CARLOS DANIEL PEREIRA DE OLIVEIRA

Códigos Hiperbólicos

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
2026

CARLOS DANIEL PEREIRA DE OLIVEIRA

Códigos Hiperbólicos

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

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

Orientador: Prof. Dr. Cícero Fernandes de Carvalho.

UBERLÂNDIA - MG
2026

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

O48 Oliveira, Carlos Daniel Pereira de, 1999-
2026 Códigos Hiperbólicos [recurso eletrônico] / Carlos Daniel Pereira de Oliveira. - 2026.

Orientador: Cícero Fernandes de Carvalho.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
DOI http://doi.org/10.14393/ufu.di.2026.162
Inclui bibliografia.
Inclui ilustrações.

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

CDU: 51

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

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 158 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4209/4154 - www.ppmat.ime.ufu.br - pgmat@ime.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, 128, PPGMAT				
Data:	20/02/2026	Hora de início:	9:00	Hora de encerramento:	11:00
Matrícula do Discente:	12412MAT001				
Nome do Discente:	Carlos Daniel Pereira de Oliveira				
Título do Trabalho:	Códigos hiperbólicos				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Determinando parâmetros de certa classe de códigos de avaliação				

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

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

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

Aprovado.

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

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

interna da UFU.

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

Documento assinado eletronicamente por **Saeed Tafazolian**, **Usuário Externo**, em 20/02/2026, às 12:31, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann**, **Professor(a) do Magistério Superior**, em 20/02/2026, às 12:51, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Cícero Fernandes de Carvalho**, **Professor(a) do Magistério Superior**, em 20/02/2026, às 18:00, 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 **7044907** e o código CRC **CC86E687**.

Referência: Processo nº 23117.006757/2026-42 SEI nº 7044907

Sumário

Dedicatória

Dedidco este trabalho aos meus pais, Raquel Pereira de Souza e Admilson Alves de Oliveira, pelo apoio incondicional e por sempre acreditarem em mim.

Agradecimentos

Agradeço, primeiramente, a Deus por ter me abençoado em mais uma trajetória acadêmica, por ter me concedido sabedoria, tranquilidade e por me guiar em todos os momentos da minha vida. Não tenho palavras para expressar a minha gratidão ao Senhor.

Agradeço ao meu pai, Admilson Alves de Oliveira, por ter me amparado financeramente durante o primeiro semestre, me auxiliando com o aluguel e a alimentação. Sem dúvida, eu não estaria aqui sem o senhor. Muito obrigado por tudo. Agradeço à minha mãe, Raquel Pereira de Souza, por estar sempre ao meu lado e por sempre me ajudar em tudo o que preciso.

Um agradecimento especial à minha avó, Ivani Pereira de Souza, por sempre confiar em mim e por todo o apoio. Obrigado por tudo que a senhora fez/faz por mim. Em especial, agradeço ao meu avô, Delson Borges, por tudo o que fez por mim e espero que o senhor esteja muito orgulhoso de mim.

Agradeço aos meus irmãos, Ingrid Daniele Pereira de Oliveira e João Paulo Alves de Souza, pelo apoio durante todo o mestrado. Agradeço também aos familiares que me ajudaram especialmente no primeiro semestre do mestrado.

Agradeço ao meu orientador, Doutor Cícero Fernandes de Carvalho, primeiramente, por estar sempre disponível para me orientar desde o início. Obrigado pelos conselhos, por ter me incentivado a melhorar meus conhecimentos, pelos diversos aprendizados ao longo do trabalho e pela amizade construída ao longo desse um ano e meio. Enfim, muito obrigado.

Agradeço ao professor e coordenador da Pós-Graduação, Victor von Neumann e à Mônica, por terem me ajudado a conquistar a bolsa de estudos. Sou eternamente grato a vocês.

Agradeço à professora Elisa Regina dos Santos, excelente profissional e amiga, com quem tive a honra de realizar estágio na disciplina de Cálculo Diferencial e Integral II. Foi um período de grande aprendizado em minha trajetória acadêmica, que, sem dúvida, será de grande valia daqui em diante .

Agradeço a todos os professores com quem tive o privilégio de aprender ao longo dessa jornada.

Agradeço aos meus colegas e amigos de mestrado - Marcos Henrique, Matheus Felipe, Silas Campos, Mateus Fernando, Ially, Mateus Deodato, José Armando, Daniella, Jânio, Mônica, Fernanda, Elisa, Alef, Ênio, Victor e Henrique - pela amizade e por toda a trajetória ao longo do mestrado. Peço desculpas, se esqueci o nome de alguém.

Agradeço aos professores Saeed Tafazolian e Victor Gonzalo, por terem aceitado o convite para fazer parte da banca que avaliou este trabalho, contribuindo para o resultado final aqui apresentado.

Agradeço aos meus amigos Elder e Carol, por estarem sempre ao meu lado, pela ajuda e pela amizade sincero ao longo do tempo.

Agradeço à FAPEMIG pelo auxílio financeiro durante o mestrado.

CARLOS, D. P. O. *Códigos Hiperbólicos.* 2026. (66 pág) Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho estudamos os assim chamados códigos hiperbólicos. Apresentamos inicialmente resultados sobre os corpos finitos e introduzimos conceitos e resultados da teoria das Bases de Gröbner, como por exemplo, as variedades afins, a pegada de um ideal e a relação entre a pegada e a variedade de um ideal. Em seguida, apresentamos os códigos hiperbólicos e através da teoria das Bases de Gröbner conseguimos determinar os parâmetros fundamentais (comprimento, dimensão e distância mínima) dos códigos hiperbólicos e demos uma caracterização dos códigos hiperbólicos através de dualidade. Tendo introduzido os pesos generalizados de Hamming e definições como conjunto denso e ótimo foi possível determinar uma cota inferior para o peso generalizado de Hamming desses códigos.

Palavras-chave: (Corpos finitos, Bases de Gröbner, Variedades afins, Códigos Hiperbólicos, Peso Generalizado de Hamming.)

CARLOS, D. P. O. *Códigos Hiperbólicos.* 2026. (66 pág) Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Abstract

In this work we study the so-called hyperbolic codes. We initially present results on finite fields and introduce concepts and results from Gröbner's Basis theory, such as affine manifolds, the footprint of an ideal, and the relationship between the footprint and the manifold of an ideal. Next, we present the hyperbolic codes and, through Gröbner's Basis theory, we were able to determine the fundamental parameters (length, dimension, and minimum distance) of the hyperbolic codes and provide a characterization of the hyperbolic codes through duality. Having introduced the generalized Hamming weights and definitions such as dense and optimal sets, it was possible to determine a lower bound for the generalized Hamming weight of these codes.

Keywords: (Finite fields, Gröbner bases, Affine manifolds, Hyperbolic codes, Generalized Hamming weights.)

Introdução

Os Códigos Corretores de Erros estão presentes no nosso cotidiano de diversas maneiras, tais como assistir a um programa de televisão, falar ao telefone, mandar um recado para alguém via e-mail ou por aplicativos de trocas de mensagens, enfim, sempre que fazemos uso de informações digitalizadas. Segundo [6], essa teoria teve origem com o trabalho pioneiro do matemático Claude Shannon, do laboratório Bell, em um trabalho publicado em 1948 e, desde então, tem se desenvolvido bastante, estabelecendo conexões entre diversas áreas do conhecimento, como a Álgebra Linear, Álgebra Comutativa, Geometria Algébrica e dentre outras. Um código corretor de erro é em essência, um modo organizado de acrescentar algum dado adicional (redundâncias) a cada informação que se queira transmitir ou armazenar, que permita, ao recuperar a informação, detectar e corrigir erros.

O objetivo principal deste trabalho é o estudo dos chamados **códigos hiperbólicos**, que são um tipo particular dos códigos lineares (um código linear é um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q^n$, onde $\mathbb{F}_q$ é um corpo finito com q elementos). Nesta dissertação iremos apresentar vários resultados acerca dos códigos hiperbólicos, tais como uma caracterização através de dualidade e determinaremos cotas inferiores para seus pesos generalizados de Hamming.

Mais especificamente, a dissertação está estruturada da seguinte forma:

No primeiro capítulo, descrevemos alguns conceitos e resultados fundamentais utilizados na abordagem do tema deste trabalho. Dentre esses conceitos, destacamos a característica de um corpo, e existência e unicidade dos corpos finitos.

O segundo capítulo é dedicado ao estudo dos códigos lineares. Neste capítulo apresentamos conceitos como a métrica de Hamming, a matriz geradora, e damos um exemplo de um código linear, a saber o código de Reed-Solomon. Para finalizar introduzimos os pesos generalizados de Hamming e alguns de seus resultados, seguindo [7].

No terceiro capítulo são apresentados os conceitos de ordem monomial, o algoritmo da divisão para polinômios em várias variáveis, bases de Gröbner, pegada de um ideal, variedades afins, a relação entre eles e o Teorema de Buchberger (veja [2]). Ao final do capítulo definimos uma função chamada *mapa de avaliação* e também os Códigos de Variedades Afins, que serão bastante utilizados no decorrer do trabalho.

No quarto capítulo apresentamos o conceito principal da dissertação, que são os códigos hiperbólicos, seguindo [5]. Apresentamos, neste capítulo, uma caracterização desses códigos e determinamos seus parâmetros fundamentais a partir da teoria das Bases de Gröbner que foi desenvolvida no capítulo precedente. Além disso, usando novamente as técnicas apresentadas no capítulo anterior e introduzindo as noções de conjunto denso e ótimo determinamos uma cota inferior para os pesos generalizados de Hamming desses códigos.

Carlos Daniel Pereira de Oliveira
Uberlândia-MG, 20 de fevereiro de 2026.

Capítulo 1

Corpos finitos

1.1 Introdução

Neste capítulo inicial introduziremos resultados importantes sobre os corpos finitos, tais como: característica de um corpo finito, polinômios irredutíveis, existência e unicidade de corpos finitos. Na elaboração dessa parte do trabalho, usaremos como referência principal [6].

Seja $\mathbb{K}$ um corpo finito (ou seja, $\mathbb{K}$ é um corpo cujo número de elementos é finito) com unidade 1. Defina o conjunto

$$\Lambda_{\mathbb{K}} := \{n \in \mathbb{N} \mid n \cdot 1 = 0\} \subset \mathbb{N},$$

onde $\mathbb{N} := \{1, 2, 3, \ldots\}$.

Afirmação: $\Lambda_{\mathbb{K}} \neq \emptyset$.

De fato, como $\mathbb{K}$ é um corpo finito, então existem $n_1, n_2 \in \mathbb{N}$, com $n_1 < n_2$ tais que $n_1 \cdot 1 = n_2 \cdot 1$. Logo, $(n_2 - n_1) \cdot 1 = 0$, com $n_2 - n_1 > 0$, e, portanto, $\Lambda_{\mathbb{K}} \neq \emptyset$.

Doravante, quando tivermos um corpo $\mathbb{K}$ a multiplicação de dois elementos $x, y \in \mathbb{K}$ será designada simplesmente por xy.

Definição 1.1.1 (Característica de um corpo)**.** *A* ***característica*** *de um corpo finito $\mathbb{K}$ é o inteiro positivo*

$$\mathrm{car}(\mathbb{K}) := \min \Lambda_{\mathbb{K}} = \min\{n \in \mathbb{N} \mid n1 = 0\}.$$

Se um corpo $\mathbb{F}$ é um subcorpo de um corpo $\mathbb{K}$, então $\mathrm{car}(\mathbb{F}) = \mathrm{car}(\mathbb{K})$*, pois $\Lambda_{\mathbb{K}} = \Lambda_{\mathbb{F}}$. Além disso, é claro que $\mathbb{K}$ é um $\mathbb{F}$-espaço vetorial.*

Proposição 1.1.2. *Seja $\mathbb{K}$ um corpo finito, então* $\mathrm{car}(\mathbb{K})$ *é um número primo.*

Demonstração. Seja $m = \mathrm{car}(\mathbb{K})$ e suponha por absurdo que m não seja primo. Ou seja, m é um número composto, o que significa que existem inteiros m_1, m_2, com $m_1, m_2 > 1$ e $m_1, m_2 < m$ tais que $m = m_1 m_2$. Assim,

$$\begin{aligned} 0 &= m1 \\ &= (m_1 m_2)1 \\ &= m_1(m_2 1) \\ &= (m_1 1)(m_2 1). \end{aligned}$$

Como $\mathbb{K}$ é um corpo, em particular, $\mathbb{K}$ é um domínio, então $m_1 1 = 0$ ou $m_2 1 = 0$. Logo, m_1 e m_2 são menores que m e pertencem a $\Lambda_{\mathbb{K}}$, o que é uma contradição, pois contraria a minimalidade de m. Portanto, $\mathrm{car}(\mathbb{K})$ é um número primo. □

Proposição 1.1.3. *Seja $\mathbb{K}$ um corpo finito com $\mathrm{car}(\mathbb{K}) = p$ e sejam $m \in \mathbb{Z}$ e $a \in \mathbb{K}$. Se $ma = 0$, então m é um múltiplo de p ou $a = 0$.*

Demonstração. Seja $ma = (m1)a = 0$. Como $\mathbb{K}$ é um corpo temos que $\mathbb{K}$ é um domínio e logo $m1 = 0$ ou $a = 0$. Se $a = 0$, acabou. Suponha que $a \neq 0$, então $m1 = 0$. Dividindo m por p, pelo algoritmo da divisão podemos escrever $m = \lambda p + r$, onde $\lambda, r \in \mathbb{Z}$, com $0 \leq r < p$. Logo,

$$\begin{aligned} 0 &= m1 \\ &= (\lambda p + r)1 \\ &= (\lambda p)1 + r1 \\ &= \lambda(p1) + r1 \\ &= \lambda 0 + r1 \\ &= r1. \end{aligned}$$

Como p é o menor inteiro positivo satisfazendo $p1 = 0$, segue que $r = 0$. Ou seja, $m = \lambda p$ e, portanto, m é múltiplo de p. □

Teorema 1.1.4. *Seja $\mathbb{K}$ um corpo finito com $\mathrm{car}(\mathbb{K}) = p$. Então, $\mathbb{K}$ contém um subcorpo isomorfo a $\mathbb{Z}_p := \mathbb{Z}/(p)$. Em particular, $\mathbb{K}$ tem p^n elementos para algum número natural n.*

Demonstração. Defina a aplicação φ dada por

$$\begin{aligned} \varphi : \mathbb{Z}_p &\to \mathbb{K} \\ \overline{n} &\mapsto n1, \end{aligned}$$

em que $\overline{n}$ denota a classe de n em $\mathbb{Z}_p$.

Vejamos que φ está bem definida. Sejam $m, n \in \mathbb{Z}$ tais que $\overline{n} = \overline{m}$. Logo, existe $\beta \in \mathbb{Z}$ onde $n = m + \beta p$. Logo,

$$n1 = (m + \beta p)1 = m1 + (\beta p)1 = m1 + \beta(p1) = m1 + \beta 0 = m1 + 0 = m1.$$

Agora, provemos que φ é um homomorfismo de corpos. Com efeito,

- $\varphi(\overline{1}) = 1$.
- sejam $\overline{m}, \overline{n} \in \mathbb{Z}_p$, com $m, n \in \mathbb{Z}$. Então

$$\begin{aligned} \varphi(\overline{m} + \overline{n}) &= \varphi(\overline{m + n}) \\ &= (m + n)1 \\ &= m1 + n1 \\ &= \varphi(\overline{m}) + \varphi(\overline{n}) \end{aligned}$$

e

$$\begin{aligned} \varphi(\overline{m} \cdot \overline{n}) &= \varphi(\overline{mn}) \\ &= (mn)1 \\ &= (m1)(n1) \\ &= \varphi(\overline{m})\varphi(\overline{n}). \end{aligned}$$

De propriedades de homomorfismos de corpos temos que $\varphi(\mathbb{Z}_p)$ é um subcorpo de $\mathbb{K}$, isomorfo a $\mathbb{Z}_p$.

Desta forma, segue que $\mathbb{K}$ é um $\mathbb{Z}_p$-espaço vetorial e como $\mathbb{K}$ é finito, temos que $\mathbb{K}$ tem dimensão finita sobre $\mathbb{Z}_p$. Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Z}_p$. Então, existem $\beta_i \in \mathbb{Z}_p$, com $i = 1, \ldots, n$ tais que todo elemento de $\mathbb{K}$ pode ser escrito de maneira única como

$$\beta_1\alpha_1 + \cdots + \beta_n\alpha_n.$$

Para cada $i = 1, \ldots, n$ temos p possibilidades para os escalares β_i, logo $\#(\mathbb{K}) = p^n$. □

No que se segue algumas propriedades importantes sobre potências da característica de um corpo finito são apresentadas.

Proposição 1.1.5. *Se $\mathbb{K}$ é um corpo finito com $\mathrm{car}(\mathbb{K}) = p$ e seja $q = p^r$, para algum inteiro positivo r. Se $a, b \in \mathbb{K}$, temos que*

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

Demonstração. Mostraremos a afirmação fazendo indução sobre r.

Primeiramente, consideremos $r = 1$. Pelo Binômio de Newton, temos

$$(a + b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{i}a^{p-i}b^i + \cdots + b^p.$$

É sabido que $p \mid \binom{p}{i}$, para todo $i = 1, \ldots, p - 1$, logo

$$(a + b)^p = a^p + b^p,$$

provando assim o caso $r = 1$.

Suponhamos que a proposição é válida para $r - 1$, ou seja

$$(a + b)^{p^{r-1}} = a^{p^{r-1}} + b^{p^{r-1}}. \tag{1.1}$$

Usando 1.1 e o caso $r = 1$, obtemos que

$$\begin{aligned}(a + b)^q &= (a + b)^{p^r} \\ &= ((a + b)^{p^{r-1}})^p \\ &= (a^{p^{r-1}} + b^{p^{r-1}})^p \\ &= (a^{p^{r-1}})^p + (b^{p^{r-1}})^p \\ &= a^{p^r} + b^{p^r} \\ &= a^q + b^q.\end{aligned}$$

□

Proposição 1.1.6. *Seja $\mathbb{K}$ um corpo finito. Sejam $a_1, \ldots, a_n \in \mathbb{K}$ com $\mathrm{car}(\mathbb{K}) = p$ e $q = p^r$, com $r \geq 0$ um número inteiro. Então*

$$(a_1 + a_2 + \cdots + a_n)^q = a_1^q + a_2^q + \cdots + a_n^q.$$

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

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

Demonstração. A demonstração será feita por indução em n e no expoente r.
É claro que para $n = 1$ e $r = 1$, o resultado é verdadeiro. Fixemos $r = 1$ e faremos a indução sobre n.
Suponha que o resultado é válido para $k > 1$, ou seja,

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

Assim para o caso $k + 1$, usando a Proposição 1.1.5 temos

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

Usando a hipótese de indução temos que

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

Agora, fixaremos n e faremos uma indução sobre r. Veja que o caso onde $r = 1$ já foi provado e suponha válido para $r > 1$. Sabemos que $p^{r+1} = p^r p$, então

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

Usando a hipótese de indução, segue que

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

Se $P(X) = a_0 + a_1X + \cdots + a_nX^n$, segue imediatamente do que acabamos de provar que

$$P(X)^q = (a_0 + a_1X + \cdots + a_nX^n)^q = a_0^q + a_1^qX^q + \cdots + a_n^qX^{nq}.$$

□

Corolário 1.1.7. *Seja $\mathbb{K}$ um corpo finito com $\mathrm{car}(\mathbb{K}) = p$. Se $q = p^r$, com $r \geq 0$, então a aplicação f_q definida por*

$$\begin{array}{rccc} f_q: & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & x^q \end{array}$$

é um isomorfismo de corpos.

Demonstração. Pelas propriedades provadas acima temos que f_q é homomorfismo. Além disso, todo homomorfismo de corpos é injetor, e como $\mathbb{K}$ é finito, também é sobrejetor. □

Corolário 1.1.8. *Sejam $\mathbb{F}$ um corpo de característica $p > 0$ e q uma potência inteira de p. O conjunto $\mathbb{K} = \{\alpha \in \mathbb{F} \mid \alpha^q - \alpha = 0\}$ é um subcorpo de $\mathbb{F}$.*

Demonstração. Observe que $\mathbb{K} \neq \emptyset$, pois $1^q - 1 = 0$, ou seja, $1 \in \mathbb{K}$. Sejam $\alpha, \beta \in \mathbb{K}$ com $\beta \neq 0$ então $\alpha^q - \alpha = 0$ e $\beta^q - \beta = 0$. Logo, pela Proposição 1.1.5 segue que

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

e

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

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

Definição 1.1.9 (Derivação de Polinômios)**.** *Seja* $\mathbb{K}$ *um corpo e considere* $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{K}[X]$ *um polinômio. Então a* ***derivada*** *de* $P(X)$*, que é denotada por* $P'(X)$*, é o polinômio*

$$P'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}.$$

É fácil ver que a derivada da soma de polinômios é a soma das derivadas desses polinômios, vale também que $(P(X)Q(X))' = P(X)'Q(X) + P(X)Q(X)'$ e a Regra da Cadeia, para composição de polinômios.

Proposição 1.1.10. *Seja* $\mathbb{K}$ *um corpo finito com* $\text{car}(\mathbb{K}) = p$ *e seja* $P(X) \in \mathbb{K}[X]$*. Então* $P'(X) = 0$ *se, e somente se, existe um polinômio* $Q(X) \in \mathbb{K}[X]$ *tal que* $P(X) = Q(X)^p$*.*

Demonstração. $\boxed{\Rightarrow}$ Seja $P(X) = a_0 + a_1X + \cdots + a_iX^i + \cdots + a_nX^n$ tal que $P'(X) = 0$. Assim, temos que

$$P'(X) = a_1 + 2a_2X + \cdots + ia_iX^{i-1} + \cdots + na_nX^{n-1} = 0.$$

Logo, $ia_i = 0$ para todo $i = 1, \ldots, n$. Pela Proposição 1.1.3, temos que ter $a_i = 0$ sempre que i não for múltiplo de p. Portanto,

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

Escolhendo $b_i \in \mathbb{K}$ tal que $b_i^p = a_{ip}$, o que é possível pelo Corolário 1.1.7, para $q = p$, e definindo $Q(X) := b_0 + b_1X + b_2X^2 + \cdots$, temos $P(X) = Q(X)^p$.

$\boxed{\Leftarrow}$ Se $P(X) = Q(X)^p$, então aplicando a Regra da Cadeia, obtemos que

$$P'(X) = pQ(X)^{p-1}Q'(X) = (p1)Q(X)^{p-1}Q'(X) = 0Q(X)^{p-1}Q'(X) = 0.$$

□

Proposição 1.1.11. *Seja* $f(X) \in \mathbb{K}[X]$ *com um fator múltiplo não constante em* $\mathbb{K}[X]$*. Então* $\text{MDC}(f(X), f'(X)) \neq 1$*, onde* $\text{MDC}(f(X), f'(X))$ *denota o máximo divisor comum entre* $f(X)$ *e* $f'(X)$*.*

Demonstração. Seja $h(X) \in \mathbb{K}[X]$ um fator múltiplo não constante de $f(X)$, então existem $r > 1$ e $g(X) \in \mathbb{K}[X]$ tais que

$$f(X) = h(X)^r g(X).$$

Assim, pela Regra do Produto temos

$$\begin{aligned} f'(X) &= rh(X)^{r-1}h'(X)g(X) + h(X)^r g'(X) \\ &= h(X)(rh(X)^{r-2}h'(X)g(X) + h(X)^{r-1}g'(X)). \end{aligned}$$

Logo, $h(X)$ é um divisor de $f'(X)$ e de $f(X)$ e, portanto, $\text{MDC}(f(X), f'(X)) \neq 1$. □

Proposição 1.1.12. *Considere* $\mathbb{K}$ *um corpo finito de característica* p *e seja* $q = p^r$*, para algum inteiro positivo* r*. O polinômio* $F(X) = X^q - X$ *não possui fatores irredutíveis múltiplos em* $\mathbb{K}[X]$*.*

Demonstração. Seja $F(X) = X^q - X$. Derivando $F(X)$, obtemos que $F'(X) = qX^{q-1} - 1 = -1$. Logo, $\text{MDC}(F(X), F'(X)) = 1$. Portanto, usando a contrapositividade da Proposição 1.1.11, $F(X)$ não possui fatores irredutíveis múltiplos em $\mathbb{K}[X]$. □

Lema 1.1.13. *Seja* $\mathbb{K}$ *um corpo com* q *elementos e seja* $\alpha \in \mathbb{K}^* =: \mathbb{K} \setminus \{0\}$*. Então*

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

Demonstração. Seja $\alpha \in \mathbb{K}^*$. Defina a função

$$\begin{array}{rccc} \varphi_\alpha : & \mathbb{K}^* & \to & \mathbb{K}^* \\ & a & \mapsto & \alpha a. \end{array}$$

Sejam $a, b \in \mathbb{K}^*$ tais que $\varphi_\alpha(a) = \varphi_\alpha(b)$. Ou seja, $\alpha a = \alpha b$, o que implica que $\alpha(a - b) = 0$. Portanto, $a = b$, e, por conseguinte, φ_α é injetora. Como $\mathbb{K}^*$ é finito, segue que φ_α é bijetora.

Se $\mathbb{K}^* = \{a_1, \ldots, a_{q-1}\}$, temos que

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

Daí,

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

Portanto, $\alpha^{q-1} = 1$. □

A partir do Lema anterior, segue o resultado a seguir.

