BRUNO ANDRADE DE SOUZA

UMA FAMÍLIA DE CÓDIGOS LOCALMENTE RECUPERÁVEIS CONTENDO CÓDIGOS ÓTIMOS

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA ELÉTRICA
2022

BRUNO ANDRADE DE SOUZA

UMA FAMÍLIA DE CÓDIGOS LOCALMENTE RECUPERÁVEIS CONTENDO CÓDIGOS ÓTIMOS

Tese apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **DOUTOR EM CIÊNCIAS.**

Área de Concentração: Processamento da Informação.
Linha de Pesquisa: Processamento Digital de Sinais.

Orientador: Prof. Dr. Antônio Cláudio Paschoarelli Veiga
Coorientador: Prof. Dr. Victor Gonzalo Lopez Neumann.

UBERLÂNDIA - MG
2022

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

S729 Souza, Bruno Andrade de, 1989-
2022 Uma famÍlia de cˆdigos localmente recuperÆveis contendo cˆdigos tÍmos [recurso eletrÙnico] / Bruno Andrade de Souza. - 2022.

Orientador: AntÙnio ClÆudio Paschoarelli Veiga.
Coorientador: Victor Gonzalo Lopez Neumann.
Tese (Doutorado) - Universidade Federal de UberlÙndia, PÚs-graduaªo em Engenharia ElØtrica.
Modo de acesso: Internet.
Disponˆvel em: http://doi.org/10.14393/ufu.te.2022.575
Inclui bibliografia.
Inclui ilustraıes.

1. Engenharia elØtrica. I. Veiga, AntÙnio ClÆudio Paschoarelli ,1963-, (Orient.). II. Neumann, Victor Gonzalo Lopez,1974-, (Coorient.). III. Universidade Federal de UberlÙndia. PÚs-graduaªo em Engenharia ElØtrica. IV. TÌtulo.

CDU: 621.3

BibliotecÆrios responsÆveis 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 Engenharia Elétrica
Av. João Naves de Ávila, 2121, Bloco 3N - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4707 - www.posgrad.feelt.ufu.br - copel@ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Engenharia Elétrica				
Defesa de:	Tese de Doutorado, 305, PPGEELT				
Data:	Trinta de setembro de dois mil e vinte e dois	Hora de início:	09:00	Hora de encerramento:	13:00
Matrícula do Discente:	11713EEL003				
Nome do Discente:	Bruno Andrade de Souza				
Título do Trabalho:	Uma família de códigos localmente recuperáveis contendo códigos ótimos				
Área de concentração:	Processamento da Informação				
Linha de pesquisa:	Processamento Digital de Sinais				
Projeto de Pesquisa de vinculação:	Coordenador do projeto: Antônio C. P. Veiga Título do projeto: Aplicações de Rádio Definido por Software em receptores digitais e como ferramenta educacional Agência financiadora: não possui Número do processo na agência financiadora: Vigência do projeto: ativo				

Reuniu-se por meio de videoconferência, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Engenharia Elétrica, assim composta: Professores Doutores: Gilberto Arantes Carrijo - FEELT/UFU; Cicero Fernandes de Carvalho - FAMAT/UFU; Luciane Quoos Conte - UFRJ; Wanderson Tenório - UFMT; Victor Gonzalo Lopez Neumann - FAMAT/UFU, coorientador do(a) candidato(a).

Iniciando os trabalhos o(a) presidente da mesa, Dr(a). Victor Gonzalo Lopez Neumann, em observância ao art. 64, §4º, da Resolução CONPEP nº 17, de 09 de junho de 2022, que veda a participação concomitante de orientadores e coorientadores em bancas, apresentou a Comissão Examinadora e o candidato(a), agradeceu a presença do público, e concedeu ao Discente a palavra para a exposição do seu trabalho. A duração da apresentação do Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

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

Aprovado(a).

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

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 **Luciane Quoos Conte**, **Usuário Externo**, em 05/10/2022, às 09:14, 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 **Wanderson Tenório**, **Usuário Externo**, em 05/10/2022, às 14:48, 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 05/10/2022, às 15:53, 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 **Gilberto Arantes Carrijo**, **Professor(a) do Magistério Superior**, em 05/10/2022, às 19:40, 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 07/10/2022, às 16:43, 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 **3975789** e o código CRC **AE06C8CD**.

Referência: Processo nº 23117.070577/2022-91 SEI nº 3975789

À minha esposa Pâmela, meus filhos Miguel e Mattias, minha mãe Edivânia e meu pai Sergio.

Agradecimentos

Agradeço a Deus em primeiro lugar por todas as bençãos realizadas em minha vida.

À minha esposa Pâmela Augusta Mundim Ventura por todo amor, carinho, companheirismo e respeito. Agradeço por estar sempre ao meu lado nessa caminhada e não medir esforços para que eu conseguisse conquistar meus objetivos. A pessoa mais linda e generosa que Deus poderia ter colocado em minha vida.

Aos meus filhos Miguel Andrade Mundim Ventura e Mattias Andrade Mundim Ventura por serem a minha fonte de inspiração e encorajamento. Os presentes mais valiosos que Deus nos deu.

À minha mãe Edvânia Aragão Andrade que sempre correu por mim em todos os momentos. Obrigado por nunca me deixar desistir e sempre me incentivar a alcançar meus objetivos.

Ao meu pai Sergio Luiz de Souza por todos os ensinamentos e por ser minha referência.

Ao meu orientador Antônio Cláudio Paschoarelli Veiga por aceitar me orientar e não medir esforços para me ajudar.

Ao meu coorientador Victor Gonzalo Lopez Neumann, pela dedicação, disposição, ensinamentos e paciência durante esse período. Me sinto honrado por termos trabalhado juntos no Mestrado e no Doutorado.

À professora Luciane Quoos e aos professores Cícero Carvalho, Gilberto Carrijo e Wanderson Tenório por aceitarem o convite para compor a banca de avaliadores.

À Faculdade de Matemática da Universidade Federal de Uberlândia por todo apoio e por me concederem um afastamento de dois anos para que eu pudesse me dedicar ao Doutorado em tempo integral.

Ao programa de pós-graduação em Engenharia Elétrica da Universidade Federal de Uberlândia e todos os docentes e funcionários do programa.

Aos meus amigos de Andradina-SP, da graduação na UFMS, do mestrado na UFU e do trabalho na UFU-Patos de Minas, muito obrigado pela torcida e parceria durante toda minha trajetória.

Por fim, agradeço a todos que, direta ou indiretamente, contribuíram de alguma forma para minha formação.

"Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito. Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes."

— Marthin Luther King

SOUZA, B. A. *Uma família de códigos localmente recuperáveis contendo códigos ótimos,* 2022. 67 p. Tese de Doutorado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Códigos localmente recuperáveis foram introduzidos por Gopalan *et al.* em 2012 e no mesmo ano Prakash *et al.* introduziram o conceito de códigos com localidade, que são um tipo de códigos localmente recuperáveis. Neste trabalho, construímos uma nova família de códigos com localidade, que são subcódigos de uma certa família de códigos de avaliação. Calculamos a dimensão e também cotas para a sua distância mínima. Em alguns casos especiais, encontramos "códigos ótimos", segundo a definição dada por Prakash *et al.*

Palavras-chave: (Códigos Cartesianos Afins, Códigos Localmente Recuperáveis).

SOUZA, B. A. *A family of locally recoverable codes containing optmial codes*, 2022. 67 p. PhD Thesis, Federal University of Uberlândia, Uberlândia-MG.

Abstract

Locally recoverable codes were introduced by Gopalan *et al.* in 2012, and in the same year Prakash *et al.* introduced the concept of codes with locality, which are a type of locally recoverable codes. In this work we introduce a new family of codes with locality, which are subcodes of a certain family of evaluation codes. We determine the dimension of these codes, and also bounds for the minimum distance. We present the true values of the minimum distance in special cases, and also show that elements of this family are "optimal codes", as defined by Prakash *et al.*

Keywords: (Affin Cartesian Codes, Locally Recoverable Codes).

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

Como conseguir que uma mensagem transmitida chegue intacta ao seu destino final apesar de todo o ruído que possa atrapalhar a transmissão? Como podemos assegurar que a informação armazenada em um suporte físico não sofra alterações apesar da deterioração do material por desgaste ou mau uso? As respostas estão na codificação para detecção e correção de erros e é disto que trataremos em nosso trabalho.

A Teoria dos Códigos é um ramo da matemática de investigação atual e em pleno desenvolvimento, possuindo diversas ramificações que utilizam ferramentas da teoria dos números, teoria de grupos, combinatória, geometria algébrica, entre outras. Os códigos corretores de erros são utilizados sempre que se deseja transmitir ou armazenar dados. O assunto é muito interessante pois mescla conceitos e técnicas da álgebra abstrata com aplicações na vida real. Por exemplo, todos nós conhecemos os códigos de barras presentes em itens de supermercado, como este:

Figura 1: Exemplo de um código de barras dos supermercados.

Associada às barras sempre está uma sequência de algarismos como o da Figura 1. Esta sequência é dividida em grupos de dígitos que identificam certas características da mercadoria, como o país, a empresa e o produto. O algarismo isolado da direita é dito **dígito verificador ou de controle**. Ele serve para confirmar que o número do código de barras está correto através de um cálculo aritmético. O sistema internacional de numeração de produtos chama-se **EAN-13 (European Article Number,** 13 **dítigos)**.

Representando o número por

$$x_1x_2x_3 - x_4x_5x_6x_7x_8 - x_9x_{10}x_{11}x_{12} - c,$$

o dígito verificador é obtido através da seguinte fórmula:

$$\left[3 \times \sum_{i=1}^{6} x_{2i} + \sum_{i=1}^{6} x_{2_{i-1}} + c\right] \mod 10 = 0. \quad (1)$$

Por exemplo, a sequência $789 - 11510 - 3118 - 9$ identifica uma goma de mascar de uma determinada marca. Um dos requisitos principais para verificar se um código de barras é valido é efetuar o calculo do digito verificador. Utilizando a fórmula (1), temos:

$$3 \times (8 + 1 + 5 + 0 + 1 + 8) + (7 + 9 + 1 + 1 + 3 + 1) + (9) = 100.$$

Como $100 \mod 10 = 0$, concluímos que 9 é de fato o dígito verificador e o código de barras está correto.

Se por imperfeição de impressão, ou por outro motivo, o leitor óptico ou o caixa do supermercado errar a leitura do código de barras ou a digitação do número trocando, por exemplo, 2 algarismos como em $789 - 11510 - 1318 - 9$? Nesse caso, as operações aritméticas aplicadas a este número resultariam em

$$3 \times (8 + 1 + 5 + 0 + 3 + 8) + (7 + 9 + 1 + 1 + 1 + 1) + 9 = 104.$$

Como o resultado não é múltiplo de 10, como deveria, terá que se repetir a digitação porque houve um engano. Ou seja, este código de barras é um código detector de erros!

O matemático C. E. Shannon, em [27], fundou a Teoria dos Códigos na década de 40 e na mesma década, teve início a Teoria dos Códigos Corretores de Erros com os trabalhos de Golay [19] e Hamming [32]. A grande descoberta da época foram os modelos de códigos capazes de detectar e corrigir erros em um sistema de comunicação. Em [27], Shannon provou que, através de uma codificação apropriada da informação, os erros introduzidos por um canal ruidoso poderiam ser reduzidos a um nível desejado, sem sacrificar a taxa de transmissão. Desde então pesquisadores vêm buscando encontrar famílias de bons códigos e também projetar decodificadores eficientes para os mesmos.

A classe de códigos mais utilizada na prática é a classe dos códigos lineares, cuja definição é a seguinte: dado um corpo finito $\mathbb{F}_q$ com q elementos. Um código $\mathcal{C} \subset \mathbb{F}_q^m$, com m natural, é um código linear se for subespaço vetorial de $\mathbb{F}_q^m$.

Neste trabalho, estamos interessados em duas classes de códigos lineares, a saber:

- Os **Códigos Cartesianos Afins**, que apareceram pela primeira vez em um trabalho de O. Geil e C. Thomsen (ver [18]) como um caso especial dos chamados códigos Reed-Muller generalizados, e mais tarde apareceram de forma independente em um artigo de H. López et al. (ver [24]).

- Os **Códigos Localmente Recuperáveis (LRC)** que foram introduzidos por Gopalan et al. (ver [21]) e no mesmo ano Prakash et al. (ver [25]) propuseram o conceito de códigos com localidade (r, δ), também chamados de códigos (r, δ)-localmente recuperáveis que generalizam a definição de códigos localmente recuperáveis com localidade r.

Recentemente, os códigos que possuem a propriedade de serem localmente recuperáveis tornaram-se cada vez mais importantes e tem recebido muita atenção, pois são aplicados em sistemas de armazenamento distribuído e em nuvem.

Motivados pela sua importância e inspirados nos trabalhos supracitados, a contribuição do nosso trabalho consiste na construção de uma nova família de subcódigos dos códigos cartesianos afins que têm a propriedade de ser (r, δ)-localmente recuperáveis.

O nosso trabalho está estruturado da seguinte maneira

- No primeiro capítulo veremos conceitos e resultados básicos da teoria de códigos corretores de erros, tais como: distância miníma, dimensão e comprimento de um código. Apresentaremos também a cota de Singleton que é um resultado clássico desta teoria e apresentaremos alguns exemplos de códigos lineares, a saber: os códigos de Reed-Solomon e os códigos de Reed-Muller.

- No segundo capítulo introduziremos a teoria de bases de Gröbner e a pegada de um ideal. Para isso, recordaremos propriedades a respeito dos ideais monomiais e do algoritmo da divisão em um anel de polinômios em várias variáveis. Faremos a demonstração do teorema da base de Hilbert, definiremos as bases de Gröbner e apresentamos as suas principais propriedades. Finalizaremos este capítulo definindo a pegada de um ideal monomial.

- Começaremos o terceiro capítulo definindo as variedades afins e as relacionando com a pegada de um ideal monomial. Em seguida, apresentaremos a construção dos códigos cartesianos afins e alguns resultados importantes sobre esses códigos.

- No quarto e último capítulo estão as nossas contribuições. Apresentaremos o conceito de códigos (r, δ)-localmente recuperáveis e alguns resultados interessantes sobre esta classe de códigos. Em seguida, definiremos uma família de subcódigos dos códigos cartesianos afins (ver Definição 3.2.3) que são (r, δ)-localmente recuperáveis. Determinaremos a dimensão (ver Corolário 4.2.2 e Teorema 4.2.4) juntamente com as cotas inferior e superior para a distância mínima (ver Teorema 4.3.1). Listaremos alguns casos onde os códigos são "ótimos"(ver Corolário 4.3.2) e também determinaremos o valor exato da distância mínima em alguns casos especiais do código (ver Teorema 4.3.1, Teorema 4.4.8 e Corolário 4.4.9). Terminaremos o capítulo com alguns exemplos numéricos e algumas comparações dos nossos códigos com códigos presentes na literatura.

Bruno Andrade de Souza
Uberlândia-MG, 30 de Setembro de 2022.

CAPÍTULO 1

CÓDIGOS CORRETORES DE ERROS

Nesta capítulo traremos os conceitos básicos da teoria dos códigos corretores, para que possamos apresentar a construção de diferentes códigos nos capítulos posteriores. Para o leitor menos familiarizado com estes conceitos, uma sugestão é que consulte qualquer livro sobre códigos corretores. Uma recomendação é a referência [23] que foi utilizada para escrever este capítulo.

1.1 Códigos Corretores

De certa maneira, podemos dizer que a construção dos códigos corretores foi inspirada no mais utilizado dos códigos pelos seres humanos: o idioma.

Na língua portuguesa, o "alfabeto" $\mathcal{A}$ é formado por 26 letras, bem como o espaço em branco considerado como letra, a cedilha e as vogais acentuadas. Uma palavra da língua portuguesa pode ser considerada um elemento de $\mathcal{A}^{46}$, onde 46 é o comprimento da palavra mais longa da língua portuguesa, supostamente **Pneumoultramicroscopicossilicovulcanoconiótico**.

Claramente, a nossa língua não é composta por todas as "palavras" possíveis formadas a partir das letras, isto é, reconhecemos algumas delas como pertencentes a língua e outras não.

Desse modo, os elementos básicos para a construção de um código são os seguintes:

- Um conjunto finito $\mathcal{A}$ chamado **alfabeto**. Denotaremos por $|\mathcal{A}| = q$ o número de elementos do alfabeto, neste caso, diz-se que o código é **q-ário**. Por exemplo, códigos em que o alfabeto é $\mathbb{Z}_2 = \{0, 1\}$ são ditos códigos binários.
- Sequências finitas de símbolos do alfabeto são chamadas de **palavras** e o número de letras de uma palavra é o seu **comprimento**. Para termos um código de fácil manejo, convencionamos que todas as palavras tenham o mesmo comprimento n.
- Um **código** q**-ário** de comprimento n e um subconjunto qualquer de palavras de comprimento n, isto é, um código $\mathcal{C}$ é um subconjunto $\mathcal{C} \subset \mathcal{A}^n$

Exemplo 1.1.1. *Considere* $\mathbb{Z}_2 = \{0, 1\}$ *como sendo o alfabeto. O Conjunto*

$$\mathcal{C} = \{00000, 01011, 10110, 11101\}$$

é um código binário, de comprimento $n = 5$.

Considerando o alfabeto como sendo $\mathbb{Z}_3 = \{0, 1, 2\}$*, então o conjunto*

$$\mathcal{C} = \{00012, 11022, 10110, 10121, 20202\}$$

é um código ternário, de comprimento $n = 5$.

Atualmente, sempre que se deseja transmitir ou armazenar dados garantindo a sua confiabilidade, utilizamos os códigos corretores de erros. São exemplos disso todas as comunicações via satélite, o armazenamento de dados em nuvem, as comunicações internas de um computador, etc. Vejamos um exemplo para ilustrar os princípios dessa teoria.

Exemplo 1.1.2. *Nos jogos de videogame antigos, os movimentos eram limitados. Por exemplo, no jogo do Bomberman, o boneco se move em um tabuleiro quadriculado, de modo que, ao darmos um dos comandos (direita, esquerda, cima ou baixo), o Bombarman se desloca do centro de uma casa para o centro da casa indicada pelo comando. Ao criar um controle para este jogo, podemos codificar os quatro comandos como elementos de* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *da seguinte forma:*

$$\begin{array}{ll} \textit{Direita} \to (0,0) & \textit{Cima} \to (1,0) \\ \textit{Esquerda} \to (0,1) & \textit{Baixo} \to (1,1). \end{array}$$

O código do lado direito na tabela acima é dito ***código da fonte****. Suponha que esses pares ordenados foram transmitidos e que o sinal no caminho sofra interferências. Imagine que a mensagem* $(0,0)$ *possa, na chegada, ser recebida como* $(0,1)$*, fazendo com que o Bomberman se desloque para Esquerda ao invés de ir para Direita.*

É necessário modificar as palavras, de modo a introduzir redundâncias que permitam detectar e corrigir erros.

Por exemplo, podemos modificar este código da seguinte forma:

$$\begin{array}{l} (0,0) \to (0,0,0,0,0) \\ (0,1) \to (0,1,0,1,1) \\ (1,0) \to (1,0,1,1,0) \\ (1,1) \to (1,1,1,0,1) \end{array}$$

Desse modo, as duas primeiras posições reproduzem o código da fonte, enquanto que as três restantes são redundâncias introduzidas. O novo código introduzido na recodificação é dito ***código de canal****.*

Agora, se na mensagem transmitida ocorrer um erro de digitação, somos capazes de descobrir o erro e corrigi-lo, o que não era possível anteriormente.

Por exemplo, se ao transmitirmos a palavra $(1,0,1,1,0)$*, a mensagem recebida for* $(1,1,1,1,0)$*. Comparando essa mensagem com as palavras do código, observamos que ela não lhe pertence, logo, detectamos erros. A palavra mais próxima (a que tem menor número de componentes diferentes) é* $(1,0,1,1,0)$*.*

Vimos que, a transmissão de dados em código entre um emissor e receptor nem sempre é feita. No processo, podem ocorrer erros que mudam a mensagem enviada. Esta situação foi descrita por *Shannon*, utilizando o seguinte esquema:

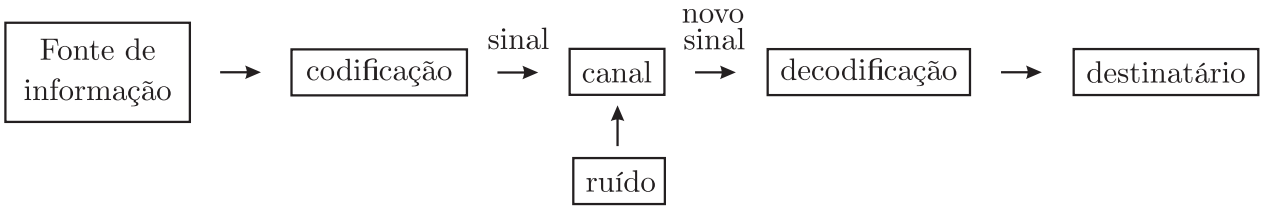

Figura 1.1: Processo de transmissão de informação

A idéia básica da teoria dos códigos corretores de erros é codificar a informação inicial, adicionando informação redundante, de modo que, ao receber o sinal modificado pelo "ruído", seja possível de alguma forma recuperar a mensagem original.

Retornando ao exemplo da língua portuguesa, suponha que recebemos uma mensagem com a palavra *profxssor*. É imediato que a mensagem contém um erro, pois não a reconhecemos como uma palavra do nosso alfabeto (é isto que fazem os programas editores de texto com correção ortográfica, que comparam cada palavra escrita com as que constam no seu dicionário interno). Mais ainda, achamos que a palavra correta deve ser a palavra *professor*, pois é a palavra da língua que mais "se aproxima" da palavra recebida.

Por outro lado, se recebemos a palavra *wato* também reconhecemos que está errada, porém, percebemos que existem várias possibilidades de correção, isto é, palavras "próximas" desta, como por exemplo, *rato*, *pato*, *gato*, etc.

Consideraremos que, ao receber um elemento y, podemos detectar se ele contém erro, ou não, se temos um critério bem definido para decidir se y pertence, ou não, a $\mathcal{C}$.

Uma vez detectado um erro, nosso critério de correção será substituir o elemento y, pelo elemento x do código $\mathcal{C}$ que seja mais próximo de y. Para isso, será necessário que não haja ambiguidades de um tal elemento.

Estas observações podem ser expressas em linguagem mais rigorosa e nos levarão aos primeiros resultados da teoria dos códigos. Para tornar precisa a noção intuitiva de proximidade entre palavras que utilizamos anteriormente, apresentamos a seguir um modo de medir a distância entre palavras em $\mathcal{A}^n$

Definição 1.1.3. *Dados dois elementos $u = (u_1, u_2, \ldots, u_n)$ e $v = (v_1, v_2, \ldots, v_n)$ de $\mathcal{A}^n$, chama-se* ***distância de Hamming*** *de u e v ao número de coordenadas que estas diferem, isto é:*

$$d(u, v) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}|.$$

Dado um código $\mathcal{C} \subset \mathcal{A}^n$, chama-se ***distância mínima de $\mathcal{C}$*** *o número*

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

Note que, de acordo com a sua definição, a distância de Hamming é sempre um número inteiro.

Exemplo 1.1.4. *Em $\mathbb{Z}_2^3$, temos:*

$$d(001, 111) = 2;$$
$$d(000, 111) = 3;$$
$$d(100, 110) = 1.$$

Observação 1.1.5. *A distância de Hamming é uma métrica sobre $\mathcal{A}^n$, isto é, dados $u, v, w \in \mathcal{A}^n$, valem as seguintes propriedades:*

(i) $d(u, v) \geq 0$, *valendo a igualdade se, e só se,* $u = v$;

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

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

Podemos definir agora os conceitos de bola e esfera em $\mathcal{A}^n$, bem como é feito em espaços métricos.

