Pedro Augusto Diniz Santos

Códigos cartesianos afins com dual complementar

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2023

Pedro Augusto Diniz Santos

Códigos cartesianos afins com dual complementar

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

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

Orientador: Prof. Dr. Cícero Fernandes de Carvalho.

UBERLÂNDIA - MG
2023

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

S237c
2024

Santos, Pedro Augusto Diniz, 1999-
Códigos cartesianos afins com dual complementar [recurso eletrônico] / Pedro Augusto Diniz Santos. - 2024.

Orientador: Cícero Fernandes de Carvalho.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Programa de Programa de Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2024.5023
Inclui bibliografia.
Inclui ilustrações.

1. Matemática. I. Carvalho, Cícero Fernandes de, 1960-, (Orient.). II. Universidade Federal de Uberlândia. Programa de Programa de Pós-graduação em Matemática. III. Título.

CDU: 51

André Carlos Francisco
Bibliotecário Documentalista - CRB-6/3408

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 160 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4209/4154 - www.posgrad.famat.ufu.br - pgmat@famat.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, 114, PPGMAT				
Data:	31 de janeiro de 2024	Hora de início:	10:00	Hora de encerramento:	11:30
Matrícula do Discente:	12212MAT009				
Nome do Discente:	Pedro Augusto Diniz Santos				
Título do Trabalho:	Códigos cartesianos afins com dual complementar				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Edital Universal 001/2021 FAPEMIG proc. APQ-00864-21.				

Reuniu-se na Sala 1F 119 (Sala Multiuso da Faculdade de Matemática) - Bloco 1F (Campus Santa Mônica) da Universidade Federal de Uberlândia e também videoconferência, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Pietro Speziali - Universidade Estadual de Campinas – UNICAMP; Victor Gonzalo Lopez Neumann - FAMAT/UFU e Cícero Fernandes de Carvalho - FAMAT/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 o 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 **Pietro Speziali**, **Usuário Externo**, em 31/01/2024, às 11:39, 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 31/01/2024, às 11:58, 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 **Cícero Fernandes de Carvalho**, **Professor(a) do Magistério Superior**, em 31/01/2024, às 12:51, 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 **5137763** e o código CRC **7F865602**.

Referência: Processo nº 23117.006451/2024-24 SEI nº 5137763

ALUNO(A): Pedro Augusto Diniz Santos.

NÚMERO DE MATRÍCULA: 12212MAT009.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Teoria de Códigos.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Códigos cartesianos afins com dual complementar.

ORIENTADOR(A): Prof(a). Dr(a). Cicero Fernandes de Carvalho.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 31 de Janeiro de 2024, às 11h30min, pela seguinte Banca Examinadora:

NOME	**ASSINATURA**
Prof(a). Dr(a). Cícero Fernandes de Carvalho. UFU - Universidade Federal de Uberlândia	_____
Prof(a). Dr(a). Pietro Speziali UNICAMP - Universidade Estadual de Campinas	_____
Prof(a). Dr(a). Victor Gonzalo Lopez Neumann UFU - Universidade Federal de Uberlândia	_____

Uberlândia-MG, 31 de Janeiro de 2024.

Sumário

Dedicatória

Dedico este trabalho à minha mãe Rosângela Diniz de Araújo, à meu pai José Francisco dos Santos Filho e à minha namorada Vitória Alves Martins.

Agradecimentos

Agradeço ao meu orientador Cícero Fernandes de Carvalho pela oportunidade de realizar este trabalho, por toda a paciência e flexibilidade nesta orientação, por todos os ensinamentos, conselhos e pela amizade.

Agradeço aos meus pais José Francisco dos Santos Filho e Rosângela Diniz de Araújo por todo apoio e carinho.

Agradeço à minha namorada Vitória Alves Martins por ser tão paciente comigo durante toda jornada, por ter me dado todo amor, apoio e carinho.

Agradeço à todos os meus familiares que me ajudaram de alguma forma.

Agradeço à todos os meus amigos, em especial Alef Alves, Augusto Tannús, Fellipe Diniz, João Victor, Juan David, Laurienny Godim, Márcio Reis, Matheus Deodato, Paulo Vitor, Ricardo Arturo, Ricardo Ribeiro, Thiago Leitão, Tiago Luiz e Vinícius Colferai.

Agradeço ao grupo do café pós aula, Augusto Tannús, Fellipe Diniz, Juan David, Ricardo Arturo e Vinícius Colferai.

Agradeço à todos os meus amigos que não foram citados por esquecimento, vocês não são menos importantes em minha jornada até aqui!

Agradeço também aos professores Daniel Cariello, Geraldo Botelho, Rosana Jafelice e Victor Gonzalo, pelas ótimas aulas, por sempre compartilharem ensinamentos, conselhos e pela amizade.

Agradeço à FAPEMIG pelo auxílio financeiro durante o mestrado.

Agradeço todos aqueles que me ajudaram de forma direta ou indiretamente em minha formação acadêmica.

Deixo aqui o meu agradecimento à todos!

SANTOS, P. A. D. *Códigos cartesianos afins com dual complementar.* 2024. (46 pág) Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho realizamos o estudo de Códigos Lineares Cartesianos Afins Generalizados com Complementar Dual, para simplificar Código LCD. Introduzimos os códigos cartesianos afins, códigos do tipo Reed-Muller, códigos do tipo Reed-Solomon e sua generalização. Utilizando relações entre variedades afins e a pegada de um ideal, foi possível determinar os parâmetros de um código: dimensão, distância mínima e comprimento. Por fim, estudamos condições para determinar se um código cartesiano tem a propriedade LCD.

Palavras-chave: Códigos Cartesianos, Códigos LCD, Pegada e Bases de Gröbner.

SANTOS, P. A. D. *Códigos cartesianos afins com dual complementar.* 2024. (46 pág) Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Abstract

In this work we carry out the study of Generalized Affine Cartesian Linear Codes with Complementary Dual. We introduce affine Cartesian codes, Reed-Muller codes, Reed-Solomon codes and their generalization. Using relationships between affine varieties and the footprint of an ideal, it was possible to determine the parameters of a code: dimension, minimum distance and length. Finally, we study conditions to determine whether a Cartesian code has the LCD property.

Keywords: Cartesian Codes, LCD Codes, Footprint and Gröbner Bases.

Introdução

O objeto principal deste trabalho são códigos lineares afins com dual complementar, para simplificar código LCD, uma propriedade introduzida por Massey em 1992 em [11]. Um código LCD é um código linear que possui apenas a palavra zero em comum com o seu dual. Lembrando que um código linear C é um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q^n$, onde $\mathbb{F}_q$ é um corpo finito. Dado tal código C, seu dual é $C^\perp := \{w \in \mathbb{F}_q^n \mid w \cdot c = 0 \text{ para todo } c \in C\}$.

Este trabalho está divido em quatro capítulos. No primeiro capítulo, apresentaremos alguns resultados e conceitos sobre Corpos Finitos, que serão essenciais para o decorrer desta dissertação.

Na segundo capítulo são introduzidos os conceitos de ordem monomial, o algoritmo da divisão para polinômios em várias variáveis, bases de Gröbner, pegada de um ideal, variedades afins e a relação entre eles.

No terceiro capítulo, é feito um estudo sobre códigos lineares apresentando resultados básicos de códigos, além de alguns exemplos de códigos. No decorrer deste capitulo introduziremos os códigos cartesianos afins e códigos cartesianos afins generalizados, que são construídos a partir da avaliação de polinômios em várias variáveis. Apresentaremos alguns resultados que envolvem esses tipos de códigos.

No último capítulo, é introduzido o conceito principal da dissertação, que são os códigos LCD, onde é apresentada uma caracterização para códigos LCD. Neste capítulo apresentaremos alguns resultados feitos em [10] envolvendo este conceito para alguns códigos de avaliação, especificamente, códigos de Reed-Solomon generalizados apresentando condições para que esse tipo de códigos tenham a propriedade LCD.

Pedro Augusto Diniz Santos
Uberlândia-MG, 31 de Janeiro de 2024.

Capítulo 1

Corpos Finitos

Neste primeiro capítulo introduziremos conceitos necessários ao desenvolvimento deste trabalho.

1.1 Característica de um Corpo

Definição 1.1. *Sejam K_1 e K_2 dois corpos. Uma função $f : K_1 \to K_2$ será chamada homomorfismo se, para todos os elementos a e b em K_1, vale que*

- $f(a+b) = f(a) + f(b)$,
- $f(a \cdot b) = f(a) \cdot f(b)$,
- $f(1) = 1$.

*Um homomorfismo bijetor de corpos será chamado de **isomorfismo**. Dois corpos serão ditos **isomorfos** se existir um isomorfismo entre eles.*

Proposição 1.2. *Seja $f : A \to B$ um homomorfismo e sejam $a_1, a_2 \in A$. Temos:*

1. $f(0) = 0$,
2. $f(-a_1) = -f(a_1)$,
3. $f(a_1 - a_2) = f(a_1) - f(a_2)$,
4. $f(a_1^{-1}) = f(a_1)^{-1}$ *para todo a invertível,*
5. *Se f é bijetora, então f^{-1} é homomorfismo.*
6. *f é injetora e $f(A)$ é um subcorpo de B.*

Demonstração. Veja em [8, Proposição 1, Pag 64]. □

Vamos denotar por $\mathbb{N}$ o conjunto dos inteiros positivos.

Definição 1.3. *Seja K um corpo finito. Seja Λ_K o conjunto*

$$\Lambda_K = \{n \in \mathbb{N}; n1 = 0\} \subseteq \mathbb{N}.$$

Proposição 1.4. *O conjunto Λ_K é não vazio.*

Demonstração. Pelo fato de K ser finito, temos que existem dois inteiros $n_1 < n_2$ tais que $n_1 1 = n_2 1$. Logo, $(n_1 - n_2)1 = 0$ com $n_2 - n_1 > 0$ e, portanto, $\Lambda_K \neq \emptyset$. □

Definição 1.5. *Define-se a característica de um corpo finito K como sendo o inteiro positivo*

$$\text{car}(K) = \min \Lambda_K = \min\{n \in \mathbb{N}; n1 = 0\}.$$

Se um corpo F é subcorpo de um corpo K, então $\text{car}(K) = \text{car}(F)$, pois $\Lambda_F = \Lambda_K$.

Proposição 1.6. *Seja K um corpo finito, então $\text{car}(K)$ é um número primo.*

Demonstração. Suponha que $\text{car}(K)$ não seja primo. Seja $m = \text{car}(K)$, então $m = m_1 \cdot m_2$, com $m_1, m_2 \in \mathbb{N}$ e $1 < m_1, m_2 < m$. Portanto,

$$0 = m1 = (m_1 \cdot m_2)1 = m_1(m_2 \cdot 1) = (m_1 \cdot 1)(m_2 \cdot 1).$$

Como K é corpo, e todo corpo é domínio de integridade, temos $m_1 \cdot 1 = 0$ ou $m_2 \cdot 1 = 0$, contradição, pois $m_1, m_2 < m$. Logo, m é primo. □

Proposição 1.7. *Seja K um corpo finito com $\text{car}(K) = p$. Se $ma = 0$ com $m \in \mathbb{Z}$ e $a \in K$, então m é múltiplo de p ou $a = 0$.*

Demonstração. Se $ma = 0$, então $(m1) \cdot a = 0$. Logo, como K é corpo, temos $m1 = 0$ ou $a = 0$. Portanto, resta mostrar que, se $m1 = 0$, então m é múltiplo de p . Suponha $m1 = 0$, pelo algoritmo da divisão, temos $m = \lambda p + r$, com $0 \leq r < p$. Portanto

$$0 = m1 = (\lambda p + r)1 = \lambda(p1) + r1 = \lambda 0 + r1 = r1,$$

e como p é o menor inteiro positivo tal que $p1 = 0$ temos $r = 0$. Assim m é múltiplo de p. □

Teorema 1.8. *Seja K um corpo finito com $\text{car}(K) = p$. Então, K contém um subcorpo isomorfo a $\mathbb{Z}_p$.*

Demonstração. Considere a seguinte aplicação

$$\begin{aligned} \varphi\colon \mathbb{Z}_p &\to K \\ [n] &\mapsto n1. \end{aligned}$$

Primeiro mostraremos que essa aplicação está bem definida. De fato, se $[m] = [n]$ com $m, n \in \mathbb{Z}$, então existe $\lambda \in \mathbb{Z}$ tal que $n = m + \lambda p$. Portanto, $n1 = (m + \lambda p)1 = m1 + \lambda(p1) = m1 + \lambda 0 = m1 + 0 = m1$.

Vejamos que φ é homomorfismo injetor. Temos que $\varphi([n]+[m]) = ([n]+[m])1 = [n]+[m] = \varphi([n]) + \varphi([m])$ e analogamente se vê que $\varphi([n][m]) = \varphi([n])\varphi([m])$, além disso $\varphi([1]) = 1$. Isso mostra que φ é homomorfismo. Se $\varphi([n]) = 0$ então $n1 = 0$ e da Proposição 1.7 temos que n é múltiplo de p, logo $[n] = [0]$. Assim φ é um homomorfismo injetor, e temos que $\varphi(\mathbb{Z}_p)$ é um subcorpo de K isomorfo a $\mathbb{Z}_p$. □

Corolário 1.9. *Seja K um corpo finito com $\text{car}(K) = p$. Então K tem p^n elementos para algum número inteiro positivo n.*

Demonstração. Na notação do teorema acima, identificando $\varphi(\mathbb{Z}_p)$ com $\mathbb{Z}_p$ podemos considerar $\mathbb{Z}_p \subset K$, e temos que K é espaço vetorial sobre $\mathbb{Z}_p$. Como K é finito, segue que K tem dimensão finita sobre $\mathbb{Z}_p$. Seja $\alpha_1, \ldots, \alpha_n$ uma base de K sobre $\mathbb{Z}_p$. Então todo elemento de K é escrito de maneira única na forma

$$\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n,$$

com $\lambda_i \in \mathbb{Z}_p$, $i = 1, \ldots, n$. Ao contar os elementos, obtemos que $|K| = p^n$. □

Proposição 1.10. *Seja K um corpo finito com $\mathrm{car}(K) = p$ e seja $q = p^r$, para algum $r \in \mathbb{N}$. Se $a_1, \ldots, a_n \in K$, temos*

$$(a_1 + \cdots + a_n)^q = a_1^q + \cdots + a_n^q.$$

Demonstração. Faremos a prova deste resultado por indução no número de elementos n e também no expoente r.

O caso $n = 1$ e $r = 1$ são triviais. Assim fixaremos $r = 1$ e faremos a indução sobre n. Suponha que o resultado é válido até k e mostraremos o caso $k + 1$.

$$(a_1 + \cdots + a_{k+1})^p = ((a_1 + \cdots + a_k) + a_{k+1})^p.$$

Pela expansão do binômio de Newton temos

$$((a_1 + \cdots + a_k) + a_{k+1})^p = \sum_{i=0}^{p} \binom{p}{i} (a_1 + \cdots + a_k)^i a_{k+1}^{p-i}$$

Observe que $p|\binom{p}{i}$ para todo $i \in \{1, \ldots, p-1\}$ e que $\binom{p}{0} = \binom{p}{p} = 1$. Logo

$$(a_1 + \cdots + a_{k+1})^p = (a_1 + \cdots + a_k)^p + a_{k+1}^p.$$

Usando agora a hipótese de indução temos

$$(a_1 + \cdots + a_k)^p = a_1^p + \cdots + a_k^p.$$

Logo,

$$(a_1 + \cdots + a_{k+1})^p = a_1^p + \cdots + a_k^p + a_{k+1}^p.$$

Para finalizar, fixaremos n e faremos uma indução sobre r. Note que o caso $r = 1$ já foi provado e suponha válido até k e mostraremos que é válido para $k + 1$. Sabemos que $p^{k+1} = p^k p$, logo

$$(a_1 + \cdots + a_n)^{p^{k+1}} = ((a_1 + \cdots + a_n)^{p^k})^p.$$

Pela hipótese de indução temos que

$$(a_1 + \cdots + a_n)^{p^{k+1}} = (a_1^{p^k} + \cdots + a_n^{p^k})^p = (a_1^{p^{k+1}} + \cdots + a_n^{p^{k+1}}).$$

□

Observação 1.11. *Seja K um corpo finito de característica p e seja q uma potência de p. Temos que se $P(X) = a_0 + a_1X + \cdots + a_nX^n \in K[X]$, então $P(X)^q = a_0^q + a_1^q X^q + \cdots + a_n^q X^{nq}$.*

Corolário 1.12. *Seja K um corpo finito de característica p. Se $q = p^r$ para algum inteiro positivo r, então f_q é um isomorfismo de corpos, onde*

$$\begin{aligned} f_q \colon K &\to K \\ x &\mapsto x^q. \end{aligned}$$

Demonstração. Observe que

$$f_q(ab) = (ab)^q = a^q b^q = f_q(a) f_q(b),$$

além disso, pela Proposição 1.10, tem-se

$$f_q(a + b) = (a + b)^q = a^q + b^q = f_q(a) + f_q(b).$$

Temos $f_q(1) = 1^q = 1$, portanto f_q é um homomorfismo.

Pela Proposição 1.2(6), se f_q for bijetora, então que é isomorfismo.

Mostremos que f_q é injetora. Sejam $a, b \in K$ tais que $f_q(a) = f_q(b)$, então $0 = f_q(a) - f_q(b) = f_q(a - b) = (a - b)^q$ logo $a = b$ e por consequência f_q é injetora. Como K é finito e f_q é injetora, por consequência é sobrejetora. Portanto f_q é isomorfismo.

□

Corolário 1.13. *Seja F um corpo de característica $p > 0$ e seja q uma potência inteira de p. Então o conjunto $K = \{\alpha \in F \mid \alpha^q - \alpha = 0\}$ é um subcorpo de F.*

Demonstração. Basta mostrar que se $\alpha, \beta \in K$, onde $\beta \neq 0$, então $\alpha - \beta, \frac{\alpha}{\beta} \in K$. Como $\alpha^q - \alpha = 0$ e $\beta^q - \beta = 0$, segue que $\alpha^q - \alpha - (\beta^q - \beta) = 0$ e pela Proposição 1.10, temos que $(\alpha - \beta)^q - (\alpha - \beta) = 0$. Implicando que $(\alpha - \beta) \in K$.

Vamos mostrar que $\frac{\alpha}{\beta} \in K$. Dados $\alpha, \beta \in K$ e $\beta \neq 0$, sabemos que $\alpha^q = \alpha$ o que implica $\alpha^q = \alpha \cdot 1 = \alpha \cdot \frac{\beta}{\beta}$. Assim $\frac{\alpha^q}{\beta} = \frac{\alpha}{\beta}$, como $\beta^q = \beta$ segue que $\frac{\alpha^q}{\beta^q} = \frac{\alpha}{\beta}$.