Corolário 1.1.14. *Seja $\mathbb{K}$ um corpo finito com q elementos. Para todo $\alpha \in \mathbb{K}$ e para todo $i \in \mathbb{N}$, temos que*

$$\alpha^{q^i} = \alpha.$$

Demonstração. Se $\alpha = 0$, o resultado segue trivialmente.
Suponha que $\alpha \neq 0$. A demonstração será feita por indução em i. Para $i = 1$, pelo Lema 1.1.13 temos que

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

Suponha que é verdadeira para $i = k - 1$, ou seja,

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

Logo, para $i = k$ segue que

$$\alpha^{q^k} = (\alpha^{q^{k-1}})^q = \alpha^q = \alpha.$$

□

Corolário 1.1.15. *Seja $\mathbb{K}$ um corpo finito com q elementos e* $\mathrm{car}(\mathbb{K}) = p$*, e suponha que $\mathbb{F}$ é uma extensão de $\mathbb{K}$. Então os elementos de $\mathbb{K}$ são os elementos de $\mathbb{F}$ que são raízes de $X^q - X = 0$, enquanto que os elementos do subcorpo $\mathbb{Z}_p$ de $\mathbb{F}$ são as raízes do polinômio $X^p - X = 0$.*

Demonstração. Note que, pelo Corolário 1.1.14, temos que os elementos de $\mathbb{K}$ são raízes do polinômio $X^q - X$. Mas esse polinômio, tendo grau q, tem no máximo q raízes, logo, as suas raízes são todos os elementos de $\mathbb{K}$. De modo análogo, prova-se a outra afirmação considerando $\mathbb{Z}_p$ no lugar de $\mathbb{K}$. □

Seja $\mathbb{K}$ um corpo finito e seja $\alpha \in \mathbb{K}^*$. Sabemos do Lema 1.1.13 que

$$\{n \in \mathbb{N} \mid \alpha^n = 1\} \neq \emptyset.$$

Definição 1.1.16 (Ordem de um elemento)**.** *A ordem de $\alpha \in \mathbb{K}^*$ é o inteiro positivo*

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

Proposição 1.1.17. *Sejam $\mathbb{K}$ um corpo finito com q elementos e $\alpha \in \mathbb{K}^*$. Se m é um inteiro positivo satisfazendo $\alpha^m = 1$, então* $\mathrm{ord}(\alpha) \mid m$*. Em particular,* $\mathrm{ord}(\alpha) \mid (q - 1)$.

Demonstração. Dividindo m por $\text{ord}(\alpha)$, pelo algoritmo da divisão existem $s, r \in \mathbb{Z}$ tais que

$$m = (\text{ord}(\alpha))s + r,$$

com $0 \leq r < \text{ord}(\alpha)$. Portanto,

$$\begin{aligned} 1 &= \alpha^m \\ &= \alpha^{(\text{ord}(\alpha))s+r} \\ &= \alpha^{(\text{ord}(\alpha))s}\alpha^r \\ &= 1\alpha^r, \end{aligned}$$

e, consequentemente, $r = 0$, pois caso contrário, contrariaria a minimalidade de $\text{ord}(\alpha)$. Logo, $\text{ord}(\alpha) \mid m$.

Por fim, pelo Lema 1.1.13, temos que $\alpha^{q-1} = 1$ e pelo que acabamos de provar, $\text{ord}(\alpha) \mid (q-1)$. □

Proposição 1.1.18. *Seja $\mathbb{K}$ um corpo finito. Sejam α, β elementos de $\mathbb{K}$ tais que*

$$\text{MDC}(\text{ord}(\alpha), \text{ord}(\beta)) = 1.$$

Então $\text{ord}(\alpha\beta) = \text{ord}(\alpha)\text{ord}(\beta)$.

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

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

o que significa que $\text{ord}(\alpha\beta) \mid mn$.

Por outro lado, se $(\alpha\beta)^t = 1$, então

$$\begin{aligned} 1 = ((\alpha\beta)^t)^m = \alpha^{tm}\beta^{tm} = 1\beta^{tm} = \beta^{tm}, \text{ e} \\ 1 = ((\alpha\beta)^t)^n = \alpha^{tn}\beta^{tn} = \alpha^{tn}1 = \alpha^{tn}. \end{aligned}$$

Logo, pela Proposição 1.1.17, temos que $n \mid tm$ e $m \mid tn$. Como $\text{MDC}(m, n) = 1$, então $m \mid t$ e $n \mid t$. Novamente usando o fato de que $\text{MDC}(m, n) = 1$, segue que $mn \mid t$, o que prova que $mn = \min\{t > 0 \mid (\alpha\beta)^t = 1\}$. Portanto, $\text{ord}(\alpha\beta) = mn$. □

Proposição 1.1.19. *Seja $\mathbb{K}$ um corpo finito e sejam $\alpha \in \mathbb{K}^*$ e $i \in \mathbb{N}$. Se* $\text{ord}(\alpha) = m$*, então*

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

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

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

Ou seja, t é o menor inteiro positivo tal que $m \mid it$, em outras palavras, it é o menor múltiplo comum entre m e i. Logo, $it = \text{MMC}(m, i)$. Como $\text{MDC}(m, i)\text{MMC}(m, i) = mi$, então

$$t = \frac{\text{MMC}(m, i)}{i} = \frac{m}{\text{MDC}(m, i)}.$$

□

1.2 Polinômios Irredutíveis

Proposição 1.2.1. *Sejam $\mathbb{K}$ um corpo finito com q elementos, $f(X)$ um polinômio mônico irredutível em $\mathbb{K}[X]$, de grau d e $\mathbb{F} = \mathbb{K}[X]/(f(X))$ um corpo. Denotaremos por $\overline{g(X)}$ a classe de $g(X)$ no quociente $\mathbb{K}[X]/(f(X))$. São válidas as seguintes afirmações:*

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

Demonstração.
1) Provemos que $\{1, \overline{X}, \overline{X^2}, \ldots, \overline{X^{d-1}}\}$ gera $\mathbb{F}$ e que é um conjunto linearmente independente. Seja $f(X) = a_0 + a_1X + \cdots + X^d \in \mathbb{K}[X]$. Dividindo $g(X) \in \mathbb{K}[X]$ por $f(X)$, existem únicos $q(X), r(X) \in \mathbb{K}[X]$ tais que

$$g(X) = q(X)f(X) + r(X),$$

onde $r(X) = 0$ ou $\text{grau}(r(X)) < \text{grau}(f(X))$. Assim, temos que

$$\overline{g(X)} = \overline{q(X)f(X)} + \overline{r(X)} = \overline{r(X)} = b_0\overline{1} + b_1\overline{X} + \cdots + b_{d-1}\overline{X^{d-1}},$$

isto é, qualquer elemento de $\mathbb{F}$ pode ser escrito como combinação linear de elementos $1, \overline{X}, \overline{X^2}$, $\ldots, \overline{X^{d-1}}$, com $b_j \in \mathbb{K}$ para todo $j = 0, \ldots, d-1$ e, portanto, gera $\mathbb{F}$ como $\mathbb{K}$-espaço vetorial.

Agora, suponha que $\sum_{i=0}^{d-1} a_i\overline{X^i} = a_0 1 + a_1\overline{X} + a_2\overline{X^2} + \cdots + a_{d-1}\overline{X^{d-1}} = \overline{0}$, então $\sum_{i=0}^{d-1} a_iX^i$ é um múltiplo de $f(X)$, que é satisfeito se e só se $a_i = 0$ para todo $i = 0, \ldots, d-1$.

2) Note que $\mathbb{F}$ é um corpo finito com q^d elementos, logo, pelo Corolário 1.1.14, temos que $\overline{X}^{q^d} = \overline{X}$.

3) Segue do item anterior que $\overline{X}^{q^d} - \overline{X} = \overline{0}$, ou seja, $\overline{X^{q^d} - X} = \overline{0}$. Portanto, $f(X)$ divide $X^{q^d} - X$ em $\mathbb{K}[X]$.

4) Seja

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

um polinômio em $\mathbb{F}[Y]$. Temos de (2) que

$$\begin{aligned} g(Y^q) &= (Y^q - \overline{X})(Y^q - \overline{X}^q)\cdots(Y^q - \overline{X}^{q^{d-1}}) \\ &= (Y^q - \overline{X}^{q^d})(Y^q - \overline{X}^q)\cdots(Y^q - \overline{X}^{q^{d-1}}) \\ &= \left((Y - \overline{X}^{q^{d-1}})(Y - \overline{X})\cdots(Y - \overline{X}^{q^{d-2}})\right)^q \\ &= (g(Y))^q. \end{aligned}$$

Assim, $g(Y^q) = (g(Y))^q$ e, portanto, se $g(Y) = b_0 + b_1Y + \cdots + b_{d-1}Y^{d-1} + Y^d$, temos que $b_i^q = b_i$ para todo $i = 0, 1, \ldots, d-1$. Sendo assim, usando o Corolário 1.1.15 segue que $g(Y) \in \mathbb{K}[Y]$.

Como $f(Y), g(Y) \in \mathbb{K}[Y]$ possuem uma raiz comum numa extensão $\mathbb{F}$ de $\mathbb{K}$, segue que o seu MDC em $\mathbb{F}[Y]$ é não constante e pertence a $\mathbb{K}[Y]$. Como $f(Y)$ é irredutível e mônico, ele

coincide com o MDC de $f(Y)$ e $g(Y)$, logo, $f(Y)$ divide $g(Y)$. Como $f(Y)$ e $g(Y)$ são polinômios mônicos de mesmo grau, eles devem ser iguais.

Por (3), temos que $g(Y)(= f(Y))$ divide $Y^{q^d} - Y$ e pela Proposição 1.1.12 não tem fatores múltiplos em nenhuma extensão $\mathbb{F}$ de $\mathbb{K}$. Portanto, as raízes $\overline{X}, \overline{X}^q, \ldots, \overline{X}^{q^{d-1}}$ de $g(Y)$ são duas a duas distintas. □

Observação 1.2.2. *Note que, pela Proposição 1.2.1, se $\overline{X} \in \mathbb{K}[X]/(f(X))$, com $f(X)$ irredutível em $\mathbb{K}[X]$ de grau d, segue que*

$$d = \min\{j \in \mathbb{N} \mid \overline{X}^{q^j} = \overline{X}\}.$$

Proposição 1.2.3. *Seja $\mathbb{K}$ um corpo finito com q elementos e seja n um inteiro positivo. Em $\mathbb{K}[X]$ vale a seguinte igualdade:*

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

onde $G_d(X)$ é o produto de todos os polinômios mônicos irredutíveis de grau d em $\mathbb{K}[X]$, e o produto na fórmula acima é efetuado sobre todos os inteiros positivos d que dividem n.

Demonstração. Seja $f(X) \in \mathbb{K}[X]$ um polinômio mônico irredutível de grau d. Pela Proposição 1.1.12, temos que $X^{q^n} - X$ não possui fatores irredutíveis múltiplos em $\mathbb{K}[X]$, então basta provar a seguinte asserção:

$$f(X) \mid (X^{q^n} - X) \iff d \mid n.$$

$\boxed{\Rightarrow}$ Suponha que $f(X) \mid (X^{q^n} - X)$. Pela Proposição 1.2.1 (3), temos que $f(X) \mid (X^{q^d} - X)$ então $f(X) \mid \text{MDC}(X^{q^n} - X, X^{q^d} - X)$. Logo, $f(X) \mid (X^{q^e} - X)$, onde $e = \text{MDC}(n, d) \leq d$. Assim, temos $\overline{X}^{q^e} = \overline{X}$ em $\mathbb{K}[X]/(f(X))$, o que pela Proposição 1.2.1 (4) só é possível se $e \geq d$. Segue que $d = e = \text{MDC}(n, d)$, e, portanto, $d \mid n$.

$\boxed{\Leftarrow}$ Se $d \mid n$ então $(X^{q^d} - X) \mid (X^{q^n} - X)$. Agora, pela Proposição 1.2.1 (3), temos que $f(X) \mid (X^{q^d} - X)$ e, portanto, $f(X) \mid (X^{q^n} - X)$. □

Corolário 1.2.4. *Seja $I(n)$ o número de polinômios mônicos irredutíveis de grau n em $\mathbb{K}[X]$, onde $\mathbb{K}$ é um corpo finito com q elementos. Temos que*

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

Demonstração. Para cada d, note que o grau do polinômio $G_d(X)$ que aparece no enunciado da Proposição acima é $dI(d)$. Portanto,

$$\begin{aligned} q^n &= \text{grau}(X^{q^n} - X) \\ &= \text{grau}(\prod_{d|n} G_d(X)) \\ &= \sum_{d|n} \text{grau}(G_d(X)) \\ &= \sum_{d|n} dI(d). \end{aligned}$$

□

Teorema 1.2.5. *Sejam $\mathbb{K}$ um corpo finito e n um número natural. Então, existe pelo menos um polinômio irredutível de grau n em $\mathbb{K}[X]$.*

Demonstração. Faremos uma indução sobre o grau n. Para $n = 1$, o resultado segue trivialmente, pois X é um polinômio irredutível.

Agora, seja $n > 1$ e suponhamos que $1 = d_1 < \cdots < d_s < n$, com $s \geq 1$, são os divisores de n. Pondo $q = \#(\mathbb{K})$ e aplicando o Corolário anterior, segue que

$$\begin{aligned} q^n &= \sum_{d|n} dI(d) \\ &= \sum_{i=1}^{s} d_i I(d_i) + nI(n) \\ &\leq \sum_{i=1}^{s} \left(\sum_{d|d_i} dI(d) \right) + nI(n) \\ &= \sum_{i=1}^{s} q^{d_i} + nI(n) \\ &< \sum_{i=0}^{d_s} q^i + nI(n) \\ &= \frac{q^{d_s+1} - 1}{q - 1} + nI(n) \\ &< q^{d_s+1} + nI(n). \end{aligned}$$

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

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

$$nI(n) > q^n - q^{\frac{n}{2}+1} = q^n(1 - q^{-\frac{n}{2}+1}) \geq 0.$$

Portanto, $I(n) > 0$. □

1.3 Existência de Corpos Finitos

Teorema 1.3.1 (Existência de Corpos Finitos)**.** *Para todos os números inteiros positivos p e n com p primo, existe um corpo com p^n elementos.*

Demonstração. De acordo com o Teorema 1.2.5, existe, para cada um dos inteiros positivos p e n com p primo, pelo menos um polinômio irredutível $f(X) \in \mathbb{Z}_p[X]$ de grau n, logo, o corpo $\mathbb{K} = \mathbb{Z}_p[X]/(f(X))$ é um dos corpos procurados, pois tem p^n elementos. □

1.4 Unicidade dos corpos finitos

Teorema 1.4.1 (Unicidade dos Corpos Finitos)**.** *Dois corpos finitos com o mesmo número de elementos são isomorfos.*

Demonstração. Seja $\mathbb{L}$ um corpo finito com p^n elementos, logo, $\text{car}(\mathbb{L}) = p$ e pelo Teorema 2.0.9 ele contém um corpo isomorfo a $\mathbb{Z}_p$. Logo, $\mathbb{L}$ é um $\mathbb{Z}_p$-espaço vetorial de dimensão n.

Como $\mathbb{L}$ é um corpo finito com p^n elementos, segue pelo Corolário 1.1.13, que a equação $X^{p^n} - X$ tem todas as suas raízes em $\mathbb{L}$ e todos os elementos de $\mathbb{L}$ são as raízes desse polinômio.

Seja $f(X) \in \mathbb{Z}_p[X]$ um polinômio mônico irredutível de grau n, cuja existência está garantida pelo Teorema 1.2.5. Pela Proposição 1.2.1 (3), sabemos que $f(X)$ divide $X^{p^n} - X$

em $\mathbb{Z}_p[X]$, logo, existe $\beta \in \mathbb{L}$ tal que $f(\beta) = 0$. Note que $\{1, \beta, \beta^2, \ldots, \beta^{n-1}\} \subset \mathbb{L}$ é um conjunto linearmente independente sobre $\mathbb{Z}_p$, pois, caso contrário, existiria um polinômio não nulo $r(X) \in \mathbb{Z}_p[X]$ de grau menor do que o grau de $f(X)$ tal que $r(\beta) = 0$. Isso implicaria que $\text{MDC}(f(X), r(X)) \neq 1$ e como $f(X)$ é irredutível, então $f(X) \mid r(X)$, o que é um absurdo, pois $\text{grau}(r(X)) < n$. Logo, $\{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{Z}_p$. Lembramos também que, pela Proposição 1.2.1 (1), que $\{1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{n-1}\}$ é uma base de $\mathbb{Z}_p[X]/(f(X))$ sobre $\mathbb{Z}_p$.

Defina a seguinte função:

$$\begin{array}{rccc} \varphi: & \mathbb{Z}_p[X]/(f(X)) & \to & \mathbb{L} \\ & \overline{a_0 + \cdots + a_{n-1}X^{n-1}} & \mapsto & a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1}. \end{array}$$

Vejamos que φ está bem definida. Com efeito, considerando duas classes $\overline{a_0 + \cdots + a_{n-1}X^{n-1}}$, $\overline{b_0 + \cdots + b_{n-1}X^{n-1}} \in \mathbb{Z}_p[X]/(f(X))$ tais que

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

existe $g(X) \in \mathbb{Z}_p[X]$ tal que

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

Portanto,

$$(a_0 + \cdots + a_{n-1}\beta^{n-1}) - (b_0 + \cdots + b_{n-1}\beta^{n-1}) = f(\beta)g(\beta) = 0,$$

ou seja,

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

Obviamente que φ é sobrejetora e é aditiva, isto é,

$$\varphi(u + v) = \varphi(u) + \varphi(v),$$

para todos $u, v \in \mathbb{Z}_p[X]/(f(X))$.
Além disso, note também que,

$$\varphi(\overline{1}) = 1.$$

Para finalizar, devemos mostrar apenas que φ é multiplicativa, isto é,

$$\varphi(uv) = \varphi(u)\varphi(v), \quad \forall u, v \in \mathbb{Z}_p[X]/(f(X)),$$

pois, já sabemos que todo homomorfismo de corpos é injetor. Sejam $u = \overline{u(X)}, v = \overline{v(X)} \in \mathbb{Z}_p[X]/(f(X))$, em que $u(X), v(X) \in \mathbb{Z}_p[X]$. Dividindo $u(X)v(X)$ por $f(X)$, pelo algoritmo da divisão existem $q(X), r(X) \in \mathbb{Z}_p[X]$ tais que

$$u(X)v(X) = f(X)q(X) + r(X),$$

onde $r(X) = 0$ ou $\text{grau}(r(X)) \leq n - 1$. Logo,

$$\overline{u(X)v(X)} = \overline{r(X)} \quad \text{e} \quad u(\beta)v(\beta) = r(\beta)$$

o que prova que

$$\varphi(uv) = r(\beta) = u(\beta)v(\beta) = \varphi(u)\varphi(v).$$

Assim, qualquer corpo com p^n elementos é isomorfo a $\mathbb{Z}_p[X]/(f(X))$ e portanto quaisquer dois corpos com p^n elementos são isomorfos. □

Doravante, se q é uma potência de p com p primo, denotaremos por $\mathbb{F}_q$ o único corpo (a menos de isomorfismo) com q elementos.

Capítulo 2

Códigos corretores de erros

O presente capítulo é dedicado aos fundamentos teóricos deste trabalho. Comecemos introduzindo o conceito de um código corretor de erro e a métrica de Hamming. Em seguida, estudaremos os códigos lineares e daremos um exemplo. Para finalizar, definimos os pesos generalizados de Hamming e algumas de suas importantes propriedades. Dentre as referências, utilizamos [6] e [7].

O ponto de partida para a construção de um código corretor de erro é dar um conjunto finito A, que é chamado de **alfabeto**. Denote por $\#(A)$, o número de elementos de A, que será simbolizado por q, ou seja, $\#(A) = q$.

Definição 2.0.1 (Código Corretor de Erro)**.** *Sejam A um alfabeto e $n \geq 1$ um número inteiro. Um **código corretor de erro** C é um subconjunto próprio qualquer de A^n. Os elementos de C são chamados de **palavras-código** ou **palavras**.*

Definição 2.0.2 (Distância de Hamming)**.** *Dados dois elementos $\mathbf{u} = (u_1, \ldots, u_n), \mathbf{v} = (v_1, \ldots, v_n)$ de A^n, a **distância de Hamming** entre $\mathbf{u}$ e $\mathbf{v}$ é definida como*

$$d(\mathbf{u}, \mathbf{v}) = \#\{i \mid u_i \neq v_i, \text{com } 1 \leq i \leq n\}.$$

Exemplo 2.0.3. *Seja $\{0,1\}^3 = \{0,1\} \times \{0,1\} \times \{0,1\}$, onde $A = \{0,1\}$. Por exemplo, temos que*

$$\begin{aligned} d((0,0,1),(1,1,1)) &= 2; \\ d((0,0,0),(1,1,1)) &= 3; \\ d((1,0,0),(1,1,0)) &= 1; \\ d((1,1,0),(1,1,1)) &= 1. \end{aligned}$$

Agora, provaremos que d, satisfaz as propriedades de uma métrica. Por essa razão, a distância de Hamming entre elementos de A^n é também chamada de **métrica de Hamming**.

Proposição 2.0.4. *Sejam $\mathbf{u} = (u_1, \ldots, u_n), \mathbf{v} = (v_1, \ldots, v_n), \mathbf{w} = (w_1, \ldots, w_n) \in A^n$. Então, são satisfeitas as seguintes propriedades:*

1. ***Não-negatividade:*** *$d(\mathbf{u}, \mathbf{v}) \geq 0$ e $d(\mathbf{u}, \mathbf{v}) = 0$ se, e somente se, $\mathbf{u} = \mathbf{v}$.*
2. ***Simetria:*** *$d(\mathbf{u}, \mathbf{v}) = d(\mathbf{v}, \mathbf{u})$.*
3. ***Desigualdade Triangular:*** *$d(\mathbf{u}, \mathbf{v}) \leq d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v})$.*

Demonstração.
1) É claro que $d(\mathbf{u}, \mathbf{v}) \geq 0$. Além disso, temos

$$\begin{aligned} d(\mathbf{u}, \mathbf{v}) = 0 &\iff \#\{i \mid u_i \neq v_i, \text{com } 1 \leq i \leq n\} = 0 \\ &\iff u_i = v_i, \forall i = 1, 2, \ldots, n \\ &\iff \mathbf{u} = \mathbf{v}. \end{aligned}$$

2) Note que

$$\begin{aligned} d(\mathbf{u}, \mathbf{v}) &= \#\{i \mid u_i \neq v_i, \text{com } 1 \leq i \leq n\} \\ &= \#\{i \mid v_i \neq u_i, \text{com } 1 \leq i \leq n\} \\ &= d(\mathbf{v}, \mathbf{u}). \end{aligned}$$

3) A contribuição das i-ésimas coordenadas de $\mathbf{u}$ e $\mathbf{v}$ para $d(\mathbf{u}, \mathbf{v})$ 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, certamente a contribuição das i-ésimas coordenadas em $d(\mathbf{u}, \mathbf{v})$ é menor ou igual a das i-ésimas coordenadas em $d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v})$ $(= 0, 1$ ou $2)$.

No outro caso, temos que $u_i \neq v_i$ e, portanto, não podemos ter $u_i = w_i$ e $w_i = v_i$ (pois, se $u_i = w_i$ e $w_i = v_i$, então $u_i = v_i$, o que é uma contradição com a hipótese). Logo, a contribuição das i-ésimas coordenadas em $d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v})$ é maior ou igual a 1, que é a contribuição das i-ésimas coordenadas em $d(\mathbf{u}, \mathbf{v})$. □

Definição 2.0.5 (Disco e esfera)**.** *Seja* $\mathbf{a}$ *um elemento de* A^n *e seja* $t \geq 0$ *um número real. Definimos o* ***disco*** *e a* ***esfera de centro em*** $\mathbf{a}$ ***e raio*** t *como sendo os conjuntos*

$$\begin{aligned} D(\mathbf{a}, t) &= \{\mathbf{u} \in A^n \mid d(\mathbf{u}, \mathbf{a}) \leq t\}, \\ S(\mathbf{a}, t) &= \{\mathbf{u} \in A^n \mid d(\mathbf{u}, \mathbf{a}) = t\}, \end{aligned}$$

respectivamente.

Como $D(\mathbf{a}, t)$ e $S(\mathbf{a}, t)$ estão contidos em A^n e sabendo que A^n é um conjunto finito, então tais conjuntos são também finitos. O resultado a seguir fornecerá as suas cardinalidades.

Lema 2.0.6. *Seja* $\mathbf{a} \in A^n$ *e seja* $r > 0$ *um número natural. Então*

$$\#(D(\mathbf{a}, r)) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

Demonstração. Note que

$$D(\mathbf{a}, i) = S(\mathbf{a}, 0) \cup S(\mathbf{a}, 1) \cup S(\mathbf{a}, 2) \cup \cdots \cup S(\mathbf{a}, i),$$

com $S(\mathbf{a}, i) \cap S(\mathbf{a}, j) = \emptyset$, sempre que $i \neq j$. Consequentemente,

$$\#(D(\mathbf{a}, i)) = \#(S(\mathbf{a}, 0)) + \#(S(\mathbf{a}, 1)) + \#(S(\mathbf{a}, 2)) + \cdots + \#(S(\mathbf{a}, i)).$$

Note que $\#(S(\mathbf{a}, i)) = \binom{n}{i}(q-1)^i$, pois temos que o número de conjuntos de i posições onde acontecem as diferenças é $\binom{n}{i}$, e para cada entrada onde uma diferença vai acontecer temos $q - 1$ possíveis escolhas de elementos de A. Portanto,

$$\#(D(\mathbf{a}, r)) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

□

Definição 2.0.7 (Distância mínima)**.** *Seja C um código. A* ***distância mínima*** *de C é o número*

$$d_{\min} := \min\{d(\mathbf{u}, \mathbf{v}) \mid \mathbf{u}, \mathbf{v} \in C \text{ e } \mathbf{u} \neq \mathbf{v}\}.$$

Dado um código C com distância mínima $d_{\min}$, define-se

$$\kappa := \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor,$$

onde $\lfloor t \rfloor$ representa a parte inteira de um número real t (que é o maior inteiro que não é maior que t).