Definição 1.1.6. *Dado um elemento $x \in \mathcal{A}^n$ e um inteiro positivo r, chama-se* ***bola centrada em x e raio*** *r, o conjunto*

$$B(x, r) = \{u \in \mathcal{A}^n : d(u, x) \leq r\}$$

e ***esfera centrada em x e raio*** *r, o conjunto*

$$S(x, r) = \{u \in \mathcal{A}^n : d(u, x) = r\}.$$

Definição 1.1.7. *Seja $\mathcal{C}$ um código com distância mínima $d_{\min}$, defina $\kappa = \left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$, onde $\lfloor t \rfloor$ representa a parte inteira de um número real t. O número k é dito* ***capacidade*** *de $\mathcal{C}$.*

Teorema 1.1.8. *Seja $\mathcal{C}$ um código com distância mínima $d_{\min}$. Então $\mathcal{C}$ pode corrigir até $\kappa = \left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$ erros e detectar até $d_{\min} - 1$ erros.*

Demonstração. Seja $x \in \mathcal{C}$ e suponhamos que ele foi recebido como um outro elemento y, com $t \leq d_{\min} - 1$ erros. Como o número t de erros acontecidos é exatamente a distância de Hamming de x a y, temos que $d(x, y) \leq d_{\min} - 1 < d_{\min}$. Isso implica que $y \notin \mathcal{C}$, e portanto, o erro pode ser detectado.

Suponha ainda que o número t de erros cometidos é menor que κ. Considere a bola $B(y, k)$. Como $d(x, y) = t \leq k$ temos que $x \in B(y, k)$. Afirmamos que x é o único elemento de $\mathcal{C}$ contido nessa bola. De fato, se existisse outro elemento $x' \in \mathcal{C}$ em $B(y, k)$, teríamos que

$$d(x, x') \leq d(x, y) + d(y, x') \leq 2k < d_{\min},$$

ABSURDO! Portanto, x é o elemento de $\mathcal{C}$ mais próximo de y e é possível corrigir o erro.

□

O processo que cada palavra r, recebida eventualmente com erros, associa uma palavra corrigida c no código é chamado é **decodificação.**

Observação 1.1.9. *Em virtude do teorema anterior, um código terá maior capacidade de corrigir erros quanto maior for a sua distância mínima. Portanto, é fundamental para a Teoria dos Códigos, poder calcular $d_{\min}$ ou pelo menos determinar uma cota inferior para ele.*

1.2 Códigos Lineares

De agora em diante, o alfabeto $\mathcal{A}$ será um corpo finito com q elementos, denotado por $\mathbb{F}_q$. Temos, portanto, para todo número natural n, um $\mathbb{F}_q$-espaço vetorial, de dimensão n, a saber: $\mathbb{F}_q^n$.

Definição 1.2.1. *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código. Dizemos que $\mathcal{C}$ é um* ***código linear*** *se for um subespaço vetorial de $\mathbb{F}_q^n$.*

Definição 1.2.2. *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear e k a dimensão de $\mathcal{C}$ como $\mathbb{F}_q$- espaço vetorial. O comprimento n, a distância mínima $d_{\min}$ e a dimensão k são ditos* ***parâmetros*** *do código $\mathcal{C}$.*

Um código com tais parâmetros é dito código $[n, k, d]_q$ ou $[n, k, d]$-código.

Vejamos a importância desses parâmetros. Seja $\mathcal{B} = \{v_1, v_2, \ldots, v_k\}$ uma base de $\mathcal{C}$, onde $\mathcal{C} \subseteq \mathbb{F}_q^n$ é um código linear tal que k é a dimensão de $\mathcal{C}$ como $\mathbb{F}_q$-espaço vetorial. Desse modo, se $v \in \mathcal{C}$, então existem (únicos) $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{F}_q$ tais que

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k.$$

Segue que o número de palavras em $\mathcal{C}$ é q^k. Assim, quanto maior for a dimensão, maior será o número de palavras de $\mathcal{C}$. Temos também que, quanto maior for a distância mínima $d_{\min}$, maior será a capacidade de detectar e corrigir erros. Assim, quanto maiores forem $d_{\min}$ e k melhor, porém, temos a seguinte relação entre os parâmetros:

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

Tal relação é dita **cota de Singleton** e sua demonstração pode ser encontrada no capítulo 10 da referência [23].

Portanto, o código ideal teria dimensão e distância mínima grandes, com comprimento curto, mas estas condições não podem ser satisfeitas ao mesmo tempo, dada a cota de Singleton.

Códigos com $d_{\min} = n-k+1$ são chamados de **códigos de máxima distância separável** ou **MDS (de Maximum Distance Separable)**.

Definição 1.2.3. *Dado $v \in \mathbb{F}_q^n$, definimos o **peso de** v como sendo o número inteiro*

$$w(v) := |\{i : x_i \neq 0\}|.$$

Em outras palavras, temos que

$$w(v) = d(v, 0),$$

onde d representa a métrica de Hamming.

Definição 1.2.4. *O **peso de um código linear** $\mathcal{C}$ é o inteiro*

$$w(\mathcal{C}) := \min\{w(v) : v \in \mathcal{C}\backslash\{0\}\}.$$

Proposição 1.2.5. *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear com distância mínima $d_{\min}$. Então*

(i) $d(u, v) = w(u - v)$, *para todo* $u, v \in \mathbb{F}_q^n$.

(ii) $d_{\min} = w(\mathcal{C})$.

Demonstração. (i) De fato, para todo $u, v \in \mathbb{F}_q^n$, temos

$$\begin{aligned} w(u-v) &= |\{i : u_i - v_i \neq 0, 1 \leq i \leq n\}| \\ &= |\{i : u_i \neq v_i, 1 \leq i \leq n\}| \\ &= d(u, v) \end{aligned}$$

Em (ii), para todo $u, v \in \mathcal{C}$, com $u \neq v$, segue-se que $z = u - v \in \mathcal{C}\backslash\{0\}$. Logo,

$$\begin{aligned} d_{\min} &= \min\{i : u_i \neq v_i, 1 \leq i \leq n\} \\ &= \min\{i : u_i - v_i \neq 0, 1 \leq i \leq n\} \\ &= \min\{i : z_i \neq 0, 1 \leq i \leq n\} \\ &= \min\{w(z) : z \in \mathcal{C}\backslash\{0\}\} \\ &= w(\mathcal{C}). \end{aligned}$$

□

Observação 1.2.6. *Podemos encontrar $d_{\min}$ a partir de $q^k - 1$ cálculos de distância, em vez de $\binom{q^k}{2}$ que devemos fazer comparando palavra por palavra de um código linear. Na prática, em códigos grandes, esse método para calcular $d_{\min}$ é inviável, pois representa um alto custo computacional. Portanto, teremos que desenvolver outros métodos para determinar (ou pelo menos estimar) a distância mínima de um código.*

Em virtude do item (ii) da Proposição 1.2.5, a distância mínima de um código linear $\mathcal{C}$ será chamada também de **peso do código** $\mathcal{C}$.

Definição 1.2.7. *(i) Dizemos que uma função $F : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ é uma **isometria linear** de $\mathbb{F}_q^n$ se, ela é uma transformação linear que preserva distâncias de Hamming, isto é,*

$$d(F(a), F(b)) = d(a, b), \text{ para todo } a, b \in \mathbb{F}_q^n.$$

(ii) Sejam $\mathcal{C}$ e $\mathcal{C}'$ dois códigos lineares em $\mathbb{F}_q^n$. Dizemos que $\mathcal{C}'$ é equivalente a $\mathcal{C}$ quando existe uma isometria linear F, de $\mathbb{F}_q^n$, tal que $F(\mathcal{C}) = C'$.

Definição 1.2.8. *Seja $\beta = \{v_1, v_2, \ldots, v_k\}$ uma base ordenada de $\mathcal{C}$ e considere a matriz G, cujas linhas são os vetores $v_i = \{v_{i1}, v_{i2}, \ldots, v_{in}\}$, com $i = 1, \ldots, k$, isto é,*

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}.$$

*A matriz G é dita **matriz geradora** de um código $\mathcal{C}$ associada à base β.*

Considere a transformação linear definida por

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ & x & \longmapsto & xG \end{array}.$$

Seja $x = (x_1, \ldots, x_k)$, temos que

$$T(x) = xG = x_1 v_1 + \ldots + x_k v_k,$$

logo $T(\mathbb{F}_q^k) = \mathcal{C}$. Desse modo, podemos considerar que $\mathbb{F}_q^k$ é o código da fonte, $\mathcal{C}$ o código do canal e a transformação T, uma codificação.

Observe que a matriz G não é univocamente determinada por $\mathcal{C}$, pois ela depende da escolha da base β.

Inversamente, podemos construir códigos a partir de matrizes geradoras G. Para isso, basta tomar uma matriz cujas linhas são linearmente independentes e definir um código como sendo a imagem da transformação linear

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ & x & \longmapsto & xG. \end{array}$$

Exemplo 1.2.9. *Considere $\mathbb{F}_2$ e seja*

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

Considere a transformação linear

$$\begin{array}{rccc} T: & \mathbb{F}_2^3 & \longrightarrow & \mathbb{F}_2^5 \\ & x & \longmapsto & xG \end{array}.$$

Obtemos um código $\mathcal{C}$ em $\mathbb{F}_2^5$, imagem de T. Por exemplo, a palavra 101 do código da fonte é codificada como 01010. Suponhamos agora que seja dada a palavra 10101 do código, e que gostaríamos de decodificá-la, ou seja, encontrar a palavra x de $\mathbb{F}_2^3$ da qual ela se origina por meio da transformação T. Teríamos que resolver o seguinte sistema:

$$\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} G = (10101),$$

ou seja,

$$\begin{cases} x_1 + x_2 + x_3 &= 1 \\ x_2 + x_3 &= 0 \\ x_1 + x_3 &= 1 \\ x_2 + x_3 &= 0 \\ x_1 + x_3 &= 1 \end{cases},$$

cuja solução é $x_1 = 1$, $x_2 = 0$ e $x_3 = 0$.

Esse sistema de equações foi fácil de se resolver, mas, em geral, se a matriz G for mais complexa, a resolução do sistema de equações associado pode ser bem trabalhosa. No entanto, se efetuarmos operações sobre as linhas de G, podemos colocar G na forma

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

Observe que

$$xG' = \begin{pmatrix} x_1 & x_2 & x_3 & x_2 & x_1 \end{pmatrix}$$

e, portanto, obtemos o valor de x tomando apenas as três primeiras entradas do vetor a ser decodificado. Assim, a palavra (10101) é facilmente decodificada como (101).

Definição 1.2.10. *A matriz geradora de um código linear $\mathcal{C}$ na **forma padrão** será a matriz: $G' = (Id_k|A)$, em que Id_k é a matriz identidade $k \times k$ e A, uma matriz $k \times (n-k)$.*

Teorema 1.2.11. *Dado um código $\mathcal{C}$, existe um código equivalente $\mathcal{C}'$ com matriz geradora na forma padrão.*

Demonstração. Seja G uma matriz geradora de $\mathcal{C}$ associada à base $\beta = \{g_1, \ldots, g_i, \ldots, g_j, \ldots, g_k\}$, onde $g_r = (g_{r1}, \ldots, g_{ri}, \ldots, g_{rj}, \ldots, g_{rn})$ para cada $r = 1, \ldots, k$.

Mostraremos que com uma sequência de operações do tipo $(L1)$, $(L2)$, $(L3)$ e $(C1)$ podemos colocar G na forma padrão, onde:

$(L1)$ Permutação de linhas;

$(L2)$ Multiplicação de uma linha por um escalar não nulo;

$(L3)$ Adição de um múltiplo escalar de uma linha a outra;

$(C1)$ Permutação de colunas.

Primeiramente, veja que as operações $L1$, $L2$ e $L3$ não alteram o código. Com efeito, se $\beta = \{g_1, \ldots, g_i, \ldots, g_j, \ldots, g_k\}$ é uma base de $\mathcal{C}$, então $\beta_1 = \{g_1, \ldots, g_j, \ldots, g_i, \ldots, g_k\}$, $\beta_2 = \{g_1, \ldots, \alpha g_i, \ldots, g_k\}$ e $\beta_3 = \{g_1, \ldots, g_i, \ldots, g_j + \alpha g_i, \ldots, g_k\}$ também são bases do código $\mathcal{C}$, onde $\alpha \in \mathbb{F}_q$. Assim, ao realizar a operação L_p em G, obtém-se a matriz G_p, que a matriz geradora do código C associada à base β_p, para cada $p = 1, 2, 3$. Logo, realizar estas operações em G não alteram o código $\mathcal{C}$.

Notemos agora que, ao aplicar a operação $(C1)$ em G, obtemos uma matriz G' que gera um código $\mathcal{C}'$ equivalente a $\mathcal{C}$.

Suponha que

$$G = \begin{pmatrix} g_{11} & \cdots & g_{1i} & \cdots & g_{1j} & \cdots & g_{1n} \\ \vdots & & & \vdots & & & \vdots \\ g_{k1} & \cdots & g_{ki} & \cdots & g_{kj} & \cdots & g_{kn} \end{pmatrix}$$

e que a operação $(C1)$ permuta as colunas i e j da matriz G.

Daí, obtemos a matriz

$$G' = \begin{pmatrix} g_{11} & \cdots & g_{1j} & \cdots & g_{1i} & \cdots & g_{1n} \\ \vdots & & & \vdots & & & \vdots \\ g_{k1} & \cdots & g_{kj} & \cdots & g_{ki} & \cdots & g_{kn} \end{pmatrix}.$$

Como as linhas de G são linearmente independentes, segue que as linhas de G' também o são. Podemos então considerar o código $\mathcal{C}'$ gerado por esta matriz.

Vejamos que $\mathcal{C}'$ é equivalente a $\mathcal{C}$, para isto, consideremos a seguinte isometria linear

$$T : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n,$$

definida por

$$T(g_{r1}, \ldots, g_{ri}, \ldots, g_{rj}, \ldots, g_{rn}) = (g_{r1}, \ldots, g_{rj}, \ldots, g_{ri}, \ldots, g_{rn}).$$

Assim, $\beta' = \{T(g1), \ldots, T(g_k)\}$ é a base de $T(\mathcal{C})$ e de $\mathcal{C}'$.

Portanto, T é uma isometria linear entre $\mathcal{C}$ e $\mathcal{C}'$, ou seja, estes códigos são equivalentes.

Além disso, segue que a composição de operações $(L1)$, $(L2)$, $(L3)$, e $(C1)$ continua resultando em um código equivalente a C.

Agora, vejamos como obter um código $\mathcal{C}'$ equivalente a $\mathcal{C}$ cuja matriz geradora está na forma padrão.

Como as linhas de G são linearmente independentes, podemos supor $g_{11} \neq 0$ via $(C1)$. Multiplicando a primeira linha pelo inverso de g_{11}, teremos o primeiro elemento da matriz igual a 1. Daí, multiplicando por $-g_{i1}$ a primeira linha e somando com a i-ésima linha, para todo $i = 2, \ldots, k$, teremos a seguinte matriz

$$\begin{pmatrix} 1 & b_{12} & \cdots & b_{1n} \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & b_{k2} & \cdots & b_{kn} \end{pmatrix}.$$

Certamente, ao menos um elemento da segunda linha dessa matriz é não nulo. Por meio da operação $(C1)$ este elemento pode ser colocado na segunda linha e segunda coluna. Multiplicando a segunda linha pelo inverso desse elemento, a matriz se transforma em

$$\begin{pmatrix} 1 & c_{12} & c_{13} & \cdots & c_{1n} \\ 0 & 1 & c_{23} & \cdots & c_{2n} \\ 0 & c_{32} & c_{33} & \cdots & c_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & c_{k2} & c_{k3} & \cdots & c_{kn} \end{pmatrix}.$$

Novamente, usando a operação $(L3)$, obtemos a matriz

$$\begin{pmatrix} 1 & 0 & d_{13} & \cdots & d_{1n} \\ 0 & 1 & d_{23} & \cdots & d_{2n} \\ 0 & 0 & d_{33} & \cdots & d_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & d_{k3} & \cdots & d_{kn} \end{pmatrix}.$$

E assim sucessivamente, até encontrarmos uma matriz na forma padrão

$$G' = (Id_k | A).$$

□

1.3 Códigos de Reed-Solomon

Para motivar os próximos capítulos, apresentaremos agora os códigos de Reed-Solomon sobre $\mathbb{F}_q$. Esta é uma importante classe de códigos bem conhecida na literatura. Tais códigos apareceram em 1960, quando foram definidos por Reed e Solomon em [31]. Vejamos como é feita a construção desses códigos.

Definição 1.3.1. *Seja $n = q-1$ e seja $\beta \in \mathbb{F}_q$ um elemento primitivo do grupo multiplicativo $\mathbb{F}_q^* = \{\beta, \beta^2, \ldots, \beta^n = 1\}$. Para $k \in \mathbb{Z}$, com $1 \leq k \leq n$, consideremos o espaço vetorial de dimensão k:*

$$\mathcal{L}_k := \{f \in \mathbb{F}_q[x] : grau(f) \leq k-1\} \cup \{0\}$$

e a aplicação $ev : \mathcal{L}_k \longrightarrow \mathbb{F}_q^n$ definida por:

$$ev(f) := (f(\beta), f(\beta^2), \ldots, f(\beta^n)) \in \mathbb{F}_q^n.$$

Esta aplicação é claramente $\mathbb{F}_q$-linear. Além disso, ev é injetora. De fato,

$$\ker ev = \{f \in \mathcal{L}_k : f(\beta) = \cdots = f(\beta^n) = 0\} = \{0\},$$

pois um polinômio não nulo f de grau menor que k, não pode ter n raízes distintas. Portanto,

$$\mathcal{C}_k := \{(f(\beta), f(\beta^2), \ldots, f(\beta^n)) : f \in \mathcal{L}_k\}$$

é um $[n,k]$-código sobre $\mathbb{F}_q$ dito **código de Reed-Solomon**.
O peso de uma palavra do código $c = ev(f) \in \mathcal{C}_k \setminus \{0\}$ é dado por:

$$\begin{aligned} w(c) &= |\{i \in \{1,\ldots,n\} : f(\beta^i) \neq 0\}| \\ &= n - |\{i \in \{1,\ldots,n\} : f(\beta^i) = 0\}| \\ &\geq n - grau(f) \\ &\geq n - (k-1) \\ &= n - k + 1. \end{aligned}$$

Logo, a distância mínima $d_{\min}$ do código $\mathcal{C}_k$ satisfaz

$$d_{\min} \geq n - k + 1. \tag{1.1}$$

Por outro lado, pela cota de Singleton, sabemos que

$$d_{\min} \leq n + 1 - k. \tag{1.2}$$

Portanto, juntando (1.1) e (1.2), obtemos

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

Assim, observe que os códigos de Reed-Solomon são códigos MDS.

1.4 Códigos de Reed-Muller

Os códigos de Reed-Muller (Ou RM) são uma das famílias mais antigas e mais estudadas de códigos. Estes códigos apareceram em 1954, quando foram definidos por Muller [29] e logo após foi dado um algoritmo de decodificação por Reed [30]. Tais códigos foram construídos inicialmente sobre $\mathbb{F}_2$ e em 1968 Kasami *et al.* em [20] estenderam a definição original para um corpo finito $\mathbb{F}_q$.

Definição 1.4.1. *Seja $\mathbb{F}_q$ um corpo finito com q elementos e n um inteiro positivo. Seja $d \in \mathbb{Z}$ tal que $1 \leq d \leq n(q-1)$. O* ***Código de Reed-Muller generalizado de ordem*** *d é o seguinte subespaço de $\mathbb{F}_q^{(q^n)}$:*

$$RM_q(d,n) = \{(f(x))_{x \in \mathbb{F}_q^n} : f \in \mathbb{F}_q[X_1, \ldots, x_n] \ \ e \ \ grau(f) \leq d\} \cup \{0\}.$$

Os parâmetros do código $RM_q(d,n)$ são:

(i) comprimento: $m = q^n$;

(ii) dimensão: $M = \sum_{t=0}^{d} \sum_{j=0}^{n} (-1)^j \binom{n}{j} \binom{t - jq + n - 1}{t - jq}$;

(iii) distância mínima: $W_1 = (q-l)q^{n-k-1}$ em que k e l são respectivamente o quociente e o resto da divisão euclidiana de d por $q-1$, ou seja, $d = k(q-1) + l$, $0 \leq l \leq q-1$.

No capítulo 3, utilizando os conceitos da teoria de bases de Gröbner, definiremos uma classe de códigos que tem como subclasse os códigos de Reed-Muller generalizados.

CAPÍTULO 2

BASES DE GRÖBNER

Sob a orientação de Wolfgang Gröbner, a teoria de Bases de Gröbner foi desenvolvida por Bruno Buchberger, durante a década de 1960. O problema principal da tese de Buchberger era determinar um método para encontrar uma base para $\mathbb{F}[X_1, \ldots, X_n]/I$ como $\mathbb{F}$-espaço vetorial. Veremos que um dos maiores empecilhos para se trabalhar com polinômios em $\mathbb{F}[X_1, \ldots, X_n]$ é que o algoritmo da divisão não se comporta como no caso de uma variável, cuja divisão euclidiana tem unicamente determinados o quociente e o resto. Em várias variáveis, a ordenação das variáveis e da divisão tem um impacto no processo. Assim, a teoria desenvolvida busca resolver tais problemas e obter resultados paralelos com o caso em uma variável. A teoria deste capítulo foi baseada nas referências [8] e [16].

2.1 Monômios e ordens monomiais

Definição 2.1.1. *Um **monômio** nas variáveis $X_1, \ldots, X_n$ é um produto da forma $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ onde todos os expoentes são inteiros não negativos.*

Escreveremos $X^\alpha = X_1^{\alpha_1} \ldots X_n^{\alpha_n}$, em que $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$. Quando $\alpha = (0, \ldots, 0)$, temos que $X^\alpha = 1$.

Definimos $|\alpha| := \alpha_1 + \cdots + \alpha_n$ como sendo o **grau total** do monômio X^α.

Seja $\mathbb{F}$ um corpo. Denotaremos por $\mathcal{M}$ o conjunto de todos os monômios em $\mathbb{F}[X_1, \ldots, X_n]$.

Definição 2.1.2. *Um **polinômio** $f \in \mathbb{F}[X_1, \ldots, X_n]$ é uma combinação linear de monômios com coeficientes em $\mathbb{F}$. Podemos escrever um polinômio f da seguinte forma*

$$f = \sum_\alpha a_\alpha X^\alpha, \;\; a_\alpha \in \mathbb{F}.$$

Definição 2.1.3. *Seja $f = \sum_\alpha a_\alpha X^\alpha \in \mathbb{F}[X_1, \ldots, X_n]$.*

*(i) chamamos a_α de **coeficiente** do monômio X^α;*

*(ii) se $a_\alpha \neq 0$, então $a_\alpha X^\alpha$ é dito **termo** de f;*

*(iii) o **grau total** de f, denotado por $\deg(f)$, é definido por*

$$\deg(f) = \max\{|\alpha|; a_\alpha \neq 0\}.$$

O grau total do polinômio nulo é indefinido.

Definição 2.1.4. *Uma* ***relação de ordem total*** *sobre um conjunto C, não vazio, é uma relação $\leq$ satisfazendo:*

(i) $c \leq c$, *para todo* $c \in C$.

(ii) Se $c_1, c_2 \in C$ *são tais que* $c_1 \leq c_2$ *e* $c_2 \leq c_1$ *então* $c_1 = c_2$.

(iii) Sejam c_1 c_2 *e* $c_3 \in C$. *Se* $c_1 \leq c_2$ *e* $c_2 \leq c_3$ *então* $c_1 \leq c_3$.

(iv) $c_1 \leq c_2$ *ou* $c_2 \leq c_1$, *para todo* $c_1, c_2 \in C$.

