TIAGO APRIGIO BEZERRA MEIRELES

Pesos de Hamming generalizados em códigos de avaliação

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2023

TIAGO APRIGIO BEZERRA MEIRELES

Pesos de Hamming generalizados em códigos de avaliação

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

Área de Concentração: Matemática.
Linha de Pesquisa: Teoria de códigos algébricos geométricos.

Orientador: Prof. Dr. Cicero Fernandes de Carvalho.

UBERLÂNDIA - MG
2023

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

M514
2023

Meireles, Tiago Aprigio Bezerra, 1999-
Pesos de Hamming generalizados em códigos de avaliação [recurso eletrônico] / Tiago Aprigio Bezerra Meireles. - 2023.

Orientador: Cicero Fernandes de Carvalho.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2023.27
Inclui bibliografia.
Inclui ilustrações.

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

CDU: 51

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

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
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, 106, PPGMAT				
Data:	17 de fevereiro de 2023	Hora de início:	16:00	Hora de encerramento:	18:00
Matrícula do Discente:	12112MAT013				
Nome do Discente:	Tiago Aprigio Bezerra Meireles				
Título do Trabalho:	Pesos de Hamming generalizados em códigos de avaliação				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Sobre pesos de Hamming de ordem superior em códigos projetivos de Reed-Muller				

Reuniu-se em webconferência pela plataforma Mconf-RNP, em conformidade com a PORTARIA Nº 36, DE 19 DE MARÇO DE 2020 da COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR - CAPES, pela Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Herivelto Martins Borges Filho - ICMC/USP; Guilherme Chaud Tizziotti - 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 ao Discente a palavra para a exposição do seu trabalho. A duração da apresentação do Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

A seguir o senhor(a) presidente concedeu a palavra, pela ordem sucessivamente, aos(às) examinadores(as), que passaram a arguir o(a) candidato(a). Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o(a) candidato(a):

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 **Herivelto Martins Borges Filho**, **Usuário Externo**, em 17/02/2023, às 17:04, 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 17/02/2023, às 17:16, 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 **Guilherme Chaud Tizziotti**, **Professor(a) do Magistério Superior**, em 17/02/2023, às 17:18, 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 **4249146** e o código CRC **AA1B96E1**.

Dedicatória

A meus pais Joaquim e Lourdes, que estiveram sempre comigo me dando suporte e conselhos, e aos meus irmãos Daniel e Marcos.

A minha noiva Julia, que esteve ao meu lado me apoiando e me incentivando durante todo o mestrado.

Aos meus colegas e professores de mestrado.

"Mas, buscai primeiro o reino de Deus, e a sua justiça, e todas estas coisas vos serão acrescentadas."

Mateus 6:33

Agradecimentos

Agradeço, primeiramente, a Deus, pois sem a Sua graça e o Seu cuidado eu não teria chegado onde cheguei. Por ter me dado forças, paciência e coragem durante todo o mestrado.

Agradeço também aos meus pais, por todos os conselhos, pelo carinho, pelo cuidado e pelo suporte.

Agradeço aos meus irmãos pela companhia e cumplicidade.

Não posso deixar de agradecer a minha noiva Julia, que foi a pessoa que acompanhou mais de perto todo esse processo, agradeço pelo seu amor, pelo carinho, por todos os conselhos e por ter me motivado a estudar mais.

Ao meu orientador, professor Cicero Fernandes de Carvalho, primeiramente, por ter aceitado a me orientar neste trabalho e também agradeço por todos os conselhos que você me deu durante esse período de mestrado.

Agradeço aos meus colegas de mestrado, Lucas, Juan, Thiago, Michel, Ricardo, Augusto, João, Laurienny, pela amizade e pelos momentos de estudos na sala do mestrado.

Agradeço a todos os professores da banca, titulares e suplentes, por terem aceito o convite para participar da banca examinadora deste trabalho.

Agradeço a CAPES, pela bolsa e pela oportunidade de participar deste programa de mestrado.

Agradeço todos aqueles que me ajudaram de forma direta ou indireta na minha formação acadêmica.

Muito obrigado a todos vocês!

MEIRELES, T. A. B. *Pesos de Hamming generalizados em códigos de avaliação.* 2023. (52 pág) p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho, realizamos o estudo do r-ésimo peso de Hamming generalizado de alguns códigos de avaliação. Introduzimos os códigos cartesianos afins, códigos do tipo Reed-Muller, códigos tóricos e códigos afins livres de quadrados. Utilizando relações entre variedades afins e a pegada de um ideal, foi possível calcular (ou dar cotas inferiores de) alguns parâmetros desses códigos, a saber, distância mínima, dimensão e o r-ésimo peso de Hamming generalizado. Finalizamos essa dissertação aplicando algumas propriedades de códigos de avaliação mostradas anteriormente e técnicas utilizando a pegada de um ideal, para calcular o segundo peso de Hamming generalizado de um código afim livre de quadrados.

Palavras-chave: Códigos de Avaliação, Pegada, r-ésimo peso de Hamming Generalizado e Bases de Gröbner.

MEIRELES, T. A. B. *Generalized Hamming weights in evaluation codes.* 2023. (52 pages) p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work, we study the r-th generalized Hamming weight of some evaluation codes. We introduce affine Cartesian codes, Reed-Muller type codes, toric codes and squarefree affine codes. Using relationships between affine varieties and the footprint of an ideal, it was possible to determine (or give lower bounds for) some parameters of these codes, namely, minimum distance, dimension and the r-th generalized Hamming weight. We finish this dissertation by applying some previously shown properties of evaluation codes and techniques using the footprint of an ideal, to determine the second generalized Hamming weight of a squarefree affine code.

Keywords: Evaluation Codes, Footprint, r-th Generalized Hamming Weight and Gröbner Basis.

Sumário

Introdução

O objeto principal deste trabalho é o código corretor de erros. Um código corretor de erros é um subconjunto de A^n, em que A é um conjunto finito qualquer, $n \in \mathbb{N}$ e A^n é o produto cartesiano de A, n vezes. Hoje em dia, os códigos corretores de erros são utilizados sempre que se deseja transmitir ou armazenar dados, garantindo a sua confiabilidade. Suponha que um emissor deseja enviar uma mensagem para alguém (seu receptor), para isso é necessário que a mensagem seja codificada, após a codificação, essa mensagem passa por algum canal de comunicação, depois é necessário decodificar o código e assim, a mensagem original chega ao receptor. Contudo, pode ocorrer algum "ruído" nesse processo e assim, o receptor receberá a mensagem com erros. No entanto, como mostramos no Teorema 2.5, o código pode corrigir até $\kappa := \left\lfloor \frac{\delta(\mathcal{C})-1}{2} \right\rfloor$ erros, onde $\delta(\mathcal{C})$ é a distância mínima do código, e detectar até $\delta(\mathcal{C})-1$ erros. Assim, é muito importante conhecer o (ou obter cotas inferiores do) parâmetro distância mínima de um código, pois quanto maior for a distancia mínima maior será a capacidade de correção de erros do código. Neste texto vamos trabalhar, mais especificamente, com códigos lineares que são subespaços vetoriais de $\mathbb{F}_q^n$, onde $\mathbb{F}_q$ é o corpo finito com q elementos e q é uma potência de um número primo. Este trabalho foi realizado tendo como base o artigo *Evaluation codes and their basic parameters* cujos autores são Rafael H. Villareal, Delio Jaramillo e Maria Vaz Pinto [9]. Entretanto, foi feita uma adaptação nas demonstrações da maioria dos resultados apresentados do artigo base, e para realizar essas adaptações foram utilizadas técnicas envolvendo a pegada de um ideal.

O conceito de distância mínima pode ser generalizado, e essa generalização é chamada de pesos de Hamming generalizados. O conceito r-ésimo peso de Hamming generalizado de um código linear inicialmente foi introduzido pelo engenheiro elétrico Victor K. Wei apresentado no artigo *Generalized Hamming weights for linear codes* [11].

No primeiro capítulo, apresentaremos alguns resultados e conceitos preliminares necessários para trabalharmos com a teoria do artigo base, tais como os conceitos de ordem monomial, bases de Gröbner, pegada de um ideal e varidades afins, o algoritmo da divisão para polinômios de várias variáveis e uma relação entre variedades afins e a pegada de um ideal.

No segundo capítulo, é feito um estudo sobre códigos lineares, lá apresentamos alguns resultados básicos de códigos (um deles é a famosa cota de Singleton) para o leitor se familiarizar com esse objeto e se acostumar com as notações utilizadas nessa teoria. Neste mesmo capítulo introduziremos os códigos cartesianos afins, apresentaremos alguns resultados, que envolve esse tipo de código, produzidos no artigo [10], contudo, as demonstrações de alguns desses resultados foram simplificadas (conforme [3]) utilizando a pegada de um ideal.

No terceiro capítulo, é introduzido o conceito principal da dissertação, a saber, o r-ésimo peso de Hamming Generalizado para códigos lineares. Neste capítulo apresentaremos alguns resultados feitos no artigo de Victor K. Wei [11] envolvendo esse conceito. Introduziremos os códigos de avaliação e calcularemos uma fórmula e uma cota inferior para o r-ésimo peso de Hamming generalizado de códigos de avaliação. Prosseguiremos nosso estudo com alguns códigos particulares de avaliação, a saber, códigos do tipo Reed-Muller, códigos tóricos e códigos afins livres de quadrados, e apresentaremos resultados envolvendo os parâmetros básicos e o

r-ésimo peso de Hamming generalizado desses códigos.

Tiago Aprigio Bezerra Meireles
Uberlândia-MG, 17 de fevereiro de 2023.

Capítulo 1

Conceitos Básicos

1.1 Ordem Monomial e o Algoritmo da Divisão para Polinômios de Várias Variáveis

Definição 1.1. Seja $\mathbb{K}$ um corpo e seja $\mathbb{K}[\mathbf{X}]$ o anel de polinômios $\mathbb{K}[X_1, \ldots, X_n]$. Um **termo** em $X_1, X_2, \ldots, X_n$ é um produto da forma $aX_1^{\alpha_1}X_2^{\alpha_2}\cdots X_n^{\alpha_n}$, em que $a \in \mathbb{K}^*$ e $\alpha_1, \ldots, \alpha_n$ são inteiros não negativos. Quando $a = 1$, $X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_n^{\alpha_n}$ é chamado de **monômio**, e por vezes será denotado por $\mathbf{X}^{\boldsymbol{\alpha}}$ (ou $\mathbf{X}^{\boldsymbol{\beta}}$, $\mathbf{X}^{\boldsymbol{\gamma}}$, etc), onde $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ e $\mathbb{N}_0$ é o conjunto dos inteiros não negativos.

Quando estamos dividindo polinômios em $\mathbb{K}[X]$ percebemos que a ordenação dos termos do polinômio é um ingrediente chave para realizar tal divisão. Por exemplo, na divisão de $p(X) = X^4 + 3X^3 - 7X + 10$ por $q(X) = X^2 + 6X + 6$ pelo método padrão, é usual seguir as seguintes etapas:

- Escrever os termos dos polinômios em ordem decrescente, ordenando-os com base na ordem de cada monômio ($1 < X < X^3 < X^4$ e $1 < X < X^2$).
- Encontrar os termos líderes, ou seja, o termo de maior grau de p e q. No nosso exemplo, o termo líder de p é $X^4 = X^2 \cdot X^2 = X^2\cdot$ (termo líder de q).
- Subtrair $X^2 \cdot q(X)$ de p para eliminar o termo líder, obtendo $-3X^3 - 6X^2 - 7X + 10$.
- Repetir o mesmo processo em $p(X) - X^2 \cdot q(X)$, etc., até obtermos um polinômio que é nulo ou tem grau menor do que 2 (resto).

No algoritmo da divisão para polinômios de uma variável, estamos lidando com ordenação de grau dos monômios de uma variável, ou seja:

$$X_1^{\alpha_1} \preccurlyeq X_1^{\beta_1}, \text{ se } \alpha_1 \leq \beta_1.$$

Veremos como generalizar esse processo para polinômios em mais de uma variável.

Definição 1.2. Escrevemos $\mathcal{M}$ para denotar o **conjunto dos monômios** de $\mathbb{K}[\mathbf{X}]$. Dado $f \in \mathbb{K}[\mathbf{X}]$ dizemos que $M \in \mathcal{M}$ aparece em f se o coeficiente de M não é nulo.

Definição 1.3. Uma **ordem monomial** em $\mathcal{M}$ é uma ordem total $\preccurlyeq$ definida sobre $\mathcal{M}$ tal que:

i) Se $\mathbf{X}^{\alpha} \preccurlyeq \mathbf{X}^{\beta}$, então $\mathbf{X}^{\alpha+\gamma} \preccurlyeq \mathbf{X}^{\beta+\gamma}$, para todos $\alpha, \beta, \gamma \in \mathbb{N}_0^n$.

ii) Qualquer subconjunto $A \subset \mathcal{M}$ tem um menor elemento, em outras palavras, se $A \subset \mathcal{M}$ é não vazio, então existe $M_1 \in \mathcal{M}$ tal que $M_1 \preccurlyeq M$ para todo $M \in \mathcal{M}$.

Exigir que $\preccurlyeq$ seja uma ordem total significa que quaisquer monômios M_1 e M_2 são comparáveis, i.e., $M_1 \preccurlyeq M_2$ ou $M_2 \preccurlyeq M_1$. Vale a pena observar, que é possível mostrar que as condições (i) e (ii) da definição acima são equivalentes às condições (i) e (ii'), onde (ii') diz que o monômio 1 é o menor elemento de $\mathcal{M}$.

Lema 1.4. *A condição que a relação seja bem-ordenada (item (ii)) é equivalente a exigir que toda sequência estritamente decrescente em* $\mathcal{M}$

$$\cdots \preccurlyeq M_3 \preccurlyeq M_2 \preccurlyeq M_1, \text{ com } M_i \neq M_{i+1},$$

eventualmente termina.

Demonstração. Veja em [4, Lemma 2, p.56]. □

Alguns exemplos básicos de ordens monomiais são dados a seguir.

Exemplo 1.5. [Ordem lexicográfica (com $X_n \preccurlyeq_{\text{lex}} \cdots \preccurlyeq_{\text{lex}} X_1$)] Dizemos que $\mathbf{X}^{\boldsymbol{\alpha}} \preccurlyeq_{\text{lex}} \mathbf{X}^{\boldsymbol{\beta}}$ se $\boldsymbol{\alpha} = \boldsymbol{\beta}$ ou se a primeira entrada não nula da esquerda para a direita em $\boldsymbol{\beta} - \boldsymbol{\alpha}$ é positiva. Por exemplo, temos $X_3^{3000} \preccurlyeq_{\text{lex}} X_1$ e $X_2^3 X_4^{1200} \preccurlyeq_{\text{lex}} X_2^3 X_3$.

Vamos provar que a ordem lexicográfica é uma ordem monomial. É fácil ver que tal ordem é uma ordem total. Agora, para a condição (i) é suficiente observar que para qualquer $\boldsymbol{\gamma} \in \mathbb{N}_0^n$, temos $(\boldsymbol{\beta} + \boldsymbol{\gamma}) - (\boldsymbol{\alpha} + \boldsymbol{\gamma}) = \boldsymbol{\beta} - \boldsymbol{\alpha}$. Logo, $\mathbf{X}^{\boldsymbol{\alpha}} \preccurlyeq_{\text{lex}} \mathbf{X}^{\boldsymbol{\beta}}$ se, e somente se, $\mathbf{X}^{\boldsymbol{\alpha}+\boldsymbol{\gamma}} \preccurlyeq_{\text{lex}} \mathbf{X}^{\boldsymbol{\beta}+\boldsymbol{\gamma}}$. Finalmente, dado qualquer conjunto de monômios $\{\mathbf{X}^{\boldsymbol{\alpha}}\}_{\boldsymbol{\alpha} \in A}$, vamos obter o menor elemento. Considere a seguinte sequência descendente de subconjuntos

$$A = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_n$$

definida recursivamente por $A_j = \{\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in A_{j-1} : \alpha_j$ é mínimo entre todas as j -ésimas entradas de todos elementos em $A_{j-1}\}$. Cada elemento de A_j é menor (com respeito a $\preccurlyeq_{\text{lex}}$) do que todos os elementos de $A \setminus A_j$. De fato, se $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in A_j$, então $\boldsymbol{\alpha} \in A_k$ com $k = 1, 2, \cdots, j-1$ e α_k é minímo entre todas as k-ésimas entradas de todos elementos em A_{k-1} com $k = 1, 2, \cdots j$. Então, dado $\boldsymbol{\beta} = (\beta_1, \cdots, \beta_n) \in A \setminus A_j$, ou seja, $\boldsymbol{\beta} \in A_k$ para algum $k \in \{0, \cdots, j-1\}$ logo, $\alpha_l = \beta_l$ para todo $l \leq k$ e $\alpha_{k+1} < \beta_{k+1}$, provando que a primeira entrada de $\beta - \alpha$ é positiva. Por outro lado, A_n tem um único elemento, que é, portanto, o menor elemento de A.

Exemplo 1.6. [Ordem lexicográfica graduada (com $X_n \preccurlyeq_{\text{grlex}} \cdots \preccurlyeq_{\text{grlex}} X_1$)] Dizemos que $\mathbf{X}^{\boldsymbol{\alpha}} \preccurlyeq_{\text{grlex}} \mathbf{X}^{\boldsymbol{\beta}}$ se $\boldsymbol{\alpha} = \boldsymbol{\beta}$, ou $\sum_{i=i}^{n} \alpha_i < \sum_{i=i}^{n} \beta_i$, ou se $\sum_{i=i}^{n} \alpha_i = \sum_{i=i}^{n} \beta_i$ então $\mathbf{X}^{\boldsymbol{\alpha}} \preccurlyeq_{\text{lex}} \mathbf{X}^{\boldsymbol{\beta}}$. Por exemplo, $X_1^5 X_2^2 \preccurlyeq_{\text{grlex}} X_2^{512}$ e $X_2^3 \preccurlyeq_{\text{grlex}} X_1^2 X_2$, pois o grau de X_2^3 é igual ao grau de $X_1^2 X_2$ e X_2^3 é menor do que $X_1^2 X_2$ na ordem lexicográfica do exemplo acima.

Exemplo 1.7. [Ordem lexicográfica reversa graduada (com $X_n \preccurlyeq_{\text{grevlex}} \cdots \preccurlyeq_{\text{grevlex}} X_1$)] Dizemos que $\mathbf{X}^{\alpha} \preccurlyeq_{\text{grevlex}} \mathbf{X}^{\beta}$ se $\boldsymbol{\alpha} = \boldsymbol{\beta}$, ou $\sum_{i=i}^{n} \alpha_i < \sum_{i=i}^{n} \beta_i$, ou se $\sum_{i=i}^{n} \alpha_i = \sum_{i=i}^{n} \beta_i$ então a primeira entrada da direita para a esquerda em $\boldsymbol{\beta} - \boldsymbol{\alpha}$ é negativa. Por exemplo, $X_1 X_3^2 \preccurlyeq_{\text{grlex}} X_1 X_2 X_5$, mas $X_1 X_2 X_5 \preccurlyeq_{\text{grevlex}} X_1 X_3^2$.

Agora, vamos aplicar as ordens monomiais citadas acima no polinômio $f(X_1, X_2, X_3) = X_1X_2 - 5X_1X_2X_3 + 3X_2^3 + 2X_3^2 \in \mathbb{K}[X_1, X_2, X_3]$. Com respeito a ordem lexicográfica, reordenaremos os termos de f em ordem decrescente. Neste caso, temos $f(X_1, X_2, X_3) = -5X_1X_2X_3 + X_1X_2 + 3X_2^3 + 2X_3^2$. Com respeito a ordem lexicográfica graduada, temos $f(X_1, X_2, X_3) = -5X_1X_2X_3 + 3X_2^3 + X_1X_2 + 2X_3^2$. E com respeito a ordem lexicográfica reversa graduada, temos $f(X_1, X_2, X_3) = 3X_2^3 - 5X_1X_2X_3 + X_1X_2 + 2X_3^2$.

Definição 1.8. Seja $f = \sum_{i=1}^{m} a_i M_i \in \mathbb{K}[\mathbf{X}]$ um polinômio não nulo, onde $a_i \in \mathbb{K}, a_i \neq 0$ e $M_i \in \mathcal{M}$ para todo $i = 1, \cdots, m$ e seja $\preccurlyeq$ uma ordem monomial definida sobre $\mathcal{M}$. Então, o **monômio líder** de f (com respeito a $\preccurlyeq$) é $M_\ell := \max\{M_i \mid i = 1, \cdots, m\}$, o **coeficiente líder** de f (com respeito a $\preccurlyeq$) é a_ℓ e o **termo líder** de f (com respeito a $\preccurlyeq$) é $a_\ell M_\ell$. Denotamos esses elementos por $M_\ell := \mathrm{lm}(f), a_\ell := \mathrm{lc}(f)$ e $a_\ell M_\ell := \mathrm{lt}(f)$.

Exemplo 1.9. Seja $f(X_1, X_2, X_3) = X_1X_2 - 5X_1X_2X_3 + 3X_2^3 + 2X_3^2 \in \mathbb{K}[X_1, X_2, X_3]$ como antes e consideremos a ordem lexicográfica. Então $\mathrm{lm}(f) = X_1X_2X_3$, $\mathrm{lc}(f) = -5$ e $\mathrm{lt}(f) = -5X_1X_2X_3$.

Na teoria das bases de Gröbner, a divisão de um polinômio em $\mathbb{K}[\mathbf{X}]$ por uma lista de polinômios nâo nulos em $\mathbb{K}[\mathbf{X}]$ é um procedimento muito importante e bastante utilizado, que definiremos agora.

Definição 1.10. Dividir $f \in \mathbb{K}[\mathbf{X}]$ por $\{g_1, \cdots, g_t\} \subset \mathbb{K}[\mathbf{X}] \setminus \{0\}$, com respeito a uma ordem monomial $\preccurlyeq$, significa encontrar quocientes $q_1, \cdots, q_t$ e um **resto** r em $\mathbb{K}[\mathbf{X}]$ tal que $f = q_1g_1 + \cdots + q_tg_t + r$, e $r = 0$ ou nenhum monômio que aparece em r é múltiplo de $\mathrm{lm}(g_i)$, para todo $i \in \{1, \cdots, t\}$.

O algoritmo usual para determinar os quocientes e o resto será mostrado depois de fazermos um exemplo que mostra como o algoritmo funciona na prática. A ideia básica do algoritmo é a mesma da que estamos acostumados quando dividimos dois polinômios de uma variável: vamos usar os termos líderes de $g_1, \cdots, g_t$ para cancelar o termo líder de f e dos polinômios subsequentes que aparecem nas etapas intermediárias do algoritmo da divisão. A novidade é que alguns dos termos líderes de alguns polinômios de algumas etapas intermediárias podem não ser múltiplos de $\mathrm{lt}(g_i)$ para todo $i \in \{1, \cdots, t\}$ e então movemos esses tais termos líderes para o resto de modo a continuarmos com a divisão.