Lema 2.0.8. *Seja C um código com distância mínima $d_{\min}$. Se $\mathbf{c}$ e $\mathbf{c}'$ são palavras distintas de C, então*

$$D(\mathbf{c}, \kappa) \cap D(\mathbf{c}', \kappa) = \emptyset.$$

Demonstração. Provaremos o resultado pelo método de contradição. Suponha que exista algum $\mathbf{x} \in D(\mathbf{c}, \kappa) \cap D(\mathbf{c}', \kappa)$, então, por definição, $d(\mathbf{x}, \mathbf{c}) \leq \kappa$ e $d(\mathbf{x}, \mathbf{c}') \leq \kappa$. Pelas propriedades de simetria e desigualdade triangular, segue que

$$d(\mathbf{c}, \mathbf{c}') \leq d(\mathbf{c}, \mathbf{x}) + d(\mathbf{x}, \mathbf{c}') \leq \kappa + \kappa = 2\kappa.$$

Se $d_{\min}$ for ímpar, então $2\kappa = d_{\min} - 1$ e se $d_{\min}$ for par, então $2\kappa < d_{\min} - 1$. Logo,

$$d(\mathbf{c}, \mathbf{c}') \leq 2\kappa \leq d_{\min} - 1 < d_{\min},$$

o que é um absurdo, pois $d(\mathbf{c}, \mathbf{c}') \geq d_{\min}$. □

No que se segue, o próximo Teorema afirma que quanto maior for a distância mínima $d_{\min}$, maior será a capacidade de detecção e correção de erros do código. Portanto, é fundamental, para a Teoria dos Códigos, poder calcular $d_{\min}$ ou pelo menos determinar uma cota inferior para ele.

Teorema 2.0.9. *Seja C um código com distância mínima $d_{\min}$. Então C pode corrigir até κ erros e detectar até $d_{\min} - 1$ erros.*

Demonstração. Se ao transmitirmos uma palavra $\mathbf{c}$ do código cometemos t erros com $t \leq \kappa$, recebendo a palavra $\mathbf{r}$, então $d(\mathbf{r}, \mathbf{c}) \leq \kappa$ ($\mathbf{r} \in D(\mathbf{c}, \kappa)$). Agora, pelo Lema 2.0.8, se $\mathbf{c}'$ é uma outra palavra do código devemos ter $\mathbf{r} \notin D(\mathbf{c}', \kappa)$, ou seja, $d(\mathbf{c}', \mathbf{r}) > \kappa$. Assim, $\mathbf{c}$ difere de $\mathbf{r}$ em exatamente t entradas, mas qualquer outra palavra do código difere de $\mathbf{r}$ mais do que t entradas, o que permite a correção de erros da palavra.

Por outro lado, dada uma palavra do código, podemos nela introduzir até $d_{\min} - 1$ erros sem encontrar outra palavra do código, e assim, a detecção do erro será possível. □

Estamos interessados no caso em que o alfabeto é $A = \mathbb{F}_q$, onde $q = p^m$, com p primo. Para cada número natural n, temos $\mathbb{F}_q^n$ um $\mathbb{F}_q$-espaço vetorial de dimensão n.

2.1 Códigos lineares

Definição 2.1.1 (Código linear)**.** *Um código $C \subset \mathbb{F}_q^n$ será chamado de* ***código linear*** *se for um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q^n$. Os* ***parâmetros do código linear*** *C são a* ***dimensão*** $\dim(C) =: k$ *de C como $\mathbb{F}_q$-espaço vetorial, o* ***comprimento*** *n de C, e a* ***distância mínima*** $d_{\min}$ *de C. Usualmente os parâmetros são denotados pela terna de inteiros $(n, k, d_{\min})$.*

Todo código linear C é por definição um espaço vetorial de dimensão finita. Seja $k = \dim(C)$ e seja $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ uma base de C. Portanto, todo elemento de C se escreve de maneira única na forma

$$\lambda_1 \mathbf{v}_1 + \cdots + \lambda_k \mathbf{v}_k,$$

onde $\lambda_i \in \mathbb{F}_q$, para todo $i = 1, \ldots, k$. Segue daí que

$$\#(C) = q^k.$$

Definição 2.1.2 (Peso de uma n-upla)**.** *Dado um elemento $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, define-se o peso de $\mathbf{x}$ como sendo o número inteiro*

$$\omega(\mathbf{x}) := \#\{i \mid x_i \neq 0\} = d(\mathbf{x}, \mathbf{0}),$$

onde d representa a métrica de Hamming e $\mathbf{0}$ o vetor nulo de $\mathbb{F}_q^n$.

Exemplo 2.1.3. *Considere $A = \mathbb{F}_2$ e sejam $\mathbf{x} = (1, 1, 1, 1, 1)$ e $\mathbf{y} = (1, 0, 0, 0, 1)$ elementos de $\mathbb{F}_2^5$. Temos que*

$$\omega(\mathbf{x}) = 5 \quad e \quad \omega(\mathbf{y}) = 2.$$

Doravante, sempre que escrevermos que $C \subset \mathbb{F}_q^n$ é um código, estaremos nos referindo C como um código linear de $\mathbb{F}_q^n$.

Definição 2.1.4 (Peso do código)**.** *Definimos o peso de um código C como sendo o inteiro*

$$\omega(C) := \min\{\omega(\mathbf{x}) \mid \mathbf{x} \in C \setminus \{0\}\}.$$

Proposição 2.1.5. *Seja C um código com distância mínima $d_{\min}$. Então*

1. *Se $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, então $d(\mathbf{x}, \mathbf{y}) = \omega(\mathbf{x} - \mathbf{y})$.*
2. *$d_{\min} = \omega(C)$.*

Demonstração.
1) Usando as definições da métrica de Hamming e peso de um código, segue que

$$d(\mathbf{x}, \mathbf{y}) = \#\{i \mid x_i \neq y_i\} = \#\{i \mid x_i - y_i \neq 0\} = \omega(\mathbf{x} - \mathbf{y}).$$

2) Sejam $\mathbf{x}, \mathbf{y} \in C$, com $\mathbf{x} \neq \mathbf{y}$, tem-se que $\mathbf{z} = \mathbf{x} - \mathbf{y} \in C \setminus \{0\}$ e $d(\mathbf{x}, \mathbf{y}) = \omega(\mathbf{z})$. Logo,

$$d_{\min} = \min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\} = \min\{\omega(\mathbf{z}) \mid \mathbf{z} \in C \setminus \{0\}\} = \omega(C).$$

□

Segue do item 2 da Proposição anterior que a distância mínima de um código C é também chamada de **peso do código** C.

Definição 2.1.6 (Matriz geradora)**.** *Seja C um código e seja $k = \dim(C)$. Seja $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ uma base ordenada de um código C e considere a matriz G, cujas linhas são os vetores $\mathbf{v}_i = (v_{i1}, \ldots, v_{in})$, com $i = 1, \ldots, k$, isto é,*

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

*A matriz G é chamada de **matriz geradora** de C associada à base B.*

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

Definição 2.1.7 (Forma Padrão da matriz geradora)**.** *Seja G uma matriz geradora de um código C. Dizemos que G está na **forma padrão** se tivermos*

$$G = (\mathrm{Id}_k \mid A),$$

onde Id_k é a matriz identidade de ordem k e A é uma matriz $k \times (n-k)$.

2.2 Códigos Duais

Definição 2.2.1 (Produto interno)**.** *Sejam $\mathbf{u} = (u_1, \ldots, u_n), \mathbf{v} = (v_1, \ldots, v_n)$ elementos de $\mathbb{F}_q^n$, define-se o **produto interno** como sendo uma função $\langle \cdot, \cdot \rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ dada por*

$$\langle \mathbf{u}, \mathbf{v} \rangle = u_1 v_1 + \cdots + u_n v_n.$$

A operação acima possui as propriedades usuais de um produto interno, ou seja, é simétrica e bilinear.

Definição 2.2.2 (Código dual)**.** *Seja C um código. O **código dual** é o conjunto*

$$C^\perp = \{\mathbf{x} \in \mathbb{F}_q^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0, \forall \mathbf{y} \in C\}.$$

Lema 2.2.3. *Seja C um código, com matriz geradora G. Temos que:*

1. *$C^\perp$ é um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q^n$.*
2. *$\mathbf{x} \in C^\perp \iff G\mathbf{x}^t = \mathbf{0}$, onde $\mathbf{x}^t$ denota o vetor $\mathbf{x}$ transposto e $\mathbf{0}$ denota a matriz coluna $k \times 1$.*

Demonstração.
1) Claramente $\mathbf{0} \in C^\perp$. Sejam $\mathbf{x}, \mathbf{y} \in C^\perp$ e seja $\lambda \in \mathbb{F}_q$. Usando a bilinearidade do produto interno, temos que

$$\langle \mathbf{x} + \lambda\mathbf{y}, \mathbf{z} \rangle = \langle \mathbf{x}, \mathbf{z} \rangle + \lambda \langle \mathbf{y}, \mathbf{z} \rangle = 0 + \lambda \cdot 0 = 0,$$

para todo $\mathbf{z} \in C$.
2) $\boxed{\Rightarrow}$ Seja $\mathbf{x} \in C^\perp$, então $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ para todo $\mathbf{y} \in C$. Em particular, para todas as linhas de G, os vetores $\mathbf{v}_1, \ldots, \mathbf{v}_k$, que constituem uma base de C, temos que $\langle \mathbf{x}, \mathbf{v}_i \rangle = 0$, para todo $i = 1, \ldots, k$. Logo, $G\mathbf{x}^t = \mathbf{0}$.
$\boxed{\Leftarrow}$ Se $G\mathbf{x}^t = \mathbf{0}$, então $\mathbf{x}$ é ortogonal a todos os elementos de uma base de C. Pela bilinearidade do produto interno, $\mathbf{x}$ é ortogonal a todos os elementos de C. Portanto, $\mathbf{x} \in C^\perp$. □

Proposição 2.2.4. *Seja C um código de dimensão k e considere $G = (\mathrm{Id_k} \mid \mathrm{A})$, matriz geradora de C na forma padrão. Então*

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

Demonstração.
1) Pelo Lema 2.2.3 (2), temos que $\mathbf{x} = (x_1, \ldots, x_n) \in C^\perp$ se, e somente se, $G\mathbf{x}^t = \mathbf{0}$. Logo,

$$(\mathrm{Id_k} \mid \mathrm{A})\,\mathbf{x}^t = \mathbf{0} \iff \begin{pmatrix} 1 & 0 & \cdots & 0 & a_{1(k+1)} & \cdots & a_{1n} \\ 0 & 1 & \cdots & 0 & a_{2(k+1)} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & a_{k(k+1)} & \cdots & a_{kn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \mathbf{0}$$

$$\iff \begin{pmatrix} x_1 + a_{1(k+1)}x_{k+1} + \cdots + a_{1n}x_n \\ x_2 + a_{2(k+1)}x_{k+1} + \cdots + a_{2n}x_n \\ \vdots \\ x_k + a_{k(k+1)}x_{k+1} + \cdots + a_{kn}x_n \end{pmatrix} = \mathbf{0}$$

$$\iff \begin{cases} x_1 = -a_{1(k+1)}x_{k+1} - \cdots - a_{1n}x_n, \\ x_2 = -a_{2(k+1)}x_{k+1} - \cdots - a_{2n}x_n, \\ \vdots \\ x_k = -a_{k(k+1)}x_{k+1} - \cdots - a_{kn}x_n, \end{cases}$$

$$\iff \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} = -A \begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix}.$$

Como q é o número de elementos de $\mathbb{F}_q$, o código $C^\perp$ tem q^{n-k} palavras, pois os a_{ij} da matriz A são fixos e existem q escolhas possíveis para cada um dos $x_{k+1}, \ldots, x_n$. Portanto, $\dim(C^\perp) = n - k$.
2) É fácil ver que as linhas de H são linearmente independentes, portanto, geram um subespaço vetorial de dimensão $n - k$. Como as linhas de H são ortogonais às linhas de G, temos que o espaço gerado pelas linhas de H está contido em $C^\perp$ e como esses dois subespaços vetoriais possuem a mesma dimensão, eles coincidem, provando assim que $H = (-A^t \mid \mathrm{Id}_{n-k})$ é uma matriz geradora de $C^\perp$. □

Lema 2.2.5. *Seja C um código de dimensão k com matriz geradora G. Uma matriz H de ordem $(n - k) \times n$, com coeficientes em $\mathbb{F}_q$ e com linhas linearmente independentes, é uma matriz geradora de $C^\perp$ se, e somente se, $G \cdot H^t = \mathbf{0}$.*

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

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

para todos $i = 1, \ldots, k$, $j = 1, \ldots, n - k$. Portanto, $G \cdot H^t = \mathbf{0}$ equivale a dizer que todos os vetores do subespaço gerado pelas linhas de H estão em $C^\perp$. Por outro lado, esse subespaço tem a mesma dimensão de $C^\perp$, logo, $G \cdot H^t = \mathbf{0}$ se, e, somente se, $C^\perp$ é gerado pelas linhas de H. □

Corolário 2.2.6. $(C^{\perp})^{\perp} = C$.

Demonstração. Sejam G e H matrizes geradoras de C e $C^{\perp}$, respectivamente. Logo, pelo Lema 2.2.5, temos que $G \cdot H^t = \mathbf{0}$. Tomando a transposta em ambos os lados na igualdade anterior, temos que

$$(G \cdot H^t)^t = \mathbf{0} \iff H \cdot G^t = \mathbf{0}.$$

Como G é uma matriz com linhas linearmente independentes de ordem $k \times n$ e $\dim(C^{\perp})^{\perp} = k$, e novamente pelo Lema 2.2.5, temos que G é uma matriz geradora de $(C^{\perp})^{\perp}$ e, portanto, $(C^{\perp})^{\perp} = C$. □

A Proposição seguinte nos permite caracterizar os elementos de um código através de uma condição de anulamento.

Proposição 2.2.7. *Seja C um código e seja H uma matriz geradora de $C^{\perp}$. Então*

$$\mathbf{v} \in C \iff H\mathbf{v}^t = \mathbf{0}.$$

Demonstração. Seja $\mathbf{v} \in C$, então pelo Corolário 2.2.6, temos que $\mathbf{v} \in (C^{\perp})^{\perp}$. Agora, pelo Lema 2.2.3 (2), temos que $H\mathbf{v}^t = 0$. □

Definição 2.2.8 (Matriz teste de paridade e síndrome de um vetor)**.** *Seja C um código e seja H uma matriz geradora de $C^{\perp}$. A matriz H é chamada de* ***matriz teste de paridade*** *de C e o vetor $H\mathbf{v}^t$ é chamado* ***síndrome*** *de $\mathbf{v}$.*

Note que, para verificar se um determinado vetor $\mathbf{v} \in \mathbb{F}_q^n$ pertence ou não a um código C com matriz geradora G, é preciso verificar se o sistema de n equações com k incógnitas $\mathbf{x} = (x_1, \ldots, x_k)$ dado por

$$\mathbf{x}G = \mathbf{v},$$

admite solução. Agora, trabalhando com uma matriz teste de paridade H, a solução pode ser encontrada bem mais rapidamente, pois basta verificar se a síndrome de $\mathbf{v}$ é o vetor nulo.

Vejamos um exemplo a seguir.

Exemplo 2.2.9. *Seja $C \subset \mathbb{F}_2^6$ um código com matriz geradora G dada por*

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

Sejam $\mathbf{v} = (1,0,0,1,1,1), \mathbf{v}' = (0,1,0,1,0,1) \in \mathbb{F}_2^6$. Note que, a matriz geradora G está na forma padrão, onde

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Assim, segue da Proposição 2.2.4 (2) que

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

Como

$$H\mathbf{v}^t = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

e

$$H(\mathbf{v}')^t = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \neq \mathbf{0}$$

então $\mathbf{v} \in C$ *e* $\mathbf{v}' \notin C$.

Os resultados seguintes mostram que a matriz teste de paridade de um código contém, de maneira bastante simples, informações sobre o valor do peso $d_{\min}$ do código.

Proposição 2.2.10. *Seja H a matriz teste de paridade de um código C. Então,*

$$\omega(C) \geq s \iff \textit{quaisquer } s-1 \textit{ colunas de } H \textit{ são linearmente independentes.}$$

Demonstração. $\boxed{\Rightarrow}$ Suponha que $\omega(C) \geq s$. Suponhamos também, por absurdo, que H tenha $s-1$ colunas linearmente dependentes, digamos $h^{i_1}, h^{i_2}, \ldots, h^{i_{s-1}}$, logo, existiriam $c_{i_1}, \ldots, c_{i_{s-1}}$ elementos em $\mathbb{F}_q$, nem todos nulos, tais que

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

Assim, considerando $\mathbf{c} = (0, \ldots, c_{i_1}, 0, \ldots, c_{i_{s-1}}, 0, \ldots, 0)$, temos que $\mathbf{c} \in C$, pois $H\mathbf{c}^t = \mathbf{0}$, e $\omega(\mathbf{c}) \leq s-1 < s$, o que é um absurdo. Portanto, quaisquer $s-1$ colunas de H são linearmente independentes.

$\boxed{\Leftarrow}$ Suponhamos, que cada conjunto de $s-1$ colunas de H é linearmente independente. Seja $\mathbf{c} = (c_1, \ldots, c_n)$ uma palavra não nula de C, e sejam $h^1, \ldots, h^n$ as colunas de H. Como H é uma matriz teste de paridade de C, pela Proposição 2.2.7, temos que

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

Como $\omega(\mathbf{c})$ é o número de coordenadas não nulas de $\mathbf{c}$, segue que se $\omega(\mathbf{c}) \leq s-1$, teríamos por 2.2 uma combinação linear nula de um número t, com $1 \leq t \leq s-1$, de colunas de H, o que é uma contradição. Logo, $\omega(\mathbf{c}) \geq s$ e, portanto, $\omega(C) \geq s$. □

Teorema 2.2.11. *Seja C um código e seja H a matriz teste de paridade. Então,*

$$\omega(C) = s \iff \textit{quaisquer } s-1 \textit{ colunas de } H \textit{ são linearmente independentes e existem } s \textit{ colunas de } H \textit{ linearmente dependentes.}$$

Demonstração. $\boxed{\Rightarrow}$ Suponha que $\omega(C) = s$, então pela Proposição 2.2.10 quaisquer $s-1$ colunas de H são linearmente independentes. Suponha ainda que quaisquer s colunas de H são linearmente independentes e novamente pela Proposição 2.2.10, segue que $\omega(C) \geq s+1 > s$, o que é um absurdo.

$\boxed{\Leftarrow}$ Como qualquer conjunto de $s-1$ colunas de H é linearmente independente, então pela Proposição 2.2.10, temos que $\omega(C) \geq s$. Como existem s colunas linearmentes dependentes, novamente pela Proposição 2.2.10, $\omega(C)$ não pode ser maior do que s e, portanto, $\omega(C) = s$. □

Corolário 2.2.12 (Cota de Singleton)**.** *Os parâmetros fundamentais $(n, k, d_{\min})$ de um código C satisfazem a seguinte desigualdade:*

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

Demonstração. Seja H uma matriz teste de paridade de um código C. Temos que o posto de H é igual a $n-k$, logo H tem $n-k$ colunas independentes. Se existe um conjunto de $n-k$ colunas que é linearmente dependente temos que $d_{\min} \leq n-k$. Se todo conjunto de $n-k$ colunas é linearmente independente então $d_{\min} = n-k+1$ (pois o posto de H é $n-k$). Assim $d_{\min} \leq n-k+1$. □

Definição 2.2.13 (Distância mínima separável)**.** *Um código C será chamado de* **MDS** ***(Maximum Distance Separable)*** *se valer a igualdade $d_{\min} = n-k+1$.*

Exemplo 2.2.14 (Códigos de Reed-Solomon)**.** *Considere o $\mathbb{F}_q$-espaço vetorial dos polinômios em $\mathbb{F}_q[X]$ de grau menor ou igual a $k-1$, incluindo o polinômio nulo, isto é,*

$$\mathbb{F}_q[X]_{k-1} = \{P \in \mathbb{F}_q[X] \mid \text{grau}(P) \leq k-1\} \cup \{0\}.$$

É claro que esse espaço vetorial tem dimensão k, com uma de suas bases dada por

$$\{1, X, X^2, \ldots, X^{k-1}\}.$$

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

$$\begin{array}{rccc} \mathrm{T}: & \mathbb{F}_q[X]_{k-1} & \to & \mathbb{F}_q^n \\ & P & \mapsto & (P(\alpha_1), \ldots, P(\alpha_n)). \end{array}$$

Veja que

$$\ker(\mathrm{T}) = \{P \in \mathbb{F}_q[X]_{k-1} \mid P(\alpha_1) = \cdots = P(\alpha_n) = 0\} = \{0\},$$

pois um polinômio não nulo P de grau menor do que k não pode ter n raízes distintas, o que significa que T é injetora. Logo, $C = \mathrm{T}(\mathbb{F}_q[X]_{k-1})$ é um código linear de comprimento n e dimensão k.

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

Uma matriz geradora de C é dada por

$$\begin{pmatrix} \mathrm{T}(1) \\ \mathrm{T}(X) \\ \mathrm{T}(X^2) \\ \vdots \\ \mathrm{T}(X^{k-1}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix},$$

pois transformações lineares bijetoras levam base em base. Agora, vamos determinar a sua distância mínima.

Já sabemos que, pela Cota de Singleton

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

Provemos que vale a outra desigualdade. Para isso, seja $\mathbf{c}$ uma palavra não nula de C, então existe $P \in \mathbb{F}_q[X]_{k-1}$ tal que

$$\mathbf{c} = (P(\alpha_1), \ldots, P(\alpha_n)).$$

Logo,

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

Portanto, $d_{\min} = n-k+1$, o que prova que os Códigos de Reed-Solomon são códigos **MDS**.

2.3 Pesos Generalizados de Hamming

Definição 2.3.1 (Suporte de um código)**.** *Seja C um código de dimensão k e seja U um subespaço de C. O* ***suporte*** *de U, denotado por $\chi(U)$, é o conjunto*

$$\chi(U) := \{i \mid \exists\ (x_1, \ldots, x_n) \in U,\ x_i \neq 0\}.$$

É claro que, para qualquer subespaço $U \subseteq \mathbb{F}_q^n$, a cardinalidade de $\chi(U)$ é um inteiro que satisfaz $1 \leq \#(\chi(U)) \leq n$.

Exemplo 2.3.2. *Consideremos $\mathbb{F}_2 = \{0, 1\}$ e $C = \{(0,0,0,0), (0,0,0,1), (1,1,1,0), (1,1,1,1)\}$ um código de $\mathbb{F}_2^4$. Considere agora os subespaços de dimensão* 1

$$D_1 = \{(0,0,0,0), (0,0,0,1)\}, \quad D_2 = \{(0,0,0,0), (1,1,1,0)\} \quad e \quad D_3 = \{(0,0,0,0), (1,1,1,1)\}.$$

Então,

$$\chi(D_1) = \{4\}, \quad \chi(D_2) = \{1,2,3\} \quad e \quad \chi(D_3) = \{1,2,3,4\}.$$

Definição 2.3.3 (r-ésimo Peso Generalizado de Hamming)**.** *Seja C um código de dimensão k e seja $r = 1, \ldots, k$. O* ***r-ésimo peso generalizado de Hamming*** *de C, denotado por d_r, é definido como sendo o número inteiro não negativo*

$$d_r := \min\{\#(\chi(U)) \mid U \text{ é um subespaço de } C \text{ com } \dim(U) = r\}.$$

O conjunto $\{d_1, \ldots, d_k\}$ é chamado de **hierarquia de pesos** de C.

Observação 2.3.4. *Retomando o Exemplo 2.3.2, no qual o alfabeto é $\mathbb{F}_2$, observamos que D_1, D_2 e D_3 são precisamente todos os $\mathbb{F}_2$-subespaços vetoriais de dimensão* 1*. Para cada um deles, a cardinalidade do suporte coincide com o peso de Hamming da palavra não nula. Assim, o primeiro peso generalizado de Hamming coincide, neste caso, com a distância mínima do código.*

Na verdade, provaremos agora que $d_1 = d_{\min}$ para qualquer corpo finito $\mathbb{F}_q$, com $q \geq 2$.

Teorema 2.3.5. *Seja C um código e seja $r = 1$. Então, $d_1 = d_{\min}$.*

Demonstração. Para $r = 1$, temos que

$$d_1 = \min\{\#(\chi(D)) \mid D \text{ é um subespaço de } C \text{ com} \dim(D) = 1\}.$$

Dado D subespaço com $\dim(D) = 1$, existe $\mathbf{x} \in D \setminus \{0\}$ tal que $D = \langle \mathbf{x} \rangle$. Portanto,

$$\begin{aligned} \chi(D) &= \{i \mid \exists\ (x'_1, \ldots, x'_n) = \mathbf{x}' \in \langle \mathbf{x} \rangle,\ x'_i \neq 0\} \\ &= \{i \mid x_i \neq 0\} \\ &= \omega(\mathbf{x}). \end{aligned}$$

Logo,

$$d_1 = \min\{\omega(\mathbf{x}) \mid \mathbf{x} \in C \setminus \{0\}\} = d_{\min}.$$

□

Segue imediatamente do Teorema anterior que o r-ésimo peso generalizado de Hamming é uma generalização do conceito de distância mínima.