Definição 2.1.5. *Uma* ***ordem monomial*** $\succ$ *no conjunto* $\mathcal{M} \subset \mathbb{F}[X_1, \ldots, X_n]$ *é qualquer relação* $\succ$ *em* $\mathbb{Z}^n_{\geq 0}$, *ou equivalentemente, qualquer relação no conjunto dos monômios* X^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$, *satisfazendo:*

(i) $\succ$ *é uma ordem total em* $\mathbb{Z}^n_{\geq 0}$;

(ii) se $\alpha \succ \beta$ *em* $\mathbb{Z}^n_{\geq 0}$ *e* $\gamma \in \mathbb{Z}^n_{\geq 0}$, *então* $\alpha + \gamma \succ \beta + \gamma$;

(iii) $\succ$ *é uma boa ordem em* $\mathbb{Z}^n_{\geq 0}$, *isto é, todo subconjunto não vazio de* $\mathbb{Z}^n_{\geq 0}$ *possui elemento mínimo em relação a* $\succ$.

A seguir, listamos algumas das ordens monomiais mais utilizadas.

Definição 2.1.6. ***Ordem Lexicográfica*** *(ou* ***ordem lex****): Sejam* $\alpha = (\alpha_1, \ldots, \alpha_n)$ *e* $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. *Dizemos que* $\alpha \succ_{lex} \beta$ *se, no vetor diferença* $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$, *a primeira coordenada não nula, da esquerda para a direita, é positiva. Escrevemos* $X^\alpha \succ_{lex} X^\beta$ *se* $\alpha \succ \beta$.

Exemplo 2.1.7.

a) $(1, 2, 0) \succ_{lex} (0, 3, 4)$, pois $\alpha - \beta = (1, -1, -4)$.

b) $(3, 2, 4) \succ_{lex} (3, 2, 1)$, pois $\alpha - \beta = (0, 0, 3)$.

c) As variáveis $X_1, \ldots, X_n$ são ordenadas usualmente pela ordem lex, de fato,

$$(1, 0, \cdots, 0) \succ_{lex} (0, 1, 0, \ldots, 0) \succ_{lex} \ldots \succ_{lex} (0, \ldots, 0, 1).$$

Definição 2.1.8. ***Ordem Lexicográfica Graduada*** *(ou* ***ordem grlex****): Sejam* $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. *Dizemos que* $\alpha \succ_{grlex} \beta$ *e escrevemos* $X^\alpha \succ_{grlex} X^\beta$, *se* $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$ *ou* $|\alpha| = |\beta|$ *e* $\alpha \succ_{lex} \beta$.

Exemplo 2.1.9. *a)* $(1, 2, 3) \succ_{grlex} (3, 2, 0)$, *pois* $|(1, 2, 3) = 6 > 5 = |(3, 2, 0)$.

b) $(1, 2, 4) \succ_{grlex} (1, 1, 5)$, *pois* $|(1, 2, 4)| = |(1, 1, 5)|$ *e* $(1, 2, 4) \succ_{lex} (1, 1, 5)$.

Definição 2.1.10. ***Ordem Lexicográfica Graduada Reversa*** *(ou* ***ordem grevlex****):*
Dizemos que $\alpha \succ_{grevlex} \beta$ *e escrevemos* $x^\alpha \succ_{grevlex} x^\beta$ *se,* $|\alpha| > |\beta|$ *ou* $|\alpha| = |\beta|$ *e a primeira coordenada não nula em* $\alpha - \beta$, *da direita para a esquerda, é negativa.*

Exemplo 2.1.11. *a)* $(4, 7, 1) \succ_{grevlex} (4, 2, 3)$, *pois* $|(4, 7, 1) = 12 > 9 = |(4, 2, 3)|$.

b) $(1, 5, 2) \succ_{grevlex} (4, 1, 3)$, *pois* $|(1, 5, 2)| = |(4, 1, 3)| = 8$ *e* $(1, 5, 2) - (4, 1, 3) = (-3, 4, -1)$.

A ordem monomial pode ser aplicada para polinômios.

Exemplo 2.1.12. *Seja* $f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2 \in \mathbb{F}[X, Y, Z]$. *Então:*

- *Com respeito a ordem lexicográfica, podemos reordenar os termos de f da seguinte forma:*

$$f = -5X^3 + 7X^2Z^2 + 4XY^2Z + 4Z^2.$$

- *Com respeito a ordem lexicográfica graduada, temos que:*

$$f = 7X^2Z^2 + 4XY^2Z - 5X^3 + 4Z^2.$$

- *Com respeito a ordem lexicográfica graduada reversa, temos que:*

$$f = 4XY^2Z + 7X^2Z^2 - 5X^3 + 4Z^2.$$

A definição a seguir é a generalização esperada para polinômios em várias variáveis.

Definição 2.1.13. *Seja $f = \sum_\alpha a_\alpha X^\alpha \in \mathbb{F}[X_1, \ldots, X_n]$ um polinômio não nulo e $\succ$ uma ordem monomial. Definimos:*

(i) O ***multigrau*** *de f é*

$$multdeg(f) = \max_{\succ}\{\alpha \in \mathbb{Z}^n_{\geq 0}; a_\alpha \neq 0\}$$

(o máximo é tomado com respeito a $\succ$).

(ii) O ***coeficiente líder*** *de f é*

$$LC(f) = a_{multdeg(f)} \in \mathbb{F}.$$

(iii) O ***monômio líder*** *de f é*

$$LM(f) = X^{multdeg(f)}$$

(com coeficiente 1)

(iv) O ***termo líder*** *de f é*

$$LT(f) = LC(f).LM(f).$$

Exemplo 2.1.14. *Seja $f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2$ e $\succ$ a ordem lex. Temos que:*

$$\begin{aligned} multdeg(f) &= (3,0,0); \\ LC(f) &= -5; \\ LM(f) &= X^3; \\ LT(f) &= -5X^3. \end{aligned}$$

2.2 O Algoritmo da Divisão em $\mathbb{F}[X_1, \ldots, X_n]$

Uma ferramenta importante na teoria das bases de Gröbner é a divisão de um polinômio por uma lista de polinômios não nulos, que é similar ao algoritmo da divisão em $\mathbb{F}[X]$. Ao dividirmos f por uma lista $f_1, \ldots, f_s \in \mathbb{F}[X_1, \ldots, X_n]$, tomaremos a divisão de f por f_1, e o resto da divisão será dividido por f_2. O processo se repete até que o restante da divisão no estágio $s-1$ é dividido por f_s e obtemos r como o resto que não é divisível por nenhum outro polinômio da lista $f_1, \ldots, f_s$.

Teorema 2.2.1. *(**Algoritmo da Divisão em** $\mathbb{F}[X_1,\ldots,X_n]$) Considere uma ordem monomial $\succ$ em $\mathcal{M}$. Seja $F = (f_1,\ldots,f_s)$ uma s-upla ordenada de polinômios em $\mathbb{F}[X_1,\ldots,X_n]$. Então, cada $f \in \mathbb{F}[X_1,\ldots,X_n]$ pode ser escrito como*

$$f = q_1 f_1 + \cdots + q_s f_s + r$$

onde $q_i, r \in \mathbb{F}[X_1,\ldots,X_n]$ e $r = 0$ ou r é uma combinação linear de monômios, com coeficientes em $\mathbb{F}$, tais que nenhum deles é divisível por algum dos $LT(f_i)$, para todo i. Chamaremos r de resto da divisão de f por F. Além disso, se $q_i f_i \neq 0$, então $multdeg(f) \geq multdeg(q_i f_i)$

Demonstração. Ver [16, Teorema 3, Capítulo 2, Seção 3]. □

Apresentaremos o algoritmo e em seguida alguns exemplos de como ele funciona na prática.

Algoritmo 1: Algoritmo da Divisão em $\mathbb{F}[X_1,\ldots,X_n]$

Entrada: $f_1,\ldots,f_s,f$
Saída: $q_1,\ldots,q_s,r$
$q_1 := 0;\ldots;q_s := 0; r := 0$
$p := f$
Enquanto: $p \neq 0$ **faça**
  $i := 1$
  divisão sucedida := falso
  Enquanto $i \leq s$ **e** *divisão sucedida* := falso **faça**
    Se $LT(f_i)$ divide $LT(p)$ **então**
      $q_i := q_i + LT(p)/LT(f_i)$
      $p := p - (LT(p)/LT(f_i))f_i$
      divisão sucedida := verdadeiro
    Senão
      $i := i + 1$
  Se *divisão sucedida* = falso **então**
    $r := r + LT(p)$
    $p := p - LT(p)$
Retorne $q_1,\ldots,q_s,r$

Exemplo 2.2.2. *Usando a ordem lexicográfica, vamos dividir $f = XY^2 + 1$ por $f_1 = XY + 1$ e $f_2 = Y + 1$. Primeiro dividimos f por f_1. Temos que $LT(f) = XY^2$ e $LT(f_1) = XY$.*

Como $LT(f)/LT(f_1) = Y$, então

$$p_1 = f - Y f_1 = -Y + 1.$$

Agora, $LT(f_1) = XY$ não divide $LT(p_1) = -Y$, então paramos de dividir por f_1 e continuamos dividindo por f_2. Observe que $LT(f_2) = Y$, logo $LT(f_2)/LT(p_1) = -1$. Assim,

$$p_2 = p_1 - (-1)f_2 = 2.$$

Portanto,

$$f = XY^2 + 1 = Y(XY + 1) + (-1)(Y + 1) + 2 = Y f_1 - f_2 + 2,$$

já que o resto $r = 2$ não é divisível nem por f_1 nem por f_2.

Exemplo 2.2.3. *O resto da divisão de um polinômio por uma lista não é único. Por exemplo,*

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

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

A primeira expressão é obtida realizando a divisão de $f = X^2Y+XY^2+Y^2$ por $f_1 = XY-1$ e $f_2 = Y^2-1$, já a segunda expressão, é obtida realizando a divisão de f por f_2 e f_1.

Exemplo 2.2.4. *Podemos ter resto não nulo dividindo f por (f_1, f_2), mas resto não nulo quando dividimos f por (f_2, f_1). Por exemplo, sejam $f = XY^2-X$, $f_1 = XY-1$ e $f_2 = Y^2-1$. Dividindo f por f_1 e f_2, temos:*

$$XY^2 - X = Y(XY-1) + 0(Y^2-1) + (-X+Y).$$

Dividindo f por f_2 e f_1, temos:

$$XY^2 - X = X(Y^2-1) + 0(XY-1) + 0.$$

Da segunda expressão, fica claro que $f \in \langle f_1, f_2\rangle$, mas não podemos concluir isso da primeira.

Em geral, a divisão em $\mathbb{F}[X_1, \ldots, X_n]$ dá condições suficientes para decidir se um polinômio f está em $\langle f_1, \ldots, f_n\rangle$, se $r = 0$, porém, cada ordem diferente dos polinômios da lista e cada ordem monomial diferente dá um resto diferente, e não é claro que para alguma dessas escolhas teremos $r = 0$, quando $f \in \langle f_1, \ldots, f_n\rangle$. Para resolver este problema utilizaremos bases de Gröbner, que serão definidas na seção 2.4.

2.3 Ideais Monomiais e o Lema de Dickson

Definição 2.3.1. *Um ideal $I \subset \mathbb{F}[X_1, \ldots, X_n]$ é um **ideal monomial** se, existe um subconjunto não vazio $A \subset \mathbb{Z}^n_{\geq 0}$ tal que*

$$I = \langle X^\alpha : \alpha \in A\rangle := \Big\{ \sum_{\alpha \in B} f_\alpha X^\alpha : f_\alpha \in \mathbb{F}[X_1, \ldots, X_n], B \subset A \ \text{é finito} \Big\}.$$

Exemplo 2.3.2. *$I = \langle X^4, X^3Y^4, X^2Y^5\rangle \subseteq \mathbb{F}[X, Y]$ é um ideal monomial.*

Proposição 2.3.3. *Seja $I = \langle X^\alpha : \alpha \in A\rangle$ um ideal monomial de $\mathbb{F}[X_1, \ldots, X_n]$. Então um monômio $X^\beta \in I$ se, e somente se, X^α divide X^β, para algum $\alpha \in A$.*

Demonstração. Seja $X^\beta \in I$, então $X^\beta = \sum_{i=1}^k h_i X^{\alpha_i}$, onde $\alpha_i \in A$ e $h_i = \sum_{j=1}^{t_i} a_{ij} X^{\gamma_{ij}}$, $a_{ij} \in \mathbb{F}$. Portanto, podemos escrever

$$X^\beta = (a_{11}X^{\gamma_{11}}X^{\alpha_1} + \cdots + a_{1t}X^{\gamma_{1t}}X^{\alpha_1}) + \cdots + (a_{k1}X^{\gamma_{k1}}X^{\alpha_k} + \cdots + a_{kt}X^{\gamma_{kt}}X^{\alpha_k}).$$

Como o lado esquerdo da igualdade é um monômio, o lado direito também deverá ser. Desse modo, alguns termos da soma do lado direito irão se cancelar. Note que, cada termo da soma do lado direito da igualdade, é divisível por algum X^{α_i}, logo, X^β tem a mesma propriedade.

Reciprocamente, seja $\alpha \in A$ tal que $X^\beta = pX^\alpha$. Logo, $X^\beta \in I$ por definição de ideal. □

Definição 2.3.4. *Seja I um ideal em $\mathbb{F}[X_1, \ldots, X_n]$, com $I \neq 0$.*

(i) Denotamos por $LT(I)$ o conjunto de termos líderes dos elementos de I. Então

$$LT(I) = \{cX^\alpha : \exists\ f \in I \ \text{tal que}\ LT(f) = cX^\alpha\}.$$

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

Observação 2.3.5. *Seja $I = \langle f_1, \ldots, f_s\rangle \neq 0$ um ideal finitamente gerado em $\mathbb{F}[X_1, \ldots, X_n]$. Claramente $\langle LT(f_1), \ldots, LT(f_s)\rangle \subset \langle LT(I)\rangle$. Com efeito, seja $f \in \langle LT(f_1), \ldots, LT(f_s)\rangle$, então $f = g_1 LT(f_1) + \cdots + g_s LT(f_s)$, com $g_i \in \mathbb{F}[X_1, \ldots, X_n]$.*

Para cada $i \in \{1, \ldots, s\}$, temos que $LT(f_i) \in LT(I) \subset \langle LT(I)\rangle$. Assim, cada parcela de f pertence a $\langle LT(I)\rangle$ e, portanto, $f \in \langle LT(I)\rangle$.

Teorema 2.3.6. ***(Lema de Dickson)*** *Seja $I = \langle X^\alpha : \alpha \in A\rangle$ um ideal monomial em $\mathbb{F}[X_1, \ldots, X_n]$. Então, I pode ser escrito da forma $I = \langle X^{\alpha_1}, \ldots, X^{\alpha_s}\rangle$, em que $\alpha_1, \ldots, \alpha_s \in A$. Em particular, I possui uma base finita.*

Demonstração. Ver [16, Teorema 5, Capítulo 2, Seção 4]. □

Observação 2.3.7. *Seja $I = \langle f_1, \ldots, f_s\rangle \neq 0$ um ideal finitamente gerado em $\mathbb{F}[X_1, \ldots, X_n]$. De um modo geral, não é verdade que $\langle LT(I)\rangle \subset \langle LT(f_1), \ldots, LT(f_s)\rangle$. Por exemplo, seja $I = \langle X^3 - 2XY, X^2Y - 2Y^2 + X\rangle$ e considere a ordem lexicográfica graduada.*

Como $X^2 = X(X^2Y - 2Y^2 + X) - Y(X^3 - 2XY)$, então $X^2 \in I$. Daí, $X^2 = LT(X^2) \in LT(I) \subset \langle LT(I)\rangle$. Mas

$$X^2 \notin \left\langle LT(X^3 - 2XY), LT(X^2Y - 2Y^2 + X)\right\rangle = \left\langle X^3, X^2Y\right\rangle,$$

que é um ideal monomial e X^2 não é múltiplo de X^3 nem de X^2Y.

Proposição 2.3.8. *Seja $I \subset \mathbb{F}[X_1, \ldots, X_n]$ um ideal com $I \neq 0$. Então:*

(i) $\langle LT(I)\rangle$ é um ideal monomial.

(ii) Existem $g_1, \ldots, g_t \in I$ tais que $\langle LT(I)\rangle = \langle (LT(g_1), \ldots, LT(g_t)\rangle$.

Demonstração. (i) Considere o ideal monomial $\langle LM(g) : g \in I\backslash\{0\}\rangle$.

Note que $\langle LM(g) : g \in I\backslash\{0\}\rangle = \langle LT(g) : g \in I\backslash\{0\}\rangle$.

Com efeito, seja $f \in \langle LM(g) : g \in I\backslash\{0\}\rangle$, então existe um subconjunto finito $A \subseteq I\backslash\{0\}$ tal que

$$f = \sum_{g\in A} a_g LM(g) = \sum_{g\in A} a_g (LC(g))^{-1} LC(g) LM(g) = \sum_{g\in A} a_g (LC(g))^{-1} LT(g)$$

logo, $f \in \langle LT(g) : g \in I\backslash\{0\}\rangle$.

Agora, seja $f \in \langle LT(g) : g \in I\backslash\{0\}\rangle$, então existe um subconjunto finito $B \subseteq I\backslash\{0\}$ tal que

$$f = \sum_{g\in B} a_g LT(g) = \sum_{g\in B} a_g LC(g) LM(g),$$

portanto, $f \in \langle LM(g) : g \in I\backslash\{0\}\rangle$.

Como $\langle LT(I)\rangle = \langle LT(g) : g \in I\backslash\{0\}\rangle = \langle LM(g) : g \in I\backslash\{0\}\rangle$, segue que $\langle LT(I)\rangle$ é um ideal monomial.

(ii) Como $\langle LT(I)\rangle$ é um ideal monomial, pelo Lema de Dickson existem $g_1,\ldots,g_t \in$ tais que $\langle LT(I)\rangle = \langle LM(g_1),\ldots,LM(g_t)\rangle$. Note que $\langle LM(g_1),\ldots,LM(g_t)\rangle = \langle LT(g_1),\ldots,LM(g_t)\rangle$. De fato, dado $f \in \langle LT(g_1),\ldots,LT(g_t)\rangle$, temos

$$\begin{aligned} f &= \sum_{i=1}^{t} a_i LM(g_i) \\ &= \sum_{i=1}^{t} a_i (LC(g_i))^{-1} LC(g_i) LM(g_i) \\ &= \sum_{i=1}^{t} a_i (LC(g_i))^{-1} LT(g_i) \in \langle LT(g_1),\ldots,LT(g_t)\rangle . \end{aligned}$$

Por outro lado, dado $f \in \langle LT(g_1),\ldots,LT(g_t)\rangle$, temos

$$\begin{aligned} f &= \sum_{i=1}^{t} a_i LT(g_i) \\ &= \sum_{i=1}^{t} a_i LC(g_i) LM(g_i) \in \langle LM(g_1),\ldots,LM(g_t)\rangle . \end{aligned}$$

Conclusão: $\langle LT(I)\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle$.

□

Observação 2.3.9. *Utilizando a notação da proposição anterior, temos que:*

$$\langle LT(I)\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle = \langle LM(g_1),\ldots,LM(g_t)\rangle .$$

Teorema 2.3.10. ***(Teorema da Base de Hilbert)*** *Todo ideal $I \subset \mathbb{F}[X_1,\ldots,X_n]$ é finitamente gerado, isto é, existem $g_1,\ldots,g_t \in I$ tais que $I = \langle g_1,\ldots,g_t\rangle$.*

Demonstração. Se $I = \{0\}$ não temos nada a provar. Suponha que $I \neq \{0\}$.

Sabemos que $\langle LT(I)\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle$, para alguns $g_1,\ldots,g_t \in I$, pela Proposição 2.3.8.

Mostraremos que $I = \langle g_1,\ldots,g_t\rangle$. Claramente $\langle g_1,\ldots,g_t\rangle \subset I$. Seja $f \in I$, utilizando o algoritmo da divisão para dividir f por $(g_1,\ldots,g_t)$, obtemos

$$f = a_1 g_1 + \cdots + a_t g_t + r,$$

onde nenhum termo de r é divisível por nenhum dos $LT(g_i)$'s, com $i \in \{1,\ldots,t\}$.

Como $r = f - a_1 g_1 - \cdots - a_t g_t$, então $r \in I$. Se $r \neq 0$, então

$$LT(r) \in LT(I) \subset \langle LT(I)\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle ,$$

logo $LT(r)$ é divisível por algum $LT(g_i)$. ABSURDO! Portanto, $r = 0$.

Assim, podemos escrever $f = a_1 g_1 + \cdots + a_t g_t$ e daí, $f \in \langle g_1,\ldots,g_t\rangle$.

Portanto, $I = \langle g_1,\ldots,g_t\rangle$. □

2.4 Bases de Gröbner

A teoria de bases de Gröbner apareceu pela primeira vez na tese de doutorado do matemático austríaco Bruno Buchberger, publicada em 1965, sob supervisão do professor Wolfgang Gröbner, que propôs o seguinte problema para sua tese: dado um ideal $I \subset \mathbb{F}[X_1, \ldots, X_n]$, encontrar uma base para $\mathbb{F}[X_1, \ldots, X_n]/I$ como $\mathbb{F}$-espaço vetorial.

Trabalhando com um anel de polinômios em uma variável a resposta é conhecida. I é gerado por um certo polinômio de grau d (no caso $I \neq 0$) e $\{1 + I, X + I, \ldots, X^{d-1} + I\}$ forma uma base para $\mathbb{F}[X]/I$. Agora, quando trabalhamos com um anel de mais de uma variável a situação muda radicalmente.

Para solucionar o problema, a ideia foi fixar uma ordem monomial em $\mathcal{M}$ e determinar um conjunto especial de geradores para o ideal I, cuja propriedade principal é que, as classes dos monômios que não são múltiplos de nenhum dos monômios líderes dos polinômios que estão nessa base especial, formam uma base para $\mathbb{F}[X_1, \ldots, X_n]/I$ como $\mathbb{F}$-espaço vetorial.

Em 1976 Buchberger chamou de "bases de Gröbner" essa base especial para I, em virtude da influência do seu orientador para realização do trabalho.

Definição 2.4.1. *Fixe uma ordem monomial $\succ$. Um subconjunto finito $G = \{g_1, \ldots, g_t\}$ de um ideal I de $\subset \mathbb{F}[X_1, \ldots, X_n]$ é dito uma* ***base de Gröbner*** *se*

$$\langle LT(g_1), \ldots, LT(g_t)\rangle = \langle LT(I)\rangle.$$

O lema a seguir nos fornece outra maneira de definir bases de Gröbner para um ideal.

Lema 2.4.2. *O conjunto $G = \{g_1, \ldots, g_t\}$ é uma base de Gröbner para I, se e somente se, para todo $f \in I$, $f \neq 0$, temos que $LM(f)$ é múltiplo de $LM(g_i)$, para algum $i \in \{1, \ldots, t\}$.*

Demonstração. Seja $f \in I$, $f \neq 0$, então

$$LM(f) \in \langle LM(I)\rangle = \langle LT(I)\rangle =^{hip} \langle LT(g_1), \ldots, LT(g_t)\rangle = \langle LM(g_1), \ldots, LM(g_t)\rangle .$$

Como $\langle LM(g_1), \ldots, LM(g_t)\rangle$ é um ideal monomial, segue que $LM(f)$ é múltiplo de $LM(g_i)$, para algum $i \in \{1, \ldots, t\}$. Reciprocamente, é óbvio que $\langle LT(g_1), \ldots, LT(g_t)\rangle \subset \langle LT(I)\rangle$.

Vejamos que $\langle LT(I)\rangle \subset \langle LT(g_1), \ldots, LT(g_t)\rangle$. Como $\langle LT(I)\rangle = \langle LM(I)\rangle$, basta mostrar que $\langle LM(I)\rangle \subset \langle LT(g_1), \ldots, LT(g_t)\rangle$, isto é, $LT(I) \subset \langle LT(g_1), \ldots, LT(g_t)\rangle$.

Por hipótese, se $f \in I$, $f \neq 0$, existe $i \in \{1, \ldots, t\}$ tal que $LM(f)$ é múltiplo e $LM(g_i)$.