Portanto, K é subcorpo de F □

Definição 1.14. *Seja K um corpo. Seja $f(X) = c_r X^r + \cdots + c_1 X + c_0 \in K[X]$. Sua derivada é o polinômio*

$$f'(X) = r c_r X^{r-1} + (r-1) c_{r-1} X^{r-2} + \cdots + c_1.$$

Não é difícil mostrar que as propriedades da derivada convencional são satisfeitas, deixaremos a cargo do leitor.

Proposição 1.15. *Seja K um corpo finito de característica p e seja $P(X) \in K[X]$. Temos que $P'(X) = 0$ se , e somente se, existe $Q(X) \in K[X]$ tal que $P(X) = Q(X)^p$.*

Demonstração. ($\Rightarrow$) Seja $P(X) = a_0 + a_1 X + \cdots + a_n X^n$ tal que $P'(X) = 0$, então $i a_i = 0$ para todo $i = 1, \ldots, n$. Segue da Proposição 1.7 que i é múltiplo de p sempre que $a_i \neq 0$, isto é

$$P(X) = a_0 + a_p X^P + a_{2p} X^{2p} + \cdots + a_{sp} X^{sp}.$$

Pelo Corolário 1.12, para todo $i = 0, \ldots, s$ existe $b_i \in K$ tal que $b_i^p = a_{ip}$. Assim basta tomar $Q(X) := b_0 + b_1 X + b_2 X^2 + \cdots + b_s X^s$.

($\Leftarrow$) Por hipótese temos que $P(X) = Q(X)^p$ e aplicando a regra da cadeia temos $P'(X) = pQ(X)^{p-1} \cdot Q'(X) = 0$. □

Proposição 1.16. *Seja K um corpo finito de característica p e seja $q = p^r$, para algum r inteiro positivo. Então o polinômio $f(X) = X^q - X$ não possui fatores irredutíveis múltiplos em $K[X]$.*

Demonstração. Suponha por absurdo que exista um fator irredutível múltiplo $h(X)$ na fatoração de $f(X)$. Então $\deg(h(X)) \geq 1$ e $f(X) = g(X)h(X)^2$ para algum $g(X) \in K[X]$. Temos que $f'(X) = g'(X)h(X)^2 + g(X)2h(X)h'(X)$, logo $h(X) \mid f'(X)$. No entanto $f'(X) = qX^{q-1} - 1 = -1$. □

Lema 1.17. *Seja K um corpo finito com q elementos. Então, para todo $\alpha \in K^*$, sendo K^* o conjunto de todos elementos invertíveis de K, temos $\alpha^{q-1} - 1 = 0$.*

Demonstração. Seja $\alpha \in K^*$. Considere a seguinte aplicação

$$\begin{aligned} \varphi_a \colon K^* &\to K^* \\ a &\mapsto \alpha a. \end{aligned}$$

Temos que φ_a é injetora e, portanto, é bijetora, pois K^* é finito. Se $K^* = \{a_1, \ldots, a_{q-1}\}$, então

$$\{\alpha a_1, \ldots, \alpha a_{q-1}\} = \{a_1, \ldots, a_{q-1}\},$$

$$\alpha a_1 \cdots \alpha a_{q-1} = a_1 \cdots a_{q-1},$$

$$\alpha^{q-1} = 1.$$

□

Corolário 1.18. *Seja K um corpo finito com q elementos. Então temos $\alpha^{q^i} = \alpha$, para todo $\alpha \in K$ e para todo i inteiro positivo.*

Demonstração. O resultado segue do Lema 1.17. □

Corolário 1.19. *Seja K um corpo finito de característica p com q elementos e seja F uma extensão de K. Então os elementos de K são os elementos de F que são raízes de $X^q - X = 0$. Além disso, os elementos do subcorpo $\mathbb{Z}_p$ de F são as raízes do polinômio $X^p - X = 0$.*

Demonstração. Segue do Corolário 1.18 que os elementos de K são raízes de $X^q - X = 0$.
Sabemos de [6, Corolario. III.1.7] que esse polinômio tem no máximo q raízes distintas, pois tem grau q.
Portanto, suas raízes são todos os elementos de K. De maneira análoga, segue que todos os elementos de $\mathbb{Z}_p$ são as raízes do polinômio $X^p - X = 0$. □

Definição 1.20. *Seja K um corpo com q elementos. A ordem de $\alpha \in K^*$ é definida pelo inteiro positivo*

$$\text{ord}(\alpha) = \min\{n \in \mathbb{N} \mid \alpha^n = 1\}.$$

Observe que pelo Lema 1.17 temos que todo elemento não nulo de K tem ordem, e ela é no máximo $q - 1$.

Proposição 1.21. *Seja K com q elementos e seja $\alpha \in K^*$. Se ocorre $\alpha^m = 1$ para algum inteiro positivo m, então* $\text{ord}(\alpha) \mid m$. *Em particular,* $\text{ord}(\alpha) \mid (q-1)$.

Demonstração. Pelo algoritmo da divisão, temos $m = \text{ord}(\alpha)s + r$, com r e s inteiros não negativos e $r < \text{ord}(\alpha)$. Então

$$1 = \alpha^m = (\alpha^{\text{ord}(\alpha)}))^s \alpha^r = 1 \cdot \alpha^r,$$

e isso implica que $r = 0$ devido a minimalidade de $\text{ord}(\alpha)$. Portanto, $\text{ord}(\alpha) \mid m$.

Além disso, segue do Lema 1.17, temos $\alpha^{q-1} = 1$. Logo

$$\text{ord}(\alpha) \mid (q-1).$$

□

Proposição 1.22. *Seja K finito e sejam $\alpha, \beta \in K$ tais que $mdc(\text{ord}(\alpha), \text{ord}(\beta)) = 1$. Então* $\text{ord}(\alpha\beta) = \text{ord}(\alpha)\text{ord}(\beta)$.

Demonstração. Sejam $m = \text{ord}(\alpha)$ e $n = \text{ord}(\beta)$. Então

$$(\alpha\beta)^{mn} = (\alpha^m)^n(\beta^n)^m = 1.$$

Além disso, caso $(\alpha\beta)^t = 1$, temos

$$1 = ((\alpha\beta)^t)^m = \alpha^{tm}\beta^{tm} = 1\beta^{tm} = \beta^{tm},$$

$$1 = ((\alpha\beta)^t)^n = \alpha^{tn}\beta^{tn} = \alpha^{tn}1 = \alpha^{tn}.$$

Portanto, temos $n \mid tm$ e $m \mid tn$ pela Proposição (1.22). Logo, $m \mid t$ e $n \mid t$, pois $mdc(m, n) = 1$. Como m e n são primos entre si, temos $mn \mid t$, e isso prova que $mn = \min\{t > 0 \mid (\alpha\beta)^t = 1\}$. Finalmente, segue que $\text{ord}(\alpha\beta) = mn$. □

Proposição 1.23. *Seja K com q elementos e seja $\alpha \in K^*$ e i um número inteiro positivo. Seja $m = \text{ord}(\alpha)$, então*

$$\text{ord}(\alpha^i) = \frac{m}{\text{mdc}(m, i)}.$$

Demonstração. Seja $t = \text{ord}(\alpha^i)$, então t é o menor inteiro positivo tal que

$$(\alpha^i)^t = \alpha^{it} = 1.$$

Por outro lado temos $m \mid it$, e assim it é o menor múltiplo de m e i. Portanto $it = \text{mmc}(m, i)$, ou seja,

$$t = \frac{\text{mmc}(m,i)}{i} = \frac{m}{\text{mdc}(m,i)}.$$

□

1.2 Polinômios Irredutíveis

Proposição 1.24. *Seja K um corpo finito com q elementos e seja $f(X)$ um polinômio mônico irredutível em $K[X]$, de grau d. Considere a extensão de corpos $F = K[X]/(f(X)) \mid K$. Vamos denotar por $[g(X)]$ a classe de $g(X)$ no quociente $K[X]/(f(X))$. Temos que*

1. *O conjunto $\{1, [X], [X^2], \ldots, [X^{d-1}]\}$ formam uma base de F sobre K.*
2. *$[X]^{q^d} = [X]$ em F.*
3. *$f(X)$ divide $X^{q^d} - X$ em $K[X]$.*
4. *Os elementos $[X], [X]^q, \ldots, [X]^{q^{d-1}}$ de F são distintos e são as raízes de $f(X)$.*

Demonstração.

1. Seja $g(X) \in K[X]$, dividindo $g(X)$ por $f(X)$ encontramos $q(X), r(X) \in K[X]$ tais que $g(X) = q(X)f(X) + r(X)$, onde $r(X) = \sum_{i=0}^{d-1} a_i X^i$. Tomando as classes em ambos os lados da igualdade, temos que $\{1, [X], [X^2], \ldots, [X^{d-1}]\}$ gera F como K-espaço vetorial. Por outro lado, se $\sum_{i=0}^{d-1} a_i[X^i] = [0]$ então $\sum_{i=0}^{d-1} a_i X^i$ é um múltiplo de $f(X)$, o que só é possível se $a_i = 0$ para todo $i = 0, \ldots, d-1$. Isso mostra que $\{1, [X], [X^2], \ldots, [X^{d-1}]\}$ é uma base para F como K-espaço vetorial.

2. Note que F é um corpo finito com q^d elementos, logo, pelo Corolário 1.18, temos que $[X]^{q^d} = [X]$.

3. Segue de $[X]^{q^d} - [X] = [0]$, ou seja, $[X^{q^d} - X] = [0]$.

4. Considere o polinômio

$$g(Y) = (Y - [X])(Y - [X]^q) \cdots (Y - [X]^{q^{d-1}}) \in F[Y].$$

Temos do item (2) que

$$g(Y)^q = ((Y - [X])(Y - [X]^q) \cdots (Y - [X]^{q^{d-1}}))^q =$$
$$(Y^q - [X])(Y^q - [X]^q) \cdots (Y^q - [X]^{q^{d-1}}) = g(Y^q).$$

Assim, $g(Y^q) = g(Y)^q$ e portanto se $g(Y) = b_0 + b_1 Y + \cdots + b_{d-1}Y^{d-1} + Y^d$, temos que $b_i^q = b_i$ para todo $i = 0, 1, 2 \ldots, d-1$. Sendo assim, segue do Corolário 1.19, segue que $g(Y) \in K[Y]$.
Como $f(Y), g(Y) \in K[Y]$ possuem uma raiz comum numa extensão F de K, segue que seu máximo divisor comum em $F[Y]$ é não constante e pertence a $K[Y]$. Como $f(Y)$ é irredutível e mônico, ele coincide com o máximo divisor comum de $f(Y)$ e $g(Y)$, logo, $f(Y)$ divide $g(Y)$. Como $f(Y)$ e $g(Y)$ são polinômios mônicos do mesmo grau, eles devem ser iguais.

Sabemos do item (3) que $g(Y) = f(Y)$ divide $Y^{q^d} - Y$, que, pela Proposição 1.16 não tem fatores múltiplos em $K[Y]$, logo as raízes $[X], [X]^q, \ldots, [X]^{q^{d-1}}$ de $g(Y)$ são duas a duas distintas, provando assim este item.

□

Observação 1.25. *Note que com a proposição acima fica provado que, se* $[X] \in K[X]/f(X)$ *com* $f(X) \in K[X]$ *irredutível de grau* d*, então*

$$d = \min\{j \in \mathbb{N} \setminus \{0\} \mid [X]^{q^j} = [X]\}.$$

Proposição 1.26. *Seja* K *um corpo finito com* q *elementos e seja* n *um inteiro positivo. Então, em* $K[X]$ *vale a igualdade:*

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

sendo $G_d(X)$ *o produto de todos os polinômios mônicos irredutíveis de grau* d *em* $K[X]$ *e o produto na igualdade acima é efetuado sobre todos os inteiros positivos* d *que dividem* n*.*

Demonstração. Seja $f(X) \in K[X]$ um polinômio mônico irredutível de grau d. Como $X^{q^n} - X$ não possui fatores múltiplos pela Proposição 1.16, basta provar a seguinte afirmação:

$$f(X) \text{ divide } X^{q^n} - X \text{ se, e somente se, } d \text{ divide } n.$$

Suponhamos inicialmente que $f(X) \mid (X^{q^n} - X)$. Como $f(X) \mid (X^{q^d} - X)$ pela Proposição 1.24(3), segue que $f(X)$ divide $\text{mdc}(X^{q^n} - X, X^{q^d} - X)$. Sabe-se que $\text{mdc}(X^{q^n} - X, X^{q^d} - X) = (X^{q^e} - X)$, onde $e = \text{mdc}(n, d) \leq d$ (v. Exemplos 1 e 2 em [8, Seção 3.2]) logo $f(X) \mid (X^{q^e} - X)$. Sendo assim $[X]^{q^e} = [X]$ em $K[X]/((f(X))$, o que pela observação que segue a Proposição acima só é possível se $e \geq d$. Segue, então, que $d = e = \text{mdc}(n, d)$ e portanto, $d \mid n$. Reciprocamente, se d divide n, temos que $(X^{q^d} - X) \mid (X^{q^n} - X)$. Como $f(X) \mid (X^{q^d} - X)$ segue que $f(X) \mid (X^{q^n} - X)$. □

Corolário 1.27. *Sejam* K *um corpo finito com* q *elementos e* $I(n)$ *o número de polinômios mônicos irredutíveis de grau* n *em* $K[X]$*. Então*

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

Demonstração. Compare os graus dos polinômios em ambos os lados da igualdade da proposição acima. □

Através do corolário acima, podemos calcular recursivamente os valores de $I(n)$ num corpo finito qualquer.

Teorema 1.28. *Seja* K *um corpo finito qualquer. Então, para cada inteiro positivo* n*, existe pelo menos um polinômios irredutível de grau* n *em* $K[X]$*.*

Demonstração. Para $n = 1$, o resultado é óbvio, pois o polinômio X é irredutível. Suponhamos agora $n > 1$. Sejam $1 = d_1 < \cdots < d_s < n$, com $s \geq 1$, os divisores de n. Seja $q = |K|$ e usando duas vezes o Corolário acima, temos que

$$q^n = \sum_{d|n} dI(d) = \sum_{i=1}^{s} d_i I(d_i) + nI(n) \leq$$

$$\sum_{i=1}^{s} \left(\sum_{d|d_i} dI(d) + nI(n) \right) = \sum_{i=1}^{s} q^{d_i} + nI(n) <$$

$$\sum_{j=0}^{d_s} q^j + nI(n) = \frac{q^{d_s+1}-1}{q-1} + nI(n) < q^{d_s+1} + nI(n).$$

Portanto,

$$nI(n) > q^n - q^{d_s+1}.$$

Como d_s divide n e $d_s < n$, temos que $n = \lambda d_s$ com $\lambda > 1$. Logo, $d_s = \frac{n}{\lambda} \leq \frac{n}{2}$ e $q^{d_s+1} \leq q^{\frac{n}{2}+1}$. Consequentemente,

$$nI(n) > q^n - q^{\frac{n}{2}+1} = q^n(1 - q^{-\frac{n}{2}+1}),$$

por consequência $I(n) > 0$. □

1.3 Classificação dos Corpos Finitos

Teorema 1.29 (Existência de corpos finitos)**.** *Para todos os inteiros positivos p e n com p primo, existe um corpo com p^n elementos.*

Demonstração. Pelo Teorema 1.28, existe, para todos os inteiros positivos p e n com p primo, um polinômio irredutível $f(X) \in \mathbb{Z}_p[X]$ de grau n. Portanto, o corpo $\mathbb{Z}_p[X]/f(X)$ é um dos corpos procurados, pois tem p^n elementos. □

Teorema 1.30 (Unicidade dos corpos finitos)**.** *Dois corpos finitos com o mesmo número de elementos são isomorfos.*

Demonstração. Seja K um corpo finito com p^n elementos, logo, a característica de K é p e pelo Teorema 1.8 ele contém um subcorpo isomorfo a $\mathbb{Z}_p$. Pelo Corolário 1.19, como K é corpo finito com p^n elementos, temos que a equação $X^{p^n} - X$ tem todas as suas raízes em K e todos os elementos de K são as raízes desse polinômio.

Seja $f(X) \in \mathbb{Z}_p[X]$ um polinômio mônico irredutível de grau n, cuja existência está garantida pelo Teorema 1.28. Vamos mostrar que se L é isomorfo a $\mathbb{Z}_p[X]/(f(X))$, logo quaisquer dois corpos com p^n elementos são isomorfos.

Pela Proposição 1.24 (3), sabemos que $f(X)$ divide $X^{p^n} - X$ em $\mathbb{Z}_p[X]$, logo, existe α em K tal que $f(\alpha) = 0$. Observe que $f(X)$ é o polinômio minimal de α sobre $\mathbb{Z}_p$, logo os elementos $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ de K são linearmente independentes sobre $\mathbb{Z}_p$, pois, caso contrário, existiria um polinômio não nulo $r(X) \in \mathbb{Z}_p[X]$ de grau menor do que o grau de $f(X)$ tal que $r(\alpha) = 0$.

Pela Observação 1.25, seguiria que $\text{mdc}(f(X), r(X)) \neq 1$ e como $f(X)$ é irredutível, teríamos $f(X)|r(X)$, o que é impossível, pois $\deg(r(X)) < n$. Logo, tais elementos formam uma base de K sobre $\mathbb{Z}_p$. Sabemos também, pela Proposição 4.2(i), que $1, [X], [X]^2 \ldots [X]^{n-1}$ é uma base de $\mathbb{Z}_p[X]/f(X)$ sobre $\mathbb{Z}_p$.