Exemplo 1.11. Vamos dividir $f = X^2Y + XY^2 + Y^2 \in \mathbb{R}[X, Y]$ por $\{g_1 = Y^2 - 1, g_2 = XY - 1\} \subset \mathbb{R}[X, Y]$. Consideremos a ordem lexicográfica sobre $\mathcal{M}$ onde $(Y \preccurlyeq_{\mathrm{lex}} X)$. Primeiro, note que $\mathrm{lm}(f) = X^2Y$ não é um múltiplo de $\mathrm{lm}(g_1) = Y^2$, mas $\mathrm{lm}(f)$ é um múltiplo de $\mathrm{lm}(g_2)$ e $\mathrm{lm}(f) = X \cdot \mathrm{lm}(g_2)$. Assim, começamos a divisão escrevendo $f - Xg_2 = XY^2 + X + Y^2$. Agora, temos que $\mathrm{lm}(XY^2 + X + Y^2) = XY^2$ e XY^2 é múltiplo de $\mathrm{lm}(g_1)$ com $\mathrm{lm}(XY^2 + X + Y^2) = X \cdot \mathrm{lm}(g_1)$. Continuamos a divisão escrevendo $(f - X \cdot g_2) - X \cdot g_1 = 2X + Y^2$. Observe agora que $\mathrm{lt}(2X + Y) = 2X$ não é um múltiplo de $\mathrm{lt}(g_1)$ nem de $\mathrm{lt}(g_2)$, então vamos considerar $2X$ como parte do resto. Logo, $((f - X \cdot g_2) - X \cdot g_1) - r_1 = Y^2$, onde $r_1 = 2X$ e continuamos a divisão notando que $\mathrm{lm}(Y^2) = Y^2$ é um múltiplo de $\mathrm{lm}(g_1)$ e $\mathrm{lm}(Y^2) = 1 \cdot \mathrm{lm}(g_1)$. Daí, temos $(((f - X \cdot g_2) - X \cdot g_1) - r_1) - 1 \cdot g_1 = 1$. Finalmente, 1 não é múltiplo de $\mathrm{lm}(g_1)$ nem de $\mathrm{lm}(g_2)$, logo consideramos 1 como parte do resto. Portanto, $(((f - X \cdot g_2) - X \cdot g_1) - r_1) - 1 \cdot g_1 - r_2 = 0$, onde $r_2 = 1$, ou seja, $f = (X + 1)g_1 + Xg_2 + 2X + 1$. A figura abaixo ilustra como foi feita a divisão.

$$
\begin{array}{r|l|l}
X^2Y + XY^2 + Y^2 & Y^2 - 1, \quad XY - 1 & \text{Resto} \\
\cline{2-3}
-X^2Y + X & X + 1, \quad X & 2X + 1 \\
\cline{1-1}
XY^2 + X + Y^2 & & \\
-XY^2 + X & & \\
\cline{1-1}
2X + Y^2 & & \\
-2X & & \\
\cline{1-1}
Y^2 & & \\
-Y^2 + 1 & & \\
\cline{1-1}
1 & & \\
-1 & & \\
\cline{1-1}
0 & &
\end{array}
$$

Teorema 1.12. *(Algoritmo da divisão em $\mathbb{K}[\boldsymbol{X}]$). Seja $\preccurlyeq$ uma ordem monomial em $\mathcal{M}$, e seja $G = (g_1, \cdots, g_t)$ uma t-upla ordenada de polinômios em $\mathbb{K}[\boldsymbol{X}]$. Então todo $f \in \mathbb{K}[\boldsymbol{X}]$ pode ser escrito como*

$$f = q_1 g_1 + \cdots + q_t g_t + r,$$

onde $q_i, r \in \mathbb{K}[\boldsymbol{X}]$, e $r = 0$ ou nenhum monômio aparecendo em r é um múltiplo de $\mathrm{lm}(g_i)$, para todo $i \in \{1, \cdots, t\}$. Além disso, $\mathrm{lm}(r) \preccurlyeq \mathrm{lm}(f)$, e se $q_i g_i \neq 0$, então $\mathrm{lm}(q_i g_i) \preccurlyeq \mathrm{lm}(f)$.

Demonstração. Veja em [4, Theorem 3, p.64].

Trabalhando com exemplos observamos que a ordem dos polinômios na sequência $(g_1, \ldots, g_t)$ tem influência na determinação do resto na divisão.

Exemplo 1.13. Seja f o mesmo polinômio do Exemplo 1.11. Em tal exemplo dividimos f pela sequência $(Y^2 - 1, XY - 1)$. Agora, dividindo f pela sequência $(XY - 1, Y^2 - 1)$ e seguindo os mesmos passos feitos no Exemplo 1.11, iremos obter resto $r = X + Y + 1$ que é diferente do resto da divisão de f por $(Y^2 - 1, XY - 1)$.

Posteriormente, veremos que se $\{g_1, \cdots, g_t\}$ é uma base de Gröbner, então o resto sempre será igual, sem importar com a ordem dos elementos da lista de polinômios.

1.2 Bases de Gröbner

Em 1965, em sua tese de doutorado (veja [2]) 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 1.14. Sejam $I \subset \mathbb{K}[\mathbf{X}]$ um ideal não nulo e $\preccurlyeq$ uma ordem monomial em $\mathcal{M}$. Um conjunto $\{g_1, \cdots, g_s\} \subset I$ é uma **base de Gröbner** de I (com respeito a $\preccurlyeq$) se para todo $f \in I, f \neq 0$, temos que $\mathrm{lm}(f)$ é um múltiplo de $\mathrm{lm}(g_i)$ para algum $i \in \{1, \cdots, s\}$.

Observe que na definição de base de Gröbner de um ideal I não estamos dizendo que essa base é uma base para o ideal I. Mostraremos no Lema 1.23 que, de fato, tal base é uma base para o ideal I.

Exemplo 1.15. Seja $I = (XY - 1, Y^2 - 1) \subset \mathbb{R}[X, Y]$ e considere a ordem lexicográfica (com $Y \preccurlyeq_{\mathrm{lex}} X$) definida sobre o conjunto dos monômios de $\mathbb{R}[X, Y]$. Então, $X^2(Y^2-1) - XY(XY-1) = -X^2 + XY \in I$ e $\mathrm{lm}(-X^2 + XY) = X^2$ não é um múltiplo de $\mathrm{lm}(XY - 1) = XY$ e de $\mathrm{lm}(Y^2 - 1) = Y^2$, ou seja, $\{XY - 1, Y^2 - 1\}$ não é uma base de Gröbner de I.

Definição 1.16. Um ideal $I \subset \mathbb{K}[\mathbf{X}]$ é um **ideal monomial** se é gerado por um conjunto de monômios.

Lema 1.17. *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal monomial, e seja $f \in \mathbb{K}[\boldsymbol{X}]$. Então as seguintes condições são equivalentes:*

i) $f \in I$.

ii) Todo termo de f pertence a I.

iii) f é uma combinação $\mathbb{K}$-linear de monômios em I.

Demonstração. As implicações $(iii) \Rightarrow (ii) \Rightarrow (i)$ e $(ii) \Rightarrow (iii)$ são triviais. Provemos $(i) \Rightarrow (ii)$. Suponha que $f \in I$, como I é ideal monomial temos que $f = \sum_{i=1}^{s} h_i M_i$, para determinados monômios $M_1, \ldots, M_s$ em I, e onde $h_1, \ldots, h_s \in \mathbb{K}[\mathbf{X}]$. Se expandirmos cada h_i como uma soma de termos, vemos que todos os termos do lado direito da igualdade anterior são múltiplos de algum monômio M_i, com $i \in \{1, \ldots, s\}$. Assim, no lado esquerdo da igualdade anterior deve acontecer o mesmo, e portanto cada termo de f é múltiplo de algum monômio M_i com $i \in \{1, \ldots, s\}$. □

Teorema 1.18 (Lema de Dickson)**.** *Seja I um ideal monomial. Então I pode ser escrito da forma $I = (M_1, \ldots, M_s)$, onde $M_i \in \mathcal{M}$ para todo $i \in \{1, \ldots, s\}$.*

Demonstração. Veja em [7, Proposition 2.23]. □

Definição 1.19. Sejam $I \subset \mathbb{K}[\mathbf{X}]$ um ideal não nulo e $\preccurlyeq$ uma ordem monomial em $\mathcal{M}$. Então, denotamos por $\mathrm{lm}(I)$ o **ideal gerado pelos monômios líderes de todos os elementos não nulos de** I.

Segue diretamente da definição que $\mathrm{lm}(I)$ é um ideal monomial.

Proposição 1.20. *Sejam $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal não nulo e $\preccurlyeq$ uma ordem monomial em $\mathcal{M}$. Um conjunto $\{g_1, \ldots, g_s\} \subset I$ é uma base de Gröbner de I se, e somente se,* $\mathrm{lm}(I) = (\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s))$.

Demonstração. Suponha que $G = \{g_1, \ldots, g_s\} \subset I$ é uma base de Gröbner de I. Seja $f \in \mathrm{lm}(I)$, como $\mathrm{lm}(I)$ é um ideal monomial, temos pelo Lema 1.17 que todos os termos de f pertencem a $\mathrm{lm}(I)$, e como G é uma base de Gröbner de I, segue que f é uma soma finita de termos que estão em $(\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s))$, ou seja, $f \in (\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s))$. Agora, dado $h \in (\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s))$, como $g_i \in I$ para todo $i \in \{1, \ldots, s\}$, segue que $h \in \mathrm{lm}(I)$. Reciprocamente, seja $f \in I$, por hipótese $\mathrm{lm}(f) \in (\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s))$, então existem $M \in \mathcal{M}$ e $i \in \{1, \ldots, s\}$, tais que $\mathrm{lm}(f) = \mathrm{lm}(g_i)M$, provando que G é uma base de Gröbner de I. □

Corolário 1.21. *Seja $\preccurlyeq$ uma ordem monomial em $\mathcal{M}$. Então, todo ideal não nulo $I \subset \mathbb{K}[\boldsymbol{X}]$ tem uma base de Gröbner.*

Demonstração. Pelo Lema de Dickson (Teorema 1.18) o ideal de monômios líderes $\mathrm{lm}(I)$ pode ser escrito como $\mathrm{lm}(I) = (\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s))$, onde $g_i \in I$ para todo $i \in \{1, \ldots, s\}$. Logo, pela Proposição 1.20 $\{g_1, \ldots, g_s\}$ é uma base de Gröbner de I. □

A partir de agora, sempre que falarmos de bases de Gröbner de I deve ficar implícito que $I \subset \mathbb{K}[\mathbf{X}]$ é um ideal de $\mathbb{K}[\mathbf{X}]$ e alguma ordem monomial foi escolhida em $\mathcal{M}$. No entanto, em alguns exemplos e resultados explicitaremos qual ordem foi escolhida.

Proposição 1.22. *Seja $\{g_1, \ldots, g_s\} \subset I$ uma base de Gröbner de I. Na divisão de $f \in \mathbb{K}[\boldsymbol{X}]$ por $\{g_1, \ldots, g_s\}$ o resto é sempre o mesmo, sem considerar a ordem que escolhemos para $g_1, \ldots, g_s$ no algoritmo da divisão.*

Demonstração. Primeiro, escolha uma ordem para $g_1, \ldots, g_s$. Depois de aplicar o algoritmo da divisão para $f \in \mathbb{K}[\mathbf{X}]$ considerando tal ordem, suponha que $f = q_1 g_1 + \cdots + q_s g_s + r$, em que $q_i \in \mathbb{K}[\mathbf{X}]$ para todo $i = 1, \ldots, s$ e $r \in \mathbb{K}[\mathbf{X}]$ tal que nenhum monômio aparecendo em r é um múltiplo de $\mathrm{lm}(g_i)$ para todo $i = 1, \ldots, s$. Agora, da mesma forma, escolhendo outra ordem para $g_1, \ldots, g_s$, suponha que, depois de efetuar o algoritmo da divisão em f considerando tal ordem, $f = \tilde{q}_1 g_1 + \cdots + \tilde{q}_s g_s + \tilde{r}$, em que $\tilde{q}_i \in \mathbb{K}[\mathbf{X}]$ para todo $i = 1, \ldots, s$ e $\tilde{r} \in \mathbb{K}[\mathbf{X}]$ tal que nenhum monômio aparecendo em $\tilde{r}$ é um múltiplo de $\mathrm{lm}(g_i)$ para todo $i = 1$. De $r - \tilde{r} = \sum_{i=1}^{s} (\tilde{q}_i - q_i) g_i \in I$ devemos ter $r - \tilde{r} = 0$, caso contrário $r - \tilde{r}$ seria um polinômio não nulo em I cujo monômio líder não é um múltiplo de $\mathrm{lm}(g_i)$ para todo $i = 1, \ldots, s$, contradizendo o fato de $\{g_1, \ldots, g_s\}$ ser uma base de Gröbner de I. □

Agora, seja $I = (XY - 1, Y^2 - 1)$. Se efetuarmos a divisão de $f = XY^2 - X$ por $\{XY - 1, Y^2 - 1\}$ temos que o resto $r = -X + Y$. No entanto, $f = X(Y^2 - 1) \in I$. Quando estamos trabalhando com bases de Gröbner de um ideal I, se $f \in I$, o resto necessariamente é 0, como mostra o resultado a seguir.

Lema 1.23. *Seja $\{g_1, \ldots, g_s\} \subset I$ uma base de Gröbner de I, então $f \in I$ se, e somente se, o resto na divisão de f por $\{g_1, \ldots, g_s\}$ é zero. Como uma consequência, $I = (g_1, \ldots, g_s)$.*

Demonstração. Seja $f \in I$, tal que $f = \sum_{i=1}^{s} q_i g_i + r$ é a divisão de f por $\{g_1, \ldots, g_s\}$. Então $r = f - \sum_{i=1}^{s} q_i g_i \in I$, ou seja, $r = 0$, caso contrário r seria um polinômio não nulo em I cujo monômio não líder não é múltiplo de $\mathrm{lm}(g_i)$ para todo $i = 1, \ldots, s$, contrariando o fato de $\{g_1, \ldots, g_s\}$ ser uma base de Gröbner de I. Isso mostra que $I \subset (g_1, \ldots, g_s)$ e, a fortiori, $I = (g_1, \ldots, g_s)$. Reciprocamente, se $f = \sum_{i=1}^{s} q_i g_i$, claramente $f \in I$. □

No Corolário 1.21 mostramos que sempre existe uma base de Gröbner para qualquer ideal não nulo I de $\mathbb{K}[\mathbf{X}]$. Agora, vamos definir alguns conceitos para depois darmos um algoritmo (Algoritmo de Buchberger) que calcula uma base de Gröbner para o ideal I.

Definição 1.24. O **mínimo múltiplo comum** dos monômios $\mathbf{X}^{\boldsymbol{\alpha}}$ e $\mathbf{X}^{\boldsymbol{\beta}}$ é definido como

$$\mathrm{mmc}(\mathbf{X}^{\boldsymbol{\alpha}}, \mathbf{X}^{\boldsymbol{\beta}}) = \mathbf{X}^{\boldsymbol{\gamma}},$$

onde $\gamma_i = \max\{\alpha_i, \beta_i\}$ para todo $i \in \{1, \ldots, n\}$.

Definição 1.25. Sejam $f, g \in \mathbb{K}[\mathbf{X}]$. O **S-polinômio** de f e g é a combinação

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

onde $lt(f) = a\mathbf{X}^{\boldsymbol{\alpha}}$ e $lt(g) = b\mathbf{X}^{\boldsymbol{\beta}}$.

Exemplo 1.26. Sejam $f = 2XY - Z^2, g = 3X^2 - Z \in \mathbb{K}[X, Y, Z]$ e consideremos a ordem lexicográfica (com $Z \preccurlyeq_{\mathrm{lex}} Y \preccurlyeq_{\mathrm{lex}} X$). Temos que, $\mathrm{lt}(f) = 2XY, \mathrm{lt}(g) = 3X^2$ e $\mathrm{mmc}(XY, X^2) = X^2Y$. Logo, $S(f, g) = \frac{1}{2}\frac{X^2Y}{XY}(2XY - Z^2) - \frac{1}{3}\frac{X^2Y}{X^2}(3X^2 - Z) = -\frac{XZ^2}{2} - \frac{YZ}{3}$.

Teorema 1.27 (Critério de Buchberger)**.** *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal. Então, uma base $G = \{g_1, \ldots, g_s\}$ de I é uma base de Gröbner de I se, e somente se, para todos pares $i \neq j$, o resto da divisão de $S(g_i, g_j)$ por G (listada em alguma ordem) é zero.*

Demonstração. Veja em [4, Theorem 6, p.86]. □

Corolário 1.28 (Algoritmo de Buchberger)**.** *Seja $I = (f_1, \ldots, f_t) \subset \mathbb{K}[\boldsymbol{X}]$ um ideal não nulo. Uma base de Gröbner de I é obtida pela iteração do seguinte procedimento:*
Para cada $i \neq j$, aplique o algoritmo da divisão aos $S-$polinômios para obter as expressões

$$S(f_i, f_j) = \sum_{l=1}^{t} h(ij)_l f_l + r(ij), \quad \operatorname{lm}(S(f_i, f_j)) \geq \operatorname{lm}(h(ij)_l f_l),$$

onde cada $\operatorname{lm}(r(ij))$ não é múltiplo de $\operatorname{lm}(f_l)$ para todo $l \in \{1, \ldots, t\}$. Se todos os restos $r(ij) = 0$, então $\{f_1, \ldots, f_t\}$ é uma base de Gröbner de I. Caso contrário, considere $f_{t+1}, \ldots, f_{t+s}$ como sendo os $r(ij)$ não nulos e junte-os para obter um novo conjunto de geradores $\{f_1, \ldots, f_t, f_{t+1}, \ldots, f_{t+s}\}$.

Demonstração. Veja em [4, Corollary 2.29]. □

Exemplo 1.29. Sejam $f_1 = XY - X, f_2 = -Y + X^2 \in \mathbb{Q}[X, Y]$ e consideremos a ordem lexicográfica (com $X \preccurlyeq_{\text{lex}} Y$). Vamos encontrar uma base de Gröbner para o ideal $I = (XY - X, -Y + X^2) \subset \mathbb{Q}[X, Y]$ utilizando o Algoritmo de Buchberger. Primeiro, encontremos o S-polinômio $S(f_1, f_2)$. Temos que, $S(f_1, f_2) = X^3 - X$ e que o resto $r'(12)$ da divisão de $S(f_1, f_2)$ por $G' = \{f_1, f_2\}$ é $f_3 \coloneqq X^3 - X = r(12)$. Agora, consideremos o novo conjunto de geradores $G = \{f_1, f_2, f_3\}$ de I. Temos que, $S(f_1, f_3) = XY - X^3$ e $S(f_2, f_3) = XY - X^5$. É claro que o resto $r(12)$ da divisão de $S(f_1, f_2)$ por G é 0. Agora, fazendo a divisão de $S(f_1, f_3)$ e de $S(f_2, f_3)$ por G, temos que, $r(13) = r(23) = 0$. Portanto, pelo Algoritmo de Buchberger, $G = \{f_1, f_2, f_3\}$ é uma base de Gröbner de I.

Teorema 1.30. *Seja $I = (g_1, \ldots, g_s) \subset \mathbb{K}[\boldsymbol{X}]$, tal que $mdc(\operatorname{lm}(g_i), \operatorname{lm}(g_j)) = 1$ para todo $i, j \in \{1, \ldots, s\}$ com $i \neq j$. Então, $G = \{g_1, \ldots, g_s\}$ é uma base de Gröbner de I.*

Demonstração. Veja em [4, Proposition 4, p.106]. □

Exemplo 1.31. Seja $I = (X^3Y - X^2Z - 4, Z^5 - X^3Y + XYZ + 4) \subset \mathbb{R}[X, Y, Z]$ e consideremos a ordem lexicográfica graduada (com $Z \preccurlyeq_{\text{grlex}} Y \preccurlyeq_{\text{grlex}} X$), pelo teorema anterior, $G = \{X^3Y - X^2Z - 4, Z^5 - X^3Y + XYZ + 4\}$ é uma base de Gröbner de I.

1.3 A Pegada de um Ideal

Vamos introduzir agora, o conceito de pegada de um ideal $I \subset \mathbb{K}[\mathbf{X}]$. Tal conceito é útil quando queremos exibir uma base de $\dfrac{\mathbb{K}[\mathbf{X}]}{I}$ como $\mathbb{K}$-espaço vetorial, como faremos no Teorema 1.37.

Definição 1.32. Sejam $I \subset \mathbb{K}[\mathbf{X}]$ um ideal não nulo e $\preccurlyeq$ uma ordem monomial em $\mathcal{M}$. A **pegada** de I (com respeito a $\preccurlyeq$) é o conjunto

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

Proposição 1.33. *Sejam $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal e $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner de I. Então a pegada de I (com respeito a mesma ordem monomial usada para obter a base de Gröbner G) é*

$$\Delta(I) = \{M \in \mathcal{M} \mid M \text{ não é múltiplo de } \operatorname{lm}(g_i) \text{ para todo } i \in \{1, \ldots, s\}\}.$$

Demonstração. Seja $M \in \Delta(I)$, temos, por definição, que M não é o monômio líder de nenhum polinômio em I. Agora, suponha, por absurdo, que M é múltiplo de algum $\mathrm{lm}(g_i) \in G$, ou seja, $M = \mathrm{lm}(g_i)M'$ para algum $M' \in \mathcal{M}$, logo, $\mathrm{lm}(M'g_i) = M'\mathrm{lm}(g_i) = M$, no entanto, $M'g_i \in I$, o que é um absurdo. Portanto, M não é múltiplo de $\mathrm{lm}(g_i)$ para todo $i \in \{1, \ldots, s\}$. Por outro lado, seja $M \in \mathcal{M}$, tal que M não é múltiplo de $\mathrm{lm}(g_i)$ para todo $i \in \{1, \ldots, s\}$, então pela definição de bases de Gröbner, sabemos que M não é o monômio líder de nenhum polinômio em I. □

Exemplo 1.34. Seja $I = (X^3 - 2XY, X^2Y - 2Y^2 + X) \subset \mathbb{Q}[X, Y]$ e consideremos a ordem lexicográfica graduada (com $Y \preccurlyeq_{\mathrm{grlex}} X$)). É fácil verificar que $\{X^2, XY, 2Y^2 - X\}$ é uma base de Gröbner de I. Então, pela proposição anterior a pegada de I é $\Delta(I) = \{1, X, Y\}$.

A partir de agora, sempre que falarmos da pegada $\Delta(I)$ de um ideal $I \subset \mathbb{K}[\mathbf{X}]$ deve ficar implícito que alguma ordem monomial foi escolhida em $\mathcal{M}$. No entanto, em alguns exemplos e resultados explicitaremos qual ordem foi escolhida.

Definição 1.35. Seja $I \subset \mathbb{K}[\mathbf{X}]$ um ideal e seja $\{f_1, \ldots, f_t\}$ uma base de I. Denotamos por $\Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$ o conjunto

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

Proposição 1.36. *Seja $I = (f_1, \ldots, f_t) \subset \mathbb{K}[\boldsymbol{X}]$. Então, $\Delta(I) \subset \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$. E se $\{f_1, \ldots, f_t\}$ for 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 $\mathrm{lm}(f_j)$ para todo $j \in \{1, \ldots, t\}$, 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 $M \in \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$, pela Proposição 1.33 temos que, $M \in \Delta(I)$. □

Teorema 1.37 (Buchberger)**.** *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal. Então*

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

é uma base de $\dfrac{\mathbb{K}[\boldsymbol{X}]}{I}$ como $\mathbb{K}$-espaço vetorial.

Demonstração. Seja G uma base de Gröbner de I com respeito a mesma ordem monomial usada para determinar $\Delta(I)$, e seja $f \in \mathbb{K}[\mathbf{X}]$. Dividindo f por G, temos que, pelo algoritmo da divisão, o resto é da forma $r = \sum_{i=1}^{t} a_i M_i$, onde $a_i \in \mathbb{K}$ e $M_i \in \Delta(I)$ para todo $i \in \{1, \ldots, t\}$. Como $f + I = r + I = \sum_{i=1}^{t} a_i(M_i + I)$, temos que $\mathcal{B}$ gera $\dfrac{\mathbb{K}[\mathbf{X}]}{I}$ como $\mathbb{K}$-espaço vetorial. Agora, suponha que $\sum_{i=1}^{l} b_i(M_i + I) = 0 + I$, onde $b_i \in \mathbb{K}$ e $M_i \in \Delta(I)$ para todo $i \in \{1, \ldots, l\}$. Então, $\sum_{i=1}^{l} b_i M_i \in I$, logo, devemos ter $b_i = 0$ para todo $i \in \{1, \ldots, l\}$. Caso contrário, $\sum_{i=1}^{l} b_i M_i$ seria um polinômio não nulo em I com o monômio líder na pegada de I. Isso mostra que $\mathcal{B}$ é linearmente independente sobre $\mathbb{K}$. Portanto, $\mathcal{B}$ é uma base de $\dfrac{\mathbb{K}[\mathbf{X}]}{I}$ como $\mathbb{K}$-espaço vetorial. □

Exemplo 1.38. Vimos no Exemplo 1.34 que, $\Delta(I) = \{1, X, Y\}$, onde $I = (X^3 - 2XY, X^2Y - 2Y^2 + X) \subset \mathbb{Q}[X, Y]$. Então, pelo teorema anterior, temos que, $\dfrac{\mathbb{Q}[X, Y]}{I}$ é um $\mathbb{Q}$-espaço vetorial de dimensão 3 e $\{1 + I, X + I, Y + I\}$ é uma base para esse espaço vetorial.