Daí,

$$LT(f) \in \langle LM(g_1), \ldots, LM(g_t)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle .$$

Portanto, $LT(I) \subset \langle LT(g_1), \ldots, LT(g_t)\rangle$ como queríamos demonstrar.

□

Ao fixarmos uma ordem monomial, segue da Proposição 2.3.8 que todo ideal $I \subset \mathbb{F}[X_1, \ldots, X_n]$, com $I \neq \{0\}$, possui uma base de Gröbner. E mais, qualquer base de Gröbner para um ideal I é uma base para I. A seguir, listamos algumas propriedades das bases de Gröbner.

Proposição 2.4.3. *Seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para um ideal $I \subset \mathbb{F}[X_1, \ldots, X_n]$ e seja $f \in \mathbb{F}[X_1, \ldots, X_n]$. Então existe um único $r \in \mathbb{F}[X_1, \ldots, X_n]$ com as seguintes propriedades:*

(i) Nenhum termo de r é divisível por qualquer dos termos $LT(g_1), \ldots, LT(g_t)$.

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

Em particular, r é o resto a divisão de f por G, não importando a ordem dos elementos de G.

Demonstração. Pelo algoritmo da divisão, temos que $f = a_1g_1 + \cdots + a_tg_t + r$, onde r satisfaz (i). Para provarmos (ii), considere $f = g + r = g^{'} + r^{'}$ satisfazendo (i) e (ii).

Logo,

$$r - r' = g' - g \in I.$$

Se $r \neq r'$, então

$$TL(r - r') \in \langle TL(I)\rangle = \langle TL(g_1), \ldots, TL(g_t)\rangle.$$

Assim, $TL(r - r')$ é divisível por algum $TL(g_i)$. Logo, $ML(r - r')$ é divisível por $TL(g_i)$. Por outro lado, como $ML(r-r')$ é um monômio de r ou r', temos que $ML(r-r')$ não é divisível por $TL(g_i)$. ABSURDO! Portanto, $r = r'$. □

Corolário 2.4.4. *Seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para um ideal $I \subset \mathbb{F}[X_1, \ldots, X_n]$ e seja $f \in \mathbb{F}[X_1, \ldots, X_n]$. Então $f \in I$ se, se somente se, o resto da divisão de f por G é zero.*

Demonstração. Se o resto é zero, claramente $f \in I$. Reciprocamente, dado $f \in I$, então $f = f + 0$ satisfaz as duas condições da proposição anterior. Pela unicidade do resto, segue o resultado.

□

Definição 2.4.5. *Sejam $f, g \in \mathbb{F}[X_1, \ldots, X_n]$ polinômios não nulos.*

*(i) Sejam $multdeg(f) = \alpha$ e $multdeg(g) = \beta$. Seja $\gamma = (\gamma_1, \ldots, \gamma_n)$, onde $\gamma_i = \max\{\alpha_i, \beta_i\}$ para cada i. Dizemos que X^γ é o **mínimo múltiplo comum** de $LM(f)$ e $LM(g)$ e denotamos por $mmc(LM(f), LM(g))$.*

*(ii) O **S-polinômio** de f e g é a seguinte combinação linear:*

$$S(f, g) = \frac{X^\gamma}{LT(f)}f - \frac{X^\gamma}{LT(g)}g.$$

Exemplo 2.4.6. *Dados $f = X^3Y^2 - X^2Y^3 + X$ e $g = 3X^4Y + Y^2$ em $\mathbb{R}[X, Y]$ com a ordem lexicográfica graduada, então $\gamma = (4, 2)$.*

Logo,

$$mmc(LM(f), LM(g)) = mmc(X^3Y^2, X^4Y) = X^4Y^2.$$

Portanto, o S-polinômio de f e g é:

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

2.5 O Algoritmo de Buchberger

Vimos anteriormente que todo ideal em $\mathbb{F}[X_1, \ldots, X_n]$ possui uma base de Gröbner. O próximo teorema nos apresenta um algoritmo para a construção de uma base de Gröbner para um ideal, dado um conjunto finito de geradores.

O resto da divisão de f por uma $s - upla$ ordenada $F = (f_1, \ldots, f_s)$ será denotado por $\overline{f}^F$.

Teorema 2.5.1. *Seja $I = \langle f_1, \ldots, f_s\rangle \neq \langle 0\rangle$ um ideal de $\mathbb{F}[X_1, \ldots, X_n]$ e considere $\succ$ uma ordem monomial. Então uma base de Gröbner de I pode ser construída em um número finito de passos aplicando o seguinte algoritmo:*

Algoritmo 2: Algoritmo de Buchberger

Entrada: $F = (f_1, \ldots, f_s)$
Saída: *uma base de Gröbner* $G = (g_1, \ldots, g_t)$ *para* I, *com* $F \subseteq G$

$G := F$
Repita
  $G' := G$
  Para *cada par* $\{p, q\}$, $p \neq q$ *em* G' ***faça***
    $r := \overline{S(p,q)}^{G'}$
    Se $r \neq 0$ ***então*** $G := G \cup \{r\}$
Até $G = G'$
Retorne G

Demonstração. Ver [16, Teorema 2, Capítulo 5, Seção 7]. □

Exemplo 2.5.2. *Seja* $\mathbb{Q}[X, Y]$ *com a ordem lexicográfica graduada e*

$$I = \langle f_1, f_2 \rangle = \langle X^3 - 2XY, X^2Y - 2Y^2 + X \rangle.$$

Então $F := (X^3 - 2XY, X^2Y - 2Y^2 + X)$.
Calculando o S-polinômio de f_1 *e* f_2*:*

$$\begin{aligned} S(f_1, f_2) &= Y(X^3 - 2XY) - X(X^2Y - 2Y^2 + X) = -X^2 \\ \overline{S(f_1, f_2)}^{F} &= -X^2 \neq 0. \end{aligned}$$

Daí, $f_3 = -X^2$ *e* $G := (f_1, f_2, f_3) = (X^3 - 2XY, X^2Y - 2Y^2 + X, -X^2)$.
Logo,

$$\begin{aligned} S(f_1, f_2) &= f_3; \\ \overline{S(f_1, f_2)}^{G} &= 0; \\ S(f_1, f_3) &= X^3 - 2XY + X(-X^3) = -2XY; \\ \overline{S(f_1, f_3)}^{G} &= -2XY \neq 0. \end{aligned}$$

Então, $f_4 := -2XY$ *e* $G := (f_1, f_2, f_3, f_4) = (X^3 - 2XY, X^2Y - 2Y^2 + X, -X^2, -2XY)$.
Segue que:

$$\begin{aligned} \overline{S(f_1, f_2)}^{G} &= \overline{S(f_1, f_3)}^{G} = 0; \\ S(f_1, f_4) &= 2Y(X^3 - 2XY) = X^2(-2XY) = -2XY^2 = -Yf_4. \end{aligned}$$

Desse modo,

$$\overline{S(f_1, f_4)}^{G} = 0.$$

Dando continuidade ao uso do algoritmo, temos que:

$$\begin{aligned} S(f_2, f_3) &= X^2Y - 2Y^2 + X + Y(-X^2) = -2Y^2 + X \\ \overline{S(f_2, f_3)}^{G} &= -2Y^2 + X \neq 0. \end{aligned}$$

Logo, $f_5 := -2Y^2 + X$ *e*

$$G := (f_1, f_2, f_3, f_4, f_5) = (X^3 - 2XY, X^2Y - 2Y^2 + X, -X^2, -2XY, -2Y^2 + X).$$

Verificando os restos dos S-polinômios, obtemos:

$$\begin{aligned}
S(f_1, f_5) &= Y^2(X^3 - 2XY) + \frac{1}{2}X^3(-2Y^2 + X) = \frac{1}{2}X^4 - 2XY^3 = \frac{1}{2}Xf_1 + \left(Y^2 - \frac{1}{2}X\right) f_4;\\
S(f_2, f_3) &= f_5;\\
S(f_2, f_4) &= X^2Y - 2Y^2 + X + \frac{1}{2}X(-2XY) = -2Y^2 + X = f_5;\\
S(f_2, f_5) &= Y(X^2 - 2Y^2 + X) + \frac{1}{2}X^2(-2Y^2 + X) = \frac{1}{2}X^3 - 2Y^3 + XY = -\frac{1}{2}Xf_3 + Yf_5;\\
S(f_3, f_4) &= Y(-X^2) - \frac{1}{2}X(-2XY) = 0;\\
S(f_3, f_5) &= -Y^2(-X^2) + \frac{1}{2}X^2(-2Y^2 + X) = \frac{1}{2}X^3 = -\frac{1}{2}Xf_3\\
S(f_4, f_5) &= -\frac{1}{2}Y(-2XY) + \frac{1}{2}(-2Y^2 + X) = \frac{1}{2}X^2 = \frac{1}{2}f_3.
\end{aligned}$$

Assim,

$$\begin{aligned}
\overline{S(f_1, f_5)}^G &= \overline{S(f_2, f_3)}^G = \overline{S(f_2, f_4)}^G = \overline{S(f_2, f_5)}^G = 0.\\
\overline{S(f_3, f_4)}^G &= \overline{S(f_3, f_5)}^G = \overline{S(f_4, f_5)}^G = 0.
\end{aligned}$$

Portanto, $G := (f_1, f_2, f_3, f_4, f_5)$ *é base de Gröbner para* I*.*

2.6 A Pegada de um Ideal

Definição 2.6.1. *Seja* $I \subset \mathbb{F}[X_1, \ldots, X_n]$ *um ideal. A* ***pegada*** *de* I *com respeito a uma ordem monomial fixada em* $\mathcal{M}$ *é o seguinte conjunto:*

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

Exemplo 2.6.2. *Dado* $I = \langle X, Y\rangle \subset \mathbb{F}[X, Y]$*, como o monômio líder de qualquer polinômio não constante de* $\mathbb{F}[X, Y]$ *é divisível por* X *ou* Y*, concluímos que* $G = \{X, Y\}$ *é uma base de Gröbner para* I *e* $\Delta(I) = \{1\}$*.*

A pegada de um ideal I está diretamente relacionada com uma base de Gröbner para I, ambas definidas com respeito a mesma ordem monomial em $\mathcal{M}$.

Proposição 2.6.3. *Seja* $I \subset \mathbb{F}[X_1, \ldots, X_n]$ *um ideal e considere* $G = \{g_1, \ldots, g_t\}$ *uma base de Gröbner para* I*. Então, um monômio* $M \in \Delta(I)$ *se, e só se,* M *não é múltiplo de* $LM(g_i)$*, para todo* $i = 1, \ldots, t$*.*

Demonstração. Suponha que M não é múltiplo de $LM(g_i)$, para todo $i = 1, \ldots, t$ então pela definição de base de Gröbner, temos que M não é monômio líder de nenhum polinômio de I.

Reciprocamente, suponha que $M \in \Delta(I)$. Se $LM(g_i)$ dividisse M teríamos que $M \in I$, contradizendo a hipótese de que $M \in \Delta(I)$. Portanto, $LM(g_i)$ não divide M, para todo $i = 1, \ldots, t$.

□

Observação 2.6.4. *Na demonstração acima utilizamos a definição de $\Delta(I)$ em uma direção e a definição de bases de Gröbner na outra. Isso sugere que os conceitos de Pegada e bases de Gröbner são equivalentes em algum sentido. De fato, são equivalentes no seguinte sentido: ao encontrarmos uma base de Gröbner para um ideal I, podemos obter a pegada de I usando apenas a proposição acima. Por outro lado, podemos iniciar com a definição de pegada e obter uma base de Gröbner para I como sendo um conjunto $G = \{g_1, \ldots, g_t\} \subset I$ tal que, o conjunto dos monômios que são múltiplos de $LM(g_i)$, para algum $I = 1, \ldots, t$ é exatamente $\mathcal{M} \setminus \Delta(I)$. No Apêndice da referência [16], pode se encontrar a prova de que tal conjunto existe e satisfaz as condições da definição de pegada.*

Faremos agora um exemplo que utiliza a Proposição 2.6.3 para obter uma representação gráfica de uma pegada. Associamos a um par ordenado (α, β), com entradas não negativas e inteiras, o monômio $X^\alpha Y^\beta$.

Exemplo 2.6.5. *Seja $I = \langle X^3 - X, Y^3 - Y, X^2Y - Y\rangle \subset \mathbb{R}[X, Y]$ e tomemos $\mathcal{M}$ com a ordem lexicográfica (onde $Y \succ_{lex} X$). Não é difícil verificar que $\{X^3-X, Y^3-Y, X^2Y-Y\}$ é uma base de Gröbner para I. Temos que $LM(X^3-X) = X^3$, $LM(Y^3-Y) = Y^3$ e $LM(X^2Y-Y) = X^2Y$, e aplicando a Proposição 2.6.3 temos a seguinte representação para $\Delta(I)$.*

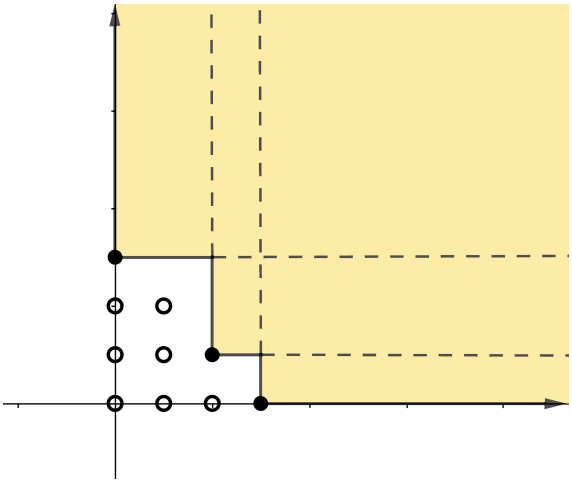

Figura 2.1: Representação gráfica da pegada de um ideal

Os pontos $(3, 0)$, $(0, 3)$ e $(2, 1)$ correspondem aos monômios líderes da base de Gröbner. Sendo assim, é possível determinar a partir destes os monômios que são múltiplos de pelo menos um deles. Segue que $\Delta(I) = \{1, X, X^2, Y, XY, Y^2, XY^2\}$.

Exemplo 2.6.6. *Seja $\mathbb{Q}[x, y]$ com a ordem lexicográfica graduada e*

$$I = \langle f_1, f_2\rangle = \langle X^3 - 2XY, X^2Y - 2Y^2 + X\rangle.$$

Do Exemplo 2.5.2, temos que

$$G = \{X^3 - 2XY, X^2Y - 2Y^2 + X, -X^2, -2XY, -2Y^2 + X\}$$

é uma base de Gröbner para I. Pela proposição 2.6.3, sabemos que $\Delta(I)$ é composto dos monômios que não são múltiplos de

$$LM(G) = \{X^3, X^2Y, X^2, XY, Y^2\}.$$

Portanto $\Delta(I) = \{1, X, Y\}$, como podemos visualizar na figura abaixo.

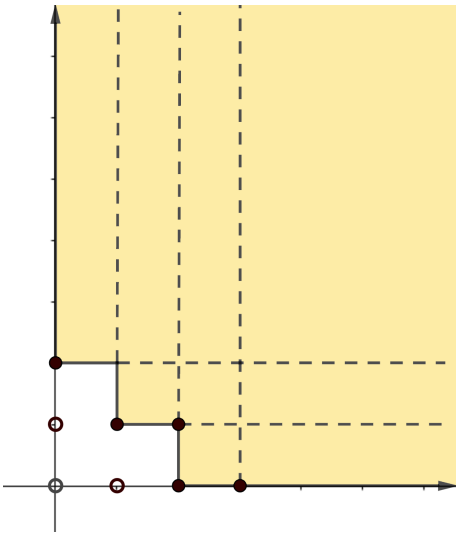

Figura 2.2: Representação gráfica da pegada de um ideal

O teorema a seguir é o principal resultado da tese de Buchberger [4].

Teorema 2.6.7. *Seja $I \subset \mathbb{F}[X_1, \ldots, X_n]$ um ideal.*
Então

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

é uma base para $\mathbb{F}[X_1, \ldots, X_n]/I$ como $\mathbb{F}$-espaço vetorial.
Em particular,

$$dim(\mathbb{F}[X_1, \ldots, X_n]/I) = |\Delta(I)|.$$

Demonstração. Seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para I com respeito a mesma ordem monomial usada para determinar $\Delta(I)$ e seja $f \in \mathbb{F}[X_1, \ldots, X_n]$.

Dividindo f por uma base de Gröbner para I, obtemos $q_1, \ldots, q_r$ e r tais que

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

onde o resto é da forma $r = \sum_{i=1}^{t} a_i M_i$ em que $a_i \in \mathbb{F}$ e $M_i \in \Delta(I)$, para todo $i = 1, \ldots, t$.

Como $f + I = q_1 g_1 + \cdots + q_t g_t + r + I$ e $q_i g_i \in I$, para todo i, temos que $f + I = r + I$. Portanto $\mathcal{B}$ gera $\mathbb{F}[X_1, \ldots, X_n]/I$ como $\mathbb{F}$-espaço vetorial.

Vejamos agora que $\mathcal{B}$ é linearmente independente sobre $\mathbb{F}$.

Suponha que $\sum_{i=1}^{l} b_i(M_i + I) = 0 + I$, com $b_i \in \mathbb{F}$ e $M_i \in \Delta(I)$, para todo $i = 1, \ldots, l$.

Então, $\sum_{i=1}^{l} b_i M_i \in I$ e assim temos que ter $b_i = 0$, para todo $i = 1, \ldots, l$, caso contrário, $\sum_{i=1}^{l} b_i M_i$ seria um elemento não nulo de I, cujo monômio líder não é monômio líder de nenhum polinômio em I. ABSURDO! □

Sejam $I \subset \mathbb{F}[x_1, \ldots, x_n]$ um ideal e $\{f_1, \ldots, f_t\}$ uma base para I. Denote por

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

Proposição 2.6.8. *$\Delta(I) \subset \Delta(LM(f_1), \ldots, LM(f_t))$ e $\Delta(I) = \Delta(LM(f_1), \ldots, LM(f_t))$ se, e só se, $\{f_1, \ldots, f_t\}$ é uma base de Gröbner para I.*

Demonstração. De fato, seja $f \in \Delta(I)$, temos que f não é monômio líder de nenhum polinômio de I. Logo, f não é divisível por f_i, para todo $i = 1, \ldots, n$, pois I é um ideal de $\mathbb{F}[X_1, \ldots, X_n]$.

Assim, conclui-se que $\Delta(I) \subset \Delta(LM(f_1), \ldots, LM(f_t))$.

Sejam $\Delta(I) = \Delta(LM(f_1), \ldots, LM(f_t))$ e $f \in I$. Como $\Delta(I) = \Delta(LM(f_1), \ldots, LM(f_t))$, temos que f é divisível por algum f_i, logo $\{f_1, \ldots, f_t\}$ é uma base de Gröbner para I.

Suponhamos agora que $\{f_1, \ldots, f_t\}$ é uma base de Gröbner.

Se $f \in \Delta(I) = \Delta(LM(f_1), \ldots, LM(f_t))$, temos que f não está em I, pois $\{f_1, \ldots, f_t\}$ é base de Gröbner, daí $f \in \Delta(I)$.

□

CAPÍTULO 3

CÓDIGOS CARTESIANOS AFINS

Neste capítulo faremos a construção dos código cartesianos afins e calcularemos os seus principais parâmetros. Este capítulo foi baseado na referência [9]

3.1 Variedades afins e a pegada de um ideal

Apresentaremos nesta seção uma relação entre a variedade afim associada a um ideal e a sua pegada, quando $\Delta(I)$ for finito.

Começamos apresentando um conceito fundamental na geometria algébrica, que relaciona álgebra e geometria.

Definição 3.1.1. *Seja $I \subset \mathbb{F}[X_1, \ldots, X_n]$ um ideal. A **variedade afim** associada a I é o conjunto*

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

Observação 3.1.2. *Não é difícil ver que: dado $I \subset \mathbb{F}[X_1, \ldots, X_n]$ um ideal, se $I = \langle g_1, \ldots, g_t \rangle$, então $(a_1, \ldots, a_n) \in V(I)$ se, e somente se, $g_i(a_1, \ldots, a_n) = 0$, para todo $i = 1, \ldots, t$.*

Definição 3.1.3. *Seja V uma variedade afim. O **ideal da variedade** V é o conjunto de todos os polinômios que se anulam em V, ou seja,*

$$I(V) := \{f \in \mathbb{F}[X_1, \ldots, X_n] : f(a_1, \ldots, a_n) = 0, \text{para todo } (a_1, \ldots, a_n) \in V\}.$$

É fácil ver que esse conjunto é, de fato, um ideal de $\mathbb{F}[X_1, \ldots, X_n]$.

Um famoso teorema de Hilbert afirma que se $\mathbb{F}$ é um corpo algebricamente fechado, então $I(V(I)) = \sqrt{I}$, onde $\sqrt{I} := \{f \in \mathbb{F}[X_1, \ldots, X_n] : f^m \in I \text{ para algum } m \in \mathbb{N}\}$ é o ideal chamado **radical de I** (ver [16], p. 183).

Uma variedade $V(I)$ pode ter infinitos pontos (tome por exemplo $I = \langle X - Y^2 \rangle \subset \mathbb{R}[X, Y]$) ou um número finito de pontos (tome por exemplo $I = \langle X^2 - 1, Y^2 - 1 \rangle \subset \mathbb{R}[X, Y]$). Para provar uma importante relação entre a variedade de I e a sua pegada, quando $\Delta(I)$ for finito, precisamos do seguinte resultado auxiliar.

Lema 3.1.4. *Seja $I \subset \mathbb{F}[X_1, \ldots, X_n]$ um ideal e sejam $P_1, \ldots, P_r$ os pontos distintos de $V(I)$. Então existem polinômios $f_1, \ldots, f_r \in \mathbb{F}[X_1, \ldots, X_n]$ tais que $f_i(P_i) = \delta_{ij}$, para todo $i, j \in \{1, \ldots, r\}$, onde δ_{ij} é o delta de Kronecker.*

Demonstração. Dados $P_i = (a_{i1}, \ldots, a_{in}) \in \mathbb{F}^n$, com $i = 1, \ldots, r$. Vamos obter f_1.

Como todos os pontos são distintos, para $i \in \{2, \ldots, r\}$, existe $j_i \in \{1, \ldots, n\}$ tal que $a_{1j_i} \neq a_{ij_i}$. Considere

$$h_i = \frac{X_{j_i} - a_{ij_i}}{a_{1j_i} - a_{ij_i}},$$

logo $h_i(P_1) = 1$ e $h_i(P_i) = 0, \text{para todo } i = 2, \ldots, r$.

Tome

$$f_1 = \prod_{i=2}^{r} h_i.$$

Daí, temos que $f_1(P_1) = 1$ e $f_1(P_i) = 0$, para todo $i = 2, \ldots, r$.

Com procedimento análogo, podemos obter $f_2, \ldots, f_r$.

□

Teorema 3.1.5. *Seja $I \subset \mathbb{F}[X_1, \ldots, X_n]$ um ideal tal que $\Delta(I)$ é um conjunto finito. Então $V(I)$ é também um conjunto finito e $|(V(I))| \leq |\Delta(I)|$.*

Demonstração. Sejam $P_1, \ldots, P_r$ pontos distintos de $V(I)$. Do lema anterior, sabemos que existem $f_1, \ldots, f_r \in \mathbb{F}[X_1, \ldots, X_n]$ tais que $f_i(P_j) = \delta_{ij}$, para todo $i, j \in \{1, \ldots, r\}$.

Afirmação: O Conjunto $\{f_1 + I, \ldots, f_r + I\}$ é um conjunto linearmente independente em $\mathbb{F}[X_1, \ldots, X_n]/I$.