Definindo

$$\begin{aligned} \sigma\colon \mathbb{Z}_p[X] &\to K \\ [a_0 + \cdots + a_{n-1}X^{n-1}] &\mapsto a_0 + \cdots + a_{n-1}\alpha^{n_1}. \end{aligned}$$

Veja que σ está bem definida, pois, se

$$[a_0 + \cdots + a_{n-1}X^{n-1}] = [b_0 + \cdots + b_{n-1}X^{n-1}],$$

para algum $g(X) \in \mathbb{Z}_p[X]$, temos que

$$(a_0 + \cdots + a_{n-1}X^{n-1}) - (b_0 + \cdots + b_{n-1}X^{n-1}) = f(X)g(X).$$

Portanto,

$$(a_0 + \cdots + a_{n-1}\alpha^{n-1}) - (b_0 + \cdots + b_{n-1}\alpha^{n-1}) = f(\alpha)g(\alpha)$$

o que prova que

$$a_0 + \cdots + a_{n-1}\alpha^{n-1} = b_0 + \cdots + b_{n-1}\alpha^{n-1}.$$

Além disso, σ é claramente sobrejetora e vale que $\sigma(a+b) = \sigma(a) + \sigma(b)$ para todos $a, b \in \mathbb{Z}_p[X]/f(X)$, ou seja, σ é aditiva. Mostremos agora que σ é multiplicativa, de fato, com $\sigma([1]) = 1$ e todo homomorfismo de corpos é injetor. Sejam $a = [a(X)]$ e $b = [b(X)]$ em $\mathbb{Z}_p[X]/f(X)$, onde $a(X)$ e $b(X)$ são polinômios em $\mathbb{Z}_p[X]$. Pelo algoritmo da divisão de polinômios, escrevemos

$$a(X)b(X) = f(X)q(X) + r(X),$$

onde $r(X)$ é zero ou é um polinômio de grau menor que n. Logo, temos que

$$[a(X)b(X)] = [r(X)] \text{ e } a(\alpha)b(\alpha) = r(\alpha),$$

o que implica que

$$\sigma(ab) = r(\alpha) = a(\alpha)b(\alpha) = \sigma(a)\sigma(b) \text{ para todos } a, b \in \mathbb{Z}_p[X]/f(X).$$

Portanto, σ é um isomorfismo.
Agora se q é uma potência de um número primo p, denotaremos doravante por $\mathbb{F}_q$ o único corpo (a menos de isomorfismo) com q elementos. □

Capítulo 2

Bases de Gröbner

2.1 Ordem Monomial e o Algoritmo da Divisão para Polinômios em Várias Variáveis

Seja K um corpo e denote por $K[\mathbf{X}]$ o anel de polinômios $K[X_1, \ldots, X_n]$. O produto $aX_1^{\alpha_1} \cdots X_n^{\alpha_n}$, onde $a \in K^*$ e $\alpha_1, \ldots, \alpha_n$ são inteiros não negativos, será chamado de **termo**, enquanto $X_1^{\alpha_1} \cdots, X_n^{\alpha_n}$ é chamado de **monômio**. O monômio $X_1^{\alpha_1} \cdots, X_n^{\alpha_n}$ em algumas vezes será denotado por $\mathbf{X}^{\alpha}$ (ou $\mathbf{X}^{\beta}$, $\mathbf{X}^{\gamma}$, etc.), onde $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ onde $\mathbb{N}_0$ é o conjunto dos inteiros não negativos.
O conjunto dos monômios de $K[\mathbf{X}]$ será denotado por $\mathcal{M}$. Dado um polinômio $f \in K[\mathbf{X}]$, dizemos que um monômio M aparece em f se o coeficiente de M é diferente de zero.

Definição 2.1. *Uma ordem monomial em $\mathcal{M}$ é uma ordem total $\preceq$ definida sobre $\mathcal{M}$ tal que*

- *Se $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3 \in \mathcal{M}$ e $\mathcal{M}_1 \preceq \mathcal{M}_2$, então $\mathcal{M}_1\mathcal{M}_3 \preceq \mathcal{M}_2\mathcal{M}_3$.*
- *Todo subconjunto não vazio de $A \subset \mathcal{M}$ possui um menor elemento.*

Alguns exemplos de ordens monomiais.

Exemplo 2.2.

- *Ordem Lexicográfica, sejam $\prod_{i=1}^n X_i^{\alpha_i}$ e $\prod_{i=1}^n X_i^{\beta_i}$ dizemos que*

$$\prod_{i=1}^n X_i^{\alpha_i} \preceq_{lex} \prod_{i=1}^n X_i^{\beta_i}$$

se existe $i \in 1, \ldots, n$ tal que $\alpha_i < \beta_i$ e $\alpha_j = \beta_j$, para todo $j < i$.

- *Ordem Lexicográfica Graduada, sejam $\prod_{i=1}^n X_i^{\alpha_i}$ e $\prod_{i=1}^n X_i^{\beta_i} \in \mathcal{M}$.*
  Dizemos que $\prod_{i=1}^n X_i^{\alpha_i} \preceq_{grlex} \prod_{i=1}^n X_i^{\beta_i}$, se

$$|\alpha| := \sum_{i=1}^n \alpha_i < |\beta| := \sum_{i=1}^n \beta_i, \text{ ou}$$
$$|\alpha| = |\beta| \text{ e } \prod_{i=1}^n X_i^{\alpha_i} \preceq_{lex} \prod_{i=1}^n X_i^{\beta_i}.$$

- *Ordem Lexicográfica Graduada Reversa, sejam $\prod_{i=1}^n X_i^{\alpha_i}$ e $\prod_{i=1}^n X_i^{\beta_i} \in \mathcal{M}$.*
  Dizemos que $\prod_{i=1}^n X_i^{\alpha_i} \preceq_{grevlex} \prod_{i=1}^n X_i^{\beta_i}$, se

$$|\alpha| = \sum_{i=1}^n \alpha_i < |\beta| = \sum_{i=1}^n \beta_i, \text{ ou}$$
$$|\alpha| = |\beta| \text{ e existe } i \in 1, \ldots, n \text{ tal que } \alpha_i > \beta_i \text{ e } \alpha_j = \beta_j \text{ para todo } j > i.$$

A seguir um exemplo de como ordenar monômios usando as ordenações acima.

Exemplo 2.3. *Considere os seguintes monômios* $X_1^5X_2X_3$ *e* $X_1^4X_2X_3^2$.
Note que $X_1^4X_2X_3^2 \preceq_{grlex} X_1^5X_2X_3$, *pois ambos os monômios tem grau total 7 e* $X_1^4X_2X_3^2 \preceq_{lex} X_1^5X_2X_3$. *Neste caso, também temos que* $X_1^4X_2X_3^2 \preceq_{grevlex} X_1^5X_2X_3$, *pois o expoente da variável* X_3 *em* $X_1^4X_2X_3^2$ *é maior que o expoente em* $X_1^5X_2X_3$.

Definição 2.4. *Sejam* $f = \sum_\alpha a_\alpha \mathbf{X}^\alpha$ *um polinômio não nulo em* $\mathbb{K}[\mathbf{X}]$ *e* $\preceq$ *uma ordem monomial.*

- *Como* f *é uma soma finita de termos um dos monômios que aparecem em* f *deve ser o maior. Esse monômio é chamado de monômio líder de* f *e será denotado por* $\mathrm{lm}(f)$.
- *O coeficiente de* $\mathrm{lm}(f)$ *é chamado de coeficiente líder de* f *e será denotado por* $\mathrm{lc}(f)$.
- *O termo líder de* f *é definido como* $\mathrm{lt}(f) := \mathrm{lc}(f) \cdot \mathrm{lm}(f)$.

A seguir apresentaremos o algoritmo da divisão em várias variáveis.

Teorema 2.5 (Algoritmo da divisão em várias variáveis)**.** *Fixe uma ordem monomial* $\preceq$ *em* $K[\mathbf{X}]$, *e seja* $F = (f_1, \ldots, f_s)$ *uma s-upla de polinômios em* $K[\mathbf{X}]$. *Então todo* $f \in K[\mathbf{X}]$ *pode ser escrito como:*

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

onde $a_1, \ldots, a_s, r \in K[\mathbf{X}]$, *e ainda ou* $r = 0$ *ou* r *é uma combinação linear, com coeficientes em* $\mathbb{K}$, *de monômios, nenhum dos quais é divisível por qualquer* $\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_s)$. *Chamamos* r *de resto da divisão de* f *por* F. *Além disso, se* $a_if_i \neq 0$ *então*

$$\mathrm{lm}(f) \succeq \mathrm{lm}(f_i).$$

Demonstração. Veja em [4, Teorema 3, Pág 64.], e demonstração mostra que o algoritmo abaixo termina após um número finito de passos.

Entrada: $f_1, \ldots, f_s, f$
Saída: $a_1, \ldots, a_s, r$
$a_1 := 0; \ldots; a_s := 0; r := 0$
while $p \neq 0$ **do**
  $i = 1$
  DIVISÃO NÃO OCORRE:=**Falso**
  while $i \leq s$ *e* ***DIVISÃO NÃO OCORRE***:=***Falso*** **do**
    if $\mathrm{lt}(f_i)$ *divide* p **then**
      $a_i := a_i + \frac{\mathrm{lt}(p)}{\mathrm{lt}f_i}$
      $p := p - \left(\frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)}\right) f_i$
      DIVISÃO NÃO OCORRE:= **Verdadeiro**
    else
      $i := i + 1$
    end
  end
  if ***DIVISÃO NÃO OCORRE***:= ***Falso*** **then**
    $r := r + \mathrm{lt}(p)$
    $p = p - \mathrm{lt}(p)$
  else
  end
end

□

A seguir será feito um exemplo para compreender o funcionamento do algoritmo da divisão e a importância da ordem monomial escolhida.

Exemplo 2.6. *Considere* $f = X^2Y + XY^2 + Y^2$, $f_1 = XY - 1$ *e* $f_2 = Y^2 - 1$ *em* $\mathbb{R}[X, Y]$ *e dividiremos* f *por* f_1 *e* f_2 *usando a ordem lexicográfica com* $Y \preceq_{lex} X$.

$$
\begin{array}{rl|l}
X^2Y + XY^2 + Y^2 & XY - 1,\ Y^2 - 1 & \textit{Resto} \\
\cline{2-2}
-X^2Y - X & X + Y, \quad 1 & X + Y + 1 \\
\cline{1-1}
XY^2 + X + Y^2 & & \\
-XY^2 - Y & & \\
\cline{1-1}
X + Y^2 + Y & & \\
-X & & \\
\cline{1-1}
Y^2 + Y & & \\
-Y^2 - 1 & & \\
\cline{1-1}
Y + 1 & & \\
-Y + 1 & & \\
\cline{1-1}
0 & &
\end{array}
$$

Descrevemos agora os processos feitos na imagem acima. Iremos utilizar o mesmo esquema feito pela divisão de polinômios em uma variável, tendo como uma única diferença a existência de mais divisores e quocientes.

Observe que $\mathrm{lm}(f) = X^2Y$, $\mathrm{lm}(f_1) = XY$ *e* $\mathrm{lm}(f_2) = Y^2$, *note que o monômio líder de* f_1 *é o único monômio líder que divide* $\mathrm{lm}(f)$, *sabendo disso começaremos dividindo* f *por* f_1. *Observe que* $\mathrm{lm}(f) = X^2Y = X\mathrm{lm}(f_1)$, *então escrevemos* $f = Xf_1 + (f - Xf_1) = Xf_1 + (XY^2 + X + Y^2)$.

Agora aplicaremos o processo ao resto intermediário $r_1 = XY^2 + X + Y^2$ *pelo algoritmo vamos dividir por* f_1, *pois* $\mathrm{lm}(r_1) = XY^2$ *é múltiplo de* $\mathrm{lm}(f_1) = XY$. *Assim escrevemos* $r_1 = Yf_1(r_1 - Yf_1) = Yf_1 + (X + Y^2 + Y)$ *e portanto*

$$f = (X + Y)f_1 + (X + Y^2 + Y).$$

Note que o resto intermediário agora é $r_2 = X + Y^2 + Y$ *e* $\mathrm{lm}(r_2) = X$ *que não é múltiplo de* $\mathrm{lm}(f_1)$ *e* $\mathrm{lm}(f_2)$. *Assim passaremos* $\mathrm{lm}(r_2)$ *para o resto final. Logo,* $r_3 = Y^2 + Y$ *e é múltiplo* $f_2 + (r_2 - f_2) = f_2 + 2X + 1$. *Deste modo, moveremos* $2X + 1$ *para o resto final, pois* $2X + 1$ *não é múltiplo de* $\mathrm{lm}(f_1)$ *e* $\mathrm{lm}(f_2)$. *Assim escrevemos* $f = (X + 1)f_2 + Xf_1 + 2X + 1$.

2.2 Bases de Gröbner

Em 1965, em sua tese de doutorado Bruno Buchberger criou o que é conhecido hoje como bases de Gröbner. Nessa seção apresentaremos esse conceito e alguns resultados que serão importantes nas próximas seções.

Definição 2.7. *Seja* $I \subseteq K[\mathbf{X}]$ *um ideal não nulo e* $\preceq$ *uma ordem monomial sobre* $\mathcal{M}$. *O conjunto* $\{g_1, \ldots, g_s\} \subseteq I$ *é uma base de Gröbner para* I *(com respeito* $\preceq$*) se para todo* $f \in I$, $f \neq 0$ *temos que* $\mathrm{lm}(f)$ *é múltiplo de* $\mathrm{lm}(g_i)$ *para algum* $i \in \{1, \ldots, s\}$.

Assumiremos que $\mathcal{M}$ é dotado de uma ordem monomial fixa e que $I \neq \langle 0 \rangle$. Mais adiante veremos que todo ideal $I \neq 0$ admite uma base de Gröbner, mas antes apresentamos algumas propriedades de tais bases. O resultado a seguir mostra que uma base de Gröbner para I é na verdade uma base para I e que podemos usá-la para decidir se um polinômio pertence a I.

Lema 2.8. *Seja* $\{g_1, \ldots, g_s\} \subseteq I$ *uma base de Gröbner para* I, *então* $f \in I$ *se, e somente se, o resto de* f *na divisão por* $\{g_1, \ldots, g_s\}$ *é zero. Como consequência* $I = \langle g_1, \ldots, g_s \rangle$.

Demonstração. ($\Leftarrow$) A volta é evidente.
($\Rightarrow$) Seja $f(\mathbf{X}) \in I$ e seja $f(\mathbf{X}) = \sum_{i=1}^{s} q_i(\mathbf{X})g_i(\mathbf{X}) + r(\mathbf{X})$ a divisão de $f(\mathbf{X})$ por $\{g_1, \ldots, g_s\}$. Então $r(\mathbf{X}) = f(\mathbf{X}) - \sum_{i=1}^{s} q_i(\mathbf{X})g_i(\mathbf{X}) \in I$ e por isso devemos ter $r(\mathbf{X}) = 0$, ou $r(\mathbf{X})$ é um polinômio não nulo em I tal que nenhum de seus monômios é múltiplo monômio líder de $g_i(\mathbf{X})$ para todo $i \in \{g_1, \ldots, g_s\}$. Como $r(\mathbf{X}) \in I$ e $\{g_1, \ldots, g_s\}$ é uma base de Gröbner, essa última possibilidade não ocorre, e temos que ter $r(\mathbf{X}) = 0$. Isso mostra que $I \subseteq \{g_1, \ldots, g_s\}$ e a fortiori $I = \langle g_1, \ldots, g_s \rangle$. □

Uma importante propriedade das bases de Gröbner é a seguinte.

Proposição 2.9. *Seja $\{g_1, \ldots, g_s\} \subseteq I$ uma base de Gröbner para I. Na divisão de $f(\mathbf{X}) \in K[\mathbf{X}]$ por $\{g_1, \ldots, g_s\}$ o resto é sempre o mesmo, independente da ordem que for escolhida para $g_1, \ldots, g_s$ no algoritmo da divisão.*

Demonstração. O algoritmo da divisão nos fornece que $f = \sum_{i=1}^{s} a_i g_i + r$, onde $\mathrm{lm}(r) \notin (\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s))$ para uma determinada ordenação e seja $f = \sum_{i=1}^{s} b_i g_i + r'$ o resultado da divisão de f por $\{g_1, \ldots, g_s\}$ usando outra ordenação para os divisores. Assim $r - r' = \sum_{i=1}^{s} b_i g_i - \sum_{i=1}^{s} a_i g_i \in I$ e suponha que $r \neq r'$, então, em particular, $\mathrm{lm}(r - r')$ não é múltiplo de nenhum $\mathrm{lm}(g_i)$ com $i \in \{1, \ldots, s\}$, pois é um dos monômios de r ou r', mas isso contradiz o fato de $\{g_1, \ldots, g_s\}$ ser base de Gröbner. Assim devemos ter $r = r'$.

□

Definição 2.10. *Seja $f(\mathbf{X}), g(\mathbf{X}) \in K[\mathbf{X}] \setminus \{0\}$, com $\mathrm{lt}(f(\mathbf{X})) = a\mathbf{X}^{\alpha}$ e $\mathrm{lt}(g(\mathbf{X})) = b\mathbf{X}^{\beta}$. Seja $\gamma_i = \max\{\alpha_i, \beta_i\}$ para $i \in \{1, \ldots, n\}$ e o conjunto $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{N}_0^n$. O S-polinômio de $f(\mathbf{X})$ e $g(\mathbf{X})$ é definido como*

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

A seguir um exemplo de como cálcular o S-polinômio.

Exemplo 2.11. *Sejam $f = X^3Y^2 - X^2Y^3 + X$ e $g = 3X^4Y + Y^2 \in \mathbb{R}[X, Y]$ com a ordem lexicográfica graduada com $Y \preceq X$.*
Então $\mathrm{lt}(f) = X^3Y^2$ e $\mathrm{lt}(g) = 3X^4Y$.

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

Teorema 2.12 (Critério de Buchberger)**.** *Seja I um ideal em $K[\mathbf{X}]$. Então uma base $G = \{g_1, \ldots, g_t\}$ para I é uma base de Gröbner para I se, e somente se, para todos os pares $i \neq j$, o resto da divisão de $S(g_i, g_j)$ por G é zero.*

Demonstração. Veja em [4, Teorema 6, pag 86]. □

Neste exemplo mostraremos uma aplicação imediata do Teorema acima.

Exemplo 2.13. *Seja* $I = \langle Y - X^2, Z - X^3 \rangle \subset \mathbb{R}[X, Y, Z]$. *Afirmamos que* $G = \{Y - X^2, Z - X^3\}$ *é uma base de Gröbner usando a ordem lexicográfica com* $X \preceq Y \preceq Z$. *Para mostrarmos isto, calcularemos o S-polinômio*

$$S\left(Y - X^2, Z - X^3\right) = \frac{YZ}{Y}\left(Y - X^2\right) - \frac{YZ}{Z}\left(Z - X^3\right) = -ZX^2 + YX^3.$$

Usando o algoritmo da divisão, temos

$$-ZX^2 + YX^3 = X^3 \cdot \left(Y - X^2\right) + \left(-X^2\right) \cdot \left(Z - X^3\right) + 0.$$

Logo, pelo teorema anterior, G *é uma base de Gröbner para* I.

Teorema 2.14. *(Algoritmo de Buchberger) Seja* $I = \langle f_1, \ldots, f_s \rangle \neq 0$ *um ideal polinomial. Então uma base de Gröbner para* I *pode ser construída em um número finito de passos seguindo o seguinte algoritmo.*

Entrada:$F = (f_1, \ldots, f_s)$
Saída: Uma base de Gröbner $G = \{g_1, \ldots, g_t\}$ para $I = \langle F \rangle$, com $F \subset G$
$G := F$
Repita
$G' := G$
Para cada par $p \neq q$ em G' **Faça**
$S := \overline{S(p, q)}^{G'}$
if $S \neq 0$ **then**
| $G := G \cup \{S\}$
else
end
Até $G = G'$

Demonstração. Veja em [4, Teorema 2, pag 91]. □

Agora vamos utilizar este algortimo para construir uma base de Gröbner para um ideal polinomial.