1.4 Variedades Afins

Definição 1.39. Um **espaço afim** de dimensão n sobre $\mathbb{K}$ é o conjunto

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

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

Definição 1.40. Seja $F = \{f_j\}_{j \in J} \subset \mathbb{K}[\mathbf{X}]$. A **variedade afim** de F é o conjunto

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

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

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

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

Definição 1.41. Dado $S \subset \mathbb{A}^n(\mathbb{K})$, o **ideal de polinômios que se anulam em** S, ou simplesmente **ideal de** S, é o conjunto

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

É facil verificar que $\mathcal{I}(S)$ é, de fato, um ideal de $\mathbb{K}[\mathbf{X}]$. Agora iremos listar algumas relações entre a variedade de um ideal e o ideal de uma variedade, e deixaremos as demonstrações a cargo do leitor.

Dado um ideal $I \subset \mathbb{K}[\mathbf{X}]$, temos

i) $I \subset \mathcal{I}(V(I))$.

ii) $S \subset V(\mathcal{I}(S))$.

iii) $V(\mathcal{I}(V(I))) = V(I)$.

Definição 1.42. O **radical de um ideal** $I \subset \mathbb{K}[\mathbf{X}]$ é o conjunto

$$\sqrt{I} \coloneqq \{f \in \mathbb{K}[\mathbf{X}] \mid f^N \in I \text{ para algum } \ N \in \mathbb{N}\}.$$

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

Não é difícil verificar que $\sqrt{I}$ é um ideal de $\mathbb{K}[\mathbf{X}]$ e que $I \subset \sqrt{I}$ e $\sqrt{\sqrt{I}} = \sqrt{I}$.

1.4.1 Uma relação entre Variedades Afins e a Pegada de um Ideal

Para provar uma importante relação entre a variedade de um ideal $I \subset \mathbb{K}[\mathbf{X}]$ e a pegada de I quando $\Delta(I)$ é um conjunto finito, precisamos do seguinte resultado auxiliar.

Lema 1.43. *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal e sejam $P_1, \ldots, P_r$ pontos distintos de $V(I)$. Então, existem polinômios $p_1, \ldots, p_r \in \mathbb{K}[\boldsymbol{X}]$, tal que $p_i(P_j) = \delta_{ij}$ para todo $i, j \in \{1, \ldots, r\}$ (onde δ_{ij} é o delta de Kronecker).*

Demonstração. Defina $P_i \coloneqq (a_{i1}, \ldots, a_{in}) \in \mathbb{K}^n$, onde $i = 1, \ldots, r$, vamos mostrar como obter p_1 que satisfaz a condição do enunciado do lema. Como todos os pontos são distintos, para $i \in \{2, \ldots, r\}$ existem $j_i \in \{1, \ldots, r\}$, tais que $a_{1j_i} \neq a_{ij_i}$. Agora, definimos $h_i \coloneqq \dfrac{X_{j_i} - a_{j_i}}{a_{1j_i} - a_{ij_i}}$, então $h_i(P_1) = 1$ e $h_i(P_i) = 0$ para todo $i = 2, \ldots, r$, então, tomando $p_1 = \displaystyle\prod_{i=2}^{r} h_i$, temos que, $p_1(P_1) = 1$ e $p_1(P_i) = 0$ para todo $i = 2, \ldots, r$. De maneira similar conseguimos obter $p_2, \ldots, p_r$ como no enunciado. □

Proposição 1.44. *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal tal que $\Delta(I)$ é um conjunto finito. Então $V(I)$ também é um conjunto finito e $|V(I)| \leq |\Delta(I)|$.*

Demonstração. Sejam $P_1, \ldots, P_r$ pontos distintos de $V(I)$, vamos encontrar um conjunto em $\dfrac{\mathbb{K}[\mathbf{X}]}{I}$ que é linearmente independente e tem r elementos. Isso vai provar a proposição, pois, no Teorema 1.37, vimos que $|\Delta(I)|$ é a dimensão de $\dfrac{\mathbb{K}[\mathbf{X}]}{I}$ como $\mathbb{K}$-espaço vetorial. Do lema acima, sabemos que existem $p_1, \ldots, p_r \in \mathbb{K}[\mathbf{X}]$ tais que, $p_i(P_j) = \delta_{ij}$ para todo $i, j \in \{1, \ldots, r\}$. Suponha que $\displaystyle\sum_{i=1}^{r} a_i(p_i + I) = 0 + I$, onde $a_1, \ldots, a_r \in k$, então $\displaystyle\sum_{i=1}^{r} a_i p_i \in I$, logo para todo $j \in \{1, \ldots, r\}$ temos $a_j = \left(\displaystyle\sum_{i=1}^{r} a_i p_i\right)(P_j) = 0$. Portanto, $\{p_1 + I, \ldots, p_r + I\}$ é um conjunto linearmente independente sobre $\mathbb{K}$, o que completa a demonstração. □

Na verdade, pode-se provar um resultado mais refinado.

Teorema 1.45. *Seja $I \subset \mathbb{K}[\boldsymbol{X}]$ um ideal tal que $\Delta(I)$ é um conjunto finito e seja L uma extensão algebricamente fechada de $\mathbb{K}$. Então, $V_L(I) \coloneqq \{(a_1, \ldots, a_n) \in \mathbb{A}^n(L) \mid f(a_1, \ldots, a_n) = 0$ para todo $f \in I\}$ é um conjunto finito e $|V_L(I)| \leq |\Delta(I)|$. Além disso, se $\mathbb{K}$ é um corpo perfeito (e.g. um corpo finito ou um corpo de característica zero) e I é um ideal radical, então $|V_L(I)| = |\Delta(I)|$*

Demonstração. Veja em [1, Theorem 8.32]. □

Capítulo 2

Códigos Lineares

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

A seguir, será apresentado um modo de medir a distância entre palavras em A^n.

Definição 2.2. Dados dois elementos $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in A^n$, a **distância de Hamming** entre u e v é definida como

$$d(u, v) \coloneqq |\{i \mid u_i \neq v_i, \text{ onde } i \in \{1, \ldots n\}\}|.$$

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 2.3. *Dados $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n), w = (w_1, \ldots, w_n) \in A^n$, valem as seguintes propriedades:*

i) $d(u, v) \geq 0$ *e* $d(u, v) = 0$ *se, e somente se,* $u = v$.

ii) $d(u, v) = d(v, u)$.

iii) $d(u, v) \leq d(u, w) + d(w, v)$.

Demonstração. Vamos demonstrar a terceira propriedade, pois a primeira e a segunda são triviais. Observe que, a contribuição das i-ésimas coordenadas de u e v para $d(u, v)$ é igual a zero se $u_i = v_i$, e igual a um se $u_i \neq v_i$. No caso em que a contribuição é zero, temos que, a contribuição das i-ésimas coordenadas a $d(u, v)$ é menor ou igual a das i-ésimas coordenadas a $d(u, w) + d(w, v)$ $(= 0, 1$ ou $2)$. Agora, quando a contribuição é um, temos $u_i \neq v_i$ e, portanto, não podemos ter $u_i = w_i$ e $w_i = v_i$. Logo, a contribuição das i-ésimas coordenadas a $d(u, w) + d(w, v)$ é maior ou igual a 1, que é a contribuição das i-ésimas coordenadas a $d(u, v)$. □

Definição 2.4. Seja $\mathcal{C}$ um código (corretor de erros). A **distância mínima** de $\mathcal{C}$ é o número

$$\delta(\mathcal{C}) \coloneqq \min\{d(u, v) \mid u, v \in \mathcal{C} \text{ e } u \neq v\}.$$

E, define-se $\kappa \coloneqq \left[\frac{\delta(\mathcal{C}) - 1}{2}\right]$, onde $[t]$ representa a parte inteira de um número real t.

Teorema 2.5. *Seja $\mathcal{C}$ um código com distância mínima $\delta(\mathcal{C})$. Então $\mathcal{C}$ pode corrigir até κ erros e detectar até $\delta(\mathcal{C}) - 1$ erros.*

Demonstração. Se ao transmitirmos uma palavra u do código cometemos t erros com $t \leq \kappa$, recebendo a palavra v, então $d(v,u) = t \leq \kappa$. Agora, seja $u' \neq u$ outra palavra do código, e suponha que, $d(v,u') \leq \kappa$, então $d(u,u') \leq d(u,v)+d(v,u') \leq 2\kappa = 2\left[\frac{\delta(\mathcal{C})-1}{2}\right] \leq 2\left(\frac{\delta(\mathcal{C})-1}{2}\right) = \delta(\mathcal{C})-1 < \delta(\mathcal{C})$, absurdo, pois $d(u,u') \geq \delta(\mathcal{C})$. Portanto, determina-se u univocamente a partir de v. Por outro lado, seja u uma palavra do código e introduza até $\delta(\mathcal{C})-1$ erros em u, digamos que a palavra com os erros introduzidos é u', assim, $d(u,u') \leq \delta(\mathcal{C})-1 < \delta(\mathcal{C})$, ou seja, u' é uma palavra que não pertence ao código e, portanto, o código consegue detectar até $\delta(\mathcal{C})-1$ erros. □

Vimos no teorema anterior que um código terá mais capacidade de correção de erros quanto maior for a sua distância mínima. Então para a Teoria dos Códigos é importante poder calcular $\delta(\mathcal{C})$ ou pelo menos determinar uma cota inferior para ele.

Agora vamos definir códigos lineares sobre um corpo finito $\mathbb{F}_q$ com q elementos, onde $q = p^r$, com p primo e $r \in \mathbb{N}$.

Definição 2.6. Um código $\mathcal{C} \subset \mathbb{F}_q^n$ será chamado de **código linear** se for um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q^n$. Os **parâmetros do código linear** $\mathcal{C}$ são a **dimensão** $\dim_{\mathbb{F}_q}\mathcal{C} =: k$ de $\mathcal{C}$ como $\mathbb{F}_q$-espaço vetorial, o **comprimento** n de $\mathcal{C}$, e a **distância mínima** $\delta(\mathcal{C})$ de $\mathcal{C}$. Usualmente os parâmetros são escritos como a terna de inteiros $[n,k,\delta(\mathcal{C})]$.

Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear, $k = \dim_{\mathbb{F}_q}\mathcal{C}$ e seja $\{\mathbf{v}_1,\ldots,\mathbf{v}_k\}$ uma base de $\mathcal{C}$, portanto, todo elemento de $\mathcal{C}$ se escreve de modo único da forma $\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \cdots + \lambda_k\mathbf{v}_k$, onde $\lambda_i \in \mathbb{F}_q$ para todo $i \in \{1,\ldots k\}$. Segue daí que $|\mathcal{C}| = q^k$.

Definição 2.7. Dado uma palavra $\mathbf{a} = (a_1,\ldots,a_n) \in \mathbb{F}_q^n$, define-se o **peso** de $\mathbf{a}$ como sendo o número inteiro

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

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 $\mathcal{C}$, significa que $\mathcal{C} \subset \mathbb{F}_q^n$ é um código linear.

Definição 2.8. Sejam um código $\mathcal{C}$ tal que $\dim_{\mathbb{F}_q}\mathcal{C} = k$, $\mathcal{B} = \{\mathbf{v}_1,\ldots,\mathbf{v}_k\}$ uma base ordenada de $\mathcal{C}$ e considere a matriz G, cujas linhas são os vetores $\mathbf{v}_i = (v_{i1},\ldots,v_{in}), i = 1,\ldots,k$, isto é,

$$G = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}$$

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

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

Definição 2.9. Sejam $\mathbf{u} = (u_1,\ldots,u_n)$ e $\mathbf{v} = (v_1,\ldots,v_n)$ elementos de $\mathbb{F}_q^n$, define-se o **produto interno** de $\mathbf{u}$ e $\mathbf{v}$ como sendo

$$\langle \mathbf{u},\mathbf{v} \rangle \coloneqq u_1v_1 + \cdots + u_nv_n.$$

A operação acima é simétrica e bilinear, ou seja, satisfaz as propriedades usuais de um produto interno sobre um espaço vetorial.

Definição 2.10. Seja $\mathcal{C}$ um código, define-se o **código dual** de $\mathcal{C}$ como sendo o conjunto

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

Fica a cargo do leitor mostrar que $\mathcal{C}^{\perp} \subset \mathbb{F}_q^n$ é um código linear com $\dim_{\mathbb{F}_q} \mathcal{C}^{\perp} = n - k$, onde $\dim_{\mathbb{F}_q} \mathcal{C} = k$ (ou veja em [8, p. 96]).

Lema 2.11. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código, com matriz geradora G, então*

$$\boldsymbol{a} \in \mathcal{C}^{\perp} \Leftrightarrow G\boldsymbol{a}^t = 0.$$

Demonstração. $\mathbf{a} \in \mathcal{C}^{\perp}$ se, e somente se, $\mathbf{a}$ é ortogonal a todos elementos de $\mathcal{C}$ se, e somente se, $\mathbf{a}$ é ortogonal a todos os elementos de uma base de $\mathcal{C}$ se, e somente se, $G\mathbf{a}^t = 0$, pois o conjunto de vetores que estão nas linhas de G forma uma base de $\mathcal{C}$. □

Lema 2.12. *Seja $\mathcal{C}$ um código com matriz geradora G e $dim_{\mathbb{F}_q}\mathcal{C} = k$. 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 $\mathcal{C}^{\perp}$ 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 a dimensão de $\mathcal{C}^{\perp}$. É fácil ver que $G \cdot H^t = 0$ equivale a dizer que todos os vetores do subespaço gerado pelas linhas de H estão em $\mathcal{C}^{\perp}$. Por outro lado, esse subespaço tem a mesma dimensão de $\mathcal{C}^{\perp}$, logo,

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

□

Em álgebra linear prova-se que $(V^{\perp})^{\perp} = V$ para qualquer espaço vetorial V de dimensão finita. Em particular, dado um código $\mathcal{C}$ temos que $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$. Apresentamos uma prova desse fato.

Corolário 2.13. *Seja $\mathcal{C}$ um código. Então $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.*

Demonstração. Sejam G e H matrizes geradoras de $\mathcal{C}$ e $\mathcal{C}^{\perp}$, respectivamente. Pelo Lema anterior, temos $G \cdot H^t = 0$, logo, $H \cdot G^t = (G \cdot H^t)^t = 0^t = 0$. Como G é uma matriz (com linhas linearmente independentes) de ordem $k \times n$ e $\dim_{\mathbb{F}_q}(\mathcal{C}^{\perp})^{\perp} = k$, segue do Lema anterior que G é uma matriz geradora de $(\mathcal{C}^{\perp})^{\perp}$ e, portanto, $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$. □

Agora, caracterizaremos os elementos de um código $\mathcal{C}$.

Proposição 2.14. *Seja $\mathcal{C}$ um código e seja H uma matriz geradora de $\mathcal{C}^{\perp}$. Então*

$$\boldsymbol{a} \in \mathcal{C} \Leftrightarrow H\boldsymbol{a}^t = 0.$$

Demonstração. Segue do Corolário acima e do Lema 2.11. □

Definição 2.15. A matriz geradora H de $\mathcal{C}^{\perp}$ é chama de **matriz teste de paridade** de $\mathcal{C}$. E dado um vetor $\mathbf{v} \in \mathbb{F}_q^n$, chamamos o vetor $H\mathbf{v}^t$ de **síndrome** de $\mathbf{v}$.

Observe que, para verificar se um determinado vetor $\mathbf{v} \in \mathbb{F}_q^n$ pertence ou não a um código $\mathcal{C}$ com matriz geradora G e $\dim_{\mathbb{F}_q}\mathcal{C} = k$, é preciso verificar se o sistema de n equações com k incógnitas, dado por $\mathbf{x}G = \mathbf{v}$, admite solução. No entanto, trabalhando com uma matriz teste de paridade H, a solução pode ser encontrada bem mais rapidamente. Basta verificar se a síndrome de $\mathbf{v}$ é o vetor nulo.

A matriz teste de paridade também contém informações sobre a distância mínima do código $\mathcal{C}$ como veremos nos resultados a seguir.

Proposição 2.16. *Seja H a matriz teste de paridade de um código $\mathcal{C}$. Temos que*

$$\delta(\mathcal{C}) \geq s \Leftrightarrow \text{ quaisquer } s-1 \text{ colunas de } H \text{ são linearmente independentes.}$$

Demonstração. Suponha que quaisquer $s-1$ colunas de H são linearmente independentes. Seja $\mathbf{a} = (a_1, \ldots, a_n)$ uma palavra não nula do código $\mathcal{C}$ e consideremos $h^1, \ldots h^n$ as colunas de H. Como $H\mathbf{a}^t = 0$, temos que $0 = H\mathbf{a}^t = \sum_{i=1}^{n} a_i h^i$. Visto que $\omega(\mathbf{a})$ é o número de coordenadas não nulas de $\mathbf{a}$, segue que se $\omega(\mathbf{a}) \leq s-1$, teríamos uma soma do tipo $\sum_{j=1}^{\omega(\mathbf{a})} a_{i_j} h^{i_j} = 0$, com $\omega(\mathbf{a}) \leq s-1$, $i_j \in \{1, \ldots, n\}$ e $a_{i_j} \neq 0$ para todo $j = 1, \ldots, \omega(\mathbf{a})$, o que é uma contradição. Logo, $\omega(\mathbf{a}) \geq s$ e, portanto, $\delta(\mathcal{C}) \geq s$. Reciprocamente, suponha que $\delta(\mathcal{C}) \geq s$. Suponha também, por absurdo, que H tenha $s-1$ colunas linearmente dependentes, a saber $h^{i_1}, \ldots, h^{i_{s-1}}$, logo, existem $a_{i_1}, \ldots, a_{i_{s-1}}$ elementos em $\mathbb{F}_q$, não todos nulos, tais que $\sum_{j=1}^{s-1} a_{i_j} h^{i_j} = 0$. Daí, considerando o vetor $\mathbf{a} = (0, \ldots, a_{i_1}, 0, \ldots, a_{i_{s-1}}, \ldots, 0, \ldots, 0)$, temos que $\mathbf{a} \in \mathcal{C}$, pois $H\mathbf{a}^t = 0$, e $\omega(\mathbf{a}) \leq s-1 < s$, o que é um absurdo. □

Teorema 2.17. *Seja H a matriz teste de paridade de um código $\mathcal{C}$. Temos que*

$$\delta(\mathcal{C}) = s \Leftrightarrow \text{ quaisquer } s-1 \text{ colunas de } H \text{ são linearmente independentes e existem } s \text{ colunas de } H \text{ linearmente dependentes.}$$

Demonstração. Suponha primeiro que $\delta(\mathcal{C}) = s$, então, pela Proposição anterior, quaisquer $s-1$ colunas de H são linearmente independentes. Agora, afirmo que, existem s colunas de H que são linearmente dependentes. De fato, suponha, por absurdo, que quaisquer s colunas de H são linearmente independentes, logo, novamente pela Proposição anterior, $\delta(\mathcal{C}) \geq s+1 > s$, o que é um absurdo.

Reciprocamente, suponha que quaisquer $s-1$ colunas de H são linearmente independentes e que existem s colunas de H linearmente dependentes. Pela Proposição anterior, temos $\delta(\mathcal{C}) \geq s$ e, de fato, temos $\delta(\mathcal{C}) = s$, pois se $\delta(\mathcal{C})$ for maior do que s, teríamos pela Proposição anterior que quaisquer s colunas de H seriam linearmente independentes, o que é uma contradição. □

Corolário 2.18 (Cota de Singleton)**.** *Os parâmetros $[n, k, \delta(\mathcal{C})]$ de um código $\mathcal{C}$ satisfazem à desigualdade*

$$\delta(\mathcal{C}) \leq n - k + 1.$$

Demonstração. Seja H uma matriz teste de paridade de $\mathcal{C}$. Sabemos que o posto de H é igual a $n-k = \dim_{\mathbb{F}_q} \mathcal{C}^{\perp}$ e pela Proposição anterior, temos que o posto de H é maior ou igual a $\delta(\mathcal{C}) - 1$ e, portanto, $n - k \geq \delta(\mathcal{C}) - 1$. □

Definição 2.19. Um código $\mathcal{C}$ será chamado de MDS (**Maximum Distance Separable**) se valer a igualdade $\delta(\mathcal{C}) = n - k + 1$.

Vejamos agora um exemplo de um código linear MDS.

Exemplo 2.20. Consideremos o $\mathbb{F}_q$-espaço vetorial $\mathbb{F}_q[X]_{\leq d-1}$ incluindo o polinômio nulo, isto é, $\mathbb{F}_q[X]_{\leq d-1} = \{p \in \mathbb{F}_q[X] \mid \deg(p) \leq d-1\} \cup \{0\}$, onde $\deg(p)$ é o grau do polinômio p. Não é difícil ver que esse espaço vetorial tem dimensão d com uma base dada por $\{1, X, X^2, \ldots, X^{d-1}\}$.

Agora sejam n um inteiro, tal que $n \geq d$, e $\alpha_1, \ldots, \alpha_n$ elementos distintos de $\mathbb{F}_q$. Consideremos a transformação linear $T : \mathbb{F}_q[X]_{\leq d-1} \longrightarrow \mathbb{F}_q^n$, tal que $T(p) = (p(\alpha_1), \ldots, p(\alpha_n))$.

Veja que $\mathrm{Ker}T = \{p \in \mathbb{F}_q[X]_{\leq d-1} \mid p(\alpha_1) = \cdots = p(\alpha_n) = 0\} = \{0\}$, pois um polinômio não nulo $p \in \mathbb{F}_q[X]_{\leq d-1}$ não pode ter $n \geq d$ raízes distintas. Segue que, T é injetora. Portanto, $\mathcal{C} = T(\mathbb{F}_q[X]_{\leq d-1})$ é um código linear de comprimento n e dimensão d. Esse código é chamado de Código de Reed-Solomon de comprimento n e dimensão d definido por $\alpha_1, \ldots, \alpha_n$.

Como transformações lineares bijetoras levam base em base, segue que uma matriz geradora do código $\mathcal{C}$ é dada por

$$G = \begin{pmatrix} T(1) \\ T(X) \\ \vdots \\ T(X^{d-1}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{d-1} & \alpha_2^{d-1} & \ldots & \alpha_n^{d-1} \end{pmatrix}.$$

Agora seja, $\mathbf{a}$ uma palavra não nula de $\mathcal{C}$. Então, existe $p \in \mathbb{F}_q[X]_{\leq d-1}$ tal que $\mathbf{a} = (p(\alpha_1) \ldots, p(\alpha_n))$. Logo,

$$\omega(\mathbf{a}) = |\{i \in \{1, \ldots, n\} \mid p(\alpha_i) \neq 0\}| = n - |\{i \in \{1, \ldots, n\} \mid p(\alpha_i) = 0\}| \geq n - deg(p) \geq n - d + 1.$$

Logo, $\delta(\mathcal{C}) \geq n - d + 1$. Por outro lado, pela Cota de Singleton (Corolário 2.18), temos $\delta(\mathcal{C}) \leq n - d + 1$. Portanto, $\delta(\mathcal{C}) = n - d + 1$, ou seja, o Código de Reed-Solomon é MDS.

2.1 Códigos Cartesianos Afins

Nesta seção, seguindo [3], iremos apresentar alguns resultados sobre um tipo particular de código.

Seja $I = (g_1, \ldots, g_t) \subset \mathbb{F}_q[\mathbf{X}]$ e consideremos o ideal $I_q \coloneqq (g_1, \ldots, g_t, X_1^q - X_1, \ldots, X_n^q - X_n)$. Da Teoria de Corpos, 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 ($\preccurlyeq_{\mathrm{grlex}}$) em $\mathcal{M} \subset \mathbb{F}_q[\mathbf{X}]$.