Com efeito, suponha que $\sum_{i=1}^{r} a_i(f_i + I) = 0 + I$, onde $a_1, \ldots, a_r \in \mathbb{F}$, então $\sum_{i=1}^{r} a_i f_i \in I$. Logo, $\sum_{i=1}^{r} a_i f_i(p_j) = 0$, isto é, $a_j = 0$, para todo $j = 1, \ldots, r$. Assim, $\{f_1 + I, \ldots, f_r + I\}$ é linearmente independente em $\mathbb{F}[X_1, \ldots, X_n]/I$. Portanto,

$$|V(I)| = r \leq dim(\mathbb{F}[x_1, \ldots, x_n]/I) = |\Delta(I)|.$$

□

Na verdade, pode-se provar um resultado mais refinado (ver [3], Teorema 8.32). Lembre que um ideal I é dito ideal radical se $I = \sqrt{I}$.

Teorema 3.1.6. *Seja $I \subset \mathbb{F}[X_1, \ldots, X_n]$ um ideal tal que $\Delta(I)$ é um conjunto finito e seja L uma extensão algebricamente fechada de $\mathbb{F}$. Então,*

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

é um conjunto finito e $|V_L(I)| \leq |\Delta(I)|$. Mais ainda, se $\mathbb{F}$ é um corpo perfeito e I é um ideal radical então $|V_L(I)| = |\Delta(I)|$.

3.2 Códigos Cartesianos Afins e seus Parâmetros

Em 1998 Fitzgerald e Lax propuseram a seguinte construção de códigos lineares. Sejam $\mathbb{F}_q$ um corpo finito com q elementos, $I = \langle g_1, \ldots, g_t \rangle \subset \mathbb{F}_q[X_1, \ldots, X_n]$ e

$$I_q = \langle g_1, \ldots, g_t, X_1^q - X_1, \ldots, X_n^q - X_n \rangle.$$

Como

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

(ver Lema 2.4 em [28]) segue que $V(I) = V(I_q)$. Consideremos a partir de agora a ordem lexicográfica graduada em $\mathcal{M} \subset \mathbb{F}_q[X_1, \ldots, X_n]$. Da Observação 2.6.8 temos que

$$|\Delta(I_q)| \leq |\Delta(LM(g_1), \ldots, LM(g_t), X_1^q, \ldots, X_n^q)| \leq q^n$$

e do Teorema 3.1.5, segue que $|V(I_q)| \leq |\Delta(I_q)$.

Seja $V(I_q) = \{P_1, \ldots, P_m\}$ e denote por $\overline{\Psi} : \mathbb{F}_q[X_1, \ldots, X_n]/I_q \to \mathbb{F}_q^m$ o homomorfismo

$$\overline{\Psi}(f + I_q) = (f(P_1), \ldots, f(P_m)).$$

Proposição 3.2.1. *O homomorfismo $\overline{\Psi}$ é um isomorfismo entre $\mathbb{F}_q$-espaços vetoriais.*

Demonstração. É imediato que $\overline{\Psi}$ é uma transformação linear, então basta mostrarmos que $\overline{\Psi}$ é sobrejetora e que $\dim(\mathbb{F}_q[X_1, \ldots, X_n]/I_q) = m$. Como $X_i^q - X_i \in I_q$, para todo $i = 1, \ldots, n$ temos que I_q é um ideal radical (ver [3], Prop. 8.14), e também para qualquer extensão L algebricamente fechada de $\mathbb{F}_q$, temos que $V_L(I_q) = V_{\mathbb{F}_q}(I_q)$, assim dos Teoremas 2.6.7 e 3.1.6 temos que $\dim(\mathbb{F}_q[X_1, \ldots, X_n]/I_q) = |\Delta(I_q)| = m$. Do Lema 3.1.4 sabemos que existem polinômios $p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ tais que $p_i(P_j) = \delta_{ij}$, para todo $i, j \in \{1, \ldots, m\}$, assim $\overline{\Psi}(p_i + I_q) = e_i$. Isso prova que $\overline{\Psi}$ é injetivo e portanto um isomorfismo.

□

O próximo conceito foi introduzido por Fitzgerald e Lax em [17].

Definição 3.2.2. *Seja L um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q[X_1, \ldots, X_n]/I_q$. O **código de variedade afim** associado a L, denotado por $C(L)$, é a imagem $\overline{\Psi}(L)$.*

Em [24], López *et al.* definiram os códigos cartesianos afins, um tipo especial de códigos de variedades afins, cuja construção é a seguinte.

Sejam $A_1, \ldots, A_n$ subconjuntos não vazios de $\mathbb{F}_q$ e seja $\mathcal{X} := A_1 \times \cdots \times A_n \subset \mathbb{F}_q^n$.

Seja $f_i = \prod_{c \in A_i}(X_i - c)$ para $i = 1, \ldots, n$. Se $I = \langle f_1, \ldots, f_n \rangle$, claramente o conjunto de zeros de I é $\mathcal{X}$, isto é, $V(I) = \mathcal{X}$. Portanto, f_i é um fator de $X_i^q - X_i = \prod_{c \in \mathbb{F}_q}(X_i - c)$, para todo $i = 1, \ldots, n$, então $I = I_q$.

Considere, para todo $d \in \mathbb{Z}, d \geq 0$, o $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q[X_1, \ldots, X_n]/I$ dado por

$$L_d := \{p + I : p = 0 \text{ ou } \deg(p) \leq d\},$$

onde $\deg(p)$ é o grau total de um polinômio $p \in \mathbb{F}_q[X_1, \ldots, X_n]$.

Definição 3.2.3. *O **código cartesiano afim** $\mathcal{C}_\mathcal{X}(d)$ é a imagem $\overline{\Psi}(L_d)$.*

Observação 3.2.4. *Note que, quando $A_i = \mathbb{F}_q$, para todo $i = 1, \ldots, n$, obtemos os códigos de Reed-Muller generalizados.*

Seja $d_i = |A_i|$ para todo $i = 1, \ldots, n$, então $|V(I)| = d_1 . \cdots . d_n$ é o comprimento de $\mathcal{C}_\mathcal{X}(d)$, para todo $d \geq 0$. Precisamos determinar a dimensão e a distância mínima para os códigos cartesianos afins.

Para determinarmos a dimensão de $\mathcal{C}_\mathcal{X}(d)$ precisaremos dos seguintes resultados auxiliares.

Lema 3.2.5. *O conjunto $\{f_1, \ldots, f_n\}$ é uma base de Gröbner para I.*

Demonstração. Como $f_i = \prod_{c \in A_i}(X_i - c)$ e $|A_i| = d_i$, temos que $LM(f_i) = X_i^{d_i}$ para todo $i = 1, \ldots, n$ de modo que

$$\Delta(I) \subset \{X_1^{\alpha_i} \ldots X_n^{\alpha_n} : 0 \leq \alpha_i < d_i, \text{para todo } i = 1, \ldots, n\}.$$

Como $|V(I)| = d_1 \dots d_n \leq |\Delta(I)| \leq d_1 \dots d_n$, segue que $|\Delta(I)| = d_1 \dots d_n$.

Isto prova que $\{f_1, \dots, f_n\}$ é uma base de Gröbner para I, do contrário, pelo algoritmo de Buchberguer, teríamos que adicionar a $\{f_1, \dots, f_n\}$ um polinômio cujo monômio líder não é múltiplo de $X_i^{d_i}$, para todo $i = 1, \dots, n$, o que implicaria $|\Delta(I)| < d_1 \dots d_n$, gerando uma contradição, pois estaríamos retirando um elemento de $\Delta(I)$ e acrescentando em $\{f_1, \dots, f_n\}$, o que causaria uma desigualdade. □

Lema 3.2.6. *O ideal de $\mathcal{X} := A_1 \times \cdots \times A_n$ é I.*

Demonstração. Do modo que $\mathcal{X}$ e I foram definidos, temos que $I \subset I(\mathcal{X})$. Assim, $V(I(\mathcal{X})) \subset V(I)$.

Como $\mathcal{X} \subset V(I(\mathcal{X}))$ e $V(I) = \mathcal{X}$, então $|V(I)| \geq |V(I(\mathcal{X}))| \geq |\mathcal{X}| = |V(I)|$.

Pela Teorema (3.1.5) e pelo lema (3.2.5), temos que $d_1 \dots d_n \leq |V(I)| \leq |\Delta(I(\mathcal{X}))| \leq |\Delta(I)| = d_1 \dots d_n$.

Como $\{f_1, \dots, f_n\} \subset I \subset I(\mathcal{X})$, pela demonstração do lema anterior temos que $\{f_1, \dots, f_n\}$ é uma base de Gröbner para $I(\mathcal{X})$, daí segue que $I = I(\mathcal{X})$ □

Agora, queremos calcular a dimensão de $\mathcal{C}_\mathcal{X}(d)$. Como $\overline{\Psi}$ é isomorfismo e $\mathcal{C}_\mathcal{X}(d) = \overline{\Psi}(L_d)$ temos que $\dim \mathcal{C}_\mathcal{X}(d) = \dim(L_d)$.

Seja

$$\Delta(I)_{\leq d} := \{M \in \Delta(I) : \deg(M) \leq d\}.$$

Proposição 3.2.7. *O conjunto $\{M + I : M \in \Delta(I)_{\leq d}\}$ é uma base para L_d.*

Demonstração. Do Teorema 2.6.7 sabemos que $\{M + I : M \in \Delta(I)_{\leq d}\}$ é um conjunto linearmente independente que contém L_d. Seja $f \in \mathbb{F}_q[X_1, \dots, X_n]$, $f \neq 0$ com $\deg(f) \leq d$.

Seja r o resto da divisão de f por $\{f_1, \dots, f_n\}$, então $f+I = r+I$ e $\deg(r) < d$. Daí temos que $r \in \Delta(I)_{\leq d}$, implicando que $f + I$ é uma combinação dos elementos de $\{M + I : M \in \Delta(I)_{\leq d}\}$, o que termina a prova.

□

Lema 3.2.8. *A dimensão de $\mathcal{C}_\mathcal{X}(d)$ é $|\Delta(I)_{\leq d}|$. Em particular $\dim \mathcal{C}_\mathcal{X}(d) = d_1 \dots d_n$ e a distância mínima de $\mathcal{C}_\mathcal{X}(d)$ é igual a 1, para todo $d \geq \sum_{i=1}^n (d_i - 1)$.*

Demonstração. Como $\dim \mathcal{C}_\mathcal{X}(d) = \dim L_d$ e $\dim L_d = |\Delta(I)_{\leq d}|$, então $\dim \mathcal{C}_\mathcal{X}(d) = |\Delta(I)_{\leq d}|$.

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

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

Daí, $\Delta(I)_{\leq d} = \Delta(I)$ onde $d \geq \sum_{i=1}^n (d_i - 1)$. Logo $|\Delta(I)_{\leq d}| = |\Delta(I)| = d_1 \cdots d_n$.

Como $\overline{\Psi}(L_d) = \mathbb{F}_q^{d_1 \dots d_n}$, segue da Cota de Singleton que a distância mínima de $\mathcal{C}_\mathcal{X}(d)$ é igual a 1. □

Teorema 3.2.9. *A dimensão de $\mathcal{C}_\mathcal{X}(d)$ para $0 \leq d < \sum_{i=1}^n (d_i - 1)$ é dada por*

$$\dim \mathcal{C}_\mathcal{X}(d) = \binom{n+d}{d} - \sum_{i=1}^{n} \binom{n+d-d_i}{d-d_i} + \cdots +$$

$$+(-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq n} \binom{n+d-d_{i_1}-\cdots-d_{i_k}}{d-d_{i_1}-\cdots-d_{i_k}} + \cdots + (-1)^n \binom{n+d-d_1-\cdots-d_n}{d-d_1-\cdots-d_n}.$$

Demonstração. Do lema anterior, temos que $\dim \mathcal{C}_{\mathcal{X}}(d) = |(\Delta(I)_{\leq d}|$. Então, $\dim \mathcal{C}_{\mathcal{X}}(d)$ é igual ao número de monômios de $\Delta(I)$ da forma $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, com $0 \leq \alpha_i \leq d_i - 1$ e $\alpha_1 + \cdots + \alpha_n \leq d$.

Vamos contar as soluções de $\alpha_1 + \cdots + \alpha_n \leq d$, sabendo que $0 \leq \alpha_i \leq d_i - 1$.

Consideremos os conjuntos:

$$\Omega = \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n : \alpha_1 + \cdots + \alpha_n \leq d\}$$

e

$$\Omega_i = \{(\alpha_1, \ldots, \alpha_n) \in \Omega : \alpha_1 + \cdots + \alpha_n \leq d \text{ e } \alpha_i \geq d_i, \text{para todo } i = 1, \ldots, n\}.$$

Assim,

$$\dim \mathcal{C}_{\mathcal{X}}(d) = |\Delta(I)_{\leq d}| = \left| \left(\Omega - \bigcup_{i=1}^{n} \Omega_i \right) \right| = |\Omega| - \left| \left(\bigcup_{i=1}^{n} \Omega_i \right) \right|.$$

Pelo princípio da inclusão - exclusão, temos que:

$$\left| \left(\bigcup_{i=1}^{n} (\Omega_i) \right) \right| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leq i_1 \leq i_2 \leq \ldots \leq i_k \leq n} |(\Omega_{i_1} \cap \cdots \cap \Omega_{i_k})|.$$

Então,

$$\dim \mathcal{C}_{\mathcal{X}}(d) = |\Delta(I)_{\leq d}| = |\Omega| + \sum_{k=1}^{n} (-1)^{k} \sum_{1 \leq i_1 \leq i_2 \leq \ldots \leq i_k \leq n} |\Omega_{i_1} \cap \cdots \cap \Omega_{i_k}|.$$

Como $|\Omega|$ é o número de soluções inteiras da equação $\alpha_1 + \cdots + \alpha_n \leq d$ temos que

$$|\Omega| = \frac{(n+d)!}{n!d!} = \binom{n+d}{d}.$$

Agora, para calcular $|\Omega_i|$ faremos uma mudança de variável. Faça $\alpha_i = d_i + b_i$, com $b_i \geq 0$, já que $\alpha_i \geq d_i$. Nesse caso, estamos contando o número de soluções inteiras da equação

$$\begin{aligned} & \alpha_1 + \cdots + (\alpha_i) + \cdots + \alpha_n \leq d \\ \Leftrightarrow \quad & \alpha_1 + \cdots + (d_i + b_i) + \cdots + \alpha_n \leq d \\ \Leftrightarrow \quad & \alpha_1 + \cdots + b_i + \cdots + \alpha_n \leq d - d_i. \end{aligned}$$

Novamente, utilizando análise combinatória temos que $|\Omega_i| = \frac{(n+d-d_i)!}{n!(d-d_i)!} = \binom{n+d-d_i}{d-d_i}$.

Procedendo de maneira análoga, temos que

$$|\Omega_{i_1} \cap \cdots \cap \Omega_{i_k}| = \binom{n+d-d_{i_1}-\cdots-d_{i_k}}{d-d_{i_1}-\cdots-d_{i_k}}.$$

Portanto,

$$\begin{aligned}
\dim(\mathcal{C}_{\mathcal{X}}(d)) &= |\Delta(I)_{\leq d}| = |\Omega| + \sum_{k=1}^{n}(-1)^k \sum_{1\leq i_1\leq i_2\leq \ldots \leq i_k\leq n} |\Omega_{i_1}\cap\cdots\cap\Omega_{i_k}| \\
&= \binom{n+d}{d} - \sum_{k=1}^{n}(-1)^k \sum_{1\leq i_1\leq i_2\leq \ldots \leq i_k\leq n} \binom{n+d-d_{i_1}-\cdots-d_{i_k}}{d-d_{i_1}-\cdots-d_{i_k}} \\
&= \binom{n+d}{d} - \sum_{i=1}^{n}\binom{n+d-d_i}{d-d_i} + \cdots + \\
&+ (-1)^k \sum_{1\leq i_1\leq i_2\leq \ldots \leq i_k\leq n} \binom{n+d-d_{i_1}-\cdots-d_{i_k}}{d-d_{i_1}-\cdots-d_{i_k}} + \cdots + \\
&+ (-1)^n \binom{n+d-d_1-\cdots-d_n}{d-d_1-\cdots-d_n}.
\end{aligned}$$

□

Para encontrarmos a distância mínima de $C_{\mathcal{X}}(d)$, para $0 \leq d < \sum_{i=1}^{n}(d_i-1)$, precisaremos do seguinte resultado:

Lema 3.2.10. *Sejam $0 < d_1 \leq \ldots \leq d_n$ e $s < \sum_{i=1}^{n}(d_i-1)$ inteiro.*
Seja $m(\alpha_1,\ldots,\alpha_n) = \prod_{i=1}^{n}(d_i-\alpha_i)$, onde $0 \leq \alpha_i < d_i$ é um inteiro, para todo $i = 1,\ldots,n$. Então

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

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

Demonstração. Considere

$$\Omega_s = \{(\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n : \alpha_1+\cdots+\alpha_n \leq s \text{ com } 0 \leq \alpha_i < d_i, i \in \{1,\ldots,n\}\}.$$

Para $(\alpha_1,\ldots,\alpha_n) \in \Omega_s$, definimos $m(\alpha_1,\ldots,\alpha_n) = (d_1-\alpha_1)(d_2-\alpha_2)\ldots(d_n-\alpha_n) > 0$.
Seja $M = \{m(\alpha_1,\ldots,\alpha_n) : (\alpha_1,\ldots,\alpha_n) \in \Omega_s\}$. Queremos calcular $\min M$.
Provaremos primeiro que se $m(\alpha_1,\ldots,\alpha_n) = \min M$ então $\alpha_1+\cdots+\alpha_n = s$.
De fato, suponha por absurdo que $\alpha_1+\cdots+\alpha_n < s$. Por hipótese $s < \sum_{i=1}^{n}(d_i-1)$.
Como $\alpha_1+\cdots+\alpha_n < s$, então existe um j tal que $\alpha_j \leq d_i - 2$.
Isso implica que $(\alpha_1,\ldots,\alpha_{j+1},\ldots\alpha_n) \in \Omega_s$.
Daí,

$$\begin{aligned}
m(\alpha_1,\ldots,\alpha_{j+1},\ldots,\alpha_n) &= (d_1-\alpha_1)(d_2-\alpha_2)\ldots(d_j-(\alpha_j+1))\ldots(d_n-\alpha_n) \\
&= (d_1-\alpha_1)(d_2-\alpha_2)\ldots(d_j-\alpha_j-1)\ldots(d_n-\alpha_n) \\
&< (d_1-\alpha_1)(d_2-\alpha_2)\ldots(d_n-\alpha_n) = m(\alpha_1,\ldots,\alpha_n).
\end{aligned}$$

Assim, $m(\alpha_1,\ldots,\alpha_n)$ não é o valor mínimo.
Portanto, o mínimo ocorre quando $\alpha_1+\cdots+\alpha_n = s$.
Por hipótese temos que $s = \sum_{i=1}^{k}(d_i-1)+l$ com $0 \leq k \leq n-1$ e $0 < l \leq d_k - 1$.
Provaremos agora que o mínimo de M é $m(\alpha_1,\ldots,\alpha_n)$ onde

$$(\alpha_1,\ldots,\alpha_n) = (d_1-1,..,d_k-1,l,0,\ldots,0).$$

Seja $(\beta_1,\ldots,\beta_n) \in \Omega_s$ tal que $m(\beta_1,\ldots,\beta_n) = \min M$ e $\beta_1+\cdots+\beta_n = s$

Temos dois casos:

Caso $k = 0$.

Nesse caso $s = l$. Suponha que $\beta_1 + \cdots + \beta_n = l$ e $m(\beta_1, \ldots, \beta_n) = \min M$

Se $\beta_1 < l$, existe $2 \leq i \leq n : \beta_i > 0$. Daí $\beta_1 + \beta_i \leq 0$ ou $\beta_1 + \beta_i > 0$.

Se $\beta_1 < l$, então existe $2 \leq i \leq n$ tal que $\beta_1 + \beta_i \leq l$, pois $\beta_1 + \cdots + \beta_n = l$.

Temos que $(\alpha_1, \ldots, \alpha_n) = (\beta_1 + \beta_i, \beta_2, \ldots, 0, \ldots, \beta_n)$ (o 0 se encontra na i-ésima entrada).

Assim,

$$\begin{aligned} m(\alpha_1, \ldots, \alpha_n) &= (d_1 - (\beta_1 + \beta_i))(d_2 - \beta_2) \ldots (d_i) \ldots (d_n - \beta_n), \\ m(\beta_1, \ldots, \beta_n) &= (d_1 - \beta_1)(d_2 - \beta_2) \ldots (d_i - \beta_i) \ldots (d_n - \beta_n). \end{aligned}$$

Logo,

$$\begin{aligned} m(\beta_1, \ldots, \beta_n) - m(\alpha_1, \ldots, \alpha_n) &= ((d_1 - \beta_1)(d_i - \beta_i) - (d_1 - (\beta_1 + \beta_i)d_i) \prod_{j=2, j \neq i}^{n} (d_j - \beta_j) \\ &= (\beta_i(d_i - d_1) + \beta_1\beta_i) \prod_{j=2, j \neq i}^{n} (d_j - \beta_j) \geq 0, \end{aligned}$$

pois $\beta_i \geq 0$, $d_i - d_1 \geq 0$ e $\beta_1\beta_i \geq 0$.

Como $m(\beta_1, \ldots, \beta_n)$ é mínimo, então $m(\alpha_1, \ldots, \alpha_n)$ também é mínimo com $\beta_1 < \alpha_1$.

Se $d_1 < l$, então repetimos o mesmo processo e encontramos $(\gamma_1, \ldots, \gamma_n)$ tal que $m(\gamma_1, \ldots, \gamma_n))$ também é mínimo com $\beta_1 \leq d_1 \leq \gamma_1$.

Isso quer dizer que, em algum momento vamos obter a n-upla $(l, 0, \ldots, 0)$ tal que $m(l, 0, \ldots, 0)$ é o mínimo de M. Assim, $\min M = (d_1 - l)d_2 \ldots d_n$.

Caso $k > 0$**:**

Suponha que exista $1 \leq i \leq k$, $\beta_i < d_i - 1$.

Existe $k + 1 \leq j \leq n$ tal que $\beta_j > 0$, pois $\beta_1 + \cdots + \beta_k < \sum_{i=1}^{k}(d_i - 1)$. Isso implica que $\beta_{k+1} + \cdots + \beta_n > l$.

Vamos estudar dois casos:

i) $\beta_i + \beta_j \leq d_i - 1$;

ii) $\beta_i + \beta_j > d_i - 1$.

No caso i), suponha que $\beta_i + \beta_j \leq d_i - 1$, $i \leq i \leq k < k + 1 \leq j \leq n$.

Assim,

$$(\alpha_1, \ldots, \alpha_n) = (\beta_1, \ldots, \beta_i + \beta_j, \ldots, 0, \ldots, \beta_n)$$

em que a j-ésima coordenada é nula.

Daí,

$$\begin{aligned} m(\alpha_1, \ldots, \alpha_n) &= (d_1 - \beta_1) \ldots (d_i - \beta_i - \beta_j) \ldots (d_j) \ldots (d_n - \beta_n), \\ m((\beta_1, \ldots, \beta_n) &= (d_1 - \beta_1) \ldots (d_n - \beta_n). \end{aligned}$$

Logo,

$$\begin{aligned} m(\beta_1, \ldots, \beta_n) - m(\alpha_1, \ldots, \alpha_n) &= ((d_i - \beta_i)(d_j - \beta_j) - (d_i - \beta_i - \beta_j)d_j) \prod_{t=1, t \neq i, j}^{n} (d_t - \beta_t) \\ &= (-d_i\beta_j + \beta_i\beta_j + \beta_j d_j) \prod_{t=1, t \neq i, j}^{n} (d_t - \beta_t) \\ &= \beta_j(d_j - d_i + \beta_i) \prod_{t=1, t \neq i, j}^{n} (d_t - \beta_t) \geq 0, \end{aligned}$$

já que $b_j > 0$, $d_j - d_i \geq 0$ e $\beta_i \geq 0$.

Sendo assim, a n-upla $(\alpha_1, \ldots, \alpha_n)$ também satisfaz a condição de ser um mínimo.

