = (1, 2, 3, 4). \end{aligned}$$

Então, $\langle \mathbf{a}, \mathbf{a} \rangle = 0$, $\langle \mathbf{b}, \mathbf{c} \rangle = 1$, $\langle \mathbf{c}, \mathbf{d} \rangle = 3$ e $\langle \mathbf{d}, \mathbf{b} \rangle = 3$.

De fato:

$$\begin{aligned} \langle \mathbf{a}, \mathbf{a} \rangle &= 0 \cdot 0 + 0 \cdot 0 + 0 \cdot 0 + 0 \cdot 0 \\ &= 0 + 0 + 0 + 0 \\ &= 0; \end{aligned}$$

e

$$\begin{aligned} \langle \mathbf{b}, \mathbf{c} \rangle &= 1 \cdot 3 + 3 \cdot 2 + 1 \cdot 2 + 4 \cdot 0 \\ &= 3 + 1 + 2 + 0 \\ &= 1; \end{aligned}$$

e

$$\begin{aligned}\langle \mathbf{c}, \mathbf{d} \rangle &= 3 \cdot 1 + 2 \cdot 2 + 2 \cdot 3 + 0 \cdot 4 \\ &= 3 + 4 + 1 + 0 \\ &= 3;\end{aligned}$$

e

$$\begin{aligned}\langle \mathbf{d}, \mathbf{b} \rangle &= 1 \cdot 1 + 2 \cdot 3 + 3 \cdot 1 + 4 \cdot 4 \\ &= 1 + 1 + 3 + 3 \\ &= 3.\end{aligned}$$

Definição 3.3.3 (Dual de um código). *Seja $\mathcal{C}$ um código. Seu dual é definido como*

$$\mathcal{C}^\perp = \{\mathbf{b} \in \mathbb{F}_q^n \mid \langle \mathbf{b}, \mathbf{a} \rangle = 0, \text{ para todo } \mathbf{a} \in \mathcal{C}\},$$

em que $\langle \mathbf{b}, \mathbf{a} \rangle$ denota o produto interno entre $\mathbf{b}$ e $\mathbf{a}$.

Definição 3.3.4 (Código com dual complementar). *Seja $\mathcal{C}$ um código. Diremos que $\mathcal{C}$ é código com dual complementar se*

$$\mathcal{C} \cap \mathcal{C}^\perp = \{\mathbf{0}\}.$$

Definição 3.3.5 (Código auto-ortogonal e auto-dual). *Seja $\mathcal{C}$ um código. Diremos que $\mathcal{C}$ é auto-ortogonal se*

$$\mathcal{C} \subseteq \mathcal{C}^\perp.$$

Se valer a igualdade, isto é, $\mathcal{C} = \mathcal{C}^\perp$, diremos que $\mathcal{C}$ é auto-dual.

Exemplo 3.3.6. *Seja $\mathcal{C} \subseteq \mathbb{F}_2^3$ um código gerado por $(1, 0, 1)$. Temos que $\mathcal{C}^\perp$ é o código que tem como base $\{(0, 1, 0), (1, 0, 1)\}$. Portanto, $\mathcal{C}$ não é código com dual complementar, é código auto-ortogonal e não é código auto-dual.*

De fato, note que

$$\begin{aligned}\mathcal{C} &= \langle (1, 0, 1) \rangle \\ &= \{(0, 0, 0), (1, 0, 1)\}.\end{aligned}$$

Agora,

$$\begin{aligned}\langle (a, b, c), (0, 0, 0) \rangle &= a \cdot 0 + b \cdot 0 + c \cdot 0 \\ &= 0,\end{aligned}$$

para todo $(a, b, c) \in \mathbb{F}_2^3$ e,

$$\begin{aligned}\langle (a, b, c), (1, 0, 1) \rangle &= a \cdot 1 + b \cdot 0 + c \cdot 1 \\ &= a + c,\end{aligned}$$

$(a, b, c) \in \mathbb{F}_2^3$. Logo, $\langle (a, b, c), (1, 0, 1) \rangle = 0$ se, e somente se, $a = c$. Assim, $(a, b, c) \in \{(0, 0, 0), (0, 1, 0), (1, 0, 1), (1, 1, 1)\}$. Portanto, segue que

$$\begin{aligned}\mathcal{C}^\perp &= \mathbb{F}_2^3 \cap \{(0, 0, 0), (0, 1, 0), (1, 0, 1), (1, 1, 1)\} \\ &= \{(0, 0, 0), (0, 1, 0), (1, 0, 1), (1, 1, 1)\} \\ &= \langle (0, 1, 0), (1, 0, 1) \rangle.\end{aligned}$$