Proposição 2.21. *$\Delta(I_q)$ é um conjunto finito.*

Demonstração. Afirmo que $\Delta(\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t), X_1^q, \ldots, X_n^q)) \leq q^n$. De fato, por definição temos que $\Delta(\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t), X_1^q, \ldots, X_n^q))$ é o conjunto dos monômios que não são múltiplos de $\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t), X_1^q, \ldots, X_n^q$, em particular, tais monômios não são múltiplos de $X_1^q, \ldots, X_n^q$, o que prova a afirmação. Pela Proposição 1.36, temos

$$|\Delta(I_q)| \leq |\Delta(\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t), X_1^q, \ldots, X_n^q)| \leq q^n,$$

o que completa a demonstração. □

Lema 2.22. *Seja $I \subset \mathbb{F}_q[\boldsymbol{X}]$ um ideal tal que $\Delta(I)$ é um conjunto finito. Então*

$$I \text{ é um ideal radical} \Leftrightarrow I \text{ contém um polinômio } f_j \in \mathbb{F}_q[X_j] \setminus \mathbb{F}_q \text{ tal que } mdc(f_j, f_j') = 1,$$

$$\text{para todo } j \in \{1, \ldots, n\},$$

onde f_j' denota a derivada usual de um polinômio.

Demonstração. Veja em [1, Proposition 8.14]. □

Proposição 2.23. *Seja $V(I_q) = \{P_1, \ldots, P_m\}$ e seja a transformação linear $\varphi : \dfrac{\mathbb{F}_q[\boldsymbol{X}]}{I_q} \longrightarrow \mathbb{F}_q^m$, tal que $\varphi(f + I_q) = (f(P_1), \ldots, f(P_m))$. Então φ é um isomorfismo de $\mathbb{F}_q$- espaços vetoriais.*

Demonstração. Primeiro vamos mostrar que $\dim_{\mathbb{F}_q} \frac{\mathbb{F}_q[\mathbf{X}]}{I_q} = m$. De fato, como o polinômio $f_j \coloneqq X_j^q - X_j$ tem q raízes distintas temos $mdc(f_j, f_j') = 1$ para todo $j \in \{1, \ldots, n\}$, e pela Proposição 2.21 o conjunto $\Delta(I_q)$ é finito, então pelo 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 1.45 temos que $|V_{\overline{\mathbb{F}_q}}(I_q)| = |\Delta(I_q)|$. Daí, $m = |V(I_q)| = |\Delta(I_q)|$. Portanto, pelo Teorema de Buchberger (Teorema 1.37), temos que $\dim_{\mathbb{F}_q} \frac{\mathbb{F}_q[\mathbf{X}]}{I_q} = |\Delta(I_q)| = m$. Agora, mostraremos que φ é sobrejetora, e assim, aplicando o Teorema do Núcleo e da Imagem o resultado estará provado. Com efeito, consideremos os polinômios $p_1, \ldots, p_m$ em $\mathbb{F}_q[\mathbf{X}]$, tais que $p_i(P_j) = \delta_{ij}$ para todo $i, j \in \{1, \ldots, m\}$ (tais polinômios existem pelo Lema 1.43), e veja que, $\varphi(p_i + I_q) = (0, \ldots, 1, 0, \ldots, 0) = e_i$, para todo $i \in \{1, \ldots, m\}$, onde 1 está na i-ésima coordenada. Como $\{e_1, \ldots, e_m\}$ é uma base de $\mathbb{F}_q^m$ como $\mathbb{F}_q$-espaço vetorial, o resultado segue. □

O seguinte conceito foi introduzido por Fitzgerald e Lax em [5].

Definição 2.24. Seja $L \subset \frac{\mathbb{F}_q[\mathbf{X}]}{I_q}$ um $\mathbb{F}_q$- subespaço vetorial de $\frac{\mathbb{F}_q[\mathbf{X}]}{I_q}$. A imagem $\mathcal{C}(L) \coloneqq \varphi(L)$ é chamada de **código de variedade afim associado à** L.

Vamos provar agora que todo código linear pode ser representado como um código de variedade afim. Para isso, precisaremos do seguinte Lema

Lema 2.25. *Sejam $P_1, \ldots, P_s$ pontos de $\mathbb{A}^n(\mathbb{F}_q)$, tal que $P_j = (a_{j1}, \ldots, a_{jn})$. Então o polinômio*

$$f_j(\boldsymbol{X}) = \prod_{l=1}^{n} [1 - (X_l - a_{jl})^{q-1}]$$

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. Sabemos que $X_i^q - X_i = \prod_{\alpha \in \mathbb{F}_q} (X_i - \alpha)$, para todo $i \in \{1, \ldots, n\}$. Logo, dado $\omega \in \mathbb{F}_q$, temos que $\frac{(X_i - \omega)^q - (X_i - \omega)}{X_i - \omega} = \frac{X_i^q - X_i}{X_i - \omega} = \prod_{\alpha \in \mathbb{F}_q \setminus \{\omega\}} (X_i - \alpha)$, ou seja, $(X_i - \omega)^{q-1} - 1 = \prod_{\alpha \in \mathbb{F}_q \setminus \{\omega\}} (X_i - \alpha)$. Assim, $1 - (\alpha - \omega)^{q-1} = 1$ se $\alpha = \omega$ e $1 - (\alpha - \omega)^{q-1} = 0$ se $\alpha \neq 0$, e daí, o resultado segue. □

Proposição 2.26. *Todo código linear $\mathcal{C} \subset \mathbb{F}_q^s$ pode ser representando como um código de variedade afim.*

Demonstração. Seja $\mathcal{C} \subset \mathbb{F}_q^s$ um código, tal que $\dim_{\mathbb{F}_q} \mathcal{C} = k$. Seja $[c_{ij}]$ uma matriz geradora de $\mathcal{C}$ com $i = 1, \ldots, k$ e $j = 1, \ldots, s$. Escolha o menor número natural n, tal que $q^n \geq s$. Seja $Y = \{P_1, \ldots, P_s\} \subset \mathbb{A}^n(\mathbb{F}_q)$ (existem pelo menos s pontos em $\mathbb{A}^n(\mathbb{F}_q)$, pois $|\mathbb{A}^n(\mathbb{F}_q)| = q^n \geq s$) e seja $I = \mathcal{I}(Y)$ o ideal de Y em $\mathbb{F}_q[\mathbf{X}]$. Vamos denotar $P_j = (a_{j1}, \ldots, a_{jn})$ para $j = 1, \ldots, s$. Temos pelo Lema anterior que o polinômio $f_j(\mathbf{X}) = \prod_{l=1}^{n} [1 - (X_l - a_{jl})^{q-1}]$, 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 $j = 1, \ldots, s$. Agora, defina $g_i + I_q \coloneqq \sum_{j=1}^{s} c_{ij}(f_j + I_q)$, para $i = 1, \ldots, k$ e tome $L = \mathbb{F}_q\{g_1 + I_q, \ldots, g_k + I_q\} \subset \frac{\mathbb{F}_q[\mathbf{X}]}{I_q}$ o subespaço gerado por $\{g_1 + I_q, \ldots, g_k + I_q\}$. Então $\mathcal{C} = \mathcal{C}(L)$, pois $\varphi(g_i + I_q) = (c_{i1}, \ldots, c_{in})$, para $i = 1, \ldots, k$ e $\varphi : \frac{\mathbb{F}_q[\mathbf{X}]}{I_q} \longrightarrow \mathbb{F}_q^s$ é tal que, $\varphi(f + I_q) = (f(P_1), \ldots, f(P_s))$. □

Agora vamos apresentar resultados sobre um tipo de códigos de variedades afins que foi introduzido por H. López, C. Rentería-Marquez e R. Villareal em [10]. Tal código é construído da seguinte forma: sejam $A_1, \ldots, A_n$ conjuntos não vazios de $\mathbb{F}_q$ e defina $X \coloneqq A_1 \times \cdots \times A_n$. Defina também $f_i \coloneqq \prod_{\alpha \in A_i} (X_i - \alpha)$ para todo $i \in \{1, \ldots, n\}$ e consideremos $I \coloneqq (f_1, \ldots, f_n)$, é fácil ver que $V(I) = X$. Como no início da seção, consideremos $I_q = (f_1, \ldots, f_n, X_1^q - X_1, \ldots, X_n^q - X_n)$ e observe que nesse caso $I = I_q$, pois f_i é um divisor de $X_i^q - X_i$ para todo $i \in \{1, \ldots, n\}$.

Definição 2.27. Seja $d \in \mathbb{N}_0$ e consideremos o $\mathbb{F}_q$-subespaço vetorial de $\dfrac{\mathbb{F}_q[\mathbf{X}]}{I}$ dado por $L_{\leq d} \coloneqq \{p + I \mid p = 0 \text{ ou } \deg(p) \leq d\}$, onde $\deg(p)$ é o grau do polinômio $p \in \mathbb{F}_q[\mathbf{X}]$. Definimos **código cartesiano afim** como sendo a imagem $\mathcal{C}_X(d) \coloneqq \varphi(L_{\leq d})$, onde $\varphi : \dfrac{\mathbb{F}_q[\mathbf{X}]}{I} \longrightarrow \mathbb{F}_q^m$ é tal que $\varphi(f + I) = (f(P_1), \ldots, f(P_m))$ e $\{P_1, \ldots, P_m\} = X = V(I)$.

No que se segue vamos determinar os parâmetros desses códigos. Observe que $|V(I)| = d_1 . \cdots . d_n$ é o comprimento de $\mathcal{C}_X(d)$ para todo $d \geq 0$. Em [10, Proposition 3.2] os autores provaram que podemos assumir que $2 \leq d_1 \leq \cdots \leq d_n$ sem perda de generalidade.

Lema 2.28. *$\{f_1, \ldots, f_n\}$ é uma base de Gröbner de I*

Demonstração. Segue diretamente do Teorema 1.30, pois $\operatorname{mdc}(\operatorname{lm}(f_i), \operatorname{lm}(f_j)) = \operatorname{mdc}(X_i^{d_i}, X_j^{d_j}) = 1$ para todo $i, j \in \{1, \ldots, n\}$ com $i \neq j$. Outra possível demonstração é a seguinte. Observe que $\Delta(I) \subset \{X_1^{\alpha_1} . \cdots . X_n^{\alpha_n} \mid 0 \leq \alpha_i < d_i \ \forall i = 1, \ldots, n\}$, pois $I = (f_1, \ldots, f_n)$ e $\operatorname{lm}(f_i) = X_i^{d_i}$ para todo $i = 1, \ldots, n$. Logo, pela Proposição 1.44 $|V(I)| = d_1 . \cdots . d_n \leq |\Delta(I)| \leq d_1 . \cdots . d_n$, ou seja, $|\Delta(I)| = d_1 . \cdots . d_n$. Isso mostra que $\mathcal{B} \coloneqq \{f_1, \ldots, f_n\}$ é uma base de Gröbner de I, caso contrário pelo algoritmo de Buchberger conseguiríamos adicionar à $\mathcal{B}$ um polinômio, cujo monômio líder não seria um múltiplo de $X_i^{d_i}$ para todo $i = 1, \ldots, n$, mas isso implicaria que $|\Delta(I)| < d_1 . \cdots . d_n$. □

Lema 2.29. *(Conforme [10, Lemma 2.3]) $\mathcal{I}(X) = I$.*

Demonstração. É claro que $I \subset \mathcal{I}(X)$, logo $\Delta(\mathcal{I}(X)) \subset \Delta(I) = \{X_1^{\alpha_1} . \cdots . X_n^{\alpha_n} \mid 0 \leq \alpha_i < d_i \ \forall i = 1, \ldots, n\}$. Então, pela Proposição 1.44 e pelo Lema acima, $d_1 . \cdots . d_n = |V(\mathcal{I}(X))| \leq |\Delta(\mathcal{I}(X))| \leq |\Delta(I)| = d_1 . \cdots . d_n$, logo, $|\Delta(\mathcal{I}(X))| = d_1 . \cdots . d_n$. Neste caso, temos $\Delta(\mathcal{I}(X)) = \{X_1^{\alpha_1} . \cdots . X_n^{\alpha_n} \mid 0 \leq \alpha_i < d_i \ \forall i = 1, \ldots, n\}$, pois $\Delta(\mathcal{I}(X)) \subset \Delta(I)$. Agora, dado $f \in \mathcal{I}(X)$, temos que, $\operatorname{lm}(f)$ é múltiplo de $\operatorname{lm}(f_i) = X_i^{d_i}$ para algum $i \in \{1, \ldots, n\}$, caso contrário, $\operatorname{lm}(f) \in \Delta(\mathcal{I}(X))$, o que é uma contradição. Então $\{f_1, \ldots, f_n\} \subset \mathcal{I}(X)$ é uma base de Gröbner de $\mathcal{I}(X)$ e, portanto, $\mathcal{I}(X) = (f_1, \ldots, f_n) = I$. □

Agora, queremos calcular a dimensão de $\mathcal{C}_X(d)$. Como φ é um isomorfismo de $\mathbb{F}_q$-espaços vetoriais e $\mathcal{C}_X(d) = \varphi(L_{\leq d})$, temos que, $\dim_{\mathbb{F}_q} \mathcal{C}_X(d) = \dim_{\mathbb{F}_q} L_{\leq d}$. Definimos $\Delta(I)_{\leq d}$ como o conjunto dos elementos de grau total menor ou igual a d que estão em $\Delta(I)$, ou seja, $\Delta(I)_{\leq d} = \Delta(I) \cap \mathbb{F}_q[\mathbf{X}]_{\leq d}$.

Proposição 2.30. *O conjunto $\{M + I \mid M \in \Delta(I)_{\leq d}\}$ é uma base de $L_{\leq d}$ como $\mathbb{F}_q$-espaço vetorial.*

Demonstração. Pelo Teorema 1.37 sabemos que o conjunto $\mathcal{B} \coloneqq \{M + I \mid M \in \Delta(I)_{\leq d}\}$ é linearmente independente, e claramente está contido em $L_{\leq d}$. Agora, seja $p \in \mathbb{F}_q[\mathbf{X}], p \neq 0$ tal que $\deg(p) \leq d$. Dividindo p por $\{f_1, \ldots, f_n\}$, temos pelo algoritmo da divisão que o resto r obtido através dessa divisão é tal que, $\operatorname{lm}(r) \preccurlyeq_{\text{grlex}} \operatorname{lm}(p)$ ou $r = 0$, ou seja, $\deg(\operatorname{lm}(r)) \leq d$ 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 $\Delta(I)_{\leq d}$ (aqui usamos que $\{f_1, \ldots, f_n\}$ é uma base de Gröbner de I), e portanto, $\mathcal{B}$ é uma base de $L_{\leq d}$ como $\mathbb{F}_q$-espaço vetorial. □

Temos a seguinte consequência do resultado acima.

Lema 2.31. *(Conforme [10, Theorem 3.1]) A dimensão de $\mathcal{C}_X(d)$ é $dim_{\mathbb{F}_q}\mathcal{C}_X(d) = |\Delta(I)_{\leq d}|$, em particular $dim_{\mathbb{F}_q}\mathcal{C}_X(d) = d_1.\cdots.d_n$ e $\delta(\mathcal{C}_X(d)) = 1$ para todo $d \geq \sum_{i=1}^{n}(d_i - 1)$.*

Demonstração. A primeira afirmação é uma consequência da Proposição acima e o fato de φ ser um isomorfismo. Para a segunda e terceira afirmação, observe que $\Delta(I) = \{X_1^{\alpha_1}.\cdots.X_n^{\alpha_n} \mid 0 \leq \alpha_i \leq d_i - 1 \ \forall i = 1, \ldots, n\}$, pois $\{f_1, \ldots, f_n\}$ é uma base de Gröbner de I. Logo, $\deg(M) \leq \sum_{i=1}^{n}\alpha_i \leq \sum_{i=1}^{n}(d_i - 1) \leq d$ para todo $M \in \Delta(I)$. Portanto, $\Delta(I)_{\leq d} = \Delta(I)$ sempre que $d \geq \sum_{i=1}^{n}(d_i - 1)$. E o resultado segue, pois $\dim_{\mathbb{F}_q}\mathcal{C}_X(d) = |\Delta(I)_{\leq d}| = d_1.\cdots.d_n$ e $\mathcal{C}_X(d) = \varphi(L_{\leq d}) = \mathbb{F}_q^{d_1.\cdots.d_n}$. □

Teorema 2.32. *(Conforme [10, Theorem 3.1]) A dimensão de $\mathcal{C}_X(d)$ para $0 \leq d < \sum_{i=1}^{n}(d_i - 1)$ é dada por*

$$dim_{\mathbb{F}_q}\mathcal{C}_X(d) = \begin{pmatrix} n+d \\ d \end{pmatrix} - \sum_{i=1}^{n}\begin{pmatrix} n+d-d_i \\ d-d_i \end{pmatrix} + \cdots +$$
$$(-1)^j \sum_{1 \leq i_1 < \cdots < i_j \leq n} \begin{pmatrix} n+d-d_{i_1}-\cdots-d_{i_j} \\ d-d_{i_1}-\cdots-d_{i_j} \end{pmatrix} + \cdots + (-1)^n \begin{pmatrix} n+d-d_{i_1}-\cdots-d_{i_n} \\ d-d_{i_1}-\cdots-d_{i_n} \end{pmatrix},$$

onde consideramos $\binom{a}{b} = 0$ se $b < 0$, e $\binom{a}{b} = \frac{a!}{(a-b)!b!}$ se $a \geq b > 0$, é o coeficiente binomial de a na classe b.

Demonstração. Pelo Lema anterior, $\dim_{\mathbb{F}_q}\mathcal{C}_X(d) = |\Delta(I)_{\leq d}|$, ou seja, a quantidade de monômios em $\Delta(I)$ da forma $X_1^{\alpha_1}.\ldots.X_n^{\alpha_n}$ com $0 \leq \sum_{i=1}^{n}\alpha_i \leq d$. Consideremos

$$h(t) \coloneqq (1 + t + \cdots + t^{d_1-1}) \cdot \ldots \cdot (1 + t + \cdots + t^{d_n-1},)$$

é fácil verificar que o coeficiente de t^e em $h(t)$ é igual ao número de monômios em $\Delta(I)$ que tem grau e, para todo $e \in \{0, \ldots, \sum_{i=1}^{n}(d_i - 1)\}$. Assim, uma maneira de obtermos o que queremos é calcularmos os coeficientes de $t^0, t, \ldots, t^d$ e então somá-los. Outra maneira mais rápida é observar que há uma bijeção entre os conjuntos $\Delta(I)_{\leq d}$ e

$$\Delta_d \coloneqq \{X_0^{\alpha_0}.X_1^{\alpha_1}.\cdots.X_n^{\alpha_n} \in \mathbb{F}_q[X_0, X_1, \ldots, X_n] \mid \text{com } \sum_{i=0}^{n}\alpha_i = d \text{ e } 0 \leq \alpha_i \leq d_i - 1 \ \forall i = 1, \ldots, n\}$$

dada por $\beta : \Delta(I)_{\leq d} \longrightarrow \Delta_d$, onde $\beta(M) = X_0^d M\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right)$ e $\beta^{-1} : \Delta_d \longrightarrow \Delta(I)_{\leq d}$ é dado por $\beta^{-1}(N) = N(1, X_1, \ldots, X_n)$. Agora, consideremos

$$H(t) \coloneqq (1 + t + t^2 + \cdots) \cdot (1 + t + \cdots + t^{d_1 - 1}) \cdot \cdots \cdot (1 + t + \cdots + t^{d_n - 1}),$$

então o coeficiente de t^d é $|\Delta_d|$. Note que,

$$H(t) = \frac{1}{1-t}.\frac{1-t^{d_1}}{1-t}.\cdots.\frac{1-t^{d_n}}{1-t}.$$

Assim, $H(t) = \left(\frac{1}{(1-t)^{n+1}}\right)\prod_{i=1}^{n}(1-t^{d_i})$. Usando que $\frac{1}{(1-t)^{n+1}} = \sum_{j=0}^{\infty}\binom{n+j}{j}t^j$, temos

$$H(t) = \left(\sum_{j=0}^{\infty}\binom{n+j}{j}\right)(1 - \sum_{i=1}^{n} t^{d_i} + \sum_{1 \leq i_1 < i_2 \leq n} t^{d_{i_1}+d_{i_2}} + \cdots + (-1)^j + \sum_{1 \leq i_1 < \cdots < i_j \leq n} t^{d_{i_1}+\cdots+d_{i_j}} + \cdots + (-1)^n t^{d_{i_1}+\cdots+d_{i_n}}).$$

Segue que, o coeficiente de t^d em $H(t)$ usando o produto acima é a expressão da $dim_{\mathbb{F}_q}\mathcal{C}_X(d)$ que está no enunciado do teorema. Como queríamos demonstrar. □

Vamos precisar do seguinte resultado para encontrar a distância mínima de $\mathcal{C}_X(d)$, com $0 \leq d < \sum_{i=1}^{n}(d_i - 1)$.

Lema 2.33. *Sejam $0 < d_1 \leq \cdots \leq d_n$ e $s < \sum_{i=1}^{n}(d_i - 1)$ inteiros. Defina $m(\alpha_1, \ldots, \alpha_n) \coloneqq \prod_{i=1}^{n}(d_i - \alpha_i)$, onde $0 \leq \alpha_i < d_i$ é um inteiro, para todo $i = 1, \ldots, n$. Então*

$$\min\{m(\alpha_1, \ldots, \alpha_n) \mid \alpha_1 + \cdots + \alpha_n \leq s\} = (d_{k+1} - \ell)\prod_{i=k+2}^{n} d_i,$$

onde k e ℓ são unicamente definidos por $s = \sum_{i=1}^{k}(d_i - 1) + \ell$ com $0 \leq \ell < d_{k+1} - 1$. Aqui, se $k + 1 = n$, então entendemos que $\prod_{i=k+2}^{n} d_i = 1$, e se $s < d_1 - 1$, então consideramos $k = 0$ e $\ell = s$.

Demonstração. Veja em [3, Lemma 2.2]. □

Teorema 2.34. *(Conforme [10, Theorem 3.8]) Seja $0 \leq d < \sum_{i=1}^{n}(d_i - 1)$. Então $\delta(\mathcal{C}_X(d)) = (d_{k+1} - \ell)\prod_{i=k+2}^{n} d_i$, onde k e ℓ são unicamente definidos por $d = \sum_{i=1}^{k}(d_i - 1) + \ell$ com $0 \leq \ell < d_{k+1} - 1$. Como no resultado acima, se $k + 1 = n$ entendemos que $\prod_{i=k+2}^{n} d_i = 1$, e se $d < d_1 - 1$ então consideramos $k = 0$ e $\ell = d$.*

Demonstração. Seja $F+I \in L_{\leq d} \setminus \{0\}$ e defina $J_F \coloneqq (F, f_1, \ldots, f_n)$. Então, o número de zeros da palavra $\varphi(F+I)$ é igual a $|V(J_F)|$, de modo que $\omega(\varphi(F+I)) = \prod_{i=1}^{n} d_i - |V(J_F)|$. Pela Proposição 1.44, temos que $|V(J_F)| \leq |\Delta(J_F)|$. Seja $M \coloneqq X_1^{\alpha_1}.\cdots.X_n^{\alpha_n}$ o monômio líder de F ($0 \leq \alpha_i < d_i$ para todo $i \in \{1, \ldots, n\}$, pois $M \in \Delta(I)_{\leq d}$), pela Proposição 1.36, temos que $\Delta(J_F) \subset \Delta(M, X_1^{d_1}, \ldots, X_n^{d_n})$, assim, $|V(J_F)| \leq \prod_{i=1}^{n} d_i - \prod_{i=1}^{n}(d_i - \alpha_i)$. Logo, $\omega(\varphi(F+I)) = \prod_{i=1}^{n} d_i - |V(J_F)| \geq \prod_{i=1}^{n} d_i - \left(\prod_{i=1}^{n} d_i - \prod_{i=1}^{n}(d_i - \alpha_i)\right) = \prod_{i=1}^{n}(d_i - \alpha_i)$, assim, pelo Lema acima $\omega(\varphi(F+I)) \geq (d_{k+1} - \ell) \prod_{i=k+2}^{n} d_i$, e portanto, $\delta(\mathcal{C}_X(d)) \geq (d_{k+1} - \ell) \prod_{i=k+2}^{n} d_i$. Para ver que essa cota inferior, na verdade, é atingida, escrevemos $A_i \coloneqq \{a_{i1}, \ldots, a_{id_i}\}$ para $i = 1, \ldots, n$ e tomemos $G(X_1, \ldots, X_n) = \left(\prod_{i=1}^{k} \prod_{j=1}^{d_i - 1}(X_i - a_{ij})\right) \prod_{j=1}^{\ell}(X_{k+1} - a_{(k+1)j})$, então $\deg(G) = \sum_{i=1}^{k}(d_i - 1) + \ell = d$ e G tem $\prod_{i=1}^{n} d_i - (d_{k+1} - \ell) \prod_{i=k+2}^{n} d_i$, assim, $\omega(\varphi(G+I)) = (d_{k+1} - \ell) \prod_{i=k+2}^{n} d_i$. □

Comparando a prova acima com a prova original apresentada em [10, Theorem 3.8], pode-se observar que a demonstração acima é mais simples. No próximo capítulo, na maioria das vezes, iremos utilizar técnicas como a de acima para determinar cotas para o r-ésimo peso de Hamming generalizado (que será definido posteriormente) de alguns códigos em específico.