No caso ii), suponha que $\beta_i + \beta_j > d_i - 1$ com $i \leq i \leq k < k+1 \leq j \leq n$.

Daí, $(\alpha_1, \ldots, \alpha_n) = (\beta_1, \ldots, d_i - 1, \ldots, \beta_i + \beta_j - (d_1 - 1), \ldots, \beta_n)$.

Assim,

$$\begin{aligned} m(\alpha_1, \ldots, \alpha_n) &= (d_1 - \beta_1) \ldots (1) \ldots (d_j - \beta_i + \beta_j) + d_i - 1) \ldots (d_n - \beta_n), \\ m(\beta_1, \ldots, \beta_n) &= (d_1 - \beta_1) \ldots (d_i - \beta_i) \ldots (d_j - \beta_j) \ldots (d_n - \beta_n). \end{aligned}$$

Com procedimento análogo, temos que:

$$m(\beta_1, \ldots, \beta_n) - m(\alpha_1, \ldots, \alpha_n) \geq 0$$

e isso implica que $m(\alpha_1, \ldots, \alpha_n)$ também é mínimo, já que $m(\beta_1, \ldots, \beta_n)$ é mínimo por hipótese.

Portanto, se existe $1 \leq i \leq k$ tal que $\beta_i < d_i - 1$, então existe $(\alpha_1, \ldots, \alpha_n)$ tal que $m(\alpha_1, \ldots, \alpha_n) = \min M$ com $\alpha_t = \beta_t$ para $1 \leq t \leq k, t \neq i$ e $\alpha_i > \beta_i$.

Isso quer dizer que, existe $(\alpha_1, \ldots, \alpha_n) = (d_1 - 1, \ldots, d_k - 1, \alpha_{k+1}, \ldots, \alpha_n)$ tal que

$$m(\alpha_1, \ldots, \alpha_n) = \min M.$$

Então $m(\alpha_1, \ldots, \alpha_n) = (d_{k+1} - \alpha_{k+1}) \ldots (d_n - \alpha_n)$ onde $\alpha_{k+1} + \cdots + \alpha_n = l$.

Pelo que foi feito no caso $k = 0$, o valor mínimo é $(d_{k+1} - l).d_{k+2} \ldots d_n$, como queríamos demonstrar.

□

Teorema 3.2.11. *Seja $0 \leq d < \sum_{i=1}^{n}(d_i - 1)$. Então a distância mínima de $\mathcal{C}_{\mathcal{X}}(d)$ é*

$$(d_{k+1} - l) \prod_{i=k+2}^{n} d_i,$$

onde k e l são unicamente definidos por $d = \sum_{i=1}^{k}(d_i - 1) + l$ com $0 \leq l < d_{k+1} - 1$.

Como no resultado anterior, se $k+1 = n$ teremos que $\prod_{i=k+2}^{n} d_i = 1$, e se $d < d_1 - 1$ então $k = 0$ e $l = d$.

Demonstração. Seja $F \in L_d$ e seja $J_F = (F, f_1, \ldots, f_n)$, então o número de zeros da palavra do código $\overline{\Psi}(F + I) = (F(P_1), \ldots, F(P_m))$ é igual a

$$|V(F) \cap \{P_1, \ldots, P_m\}| = |V(F) \cap V(f_1, \ldots, f_n)| = |V(F, f_1, \ldots, f_n)| = |V(J_F)|.$$

Assim, temos que $w(\overline{\Psi}(F + I)) = \prod_{i=1}^{n} d_i - |V(J_F)|$.

Pelo teorema 3.1.5 obtemos $|V(J_F)| \leq |\Delta(J_F)|$. Seja $M = X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ o monômio líder de F, pela observação 2.6.8 segue que $(\Delta(J_f)) \subset \Delta(M, X_1^{d_1}, \ldots, X_n^{d_n})$. Há $\prod_{i=1}^{n} d_i$ elementos da forma $X_1^{\lambda_1} \ldots X_n^{\lambda_n}$ com $0 \leq \lambda_i \leq d_i - 1$. Desses elementos, $\prod_{i=1}^{n}(d_i - \alpha_i)$ são múltiplos de $M = X_1^{\alpha_1} \ldots X_n^{\alpha_n}$, pois estamos contando os elementos $X_1^{\lambda_1} \ldots X_n^{\lambda_n}$ que satisfazem $\alpha_i \leq \lambda_i \leq d_i - 1$. Assim,

$$|\Delta(M, f_1, \ldots, f_n)| = \prod_{i=1}^{n} d_i - \prod_{i=1}^{n}(d_i - \alpha_i).$$

Daí, $|\Delta(J_F)| \leq \prod_{i=1}^{n} d_i - \prod_{i=1}^{n}(d_i - \alpha_i)$. Logo, $w(\overline{\Psi}(F + I)) \geq \prod_{i=1}^{n}(d_i - \alpha_i)$ e pelo lema anterior temos que $w(\overline{\Psi}(F + I)) \geq (d_{k+1} - l) \prod_{i=k+2}^{n} d_i$, pois $(d_{k+1} - l) \prod_{i=1}^{n}$ é o mínimo de $m(\alpha_1, \ldots, \alpha_n)$.

Para verificar que essa cota é atingida, tome $A_i = \{a_{i1}, \ldots, a_{id_i}\}$ para $i = 1, \ldots, n$ e seja

$$G(X_1, \ldots, X_n) = \left(\prod_{i=1}^{k} \prod_{j=1}^{d_i - 1} (X_i - a_{ij}) \right) \prod_{j=1}^{l} (X_{k+1} - a_{k+1_j}),$$

então

$$\deg(G) = \deg \left(\prod_{i=1}^{k} \prod_{j=1}^{d_i - 1} (X_i - a_{ij}) \right) + \deg \left(\prod_{j=1}^{l} (X_{k+1} - a_{k+1_j}) \right) = \sum_{i=1}^{k} (d_i - 1) + l = d.$$

Observe que $A_1 \times \cdots \times A_n$ possui $\prod_{i=1}^{n} d_i$ elementos, e calculemos o número de elementos em $A_1 \times \cdots \times A_n$ que não são raízes de G.

Nas k primeiras entradas temos uma única opção que é $(a_{id_1}, \ldots, a_{id_k})$, na $(k+1)$-ésima coordenada temos $d_{k+1} - l$ opções e a partir de $k+1$ temos d_i opções, para cada $i > k+1$, então G não se anula em $(d_{k+1} - l) \prod_{i=k+2}^{n} d_i$ zeros em $A_1 \times \cdots \times A_n$, assim $w(\overline{\Psi}(G + I)) = (d_{k+1} - l) \prod_{i=k+2}^{n} d_i$.

□

CAPÍTULO 4

UMA FAMÍLIA DE CÓDIGOS LOCALMENTE RECUPERÁVEIS

A classe dos códigos localmente recuperáveis foi introduzida em 2012 por Gopalan *et al.* (ver [21]). De um modo geral, as técnicas de recuperação local nos permitem reparar dados codificados perdidos por um procedimento local, o que significa utilizar uma pequena quantidade de dados em vez de todas as informações contidas em uma palavra do código. A ideia era garantir uma comunicação confiável ao usar sistemas de armazenamento distribuído e em nuvem. Assim, os autores definem que um código tem localidade r se uma entrada na posição i da palavra do código de tamanho m, puder ser recuperada de um conjunto (que pode variar de acordo com o i) de no máximo r outras entradas, para todo $i = 1, \ldots, m$. Isso garantiria a recuperação de uma palavra do código mesmo na presença de um apagamento devido, por exemplo, a uma falha de algum ponto de conexão na rede.

No mesmo ano, Prakash et al. (ver [25]) introduziram o conceito de códigos com localidade (r, δ), também chamados de códigos (r, δ)-localmente recuperáveis, que são códigos de comprimento n tais que para toda posição $i \in \{1, \ldots, m\}$, existe um subconjunto $S_i \subset \{1, \ldots, m\}$ contendo i e de tamanho no máximo $r + \delta - 1$, tal que a i-ésima entrada da palavra do código pode ser recuperada de qualquer subconjunto de r entradas com posições em $S_i \setminus \{i\}$ e pode-se recuperar qualquer entrada, mesmo com $\delta - 2$ outros apagamentos no código.

Neste capítulo estão as nossas contribuições e a referência é o nosso artigo [2].

4.1 Uma família de códigos localmente recuperáveis

Seja $\mathbb{F}_q$ um corpo finito com q elementos.

Definição 4.1.1. *Sejam m, r, δ inteiros positivos, onde $\delta \geq 2$ e $r + \delta - 1 \leq m$. Dizemos que um código (linear) $\mathcal{C} \subset \mathbb{F}_q^m$ é (r, δ)-localmente recuperável se para todo $i \in \{1, \ldots, m\}$ existe um subconjunto de posições $S_i \subset \{1, \ldots, m\}$, contendo i e de cardinalidade no máximo $r + \delta - 1$, tal que o código perfurado obtido removendo as entradas que não estão em S_i tem distância mínima pelo menos δ.*

A condição sobre a distância mínima na definição acima mostra que não se pode ter duas palavras distintas do código perfurado que coincidam em (pelo menos) r posições, assim, quaisquer r posições no conjunto S_i determinam as $\delta - 1$ posições restantes.

A definição de códigos com localidade (r, δ) foi motivada por características de armazenamento em nuvem. Os dados ficam armazenados em vários servidores e ao montarmos uma

n-upla para ser transmitida, os dados vêm de vários servidores e as vezes, um servidor pode falhar e não enviar nada, ou seja, temos um apagamento. Na figura abaixo, ilustramos esta situação. Temos uma 13-upla e um apagamento em $i = 9$. Seja $S_9 = \{1, 2, 3, 4, 5, 6, 7, 9, 13\}$ o conjunto de recuperação. Suponha que conhecemos $r = 4$ entradas (asteriscos em verde), então é possível recuperar $\delta - 1 = 5$ entradas, de acordo com as condições da definição.

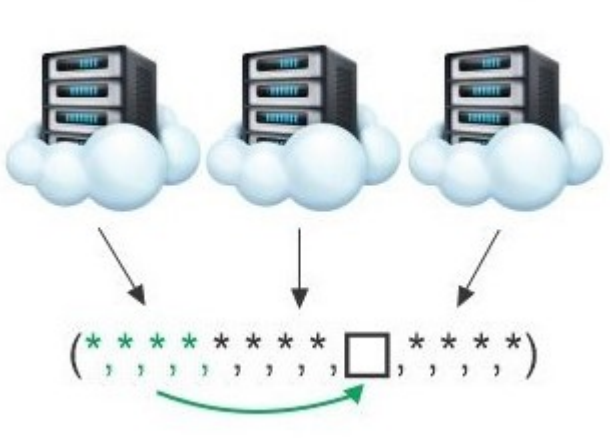

Figura 4.1: Armazenamento em nuvem

O próximo teorema estabelece uma cota superior para a distância mínima dos códigos (r, δ)-localmente recuperáveis.

Teorema 4.1.2. *A distância mínima $d_{\min}$ de um código $\mathcal{C}$ com localidade (r, δ) satisfaz*

$$d_{\min} \leq m - k + 1 - \left(\left\lceil \frac{k}{r} \right\rceil - 1 \right) (\delta - 1). \tag{4.1}$$

Demonstração. Ver [25, Teorema 2]. □

A cota acima é chamada de **cota do tipo Singlenton** vinculada a Prakash *et al.* Um código com localidade (r, δ) em que $d_{\min} = m - k + 1 - \left(\left\lceil \frac{k}{r} \right\rceil - 1 \right) (\delta - 1)$ é dito **ótimo**.

Recordaremos rapidamente como é feita a construção dos códigos cartesianos afins, utilizando as notações da referência [2]. Seja $\mathbb{F}_q$ um corpo finito com q elementos, seja $K_1, \ldots, K_n$ uma coleção de subconjuntos não vazios de $\mathbb{F}_q$, e seja

$$\mathcal{X} := K_1 \times \cdots \times K_n := \{(\alpha_1, \ldots, \alpha_n) | \, \alpha_i \in K_i \text{ para todo } i\} \subset \mathbb{F}_q^n.$$

Seja $d_i := |K_i|$ para $i = 1, \ldots, n$, então claramente $|\mathcal{X}| = \prod_{i=1}^{n} d_i =: m$, e seja $\mathcal{X} = \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_m\}$. Já vimos que o ideal de polinômios em $\mathbb{F}_q[X_1, \ldots, X_n]$ que se anulam em $\mathcal{X}$ é

$$I(\mathcal{X}) = I_{\mathcal{X}} = \left\langle \prod_{\alpha_1 \in K_1} (X_1 - \alpha_1), \ldots, \prod_{\alpha_n \in K_n} (X_n - \alpha_n) \right\rangle.$$

Dito isto, temos que o morfismo de avaliação

$$\Psi : \mathbb{F}_q[X_1, \ldots, X_n] \to \mathbb{F}_q^m$$

dado por $f \mapsto (f(\boldsymbol{\alpha}_1), \ldots, f(\boldsymbol{\alpha}_m))$ é uma transformação linear sobre $\mathbb{F}_q$ onde $\ker \Psi = I_{\mathcal{X}}$. Na verdade, Ψ é um homomorfismo sobrejetor entre $\mathbb{F}_q$-espaços vetoriais, pois para cada $i \in \{1, \ldots, m\}$ existe um polinômio tal que $f_i(\boldsymbol{\alpha}_j)$ é igual a 1, se $j = i$, ou 0, se $j \neq i$.

Seja d um inteiro não negativo. No que segue denotaremos por $\mathbb{F}_q[X_1, \ldots, X_n]_{\leq d}$ o $\mathbb{F}_q$-espaço vetorial formado por todos os polinômios de grau até d, juntos com o polinômio nulo.

Definição 4.1.3. *Seja d um inteiro não-negativo o* código cartesiano afim *(de ordem d) $\mathcal{C}_{\mathcal{X}}(d)$ definido sobre os conjuntos $K_1, \ldots, K_n$ é a imagem, via Ψ, do conjunto dos polinômios em $\mathbb{F}_q[X_1, \ldots, X_n]_{\leq d}$*

Em [24] os autores provaram que podemos ignorar, no produto cartesiano, conjuntos que só tenham um elemento e podemos supor, sem perda de generalidade que $2 \leq d_1 \leq \cdots \leq d_n$. A seguir, apresentaremos uma família de códigos que são subcódigos dos códigos cartesianos afins e em seguida, mostraremos que eles são (r, δ)-localmente recuperáveis.

Definição 4.1.4. *Sejam d e δ inteiros com $d \geq 0$ e $\delta \geq 2$, seja $s \in \{1, \ldots, n\}$ e seja $\mathcal{P}_d^{(\delta,s)}$ o conjunto de polinômios $f \in \mathbb{F}_q[X_1, \ldots, X_n]_{\leq d}$ tais que $\deg_{X_s} f < d_s - \delta + 1$, juntamente com o polinômio nulo. Denotamos por $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$ o código que é a imagem, via Ψ, do conjunto $\mathcal{P}_d^{(\delta,s)}$.*

Teorema 4.1.5. *Sejam $n \geq 2$ um número inteiro, $K_1, \ldots, K_n$ subconjuntos de $\mathbb{F}_q$ com $|K_i| = d_i$, para todo $i = 1, \ldots, n$, e $\mathcal{X} = K_1 \times \ldots \times K_n$. Sejam ainda $s \in \{1, ..., n\}$ e $\delta \geq 2$ um inteiro tal que $d_s - \delta + 1 \geq 1$. Então, para cada inteiro d não-negativo, o código $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$ é localmente recuperável com localidade (r, δ), onde $r = d_s - \delta + 1$.*

Demonstração. Seja $f \in \mathcal{P}_d^{(\delta,s)}$, então $(f(\boldsymbol{\alpha}_1), \ldots, f(\boldsymbol{\alpha}_m)) \in \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$.

Seja $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathcal{X}$ e seja

$$S_{\boldsymbol{\alpha}} = \{(\alpha_1, \ldots, \alpha_{s-1}, \beta, \alpha_{s+1}, \ldots, \alpha_n) \mid \beta \in K_s\} \subset \mathcal{X},$$

um conjunto que tem $d_s = r + \delta - 1$ elementos. Suponha que existam $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_r \in S_{\boldsymbol{\alpha}}$ tais que conhecemos os valores $f(\boldsymbol{\beta}_k) =: c_k$, para $k \in \{1, \ldots, r\}$. Provaremos que podemos deduzir o valor de $f(\boldsymbol{\beta})$ para qualquer $\boldsymbol{\beta} \in S_{\boldsymbol{\alpha}}$. Escreva $f = \sum_{i=0}^{r-1} g_i X_s^i$, onde $g_1, \ldots, g_{r-1}$ são polinômios nas variáveis $X_1, \ldots, X_{s-1}, X_{s+1}, \ldots, X_n$, e seja $b_i := g_i(\alpha_1, \ldots, \alpha_{s-1}, \alpha_{s+1}, \ldots, \alpha_n)$ para $i = 0, \ldots, r-1$. Denotando por β_k a k-ésima coordenada de $\boldsymbol{\beta}_k$, para $k = 1, \ldots, r$, obtemos que

$$c_k = f(\boldsymbol{\beta}_k) = \sum_{i=0}^{r-1} b_i \beta_k^i, \quad \text{para } k \in \{1, \ldots, r\}.$$

Este sistema de equações pode ser reescrito como uma equação matricial

$$\begin{pmatrix} 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{r-1} \\ 1 & \beta_2 & \beta_2^2 & \cdots & \beta_2^{r-1} \\ 1 & \beta_3 & \beta_3^2 & \cdots & \beta_3^{r-1} \\ 1 & : & : & \ddots & : \\ 1 & \beta_r & \beta_r^2 & \cdots & \beta_r^{r-1} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ : \\ b_{r-1} \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ : \\ c_r \end{pmatrix},$$

que tem solução única $(b_0, b_1, \ldots, b_{r-1})$, pois a matriz quadrada $r \times r$ é uma matriz de Vandermonde. Isso nos permite determinar $f(\boldsymbol{\beta})$ qualquer que seja $\boldsymbol{\beta} \in S_{\boldsymbol{\alpha}}$.

□

4.2 Sobre a dimensão de $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$

Nesta seção, vamos determinar a dimensão de $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$. Para isso, faremos um argumento similar ao utilizado para provar a fórmula da dimensão dos códigos cartesianos afins (Teorema 3.2.9).

Proposição 4.2.1. *Seja* $\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)} = \{M \in \Delta(I_{\mathcal{X}})_{\leq d} \mid \deg_{X_s} M < d_s - \delta + 1\}$. *Então* $\dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = |\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)}|$.

Demonstração. Dado $f \in \mathcal{P}_d^{(\delta,s)}$, seja $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ o seu resto na divisão por $\{f_1, \ldots, f_n\}$, então $\Psi(f) = \Psi(g)$. Pelo algoritmo da divisão, sabemos que qualquer monômio que apareça em g não é múltiplo de $LM(f_i) = X_i^{d_i}$, para todo $i = 1, \ldots, n$, e sabemos também que $\deg g \leq \deg f$ e $\deg_{X_s} g < d_s - \delta + 1$. Assim, $g \in \mathcal{P}_d^{(\delta,s)}$ e, além disso, g é uma combinação linear de monômios em $\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)}$. Isto mostra que $\dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) \leq |\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)}|$.

No capítulo 3 foi definido

$$\overline{\Psi} \colon \mathbb{F}_q[X_1, \ldots, X_n]/I_{\mathcal{X}} \to \mathbb{F}_q^m.$$

Pelas definições de $\overline{\Psi}$ e Ψ temos que $\overline{\Psi}(f + I_{\mathcal{X}}) = \Psi(f)$.

Sabemos que $\overline{\Psi}$ é um isomorfismo e é claro que $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) = \{\overline{\Psi}(h + I_{\mathcal{X}}) \mid h \in \langle \Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)} \rangle\}$, onde $\langle \Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)} \rangle$ é um $\mathbb{F}_q$-espaço vetorial gerado pelos monômios em $\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)}$.

Como $\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)} \subset \Delta(I_{\mathcal{X}})$, sabemos pelo resultado de Buchberger (ver Teorema 2.6.7) que as classes em $\mathbb{F}_q[X_1, \ldots, X_n]/I_{\mathcal{X}}$ dos monômios em $\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)}$ são linearmente independentes sobre $\mathbb{F}_q$, assim, concluimos que

$$\dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = |\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)}|.$$

□

Seja

$$\tilde{d} := \sum_{\substack{i=1 \\ i \neq s}}^{n} (d_i - 1) + d_s - \delta.$$

Corolário 4.2.2. *Se* $d \geq \tilde{d}$, *então* $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) = \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})$, *e*

$$\dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})) = (d_s - \delta + 1) \prod_{\substack{i=1 \\ i \neq s}}^{n} d_i.$$

Também $\dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d} - 1)) = \dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})) - 1$.

Demonstração. A partir da demonstração anterior, obtemos que se $M \in \Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)}$, então $\deg_{X_s}(M) < d_s - \delta + 1$ e $\deg_{X_i}(M) < d_i$, para todo $i \in \{1, \ldots, n\} \setminus \{s\}$. Assim, se $d \geq \tilde{d}$ temos que $\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)} = \Delta(I_{\mathcal{X}})_{\leq \tilde{d}}^{(\delta,s)}$ que implica $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) = \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})$. Temos também que

$$\begin{aligned}
&\dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})) = \\
&= |\{X_1^{a_1} \cdots X_n^{a_n} \mid 0 \leq a_i < d_i\,,\ i = 1, \ldots, n, i \neq s,\ \text{e } 0 \leq a_s < d_s - \delta + 1\}| \\
&= (d_s - \delta + 1) \prod_{\substack{i=1 \\ i \neq s}}^{n} d_i.
\end{aligned}$$

Observe que em $\Delta(I_{\mathcal{X}})^{(\delta,s)}_{\leq \tilde{d}}$ há apenas um monômio de grau $\tilde{d}$, de modo que

$$\dim(\mathcal{D}^{(\delta,s)}_{\mathcal{X}}(\tilde{d}-1)) = \dim(\mathcal{D}^{(\delta,s)}_{\mathcal{X}}(\tilde{d})) - 1.$$

□

Agora, para $1 \leq d < \tilde{d}$, apresentaremos uma fórmula para a dimensão de $\mathcal{D}^{(\delta,s)}_{\mathcal{X}}(d)$ em termos da dimensão de certos códigos cartesianos afins, e para isso introduziremos a seguinte notação.

Definição 4.2.3. *Para $s \in \{1,\ldots,n\}$ denotamos por $\mathcal{X}_s$ o produto*

$$\mathcal{X}_s = K_1 \times \cdots \times K_{s-1} \times K_{s+1} \times \cdots \times K_n.$$

No próximo resultado relacionamos a dimensão de $\mathcal{D}^{(\delta,s)}_{\mathcal{X}}(d)$ com as dimensões de $\mathcal{C}_{\mathcal{X}}(d)$ e do código cartesiano afim $\mathcal{C}_{\mathcal{X}_s}(d)$.

Teorema 4.2.4. *Seja $s \in \{1,\ldots,n\}$ e seja d um inteiro tal que $1 \leq d < \tilde{d}$.*

Se $1 \leq d < r = d_s - \delta + 1$, então $\dim \mathcal{D}^{(\delta,s)}_{\mathcal{X}}(d) = \dim \mathcal{C}_{\mathcal{X}}(d)$, e se $r \leq d \leq \tilde{d}$, então

$$\dim \mathcal{D}^{(\delta,s)}_{\mathcal{X}}(d) = \dim \mathcal{C}_{\mathcal{X}}(d) - \sum_{i=0}^{\delta-2} \dim \mathcal{C}_{\mathcal{X}_s}(d-r-i), \tag{4.2}$$

onde $\dim_{\mathbb{F}_q} \mathcal{C}_{\mathcal{X}_s}(d-r-i) = 0$ se $d-r-i < 0$.

Demonstração. Se $1 \leq d < r = d_s - \delta + 1$, então de acordo com as definições 3.2.3 e 4.1.4 segue que $\mathcal{D}^{(\delta,s)}_{\mathcal{X}}(d) = \mathcal{C}_{\mathcal{X}}(d)$, então assumimos agora que $r \leq d \leq \tilde{d}$.