Exemplo 2.15. *Fixe a ordem lexicográfica* $X_2 \preceq X_1$ *e seja* $I = (X_1X_2 - 1, X_2^2 - 1) \subseteq \mathbb{R}[X_1, X_2]$ *um ideal. Vamos aplicar o Algoritmo de Buchberger para encontrar uma base de Gröbner para* I.
Seja $g_1 = X_1X_2 - 1$ *e* $g_2 = X_2^2 - 1$, *então* $S(g_1, g_2) = X_2g_1 - X_1g_2 = X_1 - X_2$ *e o resto da divisão de* $S(g_1, g_2)$ *por* $\{g_1, g_2\}$ *é* $X_1 - X_2$.
Assim seja $g_3 = X_1 - X_2$ *e considere o conjunto* $\{g_1, g_2, g_3\}$ *e pode-se checar que dividindo* $S(g_1, g_2)$ *por* $\{g_1, g_2, g_3\}$, $S(g_2, g_3)$ *por* $\{g_1, g_2, g_3\}$ *e* $S(g_1, g_3)$ *por* $\{g_1, g_2, g_3\}$ *obtemos restos zero. Portanto,* $\{g_1, g_2, g_3\}$ *é uma base de Gröbner.*

Teorema 2.16. *Seja* $I = (g_1, \ldots, g_t) \subset K[\mathbf{X}]$, *tal que* $\text{mdc}(\text{lm}(g_i), \text{lm}(g_j)) = 1$ *para todo* $i, j \in \{1, \ldots, t\}$ *com* $i \neq j$. *Então,* $G = \{g_1, \ldots, g_t\}$ *é uma base de Gröbner de* I.

Demonstração. Veja em [4, Prop.4, Pag.104]. □

2.3 Pegada de um Ideal

Agora introduziremos o conceito que resolve o problema da tese de Buchberger.

Definição 2.17. *Seja $I \subseteq K[\mathbf{X}]$ um ideal. A pegada de I, com respeito a uma ordem monomial fixada em $\mathcal{M}$, é o conjunto*

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

A pegada de um ideal I tem uma relação próxima com uma base de Gröbner para I (ambos sendo definidos com respeito a mesma ordem monomial em $\mathcal{M}$).

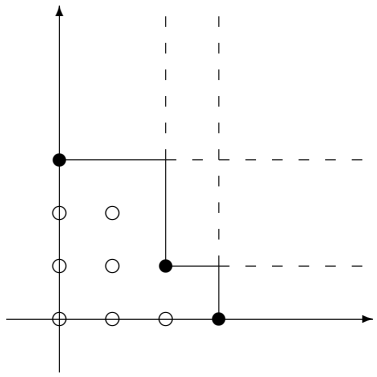
Proposição 2.18. *Sejam $I \subseteq K[\mathbf{X}]$ um ideal e $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner para I. Então um monômio M está em $\Delta(I)$ se, e somente se, M não é múltiplo de $\mathrm{lm}(g_i)$ para todo $i \in \{1, \ldots, s\}$.*

Demonstração. ($\Rightarrow$) Essa implicação segue diretamente da definição.
($\Leftarrow$) Para essa implicação, a partir da definição de base de Gröbner, sabemos que se M não é múltiplo de $\mathrm{lm}(g_i)$ para todo $i \in \{1, \ldots, s\}$, então M não é o monômio líder de nenhum polinômio de I. □

No exemplo a seguir mostraremos como usar o resultado acima para obter uma representação gráfica da pegada.

Exemplo 2.19. *Seja $I = (X_1^3 - X_1, X_2^3 - X_2, X_1^2X_2 - X_2) \subseteq \mathbb{R}[X_1, X_2]$ e $\mathcal{M}$ dotado de uma ordem lexicográfica, onde $X_2 \preceq X_1$. Não é difícil checar que $\{X_1^3 - X_1, X_2^3 - X_2, X_1^2X_2 - X_2\}$ é uma base de Gröbner para I. Temos que $\mathrm{lm}(X_1^3 - X_1) = X_1^3$, $\mathrm{lm}(X_2^3 - X_2) = X_2^3$ e $\mathrm{lm}(X_1^2X_2 - X_2) = X_1^2X_2$ e aplicando a proposição acima para determinar $\Delta(I)$ temos que a pegada de I é o conjunto*

$$\Delta(I) = \{1, X_1, X_1^2, X_2, X_1X_2, X_2^2, X_1X_2^2\}.$$



- ● *Monômios líderes da base de Gröbner de I*
- ○ *Monômios de $\Delta(I)$*

Definição 2.20. *Sejam $I = (f_1, \ldots, f_t) \subset K[\mathbf{X}]$ um ideal e $\{f_1, \ldots, f_t\}$ uma base de I. Denotamos por $\Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$ o conjunto*

$$\Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t)) := \{M \in \mathcal{M} \mid M \text{ não é múltiplo de } \mathrm{lm}(f_i) \text{ para todo } i \in \{1, \ldots, t\}\}.$$

Proposição 2.21. *Seja $I = (f_1, \ldots, f_t) \subset K[\mathbf{X}]$. Então, $\Delta(I) \subset \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$. Caso $\{f_1, \ldots, f_t\}$ seja uma base de Gröbner de I, temos que, $\Delta(I) = \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$.*

Demonstração. Seja $M \in \Delta(I)$, então M não é o monômio líder de nenhum polinômio em I, em particular, M não é múltiplo de $\mathrm{lm}(f_i)$ para todo $i \in \{1, \ldots, t\}$, logo, $M \in \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$.

Agora, suponha que $\{f_1, \ldots, f_t\}$ é uma base de Gröbner de I e seja $M \in \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$, e pela Proposição 2.18, temos que $M \in \Delta(I)$. □

Apresentamos agora a solução para o problema da tese de Buchberger, que será muito útil a seguir.

Teorema 2.22 (Buchberger)**.** *Seja $I \subseteq K[\mathbf{X}]$. Então*

$$\mathcal{B} := \{M + I \mid M \in \Delta(I)\}$$

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

Demonstração. Seja $\mathcal{G}$ uma base de Gröbner para I em relação a uma ordem monomial usada para determinar $\Delta(I)$, e seja $f(\mathbf{X}) \in K[\mathbf{X}]$. Dividindo f por $\mathcal{G}$ obtemos que o resto $r = \sum_{i=1}^{t} a_i M_i$, onde $a_i \in K[\mathbf{X}]$ e $M_i \in \Delta(I)$ para todo $i \in \{1, \ldots, t\}$. Como $f + I = r + I$, obtemos que $\mathcal{B}$ gera $K[\mathbf{X}]/I$ como um K-espaço vetorial. Agora suponha $\sum_{i=1}^{l} b_i(M_i + I) = 0 + I$ onde $b_i \in K$ e $M_i \in \Delta(I)$ para todo $i \in \{1, \ldots, l\}$. Então $\sum_{i=1}^{l} b_i M_i \in I$ devemos ter $b_i = 0$ para todo $i \in \{1, \ldots, l\}$, caso contrário $\sum_{i=1}^{l} b_i M_i$ seria um elemento não nulo de I cujo monômio líder não é múltiplo do monômio líder de nenhum polinômio de $\mathcal{G}$. O que mostra que $\mathcal{B}$ é L.I. sobre K. □

Exemplo 2.23. *Continuando o Exemplo 2.19 temos que $\mathbb{R}[X_1, X_2]/I$ é uma $\mathbb{R}$-espaço vetorial de dimensão 7 e $B = \{1 + I, X_1 + I, X_1^2 + I, X_2 + I, X_1X_2 + I, X_2^2 + I, X_1X_2^2 + I\}$ é uma base para este espaço vetorial.*

Observação 2.24. *Veja que $\Delta(I) \subset \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$. Na verdade, pela Proposição 2.18 temos que $\Delta(I) = \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$ se, e somente se, $\{f_1, \ldots, f_t\}$ é uma base de Gröbner para I.*

2.4 Variedades Afins

Definição 2.25. *O **espaço afim** de dimensão n sobre K é o conjunto*

$$\mathbb{A}^n(K) := \{(a_1, \ldots, a_n) \mid a_i \in K \text{ para todo } i \in \{1, \ldots, n\}\}.$$

Observe que $\mathbb{A}^n(K) = K^n$ como conjunto. No entanto, utilizaremos a notação $\mathbb{A}^n(K)$ para enfatizar a natureza geométrica de K^n, em vez de suas propriedades algébricas (por exemplo, como um espaço vetorial).

Definição 2.26. *Seja $F = \{f_j\}_{j \in J} \subset K[\mathbf{X}]$ onde J é um conjunto de índices. A **variedade afim associada a** F é o conjunto*

$$V(F) := \{(a_1, \ldots, a_n) \in \mathbb{A}^n(K) \mid f_j(a_1, \ldots, a_n) = 0 \text{ para todo } j \in J\}.$$

*Seja $I \subseteq K[\mathbf{X}]$ um ideal. A **variedade afim associada a** I é o conjunto*

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

Veja que segue diretamente da definição acima se $I = (g_1, \ldots, g_s)$, então $V(I) = V(\{g_1, \ldots, g_s\}) = \bigcap_{i=1}^{s} V(g_i)$.

Definição 2.27. *Dado $S \subset \mathbb{A}^n(K)$, o **ideal de polinômios que se anulam em** S, ou simplesmente **ideal de** S, é o conjunto*

$$\mathcal{I}(S) := \{f \in K[\mathbf{X}] \mid f(a_1, \ldots, a_n) = 0 \text{ para todo } (a_1, \ldots, a_n) \in S\}.$$

É fácil verificar que $\mathcal{I}(S)$ é, de fato, um ideal de $K[\mathbf{X}]$.

Definição 2.28. *O* ***radical de um ideal*** $I \subset K[\mathbf{X}]$ *é o conjunto*

$$\sqrt{I} := \{f \in K[\mathbf{X}] \mid f^m \in I, \text{ para algum inteiro positivo } m\}.$$

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

Lema 2.29. *Seja* $I \subseteq K[\mathbf{X}]$ *um ideal e sejam* $P_1, \ldots, P_r$ *pontos distintos de* $V(I)$ *e* $v_i \in K*$. *Então existem polinômios* $p_1, \ldots, p_r \in K[\mathbf{X}]$ *tal que* $p_i(P_j) = v_i\delta_{ij}$ *para todos* $i, j \in \{1, \ldots, r\}$.

Demonstração. Seja $P_i = (a_{i1}, \ldots, a_{in}) \in K^n$, onde $i = 1, \ldots, r$, mostraremos como obter p_1 conforme o enunciado do lema.

Como todos os pontos são distintos, para $i \in \{2, \ldots, r\}$ existe $j_i \in \{1, \ldots, n\}$ tal que $a_{1j_i} \neq a_{ij_i}$. Seja $h_i = (X_{j_i} - a_{ij_i})/(a_{1j_i} - a_{ij_i})$, então $h_i(P_1) = 1$ e $h_i(P_j) = 0$ para todo $j \in \{2, \ldots, r\}$. Tomando $p_1 = v_1 \prod_{i=2}^{r} h_i$ obtemos $p_1(P_i) = v_1\delta_{i1}$ para todo $i \in \{1, \ldots, r\}$.

De forma similar obtemos $p_2, \ldots, p_r$ conforme o lema. □

Proposição 2.30. *Seja* $I \subseteq K[\mathbf{X}]$ *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. Seja $V(I) = \{P_1, \ldots, P_r\}$, do lema acima temos que existem $p_1, \ldots, p_r \in K[\mathbf{X}]$ tais que $p_i(P_j) = \delta_{ij}$ para todos $i, j \in \{1, \ldots, r\}$. Afirmamos que $\{p_i + I \mid i = 1, \ldots, r\}$ é um conjunto linearmente independente. De fato, se $\sum_{i=1}^{r} a_i(p_i + I) = 0 + I$ então temos que $\sum_{i=1}^{r} a_i p_i \in I$, assim $0 = (\sum_{i=1}^{r} a_i p_i)(P_j) = a_j$ para todo j. Assim

$$|\Delta(I)| = \dim_K(K[\mathbf{X}]/I) \geq r = |V(I)|.$$

□

Teorema 2.31. *Seja* $I \subseteq K[\mathbf{X}]$ *um ideal tal que* $\Delta(I)$ *é um conjunto finito e seja* L *uma extensão algébricamente fechada de* K. *Então*

$$V_L(I) := \{(a_1, \ldots, a_n) \in L^n \mid f(a_1, \ldots, a_n) = 0 \text{ para todo } f \in I\}$$

é um conjunto finito e $|V_L(I)| \leq |\Delta(I)|$. *Além disso, se* K *é um corpo perfeito por exemplo, um corpo finito, ou um corpo de característica zero e* I *é um ideal radical, então* $|V_L(I)| = |\Delta(I)|$.

Demonstração. Veja em [2, Teo 8.32]. □

Capítulo 3

Códigos Cartesianos Afins com dual complementar

3.1 Códigos Lineares

Nesta seção iniciaremos um breve estudo da teoria de códigos e usaremos ferramentas apresentadas anteriormente para determinar propriedades importantes de um código (linear).

Definição 3.1. *Um código corretor de erros é um subconjunto $C \subseteq A^n$, onde A é um conjunto finito qualquer chamado de alfabeto e $n \in \mathbb{N}$. Os elementos de A^n são chamados de palavras.*

Definição 3.2. *Dados $\mathbf{a} = (a_1, \ldots, a_n)$ e $\mathbf{b} = (b_1, \ldots, b_n) \in A^n$, a **distância de Hamming** entre $\mathbf{a}$ e $\mathbf{b}$ é definida como*

$$d(\mathbf{a}, \mathbf{b}) = \#\{i \mid a_i \neq b_i, \text{ onde } i \in \{1, \ldots, n\}\}.$$

A distância de Hamming satisfaz as propriedades de uma métrica, como veremos a seguir. Por isso, a distância de Hamming entre elementos de A^n é também chamada de métrica de Hamming.

Proposição 3.3. *Dados $\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n)$ e $\mathbf{c} = (c_1, \ldots, c_n) \in A^n$, valem as seguintes propriedades:*

- $d(\mathbf{a}, \mathbf{b}) \geq 0$ *e* $d(\mathbf{a}, \mathbf{b}) = 0$ *se, e somente se,* $\mathbf{a} = \mathbf{b}$.
- $d(\mathbf{a}, \mathbf{b}) = d(\mathbf{b}, \mathbf{a})$.
- $d(\mathbf{a}, \mathbf{c}) \leq d(\mathbf{a}, \mathbf{b}) + d(\mathbf{b}, \mathbf{c})$.

Demonstração. Vamos demonstrar a terceira propriedade, pois a primeira e a segunda são triviais. Observe que, a contribuição das i-ésimas coordenadas de $\mathbf{a}$ e $\mathbf{c}$ para $d(\mathbf{a}, \mathbf{c})$ é igual a zero se $a_i = c_i$, e igual a um se $a_i \neq c_i$. No caso em que $a_i = c_i$ a contribuição para $d(\mathbf{a}, \mathbf{c})$ é zero; no caso em que $a_i \neq c_i$ não podemos ter $a_i = b_i$ e $c_i = b_i$, logo a contribuição das i-ésimas coordenadas para a soma $d(\mathbf{a}, \mathbf{b}) + d(\mathbf{b}, \mathbf{c})$ é pelo menos 1. Assim, vale a desigualdade. □

Definição 3.4. *Seja C um código. A **distância mínima** de C é o número*

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

Definição 3.5. *Um código $C \subseteq \mathbb{F}_q^n$ será chamado de **código linear** se for um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q^n$. Os **parâmetros do código linear** C são a **dimensão** $\dim_{\mathbb{F}_q} C := k$ de C como $\mathbb{F}_q$-espaço vetorial, o comprimento n de C, e a **distância mínima** $\delta(C)$ de C.*
Usualmente os parâmetros são escritos como a terna de inteiros $[n, k, \delta(C)]$.

Seja $C \subseteq \mathbb{F}_q^n$ um código linear, $k = \dim_{\mathbb{F}_q} C$ e seja $\{b_1, \ldots, b_k\}$ uma base de C, portanto, todo elemento de C se escreve de modo único da forma $\lambda_1 b_1 + \cdots + \lambda_k b_k$, onde $\lambda_i \in \mathbb{F}_q$ para todo $i \in \{1, \ldots, k\}$. Segue daí que $|C| = q^k$.

Definição 3.6. *Dada uma palavra $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$, define-se o **peso** de $\mathbf{a}$ como o sendo o número inteiro*

$$\omega(\mathbf{a}) := |\{i \mid a_i \neq 0\}| = \text{ quantidade de coordenadas de } \mathbf{a} \text{ que são diferentes de zero.}$$

Ou seja, $\omega(\mathbf{a}) = d(\mathbf{a}, \mathbf{0})$, onde $\mathbf{0}$ é o vetor nulo de $\mathbb{F}_q^n$ e d representa a métrica de Hamming.

A partir de agora, sempre que nos referirmos a um código C, significa que $C \subseteq \mathbb{F}_q^n$ é um código linear. Observe que, nesse caso, temos que $\delta(C) = \min\{\omega(\mathbf{a}) \mid \mathbf{a} \in C, \mathbf{a} \neq 0\}$. Isso vem do fato de que, dadas duas palavras distintas $\mathbf{a}$ e $\mathbf{b}$, temos $d(\mathbf{a}, \mathbf{b}) = d(\mathbf{a} - \mathbf{b}, \mathbf{0}) = \omega(\mathbf{a} - \mathbf{b})$.

Definição 3.7. *Sejam um C código tal que $\dim_{\mathbb{F}_q} C = k$, $\mathcal{B} = \{b_1, \ldots, b_k\}$ uma base ordenada de C e considere a matriz G, cujas as linhas são os vetores $b_i = (b_{i1}, \ldots, b_{in})$, $i \in \{1, \ldots, k\}$, isto é*

$$G = \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{k1} & \cdots & b_{kn} \end{pmatrix}.$$

*A matriz G é chamada de **matriz geradora** de C associada a $\mathcal{B}$.*

O nome matriz geradora de C se deve ao fato de C ser a imagem da transformação linear $T : \mathbb{F}_q^k \to \mathbb{F}_q^n$, tal que $T(\mathbf{a}) = \mathbf{a}G$.