Desta forma, note que

$$\begin{aligned}\mathcal{C} \cap \mathcal{C}^\perp &= \{(0, 0, 0), (1, 0, 1)\} \\ &= \langle (1, 0, 1) \rangle \\ &= \mathcal{C}.\end{aligned}$$

Portanto, $\mathcal{C}$ não é um código dual complementar, é código auto-ortogonal e não é código auto-dual.

Vamos trabalhar a partir de agora com códigos cartesianos afins. Tomamos então $S_1, \dots, S_n \subseteq \mathbb{F}_q$ subconjuntos não vazios, e seja

$$\mathcal{S} = S_1 \times \dots \times S_n.$$

Seja ainda

$$f_i = \prod_{a \in S_i} (X_i - a),$$

para todo $i = 1, \dots, n$, e

$$I = \langle f_1, \dots, f_n \rangle.$$

Dado um inteiro $d \geq 0$, seja

$$L_d = \{f + I \in \mathbb{F}_q[X]/I \mid f = 0 \text{ ou } \text{grau}(f) \leq d\}.$$

Lembramos que $\mathcal{C}(d) = \phi(L_d)$, em que ϕ é dada por (3.1).

Definição 3.3.7 (Resíduo de uma classe de polinômios). *Sejam $\mathbf{P}_k \in \mathcal{S}$, em que $\mathbf{P}_k = (a_{k1}, \dots, a_{kn})$, com $k = 1, \dots, m$ e $m = d_1 \dots d_n$, e $f + I \in \mathbb{F}_q[\mathbf{X}]/I$. O resíduo de $f + I$ no ponto $\mathbf{P}_k$ é dado por*

$$\text{Res}_{\mathbf{P}_k}(f + I) = \frac{f(\mathbf{P}_k)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)}.$$

Note que o resíduo está bem definido, isto é, ele independe do representante da classe. De fato, se g é um polinômio tal que $g + I = f + I$ então $g = f + h$, com $h \in I$, e

temos

$$\begin{aligned}
\text{Res}_{\mathbf{P}_k}(g + I) &= \text{Res}_{\mathbf{P}_k}((f + h) + I) \\
&= \frac{(f + h)(\mathbf{P}_k)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)} \\
&= \frac{f(\mathbf{P}_k)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)} + \frac{h(\mathbf{P}_k)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)} \\
&= \frac{f(\mathbf{P}_k)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)} \\
&= \text{Res}_{\mathbf{P}_k}(f + I),
\end{aligned}$$

em que $h(\mathbf{P}) = 0$, pois $h \in I$ com $I = \mathcal{I}(V(I))$ e $V(I) = \mathcal{S}$.

Vamos definir a aplicação $\text{Res}_{\mathcal{S}}: \mathbb{F}_q[\mathbf{X}]/I \longrightarrow \mathbb{F}_q^m$ como sendo

$$\text{Res}_{\mathcal{S}}(f + I) = (\text{Res}_{\mathbf{P}_1}(f + I), \dots, \text{Res}_{\mathbf{P}_m}(f + I))$$

para todo $f + I \in \mathbb{F}_q[\mathbf{X}]/I$.

Note que $\text{Res}_{\mathcal{S}}$ é um homomorfismo entre $\mathbb{F}_q$ -espaços vetoriais. De fato, sejam $f + I, g + I \in \mathbb{F}_q[X]/I$ e $\alpha \in \mathbb{F}_q$. Então, para cada $\mathbf{P}_k \in \mathcal{S}$, em que $\mathbf{P}_k = (a_{k1}, \dots, a_{kn})$, com $k = 1, \dots, m$, temos

$$\begin{aligned}
\text{Res}_{\mathbf{P}_k}((f + I) + \alpha(g + I)) &= \text{Res}_{\mathbf{P}_k}((f + \alpha g) + I) \\
&= \frac{(f + \alpha g)(\mathbf{P}_k)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)} \\
&= \frac{f(\mathbf{P}_k)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)} + \alpha \frac{g(\mathbf{P}_k)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)} \\
&= \text{Res}_{\mathbf{P}_k}(f + I) + \alpha \text{Res}_{\mathbf{P}_k}(g + I).
\end{aligned}$$