Proposição 2.3.6. *Seja C um código e seja $C_1 \subseteq C_2$, com C_1 e C_2 subcódigos de C. Então*

$$\chi(C_1) \subseteq \chi(C_2).$$

Demonstração. Seja $j \in \chi(C_1)$, então existe $(x_1, \ldots, x_n) \in C_1$, com $x_j \neq 0$. Como $C_1 \subseteq C_2$, temos $(x_1, \ldots, x_n) \in C_2$, com $x_j \neq 0$ e, portanto, $\chi(C_1) \subseteq \chi(C_2)$. □

Teorema 2.3.7 (Monotonicidade)**.** *Seja C um código. Temos que*

$$1 \leq d_1 < d_2 < \cdots < d_k \leq n.$$

Demonstração. Claramente $d_r \geq 1$ e $d_r \leq n$, para todo r. Afirmamos que

$$d_{r-1} \leq d_r,$$

para todo $r \geq 2$.

Seja $U \subseteq C$ um subespaço de $\dim(U) = r$. Como $\dim(U) = r \geq 2$, existe um subespaço próprio $V \subset U$ de $\dim(V) = r - 1$. Pela Proposição 2.3.6, temos que $\chi(V) \subseteq \chi(U)$ e então $\#(\chi(V)) \leq \#(\chi(U))$. Pela definição de d_{r-1}, segue que

$$d_{r-1} \leq \#(\chi(V)) \leq \#(\chi(U)).$$

Como a desigualdade anterior vale para todo subespaço U de dimensão r, segue que

$$d_{r-1} \leq d_r,$$

para todo $r \geq 2$.

Provemos que a desigualdade é estrita. Considere um subcódigo D com $\#(\chi(D)) = d_r$ tal que $\dim(D) = r$. Vamos construir um código de dimensão $r - 1$ tal que o suporte do código seja estritamente menor do que o de D. Seja $i \in \chi(D)$ e defina

$$D_i := \{\mathbf{x} \in D \mid x_i = 0\}.$$

É claro que D_i é um subespaço vetorial de D.
Defina a transformação linear

$$\begin{array}{rccc} \varphi: & D & \to & \mathbb{F}_q \\ & \mathbf{x} & \mapsto & \varphi(\mathbf{x}) = x_i. \end{array}$$

Temos que

$$\begin{aligned} \ker(\varphi) &= \{\mathbf{x} \in D \mid \varphi(\mathbf{x}) = 0\} \\ &= \{\mathbf{x} \in D \mid x_i = 0\} \\ &= D_i. \end{aligned}$$

Seja $y \in \mathbb{F}_q$. Como $i \in \chi(D)$, existe $\mathbf{x} = (x_1, \ldots, x_n) \in D$ com $x_i \neq 0$. Como $x_i \neq 0$ e pertence a $\mathbb{F}_q$, então existe o inverso x_i^{-1}. Defina $\lambda := yx_i^{-1} \in \mathbb{F}_q$, então

$$\varphi(\lambda\mathbf{x}) = \lambda\varphi(\mathbf{x}) = (yx_i^{-1})x_i = y(x_i x_i^{-1}) = y.$$

Pelo Teorema do Núcleo e da Imagem, segue que

$$\begin{aligned} \dim(D) &= \dim(D_i) + \dim(\mathbb{F}_q) \\ r &= \dim(D_i) + 1. \end{aligned}$$

Ou seja, $\dim(D_i) = r - 1$. Logo,

$$d_{r-1} \leq \#(\chi(D_i)) \leq \#(\chi(D)) - 1 = d_r - 1 < d_r.$$

□

O Corolário 2.2 pode ser generalizado, como segue:

Corolário 2.3.8 (Cota de Singleton Generalizada)**.** *Seja C um código, então*

$$d_r \leq n - k + r.$$

Demonstração. Conforme visto no Teorema 2.3, temos que $d_k \leq n$ e $d_r \leq d_{r+1} - 1$. Logo,

$$d_{k-1} \leq d_k - 1 \leq n - 1 = n - k + (k-1)$$
$$d_{k-2} \leq d_{k-1} - 1 \leq n - 2 = n - k + (k-2).$$

Repetindo esse argumento recursivamente, obtemos

$$d_{k-s} \leq n - s = n - k + (k-s).$$

Fazendo $k - s = r$, concluímos o que queríamos. □

Seja H a matriz teste de paridade de C e sejam $\{\beta_1, \ldots, \beta_{n-k}\}$ as linhas de H. Sejam H_i, $1 \leq i \leq n$, as colunas de H. Denote por $\langle H_i \mid i \in I\rangle$ o espaço gerado por essas colunas. Usaremos essa notação no próximo resultado.

Teorema 2.3.9. *Seja C um código. Então*

$$d_r = \min\{\#(I) \mid I \subset \{1, \ldots, n\},\ \#(I) - \dim(\langle H_i \mid i \in I\rangle) \geq r\}.$$

Demonstração. Seja $I \subset \{1, \ldots, n\}$, com $\#(I) = \ell$, definimos $S(I) := \langle H_i \mid i \in I\rangle$ e

$$S^{\perp}(I) := \left\{\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid x_i = 0 \text{ para } i \notin I \text{ e } \sum_{i \in I} x_i H_i = \mathbf{0}\right\}$$

(seguimos aqui a notação de [7], e não devemos confundir $S^{\perp}(I)$ com $S(I)^{\perp}$).

Observe que $S^{\perp}(I) \subset C$, pois se $\mathbf{x} = (x_1, \ldots, x_n) \in S^{\perp}(I)$, então $\sum_{i \in I} x_i H_i = \sum_{i=1}^{n} x_i H_i = \mathbf{0}$, ou seja, $H\mathbf{x}^t = \mathbf{0}$. Além disso, é claro que $S^{\perp}(I)$ é um subespaço vetorial de C.
Vejamos que

$$\dim(S(I)) + \dim(S^{\perp}(I)) = \ell.$$

Considere $I = \{i_1, \ldots, i_\ell\}$ e seja A a matriz

$$A = \begin{pmatrix} \beta_{1i_1} & \beta_{1i_2} & \cdots & \beta_{1i_\ell} \\ \beta_{2i_1} & \beta_{2i_2} & \cdots & \beta_{2i_\ell} \\ \beta_{3i_1} & \beta_{3i_2} & \cdots & \beta_{3i_\ell} \\ \vdots & \vdots & \vdots & \vdots \\ \beta_{(n-k)i_1} & \beta_{(n-k)i_2} & \cdots & \beta_{(n-k)i_\ell} \end{pmatrix},$$

obtida a partir das colunas de H e dos índices em I. Note que, 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. É fácil ver que existe um isomorfismo entre $W^{\perp}$ e $S^{\perp}(I)$, dado por $(\alpha_{i_1}, \ldots, \alpha_{i_\ell}) \mapsto (\gamma_1, \ldots, \gamma_n)$ onde $\gamma_i = 0$ se $i \notin I$, e $\gamma_{i_j} = \alpha_{i_j}$, para $j = 1, \ldots, \ell$. Daí vem que

$$\dim(S(I)) + \dim(S^{\perp}(I)) = \ell.$$

Seja $J \subset \{1, \ldots, n\}$ tal que $\#(J) - \dim(\langle H_i \mid i \in I\rangle) \geq r$ e $\#(J) = \min\{\#(I) \mid I \subset \{1, \ldots, n\},\ \#(I) - \dim(\langle H_i \mid i \in I\rangle) \geq r\}$. Temos então que $\#(J) - \dim(\langle H_i \mid i \in J\rangle) = r$. Com efeito, suponha, por contradição, que

$$\#(J) - \dim(\langle H_i \mid i \in J\rangle) = r' > r.$$

Tome qualquer elemento $j \in J$ e defina $J' = J \setminus \{j\}$. Logo, $\dim(S(J')) \leq \dim(S(J))$. Daí,

$$\begin{aligned} \#(J') - \dim(S(J')) &= \#(J) - 1 - \dim(S(J')) \\ &\geq \#(J) - 1 - \dim(S(J)) \\ &= r' - 1 \\ &\geq r, \end{aligned}$$

o que contraria a minimalidade de $\#(J)$.

Assim, tomamos $d := \min\{\#(I) \mid I \subset \{1, \ldots, n\},\ \#(I) - \dim(\langle H_i \mid i \in I\rangle) = r\}$, e queremos mostrar que $d = d_r$. Seja $I \subset \{1, \ldots, n\}$ tal que $\#(I) = d$ e $d - \dim(S(I)) = r$. Então $\dim(S^{\perp}(I)) = r$ e como $S^{\perp} \subset C$ temos

$$d_r \leq \#(\chi(S^{\perp}(I))) \leq \#(I) = d.$$

Falta mostrar a desigualdade contrária. Seja D um subcódigo de C de $\dim(D) = r$ tal que $\#(\chi(D)) = d_r$ e seja $I = \chi(D)$. Temos que $D \subset S^{\perp}(I)$, pois se $\mathbf{x} \in D$ então $x_j = 0$ quando $j \notin I$ e $\mathbf{0} = H\mathbf{x}^t = \sum_{i=1}^{n} x_i H_i = \sum_{i \in I} x_i H_i$. Então $\dim(S^{\perp}(I)) \geq r = \dim(D)$. Agora, suponha, por contradição, que $\dim(S^{\perp}(I)) = r' > r$, então

$$d_{r'} \leq \#(\chi(S^{\perp}(I))) \leq \#(I) = \#(\chi(D)) = d_r,$$

o que é uma contradição com a Proposição 2.3.7. Logo, $\dim(S^{\perp}(I)) = r$ e então $D = S^{\perp}(I)$. Daí, $\#(I) - \dim(S(I)) = \dim(S^{\perp}(I)) = r$ e, portanto, $d = d_r$. □

Capítulo 3

Bases de Gröbner e códigos de avaliação

Neste capítulo apresentaremos conceitos básicos da teoria de bases de Gröbner, e finalizamos com a definição dos assim chamados códigos de avaliação. No próximo capítulo utilizaremos ferramentas da teoria apresentada aqui para estudar uma família de códigos de avaliação. Denotamos por $\mathbb{N}_0$ o conjunto dos inteiros não negativos e por $\mathbb{K}[\mathbf{X}]$ o anel de polinômios $\mathbb{K}[X_1, \ldots, X_m]$. Usamos [2] como referência principal.

3.1 Monômio, Ordem Monomial e o Algoritmo da Divisão para Polinômios de Várias Variáveis

Definição 3.1.1 (Termos, monômios e grau total)**.** *Sejam $a \in \mathbb{K}^*$ e $\alpha_1, \ldots, \alpha_m \in \mathbb{N}_0$. Um **termo** em $X_1, \ldots, X_m$ é um produto da forma $aX_1^{\alpha_1} \cdots X_m^{\alpha_m}$. Quando $a = 1$, o produto $X_1^{\alpha_1} \cdots X_m^{\alpha_m}$ é chamado de **monômio**. O **grau total** desse monômio é a soma $\alpha_1 + \cdots + \alpha_m$.*

Um monômio $X_1^{\alpha_1} \cdots X_m^{\alpha_m}$ será denotado por $\mathbf{X}^{\boldsymbol{\alpha}}$ (ou $\mathbf{X}^{\boldsymbol{\beta}}, \mathbf{X}^{\boldsymbol{\gamma}}$, etc), onde $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m$. Denotamos por $\mathcal{M}$ o conjunto de todos os monômios de $\mathbb{K}[\mathbf{X}]$.

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

Definição 3.1.2 (Ordem monomial)**.** *Uma **ordem monomial** em $\mathcal{M}$ é uma ordem total $\preceq$ definida sobre $\mathcal{M}$ tal que:*

i) se $\mathbf{X}^{\boldsymbol{\alpha}} \preceq \mathbf{X}^{\boldsymbol{\beta}}$, então $\mathbf{X}^{\boldsymbol{\alpha}+\boldsymbol{\gamma}} \preceq \mathbf{X}^{\boldsymbol{\beta}+\boldsymbol{\gamma}}$, para todos os $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma} \in \mathbb{N}_0^m$;

ii) qualquer subconjunto não vazio $A \subset \mathcal{M}$ possui um menor elemento.

No que se segue, apresentamos alguns exemplos de ordens monomiais, a saber: ordem lexicográfica, lexicográfica graduada e lexicográfica graduada reversa.

Exemplo 3.1.3 (Ordem lexicográfica)**.** *A ordem lexicográfica (com $X_m \preceq \cdots \preceq X_1$) é definida como $\mathbf{X}^{\boldsymbol{\alpha}} \preceq \mathbf{X}^{\boldsymbol{\beta}}$ se $\boldsymbol{\alpha} = \boldsymbol{\beta}$, ou se a primeira entrada não nula da esquerda para a direita em $\boldsymbol{\beta} - \boldsymbol{\alpha}$ é positiva.*

Exemplo 3.1.4 (Ordem lexicográfica graduada)**.** *A ordem lexicográfica graduada (com $X_m \preceq \cdots \preceq X_1$) é definida como $\mathbf{X}^{\boldsymbol{\alpha}} \preceq \mathbf{X}^{\boldsymbol{\beta}}$ se $\boldsymbol{\alpha} = \boldsymbol{\beta}$, ou $\sum_{i=1}^m \alpha_i < \sum_{i=1}^m \beta_i$, ou se $\sum_{i=1}^m \alpha_i = \sum_{i=1}^m \beta_i$ então $\mathbf{X}^{\boldsymbol{\alpha}} \preceq \mathbf{X}^{\boldsymbol{\beta}}$, onde $\preceq$ é a ordem lexicográfica definida acima.*

Exemplo 3.1.5 (Ordem lexicográfica graduada reversa)**.** *A ordem lexicográfica graduada reversa (com $X_m \preceq \cdots \preceq X_1$) é definida como $\mathbf{X}^{\boldsymbol{\alpha}} \preceq \mathbf{X}^{\boldsymbol{\beta}}$ se $\boldsymbol{\alpha} = \boldsymbol{\beta}$, ou $\sum_{i=1}^m \alpha_i < \sum_{i=1}^m \beta_i$, ou se $\sum_{i=1}^m \alpha_i = \sum_{i=1}^m \beta_i$ então a primeira entrada não nula da direita para a esquerda em $\boldsymbol{\beta} - \boldsymbol{\alpha}$ é negativa.*

Agora, vamos aplicar as ordens monomiais citadas acima.

Exemplo 3.1.6. *Sejam* $X_1^3X_2^4X_3^7,\ X_1^7X_2^3X_3^4 \in \mathbb{R}[X_1, X_2, X_3]$ *dois monômios.*

- *Se considerarmos a ordem lexicográfica (com* $X_3 \preceq X_2 \preceq X_1$*), então* $X_1^3X_2^4X_3^7 \preceq X_1^7X_2^3X_3^4$*, pois o expoente da variável* X_1 *em* $X_1^7X_2^3X_3^4$ *é maior que o expoente em* $X_1^3X_2^4X_3^7$*.*

- *Se considerarmos a ordem lexicográfica graduada (com* $X_3 \preceq X_2 \preceq X_1$*), então* $X_1^3X_2^4X_3^7 \preceq X_1^7X_2^3X_3^4$*, pois embora eles possuam o mesmo grau* 14*, temos que* $X_1^3X_2^4X_3^7$ *é menor do que* $X_1^7X_2^3X_3^4$ *na ordem lexicográfica, conforme vimos acima.*

- *Se considerarmos a ordem lexicográfica graduada reversa (com* $X_3 \preceq X_2 \preceq X_1$*), então* $X_1^3X_2^4X_3^7 \preceq X_1^7X_2^3X_3^4$*, pois ambos os monômios têm grau igual a 14 e o expoente da variável* X_3 *em* $X_1^3X_2^4X_3^7$ *é maior que o expoente em* $X_1^7X_2^3X_3^4$*.*

Definição 3.1.7 (Monômio, termo e coeficiente líder)**.** *Sejam* $f = \sum_{i=1}^{n} a_iM_i \in \mathbb{K}[\mathbf{X}]$ *um polinômio não nulo, onde* $a_i \in \mathbb{K}^*$ *e* $M_i \in \mathcal{M}$ *para todo* $i = 1, \ldots, n$ *e seja* $\preceq$ *uma ordem monomial definida sobre* $\mathcal{M}$*. Então, o* ***monômio líder*** *de* f *(com respeito a* $\preceq$*) é* $M_\ell := \max\{M_i \mid i = 1, \ldots, n\}$*, o* ***coeficiente líder*** *de* f *(com respeito a* $\preceq$*) é* a_ℓ *e o* ***termo líder*** *de* f *(com respeito a* $\preceq$*) 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 3.1.8. *Seja* $f = 4X_1^3X_2^4X_3^2 + 5X_1X_3^9 + 7X_2^9X_3 \in \mathbb{R}[X_1, X_2, X_3]$*.*

1. *Com respeito à ordem lexicográfica (com* $X_3 \preceq X_2 \preceq X_1$*), temos:*

   - $\mathrm{LM}(f) = X_1^3X_2^4X_3^2$*;*
   - $\mathrm{LC}(f) = 4$*;*
   - $\mathrm{LT}(f) = 4X_1^3X_2^4X_3^2$*.*

2. *Com respeito à ordem lexicográfica graduada (com* $X_3 \preceq X_2 \preceq X_1$*), temos:*

   - $\mathrm{LM}(f) = X_1X_3^9$*;*
   - $\mathrm{LC}(f) = 5$*;*
   - $\mathrm{LT}(f) = 5X_1X_3^9$*.*

3. *Com respeito à ordem lexicográfica graduada reversa (com* $X_3 \preceq X_2 \preceq X_1$*), temos:*

   - $\mathrm{LM}(f) = X_2^9X_3$*;*
   - $\mathrm{LC}(f) = 7$*;*
   - $\mathrm{LT}(f) = 7X_2^9X_3$*.*

Um importante procedimento na teoria das bases de Gröbner é a divisão de um polinômio por uma lista de polinômios não nulos.

Definição 3.1.9 (Divisão de um polinômio por uma lista de polinômios não nulos)**.** *Dividir* $f \in \mathbb{K}[\mathbf{X}]$ *por* $\{g_1, \ldots, g_t\} \subset \mathbb{K}[\mathbf{X}] \setminus \{0\}$*, com respeito a uma ordem monomial* $\preceq$*, significa encontrar quocientes* $q_1, \ldots, q_t \in \mathbb{K}[\mathbf{X}]$ *e um resto* $r \in \mathbb{K}[\mathbf{X}]$ *tal que*

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

onde $r = 0$ *ou nenhum monômio que aparece em* r *é múltiplo de* $\mathrm{LM}(g_i)$*, para todo* $i = 1, \ldots, t$*.*

Na literatura sobre bases de Gröbner o leitor poderá encontrar uma descrição do algoritmo usual usado para determinar os quocientes e o resto, bem como uma prova que o algoritmo de fato termina após um número finito de etapas. Aqui, iremos apenas dar um exemplo de como isso funciona na prática.

A ideia básica do algoritmo é a mesma da qual estamos familiarizados quando dividimos dois polinômios de uma variável: usaremos os termos líderes de $g_1, \ldots, g_t$ para eliminar o termo líder de f e os termos líderes dos polinômios subsequentes que aparecem nas etapas intermediárias da divisão. A novidade aqui é que às vezes alguns dos termos líderes de alguns polinômios de algumas das etapas intermediárias não são múltiplos de nenhum $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t)$ e então devemos movê-los para o resto da divisão para continuar com a divisão.

Exemplo 3.1.10. *Consideremos o anel de polinômios $\mathbb{R}[X, Y]$ munido da ordem lexicográfica, onde $Y \preceq X$. Vamos dividir $f = X^2Y + XY^2 + Y^2$ por $\{g_1 = XY - 1,\ g_2 = Y^2 - 1\} \subset \mathbb{R}[X, Y]$. Como $\mathrm{LM}(f) = X^2Y$ é múltiplo de $\mathrm{LM}(g_1) = XY$, com $\mathrm{LM}(f) = X \cdot \mathrm{LM}(g_1)$, então começamos a divisão escrevendo*

$$f = X \cdot g_1 + X + XY^2 + Y^2.$$

Observe que $\mathrm{LM}(X + XY^2 + Y^2) = XY^2$ é múltiplo de $\mathrm{LM}(g_1)$, com $XY^2 = Y \cdot \mathrm{LM}(g_1)$, então escrevemos

$$f = X \cdot g_1 + Y \cdot g_1 + X + Y + Y^2 = (X + Y) \cdot g_1 + X + Y + Y^2.$$

Como $\mathrm{LM}(X + Y + Y^2) = X$ não é múltiplo de $\mathrm{LM}(g_1)$ ou $\mathrm{LM}(g_2) = Y^2$, então devemos considerá-lo como uma parte do resto. Logo,

$$f = X \cdot g_1 + Y \cdot g_1 + X + Y + Y^2 = (X + Y) \cdot g_1 + Y + Y^2 + r_1,$$

onde $r_1 = X$. Como $\mathrm{LM}(Y + Y^2) = Y^2$ não é múltiplo de $\mathrm{LM}(g_1)$, mas é múltiplo de $\mathrm{LM}(g_2)$, e de $Y^2 = 1 \cdot \mathrm{LM}(g_2)$ escrevemos

$$f = (X + Y) \cdot g_1 + 1 \cdot g_2 + Y + 1 + r_1.$$

Para finalizar, como os termos de $Y + 1$ não são múltiplos de $\mathrm{LM}(g_1)$ e $\mathrm{LM}(g_2)$, então consideramos esses termos como a parte final do resto e então

$$f = (X + Y) \cdot g_1 + 1 \cdot g_2 + r_1 + r_2,$$

com $r_2 = Y + 1$. Portanto, $f = q_1g_1 + q_2g_2 + r$, onde $q_1 = X + Y, q_2 = 1$ e $r = X + Y + 1$.

A figura abaixo ilustra como foi feita a divisão.

$X^2Y + XY^2 + Y^2$	$XY - 1, Y^2 - 1$	*Resto*
$\underline{-X^2Y + X}$	$X + Y, \quad 1$	$X + Y + 1$
$XY^2 + X + Y^2$		
$\underline{-XY^2 + Y}$		
$X + Y^2 + Y$		
$\underline{-X}$		
$Y^2 + Y$		
$\underline{-Y^2 + 1}$		
$Y + 1$		
$\underline{-Y - 1}$		
0		

Analisando atentamente o que foi feito acima, observamos que estamos levando em consideração a ordem em que os divisores $g_1, \ldots, g_t$ são escritos (ou seja, dividimos f pela sequência (g_1, g_2)). Se invertermos a ordem dos divisores isso vai alterar o quociente e o resto, conforme mostra o cálculo a seguir.

$$\begin{array}{r|l|l}
X^2Y + XY^2 + Y^2 & Y^2 - 1, XY - 1 & \textit{Resto} \\
\hline
\underline{-X^2Y + X} & X + 1, \qquad X & 2X + 1 \\
XY^2 + X + Y^2 & & \\
\underline{-XY^2 + X} & & \\
2X + Y^2 & & \\
\underline{-2X} & & \\
Y^2 & & \\
\underline{-Y^2 + 1} & & \\
1 & & \\
\underline{-1} & & \\
0 & &
\end{array}$$

3.2 Base de Gröbner

Nesta seção vamos apresentar elementos da teoria de bases de Gröbner, uma importante ferramenta no estudo de Álgebra Comutativa. A teoria das bases de Gröbner para anéis de polinômios foi desenvolvida por Bruno Buchberger (Áustria, 1942-) em 1965 (veja [1]), e foi assim denominada em homenagem ao seu orientador Wolfgang Gröbner (Áustria, 1899-1980).

Definição 3.2.1 (Base de Gröbner)**.** *Sejam $I \subset \mathbb{K}[\mathbf{X}]$ um ideal não nulo e $\preceq$ uma ordem monomial em $\mathcal{M}$. Dizemos que um conjunto de polinômios não nulos $\{g_1, \ldots, g_s\} \subset I$ é uma* ***base de Gröbner*** *para I (com respeito a $\preceq$) se para todo $f \in I$, com $f \neq 0$ temos que $\mathrm{LM}(f)$ é múltiplo de $\mathrm{LM}(g_i)$ para algum $i = 1, \ldots, s$.*

Exemplo 3.2.2. *Seja $I = (XY-1, Y^2-1) \subset \mathbb{R}[X, Y]$ e considere $\mathcal{M}$ com a ordem lexicográfica (com $Y \preceq X$). Então, o conjunto $\{XY - 1, Y^2 - 1\}$ não é uma base de Gröbner para I.*
Com efeito, note que $Y(XY - 1) - X(Y^2 - 1) = -Y + X \in I$ e $\mathrm{LM}(X - Y) = X$, e X não é múltiplo de $\mathrm{LM}(XY - 1) = XY$ ou de $\mathrm{LM}(Y^2 - 1) = Y^2$, então $\{XY - 1, Y^2 - 1\}$ não é uma base de Gröbner para I.

Doravante, sempre assumiremos que $\mathcal{M}$ está munido de uma ordem mononial fixa e que $I \neq (0)$. Na teoria das bases de Gröbner é sempre necessário escolher uma ordem monomial em $\mathbb{K}[\mathbf{X}]$. O próximo resultado nos diz que uma base de Gröbner é de fato uma base para I, no sentido de ser um conjunto de geradores, e ainda nos permite decidir se um polinômio não nulo f pertence ou não a I.