Definição 3.8. *Sejam $\mathbf{a} = (a_1, \ldots, a_n)$, e $\mathbf{b} = (b_1, \ldots, b_n)$ elementos de $\mathbb{F}_q^n$, define-se o **produto interno** de $\mathbf{a}$ e $\mathbf{b}$ como sendo*

$$\langle \mathbf{a}, \mathbf{b} \rangle := a_1 b_1 + \cdots + a_n b_n.$$

Definição 3.9. *Seja $C \subseteq \mathbb{F}_q^n$ um código linear, o **código dual** de C, denotado por $C^\perp \subseteq \mathbb{F}_q^n$ é dado por*

$$C^\perp := \{\mathbf{v} \in \mathbb{F}_q^n; \langle \mathbf{v}, \mathbf{u} \rangle = 0 \text{ para todo } \mathbf{u} \in C\}.$$

Lema 3.10. *Seja $C \subseteq \mathbb{F}_q^n$ um código, com matriz geradora G, então*

1. *$C^\perp \subseteq \mathbb{F}_q^n$ é um código linear.*
2. *$\mathbf{a} \in C^\perp \Leftrightarrow G\mathbf{a}^t = 0$, onde $\mathbf{a}^t$ indica o vetor $\mathbf{a}$ transposto.*
3. *$\mathbf{a} \in C^\perp \Leftrightarrow \mathbf{a}G^t = 0$,*

Demonstração. 1. Sejam $\mathbf{a}, \mathbf{b} \in C^\perp$ e $\lambda \in K$. Temos, para todo $\mathbf{x} \in C$, que

$$\langle \mathbf{a} + \lambda \mathbf{b}, \mathbf{x} \rangle = \langle \mathbf{a}, \mathbf{x} \rangle + \lambda \langle \mathbf{b}, \mathbf{x} \rangle = 0,$$

e portanto, $\mathbf{a} + \lambda \mathbf{b} \in C^\perp$, provando que $C^\perp$ é um subespaço vetorial de K^n.

2. $\mathbf{x} \in C^\perp$ se, e somente se, $\mathbf{x}$ é ortogonal a todos os elementos de C se, e somente se, $\mathbf{x}$ é ortogonal a todos os elementos da base de C, o que é equivalente a dizer que $G\mathbf{a}^t = 0$, pois as linhas de G são uma base de C.

3. Segue do item anterior e do fato de que uma matriz tem todas as entradas nulas se e só se sua transposta tem todas as entradas nulas.

□

No que se segue usamos a notação Id_k para simbolizar a matriz identidade $k \times k$.

Proposição 3.11. *Seja $C \subseteq \mathbb{F}_q^n$ um código de dimensão k com matriz geradora $G = (Id_k|A)$, na forma padrão. Então*

1. $\dim_{\mathbb{F}_q} C^\perp = n - k$;
2. $H = (-A^t \mid Id_{n-k})$ *é uma matriz geradora de* $C^\perp$.

Demonstração. Veja em [8, Proposição 2, pag 94]. □

Lema 3.12. *Suponha que C seja um código de dimensão k em $\mathbb{F}_q^n$ com matriz geradora G. Uma matriz H de ordem $(n-k)\times n$, com coeficientes em $\mathbb{F}_q$ e com linhas linearmente independentes, é uma matriz geradora de $C^\perp$ se, e somente se,*

$$G \cdot H^t = 0$$

Demonstração. As linhas de H geram um subespaço vetorial de $\mathbb{F}_q^n$ de dimensão $n-k$, portanto, igual à dimensão de $C^\perp$. Por outro lado, representado por $h_1, \ldots, h_{n-k}$ e por $g_1, \ldots, g_k$, respectivamente, as linhas de H e de G, temos que

$$\left(G \cdot H^t\right)_{i,j} = \langle g_i, h_j \rangle .$$

Portanto, $G \cdot H^t = 0$ equivale a dizer que o subespaço gerado pelas linhas de H estão em $C^\perp$. Por outro lado, esse subespaço tem mesma dimensão que $C^\perp$, logo

$$G \cdot H^t = 0 \Leftrightarrow C^\perp \text{é gerado pelas linhas de H.}$$

□

Corolário 3.13. *Seja C um código. Então $(C^\perp)^\perp = C$.*

Demonstração. Sejam G e H matrizes geradoras de C e $C^\perp$ respectivamente. Segue do lema anterior que $G \cdot H^t = 0$, logo, tomando transpostas, temos $H \cdot G^t = (G \cdot H^t)^t = 0^t = 0$. Como G é uma matriz (com linhas L.I.) de ordem $k \times n$ e $\dim_{\mathbb{F}_q}(C^\perp)^\perp = k$ temos que G é matriz geradora de $(C^\perp)^\perp$, logo $(C^\perp)^\perp = C$. □

Proposição 3.14. *Seja C um código linear e suponhamos que H seja uma matriz geradora de $C^\perp$. Temos então que*

$$v \in C \Leftrightarrow Hv^t = 0.$$

Demonstração. Pelo Corolário acima e pelo segundo item do Lema 3.10, temos $v \in C$ se, e somente se, $v \in (C^\perp)^\perp$ se, e somente se, $Hv^t = 0$. □

A proposição acima nos permite caracterizar os elementos de um código C por meio de uma condição de anulamento.

Definição 3.15. *Seja C um código e $v \in \mathbb{F}_q^n$. A matriz geradora de H de $C^\perp$ é chamada de* ***matriz teste de paridade*** *de C. O vetor Hv^t é chamado de* ***síndrome*** *de v.*

Proposição 3.16. *Seja H a matriz teste de paridade de um código C. Temos que a distância mínima de C é maior ou igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes.*

Demonstração. Suponhamos, inicialmente, que cada conjunto de $s-1$ colunas de H é linearmente independente. Seja $\mathbf{c} = (c_1, \ldots, c_n)$ uma palavra não nula de C, e sejam $h^1, \ldots, h^n$ as colunas de H. Como $H \cdot \mathbf{c}^t = 0$, temos que

$$0 = H \cdot \mathbf{c}^t = \sum_{i=1}^{n} c_i h^i. \tag{3.1}$$

Visto que $\omega(\mathbf{c})$ é o número de componentes não nulas de $\mathbf{c}$, segue que se $\omega(\mathbf{c}) \leq s-1$, teríamos por 3.1 que o vetor nulo se escreve como uma combinação linear de um número t, com $1 \leq t \leq s-1$, de colunas de H, o que é uma contradição com a hipótese. Logo, $\omega(\mathbf{c}) \geq s$ e, portanto, $\omega(C) \geq s$.

Reciprocamente, suponhamos que $\omega(C) \geq s$. Suponhamos também, por absurdo, que H tenha $s-1$ colunas linearmente dependentes, digamos $h^{i_1}, \ldots, h^{i_{s-1}}$. Logo, existiriam $c_{i_1}, \ldots, c_{i_{s-1}}$ no corpo, nem todos nulos, tais que

$$c_{i_1} h^{i_1} + \cdots + c_{i_{s-1}} h^{i_{s-1}} = 0.$$

Portanto, tomando $\mathbf{c} = (0, \ldots, c_{i_1}, \ldots, c_{i_{s-1}}, 0, \ldots, 0)$ temos $H \cdot \mathbf{c}^t = 0$ e logo $\mathbf{c} \in C$, consequentemente, $\omega(\mathbf{c}) \leq s-1 < s$, o que seria um absurdo.

□

Teorema 3.17. *Seja H a matriz teste de paridade de um código C. Temos que a distância mínima de C é igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

Demonstração. De fato, suponha que $\delta(C) = s$, logo pela Proposição 3.16 todo conjunto de $s-1$ colunas de H é linearmente independente. Por outro lado, existem s colunas de H linearmente dependentes, pois, caso contrário, pela Proposição 3.16, teríamos $\delta(C) \geq s+1$.

Reciprocamente, suponhamos que todo conjunto de $s-1$ vetores colunas de H é linearmente independente e existem s colunas linearmente dependentes. Logo, da Proposição 3.16, temos que $\omega(C) \leq s$. Mas $\omega(C)$ não pode ser maior do que s, pois neste caso, novamente pela Proposição anterior nos diria que todo conjunto com s colunas de H é linearmente independente, o que é uma contradição. □

Corolário 3.18 (Cota de Singleton)**.** *Os parâmetros (n, k, d) de um código linear satisfaz a desigualdade*

$$d \leq n - k + 1.$$

Demonstração. Se H é uma matriz teste de paridade, ela tem posto $n-k$. E pelo Teorema 3.17, $d-1$ é menor ou igual ao posto de H, segue que a desigualdade. □

Um código será chamado de **MDS** (**Maximum Distance Separeble**) se valer a igualdade $d = n - k + 1$.

3.2 Exemplos de Códigos

Nesta seção apresentaremos alguns exemplos de códigos.

Exemplo 3.19 (**Códigos de Hamming**)**.** *Um código de Hamming de ordem m sobre $\mathbb{F}_2$ é um código com matriz teste de paridade H_m de ordem $m \times n$, cujas colunas são os elementos de $\mathbb{F}_2^m \setminus \{0\}$ numa ordem qualquer.*
Veja que H_m determina o código C a menos de equivalência.
Temos, portanto, que o comprimento de um código de Hamming de ordem m é $n = 2^m - 1$ e, portanto, a sua dimensão é $k = n - m = 2^m - m - 1$.

Exemplo 3.20 (O código do Mariner 9)**.** *O código usado na nave espacial Mariner 9 é exemplo do código $R(1,m)$ definido sobre $\mathbb{F}_2$, cuja matriz geradora exibiremos a seguir. Este códigos são chamados de* ***Códigos de Reed-Muller de Primeira Ordem****.*
Considere todos os elementos de $\mathbb{F}_2^m$ e organize-os como vetores colunas de uma matriz A_m, $m \times 2^m$, de modo que o bloco $m \times 2^m - 1$ à esquerda dessa matriz seja a matriz H_m, e que a ultima coluna à direita seja o vetor zero de $\mathbb{F}_2^m$ isto é,

$$A_m = (H_m, 0).$$

Construímos uma matriz G com $(m+1)$ linhas e 2^m colunas, de tal modo que as entradas de sua primeira linha sejam todas iguais a 1 e, logo abaixo, a matiz A_m como bloco, ou seja,

$$G = \begin{pmatrix} 1 & 1 \\ H_m & 0 \end{pmatrix}$$

Denotamos por $R(1,m)$ o código cuja matriz geradora seja a matriz G. Mais à frente (veja Exemplo 3.39) mostraremos que os parâmetros desse código são $(2^m, m+1, 2^{m-1})$.

Exemplo 3.21 (Reed-Solomon)**.** *Seja $\mathbb{F}_q$ um corpo finito e considere o $\mathbb{F}_q$-espaço vetorial $\mathbb{F}_q[X]_n$ dos polinômios de $\mathbb{F}_q[X]$ de grau menor que n, incluindo o polinômio nulo, isto é*

$$\mathbb{F}_q[X]_k = \{p(X) \in \mathbb{F}_q[X]; \deg(p(X)) < k\} \bigcup \{0\}.$$

É claro que esse espaço vetorial tem dimensão n com uma base dada por

$$\mathcal{B} = \{1, X, X^2, \ldots, X^{k-1}\}$$

Sejam n um inteiro, tal que $n \geq k$, e $\alpha_1, \ldots, \alpha_n$ elementos distintos de $\mathbb{F}_q$. Considere a função definida por

$$\begin{aligned} T\colon \mathbb{F}_q[X]_k &\to \mathbb{F}_q^n \\ P(X) &\mapsto (P(\alpha_1), \ldots, P(\alpha_n)). \end{aligned}$$

Temos que T é uma transformação linear. De fato, dados $P(X), Q(X) \in \mathbb{F}_q[X]$ e $\lambda \in \mathbb{F}_q$ temos

$$T(\lambda P(X) + Q(X)) = ((\lambda P + Q)(\alpha_1), \ldots, (\lambda P + Q)(\alpha_n))$$

$$= (\lambda P(\alpha_1) + Q(\alpha_1), \ldots, \lambda P(\alpha_n) + Q(\alpha_n)) = \lambda(P(\alpha_1), \ldots, P(\alpha_n)) + (Q(\alpha_1), \ldots, Q(\alpha_n))$$

$$= \lambda T(P(X)) + T(Q(X)).$$

Além disso, T é injetora. De fato,

$$\ker T = \{P \in \mathbb{F}_q[X]_k \mid P(\alpha_1) = \cdots = P(\alpha_n) = 0\} = \{0\},$$

pois um polinômio não nulo P qualquer de grau menor que $k \leq n$ não pode ter n raízes distintas. Portanto, a imagem $C = T(\mathbb{F}_q[X]_k)$ é um código linear de comprimento n e dimensão k.

Esse código será chamado ***Código de Reed-Solomon*** *de comprimento n e dimensão k definido por $\alpha_1, \ldots, \alpha_n$.*

Proposição 3.22. *Seja C um código de Reed-Solomon de comprimento n e dimensão k. Então a distância mínima de C é $d = n - k + 1$, e por consequência os códigos de Reed-Solomon são* ***MDS****.*

Demonstração. Pelo Corolário 3.18, sabemos que $d \leq n - k + 1$. Por outro lado, seja c uma palavra não nula de C. Então existe $P(X) \in \mathbb{F}_q[X]_k$ tal que

$$c = (P(\alpha_1, \ldots, P(\alpha_n))) = T(P(X)).$$

Logo,

$$\begin{aligned}\omega(c) &= |\{i \in \{1, \ldots, n\} \mid P(\alpha_i) \neq 0\}| \\ &= n - |\{i \in \{1, \ldots, n\} \mid P(\alpha_i) = 0\}| \geq \\ n - \deg(P(X)) &\geq n - (k-1) = n - k + 1.\end{aligned}$$

Segue daí que

$$d \geq n - k + 1.$$

Portanto $d = n - k + 1$ e assim os códigos de Reed-Solomon são **MDS**. □

3.3 Códigos Cartesianos Afins Generalizados

Nesta seção, seguindo [10], iremos apresentar alguns resultados sobre um tipo particular de código. E para isso iremos utilizar ferramentas desenvolvidas em [3].

Seja $I = (g_1, \ldots, g_t) \subset \mathbb{F}_q[\mathbf{X}]$ e consideremos o ideal $I_q := (g_1, \ldots, g_t, X_1^q - X_1, \ldots, X_m^q - X_m)$. Da Proposição 1.26, sabemos que $\prod_{a \in \mathbb{F}_q}(X - a) = X^q - X$, e consequentemente $V(I) = V(I_q)$.

De agora em diante vamos sempre estar considerando a ordem lexicográfica graduada ($\preceq_{\text{grlex}}$) em $\mathcal{M} \subset \mathbb{F}_q[\mathbf{X}]$.

Proposição 3.23. *O conjunto $\Delta(I_q)$ é finito.*

Demonstração. Afirmo que $\Delta(\text{lm}(g_1), \ldots, \text{lm}(g_t), X_1^q, \ldots, X_m^q) \leq q^m$. De fato, por definição temos que $\Delta(\text{lm}(g_1), \ldots, \text{lm}(g_t), X_1^q, \ldots, X_m^q)$ é o conjunto dos monômios que não são múltiplos de $\text{lm}(g_1), \ldots, \text{lm}(g_t), X_1^q, \ldots, X_m^q$ em particular, tais monômios não são múltiplos de $X_1^q, \ldots, X_m^q$. Assim, pela Proposição 2.21, temos

$$|\Delta(I_q)| = |\Delta(\text{lm}(g_1), \ldots, \text{lm}(g_t), X_1^q, \ldots, X_m^q)| \leq q^m.$$

O que completa a demonstração. □

Lema 3.24. *Seja $I \subset \mathbb{F}_q[\mathbf{X}]$ um ideal tal que $\Delta(I)$ é um conjunto finito. Então*

I é um ideal radical $\Leftrightarrow$ Existe $f_j \in I \subset \mathbb{F}_q[X_j] \setminus \mathbb{F}_q$ tal que $\text{mdc}(f_j, f_j') = 1,\ \forall j \in \{1, \ldots, m\}$

Demonstração. Veja em [2, Poposição 8.14]. □

Seja $V(I_q) = \{P_1, \ldots, P_n\}$ e considere a seguinte aplicação linear

$$\begin{aligned}\varphi \colon \mathbb{F}_q[\mathbf{X}]/I_q &\to \mathbb{F}_q^n \\ f + I_q &\mapsto (1f(P_1), \ldots, 1f(P_n)).\end{aligned}$$

Proposição 3.25. *A aplicação linear φ é um isomorfismo entre $\mathbb{F}_q$-espaços vetoriais.*

Demonstração. Primeiro vamos mostrar que $\dim_{\mathbb{F}_q} \mathbb{F}_q[X]/I_q = m$. De fato como o polinômio $f_j := X_j^q - X_j$ tem q raízes distintas temos $\text{mdc}(f_j, f_j') = 1$ para todo $j \in \{1, \ldots, n\}$, e pela Proposição 3.23 o conjunto $\Delta(I_q)$ é finito, segue do Lema anterior I_q é um ideal radical. Observe também que, $V_{\overline{\mathbb{F}_q}}(I_q) = V(I_q)$, onde $\overline{\mathbb{F}_q}$ é o fecho algébrico de $\mathbb{F}_q$ e pelo Teorema 2.31 temos que $\left|V_{\overline{\mathbb{F}_q}}(I_q)\right| = |\Delta(I_q)|$. Assim, pelo Teorema 2.22, temos que $\dim_{\mathbb{F}_q} \mathbb{F}_q[X]/I_q = |\Delta(I_q)| = m$.

Agora, mostraremos que φ é sobrejetora, e assim, pelo Teorema do Núcleo e da Imagem o resultado seguirá. Sabendo disso, sejam $p_1, \ldots, p_m \in \mathbb{F}_q[\mathbf{X}]$, tais que $p_i(P_j) = \delta_i^j$ para todo $i, j \in \{1, \ldots, m\}$ que existem pelo Lema 2.29, e veja que, $\varphi(p_i + I_q) = e_i$ para todo $i \in \{1, \ldots, m\}$, onde e_i é um vetor da base canônica. Como $\{e_1, \ldots, e_m\}$ é uma base para $\mathbb{F}_q^m$ como $\mathbb{F}_q$-espaço vetorial. □

A seguir o conceito introduzido por Ftizgerald e Lax em [5].

Definição 3.26. *Seja $L \subset \mathbb{F}_q[\mathbf{X}]/I_q$ um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q[\mathbf{X}]/I_q$. A imagem $\varphi(L) =: C(L)$ é chamado de* ***código de variedade afim associado a*** *L.*

Uma propriedade importante que será provada, é que todo código linear pode ser representado como um código de variedade afim. Para isso, o lema abaixo se faz necessário.

Lema 3.27. *Sejam $P_1, \ldots, P_s$ pontos de $\mathbb{A}^n(\mathbb{F}_q)$ tal que $P_j = (b_{j1}, \ldots, b_{jn})$. Então o polinômio*

$$f_j(\mathbf{X}) = \prod_{i=1}^{n} [1 - (X_i - b_{ji})^{q-1}],$$

é tal que, $f_j(P) = 0$ para todo $P \in \mathbb{A}^n(\mathbb{F}_q) \setminus \{P_j\}$ e $f_j(P_j) = 1$ para $j = 1, \ldots, s$.