Defina os seguintes conjuntos:

$$\begin{aligned} \Omega_d &= \{(a_1,\ldots,a_n) \in \mathbb{N}^n \mid 0 \leq a_i < d_i \text{ , para } 1 \leq i \leq n, a_1 + \cdots + a_n \leq d\}; \\ \Omega^{(\delta,s)}_d &= \{(a_1,\ldots,a_n) \in \Omega_d \mid a_s \leq d_s - \delta\}. \end{aligned}$$

A partir dos argumentos presentes na demostração do teorema 3.2.9, obtemos que $\dim \mathcal{C}_{\mathcal{X}}(d) = |\Omega_d|$ e $\dim \mathcal{D}^{(\delta,s)}_{\mathcal{X}}(d) = |\Omega^{(\delta,s)}_d|$. Para qualquer $(a_1,\ldots,a_n) \in \Omega_d$ temos também que $a_s \leq d_s - \delta$ ou $a_s = d_s - \delta + 1 + i$ para algum i no intervalo $0 \leq i \leq \delta - 2$ (pois $a_s \leq d_s - 1$).

Se $a_s = d_s - \delta + 1 + i = r + i$, então

$$a_1 + \cdots + a_{s-1} + a_{s+1} + \cdots + a_n \leq d - r - i,$$

e para $0 \leq i \leq \delta - 2$ definimos

$$\Omega^{(0)}_{s,d-r-i} = \{(a_1,\ldots,a_n) \in \Omega_{d-r-i} \mid a_s = 0\},$$

de modo que $\Omega^{(0)}_{s,d-r-i} = \emptyset$ se i é tal que $d-r-i < 0$.

Assim, temos

$$|\Omega_d| = |\Omega^{(\delta,s)}_d| + \sum_{i=0}^{\delta-2} |\Omega^{(0)}_{s,d-r-i}|$$

e como $\dim \mathcal{C}_{\mathcal{X}_s}(d-r-i) = |\Omega^{(0)}_{s,d-r-i}|$, para todo $i \in \{0,\ldots,\delta-2\}$, a equação acima implica na equação (4.2) como queríamos demonstrar. □

4.3 Distância mínima e códigos ótimos

Nesta seção, relacionamos a distância mínima de $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$ com a distância mínima do código cartesiano afim $\mathcal{C}_{\mathcal{X}}(d)$. No que segue, denotaremos por $W^{(1)}(C)$ a distância mínima de um código C.

Seja d um inteiro no intervalo $1 \leq d < \sum_{i=1}^{n}(d_i - 1)$, e sejam k e ℓ unicamente definidos por $d = \sum_{i=1}^{k}(d_i - 1) + \ell$, com $0 < \ell \leq d_{k+1} - 1$ (se $d < d_1 - 1$ então faça $k = 0$ e $\ell = d$, se $k + 1 = n$ então entendemos que $\prod_{i=k+2}^{n} d_i = 1$).

Lembre que

$$W^{(1)}(\mathcal{C}_{\mathcal{X}}(d)) = (d_{k+1} - \ell) \prod_{i=k+2}^{n} d_i \tag{4.3}$$

(ver Teorema 3.2.11).

Teorema 4.3.1. *Seja* $d = \sum_{i=1}^{k}(d_i - 1) + \ell$ *onde* $0 \leq k < n$ *e* $0 < \ell \leq d_{k+1} - 1$.*Então*

$$\begin{aligned} W^{(1)}(\mathcal{C}_{\mathcal{X}}(d)) &\leq W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) \\ &\leq m - \dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) - \left(\left\lceil \frac{\dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)}{r} \right\rceil - 1 \right)(\delta - 1) + 1., \end{aligned} \tag{4.4}$$

onde $m = \prod_{i=1}^{n} d_i$, $r = d_s - \delta + 1$ *e para* $x \in \mathbb{R}$, $\lceil x \rceil$ *é o menor inteiro* t *tal que* $x \leq \lceil t \rceil$. *Se*

(i) $k + 2 \leq n$ *e* $d_{k+2} \leq d_s$, *ou*

(ii) $d_s \leq d_{k+1}$ *e* $0 \leq d_s - (d_{k+1} - \ell) < r$,

então $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$.

Demonstração. Como $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) \subset \mathcal{C}_{\mathcal{X}}(d)$, temos que $W^{(1)}(\mathcal{C}_{\mathcal{X}}(d)) \leq W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d))$.

Pelo teorema 4.1.5 sabemos que $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$ é localmente recuperável com localidade (r, δ), então podemos aplicar o Teorema 4.1.2 e obtermos a segunda desigualdade de (4.4).

Suponha que $k + 2 \leq n$ e $d_{k+2} \leq d_s$. Vamos considerar dois casos, $s \geq k + 2$ e $s < k + 2$.

Suponhamos primeiro que $s \geq k + 2$. Considere um elemento $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathcal{X}$, e considere ℓ elementos distintos $\beta_1, \ldots, \beta_\ell \in K_{k+1}$.

Defina o polinômio

$$f = \prod_{i=1}^{k} \prod_{\substack{\alpha \in K_i \\ \alpha \neq \alpha_i}} (X_i - \alpha) \cdot \prod_{i=1}^{\ell} (X_{k+1} - \beta_i). \tag{4.5}$$

Observe que $f \in \mathcal{P}_d^{(\delta,s)}$ de modo que $\Psi(f) \in \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$. Denotando por $w(v)$ o peso de uma palavra do código v temos que $w(\Psi(f)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$, e terminamos.

Suponha agora que $s < k + 2$, para $d_{k+2} \leq d_s$ devemos ter que $K_s = K_{k+1} = K_{k+2}$. Claramente $s \in \{1, \ldots, k + 1\}$, então substituindo K_s por K_{k+2} em (4.5) nós temos ainda que $f \in \mathcal{P}_d^{(\delta,s)}$ e $w(\Psi(f)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$.

Finalmente suponha que (ii) é satisfeita, i.e., $s \leq k+1$ e $0 \leq d_s - (d_{k+1} - \ell) < r$, e para evitar a sobreposição com o caso anterior, também assumimos que qualquer $d_s < d_{k+2}$ ou $n = k + 1$. Agora, tome

$$f = \prod_{\substack{i=1 \\ i \neq s}}^{k+1} \prod_{\substack{\alpha \in K_i \\ \alpha \neq \alpha_i}} (X_i - \alpha) \cdot \prod_{i=1}^{d_s - (d_{k+1} - \ell)} (X_s - \beta_i),$$

onde $\beta_1, \ldots, \beta_{d_s-(d_{k+1}-\ell)}$ são elementos distintos de K_s, e novamente temos que $f \in \mathcal{P}_d^{(\delta,s)}$, $\Psi(f) \in \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$ e $w(\Psi(f)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$. □

Corolário 4.3.2. *Os códigos $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})$ e $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d}-1)$ são ótimos e têm distância mínima iguais a δ e $\delta+1$, respectivamente.*

Demonstração. Temos que $\tilde{d} = \sum_{\substack{i=1 \\ i\neq s}}^{n}(d_i-1) + d_s - \delta = \sum_{i=1}^{n-1}(d_i-1) + d_n - \delta$, então de (4.3) segue que $W^{(1)}(\mathcal{C}_{\mathcal{X}}(\tilde{d})) = d_n - (d_n - \delta) = \delta$.

Por outro lado, pelo corolário 4.2.2 e o fato de que $r = d_s - \delta + 1$ obtemos que o limite superior para $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d}))$ no teorema acima é

$$m - \dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) - \left(\left\lceil \frac{\dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)}{r} \right\rceil - 1 \right)(\delta-1) + 1 =$$

$$\prod_{i=1}^{n} d_i - (d_s - \delta + 1) \prod_{\substack{i=1 \\ i\neq s}}^{n} d_i - \left(\prod_{\substack{i=1 \\ i\neq s}}^{n} d_i - 1 \right)(\delta-1) + 1 = \delta$$

então $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})) = \delta$. Da mesma forma, prova-se que $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d}-1)) = \delta+1$. □

Pode-se verificar que se $d_s = d_n$ e $d \leq \tilde{d}$ então qualquer condição (i) ou (ii) do Teorema acima é satisfeita e assim teremos $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$.

Na seção seguinte, entre outros resultados, apresentamos alguns valores para $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d))$ quando temos $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) > W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$.

Corolário 4.3.3. *Sejam $\delta \geq 2$, $n = 2$, $r = 2$, $s = 2$, $d_1 \leq d_2 = \delta + 1$ e q uma potência prima maior ou igual d_2. Para $1 \leq d \leq (d_1 - 1) + (d_2 - \delta) = d_1$, o código $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$ é ótimo com distância mínima $(d_1 - d)(\delta + 1)$.*

Demonstração. Do corolário 4.3.2, para $d = d_1 - 1$ e $d = d_1$ o código $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$ é ótimo.

Se $d < d_1 - 1$, então pela Proposição 4.2.1 temos que

$$\dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) = \frac{(d+2)(d+1)}{2} - \frac{(d)(d-1)}{2} = 2d + 1$$

e pelo Teorema 4.3.1 temos que

$$W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = (d_1 - d)d_2 = (d_1 - d)(\delta + 1).$$

Do Teorema 4.1.2, a cota superior de $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$ é

$$d_1 d_2 - (2d+1) - \left(\left\lceil \frac{2d+1}{2} \right\rceil \right)(\delta - 1) + 1 = (d_1 - d)d_2 = W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)).$$

□

4.4 Outros resultados sobre a distância mínima em um caso especial

A motivação desta seção é calcular o peso mínimo da nossa família de códigos em casos que não foram cobertos na seção anterior. Nesta seção, assumimos que $K_1, \ldots, K_n$ são corpos tais que $K_1 \subset K_2 \subset \cdots \subset K_n \subset \mathbb{F}_q$. Denotamos por $\mathrm{Aff}(\mathbb{F}_q^n)$ o grupo afim de $\mathbb{F}_q^n$, i.e., grupo das transformações de $\mathbb{F}_q^n$ do tipo $\boldsymbol{\alpha} \longmapsto A\boldsymbol{\alpha} + \boldsymbol{\beta}$, onde $A \in GL(n, \mathbb{F}_q)$ e $\boldsymbol{\beta} \in \mathbb{F}_q^n$.

Definição 4.4.1. *O grupo afim associado a $\mathcal{X}$ é* $\mathrm{Aff}(\mathcal{X}) = \{\varphi : \mathcal{X} \to \mathcal{X} \mid \varphi = \psi_{|\mathcal{X}}$ *com* $\psi \in \mathrm{Aff}(\mathbb{F}_q^n)$ *e* $\psi(\mathcal{X}) = \mathcal{X}\}$.

Seja $\{e_1, \ldots, e_n\} \subset \mathbb{F}_q^n$ a base canônica de $\mathbb{F}_q^n$, como $e_1, \ldots, e_n \in \mathcal{X}$ temos que para cada $\varphi \in \mathrm{Aff}(\mathcal{X})$ existe um único $\psi \in \mathrm{Aff}(\mathbb{F}_q^n)$ tal que $\varphi = \psi_{|\mathcal{X}}$.

Lema 4.4.2. *Seja $\psi \in \mathrm{Aff}(\mathbb{F}_q^n)$ dada por $\boldsymbol{\alpha} \longmapsto A\boldsymbol{\alpha} + \boldsymbol{\beta}$, onde*

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \quad e \quad \boldsymbol{\beta} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix},$$

e seja $\varphi = \psi_{|\mathcal{X}}$. Então $\varphi \in \mathrm{Aff}(\mathcal{X})$, se e somente se as seguintes condições forem satisfeitas:

(i) para todo $i, j \in \{1, \ldots, n\}$, $a_{ij} \in K_i$, $b_j \in K_j$ e se $K_i \subsetneqq K_j$ então $a_{ij} = 0$;

(ii) para todo $i \leq j \in \{1, \ldots, n\}$ tal que $K_{i-1} \subsetneqq K_i = K_j \subsetneqq K_{j+1}$ a submatriz quadrada formada por entradas a_{uw} com $i \leq u, w \leq j$ é invertível.

Demonstração. Seja $\psi : \boldsymbol{\alpha} \longmapsto A\boldsymbol{\alpha} + \boldsymbol{\beta} \in \mathrm{Aff}(\mathbb{F}_q^n)$ e suponha que $\psi_{|\mathcal{X}} = \varphi \in \mathrm{Aff}(\mathcal{X})$. Para $\boldsymbol{\alpha} = 0$ temos que $\varphi(0) = \boldsymbol{\beta} \in \mathcal{X}$, o que implica em $b_j \in K_j$ para todo $j \in \{1, \ldots, n\}$.

Temos também que a transformação $\psi_0 : \boldsymbol{\alpha} \longmapsto A\boldsymbol{\alpha} \in \mathrm{Aff}(\mathbb{F}_q^n)$ é tal que $\varphi_0 = \psi_{0|\mathcal{X}} \in \mathrm{Aff}(\mathcal{X})$.

Seja $\{e_1, \ldots, e_n\} \subset \mathbb{F}_q^n$ a base canônica de $\mathbb{F}_q^n$. Para qualquer $j \in \{1, \ldots, n\}$ temos que

$$\psi_0(e_j) = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix} \in \mathcal{X}$$

e então $a_{ij} \in K_i$ para todo $i \in \{1, \ldots, n\}$.

Sejam $i, j \in \{1, \ldots, n\}$ tais que $K_i \subsetneqq K_j$ (então em particular $j > i$) e escolha $\gamma_j \in K_j \backslash K_i$. Para $\gamma_j e_j \in \mathcal{X}$ temos que

$$\psi_0(\gamma_j e_j) = \begin{pmatrix} \gamma_j a_{1j} \\ \gamma_j a_{2j} \\ \vdots \\ \gamma_j a_{nj} \end{pmatrix} \in \mathcal{X}$$

e, em particular, $\gamma_j a_{ij} \in K_i$ o que só é possível se $a_{ij} = 0$.

Suponha que $K_1 \subsetneqq K_n$ e sejam $i_0, \ldots, i_t$ inteiros tais que $0 = i_0 < i_1 < \cdots < i_t = n$, onde $K_{i_u+1} = \cdots = K_{i_{u+1}}$ para todo $u = 0, \ldots, t-1$ e $K_{i_u} \subsetneqq K_{i_{u+1}}$ para todo $u \in \{1, \ldots, t-1\}$. Então a matriz A pode ser reescrita como

$$A = \begin{pmatrix} B_1 & 0 & 0 & \cdots & 0 \\ * & B_2 & 0 & \cdots & 0 \\ * & * & B_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ * & * & * & * & B_t \end{pmatrix}$$

onde para todo $j = 1, \ldots, t$ a matriz B_j é de tamanho $(i_j - i_{j-1}) \times (i_j - i_{j-1})$.

Como $\det A = \det B_1 \cdot \det B_2 \cdots \det B_t$ e $\det A \neq 0$ temos que para todo $j = 1, \ldots, t$ em B_j é invertível com coeficientes em K_{i_j}. Por outro lado, se (i) e (ii) são satisfeitas então é fácil ver que $\varphi \in \mathrm{Aff}(\mathcal{X})$. □

O grupo afim $\mathrm{Aff}(\mathcal{X})$ age sobre o conjunto de polinômios $\mathbb{F}_q[X_1, \ldots, X_n]$ da seguinte maneira: seja $f \in \mathbb{F}_q[X_1, \ldots, X_n]$, $\varphi \in \mathrm{Aff}(\mathcal{X})$ e $\psi \in \mathrm{Aff}(\mathbb{F}_q^n)$ tais que $\psi_{|\mathcal{X}} = \varphi$. Definimos $f \circ \varphi \in \mathbb{F}_q[X_1, \ldots, X_n]$ como $f \circ \varphi(X_1, \ldots, X_n) = f(\psi(X_1, \ldots, X_n))$, onde $(X_1, \ldots, X_n)$ é escrito como um vetor coluna.

Definição 4.4.3. *Dizemos que f, $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ são $\mathcal{X}$-equivalentes se existir $\varphi \in \mathrm{Aff}(\mathcal{X})$ tal que $f = g \circ \varphi$.*

Em [11] códigos cartesianos afins foram estudados como imagens de funções polinomiais avaliadas nos pontos de $\mathcal{X}$ e dois polinômios definem a mesma função se sua diferença pertencer a $I_{\mathcal{X}}$. No seguinte resultado nós reescrevemos [11, Teorema 3.5] sem usar o conceito de função.

Teorema 4.4.4. *Seja $d = \sum_{i=1}^{k}(d_i - 1) + \ell$, $0 \leq k < n$ e $0 < \ell \leq d_{k+1} - 1$, as palavras de peso mínimo do código $C_{\mathcal{X}}(d)$ são da forma $\Psi(f)$ onde $f \in \mathbb{F}_q[X_1, \ldots, X_n]_{\leq d}$ é tal que existe $g \in \mathbb{F}_q[X_1, \ldots, X_n]$, com $f - g \in I_{\mathcal{X}}$ e g é $\mathcal{X}$-equivalente ao polinômio*

$$h = \sigma \prod_{i=1, i\neq j}^{k+1} (X_i^{d_i - 1} - 1) \prod_{t=1}^{d_j - (d_{k+1} - \ell)} (X_j - \alpha_t) \ ,$$

onde $j \in \{1, \ldots, k+1\}$ é tal que $d_j - (d_{k+1} - \ell) \geq 0$, $\sigma \in \mathbb{F}_q^*$ e $\alpha_1, \ldots, \alpha_{d_j - (d_{k+1} - \ell)}$ são elementos distintos de K_j (se $d_j - (d_{k+1} - \ell) = 0$ consideramos o segundo produto como sendo igual a 1).

O resultado a seguir descreve uma propriedade de certos polinômios de grau 1 que será usada na próxima proposição.

Lema 4.4.5. *Seja $p = \gamma_1 X_1 + \cdots + \gamma_h X_h + \eta \in \mathbb{F}_q[X_1, \ldots, X_n]$, onde $\gamma_1, \ldots, \gamma_h \in \mathbb{F}_q$ e $\gamma_h \neq 0$. Então existem $\varphi \in \mathrm{Aff}(\mathcal{X})$ e $j \in \{1, \ldots, n\}$ tais que $X_j \circ \varphi = p$ se, e somente se, $\gamma_i \in K_j$ para todo $i \in \{1, \ldots, h\}$, $\eta \in K_j$ e $K_h = K_j$.*

Demonstração. Suponha que existe $\varphi \in \mathrm{Aff}(\mathcal{X})$ tal que $X_j \circ \varphi = p$ para algum $j \in \{1, \ldots, n\}$ e seja $\psi \in \mathrm{Aff}(\mathbb{F}_q^n)$ tal que $\varphi = \psi_{|\mathcal{X}}$. Se ψ é dado por $\boldsymbol{\alpha} \longmapsto A\boldsymbol{\alpha} + \boldsymbol{\beta}$, então a j-ésima linha de A tem que ser $(\gamma_1, \ldots, \gamma_h, 0, \ldots, 0)$, então $\gamma_i \in K_j$ para todo $i \in \{1, \ldots, h\}$, da mesma forma a j-ésima entrada do vetor $\boldsymbol{\beta}$ tem que ser η, de modo que $\eta \in K_j$. Pela forma geral de A, que foi descrito no Lema 4.4.2 temos que $K_h = K_j$. A prova da recíproca é simples e segue do Lema 4.4.2.

□

Definição 4.4.6. *Uma forma linear $L = \gamma_1 X_1 + \cdots + \gamma_h X_h$, onde $\gamma_h \neq 0$, $\gamma_i \in K_j$ para todo $i \in \{1, \ldots, h\}$ e $K_h = K_j$ será chamada de forma $\mathcal{X}$-linear sobre K_j.*

Proposição 4.4.7. *Seja $f \in \mathbb{F}_q[X_1, \ldots X_n]$ um polinômio de grau*

$$d = \sum_{i=1}^{k}(d_i - 1) + \ell,$$

onde $0 \leq k < n$ e $0 < \ell \leq d_{k+1} - 1$. Suponha que nenhum monômio em f seja múltiplo de $X_i^{d_i}$, para todo $i = 1, \ldots, n$. Se $w(\Psi(f)) = (d_{k+1} - \ell) \prod_{i=k+2}^{n} d_i$ então existe um monômio em f da

forma $X_{t_j}^{d_j-(d_{k+1}-\ell)}\prod_{\substack{i=1\\ i\neq j}}^{k+1} X_{t_i}^{d_i-1}$ *para algum* $1\leq j\leq k+1$ *tal que* $d_j\geq d_{k+1}-\ell$, *onde* $t_1,\ldots,t_{k+1}$ *são elementos distintos de* $\{1,\ldots,n\}$ *e* $K_{t_i}=K_i$ *para todo* $i\in\{1,\ldots,k+1\}$.

Demonstração. De (4.3) temos que $w(\Psi(f))=W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$, então pelo teorema 4.4.4 existe $j\in\{1,\ldots,k+1\}$ e um polinômio

$$g=\sigma\prod_{\substack{i=1\\ i\neq j}}^{k+1}((L_i-\alpha_i)^{d_i-1}-1)\prod_{s=1}^{d_j-(d_{k+1}-\ell)}(L_j-\beta_s),$$

onde $\sigma\in\mathbb{F}_q$, $\beta_1,\ldots,\beta_{d_j-(d_{k+1}-\ell)}$ são elementos distintos de K_j, L_i é uma forma $\mathcal{X}$-linear sobre K_i e $\alpha_i\in K_i$ para todo $i\in\{1,\ldots,k+1\}$, as formas $L_1,\ldots,L_{k+1}$ são linearmente independentes sobre $\mathbb{F}_q$, e $f-g\in I_{\mathcal{X}}$. Como $\deg(g)=d$ temos que $g\in\mathbb{F}_q[X_1,\ldots X_n]_{\leq d}$ e $\Psi(g)=\Psi(f)\in\mathcal{C}_{\mathcal{X}}(d)$.

Suponha, por um momento, que existem pelo menos dois fatores no primeiro produto na definição de g, i.e. suponha que existam $u,w\in\{1,\ldots,k+1\}$ com $u<w$ e $u,w\neq j$. Observe que o avaliando o polinômio

$$((L_u-\alpha_u)^{d_u-1}-1)((L_w-\alpha_w)^{d_w-1}-1)$$

nos pontos de $\mathcal{X}$ obtemos o valor zero, exceto para aqueles $P\in\mathcal{X}$ onde $L_u(P)=\alpha_u$ e $L_w(P)=\alpha_w$ e nesses pontos nós obtemos 1. Para qualquer $\gamma\in K_w$ obtemos os mesmos resultados avaliando o polinômio

$$((L_u-\alpha_u)^{d_u-1}-1)((L_w-\alpha_w-\gamma(L_u-\alpha_u))^{d_w-1}-1)$$

nos pontos de $\mathcal{X}$. Assim, podemos substituir, no polinômio g, o fator $(L_w-\alpha_w)^{d_w-1}-1$ pelo fator $(L_w-\alpha_w-\gamma(L_u-\alpha_u))^{d_w-1}-1$ obtendo um polinômio $\tilde{g}$ tal que $\Psi(\tilde{g})=\Psi(g)$ e a diferença $\tilde{g}-g\in I_{\mathcal{X}}$. Este raciocínio mostra que podemos realizar um processo de eliminação Gaussiana no conjunto $\{L_i-\alpha_i\mid i=1,\ldots,k+1, i\neq j\}$, começando com a forma linear com o maior índice e prosseguindo para a forma linear com o menor índice, e encontrando um conjunto de k inteiros $1\leq t_1<\cdots<t_{j-1}<t_{j+1}<\cdots<t_{k+1}\leq n$ de forma que, após o processo de eliminação, podemos assumir que $L_i=X_{t_i}+\sum_{w<t_i,w\notin A}a_{iw}X_w$ para todo $i\in\{1,\ldots,k+1\}\backslash\{j\}$, onde $A=\{t_i\mid i=1,\ldots,j-1,j+1,\ldots,k+1\}$. Observe que $K_{t_i}=K_i$ para todo $i\in\{1,\ldots,k+1\}\setminus\{j\}$ e ainda temos

$$f-\tau\prod_{\substack{i=1\\ i\neq j}}^{k+1}((L_i-\gamma_i)^{d_i-1}-1)\prod_{s=1}^{d_j-(d_{k+1}-\ell)}(L_j-\beta_s)\in I_{\mathcal{X}}$$

para algum $\tau\in\mathbb{F}_q$ e $\gamma_i\in K_i$ para todo $i\in\{1,\ldots,k+1\}\setminus\{j\}$.