Lema 3.2.3. *Seja $\{g_1, \ldots, g_s\} \subset I$ uma base de Gröbner para I. Então, $f \in I$ se, e somente se, o resto da divisão de f por $\{g_1, \ldots, g_s\}$ é zero. Como consequência, $I = (g_1, \ldots, g_s)$.*

Demonstração. $\boxed{\Leftarrow}$ Suponha que o resto da divisão de f por $\{g_1, \ldots, g_s\}$ é zero. Logo, escrevemos

$$f = q_1 g_1 + \cdots + q_s g_s,$$

onde $q_1, \ldots, q_s \in \mathbb{K}[\mathbf{X}]$. Como $g_i \in I$, para todo $i = 1, \ldots, s$ temos que $f \in I$.

$\boxed{\Rightarrow}$ Dividindo f por $\{g_1, \ldots, g_s\}$, existem $q_1, \ldots, q_s, r \in \mathbb{K}[\mathbf{X}]$ tais que

$$f = q_1 g_1 + \cdots + q_s g_s + r,$$

onde $r = 0$ ou nenhum monômio em r é múltiplo de $\mathrm{LM}(g_i)$, para todo $i = 1, \ldots, s$. Então,

$$r = f - \sum_{i=1}^{s} q_i g_i \in I.$$

Portanto, $r = 0$, pois, caso contrário r seria um polinômio não nulo em I cujo monômio líder não é 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 para I. Como consequência $I \subset (g_1, \ldots, g_s)$ e a fortiori $I = (g_1, \ldots, g_s)$. □

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

Proposição 3.2.4. *Seja $\{g_1, \ldots, g_s\} \subset I$ uma base de Gröbner para I. Na divisão de $f \in \mathbb{K}[\mathbf{X}]$ por $\{g_1, \ldots, g_s\}$ o resto é sempre o mesmo, independentemente da ordem que escolhermos para $g_1, \ldots, g_s$ no algoritmo da divisão.*

Demonstração. Suponhamos que f seja escrito da forma

$$f = q_1 g_1 + \cdots + q_s g_s + r = \tilde{q}_1 g_1 + \cdots + \tilde{q}_s g_s + \tilde{r},$$

onde $q_i, \tilde{q}_i \in \mathbb{K}[\mathbf{X}]$, para todo $i = 1, \ldots, s$ e $r, \tilde{r} \in \mathbb{K}[\mathbf{X}]$ com nenhum monômio aparecendo em r ou em $\tilde{r}$ sendo múltiplo de $\mathrm{LM}(g_i)$, para todo $i = 1, \ldots, s$. Como

$$r - \tilde{r} = \sum_{i=1}^{s} (\tilde{q}_i - q_i) g_i \in I,$$

devemos ter $r - \tilde{r} = 0$, pois, caso contrário, $r - \tilde{r}$ seria um polinômio não nulo em I cujo monômio líder não é múltiplo de $\mathrm{LM}(g_i)$, para todo $i = 1, \ldots, s$, contradizendo o fato que $\{g_1, \ldots, g_s\}$ é uma base de Gröbner para I. □

Definição 3.2.5 (S-polinômio)**.** *Sejam $f, g \in \mathbb{K}[\mathbf{X}] \setminus \{0\}$, com $\mathrm{LT}(f) = a\mathbf{X}^{\boldsymbol{\alpha}}$ e $\mathrm{LT}(g) = b\mathbf{X}^{\boldsymbol{\beta}}$. Seja $\gamma_i = \max\{\alpha_i, \beta_i\}$, para todo $i = 1, \ldots, m$ e considere $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_m) \in \mathbb{N}_0^m$. O **S-polinômio** de f e g é definido como*

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

É fácil ver que $\mathrm{LT}(\frac{1}{a}\mathbf{X}^{\boldsymbol{\gamma}-\boldsymbol{\alpha}} f) = \mathbf{X}^{\boldsymbol{\gamma}} = \mathrm{LT}(\frac{1}{b}\mathbf{X}^{\boldsymbol{\gamma}-\boldsymbol{\beta}} g)$.

Exemplo 3.2.6. *Sejam $f = 2XY - Y$ e $g = -X + 3Y^2$ polinômios em $\mathbb{R}[X, Y]$ e considere $\mathcal{M}$ munido da ordem lexicográfica com $Y \preceq X$. Observe que $\mathrm{LT}(f) = 2XY$, $\mathrm{LT}(g) = -X$ e $\boldsymbol{\gamma} = (1, 1)$.*

Portanto, o S-polinômio de f e g é

$$\begin{aligned} S(f, g) &= f + 2Yg \\ &= (2XY - Y) + (-2XY + 6Y^3) \\ &= 6Y^3 - Y. \end{aligned}$$

Teorema 3.2.7 (Critério de Buchberger)**.** *Seja $\{g_1, \ldots, g_t\} \subset I$ tal que $I = (g_1, \ldots, g_t)$. Então, $\{g_1, \ldots, g_t\}$ é uma base de Gröbner para I se, e somente se, para todos $i, j = 1, \ldots, t$, com $i \neq j$, o resto da divisão de $S(g_i, g_j)$ por $\{g_1, \ldots, g_t\}$ é zero, independentemente da ordem que tomarmos para $g_1, \ldots, g_t$ no algoritmo da divisão.*

Demonstração. Veja ([3], página 86, Teorema 6). □

Teorema 3.2.8 (Algoritmo de Buchberger)**.** *Seja $I = (g_1, \ldots, g_t)$ um ideal não nulo. Uma base de Gröbner para I pode ser construída em um número finito de passos seguindo o algoritmo:*

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

Início
  $G = \{g_1, \ldots, g_t\}$;
  $G' = \{\{g_i, g_j\} \mid g_i \neq g_j \text{ e } g_i, g_j \in G\}$;
  Enquanto $G' \neq \emptyset$ **faça**
    Escolha $\{g_i, g_j\} \in G'$;
    $G' = G' \setminus \{\{g_i, g_j\}\}$;
    Dividir $S(g_i, g_j)$ *por* G *obtendo resto* r;
    Se $r \neq 0$ **então**
      $G' = G' \cup \{\{g, r\} \mid g \in G\}$;
      $G = G \cup \{r\}$;
    Fim
  Fim
Fim

Demonstração. Veja ([3], página 91, Teorema 2). □

Exemplo 3.2.9. *No exemplo 3.2.2, vimos que $G := \{XY - 1, Y^2 - 1\}$ não é uma base de Gröbner para $I = (XY - 1, Y^2 - 1)$. Vamos usar o algoritmo de Buchberger com o objetivo de produzir uma base de Gröbner para I. Denote por $g_1 = XY - 1$ e $g_2 = Y^2 - 1$. Então, $S(g_1, g_2) = Yg_1 - Xg_2 = X - Y$ e o resto da divisão de $S(g_1, g_2)$ por $\{g_1, g_2\}$ é o próprio $X - Y$. Defina $g_3 := X - Y$ e considere o conjunto $\{XY - 1, Y^2 - 1, X - Y\}$. Agora, é claro que o resto da divisão de $S(g_1, g_2)$ por $\{g_1, g_2, g_3\}$ é zero. Além disso, é fácil ver que o resto da divisão de $S(g_1, g_3)$ e $S(g_2, g_3)$ por $\{g_1, g_2, g_3\}$ é zero. Portanto, $\{XY - 1, Y^2 - 1, X - Y\}$ é uma base de Gröbner para I.*

O problema de tese de Buchberger era: dado um ideal $I \subset \mathbb{K}[\mathbf{X}]$ determinar uma base para $\mathbb{K}[\mathbf{X}]/I$, considerando esse quociente como um $\mathbb{K}$-espaço vetorial. Agora, introduziremos o conceito que solucionou o problema da tese de Buchberger.

3.3 Pegada de um Ideal

Definição 3.3.1 (Pegada)**.** *Seja $I \subset \mathbb{K}[\mathbf{X}]$ um ideal e uma ordem monomial fixada $\preceq$ em $\mathcal{M}$. A **pegada** de um ideal I com respeito a $\preceq$ é o conjunto*

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

Proposição 3.3.2. *Sejam $I \subset \mathbb{K}[\mathbf{X}]$ um ideal e $\{g_1, \ldots, g_s\}$ uma base de Gröbner para I. Então $M \in \Delta(I)$ se, e somente se, M não é múltiplo de $\mathrm{LM}(g_i)$, para todo $i = 1, \ldots, s$.*

Demonstração. $\boxed{\Rightarrow}$ Seja $M \in \Delta(I)$. Suponha, por contradição, que M é múltiplo de $\mathrm{LM}(g_i)$ para algum $i = 1, \ldots, s$. Logo, $M = N \cdot \mathrm{LM}(g_i)$. Assim, como $g_i \in I$ e I é um ideal, então $f = N \cdot g_i \in I$ e temos

$$\mathrm{LM}(f) = N \cdot \mathrm{LM}(g_i) = M,$$

o que é um absurdo, pois $M \in \Delta(I)$.
$\boxed{\Leftarrow}$ Se M não é múltiplo de $\mathrm{LM}(g_i)$, para todo $i = 1, \ldots, s$ e se $\{g_1, \ldots, g_s\}$ é uma base de Gröbner para I, então M não é o monômio líder de nenhum polinômio em I. Logo, $M \in \Delta(I)$. □

Exemplo 3.3.3. *Seja $I = (X^3 - X, Y^3 - Y, X^2Y - Y) \subset \mathbb{R}[X, Y]$ e considere $\mathcal{M}$ munido da ordem lexicográfica $(Y \preceq X)$. Não é difícil verificar que $\{X^3 - X, Y^3 - Y, X^2Y - Y\}$ é uma base de Gröbner para $I = (X^3 - X, Y^3 - Y, X^3Y - Y)$.*
Agora, pela Proposição 3.3.2, temos que os elementos que pertencem a $\Delta(I)$ são os monômios que não são múltiplos de $\mathrm{LM}(X^3 - X) = X^3, \mathrm{LM}(Y^3 - Y) = Y^3$ ou $\mathrm{LM}(X^2Y - Y) = X^2Y$. Podemos identificar um monômio $X^\alpha Y^\beta$ como o par ordenado (α, β) de inteiros não negativos.

Os pontos $(3, 0), (0, 3)$ e $(2, 1)$ correspondem, respectivamente, aos monômios líderes dos polinômios $X^3 - X$, $Y^3 - Y$ e $X^2Y - Y$, pertencentes à base de Gröbner de I. Logo, a partir deles é fácil determinar os monômios que não são múltiplos de nenhum desses monômios líderes. Portanto, pela Proposição 3.3.2, temos que

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

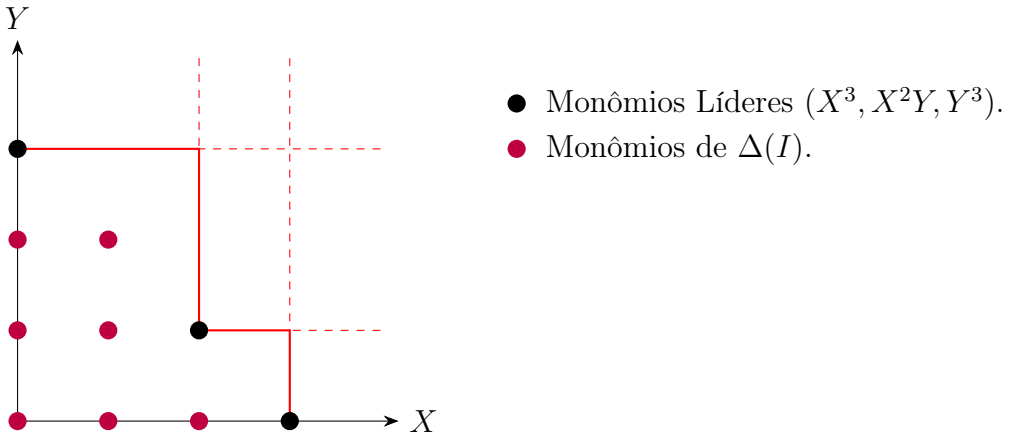


Figura 3.1: Representação da pegada do ideal $I = (X^3 - X, Y^3 - Y, X^2Y - Y)$.

Teorema 3.3.4. *Seja $I \subset \mathbb{K}[\mathbf{X}]$ um ideal. Então uma base para $\mathbb{K}[\mathbf{X}]/I$ como $\mathbb{K}$-espaço vetorial, é*

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

Em particular, se $\Delta(I)$ é um conjunto finito, então $\dim_{\mathbb{K}}(\mathbb{K}[\mathbf{X}]/I) = \#(\Delta(I))$.

Demonstração. Seja G uma base de Gröbner para I em relação à mesma ordem de monômios usada para determinar $\Delta(I)$, e seja $f \in \mathbb{K}[\mathbf{X}]$. Dividindo f por G, existem $u_1, \ldots, u_s \in \mathbb{K}[\mathbf{X}]$ e $r \in \mathbb{K}[\mathbf{X}]$ tais que $f = u_1g_1 + \cdots + u_sg_s + r$, e se $r \neq 0$ então nenhum monômio que aparece em r é múltiplo de $\mathrm{LM}(g_i)$, para todo $i = 1, \ldots, s$. Em outras palavras, r é uma combinação linear, com coeficientes em $\mathbb{K}$, de monômios de $\Delta(I)$, isto é, $r = \sum_{i=1}^{s} a_iM_i$. Como $f + I = r + I = \sum_{i=1}^{s} a_i(M_i + I)$, temos que os elementos de B geram $\mathbb{K}[\mathbf{X}]/I$ como $\mathbb{K}$-espaço vetorial.

Agora, suponha que $\sum_{i=1}^{\ell} b_i(M_i+I) = 0+I$, onde $b_i \in \mathbb{K}$ e $M_i \in \Delta(I)$ para todo $i = 1, \ldots, \ell$. Então, $\sum_{i=1}^{\ell} b_i M_i \in I$. Se algum dos coeficientes b_i for diferente de zero, então $\sum_{i=1}^{\ell} b_i M_i$ seria um elemento não nulo de I cujo monômio líder não é o monômio líder de algum polinômio em I, logo, devemos ter $b_1 = b_2 = \cdots = b_\ell = 0$, o que prova que B é linearmente independente sobre $\mathbb{K}$. □

Exemplo 3.3.5. *Vimos no Exemplo 3.3.3 que,* $\Delta(I) = \{1, X, X^2, Y, XY, Y^2, XY^2\}$, *onde* $I = (X^3 - X, Y^3 - Y, X^2Y - Y) \subset \mathbb{R}[X, Y]$. *Agora, pelo Teorema anterior, temos que* $\mathbb{R}[X, Y]/I$ *é um* $\mathbb{R}$*-espaço vetorial de dimensão* 7, *onde*

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

é uma base para esse espaço vetorial.

Seja $I \subset \mathbb{K}[\mathbf{X}]$ um ideal e $\{f_1, \ldots, f_t\}$ uma base para I. Defina o conjunto

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

Observação 3.3.6. *Seja* $I \subset \mathbb{K}[\mathbf{X}]$, *então* $\Delta(I) \subseteq \Delta(\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_t))$. *Com efeito, se* $M \in \Delta(I)$, *então, por definição,* M *não é o monômio líder de nenhum polinômio em* I *e como* $f_i \in I$, *para todo* $i = 1, \ldots, t$, *em particular,* M *não é múltiplo do monômio líder de* f_i. *Portanto,* $M \in \Delta(\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_t))$.

Na verdade, segundo a Proposição 3.3.2 temos

$$\Delta(I) = \Delta(\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_t)) \text{ se, e somente se, } \{f_1, \ldots, f_t\} \text{ é uma base de Gröbner para } I.$$

Agora, apresentaremos um conceito-chave chamado de "variedade afim". Esse conceito juntamente com o conceito de ideal de uma variedade permitem conectar a Álgebra Comutativa com a Geometria Algébrica. É usual, em Geometria Algébrica, denotar por $\mathbb{A}^m(\mathbb{K})$ o conjunto de m-uplas de $\mathbb{K}^m$, quando essas m-uplas vão ser usadas como pontos a serem substituídos em polinômios.

Definição 3.3.7 (Variedade afim)**.** *Seja* $I \subset \mathbb{K}[\mathbf{X}]$ *um ideal. A* ***variedade afim*** *associada a* I *é o conjunto dos pontos em* $\mathbb{A}^m(\mathbb{K})$ *que se anulam em todo polinômio em* I, *isto é,*

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

Proposição 3.3.8. *Se* $I = (g_1, \ldots, g_t)$ *então*

$$(a_1, \ldots, a_m) \in V(I) \iff g_i(a_1, \ldots, a_m) = 0 \quad \text{para todo } i = 1, \ldots, t.$$

Demonstração. Com efeito,

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

□

Definição 3.3.9 (Ideal de uma variedade afim)**.** *Seja* $V = V(I) \subset \mathbb{A}^m(\mathbb{K})$ *uma variedade afim. O* ***ideal de uma variedade*** V, *que denotamos por* $\mathcal{I}(V) =: \mathcal{I}(V(I))$, *é o conjunto de todos os polinômios em* $\mathbb{K}[\mathbf{X}]$ *que se anulam em todos os pontos de* $V(I)$, *isto é,*

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

Proposição 3.3.10. *$\mathcal{I}(V)$ é um ideal de $\mathbb{K}[\mathbf{X}]$.*

Demonstração. Claramente que $\mathcal{I}(V) \neq \emptyset$, pois basta tomar $f = 0$.
Sejam $f, g \in \mathcal{I}(V)$, então

$$\begin{aligned}(f+g)(a_1,\ldots,a_m) &= f(a_1,\ldots,a_m) + g(a_1,\ldots,a_m)\\ &= 0.\end{aligned}$$

Seja $f \in \mathcal{I}(V)$ e seja $h \in \mathbb{K}[\mathbf{X}]$. Então

$$\begin{aligned}(fh)(a_1,\ldots,a_m) &= f(a_1,\ldots,a_m)h(a_1,\ldots,a_m)\\ &= 0 \cdot h(a_1,\ldots,a_m) = 0.\end{aligned}$$

Isso conclui a demonstração. □

Uma variedade $V(I)$ pode ter um número infinito ou finito de pontos.

Exemplo 3.3.11. *Sejam $I = (Y - X^2)$ e $J = (X^2 - 1, Y^2 - 1)$ ideais $\mathbb{R}[X, Y]$. Observe que*

$$\begin{aligned}V(I) &= \{(a,b) \in \mathbb{A}^2(\mathbb{R}) \mid f(a,b) = 0, \text{ para todo } f \in I\}\\ &= \{(a,b) \in \mathbb{A}^2(\mathbb{R}) \mid b - a^2 = 0\}\\ &= \{(a,b) \in \mathbb{A}^2(\mathbb{R}) \mid b = a^2\}\\ &= \{(a,a^2) \mid a \in \mathbb{R}\},\end{aligned}$$

e

$$\begin{aligned}V(J) &= \{(a,b) \in \mathbb{A}^2(\mathbb{R}) \mid f(a,b) = 0, \text{ para todo } f \in J\}\\ &= \{(a,b) \in \mathbb{A}^2(\mathbb{R}) \mid a^2 - 1 = 0 \text{ e } b^2 - 1 = 0\}\\ &= \{(a,b) \in \mathbb{A}^2(\mathbb{R}) \mid a^2 = 1 \text{ e } b^2 = 1\}\\ &= \{(-1,1),(-1,-1),(1,1),(1,-1)\}\end{aligned}$$

são as variedades de I e J, respectivamente. Temos que $V(I)$ tem um número infinito de pontos, enquanto que $V(J)$ tem um número finito de pontos.

Figura 1 — Em verde a variedade afim de $I = (Y - X^2) \subseteq \mathbb{R}[X, Y]$.

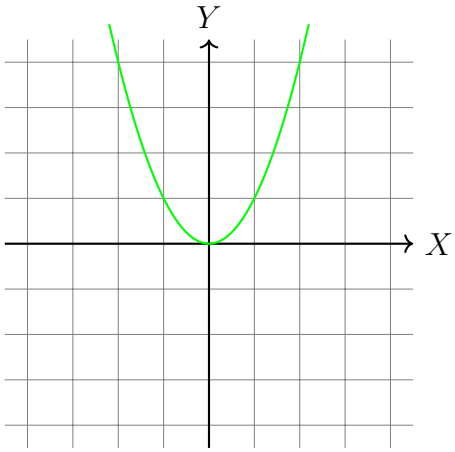
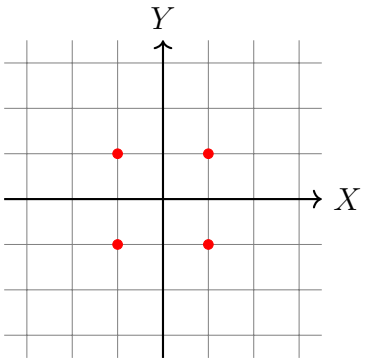


Figura 2 — Em vermelho os pontos de $V(J) = \{(-1, \pm 1), (1, \pm 1)\}$.



Lema 3.3.12. *Seja $I \subset \mathbb{K}[\mathbf{X}]$ um ideal e sejam $\mathbf{P}_1, \ldots, \mathbf{P}_r$ pontos distintos de $V(I)$. Então, existem polinômios $p_1, \ldots, p_r \in \mathbb{K}[\mathbf{X}]$, tal que $p_i(\mathbf{P}_j) = \delta_{ij}$ para todos $i, j = 1, \ldots, r$, onde δ_{ij} é o delta de Kronecker (ou seja, se $i = j$, temos que $\delta_{ij} = 1$, caso contrário $\delta_{ij} = 0$).*

Demonstração. Seja $\mathbf{P}_i = (a_{i1}, \ldots, a_{im}) \in \mathbb{A}^m(\mathbb{F}_q)$, onde $i = 1, \ldots, r$, vamos mostrar como obter p_1 conforme o enunciado do Lema. Como todos os pontos são distintos, para todo $i = 2, \ldots, r$ existe $j_i \in \{1, \ldots, m\}$, tal que $a_{ij_i} \neq a_{1j_i}$. Defina $h_i := \frac{X_{j_i} - a_{ij_i}}{a_{1j_i} - a_{ij_i}}$ para $i = 2, \ldots, r$.
Então, calculando h_i em $\mathbf{P}_i$, temos que

$$\begin{aligned} h_i(\mathbf{P}_1) &= \frac{X_{j_i}(\mathbf{P}_1) - a_{ij_i}}{a_{1j_i} - a_{ij_i}} \\ &= \frac{X_{j_i}(a_{11}, \ldots, a_{1m}) - a_{ij_i}}{a_{1j_i} - a_{ij_i}} \\ &= \frac{a_{1j_i} - a_{ij_i}}{a_{1j_i} - a_{ij_i}} \\ &= 1. \end{aligned}$$

Por outro lado, temos que $h_i(\mathbf{P}_i) = \frac{a_{ij_i} - a_{ij_i}}{a_{1j_i} - a_{ij_i}} = 0$, para todo $i = 2, \ldots, r$.

Tomando $p_1 = \prod_{i=2}^{r} h_i$, temos que $p_1(\mathbf{P}_1) = 1$ e $p_1(\mathbf{P}_i) = 0$, para todo $i = 2, \ldots, r$. Analogamente, conseguimos obter $p_2, \ldots, p_r$. □

Proposição 3.3.13. *Seja $I \subset \mathbb{K}[\mathbf{X}]$ um ideal tal que $\Delta(I)$ é um conjunto finito. Então $V(I)$ também é um conjunto finito e $\#(V(I)) \leq \#(\Delta(I))$.*

Demonstração. Sejam $\mathbf{P}_1, \ldots, \mathbf{P}_r$ pontos distintos de $V(I)$. Vamos encontrar um conjunto em $\mathbb{K}[\mathbf{X}]/I$ que é linearmente independente e tem r elementos. Isso provará a proposição, pois, no Teorema 3.3.4, vimos que $\#(\Delta(I))$ é igual a dimensão de $\mathbb{K}[\mathbf{X}]/I$ como $\mathbb{K}$-espaço vetorial.

Pelo Lema 3.3.12, existem $p_1, \ldots, p_r \in \mathbb{K}[\mathbf{X}]$ tais que $p_i(\mathbf{P}_j) = \delta_{ij}$, para todos $i, j = 1, \ldots, r$. Suponha que $\sum_{i=1}^{r} a_i(p_i + I) = 0 + I$, onde $a_1, \ldots, a_r \in \mathbb{K}$. Logo, $\sum_{i=1}^{r} a_i p_i \in I$. Então,

$$\sum_{i=1}^{r} a_i p_i(\mathbf{P}_j) = \sum_{i=1}^{r} a_i \delta_{ij} = 0.$$

Logo, $a_j = 0$, para todo $j = 1, \ldots, r$, o que demonstra que $\{p_1 + I, \ldots, p_r + I\}$ é um conjunto linearmente independente em $\mathbb{K}[\mathbf{X}]/I$. □

Na verdade, pode-se provar um resultado mais refinado. Para enunciá-lo, precisamos relembrar de duas definições básicas, a saber: radical de um ideal e ideal radical.

Definição 3.3.14 (Radical de um ideal)**.** *Definimos o* ***radical de um ideal*** *em um anel R como sendo o conjunto*

$$\sqrt{I} := \{a \in R \mid a^m \in I, \text{ para algum } m \in \mathbb{N}\}.$$

Definição 3.3.15 (Ideal radical)**.** *Dizemos que $I \subset \mathbb{K}[\mathbf{X}]$ é um* ***ideal radical*** *se $\sqrt{I} = I$.*

Teorema 3.3.16. *Seja $I \subset \mathbb{K}[\mathbf{X}]$ um ideal tal que $\Delta(I)$ é um conjunto finito e seja $\mathbb{L}$ uma extensão de $\mathbb{K}$ que é algebricamente fechada. Então*

$$V_{\mathbb{L}}(I) := \{(a_1, \ldots, a_m) \in \mathbb{L}^m \mid f(a_1, \ldots, a_m) = 0, \text{ para todo } f \in I\}$$

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

Demonstração. Veja ([1], Teorema 8.32). □

Teorema 3.3.17 (Teorema dos Zeros de Hilbert (Nullstellensatz))**.** *Seja $\mathbb{K}$ um corpo algebricamente fechado e seja $I \subseteq \mathbb{K}[\mathbf{X}]$. Então*

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

Demonstração. Veja ([3], página 183, Teorema 6). □

Doravante, sempre assumiremos que o conjunto dos monômios $\mathcal{M} \subset \mathbb{F}_q[\mathbf{X}]$ está dotado da ordem lexicográfica onde $X_m \preceq \cdots \preceq X_1$.