Demonstração. Da Proprosição 1.26 sabe-se que $X_i^q - X_i = \prod_{b \in \mathbb{F}_q}(X_i - b)$ para todo $i \in \{1, \ldots, s\}$. Dado $\alpha \in \mathbb{F}_q$, temos que

$$\prod_{b \in \mathbb{F}_q \setminus \{\alpha\}} (X_i - b) = \frac{X_i^q - X_i}{X_i - \alpha} = \frac{(X_i - \alpha)^q - (X_i - \alpha)}{(X_i - \alpha)},$$

ou seja, $(X_i - \alpha)^{q-1} - 1 = \prod_{b \in \mathbb{F}_q \setminus \{\alpha\}}(X_i - b)$. Assim, caso $X_i = \alpha$ temos que $1 - (X_i - \alpha)^{q-1} = 1$ e caso $X_i \neq \alpha$ então $1 - (X_i - \alpha)^{q-1} = 0$ e por consequência o resultado segue. □

Proposição 3.28. *Todo código linear $C \subset \mathbb{F}_q^s$ pode ser representado como um código de variedade afim.*

Demonstração. Seja $C \subset \mathbb{F}_q^s$ um código linear, tal que $\dim_{\mathbb{F}_q} C = k$. Seja $\left[c_{ij}\right]$ uma matriz geradora de C com $i = 1, \ldots, k$ e $j = 1, \ldots, s$. Escolha o menor número natural n, tal que $q^n \geq s$. Sejam $Y = \{P_1, \ldots, P_s\} \subset \mathbb{A}^n(\mathbb{F}_q)$ e $I = \mathcal{I}(Y) \subset \mathbb{F}_q[\mathbf{X}]$ o ideal polinomial que anula os pontos de Y. Denotaremos $P_j = (b_{j1}, \ldots, b_{jn})$ para todo $j = 1, \ldots, n$. E pelo Lema anterior temos que o polinômio $f_j(\mathbf{X}) = \prod_{i=1}^{n}[1 - (X_i - b_{ji})^{q-1}]$ é tal que $f_j(P) = 0$ para todo $P \in \mathbb{A}^n(\mathbb{F}_q) \setminus \{P_j\}$ e $f_j(P_j) = 1$ para todo $j = 1, \ldots, s$.

Defina $g_i + I_q := \sum_{i=1}^{s} c_{ij}(f_j + I_q)$, para todo $i = 1, \ldots, k$ e tome $L = \langle g_1 + I_q, \ldots, g_k + I_q \rangle \subset \mathbb{F}_q[\mathbf{X}]/I_q$ o subespaço gerado por $\{g_1 + I_q, \ldots, g_k + I_q\}$. Assim, $C = C(L)$, pois $\varphi(g_i + I_q) = (c_{i1}, \ldots, c_{is})$, para $i = 1, \ldots, k$ e $\varphi : \mathbb{F}_q[\mathbf{X}]/I_q \to \mathbb{F}_q^s$ é tal que $\varphi(f + I_q) = (f(P_1), \ldots, f(P_s))$. E o resultado segue. □

Agora iremos apresentar resultados sobre um tipo específico de *código de variedade afim* que foi introduzido por H. López, F. Manganiello, G. Matthews em [10]. A seguir será feita a construção de tal código.

Sejam $A_1, \ldots, A_m \subset \mathbb{F}_q$ subconjuntos não vazios de $\mathbb{F}_q$, definimos o conjunto cartesiano $\mathcal{A} := A_1 \times \cdots \times A_m$. Defina $L_i(X_i) = \prod_{c \in A_i}(X_i - c)$ para todo $i \in \{1, \ldots, m\}$ e consideremos $I = (L_1(X_1), \ldots, L_m(X_m))$, note que $V(I) = \mathcal{A}$. Como o feito acima temos o conjunto $I_q = (L_1(X_1), \ldots, L_m(X_m), X_1^q - X_1, \ldots, X_m^q - X_m)$ e observe que $I_q = I$, pois $L_i(X_i)$ é um divisor de $X_i^q - X_i$ para todo $i \in \{1, \ldots, m\}$. Diferentemente da construção feita acima, sejam $v_1, \ldots, v_n$ invertíveis de $\mathbb{F}_q$, onde $n := |\mathcal{A}|$ e defina a seguinte aplicação linear

$$\begin{aligned} \psi \colon \mathbb{F}_q[\mathbf{X}]/I_q &\to \mathbb{F}_q^n \\ f + I_q &\mapsto (v_1 f(a_1), \ldots, v_n f(a_n)) \,. \end{aligned}$$

Proposição 3.29. *A aplicação linear ψ é um isomorfismo entre $\mathbb{F}_q$-espaços vetoriais.*

Demonstração. Similar a demonstração feita na Proposição 3.25, utilizando o Lema 2.29. □

Definição 3.30. *Seja $k \in \mathbb{N}_0$ e consideremos o $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q[\mathbf{X}]/I_q$ dado por $S_{<k} := \{p + I_q \mid p = 0 \text{ ou } \deg(p) < k\}$, onde $\deg(p(\mathbf{X}))$ é o grau do polinômio $p(\mathbf{X}) \in \mathbb{F}_q[\mathbf{X}]$. A imagem $C_k(\mathcal{A}, v) := \psi(S_k)$ é chamada de* ***código de avaliação cartesiano afim generalizado*** *ou simplesmente* ***código cartesiano*** *de grau k associado a $\mathcal{A}$ e v.*

Observação 3.31. *Veja que podemos caracterizar um código cartesiano $C_k(\mathcal{A}, v)$ como o conjunto $\{\psi(p + I_q) \mid p = 0 \text{ ou } \deg(p) < k \text{ e } \deg_{X_i}(p) < n_i \text{ para todo } i \in \{1, \ldots, m\}\}$.*

Lema 3.32. *O conjunto $\{L_1(X_1), \ldots, L_m(X_m)\}$ é uma base de Gröbner de I.*

Demonstração. Como $\text{mdc}(L_i(X_i), L_j(X_j)) = 1$ para todo $i \neq j$, então pelo Teorema 2.16 o resultado segue. □

Lema 3.33. $\mathcal{I}(\mathcal{A}) = I$.

Demonstração. É claro que $I \subset \mathcal{I}(\mathcal{A})$, então segue que $\Delta(\mathcal{I}(\mathcal{A})) \subset \Delta(I) = \{X_1^{\alpha_1} \cdots X_m^{\alpha_m} \mid 0 \leq \alpha_i < n_i, \text{ onde } n_i := A_i, \text{ para todo } i \in \{1, \ldots, m\}\}$. Assim, pela Proposição 2.30 e pelo Lema acima, temos que $n_1 \cdots n_m = |V(\mathcal{I}(\mathcal{A}))| \leq |\Delta(\mathcal{I}(\mathcal{A}))| \leq |\Delta(I)| = n_1 \cdots n_m$, logo $|\Delta(\mathcal{I}(\mathcal{A}))| = n_1 \cdots n_m$. Por consequência $\Delta(\mathcal{I}(\mathcal{A})) = \{X_1^{\alpha_1} \cdots X_m^{\alpha_m} \mid 0 \leq \alpha_i < n_i, \text{ onde } n_i := A_i, \text{ para todo } i \in \{1, \ldots, m\}\}$. Agora, dado $f \in \mathcal{I}(\mathcal{A})$, temos que $\text{lm}(f)$ é múltiplo de $\text{lm}(L_i(X_i)) = X_i^{n_i}$ para algum $i \in \{1, \ldots, m\}$, caso contrário, $\text{lm}(f) \in \Delta(\mathcal{I}(\mathcal{A}))$, o que é uma contradição. Então $\{L_1(X_1), \ldots L_m(X_m)\} \subset \mathcal{I}(\mathcal{A})$ e por consequência é uma base de Gröbner de $\mathcal{I}(\mathcal{A})$ e, portanto, $\mathcal{I}(\mathcal{A}) = I$. □

Agora iremos calcular os parâmetros de $C_k(\mathcal{A}, v)$ e para isso considere o conjunto $\Delta(\mathcal{I}(\mathcal{A}))_{<k} := \{M \in \Delta(\mathcal{I}(\mathcal{A}))| \deg(M) < k\}$.

Proposição 3.34. *O conjunto $\{M + I \mid M \in \Delta(I)_{<k}\}$ é uma base de $S_{<k}$ como $\mathbb{F}_q$-espaço vetorial.*

Demonstração. Pelo Teorema 2.22 sabemos que o conjunto $\mathcal{B} := \{M + I | M \in \Delta(I)_{<k}\}$ é linearmente independente, e claramente está contido em $S_{<k}$. Agora, seja $p \in \mathbb{F}_q[\mathbf{X}]$, $p \neq 0$ tal que $\deg(p) < k$. Dividindo p por $\{L_1(X_1), \ldots, L_m(X_m)\}$, temos pelo algoritmo da divisão que o resto r obtido através dessa divisão é tal que, $\text{lm}(r) \preceq_{grlex} \text{lm}(p)$ ou $r = 0$, ou seja, $\deg(\text{lm}(r)) < kd$ ou $r = 0$. Se $r = 0$, é claro que $p + I = 0 + I$ é uma combinação $\mathbb{F}_q$-linear de elementos em $\mathcal{B}$ e se $r \neq 0$, temos $p + I = r + I$ que é uma combinação $\mathbb{F}_q$-linear de elementos em $\mathcal{B}$, pois todos os monômios aparecendo em r estão em $\Delta(I)_{<k}$ (aqui usamos que $\{L_1(X_1), \ldots, L_m(X_m)\}$ é uma base de Gröbner de I, e portanto, $\mathcal{B}$ é uma base de $S_{<k}$ como $\mathbb{F}_q$-espaço vetorial. □

Seja $c = (c_1, \ldots, c_n)$ uma palavra de $C_k(\mathcal{A}, v)$, mostraremos que existe um polinômio f_c em $S_{<k}$ tal que $\psi(f_c + I_q) = c$. Com esse propósito, para cada elemento $a = (a_1, \ldots, a_m) \in \mathcal{A}$ defina o seguinte polinômio

$$L_a(\mathbf{X}) = \frac{L_1(X_1)}{X_1 - a_1} \cdots \frac{L_m(X_m)}{X_m - a_m}.$$

Veja que $L_a(b) = 0$ para todo $b \in \mathcal{A} \mid b \neq a$ e $L_a(a) = L_1'(a_1) \cdots L_m'(a_m)$, onde $L_i'(X_i)$ denota a derivada formal de $L_i(X_i)$. De fato, veja que

$$L_a(a) = \left(\prod_{b_1 \in A_1 | b_1 \neq a_1} (b_1 - a_1) \right) \cdots \left(\prod_{b_m \in A_1 | b_m \neq a_m} (b_m - a_m) \right).$$

Por outro lado, como A_i é finito, então $A_i = \{a_1, \ldots, a_{n_i}\}$ para todo $i \in \{1, \ldots, m\}$. Sabendo disso e utilizando as regras de derivação temos,

$$L_i^{'}(X_i) = \left(\prod_{a_{j1} \in A_1 | a_{j1} \neq a_1} (X_i - a_{j1}) \right) + \cdots + \left(\prod_{a_{jm} \in A_m | a_{jm} \neq a_{n_m}} (X_i - a_{jm}) \right).$$

Logo,

$$L_i^{'}(a_i) = \left(\prod_{a_{ji} \in A_i | a_{ji} \neq a_i} (a_i - a_{ji}) \right).$$

E portanto,

$$L_1^{'}(a_1) \cdots L_m^{'}(a_m) = \left(\prod_{a_{j1} \in A_1 | a_{j1} \neq a_1} (a_1 - a_{j1}) \right) \cdots \left(\prod_{a_{jm} \in A_m | a_{jm} \neq a_{n_m}} (X_i - a_{jm}) \right) = L_a(a). \tag{3.2}$$

Como queríamos mostrar. E por fim o polinômio que queremos é

$$f_c(\mathbf{X}) := \sum_{j=1}^{n} \frac{L_{a_j}(\mathbf{X})}{L_{a_j}(a_j)} c_j. \tag{3.3}$$

Veja que $\deg_{X_i} f_c(\mathbf{X}) < n_i$ para todo $i \in \{1, \ldots, m\}$ e por construção temos que $\psi(f_c + I_q) = c$.

Os resultados abaixo determinam os parâmetros dos códigos cartesianos.

Lema 3.35. *A dimensão de $C_k(\mathcal{A}, v)$ é $\dim_{\mathbb{F}_q}(C_k(\mathcal{A}, v)) = |\Delta(I)_{<k}|$, veja que em particular $\dim_{\mathbb{F}_q}(C_k(\mathcal{A}, v)) = n_1 \cdots n_m$ e $\delta(C_k(\mathcal{A}, v)) = 1$ para todo $k \geq \sum_{i=1}^{m}(n_i - 1)$.*

Demonstração. A primeira sentença é consequência da Proposição 3.34 e pelo fato de ψ ser um isomorfismo.

Para provar a segunda e terceira afirmações, temos que $\{L_1(X_1), \ldots, L_m(X_m)\}$ é uma base de Gröbner para I temos

$$\Delta(I) = \{X_1^{\alpha_1} \cdots X_m^{\alpha_m} | 0 \leq \alpha_i \leq n_i - 1 \text{ para todo } i \in \{1, \ldots, m\}\}.$$

Portanto, $\Delta(I)_{<k} = \Delta(I)$ sempre que $k \geq \sum_{i=1}^{m}(n_i - 1)$. E o resultado segue pelo fato de $|\Delta(I)| = n_1 \cdots n_m$ e o fato de $\psi(L_k) = \mathbb{F}_q^{n_1 \cdots n_m}$. □

Teorema 3.36. *A dimensão de $C_k(\mathcal{A}, v)$ para $0 \leq k < \sum_{i=1}^{m}(n_i - 1)$ é dada por*

$$\dim_{\mathbb{F}_q}(C_k(\mathcal{A}, v)) = \binom{m+k-1}{k-1} - \sum_{i=1}^{m} \binom{m-k-1-n_i}{k-1-n_i} + \cdots +$$

$$(-1)^j \sum_{1 \leq i_1 < \cdots < i_j \leq n} \binom{m+k-1-n_{i_1} - \cdots - n_{i_j}}{k-1-n_{i_1} - \cdots - n_{i_j}} + \cdots +$$

$$(-1)^n \binom{m+k-1-n_1 - \cdots n_m}{k-1-n_1 - \cdots n_m},$$

onde estabelecemos que $\binom{a}{b} = 0$ se $b < 0$.

Demonstração. De acordo com o Lema anterior a dimensão de $C_k(\mathcal{A}, \mathbf{v})$ é igual a cardinalidade de $\Delta(I)_{<k}$, isto é, o número de monômios em $\Delta(I)$ da forma $X_1^{\alpha_1} \cdots X_m^{\alpha_m}$, onde $0 \leq \sum_{i=1}^m \alpha_i < k$. Seja $h(t) := (1 + t + \cdots + t^{n_1-1}) \cdots (1 + t + \cdots + t^{n_m-1})$, note que os coeficientes de t^e em $h(t)$ é igual ao número de monômios em $\Delta(I)$ que tem grau e para todo $e \in \{0, \ldots, \sum_{i=1}^m (n_i - 1)\}$.

Assim uma maneira de obter o que queremos é calcular os coeficientes de $t^0, t, \ldots, t^{k-1}$ e depois soma-los. Uma forma de provar isso é mostrar que existe uma bijeção entre $\Delta(I)_{<k}$ e $\Omega_{k-1} := \{X_0^{\alpha_0} \cdot X_1^{\alpha_1}, \cdots X_m^{\alpha_m} \in \mathbb{F}_q[X_0, X_1, \ldots, X_m] \mid \text{com } \sum_{i=0}^m \alpha_i = k-1 \text{ e } 0 \leq \alpha_i < n_i - 1 \text{ para todo } i \in \{i = 1, \ldots, m\}\}$, dada por $\beta : \Delta(I)_{<k} \to \Omega_{k-1}$, onde $\beta(M) = X_0^{k-1} M \cdot \left(\frac{X_1}{X_0}, \ldots, \frac{X_m}{X_0}\right)$ e $\beta^{-1} : \Omega_{k-1} \to \Delta(I)_{<k}$, dada por $\beta^{-1}(N) = N \cdot (1, X_1, \ldots, X_m)$.

Agora considere

$$H(t) := (1 + t + t^2 + \cdots)(1 + t + \cdots + t^{n_1-1}) \cdots (1 + t + \cdots + t^{n_m-1}),$$

então o coeficiente de t^{k-1} é a cardinalidade de Ω_{k-1}.
Note que podemos encarar $H(t)$ como uma função real na variável t definida em uma vizinhança adequada de 0, digamos $|t| < 1$. Então $1 + t + \cdots = \frac{1}{1-t}$, de modo que

$$H(t) = \frac{1}{1-t} \cdot \frac{1 - t^{n_1}}{1-t} \cdots \frac{1 - t^{n_m}}{1-t}.$$

Assim $H(t) = \frac{1}{(1-t)^{m+1}} \cdot \prod_{i=1}^m (1 - t^{n_i})$.
Usando que $\frac{1}{(1-t)^{m+1}} = \binom{m+j}{j} t^j$, temos

$$H(t) = \left(\sum_{j=0}^{\infty} \binom{m+j}{j} t^j\right) \cdot \left(1 - \sum_{i=1}^m t^{n_i} + \sum_{1 \leq i_1 < i_2} t^{n_{i_1} + n_{i_2}}\right) + \cdots +$$

$$\left(\sum_{j=0}^{\infty} \binom{m+j}{j} t^j\right) \left((-1)^j \sum_{1 \leq i_1 < \cdots < i_j \leq m} t^{n_{i_1} + \cdots + n_{i_j}} + \cdots + (-1)^m t^{n_{i_1} + \cdots + n_{i_m}}.\right).$$

A expressão para $\dim_{\mathbb{F}_q}(C(\mathcal{A}, v))$ na afirmação do teorema é o coeficiente de t^{k-1} em $H(t)$ calculado usando o produto acima. □

Para encontrar a distância mínima de $C_k(\mathcal{A}, v)$, para $0 \leq k < \sum_{i=1}^m (n_i - 1)$, precisaremos do seguinte resultado auxiliar.

Lema 3.37. *Seja $0 < n_1 \leq \cdots \leq n_m$ e $k < \sum_{i=1}^m (n_i - 1)$ números inteiros. Seja $m(\alpha_1, \ldots, \alpha_m) := \prod_{i=1}^m (n_i - \alpha_i)$, onde $0 \leq \alpha_i < n_i$ são inteiros para todo $i \in \{1, \ldots, m\}$. Então*

$$\min\{m(\alpha_1, \ldots, \alpha_m) | \alpha_1 + \cdots + \alpha_m \leq s\} = (n_{s+1} - l) \prod_{i=s+2}^m n_i$$

onde s e l são unicamente definidos por $k = \sum_{i=1}^s (n_i - 1) + l$ com $0 \leq l < n_{s+1} - 1$. Aqui, se $s + 1 = m$ então entendemos que $\prod_{i=s+2}^m n_i = 1$, e se $k < n_1 - 1$ então entendemos que $s = 0$ e $l = k$.