Capítulo 3

r-ésimo Peso de Hamming Generalizado de alguns códigos de avaliação

3.1 O r-ésimo peso de Hamming Generalizado de um código linear

Definição 3.1. Sejam $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear de dimensão k e D um subcódigo de $\mathcal{C}$, ou seja, D é um $\mathbb{F}_q$-subespaço vetorial de $\mathcal{C}$. O **suporte** de D é o conjunto

$$\chi(D) \coloneqq \{i \mid \exists\, (a_1, \ldots, a_n) \in D, a_i \neq 0\}.$$

O r**-ésimo peso de Hamming Generalizado** de $\mathcal{C}$ é o conjunto

$$\delta_r(\mathcal{C}) \coloneqq \min\{|\chi(D)| \mid D \text{ é um subcódigo de } \mathcal{C} \text{ com } \dim_{\mathbb{F}_q} D = r\}.$$

Definição 3.2. Seja B um subconjunto de um $\mathbb{F}_q$-espaço vetorial V. Definimos o subespaço gerado por B por $\mathbb{F}_q B$.

O suporte $\chi(\beta)$ de um vetor $\beta \in \mathbb{F}_q^n$ é $\chi(\mathbb{F}_q\{\beta\})$, isto é, $\chi(\beta)$ é o conjunto de todas as entradas não nulas de β. E observe que, para $r = 1$, $\delta_1(\mathcal{C}) = \min\{|\chi(\beta)| \mid \beta \in \mathcal{C} \setminus \{0\}\} = \delta(\mathcal{C})$ é a distância mínima do código $\mathcal{C}$.

A partir das definições acima é simples provar o seguinte resultado.

Lema 3.3. *Seja D um subcódigo de $\mathcal{C} \subset \mathbb{F}_q^n$ de dimensão $r \geq 1$. Se $\{\beta_1, \ldots, \beta_r\}$ é uma base de D com $\beta_i = (\beta_{i1}, \ldots, \beta_{in})$ para $i = 1, \ldots, r$, então $\chi(D) = \bigcup_{i=1}^{r} \chi(\beta_i)$ e $|\chi(D)|$ é o número de colunas não nulas da matriz*

$$\begin{pmatrix} \beta_{11} & \cdots & \beta_{1i} & \cdots & \beta_{1n} \\ \beta_{21} & \cdots & \beta_{2i} & \cdots & \beta_{2n} \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ \beta_{r1} & \cdots & \beta_{ri} & \cdots & \beta_{rn} \end{pmatrix}.$$

Definição 3.4. A **hierarquia de pesos** de um código linear $\mathcal{C}$ de dimensão k é definida como sendo a sequência $(\delta_1(\mathcal{C}), \ldots, \delta_k(\mathcal{C}))$.

Proposição 3.5. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear de dimensão $k > 0$. Então*

$$1 \leq \delta_1(\mathcal{C}) < \cdots < \delta_k(\mathcal{C}) \leq n.$$

Demonstração. Vejamos que $\delta_{r-1}(\mathcal{C}) \leq \delta_r(\mathcal{C})$. De fato, sejam D um subcódigo de $\mathcal{C}$ de dimensão r tal que $\delta_r(\mathcal{C}) = |\chi(D)|$ e B uma matriz geradora de D, pelo Lema 3.3 $|\chi(D)|$ é o número de colunas não nulas da matriz B. Agora, eliminemos uma linha qualquer de B e consideremos a matriz formada pelas entradas de B com exceção da linha que eliminamos. Essa nova matriz, digamos, A, é uma matriz geradora para um subcódigo de $\mathcal{C}$ de dimensão $r-1$ com suporte menor ou igual a $|\chi(D)|$. Concluímos que, $\delta_{r-1}(\mathcal{C}) \leq |\chi(A)| \leq |\chi(D)| = \delta_r(\mathcal{C})$.

Resta provar que as desigualdades são estritas. Seja D um subcódigo de $\mathcal{C}$ tal que $|\chi(D)| = \delta_r(\mathcal{C})$ e $\dim_{\mathbb{F}_q} D = r$. Seja $i \in \chi(D)$, através do processo de eliminação gaussiana na matriz geradora B do subcódigo D, conseguimos obter uma nova matriz cuja i-ésima coluna tem $r-1$ entradas nulas e uma entrada igual a 1, digamos, na j-ésima linha. Eliminando essa j-ésima linha, obtemos uma matriz geradora de um subespaço D_i, que tem dimensão igual a $r-1$ e não tem i no suporte. Portanto, $\delta_{r-1}(\mathcal{C}) \leq |\chi(D_i)| \leq |\chi(D)| - 1 = \delta_r(\mathcal{C}) - 1 < \delta_r(\mathcal{C})$. □

Corolário 3.6 (Cota de Singleton Generalizada)**.** *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear de dimensão $k > 0$. Então $r \leq \delta_r(\mathcal{C}) \leq n - k + r$.*

Demonstração. Pela Proposição acima, temos que, $\delta_r(\mathcal{C}) \leq \delta_{r+1}(\mathcal{C}) - 1 \leq (\delta_{r+2}(\mathcal{C}) - 1) - 1 = \delta_{r+2}(\mathcal{C}) - 2 \leq \cdots \leq \delta_{r+(k-r)}(\mathcal{C}) - (k-r) = \delta_k(\mathcal{C}) - k + r \leq n - k + r$. Para ver que $\delta_r(\mathcal{C}) \geq r$, observe que todo subcódigo D de $\mathcal{C}$, com $\dim_{\mathbb{F}_q} D = r$, admite uma matriz geradora (escalonada) com r colunas não nulas. □

Teorema 3.7. *Sejam $\mathcal{C} \subset \mathbb{F}_q^n$ um código, H a matriz teste de paridade de $\mathcal{C}$ e $H_i, 1 \leq i \leq n$, os vetores colunas de H. Então*

$$\delta_r(\mathcal{C}) = \min\{|I| \mid I \subset \{1, \ldots, n\}, |I| - \dim_{\mathbb{F}_q}(\mathbb{F}_q\{H_i \mid i \in I\}) \geq r\}$$

Demonstração. Dado $I \subset \{1, 2, \ldots, n\}$, com $|I| = \ell$, definimos $S(I) \coloneqq \mathbb{F}_q\{H_i \mid i \in I\}$ e

$$S^{\perp}(I) \coloneqq \left\{ \mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{A}^n(\mathbb{F}_q) \mid a_i = 0 \text{ para } i \notin I, \text{ e} \sum_{i \in I} a_i H_i = \mathbf{0} \right\}.$$

Afirmo que $\dim_{\mathbb{F}_q}(S(I)) + \dim_{\mathbb{F}_q}(S^{\perp}(I)) = \ell$. Seja $I = \{i_1, \ldots, i_\ell\}$ e A a matriz

$$A = \begin{pmatrix} \beta_{1i_1} & \beta_{1i_2} & \cdots & \beta_{1i_\ell} \\ \beta_{2i_1} & \beta_{2i_2} & \cdots & \beta_{2i_\ell} \\ \vdots & \vdots & \vdots & \vdots \\ \beta_{(n-k)i_1} & \beta_{(n-k)i_2} & \cdots & \beta_{(n-k)i_\ell} \end{pmatrix},$$

obtida a partir das colunas de H e dos índices em I. O subespaço $W \subset \mathbb{F}_q^\ell$ gerado pelas linhas de A tem a mesma dimensão de $S(I)$, pois ambas as dimensões são iguais ao posto de A. Existe um isomorfismo entre $W^{\perp}$ e $S^{\perp}(I)$ logo $\dim_{\mathbb{F}_q} S(I) + \dim_{\mathbb{F}_q} S^{\perp}(I) = \ell$.

Observe também que $S^{\perp}(I)$ é um subcódigo de $\mathcal{C}$, pois dado $\mathbf{a} = (a_1, \ldots, a_n) \in S^{\perp}(I)$ temos que $\sum_{i=1}^{n} a_i H_i = \mathbf{0}$, ou seja, $H\mathbf{a}^t = \mathbf{0}$.

Seja D um subcódigo de $\mathcal{C}$ de $\dim_{\mathbb{F}_q} D = r$ tal que $|\chi(D)| = \delta_r(\mathcal{C})$ e consideremos $I = \chi(D)$. Veja que $D \subset S^{\perp}(I)$, pois se $\mathbf{a} \in D$ temos que $a_i = 0$ para todo $i \notin \chi(D) = I$ e $\mathbf{0} = H\mathbf{a}^t = \sum_{i=1}^{n} a_i H_i = \sum_{i \in I} a_i H_i$. Então $\dim_{\mathbb{F}_q} S^{\perp}(I) \geq r = \dim_{\mathbb{F}_q} D$. Suponha, por contradição, que $\dim_{\mathbb{F}_q} S^{\perp}(I) = r' > r$, assim, $\delta_{r'}(\mathcal{C}) \leq |\chi(S^{\perp}(I))| \leq |I| = |\chi(D)| = \delta_r(C)$, contradição com a Proposição 3.5. Logo, $\dim_{\mathbb{F}_q} S^{\perp}(I) = r$ e então $D = S^{\perp}(I)$. Daí, $|I| - \dim_{\mathbb{F}_q} S(I) = \dim_{\mathbb{F}_q} S^{\perp}(I) = r$.

Defina $d := \min\{|I| \mid I \subset \{1,\dots,n\}, |I| - \dim_{\mathbb{F}_q}(\mathbb{F}_q\{H_i \mid i \in I\}) = r\}$ e seja $I \subset \{1,\dots,n\}$ tal que $|I| = d$ e $d - \dim_{\mathbb{F}_q} S(I) = r$. Então $\dim_{\mathbb{F}_q} S^\perp(I) = d - \dim_{\mathbb{F}_q} S(I) = d - (d-r) = r$, logo, $S^\perp(I) \subset \mathcal{C}$ é um subcódigo de $\dim_{\mathbb{F}_q} S^\perp(I) = r$. Daí, $\delta_r(\mathcal{C}) \leq |\chi(S^\perp(I))| \leq |I| = d$. No parágrafo acima mostramos que existe I tal que $|I| - \dim_{\mathbb{F}_q} S(I) = r$ e $|I| = \delta_r(\mathcal{C})$. Daí vem que $d = \delta_r(\mathcal{C})$.

□

Exemplo 3.8. Seja

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

a matriz geradora de um código $\mathcal{C} \subset \mathbb{F}_2^5$. Seja

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

como $GH^t = \mathbf{0}$, pelo Lema 2.12 H é a matriz teste de paridade de $\mathcal{C}$.

Seja I um subconjunto de $\{1,\dots,5\}$. Considere o subespaço vetorial gerado pelas colunas H_i de G para $i \in I$. Queremos encontrar I de tal modo que $|I| - \dim_{\mathbb{F}_q}\mathbb{F}_q\{H_i \mid i \in I\} = r$, com $1 \leq r \leq 3$, e $|I| = \min\{|I| \mid |I| - \dim_{\mathbb{F}_q}\mathbb{F}_q\{H_i \mid i \in I\} = r\}$. Para $r = 1$, vemos que o menor dos conjuntos de colunas satisfazendo $\dim_{\mathbb{F}_q}\mathbb{F}_q\{H_i \mid i \in I\} = 1$ são $I = \{2,4\}$ ou $I = \{3,5\}$. Então pelo Teorema acima $\delta_1(\mathcal{C}) = 2$. Para $r = 2$, pela Proposição 3.5 $\delta_1(\mathcal{C}) = 2 < \delta_2(\mathcal{C}) \neq 1, 2$ e observe que não existe nenhum subconjunto $I \subset \{1,\dots,5\}$ com 3 elementos tal que $|I| - \dim_{\mathbb{F}_q}\mathbb{F}_q\{H_i \mid i \in I\} = 2$, mas para $I = \{1,2,3,4\}$ temos a igualdade desejada, logo, pelo Teorema acima $\delta_2(\mathcal{C}) = 4$. Para $r = 3$, basta observar que o número de colunas não nulas de G é igual a 5 (ou use a Proposição 3.5), e então $\delta_3(\mathcal{C}) = 5$.

O próximo Teorema dá uma relação entre os pesos generalizados de $\mathcal{C}$ e os pesos generalizados do código dual $\mathcal{C}^\perp$.

Teorema 3.9. *(Dualidade) Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código de $\dim_{\mathbb{F}_q}\mathcal{C} = k$, então*

$$\{\delta_r(\mathcal{C}) \mid 1 \leq r \leq k\} = \{1,\dots,n\} \setminus \{n+1-\delta_r(\mathcal{C}^\perp) \mid 1 \leq r \leq n-k\}.$$

Demonstração. Seja D um subespaço de $C^\perp$ tal que $\dim D = r$ e $|\mathcal{X}(D)| = \delta_r(C^\perp)$, e seja H uma matriz geradora para $C^\perp$. Temos que H é uma matriz $(n-k) \times k$, e podemos assumir que as r primeiras linhas de H sejam uma base para D. Podemos assumir ainda, depois de um processo de escalonamento, e de permutações de colunas, que H seja da forma

$$H = \left(\begin{array}{ccc:ccc:ccc} & & & 0 & \cdots & 0 & * & \cdots & * & 0 & \cdots & 0 \\ & \mathrm{Id}_r & & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ & & & 0 & \cdots & 0 & * & \cdots & * & 0 & \cdots & 0 \\ \hdashline 0 & \cdots & 0 & & & & * & \cdots & * & * & \cdots & * \\ \vdots & \ddots & \vdots & & \mathrm{Id}_{n-k-r} & & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & & & & * & \cdots & * & * & \cdots & * \end{array}\right).$$

$$\underbrace{\qquad\qquad}_{T} \quad \underbrace{\qquad\qquad}_{U} \quad \underbrace{\qquad\qquad}_{V}$$

Observe, olhando as r primeiras linhas, que devido à escolha de D o número de colunas no conjunto U mais r deve ser igual a $\delta_r(C^\perp)$, logo os conjuntos T e V contêm um total de $n - \delta_r(C^\perp)$ colunas.

Consideremos a projeção dos vetores $v \in C^\perp \subset \mathbb{F}_q^n$ sobre $\mathbb{F}_q^{n-\delta_r(C^\perp)}$ na qual consideramos apenas as entradas correspondentes às colunas dos conjuntos T e V. A projeção dos vetores nas

$n-k-r$ últimas linhas da matriz acima vai gerar um subespaço $W \subset \mathbb{F}_q^{n-\delta_r(C^\perp)}$ de dimensão $n-k-r$. É claro que $W^\perp \subset \mathbb{F}_q^{n-\delta_r(C^\perp)}$ tem dimensão igual a $(n-\delta_r(C^\perp)) - (n-k-r) = k+r-\delta_r(C^\perp)$. Usando os vetores de $W^\perp$ podemos construir um subespaço $E \subset C$, de dimensão $t := k+r-\delta_r(C^\perp)$, cujos vetores têm as primeiras r entradas nulas e também têm zero nas posições correspondentes às colunas do conjunto U. Isso mostra que $d_t(C) \leq n-\delta_r(C^\perp)$, e a fortiori temos $d_i(C) \leq n-\delta_r(C^\perp)$ para todo $i \in \{1,\ldots,t\}$.

Suponha agora, por absurdo que $d_{t+j}(C) = n-\delta_r(C^\perp)+1$ para algum $j \in 1,\ldots,k-t$. Nesse caso, existe uma matriz geradora G para C cujas $t+j$ primeiras linhas são uma base de um subespaço $D' \subset C$ cujo suporte tem cardinalidade igual a $n-\delta_r(C^\perp)+1$. Como acima, depois de um processo de escalonamento, e de permutações de colunas, que G seja da forma e

$$G = \left(\begin{array}{ccc:ccc:ccc:ccc} & & & 0 & \cdots & 0 & * & \cdots & * & 0 & \cdots & 0 \\ & \mathrm{Id}_{t+j} & & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ & & & 0 & \cdots & 0 & * & \cdots & * & 0 & \cdots & 0 \\ \hdashline 0 & \cdots & 0 & & & & * & \cdots & * & * & \cdots & * \\ \vdots & \ddots & \vdots & & \mathrm{Id}_{k-t-j} & & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & & & & * & \cdots & * & * & \cdots & * \end{array}\right)$$

$$\underbrace{\qquad\qquad}_{T'} \quad \underbrace{\qquad\qquad}_{U'} \quad \underbrace{\qquad\qquad}_{V'}$$

Como o suporte de D' tem cardinalidade $n-\delta_r(C^\perp)+1$, vemos que os conjuntos de colunas T' e V' têm um total de $\delta_r(C^\perp)-1$ colunas. Como acima, consideramos a projeção de $v \in C \subset \mathbb{F}_q^n$ sobre $\mathbb{F}_q^{\delta_r(C^\perp)-1}$ na qual consideramos apenas as entradas correspondentes às colunas dos conjuntos T' e V'. A projeção das últimas $k-t-j$ linhas de G gera um espaço de dimensão $k-t-j$, cujo dual em $\mathbb{F}_q^{\delta_r(C^\perp)-1}$ tem dimensão igual a $\delta_r(C^\perp)-1-(k-t-j) = \delta_r(C^\perp)-1-(k-(k+r-\delta_r(C^\perp))-j) = r+j-1$. A partir desse espaço dual podemos obter um subespaço de $C^\perp$ de dimensão $r+j-1$ cujo suporte é no máximo $\delta_r(C^\perp)-1$, absurdo, já que $r+j-1 \geq r$. □

3.2 Códigos de Avaliação

Definição 3.10. Seja $X = \{P_1,\ldots,P_m\}$ um conjunto de pontos distintos do espaço afim $\mathbb{A}^n(\mathbb{F}_q)$. A **função de avaliação**, denotada por ev, é a função $\mathbb{F}_q$-linear dada por

$$\mathrm{ev} : \frac{\mathbb{F}_q[\mathbf{X}]}{I} \longrightarrow \mathbb{F}_q^m, \quad f+I \mapsto (f(P_1),\ldots,f(P_m)),$$

onde $I \coloneqq \mathcal{I}(X)$. Seja $\mathcal{L}$ um subespaço vetorial de $\dfrac{\mathbb{F}_q[\mathbf{X}]}{I}$. A imagem $\mathcal{L}_X \coloneqq \mathrm{ev}(\mathcal{L})$ é chamada de **código de avaliação sobre** X.

Veja que, a função ev, como denotada acima, é um isomorfismo entre $\mathbb{F}_q$-espaços vetoriais. De fato, como $X_j^q - X_j \in I$ para todo $j \in \{1,\ldots,n\}$, temos que $I = I_q$, e como $V(I = I_q) = X$, segue da Proposição 2.23 que ev é um isomorfismo.

Veremos agora que, todo código de variedade afim é um código de avaliação. Para isso, precisaremos dos seguintes resultados auxiliares.

Lema 3.11. *(Lema de Seidenberg) Seja $I \subsetneq \mathbb{K}[\boldsymbol{X}]$ um ideal próprio tal que $\Delta(I)$ é um conjunto finito e $\mathbb{K}$ é um corpo qualquer. Se, para todo $i = 1,\ldots,n$ existe em I um polinômio não constante $f_i \in \mathbb{K}[X_i]$, com $mdc(f_i, f_i') = 1$, onde f_i' denota a derivada usual de um polinômio, então qualquer ideal próprio de $\mathbb{K}[\boldsymbol{X}]$ contendo I é um ideal radical.*

Demonstração. Veja, por exemplo, em [1, Lemma 8.13]. □

Teorema 3.12 (Hilbert Nullstellensatz)**.** *Seja $\mathbb{K}$ um corpo, $\mathbb{L}$ uma extensão algebricamente fechada de $\mathbb{K}$, e $f, g_1, \ldots, g_m \in \mathbb{K}[\boldsymbol{X}]$. Então são equivalentes:*

1. *Para todo $a \in \mathbb{L}^n, g_1(a) = \cdots = g_m(a) = 0$ implica que $f(a) = 0$.*
2. *$f \in \sqrt{(g_1, \ldots, g_m)}$.*

Demonstração. Veja em [1, Theorem 7.40]. □

Corolário 3.13. *Seja $I \subset \mathbb{F}_q[\boldsymbol{X}]$ um ideal tal que $X_i^q - X_i \in I$ para todo $i \in \{1, \ldots, n\}$. Então $\mathcal{I}(V(I)) = I$.*

Demonstração. Sejam $I = (g_1, \ldots . g_m) \subset \mathbb{F}_q[\mathbf{X}]$ um ideal tal que $X_i^q - X_i \in I$ para todo $i \in \{1, \ldots, n\}$, $f \in \mathcal{I}(V(I))$ e $a = (a_1, \ldots, a_n) \in \overline{\mathbb{F}_q}$ tal que $g_1(a) = \cdots = g_m(a) = 0$. Então $a_i^q - a_i = 0$ para todo $i \in \{1, \ldots, n\}$. Assim, $a_i \in \mathbb{F}_q$ para todo $i \in \{1, \ldots, n\}$. Logo, $a \in V(I)$ e assim, $f(a) = 0$. Pelo Teorema anterior segue que $f \in \sqrt{I}$. Portanto, $\mathcal{I}(V(I)) \subset \sqrt{I} = I$ (a última igualdade vem do Lema 3.11). □

Proposição 3.14. *Seja $I \subset \mathbb{F}_q[\boldsymbol{X}]$ um ideal e $\mathcal{L} \subset \dfrac{\mathbb{F}_q[\boldsymbol{X}]}{I_q}$ um subespaço vetorial. Então o código de variedade afim $\mathcal{C}(\mathcal{L})$ é igual a $\mathcal{L}_X$, onde $X = V(I_q)$.*

Demonstração. Temos que I_q é um ideal radical, e pelo Corolário acima temos que $I_q = \mathcal{I}(V(I_q)) = \mathcal{I}(X)$. E o resultado segue, pois nesse caso ev $= \varphi$ (φ conforme definido na Proposição 2.23). □

Proposição 3.15. *Seja $X \subset \mathbb{A}^n(\mathbb{K})$ um subconjunto finito. Para cada $1 \leq j \leq n$, existe um polinômio $f_j \in \mathbb{K}[X_j] \setminus \mathbb{K}$ tal que $f_j \in \mathcal{I}(X)$, com $mdc(f_j, f_j') = 1$ e qualquer ideal próprio de $\mathbb{K}[\boldsymbol{X}]$ que contém $\mathcal{I}(X)$ é um ideal radical.*