3.4 Códigos de variedade afim

Na presente seção faremos a construção dos códigos de variedade afim, conforme definidos em [4]. Seja $I = (g_1, \ldots, g_t) \subset \mathbb{F}_q[\mathbf{X}]$ um ideal e seja $I_q := (g_1, \ldots, g_t, X_1^q - X_1, \ldots, X_m^q - X_m)$. Pela Proposição 1.2.3, temos que $\prod_{a \in \mathbb{F}_q}(X - a) = X^q - X$ e, assim segue trivialmente $V(I) = V(I_q)$.

Agora, pela Observação 3.3.6

$$\#(\Delta(I_q)) \leq \#(\Delta(\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t), X_1^q, \ldots, X_m^q)) \leq q^m.$$

Logo, pela Proposição 3.3.13 temos que $\#(V(I_q)) \leq \#(\Delta(I_q))$, ou seja, o número de zeros comuns em I_q é finito, digamos, $V(I_q) = \{\mathbf{P}_1, \ldots, \mathbf{P}_n\}$. Defina a função ev dada por

$$\begin{array}{rccc} \mathrm{ev}: & \mathbb{F}_q[\mathbf{X}]/I_q & \to & \mathbb{F}_q^n \\ & f + I_q & \mapsto & \mathrm{ev}(f + I_q) = (f(\mathbf{P}_1), \ldots, f(\mathbf{P}_n)). \end{array} \tag{3.1}$$

Proposição 3.4.1. *A função* ev *é um isomorfismo entre $\mathbb{F}_q$-espaços vetoriais.*

Demonstração. Claramente a função ev está bem definida e é uma transformação linear. Agora, $X_i^q - X_i \in I_q$, para todo $i = 1, \ldots, m$ e, portanto, I_q é um ideal radical (veja e. g. [1], 1993, Prop. 8.14). Se $\mathbb{L}$ é um corpo algebricamente fechado contendo $\mathbb{F}_q$, temos que $V_{\mathbb{L}}(I_q) = V_{\mathbb{F}_q}(I_q)$, e pelo Teorema 3.3.16 temos que $\#(V_{\mathbb{L}}(I_q)) = \#(\Delta(I_q))$. Agora, pelo Teorema de Buchberger, temos que $\dim(\mathbb{F}_q[\mathbf{X}]/I_q) = \#(\Delta(I_q)) = n$.

Agora, provaremos que ev é sobrejetora e, assim, aplicando o Teorema do Núcleo e da Imagem o resultado estará provado. Pelo Lema 3.3.12, existem polinômios $p_1, \ldots, p_n \in \mathbb{F}_q[\mathbf{X}]$ tais que $p_i(P_j) = \delta_{ij}$, para todos os $i, j = 1, \ldots, n$. Logo, $\mathrm{ev}(p_i + I_q) = \mathbf{e}_i$, onde $\mathbf{e}_i$ é o i-ésimo vetor da base canônica de $\mathbb{F}_q^n$, para todo $i = 1, \ldots, n$. □

Definição 3.4.2 (Código de variedade afim)**.** *Seja L um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q[\mathbf{X}]/I_q$, a imagem $C(L) := \mathrm{ev}(L)$ é um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q^n$, que é chamado de* ***código de variedade afim*** *associado a L.*

Capítulo 4

Códigos hiperbólicos

Neste capítulo apresentamos uma família de códigos de variedade afim chamados de **códigos hiperbólicos**. Nosso objetivo principal é determinar seus parâmetros fundamentais usando a teoria das bases de Gröbner e obter uma caracterização dos pesos generalizados de Hamming desses códigos a partir das noções de conjuntos densos e ótimos. Usamos como referência principal [5].

4.1 Introdução

Seguindo o que foi feito na seção 3.4 tomamos $I = I_q = (X_1^q - X_1, \ldots, X_m^q - X_m)$. Nesse caso $V(I) = \mathbb{A}^m(\mathbb{F}_q)$, e escrevemos $\mathcal{X} := \mathbb{A}^m(\mathbb{F}_q)$. Vamos escrever $n := |\mathcal{X}| = q^m$. Lembramos que $\mathcal{M}$ denota o conjunto dos monômios de $\mathbb{F}_q[\mathbf{X}]$, e que dados $M_1, \ldots, M_u \in \mathcal{M}$ temos que $\Delta(M_1, \ldots, M_u)$ é o conjunto dos monômios em $\mathcal{M}$ que <u>não</u> são múltiplos de M_i para todo $i = 1, \ldots, u$.

Definição 4.1.1 (Código hiperbólico)**.** *Seja $s \geq 0$ um inteiro e defina a função*

$$\begin{array}{rccc} D: & \mathcal{M} & \to & \mathbb{N}_0 \\ & M & \mapsto & D(M) = \#(\Delta(M, X_1^q, \ldots, X_m^q)). \end{array}$$

*O **código hiperbólico** $E(s)$ é definido como o subespaço gerado por* $\mathrm{ev}(M + I_q)$*, onde* ev *é a aplicação definida em* (3.1) *e M é tal que $D(M) \leq s$, isto é,*

$$E(s) := \langle \{\mathrm{ev}(M + I_q) \mid M \in \mathcal{M},\ D(M) \leq s\} \rangle.$$

É óbvio que $E(s)$ é um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q^n$, ou seja, $E(s)$ é um código de $\mathbb{F}_q^n$.

Em [5] os autores, na definição de código hiperbólico e em diversos outros lugares, escrevem $\Delta((M, X_1^q, \ldots, X_m^q))$ ao invés de $\Delta(M, X_1^q, \ldots, X_m^q)$, ou seja, consideram a pegada do ideal $(M, X_1^q, \ldots, X_m^q)$. Ocorre que $\Delta((M, X_1^q, \ldots, X_m^q)) = \Delta(M, X_1^q, \ldots, X_m^q)$, porque um conjunto de geradores formado por monômios é uma base de Gröbner para o ideal definido por ele (porque o S-polinômio de um par de monômios é zero) e devido também à Proposição 3.3.2.

Observação 4.1.2. *Da definição da aplicação D vem que para todo $M \notin \Delta(I)$ temos*

$$\Delta(M, X_1^q, \ldots, X_m^q) = \Delta(I)$$

logo $\#(\Delta(M, X_1^q, \ldots, X_m^q)) = q^m$. Além disso, se $M \in \Delta(I)$ então $\#(\Delta(M, X_1^q, \ldots, X_m^q)) < q^m$. Assim, para $s \geq q^m$ temos que $E(s)$ é gerado pelas classes de todos os monômios em $\Delta(I)$. Logo, devido ao Teorema 3.3.4 e ao fato de ev *ser um isomorfismo, temos que $E(s) = \mathbb{F}_q^n$. Assim, para evitar trivialidades, redefinimos $E(s)$ como*

$$E(s) := \langle \{\mathrm{ev}(M + I_q) \mid M \in \Delta(I),\ D(M) \leq s\} \rangle.$$

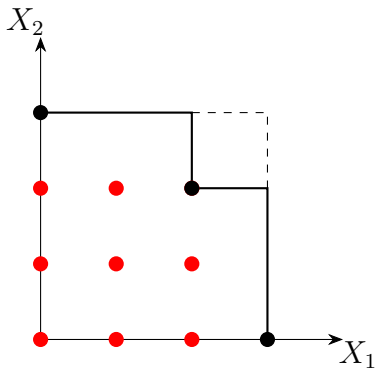
A seguir, apresentamos uma fórmula para o número $\#(\Delta(M, X_1^q, \ldots, X_m^q))$, com $M \in \Delta(I)$. Para tornar a ideia clara, analisamos primeiro um exemplo no caso $m = 2$. Depois generalizamos o argumento para $m \geq 2$.

Exemplo 4.1.3. *Tomamos $m = 2$ e $M = X_1^{\alpha_1} X_2^{\alpha_2} \in \Delta(I)$. Observe que o número de monômios que não são múltiplos de nenhum dos monômios M, X_1^q, X_2^q é dado por*

$$\#(\Delta(M, X_1^q, X_2^q)) = q^2 - \#\{X_1^{a_1} X_2^{a_2} \in \Delta(I) \mid a_1 \geq \alpha_1 \ e \ \ a_2 \geq \alpha_2\}.$$

Mas, $\#\{X_1^{a_1} X_2^{a_2} \in \Delta(I) \mid a_1 \geq \alpha_1 \ e \ \ a_2 \geq \alpha_2\} = (q - \alpha_1)(q - \alpha_2)$. Logo,

$$\#(\Delta(M, X_1^q, X_2^q)) = q^2 - (q - \alpha_1)(q - \alpha_2).$$



De maneira geral, temos o seguinte resultado.

Proposição 4.1.4. *Dado $m \geq 2$ e $M = X_1^{\alpha_1} \cdots X_m^{\alpha_m} \in \Delta(I)$ temos que*

$$D(M) = q^m - (q - \alpha_1) \cdots (q - \alpha_m).$$

Demonstração. Existem q^m monômios $X_1^{\beta_1} \cdots X_m^{\beta_m}$, com $0 \leq \beta_i \leq q - 1$ que não são múltiplos de X_i^q, para todo $i = 1, \ldots, m$. Desses, exatamente $(q - \alpha_1) \cdots (q - \alpha_m)$ são múltiplos de M e, portanto,

$$D(M) = q^m - (q - \alpha_1) \cdots (q - \alpha_m).$$

□

Exemplo 4.1.5. *Considerando o anel $\mathbb{F}_3[X_1, X_2, X_3]$ e $I = (X_1^3 - X_1, X_2^3 - X_2, X_3^3 - X_3)$, vamos construir o código hiperbólico $E(19)$. Por definição, é necessário analisar os monômios $M = X_1^{\alpha_1} X_2^{\alpha_2} X_3^{\alpha_3} \in \Delta(I)$ com $\alpha_i = 0, 1, 2$, para todo $i = 1, 2, 3$, tais que $D(M) \leq 19$. Para isso, escrevemos os resultados de $D(M)$ como entradas de matrizes A_k, onde cada termo (i, j) da matriz A_k é dado por $D(X_1^{i-1} X_2^{j-1} X_3^{k-1})$, para todo $k = 1, 2, 3$.*

Cálculos para a obtenção da matriz A_1.

Valor	*Cálculo*	*Resultado obtido*
$D(1)$	$3^3 - (3-0)(3-0)(3-0)$	0
$D(X_2)$	$3^3 - (3-0)(3-1)(3-0)$	9
$D(X_2^2)$	$3^3 - (3-0)(3-2)(3-0)$	18
$D(X_1)$	$3^3 - (3-1)(3-0)(3-0)$	9
$D(X_1X_2)$	$3^3 - (3-1)(3-1)(3-0)$	15
$D(X_1X_2^2)$	$3^3 - (3-1)(3-2)(3-0)$	21
$D(X_1^2)$	$3^3 - (3-2)(3-0)(3-0)$	18
$D(X_1^2X_2)$	$3^3 - (3-2)(3-1)(3-0)$	21
$D(X_1^2X_2^2)$	$3^3 - (3-2)(3-2)(3-0)$	24

Cálculos para a obtenção da matriz A_2.

Valor	*Cálculo*	*Resultado obtido*
$D(X_3)$	$3^3-(3-0)(3-0)(3-1)$	9
$D(X_2X_3)$	$3^3-(3-0)(3-1)(3-1)$	15
$D(X_2^2X_3)$	$3^3-(3-0)(3-2)(3-1)$	21
$D(X_1X_3)$	$3^3-(3-1)(3-0)(3-1)$	15
$D(X_1X_2X_3)$	$3^3-(3-1)(3-1)(3-1)$	19
$D(X_1X_2^2X_3)$	$3^3-(3-1)(3-2)(3-1)$	23
$D(X_1^2X_3)$	$3^3-(3-2)(3-0)(3-1)$	21
$D(X_1^2X_2X_3)$	$3^3-(3-2)(3-1)(3-1)$	23
$D(X_1^2X_2^2X_3)$	$3^3-(3-2)(3-2)(3-1)$	25

Cálculos para a obtenção da matriz A_3.

Valor	*Cálculo*	*Resultado obtido*
$D(X_3^2)$	$3^3-(3-0)(3-0)(3-2)$	18
$D(X_2X_3^2)$	$3^3-(3-0)(3-1)(3-2)$	21
$D(X_2^2X_3^2)$	$3^3-(3-0)(3-2)(3-2)$	24
$D(X_1X_3^2)$	$3^3-(3-1)(3-0)(3-2)$	21
$D(X_1X_2X_3^2)$	$3^3-(3-1)(3-1)(3-2)$	23
$D(X_1X_2^2X_3^2)$	$3^3-(3-1)(3-2)(3-2)$	25
$D(X_1^2X_3^2)$	$3^3-(3-2)(3-0)(3-2)$	24
$D(X_1^2X_2X_3^2)$	$3^3-(3-2)(3-1)(3-2)$	25
$D(X_1^2X_2^2X_3^2)$	$3^3-(3-2)(3-2)(3-2)$	26

Temos então

$$A_1=\begin{pmatrix}\boxed{0} & \boxed{9} & \boxed{18}\\ \boxed{9} & \boxed{15} & 21\\ \boxed{18} & 21 & 24\end{pmatrix},\ A_2=\begin{pmatrix}\boxed{9} & \boxed{15} & 21\\ \boxed{15} & \boxed{19} & 23\\ 21 & 23 & 25\end{pmatrix}\ \ e\ \ A_3=\begin{pmatrix}\boxed{18} & 21 & 24\\ 21 & 23 & 25\\ 24 & 25 & 26\end{pmatrix}.$$

Assim

$$\begin{aligned}E(19)&=\langle\{\mathrm{ev}(M+I)\mid M\in\Delta(I),\,D(M)\le 19\}\rangle\\&=\mathrm{ev}(\langle\{1+I,X_1+I,X_1^2+I,X_2+I,X_1X_2+I,\\&\qquad X_2^2+I,X_3+I,X_1X_3+I,X_2X_3+I,X_1X_2X_3+I,X_3^2+I\}\rangle).\end{aligned}$$

Portanto, a dimensão de $E(19)$ é $k=11$ e o seu comprimento é igual a $n=3^3=27$.

Definição 4.1.6. *Vamos denotar por $\mathcal{M}(q,s)$ o conjunto $\{M\in\Delta(I)\mid D(M)\le s\}$.*

Proposição 4.1.7. *A dimensão de $E(s)$ é igual a $k=\#(\mathcal{M}(q,s))$.*

Demonstração. O resultado segue diretamente do fato de que o mapa de avaliação ev é um isomorfismo. □

Na próxima proposição, determinamos o comprimento e uma cota inferior para a distância mínima do código hiperbólico.

Proposição 4.1.8. *O comprimento do código $E(s)$ é q^m e a sua distância mínima satisfaz $d_{\min}\ge q^m-s$.*

Demonstração. Claramente o comprimento é q^m. Seja $\mathrm{ev}(\sum_{i=1}^{t}\gamma_i M_i + I)$, uma palavra não nula de $E(s)$, com $\gamma_i \in \mathbb{F}_q$ e $M_i \in \mathcal{M}(q,s)$, para todo $i = 1,\ldots,t$. Suponha, sem perda de generalidade que $M_j \preceq M_t$, para todo $j = 1,\ldots,t-1$ e que $\gamma_t \neq 0$.
Considere o ideal

$$J := (\sum_{i=1}^{t}\gamma_i M_i, X_1^q - X_1, \ldots, X_m^q - X_m).$$

Temos que

$$\omega(\mathrm{ev}(\sum_{i=1}^{t}\gamma_i M_i + I)) = n - \#(V(J)) = q^m - \#(V(J)).$$

Pela Observação 3.3.6, tem-se $\Delta(J) \subseteq \Delta(M_t, X_1^q, \ldots, X_m^q)$, e em particular

$$\#(\Delta(\sum_{i=1}^{t}\gamma_i M_i, X_1^q - X_1, \ldots, X_m^q - X_m)) \leq s.$$

Pela Proposição 3.3.13, temos que $\#(V(J)) \leq \#(\Delta(J)) \leq s$. Logo $\omega(\mathrm{ev}(\sum_{i=1}^{t}\gamma_i M_i + I)) \geq q^m - s$, e assim $d_{\min} \geq q^m - s$. □

Na verdade, como veremos a seguir, se s for escolhido de maneira adequada temos a igualdade satisfeita.

Definição 4.1.9. *Defina* $S := \{D(M) \mid M \in \Delta(I)\}$.

Teorema 4.1.10. *Se* $s' \in \mathbb{N}_0$ *então existe um único* $s \in S$ *tal que* $E(s') = E(s)$. *A distância mínima de* $E(s)$ *é igual a* $d_{\min} = q^m - s$.

Demonstração. **Existência:** Seja $s' \in \mathbb{N}_0$ e defina

$$s := \max\{t \in S \mid t \leq s'\} \in S.$$

Tal s existe, pois S é finito e não vazio (pois $D(1) = 0 \in S$). Afirmamos que $\mathcal{M}(q,s') = \mathcal{M}(q,s)$.

Com efeito, se $M \in \mathcal{M}(q,s')$, então por definição $D(M) \leq s'$. Como $D(M) \in S$ e $s = \max\{t \in S \mid t \leq s'\}$ então $D(M) \leq s$. Logo, $M \in \mathcal{M}(q,s)$. Por outro lado, se $M \in \mathcal{M}(q,s)$, então $D(M) \leq s$. Como $s \leq s'$, segue que $D(M) \leq s'$, logo $M \in \mathcal{M}(q,s')$. Portanto, $\mathcal{M}(q,s') = \mathcal{M}(q,s)$ e, consequentemente, $E(s') = E(s)$.

Unicidade: Suponha que existam $s_1, s_2 \in S$, com $s_1 < s_2$ tais que $E(s_1) = E(s_2)$. Como $s_2 \in S$, existe um monômio $M \in \Delta(I)$ tal que $D(M) = s_2$. Como $s_1 < s_2$ temos $\mathcal{M}(q,s_1) \subsetneqq \mathcal{M}(q,s_2)$ e logo $E(s_1) \subsetneqq E(s_2)$, absurdo.

Agora, provemos que $d_{\min} = q^m - s$. Pela Proposição 4.1.8 precisamos apenas encontrar uma palavra não nula $\mathrm{ev}(\sum_{i=1}^{t}\gamma_i M_i + I)$ em $E(s)$ de peso igual a $q^m - s$, ou seja, precisamos encontrar um polinômio não nulo $\sum_{i=1}^{t}\gamma_i M_i$, com $\gamma_i \in \mathbb{F}_q$ e $M_i \in \mathcal{M}(q,s)$, para todo $i = 1,\ldots,t$ que tenha s zeros diferentes em $\mathbb{F}_q^m$. Primeiro, escolha $M \in \mathcal{M}(q,s)$ tal que $D(M) = s$, digamos, $M = X_1^{a_1}\cdots X_m^{a_m}$. Portanto,

$$s = \#(\Delta(M, X_1^q, \ldots, X_m^q)) = q^m - (q-a_1)(q-a_2)\cdots(q-a_m).$$

Considere $\mathbb{F}_q = \{\alpha_1, \ldots, \alpha_q\}$ e defina o polinômio

$$P(X_1,\ldots,X_m) := (X_1-\alpha_1)\cdots(X_1-\alpha_{a_1})(X_2-\alpha_1)\cdots(X_2-\alpha_{a_2})\cdots(X_m-\alpha_1)\cdots(X_m-\alpha_{a_m}).$$

Note que P é um polinômio da forma desejada. Os elementos de $\mathbb{F}_q^m$ que não são zeros de P são precisamente os elementos da forma $(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_m})$, com $i_1 > a_1, \ldots, i_m > a_m$, e portanto o número de não zeros é $(q-a_1)\cdots(q-a_m)$. De $(q-a_1)\cdots(q-a_m) = q^m - s$ temos que $d_{\min} = q^m - s$. □

Exemplo 4.1.11. *Retomando o Exemplo 4.1.5 vimos que* $D(X_1X_2X_3) = 19$. *Como* $D(X_1X_2X_3) = 19 \in S$ *então o Teorema 4.1.10 pode ser aplicado e, portanto, a distância mínima de* $E(19)$ *é igual a* $d_{\min} = 3^3 - 19 = 8$.

Doravante, sempre assumiremos que $s \in S$.

Definição 4.1.12. *Dado um inteiro* $s \geq 0$, *defina*

$$\mathcal{N}(q,s) := \{X_1^{a_1} \cdots X_m^{a_m} \in \Delta(I) \mid \prod_{i=1}^{m}(a_i+1) < q^m - s\}.$$

Teorema 4.1.13. *Seja* $s \geq 0$ *e, considere o anel* $\mathbb{F}_q[\mathbf{X}]$. *Temos*

$$E(s) = \{\mathbf{c} \in \mathbb{F}_q^n \mid \langle \mathbf{c}, \mathrm{ev}(M+I)\rangle = 0, \text{ para todo } M \in \mathcal{N}(q,s)\},$$

onde $\langle \cdot, \cdot \rangle$ *denota o produto interno usual em* $\mathbb{F}_q^n$.

Demonstração. Defina

$$\mathrm{Hyp}_q(s,m) := \{\mathbf{c} \in \mathbb{F}_q^n \mid \langle \mathbf{c}, \mathrm{ev}(N+I)\rangle = 0, \text{ para todo } N \in \mathcal{N}(q,s)\}.$$

Sejam $M \in \mathcal{M}(q,s)$ e $N \in \mathcal{N}(q,s)$, onde $M = X_1^{a_1} \cdots X_m^{a_m}$ e $N = X_1^{b_1} \cdots X_m^{b_m}$, com $a_i, b_i < q$, para todo $i = 1, \ldots, m$. Primeiro, provemos que $E(s) \subseteq \mathrm{Hyp}_q(s,m)$. Para isso, como o produto interno é bilinear então basta verificar que $\langle \mathrm{ev}(M+I), \mathrm{ev}(N+I)\rangle = 0$. Escrevendo $\mathbf{P}_j = (\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_m})$, para todo $j = 1, \ldots, n$, temos que

$$\begin{aligned}
\langle \mathrm{ev}(M+I), \mathrm{ev}(N+I)\rangle &= \langle (M(\mathbf{P}_1), \ldots, M(\mathbf{P}_n)), (N(\mathbf{P}_1), \ldots, N(\mathbf{P}_n))\rangle \\
&= M(\mathbf{P}_1)N(\mathbf{P}_1) + \cdots + M(\mathbf{P}_n)N(\mathbf{P}_n) \\
&= X_1^{a_1} \cdots X_m^{a_m}(\mathbf{P}_1)X_1^{b_1} \cdots X_m^{b_m}(\mathbf{P}_1) + \cdots + X_1^{a_1} \cdots X_m^{a_m}(\mathbf{P}_n)X_1^{b_1} \cdots X_m^{b_m}(\mathbf{P}_n) \\
&= \alpha_{11}^{a_1}\alpha_{12}^{a_2} \cdots \alpha_{1m}^{a_m}\alpha_{11}^{b_1}\alpha_{12}^{b_2} \cdots \alpha_{1m}^{b_m} + \cdots + \alpha_{n1}^{a_1}\alpha_{n2}^{a_2} \cdots \alpha_{nm}^{a_m}\alpha_{n1}^{b_1}\alpha_{n2}^{b_2} \cdots \alpha_{nm}^{b_m} \\
&= \alpha_{11}^{a_1+b_1} \cdots \alpha_{1m}^{a_m+b_m} + \cdots + \alpha_{n1}^{a_1+b_1} \cdots \alpha_{nm}^{a_m+b_m} \\
&= \sum_{i=1}^{q} \alpha_i^{a_1+b_1} \cdots \sum_{i=1}^{q} \alpha_i^{a_m+b_m},
\end{aligned}$$

onde $\mathbb{F}_q = \{\alpha_1, \ldots, \alpha_q\}$.

Vamos mostrar que se existe um índice j tal que $a_j + b_j \not\equiv 0 \bmod(q-1)$, então $\langle \mathrm{ev}(M+I), \mathrm{ev}(N+I)\rangle = 0$. Seja g um gerador do grupo cíclico $\mathbb{F}_q^*$, e seja $k = a_j + b_j$, observe que $\sum_{i=1}^{q} \alpha_i^{a_j+b_j} = 1 + g^k + g^{2k} + \cdots + g^{(q-2)k}$. Temos que $g^k \neq 1$, e mais ainda,

$$(1 + g^k + \cdots + (g^k)^{q-2})(1 - g^k) = 1 - (g^k)^{q-1} = 1 - (g^{q-1})^k = 0.$$

Isso mostra que $1 + g^k + g^{2k} + \cdots + g^{(q-2)k} = 0$.

Assim, $\sum_{i=1}^{q} \alpha_i^{a_j+b_j} = 0$ e logo $\langle \mathrm{ev}(M+I), \mathrm{ev}(N+I)\rangle = 0$.

Suponha agora que para todo $i = 1, \ldots, m$ temos $a_i + b_i \equiv 0 \bmod(q-1)$. Como $0 \leq a_i, b_i \leq q-1$ para todo $i = 1, \ldots, m$ temos que ter ou $a_i + b_i = 0$, ou $a_i + b_i = q-1$ ou $a_i + b_i = 2q-2$.