Seja $i\in\{1,\ldots,k+1\}\backslash\{j\}$ tal que $K_{t_i}\subset K_j$ e seja $\xi\in K_j$, então os polinômios

$$((L_i-\gamma_i)^{d_i-1}-1)\prod_{s=1}^{d_j-(d_{k+1}-\ell)}(L_j-\beta_s)$$

e

$$((L_i-\gamma_i)^{d_i-1}-1)\prod_{s=1}^{d_j-(d_{k+1}-\ell)}(L_j-\beta_s-\xi(L_i-\gamma_i))$$

produzem o mesmo valor quando avaliados em qualquer $P \in \mathcal{X}$, então a diferença deles está em $I_{\mathcal{X}}$. Como antes, após um processo de eliminação de Gauss-Jordan, podemos assumir que $L_j = X_{t_j} + \sum_{w<t_j, w\notin A} a_{j,w}X_w$, com $t_j \notin A$ e $K_{t_j} = K_j$. Novamente,

$$f - \eta \prod_{\substack{i=1\\ i\neq j}}^{k+1}((L_i-\gamma_i)^{d_i-1}-1) \prod_{s=1}^{d_j-(d_{k+1}-\ell)} (L_j-\theta_s) \in I_{\mathcal{X}},$$

ainda se mantém, para alguns $\eta \in \mathbb{F}_q$ e $\theta_s \in K_j$, $s = 1, \ldots, d_j - (d_{k+1} - \ell)$. Utilizando a ordem lexicográfica onde $X_1 < \cdots < X_n$, percebemos que o monômio líder do polinômio do lado direito na diferença acima é

$$M = X_{t_j}^{(d_j-(d_{k+1}-\ell)} \prod_{\substack{i=1\\ i\neq j}}^{k+1} X_{t_i}^{d_i-1}.$$

Já o resto na divisão de $f - g$ pela base de Gröbner $\{X_1^{d_1} - X_1, \ldots, X_n^{d_n} - X_n\}$ é zero e M não é múltiplo de $X_i^{d_i}$ para todo $i = 1, \ldots, n$. Portanto, concluímos que este monômio também deve aparecer em f. □

Aplicamos o resultado acima para obter uma recíproca para o Teorema 4.3.1.

Teorema 4.4.8. *Suponha que $K_1, \ldots, K_n$ são corpos tais que $K_1 \subset K_2 \subset \cdots \subset K_n \subset \mathbb{F}_q$. Seja $d = \sum_{i=1}^{k}(d_i - 1) + \ell$ onde $0 \leq k < n$ e $0 < \ell \leq d_{k+1} - 1$. Se $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$ então uma das seguintes condições deve ser válida:*

(i) $k + 2 \leq n$ *e* $d_{k+2} \leq d_s$;

(ii) $d_s \leq d_{k+1}$ *e* $0 \leq d_s - (d_{k+1} - \ell) < r$.

Demonstração. Suponha que a condição (i) não é satisfeita, então $n = k + 1$ ou $d_s < d_{k+2}$, o que implica, em ambos os casos, que $d_s \leq d_{k+1}$. Se a condição (ii) também não é satisfeita, então devemos ter $d_s - (d_{k+1} - \ell) < 0$ ou $r \leq d_s - (d_{k+1} - \ell)$. Assim, se as condições (i) e (ii) não forem satisfeitas, então $n = k+1$ ou $d_s < d_{k+2}$ e $d_s - (d_{k+1} - \ell) < 0$ ou $d_s - (d_{k+1} - \ell) \geq r$.

Suponha que $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$ e seja $f \in \mathcal{P}_d^{(\delta,s)}$ um polinômio de grau d tal que

$$w(\Psi(f)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d)).$$

Pela proposição 4.4.7 existe um monômio em f da forma

$$M_j = X_{t_j}^{d_j-(d_{k+1}-\ell)} \prod_{\substack{i=1\\ i\neq j}}^{k+1} X_{t_i}^{d_i-1}$$

para algum $1 \leq j \leq k + 1$ tal que $d_j \geq d_{k+1} - \ell$, onde $t_1, \ldots, t_{k+1}$ são elementos distintos de $\{1, \ldots, n\}$ e $K_{t_i} = K_i$ para todo $i \in \{1, \ldots, k + 1\}$.

Se $n = k + 1$ então $\{t_1, \ldots, t_{k+1}\} = \{1, \ldots, k + 1\}$, o que implica que $s = t_i$ para algum $i \in \{1, \ldots, k+1\}$. Se $\deg_{X_s} M_j = d_s - 1$, então $\deg_{X_s} M_j \geq d_s - \delta + 1$ e se $\deg_{X_s} M_j = d_s - (d_{k+1} - \ell)$ então não podemos ter $d_s - (d_{k+1} - \ell) < 0$, então devemos ter $d_s - (d_{k+1} - \ell) \geq r$, o que leva a uma contradição, pois também devemos ter $\deg_{X_s} M_j < d_s - \delta + 1 = r$.

Agora suponha que $k + 1 < n$ e $d_s < d_{k+2}$. Seja u um inteiro tal que $s < u \leq k + 2$ e $d_{u-1} < d_u = d_{k+2}$. Da definição do conjunto $\{t_1, \ldots, t_{k+1}\}$ temos, em particular, que $K_{t_i} = K_i$ para todo $i \in \{1, \ldots, u-1\}$, então $s = t_i$ para algum $i \in \{1, \ldots, u-1\} \subset \{1, \ldots, k+1\}$. Como acima, analisando o grau de M_j obtemos que $f \notin \mathcal{P}_d^{(\delta,s)}$, que finaliza a demonstração. □

Assim, se as condições (i) e (ii) do teorema acima não forem satisfeitas, então do teorema 4.4.8 temos que $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) > W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$. Como $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) \subset \mathcal{C}_{\mathcal{X}}(d)$ nós devemos ter $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) \geq W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$ onde $W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$ denota o segundo peso mínimo de uma palavra do código em $\mathcal{C}_{\mathcal{X}}(d)$, também chamado de próximo peso mínimo de $\mathcal{C}_{\mathcal{X}}(d)$. Os valores para $W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$ foram determinados em uma série de artigos [8], [10] e [12]. Esses artigos contêm, em particular, os valores para o caso especial em que $\mathcal{X} = \mathbb{F}_q^n$, que já havia sido determinado por uma combinação de resultados por vários autores. O leitor pode encontrar um levantamento histórico desses resultados em [11].

A partir desses artigos, obtemos que, escrevendo $d = \sum_{i=1}^{k}(d_i - 1) + \ell$ onde $0 \leq k < n$ e $0 < \ell \leq d_{k+1} - 1$, os valores para $W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$ são os seguintes:

1. se $n = k + 1$ então (ver [8, Teorema 2.6])
$$W^{(2)}(\mathcal{C}_{\mathcal{X}}(d)) = d_n - \ell + 1;$$

2. se $3 \leq d_1 \leq \cdots \leq d_n$ e também $\ell = 1$ e $d_{k+1} < d_{k+2}$, ou $\ell \geq 2$ então (ver [10, Teorema 3.10])
$$W^{(2)}(\mathcal{C}_{\mathcal{X}}(d)) = (d_{k+1} - \ell + 1)(d_{k+2} - 1) \prod_{i=k+3}^{n} d_i;$$

3. se $4 \leq d_i = q$ então $i \in \{1, \ldots, n\}$ e $\ell = 1$ então (ver [12, Teorema 3.5])
$$W^{(2)}(\mathcal{C}_{\mathcal{X}}(d)) = q^{n-k};$$

4. Para todos os outros casos onde $d_{k+1} = d_{k+2}$, $\ell = 1$ e $3 \leq d_1 \leq \cdots \leq d_n$ então (ver [12, Teorema 3.5])
$$W^{(2)}(\mathcal{C}_{\mathcal{X}}(d)) = (d_{k+1}^2 - 1) \prod_{i=k+3}^{n} d_i.$$

Corolário 4.4.9. *Suponha $n = k + 1$ ou $3 \leq d_1 \leq \cdots \leq d_n$, se as condições (i) e (ii) da proposição acima não forem satisfeitas e $d_s - (d_{k+1} - \ell) = r$ então*

$$W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = \begin{cases} d_n - \ell + 1 & \text{se } n = k + 1; \\ (d_{k+1} - \ell + 1)(d_{k+2} - 1) \prod_{i=k+3}^{n} d_i & \text{se } n > k + 1. \end{cases}$$

Demonstração. Se (i) e (ii) do Teorema 4.4.8 não forem satisfeitas então como na prova acima, obtemos que $n = k + 1$ ou $d_s < d_{k+2}$, e $d_s - (d_{k+1} - \ell) < 0$ ou $d_s - (d_{k+1} - \ell) \geq r$. Essas duas últimas desigualdades nós substituímos pela hipótese $d_s - (d_{k+1} - \ell) = r$.

Seja
$$g = \prod_{\substack{i=1 \\ i \neq s}}^{k+1} (X_i^{d_i - 1} - 1) \cdot \prod_{h=1}^{d_s - (d_{k+1} - \ell) - 1} (X_s - \beta_h),$$

então $\deg(g) = \sum_{i=1,\, i \neq s}^{k+1}(d_i - 1) + d_s - (d_{k+1} - \ell) - 1 = \sum_{i=1}^{k}(d_i - 1) + \ell - 1 = d - 1$ (se $d_s - (d_{k+1} - \ell) = 1$ então tomamos o segundo produto na definição de g como sendo 1 e ainda obtemos $\deg(g) = d - 1$). Claramente $g \in \mathcal{P}_d^{(\delta,s)}$ desde que $\deg_{X_s} g < r$.

Suponha que $n = k + 1$,como $w(\Psi(g)) = d_{k+1} - \ell + 1$ teremos que $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$ (dos dados acima sobre $W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$.

Agora tratamos o caso em que $k+1 < n$, então nós temos $d_s < d_{k+2}$, e a partir da hipótese, também temos $3 \leq d_1 \leq \cdots \leq d_n$. Suponha que $d_{k+1} < d_{k+2}$ e seja $f = g.X_{k+2}$, então $\deg(f) = d$ e $f \in \mathcal{P}_d^{(\delta,s)}$, para $w(\Psi(f)) = (d_{k+1} - \ell + 1)(d_{k+2} - 1)\prod_{i=k+3}^{n} d_i$ temos que $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$. No caso onde $d_{k+1} = d_{k+2}$ para $d_s < d_{k+2}$ e $d_s - (d_{k+1} - \ell) = \ell - (d_{k+2} - d_s) = r \geq 1$ vemos que devemos ter $\ell \geq 2$, então novamente temos $w(\Psi(f)) = W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$, finalizando a demonstração. □

4.5 Exemplos e comparações

Nesta seção, apresentamos algumas tabelas com dados numéricos obtidos a partir dos resultados acima. Nas tabelas, usamos a seguinte notação: $m = |\mathcal{X}|$ é o comprimento de $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$, $\kappa = \dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$, $v = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$, $w = W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d))$ e denotamos por

$$N = m - \kappa - \left(\left\lceil \frac{\kappa}{r} \right\rceil - 1\right)(\delta - 1) + 1$$

a cota superior para a distância mínima,que aparece no Teorema 4.3.1. Nas tabelas d percorre o intervalo $1 \leq d \leq \tilde{d}$. Quando $w \neq v$ então $w \geq W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$ e na Seção anterior os valores para $W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$ são apresentados. Ainda, quando $w \neq v$ e estamos nas hipóteses do Corolário 4.4.9, então escrevemos o valor verdadeiro de w.

Na tabela 4.1, para os d listados sempre teremos que $w = v$.

$\mathcal{D}_{\mathcal{X}}^{(25,2)}(d)$

d	4	5	10	15	20	25	26	27	28	29	30
m	343	343	343	343	343	343	343	343	343	343	343
κ	15	21	56	91	126	160	165	169	172	174	175
w	147	98	45	40	35	30	29	28	27	26	25
N	329	323	240	181	98	40	35	31	28	26	25

Tabela 4.1: $\mathcal{X} := \mathbb{F}_7 \times \mathbb{F}_{49}$

Na tabela 4.2, para alguns valores de d temos que $w \neq v$.

$\mathcal{D}_{\mathcal{X}}^{(4,1)}(d)$

d	2	3	24	25	26	27	47	48	49
m	3125	3125	3125	3125	3125	3125	3125	3125	3125
κ	9	16	625	674	721	766	1246	1249	1250
v	1875	1250	125	100	75	50	6	5	4
w	2400	≥ 1800	125	100	96	≥ 72	≥ 7	5	4
N	3105	3089	1565	1444	1325	1214	14	5	4

Tabela 4.2: $\mathcal{X} := \mathbb{F}_5 \times \mathbb{F}_{25} \times \mathbb{F}_{25}$

Pelo Corolário 4.3.3 obtemos códigos ótimos cuja distância mínima é múltipla de $\delta + 1$, por exemplo, os códigos obtidos na tabela 4.3.

Códigos ótimos estão sendo estudados ativamente (ver [6], [7], [13], [14], [15] e [22], entre muitos outros artigos). Finalizamos esta seção com comparações dos nossos códigos com códigos que aparecem em alguns dos artigos acima.

Em [15, Corolário 1], os autores encontraram códigos ótimos com distância mínima $\delta + 1$, $\delta + 2$ e 2δ, enquanto que no Corolário 4.3.2 nós encontramos códigos com distância mínima igual a δ e $\delta + 1$ e no Corolário 4.3.3 construímos códigos ótimos cuja distância mínima pode ser ajustada para ser um entre vários múltiplos de $\delta + 1$.

$\mathcal{D}_{\mathcal{X}}^{(12,2)}(d)$

d	1	2	3	4	5	6	7	8	9	10
m	130	130	130	130	130	130	130	130	130	130
κ	3	5	7	9	11	13	15	17	19	20
w	117	104	91	78	65	53	39	26	13	12
N	117	104	91	78	65	53	39	26	13	12

Tabela 4.3: $\mathcal{X} := A_1 \times A_2$, $|A_1| = 10$, $|A_2| = 13$ e $q \geq 13$

Em [6, Exemplo 1], os autores apresentam códigos com parâmetros $[12, 5, 4]_7$ e $(r, \delta) = (2, 3)$. Neste caso, a distância mínima é $4 = \delta + 1$. Pelo Corolário 4.3.3, escolhendo $(d_1, d_2) = (3, 4)$ e a mesma localidade (r, δ), nós obtemos o mesmo código ótimo que eles encontraram, além de outros dois com parâmetros $[12, 3, 8]$, $[12, 5, 4]$ e $[12, 6, 3]$ para todo $q \geq 4$.

Finalmente, observamos que em [13], os autores apresentaram códigos cíclicos ótimos com localidade (r, δ) tais que o comprimento divide $q + 1$, enquanto que o comprimento dos nossos códigos não tem essa restrição.

CAPÍTULO 5

CONSIDERAÇÕES FINAIS E PROPOSTAS FUTURAS DE TRABALHO

Ao longo deste trabalho, estudamos os códigos cartesianos afins propostos por López *et al.* em [24] e também os códigos (r, δ)-localmente recuperáveis propostos por Prakash *et al.* em [25]. Encontramos uma nova família de subcódigos dos códigos cartesianos afins que são (r, δ)-localmente recuperáveis. Calculamos os principais parâmetros destes códigos e em alguns casos, encontramos códigos ótimos.

Por último, enunciamos algumas propostas para trabalhos futuros.

- Continuar trabalhando na construção de códigos localmente recuperáveis a partir de famílias de códigos presentes na literatura. Por exemplo, em [26], Carvalho e Neumann estudaram códigos do tipo Reed-Muller projetivos, isto é, códigos obtidos por uma avaliação de polinômios homogêneos com um grau fixado em pontos de uma variedade projetiva. Como perspectiva de trabalho futuro, pode-se tentar verificar se os códigos estudados em [26] são localmente recuperáveis ou construir subcódigos dos códigos tipo Reed-Muller projetivos que são localmente recuperáveis.

- Verificar a potencialidade dos nossos códigos na transmissão de imagens. Esta proposta seria para trabalhar em conjunto com pesquisadores do departamento de Engenharia Elétrica da Universidade Federal de Uberlândia.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] W.W. Adams and P. Loustaunau,"An Introduction to Grobner Bases," *Graduate studies in Mathematics*, vol. 3 New York, NY, USA: AMS, 1994. https://doi.org/10.1090/gsm/003

[2] B. Andrade, C. Carvalho, V. G. L. Neumann and A. C. P. Veiga, "A Family of Codes With Locality Containing Optimal Codes", *IEEE Access,* vol. 10, pp. 39145–39153, Apr. 2022. https://doi.org/10.1109/ACCESS.2022.3165032.

[3] T. Becker and V. Weispfenning, *Gröbner Bases - A computational approach to commutative algebra*, Berlin, Germany: Springer Verlag, 1998, 2nd. pr.

[4] B. Buchberger, "Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal," Ph.D. dissertation, Math. Inst., Univ. Innsbruk, Innsbruck, Austria, 1965.

[5] B. Buchberger, "Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal," *J. Symbolic Comput.,* vol. 41, pp.475-511, Mar./Apr. 2006. https://doi.org/10.1016/j.jsc.2005.09.007.

[6] H. Cai, Y. Miao, M. Schwartz and X. Tang, "On Optimal Locally Repairable Codes with Super-Linear Length," *IEEE Trans. Inf. Theory*, vol. 66, no. 8, pp. 4853–4868, Aug. 2020. https://doi.org/10.1109/TIT.2020.2977647.

[7] H. Cai and M. Schwartz, "On Optimal Locally Repairable Codes and Generalized Sector-Disk Codes," *IEEE Trans. Inf. Theory*, vol. 67, pp. 686–704, Feb. 2021. https://doi.org/10.1109/TIT.2020.3037268.

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

[9] C. Carvalho, "Gröbner bases methods in coding theory," *Contemp. Math.*, 642 pp. 73–86, Jan. 2015. https://doi.org/10.1090/conm/642/12881.

[10] C. Carvalho and V.G.L. Neumann, "On the next-to-minimal weight of affine cartesian codes," *Finite Fields Appl.*, vol. 44, pp. 113–134, Mar. 2017. https://doi.org/10.1016/j.ffa.2016.11.005.

[11] C. Carvalho and V.G.L. Neumann, "An extension of Delsarte, Goethals and Mac Williams theorem on minimal weight codewords to a class of Reed-Muller type codes." In: Ron Donagi; Tony Shaska. (Org.). Integrable Systems and Algebraic Geometry v. 2, Cambridge University Press, pp. 313–345, Mar. 2020. https://doi.org/10.1017/9781108773355.010.

[12] C. Carvalho and V.G.L. Neumann, "Completing the determination of the next-to-minimal weights of affine cartesian codes," *Finite Fields Appl.*, vol. 69, 101775, 13 pp., Jan. 2021. https://doi.org/10.1016/j.ffa.2020.101775.

[13] B. Chen, S-T. Xia, J. Hao and F-W. Fu, "Constructions of Optimal Cyclic (r, δ) Locally Repairable Codes," *IEEE Trans. Inf. Theory*, vol 64, no. 8, pp 2499–2511, Apr. 2018.https://doi.org/10.1109/TIT.2017.2761120.

[14] B. Chen, W. Fang, S-T. Xia, F-W. Fu, "Constructions of Optimal (r, δ) Locally Repairable Codes via Constacyclic Codes,"*IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5253–5263, Aug. 2019. https://doi.org/10.1109/TCOMM.2019.2916085.

[15] B. Chen and J. Huang, "A Construction of Optimal (r, δ)-Locally Recoverable codes," *IEEE Access*, vol. 7, pp. 180349–180353, Dec. 2019. https://doi.org/10.1109/ACCESS.2019.2957942.

[16] D. Cox, J. Little and D. O'Shea, "Ideals, varieties and algorithms," 3rd. ed. New York, NY, USA: *Springer-Verlag*, 2007. https://doi.org/10.1007/978-0-387-35651-8.

[17] J.Fitzgerald, R.F. Lax, "Decoding affine variety codes using Gröbner bases," *Des. Codes Cryptogr.*, vol. 13, no. 2, pp. 2147-158, Feb. 1998. https://doi.org/10.1023/A:1008274212057.

[18] O. Geil and C. Thomsen, "Weighted Reed-Muller codes revisited." *Des. Codes Cryptogr*, vol. 66, pp. 195–220, May 2012. https://doi.org/10.1007/s10623-012-9680-8.

[19] M. J. E. Golay, "Notes on digital coding", *Proc. of the I.R.E,* vol. 37, 657, Jul. 1949. https://doi.org/10.1109/JRPROC.1949.233620.

[20] T. Kasami, S. Lin, and W. Peterson, "New generalizations of the Reed- Muller codes–I: Primitive codes," *IEEE Trans. Inf. Theory,* vol. 14, no. 2, pp. 189-199, Mar. 1968. https://doi.org/10.1109/TIT.1968.1054127.

[21] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin," On the locality of codeword symbols," *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6925–6934, Aug. 2012. https://doi.org/10.1109/TIT.2012.2208937.

[22] J. Hao, S.-T Xia and B. Chen, "On the linear codes with (r, δ)-locality for distributed storage," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp.1-6. https://doi.org/10.1109/ICC.2017.7997028.

[23] A. Hefez., M. L. T. Villela, "Códigos Corretores de Erros," *Série de Computação e Matemática*, IMPA, Rio de Janeiro, 2008.

[24] H. H. López, C. Rentería-Márquez, R. H. Villarreal, "Affine cartesian codes," *Des. Codes Cryptogr.*, vol. 71, no. 1, pp. 5–19, Apr. 2014. https://doi.org/10.1007/s10623-012-9714-2.

[25] N. Prakash, G. M. Kamath, V. Lalitha, and P. V. Kumar, "Optimal linear codes with a local-error-correction property," in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jul. 2012, pp. 2776–2780. https://doi.org/10.1109/ISIT.2012.6284028.

[26] C. Carvalho and V.G.L. Neumann, "Projective Reed-Muller type codes on rational normal scrolls," *Finite Fields Appl.*, vol. 37, pp. 85-107, Jan. 2016. https://doi.org/10.1016/j.ffa.2015.09.004.

[27] C. E. Shannon, "A mathematical theory of communication," *The Bellsystem technical journal,* vol. 27, no. 3, pp. 379-423, Jul. 1948. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

[28] R. Lidl, H. Niederreiter, " Finite Fields," *Enciclopedia of Mathematics and Its Applications,* vol. 20. Cambridge, 1997.

[29] D. E. Muller, "Application of boolean algebra to switching circuit design and to error detection," *Trans. I.R.E. Prof. Group Electron. Comput.*, vol. EC 3, no. 3, pp. 6–12, Sep. 1954. https://doi.org/10.1109/IREPGELC.1954.6499441.

[30] I. S. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *Trans. IRE Prof. Group Inf. Theory,* vol. 4, no. 4, pp. 38–49, Sep. 1954. https://doi.org/10.1109/TIT.1954.1057465.

[31] I. S. Reed and G. Solomon, "Polynomial codes over certain finitefields," *Journal of the society for industrial and applied mathematics,* vol. 8, no. 2, pp. 300–304, 1960. https://doi.org/10.1137/0108018.

[32] R. W. Hamming. "Error detecting and error correcting codes," *The Bellsystem technical journal,* vol. 29, no. 2, pp.147–160, Apr. 1950. https://doi.org/10.1002/j.1538-7305.1950.tb00463.x.