Demonstração. Observe que o mínimo deve ser alcançado quando $k - 1 = \sum_{i=1}^m \alpha_i$ e o Lema afirma que ele é alcançado na m-upla $(n_1 - 1, \ldots, n_s - 1, l, 0, \ldots, 0)$. Portanto, seja $\alpha = (\alpha_1, \ldots, \alpha_m)$ com $\sum_{i=1}^m \alpha_i = k - 1$ e assuma que $\alpha_{i_1} < n_{i_1} - 1$ para todo $i_1 \in \{1, \ldots, s\}$. Se existe $i_2 \in \{s + 1, \ldots, m\}$ tal que $\alpha_{i_2} > 0$ e $\alpha_{i_1} + \alpha_{i_2} \leq n_{i_1} - 1$ então denotamos por α' a m-upla de α substituindo α_{i_1} por $\alpha_{i_1} + \alpha_{i_2}$ e α_{i_2} por 0. Assim, temos

$$m(\alpha) - m(\alpha') = \prod_{i=1}^m (n_i - \alpha_i) - \prod_{i=1}^m (n_i - \alpha_i') = (\alpha_{i_1}\alpha_{i_2} + (n_{i_2} - n_{i_1})\alpha_{i_2}) \cdot \prod_{i=1 \text{ e } i \neq i_1, i_2}^m (n_i - \alpha_i) \geq 0,$$

então $m(\alpha) \geq m(\alpha')$. Se existe $i_2 \in \{s+1, \ldots, m\}$ tal que $\alpha_{i_2} > 0$ e $\alpha_{i_1} + \alpha_{i_2} > n_{i_1} - 1$ então denotamos por α'' a m-upla obtida de α pela substituindo α_{i_1} por $d_{i_1} - 1$ e α_{i_2} por $\alpha_{i_2} - (d_{i_1} - 1\alpha_{i_1})$. Assim temos

$$m(\alpha) - m(\alpha'') = (d_{i_1} - 1\alpha_{i_1})(d_{i_2} - 1\alpha_{i_2}) \cdot \prod_{i=1 \text{ e } i \neq i_1, i_2} (n_i - \alpha_i) \geq 0$$

logo, $m(\alpha) \geq m(\alpha'')$. Isso prova que se m atingir seu mínimo em α, podemos assumir que $\alpha_i = n_i - 1$ para todo $i \in \{1, \ldots, s\}$. Da mesma forma, pode-se assumir $\alpha_{s+1} = l$. □

Teorema 3.38. *Seja $0 \leq k < \sum_{i=1}^{m}(n_i - 1)$, a distância mínima de $C_k(\mathcal{A}, v)$ é $(n_{s+1} - l)\prod_{i=s+2}^{m}(n_i - 1)$, onde s e l são unicamente definidos por $k = \sum_{i=1}^{s}(n_i - 1) + l$ com $0 \leq l < n_{s+1} - 1$. Como o resultado acima, se $s + 1 = m$ entendemos que $\prod_{i=s+2}^{m} n_i = 1$ e se $k < n_1 - 1$ então estabelecemos $s = 0$ e $l = k$.*

Demonstração. Seja $F \in S_{<k}$ e seja $J_F := (F, L_1(X_1), \ldots, L_m(X_m))$. Então o número de zeros do código $\psi(F + I)$ é igual a $|V(J_F)|$ para que o peso desse código seja $\omega(\psi(F + \mathcal{I}(\mathcal{A}))) = \prod_{i=1}^{m} n_i - |V(J_F)|$. Pela Proposição 2.30, temos que $|V(J_F)| \leq |\Delta(J_F)|$. Seja $M := X_1^{\alpha_1} \cdots X_m^{\alpha_m}$ o monômio líder de F pela Observação [], temos que $|\Delta(J_F)| \subset \Delta(M, X_1^{n_1}, \ldots, X_m^{n_m})$, logo $|\Delta(J_F)| \leq \prod_{i=1}^{m}(n_i - \alpha_i)$.

Assim $\omega(\psi(F + I)) \leq \prod_{i=1}^{m}(n_i - \alpha_i)$ e do Lema anterior temos que $\omega(\psi(F + I)) \geq (n_{s+1} - l) \cdot \prod_{i=s+2}^{m} n_i$. Para ver que o limite é realmente alcançado, escrevemos $A_i := \{a_{i_1}, \ldots, a_{i_{n_i}}\}$ para $i \in \{1, \ldots, m\}$ e seja $G(X_1, \ldots, X_m) = \left(\prod_{i=1}^{s}\prod_{j=1}^{n_i-1}(X_i - a_{ij})\right)\prod_{j=1}^{l}(X_{s+1} - a_{s+1_j})$, então $\deg(G) = k$ e G tem $\prod_{i=1}^{m} n_i - (n_{s+1} - l)\prod_{i=s+2}^{m} n_i$ zeros em $\mathcal{A}$, então $\omega(\varphi(G + I) = (n_{s+1} - l)\prod_{i=s+2}^{m} n_i$. □

A seguir será feita a construção do Exemplo 3.20, utilizando as ferramentas desenvolvidas acima. Considere o corpo finito $\mathbb{F}_2$ e $I_2 = (X_1^2 - X_1, \ldots, X_m^2 - X_m) \subset \mathbb{F}_2[\mathbf{X}]$ o ideal polinomial que se anula em todos pontos $P_1, \ldots, P_{2^m}$ do espaço afim $\mathbb{A}(\mathbb{F}_2)$. A Proposição 3.25, garante que $\varphi : \mathbb{F}_2[\mathbf{X}]/I_2 \to \mathbb{F}_2^{2^m}$ dada por $\varphi(f + I_q) = (f(P_1), \ldots, f(P_{2^m}))$ é uma transformação linear entre $\mathbb{F}_2$-espaços vetoriais.

Exemplo 3.39 (Reed-Muller)**.** *O código de Reed-Muller de Primeira Ordem é definido como o seguinte conjunto $RM(m, 1) = \{\varphi(f + I_2) \mid f = 0$ ou $\deg(f) = 1\}$.*

*Observe que esse é o mesmo código definido no Exemplo 3.20. De fato, por definição o código é gerado pela avaliação das classes de $\{1 + I_2, X_1 + I_2, \ldots, X_m + I_2\}$ nos pontos de $\mathbb{F}_2^m$. Ordenando esse pontos de modo que o ponto com todas as coordenadas nulas seja o último, obtemos a matriz geradora descrita no Exemplo 3.20. Na notação introduzida acima, temos que esse código seria o $C_2(\mathbb{F}_2^m, (1, \ldots, 1))$. Usando os resultados acima vemos que o $RM(m, 1)$ tem os seguintes parâmetros: o **comprimento** é 2^m, a **dimensão** é $m + 1$ e a **distância mínima** é 2^{m-1}.*

O resto desta seção é dedicado a provar que o dual do código cartesiano $C_k(\mathcal{A}, v)$ é $C_{k'}(\mathcal{A}, v')$ onde $k' := \sum_{i=1}^{m}(n_i - 1) - k + 1$ e v' será descrito abaixo. Com essa finalidade, o seguinte resultado se faz útil.

Lema 3.40. *Seja $k' = \sum_{i=1}^{m}(n_i - 1) - k + 1$. Então $\dim(C_k(\mathcal{A}, v)) + \dim(C_{k'}(\mathcal{A}, v)) = n_1 \cdots n_m$.*

Demonstração. Observe que a dimensão de $C_k(\mathcal{A}, v)$ dada no Teorema 3.36 é o número de soluções inteiras da seguinte desigualdade

$$x_1 + \cdots + x_m \leq k - 1, \text{ com } 0 \leq x_i \leq n_i - 1 \text{ para } i \in \{1, \ldots, m\} \tag{3.4}$$

O número de soluções interiras da desigualdade

$$y_1 + \cdots + y_m > k-1, \text{ com } 0 \leq y_i \leq n_i - 1 \text{ para } i \in \{1, \ldots, m\} \tag{3.5}$$

onde $y_i = n_i - 1 - x_i$ para todo $i \in \{1, \ldots, m\}$, é o mesmo número de soluções inteiras da desigualdade

$$x_1 + \cdots + x_m < \sum_{i=1}^{m}(n_i - 1) - k + 1 = k', \text{ onde } 0 \leq x_i \leq n_i - 1 \text{ para todo } i \in \{1, \ldots, m\} \tag{3.6}$$

que é a dimensão de $C_{k'}(\mathcal{A}, v)$. Por outro lado, dada uma m-upla de inteiros $(\alpha_1, \ldots, \alpha_m)$, onde $0 \leq \alpha_i \leq n_i - 1$ para todo $i = 1, \ldots, m$, é claro que ou $\sum_{i=1}^{m} \alpha_i \leq k-1$ ou $\sum_{i=1}^{m} \alpha_i > k-1$, logo o número de soluções inteiras de (3.4) somado ao número de soluções inteiras de (3.5) é igual a $n_1 \cdots n_m$, e o resultado segue. □

Chegamos ao resultado principal desta seção.

Teorema 3.41. *Seja* $\mathbf{a_1}, \ldots, \mathbf{a_n}$ *pontos do conjunto Cartesiano* $\mathcal{A} = A_1 \times \cdots \times A_m$. *O dual de* $C_k(\mathcal{A}, v)$ *é*

$$C_k(\mathcal{A}, v)^{\perp} = C_{k'}(\mathcal{A}, v'),$$

onde $k' = \sum_{i=1}^{m}(n_i - 1) - k + 1$ *e* v' *é dado por* $v_i' := (v_i L_{\mathbf{a_i}}(\mathbf{a_i}))^{-1}$.

Demonstração. Seja $f(\mathbf{X})$ um elemento de $S_{<k}$ tal que $\deg_{X_i}(f(\mathbf{X})) < n_i$ para $i \in \{1, \ldots, m\}$ e seja $g(\mathbf{X})$ um elemento de $S_{<k'}$ tal que $\deg_{X_i} < n_i$ para $i \in \{1, \ldots, m\}$. Pelo algoritmo da divisão em S, existem $f_1(\mathbf{X}), \ldots, f_m(\mathbf{X}), r(\mathbf{X}) \in S$ tal que

$$f(\mathbf{X})g(\mathbf{X}) = \sum_{i=1}^{m} f_i(\mathbf{X})L_i(X_i) + r(\mathbf{X}),$$

onde $\deg_{X_i}(r(\mathbf{X})) < n_i$ para $i \in \{1, \ldots, m\}$ e

$$\deg(r(\mathbf{X})) \leq \deg(f(\mathbf{X})g(\mathbf{X})) \leq k - 1 + k' - 1 = \sum_{i=1}^{m}(n_i - 1) - 1. \tag{3.7}$$

Observe que $r(\mathbf{a}) = (fg)(\mathbf{a})$ para todo $\mathbf{a} \in \mathcal{A}$. Então, usando os comentários que estão logo após a prova da Proposição 3.34, e que culminam na equação 3.3 temos que

$$r(\mathbf{X}) = \sum_{\mathbf{a} \in \mathcal{A}} \frac{L_{\mathbf{a}}(\mathbf{X})}{L_{\mathbf{a}}(\mathbf{a})}(fg)(\mathbf{a}). \tag{3.8}$$

Da definição de $L_{\mathbf{a}}(\mathbf{X})$, $\mathbf{a} \in \mathcal{A}$, vem que o coeficiente do monômio de grau $\sum_{i=1}^{m}(n_i - 1)$ do lado direito (3.8) é dado por

$$\sum_{\mathbf{a} \in \mathcal{A}} \frac{(fg)(\mathbf{a})}{L_{\mathbf{a}}(\mathbf{a})} = \sum_{\mathbf{a} \in \mathcal{A}} \frac{f(\mathbf{a})g(\mathbf{a})}{L_{\mathbf{a}}(\mathbf{a})} = \sum_{\mathbf{a} \in \mathcal{A}} \frac{v_{\mathbf{a}} f(\mathbf{a})g(\mathbf{a})}{v_{\mathbf{a}} L_{\mathbf{a}}(\mathbf{a})} = \tag{3.9}$$

$$= (v_{\mathbf{a_1}} f(\mathbf{a_1}), \ldots, v_{\mathbf{a_n}} f(\mathbf{a_n})) \cdot \left(\frac{g(\mathbf{a_1})}{v_{\mathbf{a_1}} L_{\mathbf{a_1}}(\mathbf{a_1})}, \ldots, \frac{g(\mathbf{a_n})}{v_{\mathbf{a_n}} L_{\mathbf{a_n}}(\mathbf{a_n})} \right) \tag{3.10}$$

Por (3.7) $\deg(r(\mathbf{X})) < \sum_{i=1}^{m}(n_i - 1)$ então o coeficiente do monômio de grau $\sum_{i=1}^{m}(n_i - 1)$ do lado esquerdo de (3.8) é 0. Assim, o produto escalar mostrado em (3.10) é 0.
O lado esquerdo do produto escalar dado em (3.8) é um elemento arbitrário de $C_k(\mathcal{A}, v)$ e o lado direito do produto escalar da equação (3.8) é um elemento arbitrário de $C_{k'}(\mathcal{A}, v')$. Assim, a demonstração está completa, pois $\dim(C_{k'}(\mathcal{A}, v')) = \dim(C_{k'}(\mathcal{A}, v)) = \dim(C_k(\mathcal{A}, v)^{\perp})$ onde a última igualdade segue do Lema 3.40. □

Capítulo 4

Códigos Cartesianos LCD

4.1 Códigos Lineares LCD

Relembramos que um código linear C de dimensão k e comprimento n é um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q^n$ de dimensão k e a matriz geradora de C é qualquer matriz cuja as linhas formam uma base para C. Lembramos ainda que dois vetores $u, v \in \mathbb{F}_q$ são ortogonais se $u \cdot v = 0$ e por fim, que o código dual de C é $C^\perp := \{u \in \mathbb{F}_q^n \mid c \cdot u = 0 \text{ para todos } c \in C\}$.

Observamos que, ao contrário do que acontece com espaços vetoriais definidos sobre o corpo dos números reais, quando o corpo dos escalares é finito pode acontecer de termos $C \cap C^\perp \supsetneqq \{0\}$. Por exemplo, sena C o subespaço de $\mathbb{F}_2^2$ gerado por $(1,1)$, temos que $\dim(C) = 1 = \dim(C^\perp)$ e como $(1,1) \cdot (1,1) = 0$ temos $C = C^\perp$.

Definição 4.1. *Um código linear C sobre um corpo $\mathbb{F}_q$ é dito um* ***código linear com dual complementar*** *ou simplesmente, um* ***código LCD*** *se $C \cap C^\perp = \{0\}$.*

Lema 4.2. *Um código linear $C \subset \mathbb{F}_q^m$ é LCD se e só se existe uma aplicação linear $\Pi_C : \mathbb{F}_q^m \to C$ tal que $\Pi_C(w) = w$ para todo $w \in C$ e cujo núcleo seja $C^\perp$.*

Demonstração. Se $C \cap C^\perp = \{0\}$, como $\dim(C^\perp) = m - \dim(C)$ temos $\mathbb{F}_q^m = C \oplus C^\perp$, logo todo $u \in \mathbb{F}_q^m$ se escreve de maneira única como $u = w + w^\perp$ com $w \in C$ e $w^\perp \in C^\perp$, e definindo $\Pi_C(u) := w$ para todo $u \in \mathbb{F}_q^m$ temos que Π_C é linear, tem C como imagem e $C^\perp$ como núcleo.

Por outro lado, é claro que dada uma transformação linear Π_C como no enunciado temos que ter $C \cap C^\perp = \{0\}$. □

Uma transformação Π_C como a do enunciado acima, quando existe, é chamada de *projeção orotogonal sobre C*.

Em [11] é apresentada uma maneira para caraterizar se um código é LCD a partir de sua matriz geradora.

Proposição 4.3. *Seja $C \subset \mathbb{F}_q^m$ um código de dimensão k. Se G é a matriz geradora de um código linear C, então C código é LCD se, e somente se, a matriz GG^t (quadrada, de tamanho $k \times k$) é não singular. Mais ainda, se C é um código LCD, então a aplicação linear Π dada por*

$$u \mapsto u\left(G^t(GG^t)^{-1}G\right)$$

é a projeção ortogonal sobre C (no produto acima v é visto como um vetor linha).

Demonstração. Suponha que GG^t é não singular. Observe que para todo $u \in \mathbb{F}_q^m$ temos $u\left(G^t(GG^t)^{-1}G\right) = \left(uG^t(GG^t)^{-1}\right)G \in C$.

Dado $w \in C$, isto é, se $w = uG$ para algum u, temos que

$$w\left(G^t(GG^t)^{-1}G\right) = uG\left(G^t(GG^t)^{-1}G\right) = u(GG^t)(GG^t)^{-1})G = uG = w.$$

Vejamos agora que o núcleo de Π é $C^{\perp}$. Se u está no núcleo de Π então $u\left(G^t(GG^t)^{-1}G\right) = 0$ e multiplicando ambos os lados da equação, à direita, por G^t temos $(uG^t)(GG^t)^{-1})(GG^t) = 0$, logo $uG^t = 0$ e do Lema 3.10 (3) temos que $u \in C^{\perp}$. Por outro lado, se $u \in C^{\perp}$ então $uG^t = 0$ e temos $\left(uG^t(GG^t)^{-1}\right)G = (uG^t)(GG^t)^{-1}G = 0(GG^t)^{-1}G = 0$, o que completa a prova de que o núcleo de Π é $C^{\perp}$. Do Lema acima temos então que C é código LCD.

Suponha agora que GG^t é singular. Então existe um vetor não nulo $v \in \mathbb{F}_q^k$ tal que $vGG^t = 0$. Observe que vG é um vetor não nulo em C, e vamos mostrar que vG está também em $C^{\perp}$. De fato, se $w \in C$ então w pode ser escrito como $w = v'G$ para algum $v' \in \mathbb{F}_q^k$ e temos

$$(vG)w^t = (vG)(v'G)^t = vGG^t(v')^t = 0(v')^t = 0,$$

ou seja, $vG \in C^{\perp}$. Isso mostra que C não é um código LCD. □

4.2 Encontrando Códigos LCD a partir de Códigos Cartesianos

Nesta seção, apresentaremos alguns resultados sobre códigos cartesianos $C_k(\mathcal{A}, v)$ onde $\mathcal{A} = A_1 \times \cdots \times A_m \subseteq \mathbb{F}_q^m$, que são LCD. Como resultado, várias construções explícitas para códigos LCD são encontradas.