Vamos assumir que $a_j + b_j = 0$ para algum $j \in \{1, \ldots, m\}$. Temos que

$$\sum_{\alpha \in \mathbb{F}_q} \alpha^{a_j+b_j} = q \cdot 1 = 0.$$

Finalmente, temos que analisar o caso onde para todo $i = 1, \ldots, m$ acontece $a_i + b_i = q - 1$ ou $a_i + b_i = 2(q-1)$. Suponha que $a_i + b_i = q - 1$, para todo $i = 1, \ldots, r$ e $a_i + b_i = 2(q-1)$, para todo $i = r+1, \ldots, m$, e observe que a única possibilidade, no segundo caso, é termos $a_i = b_i = q - 1$, para todo $i = r+1, \ldots, m$. De qualquer forma, temos que $q - a_i = b_i + 1$ para todo $i = 1, \ldots, m$. Como $M \in \mathcal{M}(q, s)$ então $q^m - \prod_{i=1}^{m}(q - a_i) \leq s$. Portanto,

$$\begin{aligned} q^m - s &\leq \prod_{i=1}^{m}(q - a_i) \\ &= \prod_{i=1}^{r}(b_i + 1) \\ &= \frac{\prod_{i=1}^{m}(b_i + 1)}{q^{m-r}} \\ &< \frac{q^m - s}{q^{m-r}}, \end{aligned}$$

uma contradição, então esse caso na verdade nunca ocorre. Portanto, $E(s) \subseteq \mathrm{Hyp}_q(s, m)$. Por outro lado, como ev é um isomorfismo e a dimensão do espaço gerado pela avaliação das classes de monômios em $\mathcal{N}(q, s)$ é $\#(\mathcal{N}(q, s))$, temos que

$$\begin{aligned} \dim(\mathrm{Hyp}_q(s, m)) &= q^m - \#\{(a_1, \ldots, a_m) \mid 0 \leq a_i < q, i = 1, \ldots, m, \prod_{i=1}^{m}(a_i + 1) < q^m - s\} \\ &= \#\{(a_1, \ldots, a_m) \mid 0 \leq a_i < q, i = 1, \ldots, m, \prod_{i=1}^{m}(a_i + 1) \geq q^m - s\} \end{aligned}$$

e

$$\begin{aligned} \dim(E(s)) &= \#\{(a_1, \ldots, a_m) \mid 0 \leq a_i < q, i = 1, \ldots, m,\ D(X_1^{a_1} \cdots X_m^{a_m}) \leq s\} \\ &= \#\{(a_1, \ldots, a_m) \mid 0 \leq a_i < q, i = 1, \ldots, m,\ \prod_{i=1}^{m}(q - a_i) \geq q^m - s\}. \end{aligned}$$

Agora, defina a função

$$\begin{array}{rccc} \mathrm{T}: & A_1 & \to & A_2 \\ & (z_1, \ldots, z_m) & \mapsto & \mathrm{T}(z_1, \ldots, z_m) = (q - z_1 - 1, \ldots, q - z_m - 1), \end{array}$$

onde

$$A_1 := \{(a_1, \ldots, a_m) \mid 0 \leq a_i < q, i = 1, \ldots, m, \prod_{i=1}^{m}(q - a_i) \geq q^m - s\}$$

e

$$A_2 := \{(a_1, \ldots, a_m) \mid 0 \leq a_i < q, i = 1, \ldots, m, \prod_{i=1}^{m}(a_i + 1) \geq q^m - s\}.$$

Provemos que é bijetora. Com efeito, sejam $\mathbf{y} = (y_1, \ldots, y_m) \in A_1$ e $\mathbf{z} = (z_1, \ldots, z_m) \in A_1$ tais que $\mathrm{T}(\mathbf{y}) = \mathrm{T}(\mathbf{z})$. Assim, $(q - y_1 - 1, \ldots, q - y_m - 1) = (q - z_1 - 1, \ldots, q - z_m - 1)$, ou seja, $q - y_i - 1 = q - z_i - 1$, para todo $i = 1, \ldots, m$. Logo, $y_i = z_i$, para todo $i = 1, \ldots, m$. Portanto, $\mathbf{y} = \mathbf{z}$.

Seja $\mathbf{w} = (w_1, \ldots, w_m) \in A_2$ e defina $\mathbf{z} := (z_1, \ldots, z_m)$, com $z_i = q - w_i - 1$, para todo $i = 1, \ldots, m$. É fácil ver que $\mathbf{z} \in A_1$. Então

$$\begin{aligned}
\mathrm{T}(\mathbf{z}) &= \mathrm{T}(z_1, \ldots, z_m) \\
&= \mathrm{T}(q - w_1 - 1, \ldots, q - w_m - 1) \\
&= (q - (q - w_1 - 1) - 1, \ldots, q - (q - w_m - 1) - 1) \\
&= (w_1, \ldots, w_m) \\
&= \mathbf{w}.
\end{aligned}$$

Logo, T é sobrejetora.

Como $E(s)$ está contido em $\mathrm{Hyp}_q(s, m)$ e ambos possuem a mesma dimensão segue que $E(s) = \mathrm{Hyp}_q(s, m)$ e o resultado está provado. □

Observação 4.1.14. *Segue do Teorema 4.1.13 que agora temos uma matriz teste de paridade dos códigos hiperbólicos.*

Definição 4.1.15. *Seja $a \in \mathbb{N}$. Defina o número inteiro*

$$V(m, a) := \#\{(x_1, \ldots, x_m) \in \mathbb{N}^m \mid 1 \leq x_i \leq q, \text{ para todo } i = 1, \ldots, m \text{ e } \prod_{i=1}^{m} x_i \leq a\}.$$

Claramente $1 \leq V(m, a) \leq q^m$, para todos $m \geq 1$ e $a \in \mathbb{N}$. Em seguida, vejamos um exemplo.

Exemplo 4.1.16. *Seja $m = 2$ e seja $q = 3$. Assim,*

- *se $a = 1$, então*

$$\begin{aligned}
V(2, 1) &= \#\{(x_1, x_2) \in \mathbb{N}^2 \mid 1 \leq x_1, x_2 \leq 3 \text{ e } x_1 x_2 \leq 1\} \\
&= \#\{(1, 1)\} = 1;
\end{aligned}$$

- *se $a = 2$, então*

$$\begin{aligned}
V(2, 2) &= \#\{(x_1, x_2) \in \mathbb{N}^2 \mid 1 \leq x_1, x_2 \leq 3 \text{ e } x_1 x_2 \leq 2\} \\
&= \#\{(1, 1), (1, 2), (2, 1)\} = 3;
\end{aligned}$$

- *se $a = 3$, então*

$$\begin{aligned}
V(2, 3) &= \#\{(x_1, x_2) \in \mathbb{N}^2 \mid 1 \leq x_1, x_2 \leq 3 \text{ e } x_1 x_2 \leq 3\} \\
&= \#\{(1, 1), (1, 2), (1, 3), (2, 1), (3, 1)\} = 5;
\end{aligned}$$

- *se $a = 4$, então*

$$\begin{aligned}
V(2, 4) &= \#\{(x_1, x_2) \in \mathbb{N}^2 \mid 1 \leq x_1, x_2 \leq 3 \text{ e } x_1 x_2 \leq 4\} \\
&= \#\{(1, 1), (1, 2), (1, 3), (2, 1), (3, 1), (2, 2)\} = 6;
\end{aligned}$$

- *se $a = 5$, então*

$$\begin{aligned}
V(2, 5) &= \#\{(x_1, x_2) \in \mathbb{N}^2 \mid 1 \leq x_1, x_2 \leq 3 \text{ e } x_1 x_2 \leq 5\} \\
&= V(2, 4);
\end{aligned}$$

- *se* $a = 6$, *então*

$$\begin{aligned} V(2,6) &= \#\{(x_1,x_2) \in \mathbb{N}^2 \mid 1 \leq x_1, x_2 \leq 3 \text{ e } x_1x_2 \leq 6\} \\ &= \#\{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2)\} = 8; \end{aligned}$$

- *se* $a = 7$, *então*

$$\begin{aligned} V(2,7) &= \#\{(x_1,x_2) \in \mathbb{N}^2 \mid 1 \leq x_1, x_2 \leq 3 \text{ e } x_1x_2 \leq 7\} \\ &= V(2,6); \end{aligned}$$

- *se* $a = 8$, *então*

$$\begin{aligned} V(2,8) &= \#\{(x_1,x_2) \in \mathbb{N}^2 \mid 1 \leq x_1, x_2 \leq 3 \text{ e } x_1x_2 \leq 8\} \\ &= V(2,6); \end{aligned}$$

- *se* $a = 9$, *então*

$$\begin{aligned} V(2,9) &= \#\{(x_1,x_2) \in \mathbb{N}^2 \mid 1 \leq x_1, x_2 \leq 3 \text{ e } x_1x_2 \leq 9\} \\ &= \#\{(1,1),(1,2),(2,1),(1,3),(3,1),(2,2),(2,3),(3,2),(3,3)\} = 9. \end{aligned}$$

Observação 4.1.17. *Vimos no Teorema 4.1.13 que*

$$\dim(\mathrm{Hyp}_q(s,m)) = q^m - \#\{(a_1,\ldots,a_m) \mid 0 \leq a_i < q,\ i = 1,\ldots,m, \prod_{i=1}^{m}(a_i+1) < q^m - s\}.$$

Defina $x_i := a_i + 1$, *para todo* $i = 1,\ldots,m$. *Então* $1 \leq x_i \leq q$, *para todo* $i = 1,\ldots,m$ *e* $\prod_{i=1}^{m}(a_i+1) = \prod_{i=1}^{m} x_i$. *É fácil ver que existe uma bijeção entre* $\{(a_1,\ldots,a_m) \mid 0 \leq a_i < q,\ i = 1,\ldots,m, \prod_{i=1}^{m}(a_i+1) < q^m - s\}$ *e* $\{(x_1,\ldots,x_m) \mid 1 \leq x_i \leq q,\ i = 1,\ldots,m, \prod_{i=1}^{m} x_i \leq q^m - s - 1\}$ *dada por* $\varphi(a_1,\ldots,a_m) = (a_1+1,\ldots,a_m+1)$. *Portanto, usando a definição do número* $V(m,a)$ *temos que*

$$\begin{aligned} \dim(\mathrm{Hyp}_q(s,m)) &= q^m - \#\{(x_1,\ldots,x_m) \mid 1 \leq x_i \leq q,\ i = 1,\ldots,m, \prod_{i=1}^{m} x_i \leq q^m - s - 1\} \\ &= q^m - V(m, q^m - s - 1). \end{aligned}$$

No que se segue, vejamos algumas propriedades do número $V(m,a)$.

Proposição 4.1.18. *Seja* $a \in \mathbb{N}$. *Então*
i) $V(1,a) = \min\{a,q\}$;
ii) $V(m,a) = \sum_{j=1}^{q} V\left(m-1, \left\lfloor \frac{a}{j} \right\rfloor\right)$, *para todo* $m \geq 2$;
iii) $V(2,a) = bq + \sum_{j=b+1}^{\min\{a,q\}} \left\lfloor \frac{a}{j} \right\rfloor$, *onde* $b := \min\left\{ \left\lfloor \frac{a}{q} \right\rfloor, q \right\}$, *com a última soma igual a zero se* $b = q$;
iv) Se $q = 2$, *então* $V(m,a) = \sum_{j=0}^{i} \binom{m}{j}$, *se* $2^i \leq a < 2^{i+1}$.

Demonstração. (i) Se $a \geq q$, então

$$V(1,a) = \#\{x \in \mathbb{N} \mid 1 \leq x \leq q \text{ e } x \leq a\} = q = \min\{a,q\}.$$

Se $a \leq q$, então

$$V(1,a) = \#\{x \in \mathbb{N} \mid 1 \leq x \leq q \text{ e } x \leq a\} = a = \min\{a,q\}.$$

Logo, $V(1,a) = \#\{x \in \mathbb{N} \mid 1 \leq x \leq q,\ x \leq a\} = \min\{a,q\}$.

(ii) Suponha que $m \geq 2$. Como $x_m \in \{1,\ldots,q\}$ temos

$$\{(x_1,\ldots,x_{m-1},x_m) \in \mathbb{N}^m \mid 1 \leq x_i \leq q,\ i=1,\ldots,m \ \text{ e } \prod_{i=1}^{m} x_i \leq a\} =$$
$$\bigcup_{j=1}^{q} \left\{ (x_1,\ldots,x_{m-1},j) \mid 1 \leq x_i \leq q,\ i=1,\ldots,m-1 \ \text{ e } \prod_{i=1}^{m-1} x_i \leq \left\lfloor \frac{a}{j} \right\rfloor \right\}$$

e portanto

$$V(m,a) = \#\left\{ (x_1,\ldots,x_{m-1},j) \in \mathbb{N}^m \mid 1 \leq x_i \leq q,\ i=1,\ldots,m-1 \ \text{ e } \prod_{i=1}^{m-1} x_i \leq \left\lfloor \frac{a}{j} \right\rfloor \right\}$$
$$= \sum_{j=1}^{q} V\left(m-1, \left\lfloor \frac{a}{j} \right\rfloor\right).$$

Dos itens (i) e (ii) segue que, para todo $a \in \mathbb{N}$, podemos calcular o número $V(m,a)$ recursivamente.

(iii) Das propriedades (i) e (ii) segue que

$$V(2,a) = \sum_{j=1}^{q} V\left(1, \left\lfloor \frac{a}{j} \right\rfloor\right) = \sum_{j=1}^{q} \min\left\{ \left\lfloor \frac{a}{j} \right\rfloor, q \right\}. \tag{4.1}$$

Defina $b := \min\left\{ \left\lfloor \frac{a}{q} \right\rfloor, q \right\}$. Para $1 \leq j \leq b$, tem-se que $\left\lfloor \frac{a}{j} \right\rfloor \geq \left\lfloor \frac{a}{b} \right\rfloor \geq q$ e temos

$$\min\left\{ \left\lfloor \frac{a}{j} \right\rfloor, q \right\} = q.$$

Se $q \leq \left\lfloor \frac{a}{q} \right\rfloor$, então $b = q$ e

$$V(2,a) = \sum_{j=1}^{q} q = q^2.$$

Se $\left\lfloor \frac{a}{q} \right\rfloor < q$, então para $\left\lfloor \frac{a}{q} \right\rfloor < j$ tem-se que $\frac{a}{q} \leq j$ e $\frac{a}{j} \leq q$. Logo,

$$\min\left\{ \left\lfloor \frac{a}{j} \right\rfloor, q \right\} = \left\lfloor \frac{a}{j} \right\rfloor.$$

Assim,

$$V(2,a) = \sum_{j=1}^{q} \min\left\{ \left\lfloor \frac{a}{j} \right\rfloor, q \right\} = \sum_{j=1}^{b} q + \sum_{j=b+1}^{q} \left\lfloor \frac{a}{j} \right\rfloor = bq + \sum_{j=b+1}^{q} \left\lfloor \frac{a}{j} \right\rfloor.$$

Como $\left\lfloor \frac{a}{j} \right\rfloor = 0$ se $j > a$, então

$$V(2,a) = bq + \sum_{j=b+1}^{\min\{a,q\}} \left\lfloor \frac{a}{j} \right\rfloor.$$

(*iv*) Se $q = 2$, temos que $x_i \in \{1, 2\}$, para todo $i = 1, \ldots, m$. O produto $\prod_{i=1}^{m} x_i$ é 2^t, onde t é o número de coordenadas iguais a 2. A condição $\prod_{i=1}^{m} x_i \leq a$ equivale a

$$2^t \leq a \quad \Longleftrightarrow \quad t \leq i := \lfloor \log_2 a \rfloor.$$

Para cada t fixo (número de entradas iguais a 2), existem $\binom{m}{t}$ escolhas de posições para essas coordenadas (as demais valem 1). Logo,

$$V(m, a) = \sum_{t=0}^{\min\{m,i\}} \binom{m}{t}.$$

Se $i \geq m$, isso coincide com 2^m (segue imediatamente do Binômio de Newton), e se $i < m$, obtém-se que $V(m, a) = \sum_{j=0}^{i} \binom{m}{j}$. □

4.2 Pesos generalizados de Hamming para os Códigos Hiperbólicos

Na presente seção, bem como nas seções subsequentes, estudaremos os pesos generalizados de Hamming dos códigos hiperbólicos. Para isso, comecemos relembrando o conceito de peso generalizado de Hamming, introduzido na seção 2.3.

Definição 4.2.1. *Seja C um código de dimensão k e seja $r = 1, \ldots, k$. O r-**ésimo peso generalizado de Hamming** de C, denotado por d_r, é definido como sendo o número inteiro não negativo*

$$d_r := \min\{\#(\chi(U)) \mid U \text{ é um subespaço de } C \text{ com } \dim(U) = r\},$$

onde $\chi(U) := \{i \mid \exists\ (x_1, \ldots, x_n) \in U,\ x_i \neq 0\}$.

Com o objetivo de calcular o (ou pelo menos dar uma cota inferior para o) r-ésimo peso generalizado de Hamming do código hiperbólico, introduzimos o seguinte número.

Definição 4.2.2. *Defina o número inteiro não negativo*

$$\eta_r(q, s, m) := \max\left\{ \#(\Delta(M_1, \ldots, M_r, X_1^q, \ldots, X_m^q)) \;\middle|\; \begin{array}{l} M_i \neq M_j, \text{ para todo } i \neq j, \\ M_i \in \mathcal{M}(q, s),\ i = 1, \ldots, r \end{array} \right\},$$

onde $\Delta(M_1, \ldots, M_r, X_1^q, \ldots, X_m^q)$ é o conjunto dos monômios que <u>não</u> são múltiplos de nenhum dos monômios $M_1, \ldots, M_r, X_1^q, \ldots, X_m^q$.

Observação 4.2.3. *Observe que, para determinar $\eta_r(q, s, m)$ é necessário analisar $\binom{\mathcal{M}(q,s)}{r}$ números.*

No que se segue, sempre que tivermos um conjunto $F = \{M_1, \ldots, M_i\}$ designaremos $(M_1, \ldots, M_i, X_1^q, \ldots, X_m^q)$ por $(F, X_1^q, \ldots, X_m^q)$.

Sejam $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m)$ e $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_m)$ em $\mathbb{N}_0^m$. Lembramos que o **máximo divisor comum** dos monômios $\mathbf{X}^{\boldsymbol{\alpha}} = X_1^{\alpha_1} \cdots X_m^{\alpha_m}$ e $\mathbf{X}^{\boldsymbol{\beta}} = X_1^{\beta_1} \cdots X_m^{\beta_m}$ é

$$\mathrm{MDC}(\mathbf{X}^{\boldsymbol{\alpha}}, \mathbf{X}^{\boldsymbol{\beta}}) = X_1^{\delta_1} \cdots X_m^{\delta_m},$$

onde $\delta_i = \min\{\alpha_i, \beta_i\}$, para todo $i = 1, \ldots, m$.

4.3 Conjunto denso e ótimo de tamanho r

Definição 4.3.1 (Conjunto denso)**.** *Seja $D = \{M_1, \ldots, M_r\} \subseteq \mathcal{M}(q, s)$. Dizemos que D é um* ***conjunto denso relacionado a*** *$E(s)$ se*

$$\{X_1^{b_1} \cdots X_m^{b_m} \in \Delta(D, X_1^q, \ldots, X_m^q) \mid b_i \geq a_i, \text{para todo } i = 1, \ldots, m\} \subseteq \mathcal{M}(q, s),$$

onde $X_1^{a_1} \cdots X_m^{a_m} = \mathrm{MDC}(M_1, \ldots, M_r)$ (no caso em que $r = 1$ convencionamos que $\mathrm{MDC}(M_1) = M_1$).

Definição 4.3.2 (Conjunto ótimo de tamanho r)**.** *Seja $D = \{M_1, \ldots, M_r\} \subseteq \mathcal{M}(q, s)$. Dizemos que D é um* ***conjunto ótimo de tamanho*** *r* ***relacionado a*** *$E(s)$ se $M_i \neq M_j$, com $i \neq j$ e satisfaz*

$$\#(\Delta(D, X_1^q, \ldots, X_m^q)) = \eta_r(q, s, m).$$

Exemplo 4.3.3. *Retomando os Exemplos 4.1.5 e 4.1.11, vamos determinar os conjuntos densos e ótimos de tamanhos 1 e 2. De acordo com o Exemplo 4.1.5 temos*

$$\mathcal{M}(3, 19) = \{1, X_1, X_1^2, X_2, X_1X_2, X_2^2, X_3, X_1X_3, X_2X_3, X_1X_2X_3, X_3^2\}.$$

Entre todos esses monômios notemos que o monômio $X_1X_2X_3$ é tal que

$$\eta_1(3, 19, 3) = \#(\Delta(X_1X_2X_3, X_1^3, X_2^3, X_3^3)) = 19.$$

Portanto, o conjunto $\{X_1X_2X_3\}$ é ótimo de tamanho 1 relacionado a $E(19)$. Além disso, como

$$\{X_1^{b_1}X_2^{b_2}X_3^{b_3} \in \Delta(X_1X_2X_3, X_1^3, X_2^3, X_3^3) \mid b_i \geq 1, \text{ para todo } i = 1, 2, 3\} = \emptyset \subseteq \mathcal{M}(3, 19),$$

com $\mathrm{MDC}(X_1X_2X_3) = X_1X_2X_3$, temos que o conjunto $\{X_1X_2X_3\}$ é denso relacionado a $E(19)$.
Agora, determinaremos o(s) conjunto(s) ótimo(s) de tamanho 2 relacionados a $E(19)$. Para isso, devemos analisar, para cada par de monômios distintos M_1 e M_2 em $\mathcal{M}(3, 19)$, a cardinalidade do conjunto $\Delta(M_1, M_2, X_1^3, X_2^3, X_3^3)$, isto é, o número de monômios que não são múltiplos de nenhum dos monômios M_1, M_2, X_1^3, X_2^3 e X_3^3. Como $\#(\mathcal{M}(3, 19)) = 11$, existem exatamente $\binom{11}{2} = 55$ pares a serem considerados. A seguir, separamos a análise em casos, em que para cada um, fixamos um dos monômios M_1 em $\mathcal{M}(3, 19)$ e combinamos com todos os monômios possíveis M_2 de $\mathcal{M}(3, 19)$, com $M_1 \neq M_2$.

- *Seja $M_1 = 1$. Como todo monômio $M \in \Delta(I)$ é múltiplo de 1, então*

  $$\#(\Delta(1, M_2, X_1^3, X_2^3, X_3^3)) = 0,$$

  para todo $M_2 \in \mathcal{M}(3, 19)$.