Desta forma,

$$\begin{aligned}
\text{Res}_{\mathcal{S}}((f + I) + \alpha(g + I)) &= \text{Res}_{\mathcal{S}}((f + \alpha g) + I) \\
&= (\text{Res}_{\mathbf{P}_1}((f + \alpha g) + I), \dots, \text{Res}_{\mathbf{P}_m}((f + \alpha g) + I)) \\
&= (\text{Res}_{\mathbf{P}_1}(f + I), \dots, \text{Res}_{\mathbf{P}_m}(f + I)) + \\
&\quad + \alpha(\text{Res}_{\mathbf{P}_1}(g + I), \dots, \text{Res}_{\mathbf{P}_m}(g + I)) \\
&= \text{Res}_{\mathcal{S}}(f + I) + \alpha \text{Res}_{\mathcal{S}}(g + I).
\end{aligned}$$

Agora, seja $f + I \in \ker(\text{Res}_S)$. Então, $\text{Res}_S(f + I) = \mathbf{0}$, ou seja, $\text{Res}_{\mathbf{P}_k}(f + I) = 0$, para todo $\mathbf{P}_k \in \mathcal{S}$, com $k = 1, \dots, n$. Daí,

$$\frac{f(\mathbf{P}_k)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)} = 0,$$

para todo $\mathbf{P}_k \in \mathcal{S}$, com $k = 1, \dots, n$, ou seja, $f(\mathbf{P}_k) = 0$, para todo $\mathbf{P}_k \in \mathcal{S}$, com $k = 1, \dots, n$. Isso significa que $f \in \mathcal{I}(\mathcal{S})$, mas, pelo Lema 3.2.7, temos que $\mathcal{I}(\mathcal{S}) = I$. Então, $f \in I$, ou ainda, $f + I = I$. Portanto, a função resíduo $\text{Res}_S: \mathbb{F}_q[\mathbf{X}]/I \rightarrow \mathbb{F}_q^m$ é um monomorfismo.

Teorema 3.3.8. *Sejam $\mathbf{P}_1, \dots, \mathbf{P}_m \in \mathcal{S}$ e $\mathcal{C}(d)$ um código afim. O dual de $\mathcal{C}(d)$ é dado por*

$$\mathcal{C}^\perp(d) = \text{Res}_S(L_{d'}),$$

em que $d' = \sum_{i=1}^n (d_i - 1) - d - 1$ e com $L_{d'} \subseteq \mathbb{F}_q[\mathbf{X}]/I$.

Demonstração. Sejam $f + I \in L_d$ e $g + I \in L_{d'}$. Pelo algoritmo da divisão, existem $h_1, \dots, h_n, r \in \mathbb{F}_q[\mathbf{X}]$ tais que

$$fg = h_1 f_1 + \dots + h_n f_n + r,$$

com $r = 0$ ou nenhum monômio que aparece em r sendo múltiplo de $\text{ml}(f_i)$, para todo $i = 1, \dots, n$. Além disso,

$$\begin{aligned} \text{grau}(r) &\leq \text{grau}(fg) \\ &\leq \text{grau}(f) + \text{grau}(g) \\ &= d + d' \\ &= d + \sum_{i=1}^n (d_i - 1) - d - 1 \\ &= \sum_{i=1}^n (d_i - 1) - 1. \end{aligned}$$

Note que, para todo $k = 1, \dots, m$, escrevemos $\mathbf{P}_k = (a_{k1}, \dots, a_{kn})$ e

$$\begin{aligned} (fg)(\mathbf{P}_k) &= (h_1 f_1)(\mathbf{P}_k) + \dots + (h_n f_n)(\mathbf{P}_k) + r(\mathbf{P}_k) \\ &= r(\mathbf{P}_k). \end{aligned}$$

Considere o polinômio

$$\begin{aligned}
\tilde{r} &= \sum_{\mathbf{P}_k \in \mathcal{S}} \left(\text{Res}_{\mathbf{P}_k}(fg + I) \cdot \prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (X_i - a'_i) \right) \\
&= \sum_{\mathbf{P}_k \in \mathcal{S}} \left(\frac{(fg)(\mathbf{P}_k)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)} \cdot \prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (X_i - a'_i) \right) \\
&= \sum_{\mathbf{P}_k \in \mathcal{S}} \left((fg)(\mathbf{P}_k) \cdot \frac{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (X_i - a'_i)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)} \right) \\
&= \sum_{\mathbf{P}_k \in \mathcal{S}} \left((fg)(\mathbf{P}_k) \cdot \prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} \left(\frac{X_i - a'_i}{a_{ki} - a'_i} \right) \right).
\end{aligned} \tag{3.2}$$