Demonstração. Sejam $P_1, \ldots, P_m$ os pontos de X. Escrevendo $P_i = (p_{i1}, \ldots, p_{in})$ com $p_{ij} \in \mathbb{K}$ para todos $i \in \{1, \ldots, m\}$ e $j \in \{1, \ldots, n\}$. Para cada $1 \leq j \leq n$ consideremos o conjunto

$$D_j \coloneqq \{p_{ij} \mid i = 1, \ldots, m\} = \{a_{1j}, \ldots, a_{d_j j}\},$$

onde $a_{1j}, \ldots, a_{d_j j}$ são elementos distintos de $\mathbb{K}$ e $d_j = |D_j|$ para $j \in \{1, \ldots, n\}$. Os polinômios de uma variável dados por

$$f_j \coloneqq (X_j - a_{1j}). \cdots .(X_j - a_{d_j j}), j = 1, \ldots, n$$

se anulam em todos os pontos de X. Agora, como cada f_j é um polinômio separável de $\mathbb{K}[X_j]$ (pois todas suas raízes são simples) para $j = 1, \ldots, n$, temos que, $\text{mdc}(f_j, f_j') = 1$. Portanto, o resultado segue do Lema 3.11. □

Corolário 3.16. *Nas hipóteses da proposição acima $|\Delta(\mathcal{I}(X))| < \infty$.*

Lema 3.17. *Seja X um subconjunto finito de $\mathbb{A}^n(\mathbb{F}_q)$. Se F é um subconjunto finito de $\mathbb{F}_q[\boldsymbol{X}]$, então*

$$|V(F) \cap X| = |\Delta(\mathcal{I}(X) + (F))|.$$

Demonstração. Afirmo que $V(F) \cap X = V(\mathcal{I}(X) + (F))$. De fato,

$$\begin{aligned} & P \in V(F) \cap X \Rightarrow P \in X \text{ e } f(P) = 0 \text{ para todo } f \in F \\ \Rightarrow & g(P) = g_1(P) + g_2(P) = 0, \text{ com } g_1 \in \mathcal{I}(X), g_2 \in (F), \text{ para todo } g \in \mathcal{I}(X) + (F) \\ \Rightarrow & P \in V(\mathcal{I}(X) + (F)). \end{aligned}$$

Por outro lado, como $\mathcal{I}(X) \subset \mathcal{I}(X) + (F)$ e $(F) \subset \mathcal{I}(X) + (F)$, segue que $V(\mathcal{I}(X) + (F)) \subset V(F) \cap V(\mathcal{I}(X)) = V(F) \cap X$. Veja também que, $|\Delta(\mathcal{I}(X)+(F))| < \infty$, pois $|\Delta(\mathcal{I}(X)+(F))| \leq \Delta(\mathcal{I}(X)) < \infty$. Agora, se $(F) = \mathbb{F}_q[\mathbf{X}]$, temos que $V(F) \cap X = V(\mathcal{I}(X) + (F)) = V(\mathbb{F}_q[\mathbf{X}]) = \emptyset = \Delta(\mathbb{F}_q[\mathbf{X}]) = \Delta(\mathcal{I}(X) + (F))$. Se $(F) \neq \mathbb{F}_q[\mathbf{X}]$, pela Proposição acima $\mathcal{I}(X) + (F)$ é um ideal radical, pois $\mathcal{I}(X) + (F)$ é um ideal próprio de $\mathbb{F}_q[\mathbf{X}]$ e $\mathcal{I}(X) \subset \mathcal{I}(X) + (F)$. E sabemos que, $V(\mathcal{I}(X) + (F)) = V_{\overline{\mathbb{F}_q}}(\mathcal{I}(X) + (F))$. Assim, pelo Teorema 1.45, $|V(\mathcal{I}(X) + (F))| = |\Delta(\mathcal{I}(X) + (F))|$. Portanto, $|V(F) \cap X| = |\Delta(\mathcal{I}(X) + (F))|$. □

Definição 3.18. Se $F = \{f_1, \ldots, f_t\}$ é um conjunto finito de polinômios de $\mathbb{F}_q[\mathbf{X}]$ definiremos

$$\mathrm{lm}(F) = (\mathrm{lm}(f_1) \ldots, \mathrm{lm}(f_t)).$$

Observe que, pela definição acima, podemos ter

$$\mathrm{lm}(F) \neq \mathrm{lm}((F)) = (\{\mathrm{lm}(f) \mid f \in (F), f \neq 0\}).$$

Teorema 3.19. *Seja $X \subset \mathbb{A}^n(\mathbb{F}_q)$. Se F é um conjunto finito de polinômios de $\mathbb{F}_q[\boldsymbol{X}]$, então*

$$|V(F) \cap X| = |\Delta(\mathcal{I}(X) + (F))| \leq |\Delta(\mathrm{lm}(\mathcal{I}(X)) + \mathrm{lm}(F))| \leq |\Delta(\mathcal{I}(X))| = |X|.$$

Além disso, $|\Delta(\mathcal{I}(X) + (F))| < |\Delta(\mathcal{I}(X))|$ se $(F) \nsubseteq \mathcal{I}(X)$.

Demonstração. A igualdade do lado esquerdo segue do Lema acima e como a função de avaliação $\mathrm{ev} : \dfrac{\mathbb{F}_q[\mathbf{X}]}{\mathcal{I}(X)} \longrightarrow \mathbb{F}_q^m$, tal que, $f + I \mapsto (f(P_1), \ldots, f(P_m))$, é um isomorfismo, segue que $|\Delta(\mathcal{I}(X))| = \dim_{\mathbb{F}_q} \dfrac{\mathbb{F}_q[\mathbf{X}]}{\mathcal{I}(X)} = \dim_{\mathbb{F}_q} \mathbb{F}_q^{|X|} = |X|$. Agora, seja $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner de $\mathcal{I}(X)$, então $\mathcal{I}(X) + (F) = (G \cup F)$. Assim, pela Proposição 1.36, temos que

$$\Delta(\mathcal{I}(X) + (F)) \subset \Delta(\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s), \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t)).$$

Observe que, como $G = \{g_1, \ldots, g_s\}$ é uma base de Gröbner de $\mathcal{I}(X)$, vale que $(\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s)) = \mathrm{lm}(\mathcal{I}(X))$ logo $\{\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s), \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t)\}$ é um conjunto gerador para $\mathrm{lm}(\mathcal{I}(X)) + \mathrm{lm}(F)$. Além disso, um conjunto de monômios é uma base de Gröbner para o ideal gerado por ele, logo

$$\Delta(\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s), \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t)) = \Delta(\mathrm{lm}(\mathcal{I}(X)) + \mathrm{lm}(F)).$$

Também temos $\Delta(\mathrm{lm}(\mathcal{I}(X)) + \mathrm{lm}(F)) \subset \Delta(\mathrm{lm}(\mathcal{I}(X)) = \Delta(\mathcal{I}(X))$.

Portanto, $|\Delta(\mathcal{I}(X) + (F))| \leq |\Delta(\mathrm{lm}(\mathcal{I}(X)) + \mathrm{lm}(F))| \leq |\Delta(\mathcal{I}(X))|$.

Agora, vamos provar a segunda parte do Teorema. Se $(F) \nsubseteq \mathcal{I}(X)$, então $\mathcal{I}(X) \subsetneq \mathcal{I}(X)+(F)$ e pela Proposição 3.15, $\mathcal{I}(X) + (F)$ é um ideal radical, e sabemos que $V(\mathcal{I}(X) + (F)) = V_{\overline{\mathbb{F}_q}}(\mathcal{I}(X) + (F))$ e que $V(\mathcal{I}(X)) = V_{\overline{\mathbb{F}_q}}(\mathcal{I}(X))$. Suponha, por absurdo, que $V(\mathcal{I}(X) + (F)) = V(\mathcal{I}(X))$, então

$$\begin{aligned} & \mathcal{I}(V(\mathcal{I}(X) + (F))) = \mathcal{I}(V(\mathcal{I}(X))) \Rightarrow \mathcal{I}(V_{\overline{\mathbb{F}_q}}(\mathcal{I}(X) + (F))) = \mathcal{I}(V_{\overline{\mathbb{F}_q}}(\mathcal{I}(X))) \\ \Rightarrow & \mathcal{I}(X) + (F) = \mathcal{I}(X), \end{aligned}$$

o que é um absurdo. Daí, $V(\mathcal{I}(X) + (F)) \subsetneq V(\mathcal{I}(X))$, e então, $|V(\mathcal{I}(X) + (F))| < |V(\mathcal{I}(X))|$. Portanto, pelo lema acima $|\Delta(\mathcal{I}(X) + (F))| = |V(\mathcal{I}(X) + (F))| < |V(\mathcal{I}(X))| = |X| = |\Delta(\mathcal{I}(X))|$. □

Definição 3.20. Seja $\mathcal{L}$ um subespaço vetorial de $\dfrac{\mathbb{F}_q[\mathbf{X}]}{\mathcal{I}(X)}$ de $\dim_{\mathbb{F}_q}\mathcal{L} = k$. Dado um inteiro $1 \leq r \leq k$, definimos

$$(\mathcal{L})_r \coloneqq \{F' = \{f_1 + I, \ldots, f_r + I\} \subset \mathcal{L} \mid F' \text{ é um subconjunto linearmente independente de } \mathcal{L}\},$$

onde $I \coloneqq \mathcal{I}(X)$.

Observação 3.21. A partir de agora consideraremos $I = \mathcal{I}(X)$. Além disso, sempre que tomarmos algum representante $f \in \mathbb{F}_q[\mathbf{X}]$ para uma classe $f + I$, estaremos assumindo que os monômios que aparecem em f estão em $\Delta(I)$. Observe que, pelo Teorema 1.37, existe um único tal representante para essa classe.

Teorema 3.22. *Sejam $X = \{P_1, \ldots, P_m\}$ um subconjunto de $\mathbb{A}^n(\mathbb{F}_q)$ e $\mathcal{L}$ um subespaço vetorial de $\dfrac{\mathbb{F}_q[\boldsymbol{X}]}{I}$. Então*

$$\delta_r(\mathcal{L}_X) = |\Delta(I)| - \max\{|\Delta(I + (F))| \mid F' \in (\mathcal{L})_r\} \text{ para } 1 \leq r \leq \dim_{\mathbb{F}_q} \mathcal{L}_X,$$

onde $F = \{f_1, \ldots, f_r\}$ se $F' = \{f_1 + I, \ldots, f_r + I\}$.

Demonstração. Primeiro vamos mostrar que

$$\{|\chi(D)| \mid D \text{ é um subcódigo de } \mathcal{L}_X \text{ e } \dim_{\mathbb{F}_q} D = r\} = \{|X \setminus V(F)| \mid F' \in (\mathcal{L})_r\}.$$

De fato, seja D um subcódigo de $\mathcal{L}_X$ de $\dim_{\mathbb{F}_q} D = r$ com matriz geradora $G = (\beta_{ij})$, com $1 \leq i \leq r$ e $1 \leq j \leq m$, como a função de avaliação ev é um isomorfismo de $\mathbb{F}_q$-espaços vetoriais temos que existe $F' = \{f_1 + I, \ldots, f_r + I\} \in (\mathcal{L})_r$ tal que $\mathrm{ev}(f_j + I) = (f_j(P_1), \ldots, f_j(P_m)) = (\beta_{j1}, \ldots, \beta_{jm}) \coloneqq \beta_j$ para todo $j \in \{1, \ldots, r\}$. Observe que a j-ésima coluna de G não é nula se, e somente se, $P_j \in X \setminus V(F)$. Assim, pelo Lema 3.3 $|\chi(D)| = |X \setminus V(F)|$. Por outro lado, seja $F' = \{f_1 + I, \ldots, f_r + I\} \in (\mathcal{L})_r$ e defina $\beta_i = \mathrm{ev}(f_i + I) = (f_i(P_1), \ldots, f_i(P_m))$ para todo $i \in \{1, \ldots, r\}$. Tomando $D = \mathbb{F}_q\{\beta_1\} + \cdots + \mathbb{F}_q\{\beta_r\}$ temos que D é um subcódigo de $\mathcal{L}_X$ de $\dim_{\mathbb{F}_q} D = r$, pois como ev é um isomorfismo e $F' \in (\mathcal{L})_r$ o conjunto $\{\beta_1, \ldots, \beta_r\} \subset \mathcal{L}_X$ é linearmente independente e é uma base de D. Daí, usando novamente o Lema 3.3 segue que $|X \setminus V(F)| = |\chi(D)|$.

Portanto, pelo que foi provado acima, pelo Lema 3.17 e pelo fato da função de avaliação ev ser um isomorfismo temos que

$$\begin{aligned}
\delta_r(\mathcal{L}_X) &= \min\{|\chi(D)| \mid D \text{ é um subcódigo de } \mathcal{L}_X \text{ e } \dim_{\mathbb{F}_q} D = r\} \\
&= \min\{|X \setminus V(F)| \mid F' \in (\mathcal{L})_r\} \\
&= \min\{|X \setminus (V(F) \cap X)| \mid F' \in (\mathcal{L})_r\} \\
&= |X| - \max\{|V(F) \cap X| \mid F' \in (\mathcal{L})_r\} \\
&= m - \max\{|\Delta(I + (F))| \mid F' \in (\mathcal{L})_r\} \\
&= |\Delta(I)| - \max\{|\Delta(I + (F))| \mid F' \in (\mathcal{L})_r\}.
\end{aligned}$$

□

Definição 3.23. Seja X um subconjunto de $\mathbb{A}^n(\mathbb{F}_q)$ e fixe uma ordem monomial $\preccurlyeq$ em $\mathcal{M}$. Dado um subsespaço vetorial $\mathcal{L}$ de $\dfrac{\mathbb{F}_q[\mathbf{X}]}{I}$ e um inteiro $1 \leq r \leq \dim_{\mathbb{F}_q}\mathcal{L}$ definimos o conjunto

$$\mathrm{lm}_{\preccurlyeq}(\mathcal{L}) \coloneqq \{\mathrm{lm}(f) \mid f + I \in \mathcal{L}\},$$

lembrando que, segundo a observação 3.21, o representante f é escolhido de maneira específica, e definimos também

$$\mathcal{N}_{\preccurlyeq,r} \coloneqq \{N = \{N_1, \ldots, N_r\} \mid N \subset \mathrm{lm}_{\preccurlyeq}(\mathcal{L}) \text{ e } N_i \neq N_j \text{ para todo } i, j \in \{1, \ldots, r\}\}.$$

Definimos como **r-ésima pegada do código de avaliação $\mathcal{L}_X$** o número

$$\mathrm{fp}_r(\mathcal{L}_X) \coloneqq |\Delta(I)| - \max\{|\Delta(\mathrm{lm}(I) + (N))| \mid N \in \mathcal{N}_{\preccurlyeq,r}\},$$

onde $\mathrm{lm}(I)$ é o ideal gerado pelos monômios líderes (com relação a $\preccurlyeq$) de todos os elementos não nulos que estão em I.

Teorema 3.24. *Seja X um subconjunto de $\mathbb{A}^n(\mathbb{F}_q)$ e fixe uma ordem monomial $\preccurlyeq$. Seja $\mathcal{L}$ um subespaço vetorial de $\dfrac{\mathbb{F}_q[\boldsymbol{X}]}{I}$ e seja $\mathcal{L}_X$ o código de avaliação sobre X. Então*

$$\mathrm{fp}_r(\mathcal{L}_X) \leq \delta_r(\mathcal{L}_X) \text{ para } 1 \leq r \leq \dim_{\mathbb{F}_q}\mathcal{L}_X.$$

Demonstração. Pelo Teorema 3.22 existe $F' \in (\mathcal{L})_r$ tal que $\delta_r(\mathcal{L}_X) = |\Delta(I)| - |\Delta(I + (F))|$. Suponha que $F = \{f_1, \ldots, f_r\}$, como $F' = \{f_1 + I, \ldots, f_r + I\}$ é um conjunto linearmente independente então F é linearmente independente também. Se existir $i \in \{2, \ldots, r\}$ tal que $\mathrm{lm}(f_1) = \mathrm{lm}(f_i)$ tomamos $g_1 = f_1$, $g_i' = f_1 - \dfrac{lc(f_1)}{lc(f_i)} f_i$ e $g_j' = f_j$ se $\mathrm{lm}(f_j) \neq \mathrm{lm}(f_1)$, fazendo o mesmo processo (eliminação Gaussiana) que fizemos para f_1 obtemos um conjunto $G = \{g_1, \ldots, g_r\}$ tal que $\mathrm{lm}(g_i) \neq \mathrm{lm}(g_j)$ para todo $i, j \in \{1, \ldots, r\}$ e $(F) = (G)$. Assim, $\delta_r(\mathcal{L}_X) = |\Delta(I)| - |\Delta(I + (G))|$ e $\{\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_r)\} \in \mathcal{N}_{\preccurlyeq,r}$. Então, pelo Teorema 3.19, temos que

$$|\Delta(I + (G))| \leq |\Delta(\mathrm{lm}(I) + \mathrm{lm}(G))| \leq \max\{|\Delta(\mathrm{lm}(I) + (N))| \mid N \in \mathcal{N}_{\preccurlyeq,r}\}.$$

Portanto,

$$\mathrm{fp}_r(\mathcal{L}_X) = |\Delta(I)| - \max\{|\Delta(\mathrm{lm}(I) + (N))| \mid N \in \mathcal{N}_{\preccurlyeq,r}\} \leq |\Delta(I)| - |\Delta(I + (G))| = \delta_r(\mathcal{L}_X),$$

ou seja, a r-ésima pegada $\mathrm{fp}_r(\mathcal{L}_X)$ é uma cota inferior para o r-ésimo peso de Hamming generalizado $\delta_r(\mathcal{L}_X)$.

□

3.2.1 Códigos do tipo Reed-Muller

Definição 3.25. Fixe um grau $d \geq 1$, considere o $\mathbb{F}_q$-subespaço vetorial $L_{\leq d}$ de $\dfrac{\mathbb{F}_q[\mathbf{X}]}{I}$ como na Definição 2.27 e seja $X = \{P_1, \ldots, P_m\}$ um subconjunto de $\mathbb{A}^n(\mathbb{F}_q)$. O código de avaliação $\mathrm{ev}(L_{\leq d}) \coloneqq \mathcal{C}_X(d)$ é chamado de **código do tipo Reed-Muller de grau d sobre X**.

Proposição 3.26. *Para todo $d \geq 1$ as seguintes afirmações são verdadeiras*

i) $\dim_{\mathbb{F}_q}\mathcal{C}_X(d) = |\Delta(I) \cap \mathbb{F}_q[\boldsymbol{X}]_{\leq d}|$.

ii) $\dim_{\mathbb{F}_q}\mathcal{C}_X(d) \leq \dim_{\mathbb{F}_q}\mathcal{C}_X(d+1)$.

iii) $\dim_{\mathbb{F}_q}\mathcal{C}_X(d) = m$ *para todo* $d \geq m - 1$.

iv) Se $\delta(\mathcal{C}_X(d)) \geq 2$ *então* $\delta(\mathcal{C}_X(d+1)) < \delta(\mathcal{C}_X(d))$, *e se* $\delta(\mathcal{C}_X(d)) = 1$ *então* $\delta(\mathcal{C}_X(e)) = 1$ *para todo* $e \geq d$.

v) $\delta(\mathcal{C}_X(d)) = 1$ *para todo* $d \geq m - 1$.

Demonstração. (i) Como a função de avaliação é um isomorfismo temos que $\dim_{\mathbb{F}_q} L_{\leq d} = \dim_{\mathbb{F}_q} \mathcal{C}_X(d)$ para todo $d \geq 1$ e pela Proposição 2.30 $\dim_{\mathbb{F}_q} L_{\leq d} = |\Delta(I) \cap \mathbb{F}_q[\mathbf{X}]_{\leq d}|$.

(ii) Seja $P \in \mathcal{C}_X(d)$ então existe $f + I \in L_{\leq d}$ tal que $P = (f(P_1), \ldots, f(P_m))$. Como $\deg(f) \leq d < d+1$ segue que $P \in C_X(d+1)$, logo $\mathcal{C}_X(d) \subset \mathcal{C}_X(d+1)$ para todo $d \geq 1$. Portanto, $\dim_{\mathbb{F}_q} \mathcal{C}_X(d) \leq \dim_{\mathbb{F}_q} \mathcal{C}_X(d+1)$ para todo $d \geq 1$.

(iii) Como $V(I) = V(\mathcal{I}(X)) = X = \{P_1, \ldots, P_m\}$ pela Proposição 1.44 existem polinômios $p_1, \ldots, p_m$, com $\deg(p_j) = m - 1 \leq d$ para todo $j \in \{1, \ldots, m\}$, tais que $\mathrm{ev}(p_j + I) = \boldsymbol{e_j} = (0, \ldots, 1, 0, \ldots, 0)$ (onde 1 está na j-ésima coordenada) para todo $1 \leq j \leq m$. Portanto, como $p_j + I \in L_{\leq d}$ para todo $1 \leq j \leq m$, $\mathcal{C}_X(d) \subset \mathbb{F}_q^m$ e $\{\boldsymbol{e_1}, \ldots, \boldsymbol{e_m}\} \subset \mathcal{C}_X(d)$ é uma base de $\mathbb{F}_q^m$ segue que $\dim_{\mathbb{F}_q} \mathcal{C}_X(d) = m$ para todo $d \geq m - 1$.

(iv) No item (ii) provamos que $\mathcal{C}_X(d) \subset \mathcal{C}_X(d+1)$ para todo $d \geq 1$, logo $\{\omega(\mathbf{a}) \mid \mathbf{a} \in \mathcal{C}_X(d) \setminus \{0\}\} \subset \{\omega(\mathbf{b}) \mid \mathbf{b} \in \mathcal{C}_X(d+1) \setminus \{0\}\}$, e então $\delta(\mathcal{C}_X(d+1)) \leq \delta(\mathcal{C}_X(d))$ para todo $d \geq 1$. Primeiro façamos o caso quando $\delta(\mathcal{C}_X(d)) \geq 2$. Seja $f + I \in L_{\leq d}$ tal que $P = (f(P_1), \ldots, f(P_m))$ e $\omega(P) = \delta(\mathcal{C}_X(d)) \geq 2$. Então, sem perda de generalidade, suponha que $f(P_i) \neq 0$ para $1 \leq i \leq 2$. Considere $P_1 = (a_1, \ldots, a_n)$ e $P_2 = (b_1, \ldots, b_n)$, como $P_1 \neq P_2$ existe $k \in \{1, \ldots, n\}$ tal que $a_k \neq b_k$, e defina $g = f.(a_k - X_k)$. Logo $g + I \in L_{\leq d+1}$, $g(P_1) = 0$ e $g(P_2) \neq 0$, então g tem mais zeros do que f. Portanto, $\delta(\mathcal{C}_X(d+1)) \leq \omega(Q) < \omega(P) = \delta(\mathcal{C}_X(d))$ onde $Q = (0, g(P_2), \ldots, g(P_m)) \in \mathcal{C}_X(d+1) \setminus \{0\}$.

Se $\delta(\mathcal{C}_X(d)) = 1$, pela desigualdade que mostramos no início da demonstração, o resultado segue.