4.2.1 Código de Reed-Solomon Generalizado (caso $m = 1$)

Começaremos com o caso em que $m = 1$, significando $\mathcal{A} = A := \{a_1, \ldots, a_n\} \subseteq \mathbb{F}_q$, então $n_1 = n$. Observe que neste caso o código cartesiano $C_k(\mathcal{A}, v)$ é o código Reed-Solomon Generalizado $GSR(\mathcal{A}, v)$ apresentado em [8] e que é dado da forma

$$GSR(\mathcal{A}, v) := \{(v_1 f(a_1), \ldots, v_n f(a_n)) \mid f(X) + I_q \in \mathbb{F}_q[X]/I_q, deg(f(X)) < k\}.$$

Lembremos que $L(X) = \prod_{a \in A}(X - a)$ e $L_a(X) = \frac{L(X)}{(X-a)}$ para cada elemento $a \in A$. Pelo Teorema 3.41, temos

$$\begin{aligned} C_k(A, v)^{\perp} &= \left\{ \left(\frac{g(a_1)}{v_1 L_{a_1}(a_1)}, \ldots, \frac{g(a_n)}{v_n L_{a_n}(a_n)} \right) \mid g(X) + I_q \in \mathbb{F}_q[X]/I_q, \deg g(X) < n - k \right\} \\ &= C_{n-k}(A, v') = GRS_{n-k}(A, v'). \end{aligned}$$

Estamos interessados em encontrar condições em A e v tais que $C_k(A, v)$ seja LCD. Observe que o código cartesiano $C_k(A, v)$ não é LCD se, e somente se, houver polinômios $f(X) \in S_{<k}$ e $g(X) \in S_{<n-k}$ tais que

$$(v_1 f(a_1), \ldots, v_n f(a_n)) = \left(\frac{g(a_1)}{v_1 L_{a_1}(a_1)}, \ldots, \frac{g(a_n)}{v_n L_{a_n}(a_n)} \right).$$

Isso vale se, e somente se,

$$\left(v_1^2 L_{a_1}(a_1) f(a_1), \ldots, v_n^2 L_{a_n}(a_n) f(a_n)\right) = (g(a_1), \ldots, g(a_n)). \tag{4.1}$$

A equação (4.1) motiva a seguinte definição.

Definição 4.4. *O polinômio associado ao código $C_k(A, v)$ é dado por*

$$H(X) := \sum_{i=1}^{n} v_i^2 L_{a_i}(X). \tag{4.2}$$

Note que $H(a_i) = v_i^2 L_{a_i}(a_i)$ para todo $a_i \in A$ e $\deg(H) < n$. Observe também que $H(X)$ e $L(X)$ são coprimos em $\mathbb{F}_q[X]$, pois os únicos polinômios irredutíveis (e mônicos) que dividem $L(X)$ são os da forma $X - a_i$, com $a_i \in A$, mas $X - a \nmid H(X)$ já que $H(a_i) = v_i^2 L_{a_i}(a_i) \neq 0$.

Proposição 4.5. *O código cartesiano $C_k(A, v)$ é LCD se, e somente se, para todos polinômios não nulos $f(X) \in S_{<k}$ e $g(X) \in S_{<n-k}$ tais que*

$$H(X)f(X) - g(X) \notin \langle L(X) \rangle,$$

onde $H(X)$ é definido em (4.2).

Demonstração. A equação (4.1) vale se, e somente se $X - a_i \mid v_i^2 L_{a_i}(X) - g(X)$ para todo $a_i \in A$, e como $X - a_i$ é coprimo com $X - a_j$ se $i \neq j$, a equação vale se e somente se $L(X)$ divide $H(X)f(X) - g(X)$. □

Como $H(X)$ e $L(X)$ são coprimos, o Algoritmo Euclidiano Estendido da Divisão (veja mais detalhes em [7, Cap. 3]), existem um número natural t, polinômios $g_i(X), h_i(X)$ e $f_i(X) \in \mathbb{F}_q[X]$ com $i \in 0, \ldots, t+1$ e polinômios $q_i(X) \in \mathbb{F}_q[X]$ com $i \in \{1, \ldots, t\}$ tal que

$$g_0(X) = L(X), g_1(X) = H(X), h_0(X) = f_1(X) = 1, h_1(X) = f_0(X) = 0$$
$$g_{i-1}(X) = q_i(X)g_i(X) + g_{i+1}(X), \text{onde } \deg(g_{i+1}(X)) < \deg(g_i)(X) \forall i \in \{1, \ldots, t\}$$
$$g_i(X) = h_i(X)L(X) + f_i(X)H(X) \forall i \in \{0, \ldots, t\} \tag{4.3}$$
$$\deg(f_i(X)) = \deg(L(X)) - \deg(g_{i-1}(X)) = n - \deg(g_{i-1}(X)) \forall i \in \{1, \ldots, t\} \tag{4.4}$$
$$g_{t+1}(X) = 1$$

O que segue é a base de nossos principais resultados desta seção.

Proposição 4.6. *Seja $C_k(A, v)$ um código cartesiano e $g_0(X), \ldots, g_{t+1}(X)$ os restos Algoritmo Euclidiano Estendido obtidos dos polinômios $L(X) = \prod_{a_i \in A}(X - a_i)$ e $H(X) = \sum_{a_i \in A} v_i^2 L_{a_i}(X)$. Então, $C_k(A, v)$ é LCD se, e somente se, para todo $i \in 1, \ldots, t+1$ ocorre uma das condições a seguir*

1. $\deg g_{i-1}(X) \leq n - k$.
2. *Se* $\deg g_{i-1}(X) > n - k$ *então* $\deg g_i \geq n - k$.

Demonstração. Provaremos ambas as implicações através da contra positiva.
($\Rightarrow$) Assuma que exista $i \in 1, \ldots, t$ tal que $\deg(g_i(X)) < n - k < \deg(g_{i-1}(X))$. Então por (4.3) e (4.4), existem $f_i(X), g_i(X)$ e $h_i(X)$ em $\mathbb{F}_q[X]$ tal que $L(X)h_i(X) + H(X)f_i(X) = g_i(X)$, e $\deg(g_i(X)) < n - k$ e $\deg(f_i(X)) = n - \deg(g_{i-1}(X)) < k$. Pela Proposição 4.5, $C_k(A, v)$ não é LCD.
($\Leftarrow$) Assuma que $C_k(A, v)$ não é LCD. Pela Proposição 4.5, existem polinômios $f(X), g(X)$ e $h(X)$ em $\mathbb{F}_q[X]$ tal que $\deg(f(X)) < k$, $\deg(g(X)) < n - k$ e

$$L(X)h(X) + H(X)f(X) = g(X). \tag{4.5}$$

Seja $g_i(X)$ o resto tal que $\deg(g_i(X)) \leq \deg(g(X))$ e $\deg(g_{i-1}(X)) > \deg(g(X))$. Observe que $\deg(g_i(X)) \leq \deg(g(X)) < n - k$. Isso significa que agora só precisamos mostrar que

$\deg(g_{i-1}(X)) > n-k$. Assim, multiplicando por $g(X)$ a equação (4.3) e por $g_i(X)$ a equação (4.5), obtemos que

$$g(X)g_i(X) = g(X)\left(h_i(X)L(X) + f_i(X)H(X)\right) \tag{4.6}$$

$$g_i(X)g(X) = g_i(X)\left(L(X)h(X) + H(X)f(X)\right) \tag{4.7}$$

Subtraindo da equação (4.6) a equação (4.7) temos

$$L(X)\left(h(X)g_i(X) - h_i(X)g(X)\right) + H(X)\left(f(X)g_i(X) - f_i(X)g(X)\right) = 0.$$

Como $L(X)$ e $H(X)$ são coprimos segue que, $L(X)$ divide $f(X)g_i(X) - f_i(X)g(X)$. Além disso, segue que

$$\deg(f(X)g_i(X)) = \deg(f(X)) + \deg(g_i(X)) < \deg(f(X)) + \deg(g(X)) < n. \tag{4.8}$$

Da equação (4.4) segue que

$$\begin{aligned}\deg(f_i(X)g(X)) &= \deg(f_i(X)) + \deg(g(X)) \\ &= n - \deg(g_i(X)) + \deg(g(X)) < n - \deg(g(X)) + \deg(g(X)) = n.\end{aligned} \tag{4.9}$$

Como $L(X)$ divide $f(X)g_i(X) - f_i(X)g(X)$ e $\deg(f(X)g_i(X) - f_i(X)g(X)) < n$, temos que $f(X)g_i(X) = f_i(X)g(X)$, logo $\deg(f_i(X)) = \deg(f(X)) + \deg(g_i(X)) - \deg(g(X))$. Da equação (4.4) temos que $\deg(g_{i-1}(X)) = n - \deg(f_i(X)) = n - (\deg(f(X)) + \deg(g_i(X)) - \deg(g(X))) > n-k$, completando a demonstração.

□

O teorema a seguir é o principal resultado desta seção e seguirá diretamente como um corolário da Proposição 4.6.

Teorema 4.7. *Seja $C_k(A,v)$ um código cartesiano e $g_0(X), \ldots, g_{t+1}(X)$ os restos do Algoritmo Euclidiano Estendido aplicado aos polinômios $L(X) = \prod_{a_i \in A}(X - a_i)$ e $H(X) = \sum_{a_i \in A} v_i L_{a_i}(X)$. Então, $C_k(A,v)$ é LCD se, e somente se*

$$n - k \in \{n, n-1, n-2, \ldots, \deg(g_1(X)), \ldots, \deg(g_{t+1}(X))\}.$$

Demonstração. Segue diretamente da Proposição 4.6. □

4.2.2 Códigos Cartesianos afins (caso $m > 1$)

Sejam $a_1, \ldots, a_n$ os pontos do conjunto cartesiano $\mathcal{A} = A_1 \times \cdots \times A_m$. Pelo Teorema 3.41, o dual de $C_k(\mathcal{A}, v)$ é dado por

$$C_k(\mathcal{A}, v)^{\perp} = C_{k'}(\mathcal{A}, v'),$$

onde $k' = \sum_{i=1}^{m}(n_i - 1) - k + 1$ e v' é definido por $v_i' := v_i^{-1} L_{a_i}(a_i)^{-1}$ para todo $i = 1, \ldots, n$. Assim o código cartesiano $C_k(\mathcal{A}, v)$ não é LCD se, e somente se, exitem polinômios $f(X) \in S_{<k}$ e $g(\mathbf{X}) \in S_{<k'}$ tais que

$$(v_1 f(a_1), \ldots, v_n f(a_n)) = \left(\frac{g(a_1)}{v_1 L_{a_1}(a_1)}, \ldots, \frac{g(a_n)}{v_n L_{a_n}(a_n)}\right). \tag{4.10}$$

A equação (4.10) vale se, e somente se,

$$v_i^2 L_{a_i}(a_i) f(a_i) = g(a_i) \text{ para todo } a_i \in \mathcal{A} \tag{4.11}$$

O polinômio associado a $C_k(\mathcal{A}, v)$ é definido por

$$H(\mathbf{X}) := \sum_{a_i \in \mathcal{A}} v_i^2 L_{a_i}(\mathbf{X}) \tag{4.12}$$

Observação 4.8. *Algumas propriedades importantes do polinômio associado ao código cartesiano $C_k(\mathcal{A}, v)$.*

1. *Para todo $a_i \in \mathcal{A}$, $H(a_i) = v_i^2 L_{a_i}(a_i)$.*
2. *$\deg_{\boldsymbol{X}_i}(H(\boldsymbol{X})) < n_i$ para todo $i \in 1, \ldots, m$.*
3. *Se $G(\boldsymbol{X})$ é um elemento de $\mathbb{F}_q[\boldsymbol{X}]$ que satisfaz 1 e 2, então $G(\boldsymbol{X}) = H(\boldsymbol{X})$.*

Os fatos (1) e (2) vêm da definição dos polinômios $L_{a_i}(\boldsymbol{X})$, enquanto (3) vem da equação (3.3) *e dos comentários que a precedem.*

A partir disso, obtemos a seguinte caracterização para os códigos LCD.

Proposição 4.9. *O código Cartesiano $C_k(\mathcal{A}, v)$ é LCD se, e somente se, para todos os polinômios diferentes de zero $f(\boldsymbol{X}) \in S_k$ e $g(\boldsymbol{X}) \in S_{<k'}$ temos que*

$$H(\boldsymbol{X})f(\boldsymbol{X}) - g(\boldsymbol{X}) \in I_q, \tag{4.13}$$

onde $H(\boldsymbol{X})$ é o polinômio associado a $C_k(\mathcal{A}, v)$ definido em (4.12).

Demonstração. A equação (4.11) vale se, e somente se, $(Hf - g)(\mathbf{X})$ se anula em todos os pontos de $\mathcal{A}$, ou seja, se e só se $(Hf - g)(\mathbf{X}) \in I_q$. □

Em seguida, nos concentramos em uma família especial de códigos cartesianos.

Definição 4.10. *Para $i \in \{1, \ldots, m\}$, escreva $A_i := \{a_{i1}, \ldots, a_{in_i}\} \subseteq \mathbb{F}_q$ e seja $v_i := (v_{i1}, \ldots, v_{in_i}) \in (\mathbb{F}_q^*)^{n_i}$. O vetor Cartesiano $v_1 \times \cdots \times v_m \in \mathbb{F}_q^n$ é definido como um vetor de comprimento $n := n_1 \cdots n_m$ com*

$$(v_1 \times \cdots \times v_m)_{\boldsymbol{a}} := v_{1j_1} \cdots v_{mj_m} \text{ onde } \boldsymbol{a} = (a_{1j_1}, \ldots, a_{mj_m}).$$

Teorema 4.11. *Se $k < min\{n_i \mid i \in \{1, \ldots, m\}\}$ e $C_k(\mathcal{A}, v_1 \times \cdots \times v_m)$ é LCD, então $C_k(A_i, v_i)$ é LCD para todo $i \in \{1, \ldots, m\}$.*

Demonstração. Se existe $i \in \{1, \ldots m\}$ tal que $C_k(A_i, v_i)$ não é LCD, pela proposição 4.5, existem polinômios $f(X_i), g(X_i)$ e $h(X_i) \in \mathbb{F}[\mathbf{X}]$ tais que $\deg(f(X_i)) < k$ e $\deg(g(X_i)) < n_i - k$ e

$$L_i(X_i)h(X_i) + H_i(X_i)f(X_i) = g(X_i).$$

Para $j \neq i$, seja $H_j(X_j)$ um polinômio associado a $C_k(A_j, v_j)$ definida na equação (4.12). E a seguinte equação vale

$$f(X_i) \cdot \prod_{j=1}^{m} H_j(X_j) = g(X_i) \prod_{j=1 j \neq i}^{m} (H_j(X_j)) \mod L_i(X_i).$$

Observe que $\deg(g(X_i) \prod_{j=1 j \neq i}^{m}(H_j(X_j))) < \sum_{i=1}^{m}(n_i - 1) - k + 1$. Veja que pela Observação 4.8 condição 3 o polinômio $\prod_{j=1}^{m} H_j(X_j)$ é o polinômio associado a $C_k(\mathcal{A}, \mathbf{v_1} \times \cdots \times \mathbf{v_m})$, e pela Proposição 4.5 a tese segue. □

Teorema 4.12. *Se todos os códigos cartesianos $C_{t_1}(A_1, v_1), \ldots, C_{t_m}(A_m, v_m)$ não são LCD, então o código cartesiano $C_{t_1+\cdots+t_m}(\mathcal{A}, v_1 \times \cdots \times v_m)$ não é LCD.*

Demonstração. Assuma para todo $i \in \{1, \ldots, m\}$ que $C_{t_i}(A_i, \mathbf{v_i})$ não é LCD. Pela Proposição 4.5 existem polinômios $f_i(X_i), g_i(X_i)$ e $h_i(X_i) \in \mathbb{F}_q[X_i]$ tais que $\deg(f_i(X_i)) < t_i, \deg(g_i(X_i)) \leq n_i - 1 - t_i$ e

$$L_i(X_i)h_i(X_i) + H_i(X_i)f_i(X_i) = g_i(X_i) \text{ para } i \in \{1, \ldots, m\}, \tag{4.14}$$

onde $H_i(X_i)$ é o polinômio associado a $C_{t_i}(A, \mathbf{v_i})$ definido na Equação (4.2). Multiplicando todas as m equações pela Equação (4.14), obtemos a seguinte expressão

$$L(\mathbf{X})G(\mathbf{X}) + H(\mathbf{X})f_1(X_1)\cdots f_m(X_m) = g_1(X_1)\cdots g_m(X_m), \tag{4.15}$$

onde $L(\mathbf{X}) \in I$ e pela Observação 4.8, temos que $H(\mathbf{X}) = H(X_1)\cdots H(X_m)$ é o polinômio associado a $C_{t_1+\cdots+t_m}(\mathcal{A}, v_1 \times \cdots \times v_m)$. Além disso, observe que $\deg(f_1(X_1)\cdots f_m(X_m)) < t_1 + \cdots + t_m$ e $\deg(g_1(X_1)\cdots g_m(X_m))\sum_{i=1}^{m}(n_i - 1) - (t_1 + \cdots + t_m)$. Pela Proposição 4.9 o resultado segue. □

Referências Bibliográficas

[1] Alon, N. Combinatorial nullstellensatz. Combinatorics, Probability and Computing. Cambridge University Press. V 8, N 1-2, Pags 7 -29, 1999.

[2] Becker, Thomas e Weispfenning, Volker. Gröbner bases. Springer, 1993.

[3] Carvalho, C. Applications of results from commutative algebra to the study of certain evaluation codes, Lecture notes of CIMPA Research School on Algebraic Methods in Coding Theory, Sao Paulo, Brazil, July 2017.

[4] Cox, David e Little, John e O'Shea, Donal. Springer, 2013.

[5] Fitzgerald, Jeanne and Lax, Robert F. Decoding affine variety codes using Gröbner bases. Designs, Codes and Cryptography, Springer, V 13, Pags 147–158, 1998.

[6] Garcia, Arnaldo e Lequain, Yves. Elementos de álgebra. Instituto de Matemática Pura e Aplicada, 2006.

[7] Gathen, J. von zur; Gerhard, J. Modern Computer Algebra, third edition, Cambridge University Press, 2013.

[8] Hefez, Abramo and Villela, Maria Lúcia T. Códigos corretores de erros. Instituto de Matematica Pura e Aplicada, 2008.

[9] Lidl, Rudolf e Niederreiter, Harald. Introduction to finite fields and their applications. Cambridge university press, 1994.

[10] López, Hiram H e Manganiello, Felice e Matthews, Gretchen L. Affine Cartesian codes with complementary duals. Elsevier, Finite Fields and Their Applications, V 57, Pags 13-28, 2019.

[11] Massey, James L. Linear codes with complementary duals. Elsevier, Discrete Mathematics, V 106 Pags 337–342, 1992.