Observe que

$$\left(\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} \left(\frac{X_i - a'_i}{a_{ki} - a'_i} \right) \right) (\mathbf{P}_\ell) = \delta_{\ell k}$$

para todo $\ell = 1, \dots, m$. Assim $\tilde{r}(\mathbf{P}_k) = (fg)(\mathbf{P}_k) = r(\mathbf{P}_k)$ para todo $k = 1, \dots, m$. Observe ainda que, para todo $i = 1, \dots, n$ o polinômio

$$\prod_{a'_i \in S_i \setminus \{a_{ki}\}} \left(\frac{X_i - a'_i}{a_{ki} - a'_i} \right)$$

tem grau $d_i - 1$, para todo $k = 1, \dots, m$. Assim, o polinômio

$$\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} \left(\frac{X_i - a'_i}{a_{ki} - a'_i} \right)$$

tem grau $\sum_{i=1}^n (d_i - 1)$ e seus monômios estão em $\Delta(I)$, para todo $k = 1, \dots, m$. De $\tilde{r} - r \in I$

vem que $\tilde{r} = r$. Como $\text{grau}(r) < \sum_{i=1}^n (d_i - 1)$ temos que ter o coeficiente do termo de grau

$\sum_{i=1}^n (d_i - 1)$ do segundo membro da Equação (3.2) igual a zero, ou seja,

$$\sum_{\mathbf{P}_k \in \mathcal{S}} \frac{(fg)(\mathbf{P}_k)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)} = 0.$$

Daí vem que

$$\begin{aligned}
0 &= \sum_{\mathbf{P}_k \in \mathcal{S}} \frac{(fg)(\mathbf{P}_k)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)} \\
&= \sum_{\mathbf{P}_k \in \mathcal{S}} \frac{f(\mathbf{P}_k) \cdot g(\mathbf{P}_k)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)} \\
&= \sum_{\mathbf{P}_k \in \mathcal{S}} \left(f(\mathbf{P}_k) \cdot \frac{g(\mathbf{P}_k)}{\prod_{i=1}^n \prod_{a'_i \in S_i \setminus \{a_{ki}\}} (a_{ki} - a'_i)} \right) \tag{3.3} \\
&= \sum_{\mathbf{P}_k \in \mathcal{S}} f(\mathbf{P}_k) \cdot \text{Res}_{\mathbf{P}_k}(g + I) \\
&= \langle (f(\mathbf{P}_1), \dots, f(\mathbf{P}_m)), (\text{Res}_{\mathbf{P}_1}(g + I), \dots, \text{Res}_{\mathbf{P}_m}(g + I)) \rangle \\
&= \langle \phi(f + I), \text{Res}_{\mathcal{S}}(g + I) \rangle.
\end{aligned}$$

Note que na Equação (3.3), o termo à esquerda do produto interno é um elemento arbitrário de $\mathcal{C}(d)$, enquanto que o termo à direita do produto interno é um elemento arbitrário de $\text{Res}_{\mathcal{S}}(L_{d'})$. Isso mostra que

$$\text{Res}_{\mathcal{S}}(L_{d'}) \subseteq \mathcal{C}^\perp(d).$$

Agora,

$$\begin{aligned}
\dim(\text{Res}_{\mathcal{S}}(L_{d'})) &= \dim(\mathcal{C}(d')) \\
&= \dim(\mathcal{C}^\perp(d)),
\end{aligned}$$