- *Seja $M_1 = X_1$.*

  $$\begin{aligned}
  &\#(\Delta(X_1, X_2, X_1^3, X_2^3, X_3^3)) = 3\\
  &\#(\Delta(X_1, X_3, X_1^3, X_2^3, X_3^3)) = 3\\
  &\#(\Delta(X_1, X_1^2, X_1^3, X_2^3, X_3^3)) = 6\\
  &\#(\Delta(X_1, X_2^2, X_1^3, X_2^3, X_3^3)) = 6\\
  &\#(\Delta(X_1, X_3^2, X_1^3, X_2^3, X_3^3)) = 6\\
  &\#(\Delta(X_1, X_1X_2, X_1^3, X_2^3, X_3^3)) = 9\\
  &\#(\Delta(X_1, X_1X_3, X_1^3, X_2^3, X_3^3)) = 9\\
  &\#(\Delta(X_1, X_2X_3, X_1^3, X_2^3, X_3^3)) = 9\\
  &\#(\Delta(X_1, X_1X_2X_3, X_1^3, X_2^3, X_3^3)) = 9
  \end{aligned}$$

- *Seja* $M_1 = X_2$.

$$\begin{aligned}
&\#(\Delta(X_2, X_3, X_1^3, X_2^3, X_3^3)) = 3\\
&\#(\Delta(X_2, X_1^2, X_1^3, X_2^3, X_3^3)) = 6\\
&\#(\Delta(X_2, X_2^2, X_1^3, X_2^3, X_3^3)) = 6\\
&\#(\Delta(X_2, X_3^2, X_1^3, X_2^3, X_3^3)) = 6\\
&\#(\Delta(X_2, X_1X_2, X_1^3, X_2^3, X_3^3)) = 9\\
&\#(\Delta(X_2, X_1X_3, X_1^3, X_2^3, X_3^3)) = 9\\
&\#(\Delta(X_2, X_2X_3, X_1^3, X_2^3, X_3^3)) = 9\\
&\#(\Delta(X_2, X_1X_2X_3, X_1^3, X_2^3, X_3^3)) = 9
\end{aligned}$$

- *Seja* $M_1 = X_3$.

$$\begin{aligned}
&\#(\Delta(X_3, X_1^2, X_1^3, X_2^3, X_3^3)) = 6\\
&\#(\Delta(X_3, X_2^2, X_1^3, X_2^3, X_3^3)) = 6\\
&\#(\Delta(X_3, X_3^2, X_1^3, X_2^3, X_3^3)) = 9\\
&\#(\Delta(X_3, X_1X_2, X_1^3, X_2^3, X_3^3)) = 5\\
&\#(\Delta(X_3, X_1X_3, X_1^3, X_2^3, X_3^3)) = 9\\
&\#(\Delta(X_3, X_2X_3, X_1^3, X_2^3, X_3^3)) = 9\\
&\#(\Delta(X_3, X_1X_2X_3, X_1^3, X_2^3, X_3^3)) = 9
\end{aligned}$$

- *Seja* $M_1 = X_1^2$.

$$\begin{aligned}
&\#(\Delta(X_1^2, X_2^2, X_1^3, X_2^3, X_3^3)) = 8\\
&\#(\Delta(X_1^2, X_3^2, X_1^3, X_2^3, X_3^3)) = 8\\
&\#(\Delta(X_1^2, X_1X_2, X_1^3, X_2^3, X_3^3)) = 10\\
&\#(\Delta(X_1^2, X_1X_3, X_1^3, X_2^3, X_3^3)) = 10\\
&\#(\Delta(X_1^2, X_2X_3, X_1^3, X_2^3, X_3^3)) = 10\\
&\#(\Delta(X_1^2, X_1X_2X_3, X_1^3, X_2^3, X_3^3)) = 10
\end{aligned}$$

- *Seja* $M_1 = X_2^2$.

$$\begin{aligned}
&\#(\Delta(X_2^2, X_3^2, X_1^3, X_2^3, X_3^3)) = 9\\
&\#(\Delta(X_2^2, X_1X_2, X_1^3, X_2^3, X_3^3)) = 6\\
&\#(\Delta(X_2^2, X_1X_3, X_1^3, X_2^3, X_3^3)) = 10\\
&\#(\Delta(X_2^2, X_2X_3, X_1^3, X_2^3, X_3^3)) = 8\\
&\#(\Delta(X_2^2, X_1X_2X_3, X_1^3, X_2^3, X_3^3)) = 8
\end{aligned}$$

- *Seja* $M_1 = X_3^2$.

$$\begin{aligned}
&\#(\Delta(X_3^2, X_1X_2, X_1^3, X_2^3, X_3^3)) = 10\\
&\#(\Delta(X_3^2, X_1X_3, X_1^3, X_2^3, X_3^3)) = 8\\
&\#(\Delta(X_3^2, X_2X_3, X_1^3, X_2^3, X_3^3)) = 8\\
&\#(\Delta(X_3^2, X_1X_2X_3, X_1^3, X_2^3, X_3^3)) = 10
\end{aligned}$$

- *Seja* $M_1 = X_1X_2$.

$$\#(\Delta(X_1X_2, X_1X_3, X_1^3, X_2^3, X_3^3)) = 11$$
$$\#(\Delta(X_1X_2, X_2X_3, X_2^3, X_3^3)) = 7$$
$$\#(\Delta(X_1X_2, X_1X_2X_3, X_1^3, X_2^3, X_3^3)) = 15$$

- *Seja* $M_1 = X_1X_3$.

$$\#(\Delta(X_1X_3, X_2X_3, X_1^3, X_2^3, X_3^3)) = 7$$
$$\#(\Delta(X_1X_3, X_1X_2X_3, X_1^3, X_2^3, X_3^3)) = 15$$

- *Seja* $M_1 = X_2X_3$.

$$\#(\Delta(X_2X_3, X_1X_2X_3, X_1^3, X_2^3, X_3^3)) = 15$$

Dessa forma, temos que

$$\eta_2(3, 19, 3) = \#(\Delta(X_iX_j, X_1X_2X_3, X_1^3, X_2^3, X_3^3)) = 15.$$

Portanto, todos os conjuntos da forma $D = \{X_iX_j, X_1X_2X_3\}$*, com* $i \neq j$*, são conjuntos ótimos de tamanho* 2 *relacionado a* $E(19)$.
Como

$$\{X_1^{b_1}X_2^{b_2}X_3^{b_3} \in \Delta(X_iX_j, X_1X_2X_3, X_1^3, X_2^3, X_3^3) \mid b_i \geq 1,\ b_j \geq 1\} = \emptyset \subseteq \mathcal{M}(3, 19),$$

onde $\mathrm{MDC}(X_iX_j, X_1X_2X_3) = X_iX_j$*, com* $i \neq j$*, então os conjuntos da forma* $\{X_iX_j, X_1X_2X_3\}$ *também são densos relacionados a* $E(19)$.

Exemplo 4.3.4. *Considere* $M = X_1^{a_1} \cdots X_m^{a_m} \in \Delta(I)$*. Observe que*

$$\{X_1^{b_1} \cdots X_m^{b_m} \in \Delta(M, X_1^q, \ldots, X_m^q) \mid b_i \geq a_i,\ \textit{para todo } i = 1, \ldots, m\} = \emptyset \subseteq \mathcal{M}(q, s),$$

onde $\mathrm{MDC}(M) = X_1^{a_1} \cdots X_m^{a_m}$*. Portanto, o conjunto* $\{M\}$ *é denso relacionado a* $E(s)$.

Teorema 4.3.5. *O* r*-ésimo peso generalizado de Hamming de* $E(s)$ *satisfaz*

$$d_r \geq q^m - \eta_r(q, s, m). \tag{4.2}$$

Se existir um conjunto denso e ótimo de tamanho r *então vale a igualdade em 4.2.*

Demonstração. Se para cada j escrevemos

$$f_j = \sum_{i=1}^{t_j} \gamma_{ij} M_{ij} \quad \text{e} \quad \mathrm{LM}(f_j) = M_{t_j j},$$

onde todos os $M_{t_j j}$ são distintos,

$$E(f_1, \ldots, f_j) = \langle \{\mathrm{ev}(f_1 + I), \ldots, \mathrm{ev}(f_r + I)\} \rangle \subseteq E(s)$$

e d_r é o mínimo dentre os $\#(\chi(E(f_1, \ldots, f_j))$. Definimos $J = \langle f_1, \ldots, f_r \rangle + I$. Lembre que $\chi(E(f_1, \ldots, f_j))$ é o conjunto de coordenadas que não se anulam em algum ponto de $\mathbb{F}_q^m$.

Por abuso de notação, podemos denotar as coordenadas do código pelos pontos de $\mathbb{F}_q^m$. Daí, $p \in \mathcal{X}(E(f_1,\ldots,f_r)) \iff \exists\ f \in J$ tal que $f(p) \neq 0$. Logo, $V(J)$ e $\mathcal{X}(E(f_1,\ldots,f_r)$ são disjuntos e a união deles é $\mathbb{F}_q^m$. Temos, para todo $j = 1,\ldots,r$, que

$$\#(\chi(E(f_1,\ldots,f_r)) = q^m - \#(V(J)).$$

Pela Observação 3.3.6 temos

$$\Delta(J) \subseteq \Delta(M_{t_1},\ldots,M_{t_r},X_1^q,\ldots,X_m^q).$$

Pela Proposição 3.3.13 e pela inclusão acima, temos que

$$\#(V(J)) \leq \#(\Delta(J)) \leq \#(\Delta(M_{t_1},\ldots,M_{t_r},X_1^q,\ldots,X_m^q)).$$

Em particular, $\#(V(J)) \leq \eta_r(q,s,m)$. Logo $\mathrm{ev}(f_j) \geq q^m - \eta_r(q,s,m)$, e assim $d_r \geq q^m - \eta_r(q,s,m)$.

Agora, suponha que $D_1 = \{M_1,\ldots,M_r\}$ é um conjunto denso e ótimo de tamanho r relacionado a $E(s)$. Acabamos de provar que $d_r \geq q^m - \eta_r(q,s,m)$ então $d_r \geq q^m - \#(\Delta(D_1,X_1^q,\ldots,X_m^q))$. Para provar a igualdade, basta provar que

$$d_r \leq q^m - \#(\Delta(D_1,X_1^q,\ldots,X_m^q)),$$

pois, se D_1 é um conjunto ótimo de tamanho r temos então

$$d_r = q^m - \#(\Delta(D_1,X_1^q,\ldots,X_m^q)) = q^m - \eta_r(q,s,m).$$

Considere $\mathrm{MDC}(M_1,\ldots,M_r) = X_1^{a_1}\cdots X_m^{a_m}$ e defina o seguinte conjunto:

$$D_2 := \{X_1^{b_1}\cdots X_m^{b_m} \in \mathcal{M}(q,s) \mid b_i \geq a_i,\ \text{para todo } i = 1,\ldots,m\}.$$

Claramente $D_1 \subseteq D_2$. Afirmamos que $\Delta(D_2,X_1^q,\ldots,X_m^q) \subseteq \Delta(D_1,X_1^q,\ldots,X_m^q)$. Com efeito, se $M \in \Delta(D_2,X_1^q,\ldots,X_m^q)$ então M não é múltiplo de nenhum dos monômios que estão em D_2 e $X_1^q,\ldots,X_m^q$, em particular, M não é múltiplo de nenhum dos monômios em D_1. Como D_1 é denso, segue por definição que os elementos em $\Delta(D_1,X_1^q,\ldots,X_m^q)$ que não pertencem a $\Delta(D_2,X_1^q,\ldots,X_m^q)$ estão todos em $\mathcal{M}(q,s)$. Se um monômio não pertence a $\Delta(D_2,X_1^q,\ldots,X_m^q)$ então é da forma $X_1^{b_1}\cdots X_m^{b_m}$ com $b_i \geq a_i$, para todo $i = 1,\ldots,m$. Logo, pela definição de D_2 temos $D_2 = \mathcal{M}(q,s) \setminus \Delta(D_2,X_1^q,\ldots,X_m^q)$. Dentre eles os monômios $M_1,\ldots,M_r$ são elementos de D_2 que não estão em $\Delta(D_2,X_1^q,\ldots,X_m^q)$ e, como esses monômios não estão em $\Delta(D_1,X_1^q,\ldots,X_m^q)$, então

$$\#(\Delta(D_1,X_1^q,\ldots,X_m^q)) - \#(\Delta(D_2,X_1^q,\ldots,X_m^q)) \leq \#(D_2) - r. \tag{4.3}$$

Seja $\mathbb{F}_q = \{\alpha_1,\ldots,\alpha_q\}$ e defina a função $\mathrm{T} : D_2 \to \mathbb{F}_q[\mathbf{X}]$ dada por

$$\mathrm{T}(X_1^{b_1}\cdots X_m^{b_m}) := (X_1-\alpha_1)\cdots(X_1-\alpha_{b_1})(X_2-\alpha_1)\cdots(X_2-\alpha_{b_2})\cdots(X_m-\alpha_1)\cdots(X_m-\alpha_{b_m}).$$

Claramente $\langle\{\mathrm{ev}(T(M)+I) \mid M \in D_2\}\rangle$ é um subespaço de $E(s)$ de dimensão $\#(D_2)$. Novamente, pela definição de D_2 temos que $a_i \leq b_i$, para todo $i = 1,\ldots m$, logo

$$(X_1-\alpha_1)\cdots(X_1-\alpha_{a_1})(X_2-\alpha_1)\cdots(X_2-\alpha_{a_2})\cdots(X_m-\alpha_1)\cdots(X_m-\alpha_{a_m})$$

é fator de todos os polinômios na imagem de T. O número de não zeros desse polinômio é $(q-a_1)\cdots(q-a_m)$. Então, o tamanho do suporte do subespaço $\langle\{\mathrm{ev}(P(M)+I) \mid M \in D_2\}\rangle$ de dimensão $\#(D_2)$ é no máximo $(q-a_1)\cdots(q-a_m)$. Logo,

$$\begin{aligned} d_{\#(D_2)} &\leq (q-a_1)(q-a_2)\cdots(q-a_m) \\ &= q^m - (q^m - (q-a_1)(q-a_2)\cdots(q-a_m)) \\ &= q^m - \#(\Delta(D_2,X_1^q,\ldots,X_m^q)). \end{aligned} \tag{4.4}$$

Pelo Teorema 2.3.7 temos

$$d_r \leq d_{r+1} - 1. \tag{4.5}$$

Portanto, usando 4.3, 4.4 e 4.5, segue que

$$\begin{aligned} d_r &\leq d_{\#(D_2)} - (\#(D_2) - r) \\ &\leq q^m - \#((\Delta(D_2, X_1^q, \ldots, X_m^q)) - (\#(D_2) - r) \\ &\leq q^m - \#(\Delta(D_1, X_1^q, \ldots, X_m^q)) + (\#(D_2) - r) - (\#(D_2) - r) \\ &= q^m - \#(\Delta(D_1, X_1^q, \ldots, X_m^q)). \end{aligned}$$

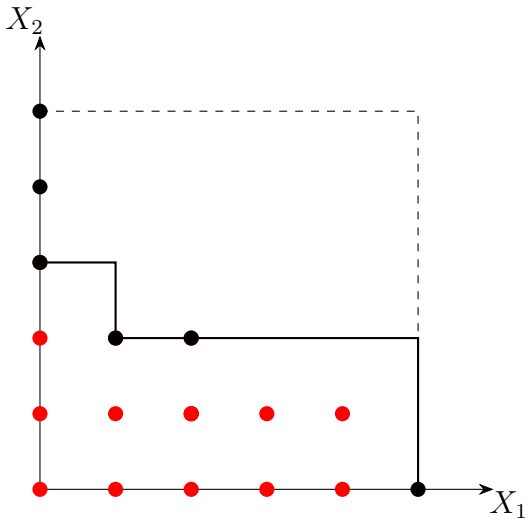
□

Vimos no Exemplo 4.3.4 que sempre existe um conjunto ótimo e denso de tamanho 1, logo o resultado acima é uma generalização do Teorema 4.1.10.

Exemplo 4.3.6. *Tome $q = 5$ e $m = 2$, e considere o código hiperbólico $E(16)$. Vamos determinar o terceiro e quarto peso generalizado de Hamming. Primeiro, note que*

$$\mathcal{M}(5, 16) = \{1, X_1, X_2, X_1^2, X_2^2, X_1^3, X_2^3, X_1X_2^2, X_1X_2, X_1^2X_2, X_1^2X_2^2\}.$$

Pela definição, deveríamos analisar, $\#(\Delta(M_1, M_2, M_3, X_1^5, X_2^5))$, isto é, o número de monômios que não são múltiplos de nenhum dos monômios M_1, M_2, M_3, X_1^5 e X_2^5, onde $M_i \in \mathcal{M}(5, 16)$, com $M_i \neq M_j$ para todo $i \neq j$. Como $\#(\mathcal{M}(5, 19)) = 11$, existem exatamente $\binom{11}{3} = 165$ ternas a serem consideradas. Aqui, vejamos isso somente através de uma figura que a maior de suas cardinalidades ocorre quando os monômios são iguais a $M_1 = X_2^3, M_2 = X_1X_2^2$ e $M_3 = X_1^2X_2^2$, e podemos ver que $\#(\Delta(X_2^3, X_1X_2^2, X_1^2X_2^2, X_1^5, X_2^5)) = 11$ (veja a figura a seguir).
Dessa forma, temos que o conjunto $D_1 = \{X_2^3, X_1X_2^2, X_1^2X_2^2\}$ é ótimo de tamanho 2 relacionado a $E(16)$.



Afirmamos que D_1 é um conjunto denso relacionado a $E(16)$. Primeiro, observe que

$$\begin{aligned} \Delta(D_1, X_1^5, X_2^5) &= \Delta(X_2^3, X_1X_2^2, X_1^2X_2^2, X_1^5, X_2^5) = \Delta(X_1X_2^2, X_1^2X_2^2, X_1^5, X_2^3) \\ &= \{1, X_1, X_2, X_1^2, X_2^2, X_1^3, X_1^4, X_1X_2, X_1^2X_2, X_1^3X_2, X_1^4X_2\}. \end{aligned}$$

Temos que $\mathrm{MDC}(X_2^3, X_1X_2^2, X_1^2X_2^2) = X_2^2$, *e também vale que*

$$\{X_1^{b_1}X_2^{b_2} \in \Delta(D_1, X_1^5, X_2^5) \mid b_1 \geq 0,\ b_2 \geq 2\} = \{X_2^2\} \subseteq \mathcal{M}(5, 16),$$

logo D_1 é um conjunto denso relacionado a $E(16)$. Portanto, pelo Teorema 4.3.5 segue que

$$d_3 = 5^2 - \eta_3(5, 16, 2) = 25 - 11 = 14.$$

De forma análoga ao que fizemos anteriormente, temos que $D_2 := \{X_2^2, X_2^3, X_1X_2^2, X_1^2X_2^2\}$ é um conjunto denso e ótimo de tamanho 4 relacionado a $E(16)$. Portanto, pelo Teorema 4.3.5 temos que

$$d_4 = 5^2 - \eta_4(5, 16, 2).$$

Além disso, como $\#(\Delta(D_2, X_1^5, X_2^5)) = \#(\Delta(D_1, X_1^5, X_2^5)) - 1$ então $d_4 = d_3 + 1 = 14 + 1 = 15$.

Agora, consideremos o número de variáveis igual a dois e vamos também restringir ao segundo peso generalizado de Hamming do código hiperbólico.

4.4 Segundo Peso Generalizado de Hamming do Código Hiperbólico

Lema 4.4.1. *Considere $m = 2$ e seja $E(s)$ um código hiperbólico de dimensão pelo menos igual a 2, então existe um conjunto denso e ótimo de tamanho 2 relacionado a $E(s)$.*

Demonstração. Seja $O = \{X_1^a X_2^b, X_1^{a+u} X_2^{b-v}\} \subseteq \mathcal{M}(q, s)$ um conjunto ótimo de tamanho 2. Provemos que O é um conjunto denso ou a partir de O, construíremos um conjunto ótimo e denso relacionado a $E(s)$.

Observe que não podemos ter simultaneamente $-u, v < 0$ nem $-u, v > 0$. De fato, se $-u, v < 0$, então tomando $X_1^{a+u} X_2^b \in \mathcal{M}(q, s)$ temos que $\{X_1^{a+u} X_2^b, X_1^{a+u} X_2^{b-v}\} \subseteq \mathcal{M}(q, s)$ é tal que

$$\#(\Delta(X_1^{a+u} X_2^b, X_1^{a+u} X_2^{b-v}, X_1^q, X_2^q)) > \#(\Delta(X_1^a X_2^b, X_1^{a+u} X_2^{b-v}, X_1^q, X_2^q)),$$

logo $\{X_1^a X_2^b, X_1^{a+u} X_2^{b-v}\}$ não é ótimo, o que é um absurdo.

Analogamente, se $-u, v > 0$ então tomando $X_1^a X_2^{b-v} \in \mathcal{M}(q, s)$ temos que $\{X_1^a X_2^b, X_1^a X_2^{b-v}\} \subseteq \mathcal{M}(q, s)$ é tal que

$$\#(\Delta(X_1^a X_2^b, X_1^a X_2^{b-v}, X_1^q, X_2^q)) > \#(\Delta(X_1^a X_2^b, X_1^{a+u} X_2^{b-v}, X_1^q, X_2^q)),$$

logo $\{X_1^a X_2^b, X_1^{a+u} X_2^{b-v}\}$ não é ótimo, o que é um absurdo.

Podemos assumir sem perda de generalidade que $u, v \geq 0$. Primeiro, vamos analisar o caso em que $u = 0$ ou $v = 0$, e sem perda de generalidade vamos supor que $u = 0$ e $v > 0$, ou seja $O = \{X_1^a X_2^b, X_1^a X_2^{b-v}\}$. Temos que $\mathrm{MDC}(X_1^a X_2^b, X_1^a X_2^{b-v}) = X_1^a X_2^{b-v}$, e também vale que

$$\{X_1^{b_1} X_2^{b_2} \in \Delta(X_1^a X_2^b, X_1^a X_2^{b-v}, X_1^q, X_2^q) \mid b_1 \geq a,\ b_2 \geq b - v\} = \emptyset \subseteq \mathcal{M}(q, s),$$

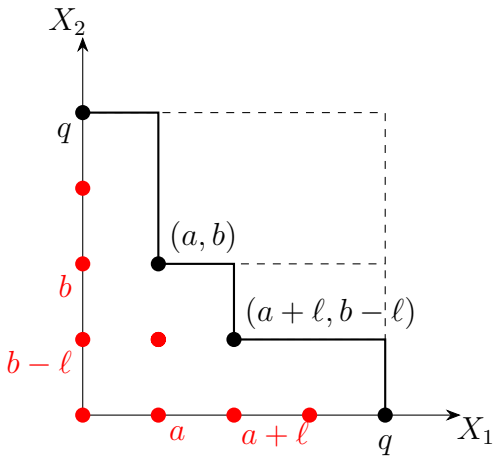
logo O é um conjunto denso relacionado a $E(s)$ e o resultado está provado.

Sejam $u, v \geq 1$. Se $u = v =: \ell$ então $O = \{X_1^a X_2^b, X_1^{a+\ell} X_2^{b-\ell}\}$. Como $X_1^{a+\ell} X_2^{b-\ell} \in \Delta(I)$, então

$$1 \leq \ell \leq q - 1 - a. \tag{4.6}$$

Observe que

$$\begin{aligned} \#(\Delta(X_1^a X_2^b, X_1^{a+\ell} X_2^{b-\ell}, X_1^q, X_2^q)) &= q^2 - (q-a)(q-b) - \ell(q-a-\ell) \\ &= (aq + bq - ab) - (q-a)\ell + \ell^2. \end{aligned} \tag{4.7}$$



Observe que $(aq+bq-ab)-(q-a)\ell+\ell^2$ como um polinômio em ℓ de grau dois, com ℓ no intervalo $[1, q-a-1]$. Assim, derivando e igualando a zero obtemos $-(q-a)+2\ell=0$ e, portanto, $\ell=\frac{q-a}{2}$ é um ponto crítico e além disso, é um ponto de mínimo global, pois derivando novamente temos que a segunda derivada é positiva. Esse valor (possivelmente não inteiro) de ℓ está situado precisamente no centro do intervalo $[1, q-1-a]$. Como o gráfico de $(aq+bq-ab)-(q-a)\ell+\ell^2$ é uma parábola, $\frac{q-a}{2}$ é um ponto de mínimo global, temos que o conjunto O é um conjunto ótimo, de tamanho 2, quando $\ell=1$.

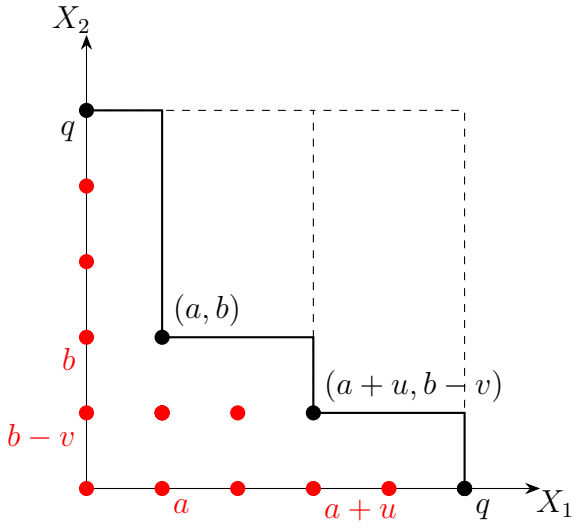
Afirmamos ainda que $O'=\{X_1^aX_2^b, X_1^{a+1}X_2^{b-1}\}$ é um conjunto denso relacionado a $E(s)$. Temos que $\mathrm{MDC}(X_1^aX_2^b, X_1^{a+1}X_2^{b-1})=X_1^aX_2^{b-1}$, e mais ainda, que

$$\{X_1^{b_1}X_2^{b_2}\in\Delta(O', X_1^q, X_2^q)\mid b_1\geq a,\ b_2\geq b-1\}=\{X_1^aX_2^{b-1}\}\subseteq\mathcal{M}(q,s),$$

então O' é denso. Portanto, para o caso $u=v=\ell$, o resultado também está provado.

Para finalizar, suponha sem perda de generalidade que $0<v<u$. Primeiro, temos que

$$\begin{aligned}\#(\Delta(X_1^aX_2^b, X_1^{a+u}X_2^{b-v}, X_1^q, X_2^q)) &= q^2-(q-(a+u))(q-(b-v))-u(q-b)\\ &\leq q^2-(q-a-u)(q-b+v)-(q-b)-v(q-b). \qquad (4.8)\end{aligned}$$



Defina o conjunto

$$O''\coloneqq\{X_1^{a+u-1}X_2^{b-v}, X_1^{a+u}X_2^{b-v}\}\subseteq\mathcal{M}(q,s).$$

Afirmamos que O'' é denso. Com efeito, $\mathrm{MDC}(X_1^{a+u-1}X_2^{b-v}, X_1^{a+u}X_2^{b-v}) = X_1^{a+u-1}X_2^{b-v}$ e temos que

$$\{X_1^{b_1}X_2^{b_2} \in \Delta(O'', X_1^q, X_2^q) \mid b_1 \geq a+u-1,\, b_2 \geq b+v\} = \emptyset \subseteq \mathcal{M}(q,s),$$

provando a afirmação.

Como $X_1^a X_2^b \in \Delta(I)$ então $b \leq q-1$. Daí,

$$\begin{aligned}\#(\Delta(X_1^{a+u-1}X_2^{b-v}, X_1^{a+u}X_2^{b-v}, X_1^q, X_2^q)) &= q^2 - (q-a-u)(q-b+v) - (q-b) - u \\ &\geq q^2 - (q-a-u)(q-b+v) - (q-b) - v(q-b) \qquad (4.9)\end{aligned}$$

e, portanto, comparando 4.8 e 4.9, como O é um conjunto ótimo então O'' também é ótimo. □

Proposição 4.4.2. *Considere $m = 2$. O segundo peso generalizado de Hamming de um código hiperbólico $E(s)$ de dimensão pelo menos 2 é igual a*

$$d_2 = q^2 - \eta_2(q, s, 2).$$

Demonstração. O resultado segue diretamente do Teorema 4.3.5 e do Lema 4.4.1. □

Referências Bibliográficas

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

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

[3] 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.

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

[5] GEIL, O.; HØHOLDT, T. **On Hyperbolic Codes.** In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC 2001). Lecture Notes in Computer Science, vol. 2227. Berlin: Springer, p. 159-171, 2001. DOI: https://doi.org/10.1007/3-540-45624-4_17.

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

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