(v) Como $d \geq m - 1$, pelo item (iii), $\mathcal{C}_X(d) = \mathbb{F}_q^m$. Logo $\delta(\mathcal{C}_X(d)) = 1$ para todo $d \geq m - 1$. □

Corolário 3.27. *Seja $X = \{P_1, \ldots, P_m\}$ um subconjunto de $\mathbb{A}^n(\mathbb{F}_q)$. Então*

$$\delta_r(\mathcal{C}_X(d)) = |\Delta(I)| - \max\{|\Delta(I + (F))| \mid F' \in (L_{\leq d})_r\} \text{ para } 1 \leq r \leq \dim_{\mathbb{F}_q} \mathcal{C}_X(d) = |\Delta(I) \cap \mathbb{F}_q[\boldsymbol{X}]_{\leq d}|.$$

Demonstração. Segue diretamente do Teorema 3.22 e do item (i) da Proposição anterior. □

Corolário 3.28. *Seja X um subconjunto de $\mathbb{A}^n(\mathbb{F}_q)$ e seja $L_d \coloneqq \{f + I \mid deg(f) = d\}$. Se $d \geq 2$ e $\delta(\mathcal{C}_X(d-1)) > 1$ então*

$$\delta(\mathcal{C}_X(d)) = |\Delta(I)| - \max\{|\Delta(I + (f))| \mid f + I \in L_d\}.$$

Demonstração. Pelo Corolário anterior temos que

$$\begin{aligned} \delta(\mathcal{C}_X(d)) &= |\Delta(I)| - \max\{|\Delta(I + (f))| \mid f + I \in L_{\leq d} \setminus \{0\}\} \\ &\leq |\Delta(I)| - \max\{|\Delta(I + (f))| \mid f + I \in L_d\}. \end{aligned}$$

Isso prova a desigualdade "$\leq$". Para mostrar a desiguladade "$\geq$" tome $f + I \in L_{\leq d} \setminus \{0\}$ tal que $\delta(\mathcal{C}_X(d)) = |\Delta(I)| - |\Delta(I + (f))|$. É suficiente provar que f tem grau d, pois nesse caso $-|\Delta(I + (f))| \geq -\max\{|\Delta(I + (f))| \mid f \in L_d\}$, e assim a equação acima se torna uma igualdade. Suponha, por contradição, que $\deg(f) < d$, então pelo item (iv) da Proposição 3.26 e pelo Corolário acima temos

$$\delta(\mathcal{C}_X(d)) < \delta(\mathcal{C}_X(d-1)) \leq |\Delta(I)| - |\Delta(I + (f))| = \delta(\mathcal{C}_X(d)),$$

o que é uma contradição. Portanto, $\deg(f) = d$. □

3.2.2 Códigos Tóricos

O próximo tipo de código foi introduzido por Hansen em [6].

Definição 3.29. Seja $1 \leq d \leq n$ um inteiro e $n \geq 2$. O **toro afim** do espaço afim $\mathbb{A}^n(\mathbb{F}_q)$ é dado por $T \coloneqq (\mathbb{F}_q^*)^n$. Definimos o conjunto

$$\begin{aligned} V_d &\coloneqq \left\{ X_1^{\alpha_1} \cdots X_n^{\alpha_n} + I \mid \alpha_j \in \{0,1\} \text{ para todo } j \in \{1, \cdots, n\} \text{ e } \sum_{i=1}^{n} \alpha_i = d \right\} \\ &= \{M + I \mid M \in \mathcal{M} \text{ é livre de quadrados e } \deg(M) = d\}, \end{aligned}$$

onde $I = \mathcal{I}(T)$. O **código tórico de grau** d é $ev(\mathbb{F}_q V_d) =: \mathcal{C}_d$ (considerando $X = T$).

Lema 3.30. *Sejam $d_1, \ldots, d_n$ inteiros positivos e seja $L = (X_1^{d_1}, \ldots, X_n^{d_n})$. Se $M = X_1^{a_1} \cdots X_n^{a_n}$ não estiver em L então*

$$|\Delta(L + (M))| = d_1 \cdots d_n - \prod_{i=1}^{n} (d_i - a_i).$$

Demonstração. Seja $M = X_1^{a_1} \cdots X_n^{a_n}$ um monômio que não está em L. Então M não é um múltiplo de $X_j^{d_j}$ para todo $j \in \{1, \ldots, n\}$, logo $0 \leq a_j < d_j$ para todo $1 \leq j \leq n$.

Observe que $\{X_1^{d_1}, \ldots, X_n^{d_n}\}$ é uma base de Gröbner de L e

$$\Delta(L) = \{N = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \mid 0 \leq \alpha_j < d_j \text{ para todo } j \in \{1, \ldots, n\}\}.$$

Logo $|\Delta(L)| = d_1 \cdots d_n$. Também temos que $\Delta(L + (M)) \subset \Delta(L)$, pois $L \subset L + (M)$, então

$$|\Delta(L + (M))| = |\Delta(L)| - |\{N \in \Delta(L) \mid N \notin \Delta(L + (M))\}|. \tag{3.1}$$

Temos

$$\begin{aligned} &\{N = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in \Delta(L) \mid N \notin \Delta(L + (M))\} \\ =&\{X_1^{\alpha_1} \cdots X_n^{\alpha_n} \mid a_j \leq \alpha_j < d_j \text{ para todo } j \in \{1, \ldots, n\}\}, \end{aligned}$$

pois $\{X_1^{d_1}, \ldots, X_n^{d_n}, M\}$ é uma base de Gröbner de $L + (M)$. Daí,

$$|\{N = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in \Delta(L) \mid N \notin \Delta(L + (M))\}| = \prod_{i=1}^{n} (d_i - a_i).$$

Portanto, de 3.1

$$|\Delta(L + (M))| = d_1 \cdots d_n - \prod_{i=1}^{n} (d_i - a_i).$$

□

Lema 3.31. *Se $q \geq 3$, então $\mathrm{lm}(I) = (X_1^{q-1}, \ldots, X_n^{q-1})$. Se M é um monômio livre de quadrados, então $M \in \Delta(I)$.*

Demonstração. Como $T = \mathbb{F}_q^* \times \cdots \times \mathbb{F}_q^*$ segue do Lema 2.29 que $I = (f_1, \ldots, f_n)$, onde $f_j = \prod_{\gamma \in \mathbb{F}_q^*} (X_j - \gamma)$ para todo $1 \leq j \leq n$. Então $f_j = X_j^{q-1} - 1$ para todo $1 \leq j \leq n$, pois $\prod_{\gamma \in \mathbb{F}_q} (X_j - \gamma) = X_j^q - X_j$ para todo $1 \leq j \leq n$, ou seja, $I = (X_1^{q-1} - 1, \ldots, X_n^{q-1} - 1)$. Pelo Lema 2.28 $\{X_1^{q-1} - 1, \ldots, X_n^{q-1} - 1\}$ é uma base de Gröbner de I, logo $\mathrm{lm}(I) = (X_1^{q-1}, \ldots, X_n^{q-1})$.

Agora seja M é um monômio livre de quadrados, então $M = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ com α_j igual a 0 ou 1 para todo $1 \leq j \leq n$, como $q \geq 3$ e $\mathrm{lm}(I) = (X_1^{q-1}, \ldots, X_n^{q-1})$ segue que $M \notin \mathrm{lm}(I)$, ou seja, $M \in \Delta(I)$. □

O próximo resultado é verdadeiro independentemente da escolha do representante de $f+I$.

Proposição 3.32. *Se $f+I \neq 0+I \in \mathbb{F}_q V_d, q \geq 3$ e $1 \leq d < n$, então*

$$|V(f) \cap T| \leq (q-1)^n - (q-2)^d (q-1)^{n-d}.$$

Demonstração. Primeiro vamos mostrar que $|V(f) \cap T|$ não depende do representante da classe $f+I$. De fato, se $f+I = g+I$ então $g = f+h$ para algum $h \in I$, logo, se $P \in V(f) \cap T$ temos que $g(P) = f(P) + h(P) = 0$, pois $h \in \mathcal{I}(T)$. Da mesma forma, se $P \in V(g) \cap T$ temos que $f(P) = 0$.

Seja $0+I \neq f+I \in \mathbb{F}_q V_d$, considerando $f = \sum_{i=1}^{s} \alpha_i M_i$, onde M_i é um monômio livre de quadrados e $\deg(M_i) = d$ para todo $1 \leq i \leq s$, pelo Lema anterior $M \coloneqq \operatorname{lm}(f) \in \Delta(I)$ logo $M \notin \operatorname{lm}(I) = (X_1^{q-1}, \ldots, X_n^{q-1})$. Como M é livre de quadrados e tem grau d temos que, escrevendo $M = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, existem $n-d$ potências iguais a 0 e d potências iguais a 1. Portanto, pelo Teorema 3.19 e pelo Lema 3.30 temos que

$$|V(f) \cap T| \leq |\Delta(\operatorname{lm}(I) + (M))| = (q-1)^n - ((q-1)-1)^d ((q-1)-0)^{n-d} = (q-1)^n - (q-2)^d (q-1)^{n-d}.$$

□

Proposição 3.33. *Seja $\mathcal{C}_d$ o código tórico de grau d. Então o comprimento de $\mathcal{C}_d$ é igual a $(q-1)^n, \dim_{\mathbb{F}_q}(\mathcal{C}_d) = \binom{n}{d}$ se $q \geq 3$, e $\dim_{\mathbb{F}_q}(\mathcal{C}_d) = 1$ se $q = 2$.*

Demonstração. O comprimento de $\mathcal{C}_d$ é igual a $|T| = (q-1)^n$.

Se $q \geq 3$, então pelo Lema 3.31 $V_d \subset \mathcal{B} = \{M + I \mid M \in \Delta(I)\}$ logo V_d é um conjunto linearmente independente, pois $\mathcal{B}$ é uma base de $\dfrac{\mathbb{F}_q[\mathbf{X}]}{I}$ como $\mathbb{F}_q$-espaço vetorial. Como

$$V_d = \left\{ X_1^{\alpha_1} \cdots X_n^{\alpha_n} + I \mid \alpha_j \in \{0,1\} \text{para todo } j \in \{1, \cdots, n\} \text{ e } \sum_{i=1}^{n} \alpha_i = d \right\},$$

segue que $\dim_{\mathbb{F}_q} \mathcal{C}_d = \dim_{\mathbb{F}_q} \mathbb{F}_q V_d = |V_d| = \binom{n}{d}$.

Se $q = 2$ temos que $T = \{(1, \ldots, 1)\}$, logo $\mathcal{C}_d = \mathbb{F}_2$ (pois $ev(X_1 X_2 \cdots X_d + I) = 1 \neq 0$). Portanto, $\dim_{\mathbb{F}_q} \mathcal{C}_d = 1$ se $q = 2$. □

Teorema 3.34. *Seja $\mathcal{C}_d$ o código tórico de grau d. Então*

$$\delta(\mathcal{C}_d) = \begin{cases} (q-2)^d (q-1)^{n-d} & \text{se } d \leq \dfrac{n}{2}, q \geq 3, \\ (q-2)^{n-d} (q-1)^d & \text{se } \dfrac{n}{2} < d < n, q \geq 3, \\ (q-1)^n & \text{se } d = n, \\ 1 & \text{se } q = 2. \end{cases}$$

Demonstração. Suponha que $n \geq 2d$ e $q \geq 3$. Defina $\eta(d) \coloneqq (q-2)^d (q-1)^{n-d}$ e $\phi(d) \coloneqq (q-1)^n - \eta(d)$. Pelo Teorema 3.22 e pelo Lema 3.17 temos que existe $0+I \neq f+I \in \mathbb{F}_q V_d$, tal que

$$\begin{aligned} \delta(\mathcal{C}_d) &= |\Delta(I)| - \max\{|\Delta(I + (g))| \mid 0 + I \neq g + I \in \mathbb{F}_q V_d\} \\ &= (q-1)^n - |\Delta(I + (f))| = (q-1)^n - |V(f) \cap T|. \end{aligned}$$

Assim, pela Proposição 3.32, temos que $|V(f) \cap T| \leq \phi(d)$ e portanto $\delta(\mathcal{C}_d) \geq \eta(d)$. Considere o polinômio

$$f_d = h_1 \cdots h_d = (X_1 - X_2) \cdots (X_{2d-1} - X_{2d}),$$

onde $h_i = X_{2i-1} - X_{2i}$ para $i = 1, \ldots, d$. É fácil ver que $f_d + I \in \mathbb{F}_q V_d$. Vamos provar que f_d não zera em $\eta(d)$ pontos de T. Seja $P = (a_1, \ldots, a_n) \in T = (\mathbb{F}_q^*)^n$, para f_d não zerar em P devemos ter $a_{2i-1} \neq a_{2i}$, $1 \leq i \leq d$ e a_j pode ser qualquer elemento de $\mathbb{F}_q^*$ para todo $j \in \{2d+1, \ldots, n\}$. Assim, em h_i temos $q-1$ possibilidades de elementos de $\mathbb{F}_q^*$ para uma variável e $q-2$ possibilidades para a outra variável, $i = 1, \ldots, d$. Logo a quantidade de pontos de T que não zeram f_d é $(q-1)^d(q-2)^d(q-1)^{n-2d} = (q-2)^d(q-1)^{n-d} = \eta(d)$. Assim, $\eta(d) = \omega(ev(f_d + I)) \geq \delta(\mathcal{C}_d) \geq \eta(d)$. Portanto, $\delta(\mathcal{C}_d) = \eta(d) = (q-2)^d(q-1)^{n-d}$ quando $d \leq \dfrac{n}{2}$ e $q \geq 3$.

Suponha que $n < 2d, d < n$ e $q \geq 3$. O toro afim é um grupo multiplicativo com a operação de multiplicação componente a componente e a função $\sigma : T \longrightarrow T, (a_1, \ldots, a_n) \mapsto (a_1^{-1}, \ldots, a_n^{-1})$ é um isomorfismo de grupo. Definindo $Q_i \coloneqq \sigma(P_i)$ para $i = 1, \ldots, m$, podemos escrever

$$T = \{P_1, \ldots, P_m\} = \{Q_1, \ldots, Q_m\}.$$

Vamos denotar o código tórico de grau d com respeito a $\{P_1, \ldots, P_m\}$ por $\mathcal{C}_d$ e vamos denotar o código tórico de grau $n-d$ com respeito a $\{Q_1, \ldots, Q_m\}$ por $\mathcal{C}_{n-d}$. Assim,

$$\mathcal{C}_d = \{(f(P_1), \ldots, f(P_m)) \mid f \in \mathbb{F}_q V_d\},$$
$$\mathcal{C}_{n-d} = \{g(Q_1), \ldots, g(Q_m)) \mid g \in \mathbb{F}_q V_{n-d}\}.$$

Observe que os parâmetros básicos do código tórico de grau $n-d$ com respeito a $\{P_1, \ldots, P_m\}$ é o mesmo que o código tórico de grau $n-d$ com respeito a qualquer reordenação dos pontos de $\{P_1, \ldots, P_m\}$.

Seja $\{M_1, \ldots, M_\ell\}$ o conjunto de todos os monômios livres de quadrados de S de grau d. Defina $M_i^c \coloneqq \dfrac{X_1 \cdots X_n}{M_i}$ para $i = 1, \ldots, n$, note que $\{M_1^c, \ldots, M_\ell^c\}$ é o conjunto de todos os monômios livres de quadrados de S de grau $n-d$. Dado $f + I \in \mathbb{F}_q V_d$ podemos tomar $f = \sum_{i=1}^{\ell} \lambda_i M_i$ (existe um único tal representante), e definimos $f^c = \sum_{i=1}^{\ell} \lambda_i M_i^c$. Das igualdades

$$\begin{aligned} X_1 \cdots X_n f^c(\frac{1}{X_1}, \ldots, \frac{1}{X_n}) &= X_1 \cdots X_n \sum_{i=1}^{\ell} \lambda_i M_i^c(\frac{1}{X_1}, \ldots, \frac{1}{X_n}) \\ &= \sum_{i=1}^{\ell} \lambda_i M_i(X_1, \ldots, X_n) = f(X_1, \ldots, X_n), \end{aligned}$$

temos que $X_1 \cdots X_n f^c(X_1^{-1}, \ldots, X_n^{-1}) = f(X_1, \ldots, X_n)$. Logo, tomando $P_k = (a_{k1}, \ldots, a_{kn})$ temos que

$$a_{k1} \cdots a_{kn} f^c(a_{k1}^{-1}, \ldots, a_{kn}^{-1}) = a_{k1} \cdots a_{kn} f^c(Q_k) = f(P_k) \tag{3.2}$$

para $k = 1, \ldots, m$. Observe que a aplicação $\psi : \mathbb{F}_q V_d \to \mathbb{F}_q V_{n-d}$, dada por $\psi(f + I) = f^c + I$ é um isomorfismo de espaços vetoriais. Existe um diagrama comutativo

$$\begin{array}{ccc} \mathbb{F}_q V_d & \xrightarrow{\text{ev}} & \mathcal{C}_d \\ \downarrow \psi & & \downarrow \psi' \\ \mathbb{F}_q V_{n-d} & \xrightarrow{\text{ev}} & \mathcal{C}_{n-d} \end{array} \quad \text{dado por} \quad \begin{array}{ccc} f + I & \to & (f(P_1), \ldots, f(P_m)) \\ \downarrow & & \downarrow \\ f^c + I & \to & (f^c(Q_1), \ldots, f^c(Q_m)) \end{array}$$

e usando que ψ e as aplicações ev são isomorfismos temos que ψ' é um isomorfismos de $\mathbb{F}_q$-espaços vetoriais. Pela Equação 3.2, $f(P_k) = 0$ se, e somente se, $f^c(Q_k) = 0$ para todo $k = 1, \ldots, m$. Assim, os códigos lineares $\mathcal{C}_d$ e $\mathcal{C}_{n-d}$ tem a mesma distância mínima. Como $\dfrac{n}{2} < d$ temos que $n - d < \dfrac{n}{2}$, pela parte anterior , segue que

$$\delta(\mathcal{C}_{n-d}) = (q-2)^{n-d}(q-1)^d.$$

Portanto, a distância mínima de $\mathcal{C}_d$ é igual a $(q-2)^{n-d}(q-1)^d$.

Suponha que $d = n$. Então $\mathbb{F}_q V_d = \mathbb{F}_q\{f+I \coloneqq X_1 \cdots X_n + I\}$ e $\mathcal{C}_d = \mathbb{F}_q\{(f(P_1), \ldots, f(P_m))\}$. Como as coordenadas de P_k são todas diferentes de zero para todo $k \in \{1, \ldots, m\}$ segue que todas as coordenadas de $\{(f(P_1), \ldots, f(P_m))\}$ são nulas. Portanto, $\delta(\mathcal{C}_d) = m = (q-1)^n$.

Suponha que $q = 2$. Então $T = \{(1, \ldots, 1)\}, m = 1$ e $\mathcal{C}_d = \mathbb{F}_2$, portanto, $\delta(\mathcal{C}_d) = 1$. □

Corolário 3.35. *Seja f um polinômio homogêneo monomialmente livre de quadrados de grau $d \geq 1$, ou seja, $f = \sum_{i=1}^{\ell} \lambda_i M_i$ onde M_i é um monômio livre de quadrados de grau d para todo $1 \leq i \leq \ell$. Se $q \geq 3$ e $\frac{n}{2} < d < n$, então*

$$|V(f) \cap T| \leq (q-1)^n - (q-2)^{n-d}(q-1)^d,$$

e existe um polinômio monomialmente livre de quadrados de grau d tal que a igualdade é válida.

Demonstração. Pelo teorema anterior temos que

$$\delta(\mathcal{C}_d) = (q-2)^{n-d}(q-1)^d.$$

Portanto, se $f \notin \mathbb{F}_q$ é um polinômio homogêneo monomialmente livre de quadrados de grau d, então $f + I \in \mathbb{F}_q V_d$ e $|V(f) \cap T| \leq (q-1)^n - \delta(\mathcal{C}_d) = (q-1)^n - (q-2)^{n-d}(q-1)^d$.

Agora vamos construir um polinômio homogêneo monomialmente livre de quadrados de grau d tal que a igualdade é válida. Como $d+1 \leq n \leq 2d-1$ existe $1 \leq k \leq d-1$ tal que $n = d+k$, e observe que $2k < n$, pois $n < 2d$, logo $2(n-d) < n$. Considere o seguinte polinômio homogêneo monomialmente livre de quadrados de grau $k = n - d$

$$g_k \coloneqq h_1 \ldots h_k = (X_1 - X_2) \cdots (X_{2k-1} - X_{2k}),$$

onde $h_i = X_{2i-1} - X_{2i}$ para $i = 1, \ldots, k$. Como $n < 2d$, utilizando o mesmo argumento da primeira parte da demonstração do Teorema anterior, temos que a quantidade de pontos de T que g_k não se anula é $(q-2)^k(q-1)^{n-k} = (q-2)^{n-d}(q-1)^d$. Portanto,

$$|V(g_k) \cap T| = (q-1)^n - (q-2)^{n-d}(q-1)^d.$$

Na segunda parte do Teorema anterior provamos que $\psi : \mathbb{F}_q V_{n-d} \longrightarrow \mathbb{F}_q V_d$ é um isomorfismo de espaços vetoriais, onde $\psi(g + I) = g^c + I$, e que $g(Q_k) = 0$ se, e somente se, $g^c(P_k) = 0$. Portanto,

$$|V(g_k^c) \cap T| = |V(g_k) \cap T| = (q-1)^n - (q-2)^{n-d}(q-1)^d$$

e g_k^c é um polinômio monomialmente livre de quadrados de grau d. □

A distância mínima $\delta(\mathcal{C}_T(d))$ do código afim do tipo Reed-Muller $\mathcal{C}_T(d)$ é não-crescente como função de d (Proposição 3.26). No entanto, isso não ocorre com a distância mínima do código tórico $\mathcal{C}_d$ como veremos no exemplo abaixo.

Exemplo 3.36. Se $n = 5$ e $q = 4$, usando o Teorema 3.34, obtemos a lista de valores dos comprimentos, dimensões e distâncias mínimas de $\mathcal{C}_d$, para $1 \leq d \leq 5$ dados na tabela abaixo.

3.2.3 Códigos de Avaliação Afins Livre de Quadrados

Definição 3.37. Sejam $d \leq n$ um inteiro e $T = (\mathbb{F}_q^*)^n$ o toro afim. Definimos o conjunto

$$V_{\leq d} \coloneqq \{M + I \mid M \in \mathcal{M} \text{ é livre de quadrados e } 0 \leq \deg(M) \leq d\},$$

onde $I = \mathcal{I}(T)$. O **código de avaliação livre de quadrados de grau d sobre T** é $ev(\mathbb{F}_q V_{\leq d}) =: \mathcal{C}_{\leq d}$ (considerando $X = T$).

Tabela 3.1: Parâmetros Básicos de um código tórico

d	1	2	3	4	5
m	243	243	243	243	243
$\dim_{\mathbb{F}_q} \mathcal{C}_d$	5	10	10	5	1
$\delta(\mathcal{C}_d)$	54	108	108	54	1

Proposição 3.38. *Seja $f + I \neq 0 + I \in \mathbb{F}_q V_{\leq d}$. Se $q \geq 3$ e $d \leq n$, então*

$$|V(f) \cap T| \leq (q-1)^n - (q-2)^d (q-1)^{n-d},$$

com igualdade se $f = (X_1 - 1) \cdots (X_d - 1)$.

Demonstração. Procedendo como na demonstração da Proposição 3.32 pode-se mostrar que $|V(f) \cap T|$ não depende do representante de $f + I$.