em que a última igualdade é verdadeira pelo Lema 3.2.9. Portanto, segue que

$$\mathcal{C}^\perp(d) = \text{Res}_{\mathcal{S}}(L_{d'}),$$

em que $d' = \sum_{i=1}^n (d_i - 1) - d - 1$, como desejávamos. ■

Corolário 3.3.9. *Uma base para o dual de $\mathcal{C}(d)$ é*

$$\{\text{Res}_{\mathcal{S}}(M + I) \mid M \in \Delta(I)_{d'}\}.$$

Demonstração. É uma consequência do Teorema 3.3.8 e da Proposição 3.2.8. ■

Exemplo 3.3.10. *Se considerarmos o Exemplo 3.2.4, segue que:*

(i) Para $d = 0$, temos $d' = 1$ e uma base para $\mathcal{C}^\perp(d)$ é

$$\{(1, 1, 1, 1), (\alpha, \beta, \alpha, \beta), (0, 0, 1, 1)\};$$

(ii) Para $d = 1$, temos $d' = 0$ e uma base para $\mathcal{C}^\perp(d)$ é

$$\{(1, 1, 1, 1)\};$$

(iii) Para $d \geq 2$, temos $d' < 0$ e uma base para $\mathcal{C}^\perp(d)$ é

$$\{(0, 0, 0, 0)\}.$$

De fato, já sabemos que $\Delta(I) = \{1, Y, X, XY\}$. Logo:

(i) Para $d = 0$, temos $d' = \sum_{i=1}^2 (d_i - 1) - 1$. Daí, $d' = 1$, pois $d_1 = 2$ e $d_2 = 2$. Assim,

$$\Delta(I)_{d'} = \{1, Y, X\},$$

e

$$\begin{aligned} \text{Res}_{\mathcal{S}}(1 + I) &= \left(\frac{1}{(0-1)(\alpha-\beta)}, \frac{1}{(0-1)(\beta-\alpha)}, \right. \\ &\quad \left. \frac{1}{(1-0)(\alpha-\beta)}, \frac{1}{(1-0)(\beta-\alpha)} \right) \\ &= \left(\frac{1}{1 \cdot 1}, \frac{1}{1 \cdot 1}, \frac{1}{1 \cdot 1}, \frac{1}{1 \cdot 1} \right) \\ &= (1, 1, 1, 1), \end{aligned}$$

e

$$\begin{aligned} \text{Res}_{\mathcal{S}}(Y + I) &= \left(\frac{\alpha}{(0-1)(\alpha-\beta)}, \frac{\beta}{(0-1)(\beta-\alpha)}, \right. \\ &\quad \left. \frac{\alpha}{(1-0)(\alpha-\beta)}, \frac{\beta}{(1-0)(\beta-\alpha)} \right) \\ &= \left(\frac{\alpha}{1 \cdot 1}, \frac{\beta}{1 \cdot 1}, \frac{\alpha}{1 \cdot 1}, \frac{\beta}{1 \cdot 1} \right) \\ &= (\alpha, \beta, \alpha, \beta), \end{aligned}$$

e

$$\begin{aligned} \text{Res}_{\mathcal{S}}(X + I) &= \left(\frac{0}{(0-1)(\alpha-\beta)}, \frac{0}{(0-1)(\beta-\alpha)}, \right. \\ &\quad \left. \frac{1}{(1-0)(\alpha-\beta)}, \frac{1}{(1-0)(\beta-\alpha)} \right) \\ &= \left(\frac{0}{1 \cdot 1}, \frac{0}{1 \cdot 1}, \frac{1}{1 \cdot 1}, \frac{1}{1 \cdot 1} \right) \\ &= (0, 0, 1, 1). \end{aligned}$$

Portanto, pelo Corolário 3.3.9, o conjunto

$$\{(1, 1, 1, 1), (\alpha, \beta, \alpha, \beta), (0, 0, 1, 1)\}$$

é uma base para $\mathcal{C}^\perp(d)$.

(ii) Para $d = 1$, temos $d' = \sum_{i=1}^2 (d_i - 1) - 2$. Daí, $d' = 0$, pois $d_1 = 2$ e $d_2 = 2$. Assim,

$$\Delta(I)_{d'} = \{1\},$$

e

$$\begin{aligned} \text{Res}_S(1 + I) &= \left(\frac{1}{(0-1)(\alpha-\beta)}, \frac{1}{(0-1)(\beta-\alpha)}, \right. \\ &\quad \left. \frac{1}{(1-0)(\alpha-\beta)}, \frac{1}{(1-0)(\beta-\alpha)} \right) \\ &= \left(\frac{1}{1 \cdot 1}, \frac{1}{1 \cdot 1}, \frac{1}{1 \cdot 1}, \frac{1}{1 \cdot 1} \right) \\ &= (1, 1, 1, 1). \end{aligned}$$

Portanto, pelo Corolário 3.3.9, o conjunto

$$\{(1, 1, 1, 1)\}$$

é uma base para $\mathcal{C}^\perp(d)$.

(iii) Para $d \geq 2$, temos $d' \leq \sum_{i=1}^2 (d_i - 1) - 3$. Daí, $d' < 0$, pois $d_1 = 2$ e $d_2 = 2$. Sabemos que

$$\dim(\mathcal{C}(d)) + \dim(\mathcal{C}^\perp(d)) = 4,$$

e como $\dim(\mathcal{C}(d)) = 4$, para todo $d \geq 2$, segue que $\dim(\mathcal{C}^\perp(d)) = 0$. Ou seja,

$$\mathcal{C}^\perp(d) = \{(0, 0, 0, 0)\}.$$

Portanto, o conjunto

$$\{(0, 0, 0, 0)\}$$

é uma base para $\mathcal{C}^\perp(d)$.

Conclusão

Como pudemos observar ao longo desta dissertação e dos exemplos apresentados, a noção de Pegada desempenha um papel fundamental na compreensão e na otimização das ferramentas dos Códigos Afins. Seu uso permite reduzir significativamente o conjunto de busca, facilitando, por exemplo, a determinação de uma base para um código. Além disso, a Pegada proporciona uma abordagem mais eficiente para os cálculos necessários, eliminando redundâncias e tornando as operações mais diretas e organizadas. Esse aspecto é particularmente vantajoso ao lidarmos com grandes conjuntos de dados ou quando buscamos otimizar algoritmos computacionais aplicados à codificação.

Já o Lema 3.2.9 nos traz um resultado interessante, pois, de maneira trivial, temos a relação

$$\dim(\mathcal{C}(d)) + \dim(\mathcal{C}^\perp(d)) = d_1 \cdots d_n.$$

No entanto, o que torna esse resultado peculiar é que estamos lidando com dois códigos aparentemente distintos, que, quando considerados juntos, possuem a mesma dimensão do espaço total. Em outras palavras, verificamos que

$$\dim(\mathcal{C}(d)) + \dim(\mathcal{C}(d')) = d_1 \cdots d_n.$$

Diante dessa observação, surge naturalmente a seguinte questão: será que o dual de $\mathcal{C}(d)$ coincide com $\mathcal{C}(d')$, ou seja, $\mathcal{C}^\perp(d) = \mathcal{C}(d')$?

Intuitivamente, essa igualdade poderia parecer plausível à primeira vista, mas, ao analisarmos mais a fundo, verificamos que ela não se verifica de forma absoluta. O motivo principal para isso está na estrutura das funções envolvidas. Enquanto a função de avaliação ϕ mantém suas entradas multiplicadas pela constante 1, a função resíduo Res_S pode envolver multiplicações por constantes diferentes de 1, alterando significativamente a estrutura do código. Essa diferença pode ser observada mais formalmente através do Teorema 3.3.8.

Uma decorrência imediata desse fato revela uma limitação estrutural dos Códigos Afins: seu dual, em geral, não pertence à mesma classe. Ou seja, o dual de um Código Afim não é necessariamente um Código Afim. Isso contrasta com outras classes de códigos corretores de erro, onde frequentemente o dual mantém a mesma estrutura.

Além disso, vale ressaltar que essa característica não apenas afeta a interpretação teórica dos códigos, mas também influencia diretamente a maneira como eles são utilizados em aplicações práticas. Em diversas situações, a dualidade de um código é explorada para otimizar processos de decodificação e melhorar a eficiência da transmissão de informações.

No entanto, no caso dos Códigos Afins, essa abordagem exige um cuidado adicional, pois a estrutura do dual pode não preservar todas as propriedades desejadas.

Esse comportamento nos leva a uma mudança de paradigma: ao considerarmos o dual de um Código Afim, entramos no contexto dos Códigos Cartesianos, onde tanto o conjunto $\mathcal{S}$ quanto a função ϕ sofrem modificações. Isso reforça a ideia de que os Códigos Afins constituem um caso particular dentro da classe mais geral dos Códigos Cartesianos.

Esse resultado abre espaço para investigações futuras. Uma possível linha de pesquisa seria a busca por condições que garantam que o dual de um código permaneça na mesma classe desse código. Poderíamos, por exemplo, investigar quais características do conjunto $\mathcal{S}$ ou da função resíduo poderiam ser ajustadas para manter essa propriedade. No entanto, seguir por esse caminho exigiria o desenvolvimento de novos resultados teóricos, que poderiam modificar a abordagem estabelecida nesta dissertação e até mesmo tornar algumas das conclusões aqui apresentadas obsoletas ou insuficientes.