Seja $f + I \neq 0 + I \in \mathbb{F}_q V_{\leq d}$ e considere $f = \sum_{i=1}^{\ell} \lambda_i M_i$, onde M_i é um monômio livre de quadrados e $\deg(M_i) \leq d$ para todo $1 \leq i \leq \ell$. Se $e = \deg(f)$, temos que

$$\begin{aligned}
&\frac{1}{q-1} \leq \frac{1}{q-2} \Rightarrow \frac{1}{(q-1)^{d-e}} \leq \frac{1}{(q-2)^{d-e}} \\
\Rightarrow &\frac{1}{(q-1)^{d-e}} \leq \frac{(q-2)^e}{(q-2)^d} \Rightarrow \frac{(q-1)^n}{(q-1)^{d-e+n}} \leq \frac{(q-2)^e}{(q-2)^d} \\
\Rightarrow &\frac{(q-1)^{n-d}}{(q-1)^{n-e}} \leq \frac{(q-2)^e}{(q-2)^d} \Rightarrow (q-2)^d (q-1)^{n-d} \leq (q-2)^e (q-1)^{n-e} \\
\Rightarrow &(q-1)^n - (q-2)^e (q-1)^{n-e} \leq (q-1)^n - (q-2)^d (q-1)^{n-d}.
\end{aligned}$$

Observando o que queremos mostrar podemos supor que $d = \deg(f)$. Seja $\preccurlyeq_{\text{grlex}}$ a ordem lexicográfica graduada em $\mathcal{M}$ e $M = \text{lm}(f)$ o monômio líder de f com respeito a $\preccurlyeq_{\text{grlex}}$. Observe que M é livre de quadrados e $d = \deg(M)$. Pelo Lema 3.31 $L \coloneqq \text{lm}(I)$ é gerado pelo conjunto de monômios $\{X_i^{q-1}\}_{i=1}^n$. Como $q \geq 3, M \notin L$. Assim, pelo Teorema 3.19 e pelo Lema 3.30, temos que

$$\begin{aligned}
|V(f) \cap T| = |\Delta(I + (f))| &\leq |\Delta(L + (M))| = (q-1)^n - ((q-1)-1)^d (q-1)^{n-d} \\
&= (q-1)^n - (q-2)^d (q-1)^{n-d}.
\end{aligned}$$

Agora, suponha que $f = h_1 \cdots h_d$, onde $h_i = X_i - 1$ para $i = 1, \ldots, d$. É fácil ver que $f + I \in \mathbb{F}_q V_{\leq d}$. Como feito na demonstração da primeira parte do Teorema 3.34 pode-se mostrar que $|V(f) \cap T| = (q-1)^n - (q-2)^d (q-1)^{n-d}$. □

Proposição 3.39. *Seja $\mathcal{C}_{\leq d}$ um código de avaliação livre de quadrados sobre $T = (\mathbb{F}_q^*)^n$. Então o comprimento de $\mathcal{C}_{\leq d}$ é $(q-1)^n, \dim \mathcal{C}_{\leq d} = \sum_{i=0}^{d} \binom{n}{i}$ se $q \geq 3$, e $\dim \mathcal{C}_{\leq d} = 1$ se $q = 2$.*

Demonstração. O comprimento m do código $\mathcal{C}_{\leq d}$ é o número de pontos de T, ou seja, $m = (q-1)^n$. Suponha que $q \geq 3$, pelo Lema 3.31 temos que $V_{\leq d} \subset \mathcal{B} = \{M + I \mid M \in \Delta(I)\}$ logo V_d é um conjunto linearmente independente, pois $\mathcal{B}$ é uma base de $\dfrac{\mathbb{F}_q[\mathbf{X}]}{I}$ como $\mathbb{F}_q$-espaço vetorial. Como

$$V_{\leq d} = \bigcup_{k=0}^{d} \left\{ X_1^{\alpha_1} \cdots X_n^{\alpha_n} + I \mid \alpha_j \in \{0,1\} \text{para todo } j \in \{1, \cdots, n\} \text{ e } \sum_{i=1}^{n} \alpha_i = k \right\},$$

segue que $\dim \mathcal{C}_{\leq d} = \dim \mathbb{F}_q V_{\leq d} = \sum_{i=0}^{d} \binom{n}{i}$.

Suponha que $q = 2$, então $T = \{(1, \ldots, 1)\}$ logo $\mathcal{C}_{\leq d} = \mathbb{F}_2$ (pois $ev(X_1 X_2 \cdots X_d + I) = 1 \neq 0$). Portanto, $\dim_{\mathbb{F}_q} \mathcal{C}_{\leq d} = 1$ se $q = 2$. □

Corolário 3.40. *Seja $\mathcal{C}_{\leq d}$ um código de avaliação livre de quadrados sobre T. Então*

$$\delta_r(\mathcal{C}_{\leq d}) = |\Delta(I)| - \max\{|\Delta(I + (F))| \mid F' \in (\mathbb{F}_q V_{\leq d})_r\} \text{ para } d \geq 1 \text{ e } 1 \leq r \leq \dim_{\mathbb{F}_q} \mathcal{C}_{\leq d}.$$

Demonstração. Segue diretamente do Teorema 3.22. □

Para mostrar uma cota inferior para $\delta_r(\mathcal{C}_{\leq d})$, seja $\mathcal{J}_{d,r}$ a família de todos conjuntos $S = \{M_1, \ldots, M_r\}$ tal que $M_1, \ldots, M_r$ são monômios livres de quadrados distintos de $\mathbb{F}_q[\mathbf{X}]_{\leq d}$. A r-ésima pegada livre de quadrados de $\mathcal{C}_{\leq_d}$ de grau d, denotada por $\rho_I(d, r)$, é dada por

$$\rho_I(d, r) \coloneqq |\Delta(I)| - \max\{|\Delta(\mathrm{lm}(I) + (S))| \mid S \in \mathcal{J}_{d,r}\}.$$

Corolário 3.41. *$\rho_I(d, r) \leq \delta_r(\mathcal{C}_{\leq d})$ para $d \geq 1$ e $1 \leq r \leq \dim_{\mathbb{F}_q} \mathcal{C}_{\leq d}$.*

Demonstração. Segue diretamente do Teorema 3.24. □

Teorema 3.42. *Seja $\mathcal{C}_{\leq d}$ o código de avaliação livre de quadrados sobre o toro afim T. Se $q \geq 3$, então a distância mínima $\delta(\mathcal{C}_{\leq d})$ de $\mathcal{C}_{\leq d}$ é $(q-2)^d(q-1)^{n-d}$.*

Demonstração. Pelo Corolário 3.40 temos que

$$\begin{aligned}\delta(\mathcal{C}_{\leq d}) =& |\Delta(I)| - \max\{|\Delta(I + (f))| \mid f + I \in (\mathbb{F}_q V_{\leq d})^*\} \\ =& |T| - \max\{|V(f) \cap T| \mid f + I \in (\mathbb{F}_q V_{\leq d})^*\}.\end{aligned}$$

Como $q \geq 3$, pela Proposição 3.38, temos que

$$\max\{|V(f) \cap T| \mid f + I \in (\mathbb{F}_q V_{\leq d})^*\} \leq |T| - (q-2)^d(q-1)^{n-d}.$$

Logo,

$$\delta(\mathcal{C}_{\leq d}) \geq (q-2)^d(q-1)^{n-d}.$$

Novamente, pela Proposição 3.38, existe $f + I \in \mathbb{F}_q V_{\leq d}$ tal que $\omega(\mathrm{ev}(f + I)) = (q-2)^d(q-1)^{n-d}$. Portanto, $\delta(\mathcal{C}_{\leq d}) = (q-2)^d(q-1)^{n-d}$. □

Teorema 3.43. *Se $q \geq 3$ e $d \geq 1$, então o segundo peso de Hamming generalizado de $\mathcal{C}_{\leq d}$ é*

$$\delta_2(\mathcal{C}_{\leq d}) = \begin{cases} (q-2)^{n-1}(q-1) & \text{se } d = n \\ (q-2)^d(q-1)^{n-d-1}q & \text{se } d < n. \end{cases}$$

Demonstração. Primeiro vamos mostrar que se $n = 1$ (logo $d = n = 1$ e $T = \mathbb{F}_q^*$) então $\delta_2(\mathcal{C}_{\leq 1}) = q - 1$. De fato, como $q \geq 3$ pela Proposição 3.39 $\dim_{\mathbb{F}_q} \mathcal{C}_{\leq 1} = 2$, e veja que $\{1 + I, X_1 + I\}$ é uma base de $\mathcal{C}_{\leq 1}$. Como $\mathrm{ev}(1 + I) = (1, \ldots, 1)$ segue que $\delta_2(\mathcal{C}_{\leq 1}) = |\chi(\mathcal{C}_{\leq 1})| = q - 1$. A partir de agora vamos supor que $n \geq 2$.

O suporte de um monômio M, denotado por $\mathrm{supp}(M)$, é o conjunto de todos X_i, $1 \leq i \leq n$, que aparecem em M. Tome $\{M_1, M_2\} \in \mathcal{J}_{d,2}$, e suponha que $M_1 = X_1^{\alpha_1} \ldots X_n^{\alpha_n}, M_2 = X_1^{\beta_1} \ldots X_n^{\beta_n}$. Definimos $e = \deg(M_1), f = \deg(M_2), A = \mathrm{supp}(M_1)$, e $B = \mathrm{supp}(M_2)$. Podemos assumir que $e \leq f \leq d$. Defina $L \coloneqq (\{X_i^{q-1}\}_{i=1}^n)$ e $J \coloneqq (L, M_1, M_2)$, ($L = \mathrm{lm}(I)$ pelo Lema 3.31). Vamos mostrar que

$$|\Delta(J)| = (q-1)^n - (q-2)^e(q-1)^{n-e} - (q-2)^f(q-1)^{n-f} + (q-2)^{|A \cup B|}(q-1)^{n-|A \cup B|}. \quad (3.3)$$

De fato, como $J = (L, M_1, M_2)$ é um ideal monomial temos que $\{X_1^{q-1}, \ldots, X_n^{q-1}, M_1, M_2\}$ é uma base de Gröbner de J. Assim, para determinar $|\Delta(J)|$ basta calcularmos a quantidade de monômios que não são múltiplos de $X_1^{q-1}, \ldots, X_n^{q-1}, M_1$ e M_2. Defina $S_1 \coloneqq \{M \in \mathcal{M} \mid M$ não é múltiplo de $X_1^{q-1}, \ldots, X_n^{q-1}\}, S_2 \coloneqq \{M \in S_1 \mid M$ é múltiplo de $M_1\}$ e $S_3 \coloneqq \{M \in S_1 \mid M$ é múltiplo de $M_2\}$. Observe que $|S_1| = (q-1)^n$, pois os elementos que estão em K são todos os monômios da forma $X_1^{a_1} \ldots X_n^{a_n}$, com $0 \leq a_j \leq q-2$ para todo $1 \leq j \leq n$. $|S_2| = (q-2)^e(q-1)^{n-e}$, pois todos os elementos de S_2 são da forma $X_1^{a_1} \ldots X_n^{a_n}$, com $1 \leq a_j \leq q-2$ se $X_j \in A$, $0 \leq a_j \leq q-2$ se $X_j \notin A$ para todo $1 \leq j \leq n$ e $|A| = e$. Da mesma forma, $|S_3| = (q-2)^f(q-1)^{n-f}$. $|S_2 \cap S_3| = (q-2)^{|AUB|}(q-1)^{n-|A\cup B|}$, pois todos os elementos de $S_2 \cap S_3$ são da forma $X_1^{a_1} \ldots X_n^{a_n}$, com $1 \leq a_j \leq q-2$ se $X_j \in A \cup B$, $0 \leq a_j \leq q-2$ se $X_j \notin A \cup B$ para todo $1 \leq j \leq n$. Portanto,

$$\begin{aligned}
|\Delta(J)| =& |S_1| - |S_2 \cup S_3| = |S_1| - (|S_2| + |S_3| - |S_2 \cap S_3|) \\
=& (q-1)^n - ((q-2)^e(q-1)^{n-e} - (q-2)^f(q-1)^{n-f} - (q-2)^{|AUB|}(q-1)^{n-|A\cup B|}) \\
=& (q-1)^n - (q-2)^e(q-1)^{n-e} - (q-2)^f(q-1)^{n-f} + (q-2)^{|AUB|}(q-1)^{n-|A\cup B|}.
\end{aligned}$$

Suponha que $d = n$. Como M_1, M_2 são monômios livres de quadrados distintos, temos que $e < n$. Com efeito, se $e = n$, então $e = f = n$ e $M_1 = X_1 \ldots X_n = M_2$, que é uma contradição. Primeiro, vamos mostrar a desigualdade $\delta_2(\mathcal{C}_{\leq d}) \geq (q-2)^{n-1}(q-1)$. Pelo Corolário 3.41, $\delta_2(\mathcal{C}_{\leq_d}) \geq \rho_I(d, 2)$. Logo, é suficiente mostrar a desigualdade $\rho_I(d, 2) \geq (q-2)^{n-1}(q-1)$, ou seja, queremos mostrar que para quaisquer $\{M_1, M_2\} \in \mathcal{J}_{d,2}$ temos

$$\Delta(L + (M_1, M_2)) \leq (q-1)^n - (q-2)^{n-1}(q-1).$$

Usando a Equação 3.3 e fazendo simplificações chegamos a

$$(q-2)^{n-1}(q-1) + (q-2)^{|A\cup B|}(q-1)^{n-|A\cup B|} \leq (q-2)^e(q-1)^{n-e} + (q-2)^f(q-1)^{n-f}.$$

A desigualdade acima é válida lembrando que $e \leq n-1$, que

$$\begin{aligned}
\frac{q-2}{q-1} < 1 \Rightarrow \left(\frac{q-2}{q-1}\right)^{n-1} &\leq \left(\frac{q-2}{q-1}\right)^e \\
\Rightarrow \frac{(q-2)^{n-1}(q-1)}{(q-1)^n} &\leq \frac{(q-2)^e}{(q-1)^e} \\
\Rightarrow (q-2)^{n-1}(q-1) &\leq (q-2)^e(q-1)^{n-e}.
\end{aligned}$$

e ainda que, de $f = |B| \leq |A \cup B|$ e $\dfrac{q-2}{q-1} < 1$ temos

$$\begin{aligned}
\left(\frac{q-2}{q-1}\right)^{|A\cup B|} &\leq \left(\frac{q-2}{q-1}\right)^f \\
\Rightarrow \frac{(q-2)^{|A\cup B|}(q-1)^{n-|A\cup B|}}{(q-1)^{|A\cup B|}(q-1)^{n-|A\cup B|}} &\leq \frac{(q-2)^f}{(q-1)^f} \\
\Rightarrow (q-2)^{|A\cup B|}(q-1)^{n-|A\cup B|} &\leq (q-2)^f(q-1)^{n-f}.
\end{aligned} \tag{3.4}$$

Então

$$\max\{|\Delta(L + (M_1, M_2))| \mid \{M_1, M_2\} \in \mathcal{J}_{d,2}\} \leq (q-1)^n - (q-2)^{n-1}(q-1),$$

e portanto,

$$\rho_I(d, 2) \geq (q-2)^{n-1}(q-1).$$

Agora, vamos mostrar a desigualdade $\delta_2(\mathcal{C}_{\leq d}) \leq (q-2)^{n-1}(q-1)$. Pelo Corolário 3.40 e pelo Lema 3.17, é suficiente encontrar $\{f_1+I, f_2+I\} \in (\mathbb{F}_q V_{\leq d})_2$ tal que

$$|\Delta(I+(f_1,f_2))| = |V(f_1,f_2)\cap T| = |V(f_1)\cap V(f_2)\cap T| = (q-1)^n - (q-2)^{n-1}(q-1).$$

Sejam $f_1 = (X_1-1)\dots(X_n-1)$ e $f_2 = (X_2-1)\dots(X_n-1)$. Observe que a classe de cada monômio que aparece em f_1 e f_2 é um elemento da base de $\mathbb{F}_q V_{\leq_d}$ e $f_1 \neq f_2$, logo não é difícil ver que $\{f_1+I, f_2+I\}$ é um subconjunto linearmente independente de $\mathbb{F}_q V_{\leq_d}$. Temos que $|V(f_1,f_2)\cap T| = |V(f_2)\cap T|$. Como $\deg(f_2) = d-1$ e $d=n$, pela Proposição 3.38, temos que

$$|V(f_2)\cap T| = (q-1)^n - (q-2)^{n-1}(q-1),$$

o que completa a prova do caso $d=n$.

Suponha que $d<n$. Primeiro vamos mostrar a desigualdade $\delta_2(\mathcal{C}_{\leq_d}) \geq (q-2)^d(q-1)^{n-d-1}q$. Pelo Corolário 3.41, $\delta_2(\mathcal{C}_{\leq_d}) \geq \rho_I(d,2)$. Logo, é suficiente mostrar que $\rho_I(d,2) \geq (q-2)^d(q-1)^{n-d-1}q$. Então só precisamos mostrar que a seguinte desigualdade

$$|\Delta(L+(M_1,M_2))| \leq (q-1)^n - (q-2)^d(q-1)^{n-d-1}q$$

é válida para qualquer $\{M_1,M_2\} \in \mathcal{J}_{d,2}$. Observe que, pela Equação 3.3, essa desigualdade é equivalente a

$$\begin{aligned}&(q-2)^d(q-1)^{n-d-1}q + (q-2)^{|A\cup B|}(q-1)^{n-|A\cup B|} \leq \\ &(q-2)^e(q-1)^{n-e} + (q-2)^f(q-1)^{n-f}.\end{aligned} \tag{3.5}$$

Para mostrar essa desigualdade vamos considerar dois casos.

(Caso 1) Suponha que $e=d$. Então $e=f=d$. Substituindo $e=f=d$ na Equação 3.5 temos que

$$\begin{aligned}&(q-2)^{|A\cup B|}(q-1)^{n-|A\cup B|} \leq 2(q-2)^d(q-1)^{n-d} - (q-2)^d(q-1)^{n-d-1}q \Leftrightarrow \\ &(q-2)^{|A\cup B|}(q-1)^{n-|A\cup B|} \leq (q-2)^d(q-1)^{n-d}(2-(q-1)^{-1}q) \Leftrightarrow \\ &(q-2)^{|A\cup B|}(q-1)^{n-|A\cup B|} \leq (q-2)^d(q-1)^{n-d}\frac{q-2}{q-1} \Leftrightarrow \\ &(q-2)^{|A\cup B|}(q-1)^{n-|A\cup B|} \leq (q-2)^{d+1}(q-1)^{n-d-1}.\end{aligned}$$

Logo, a Equação 3.5 é equivalente a

$$(q-2)^{|A\cup B|}(q-1)^{n-|A\cup B|} \leq (q-2)^{d+1}(q-1)^{n-d-1}. \tag{3.6}$$

Observe que neste caso $|A\cup B| \geq d+1$, pois, se $|A\cup B| = d$ teríamos $M_1 = M_2$. Daí, a Equação 3.6 é válida. De fato,

$$\begin{aligned}\frac{q-2}{q-1} < 1 \Rightarrow &\frac{(q-2)^{|A\cup B|}}{(q-1)^{|A\cup B|}} \leq \frac{(q-2)^{d+1}}{(q-1)^{d+1}} \\ \Rightarrow &\frac{(q-2)^{|A\cup B|}(q-1)^n}{(q-1)^{|A\cup B|}(q-1)^n} \leq \frac{(q-2)^{d+1}}{(q-1)^{d+1}} \\ \Rightarrow &(q-2)^{|A\cup B|}(q-1)^{n-|A\cup B|} \leq (q-2)^{d+1}(q-1)^{n-d-1}.\end{aligned}$$

(Caso 2) Suponha que $e<d$. Definindo $k=d-e$, vamos mostrar, por indução, que $(q-2)^k q \leq (q-1)^{k+1}$ para todo $k \geq 1$. Com efeito, se $k=1$ temos que $(q-2)q = (q-1)^2 - 1 \leq (q-1)^2$. Agora, seja $k \geq 1$ e suponha que a desigualdade $(q-2)^k q \leq (q-1)^{k+1}$ é válida, então,

como $q-2 < q-1$ e usando a hipótese de indução, segue que $(q-2)^{k+1}q \leq (q-1)^{k+2}$, como queríamos demonstrar. Daí, temos que

$$\begin{aligned}(q-2)^{d-e}q \leq (q-1)^{d-e+1} &\Rightarrow (q-2)^{d-e}q(q-1)^{n-d-1} \leq (q-1)^{d-e+1}(q-1)^{n-d-1} \\ &\Rightarrow (q-2)^{d-e}(q-1)^{n-d-1}q \leq (q-1)^{n-e} \\ &\Rightarrow (q-2)^{d}(q-1)^{n-d-1}q \leq (q-1)^{n-e}(q-2)^{e},\end{aligned}$$

e pela Equação 3.4 temos que

$$(q-2)^{|A\cup B|}(q-1)^{n-|A\cup B|} \leq (q-2)^{f}(q-1)^{n-f}.$$

A partir dessas últimas duas desigualdades mostramos que a Equação 3.5 é válida neste caso. Finalmente, vamos mostrar que $\delta_2(\mathcal{C}_{\leq_d}) \leq (q-2)^d(q-1)^{n-d-1}q$. Pelo Corolário 3.40 e pelo Lema 3.17, é suficiente encontrar $\{f_1+I, f_2+I\} \in (\mathbb{F}_q V_{\leq d})_2$ tal que

$$|\Delta(I+(f_1,f_2))| = |V(f_1,f_2)\cap T| = |V(f_1)\cap V(f_2)\cap T| = (q-1)^n - (q-2)^d(q-1)^{n-d-1}q.$$

Sejam $f_1 = (X_1-1)\dots(X_d-1)$, $f_2 = (X_2-1)\dots(X_{d+1}-1)$ e $g = (X_1-1)\dots(X_{d+1}-1)$. Observe que a classe de cada monômio que aparece em f_1 e f_2 é um elemento da base de $\mathbb{F}_q V_{\leq_d}$ e $f_1 \neq f_2$, logo não é difícil ver que $\{f_1+I, f_2+I\}$ é um subconjunto linearmente independente de $\mathbb{F}_q V_{\leq_d}$. Temos que $|(V(f_1)\cup V(f_2))\cap T| = |V(g)\cap T|$. Pela Proposição 3.38 segue que

$$\begin{aligned}|V(f_1,f_2)\cap T| &= |V(f_1)\cap T| + |V(f_2)\cap T| - |V(g)\cap T| \\ &= 2((q-1)^n - (q-2)^d(q-1)^{n-d}) - ((q-1)^n - (q-2)^{d+1}(q-1)^{n-d-1}) \\ &= (q-1)^n - 2(q-2)^d(q-1)^{n-d} + (q-2)^{d+1}(q-1)^{n-d-1} \\ &= (q-1)^n - (q-2)^d(q-1)^{n-d-1}(2(q-1)-(q-2)) \\ &= (q-1)^n - (q-2)^d(q-1)^{n-d-1}q.\end{aligned}$$

Isso completa a demonstração do caso $d < n$. □

Exemplo 3.44. Se $n=7$ e $q=4$, usando o Teorema anterior, temos que o segundo peso de Hamming Generalizado de $\mathcal{C}_{\leq_d}$ é

$$\delta_2(\mathcal{C}_{\leq d}) = \begin{cases} 3(2^6) = 192 & \text{se } d = 7 \\ 4(2^d)(3^{6-d}) & \text{se } d < 7. \end{cases}$$

Referências Bibliográficas

[1] BECKER, T.; WEISPFENNING V. **Gröbner Bases - A computational approach to commutative algebra**, Berlin, Germany: Springer Verlag, 1998, 2nd. pr.

[2] BUCHBERGER, B. **Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal**. Mathematical Institute, University of Innsbruck, Austria. PhD Thesis. 1965. An English translation appeared in J. Symbolic Comput. 41 (2006) 475-511. https://doi.org/10.1016/j.jsc.2005.09.007.

[3] CARVALHO, C. **On the second Hamming weight of some Reed-Muller type codes**. Finite Fields Appl. vol. 24, pp. 88-94, 2013. https://doi.org/10.1016/j.ffa.2013.06.004.

[4] COX, D. A.; LITTLE, J.; O'SHEA, D. **Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra**. 4ª Edição. Springer, 2013.

[5] FITZGERALD, J.; LAX, R. F. **Decoding affine variety codes using Gröbner Bases**. Des. Codes and Cryptogr., vol. 13, pp. 147-158, 1998. https://doi.org/10.1023/A:1008274212057.

[6] HANSEN, J. P. **Toric surfaces and error-correcting codes**. In: Coding Theory, Cryptography, and Related Areas, pp. 132-142. Springer, Berlin, 2000.

[7] HASSET, B. **Introduction to algebraic geometry**. Cambridge University Press, 2007. https://doi.org/10.1017/CBO9780511755224.

[8] HEFEZ, A.; VILLELA, M. L. **Códigos Corretores de Erros**. 2ª Edição. Instituto Nacional de Matemática Pura e Aplicada, 2008.

[9] JARAMILLO, D.; VAZ PINTO, M.; VILLARREAL, R. H. **Evaluation codes and their basic parameters**. Designs, Codes and Cryptography, v. 89, n. 2, pp. 269-300, 2021. https://doi.org/10.1007/s10623-020-00818-8.

[10] LÓPEZ, H. H.; RENTERÍA-MARQUEZ, C.; VILLAREAL, R. H. **Affine cartesian codes**. Des. Codes and Cryptogr., vol. 71, pp. 5-19, 2014.

[11] WEI, V. K. **Generalized Hamming weights for linear codes**. IEEE Transactions on information theory, v. 37, n. 5, pp. 1412-1418, 1991. https://doi.org/10.1109/18.133259.