Referências

- BECKER, T.; WEISPFENNING, V. *Gröbner bases: a computational approach to commutative algebra*. 1st. ed. [S.l.]: Springer-Verlag New York, 1993. (Graduate Texts in Mathematics). DOI: <https://doi.org/10.1007/978-1-4612-0913-3>.
- CARVALHO, C. F. de. *Applications of results from commutative algebra to the study of certain evaluation codes*. 2017. CIMPA School on Algebraic Methods in Coding Theory. Notas de aula.
- COX, D. A.; LITTLE, J.; O'SHEA, D. *Ideals, Varieties, and Algorithms*. 4th. ed. [S.l.]: Springer Cham, 2015. (Undergraduate Texts in Mathematics). DOI: <https://doi.org/10.1007/978-3-319-16721-3>.
- GOLAY, M. J. E. Notes on digital coding. *Proceedings of the IRE*, v. 37, n. 6, p. 657 – 657, 1949. DOI: <https://doi.org/10.1109/JRPROC.1949.233620>.
- HAMMING, R. W. Error detecting and error correcting codes. *The Bell System Technical Journal*, v. 29, n. 2, p. 147 – 160, 1950. DOI: <https://doi.org/10.1002/j.1538-7305.1950.tb00463.x>.
- HEFEZ, A.; VILLELA, M. L. T. *Códigos Corretores de Erros*. 2nd. ed. [S.l.]: Associação Instituto Nacional de Matemática Pura e Aplicada, 2017. (Coleção Matemática e Aplicações).
- LOPEZ, H. H.; MANGANIELLO, F.; MATTHEWS, G. L. Affine cartesian codes with complementary duals. *Finite Fields and Their Applications*, v. 57, p. 13 – 28, 2019. DOI: <https://doi.org/10.1016/j.ffa.2019.01.004>.
- LOPEZ, H. H.; MATTHEWS, G. L.; SOPRUNOV, I. Monomial-cartesian codes and their duals, with applications to lcd codes, quantum codes, and locally recoverable codes. *Designs, Codes and Cryptography*, v. 88, p. 1673 – 1685, 2020. DOI: <https://doi.org/10.1007/s10623-020-00726-x>.
- LOPEZ, H. H.; RENTERIA-MARQUEZ, C.; VILLARREAL, R. H. Affine cartesian codes. *Designs, Codes and Cryptography*, v. 71, n. 1, p. 5 – 19, 2012. DOI: <https://doi.org/10.1007/s10623-012-9714-2>.
- MACWILLIAMS, F.; SLOANE, N. *The Theory of Error-Correcting Codes*. 1st. ed. [S.l.]: North Holland Publishing Company, 1977. (North-Holland Mathematical Library 16).
- SANTOS, J. P. de O. *Introdução à Teoria dos Números*. 4th. ed. [S.l.]: IMPA, 2024. (Coleção Matemática Universitária).
- SHANNON, C. E. A mathematical theory of communication. *The Bell System Technical Journal*, v. 27, n. 3, p. 379 – 423, 1948. DOI: <https://doi.org/10.1002/j.1538-7305.1948.tb01338.x>.

Índice Remissivo

A		I	
Algoritmo de Buchberger	38	Ideal de uma variedade afim	44
		Inequação de Singleton	64
B		M	
Base de Gröbner	32	Monômio	29
		líder	30
C		O	
Característica de um corpo	52	Ordem monomial	29
Coeficiente líder	30	lexicográfica	29
Comprimento de um código	64	lexicográfica graduada	30
Crítério de Buchberger	35	lexicográfica graduada inversa	30
Código		P	
afim	66	Pegadas	40
de Reed-Muller	69		
de variedade afim	66	R	
linear	61	Resíduo de uma classe de polinômios	78
Código auto-ortogonal e auto-dual	77	S	
Código com dual complementar	77	S-polinômio	34
D		T	
Dimensão de um código	64	Termo	29
Distância		líder	30
de Hamming	62	V	
mínima de um código	63	Variedade afim	44
Divisão polinomial	30		
Dual de um código	77		
H			
Homomorfismo entre corpos	49		