UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
DEPTO DE MATEMÁTICA

Rafaela Cristina Oliveira da Cunha

Códigos corretores de erros e um exemplo de aplicação na biologia

Juiz de Fora
2023

Rafaela Cristina Oliveira da Cunha

Códigos corretores de erros e um exemplo de aplicação na biologia

Trabalho de conclusão de curso apresentado ao Depto de Matemática da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de bacharel em Matemática.

Orientadora: Profa. Dra. Beatriz Casulari da Motta Ribeiro

Juiz de Fora

2023

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

da Cunha, Rafaela Cristina O.
Códigos corretores de erros e um exemplo de aplicação na biologia / Rafaela Cristina Oliveira da Cunha. – 2023.
117 f. : il.

Orientadora: Beatriz Casulari da Motta Ribeiro
Trabalho de Conclusão de Curso (graduação) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Depto de Matemática, 2023.

1. Corpos Finitos. 2. Códigos Corretores de Erros. 3. DNA. I. Ribeiro, Beatriz Casulari da Motta, orient. II. Título.

Rafaela Cristina Oliveira da Cunha

Códigos corretores de erros e um exemplo de aplicação na biologia

Trabalho de conclusão de curso apresentado ao Depto de Matemática da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de bacharel em Matemática.

Aprovada em 17 de janeiro de 2023

BANCA EXAMINADORA

Profa. Dra. Beatriz Casulari da Motta Ribeiro - Orientadora
Universidade Federal de Juiz de Fora

Profa. Dra. Flaviana Andréa Ribeiro
Universidade Federal de Juiz de Fora

Prof. Dr. Frederico Sercio Feitosa
Universidade Federal de Juiz de Fora

Dedico este trabalho à minha mãe, minha irmã
e meus amigos.

AGRADECIMENTOS

À Deus em primeiro lugar, pois sem Ele eu não seria nada.

À minha mãe, Isabel, e à minha irmã, Júlia, por todo apoio incondicional, pelos incentivos constantes, pelo suporte nos momentos difíceis e pela confiança depositada em mim. Aos meus familiares, em especial, aos meus tios Helieber, Luciene, Paulo e Léia e, à minha prima Carol, pelo apoio dado.

Ao Gabriel, pelas conversas, pelo carinho, pelas diversões, experiências únicas inesquecíveis que me possibilita diariamente e por todo apoio e companhia nos momentos bons e ruins.

À professora e orientadora Beatriz Casulari da Motta Ribeiro, por aceitar me orientar neste trabalho, me guiando com a maior dedicação possível, para me propiciar o maior entendimento quanto à teoria de Códigos Corretores de Erros. Também, por ter me proporcionado a oportunidade de conhecer e estudar os corpos finitos.

Ao professor Sérgio Guilherme de Assis Vasconcelos, por ter me motivado e apoiado durante toda minha trajetória acadêmica. Também, por ter sido meu primeiro orientador de iniciação científica, pelos ensinamentos passados como professor das disciplinas que ministrou e que tive o prazer de cursar, e, por ter me ensinado boa parte do que hoje sei sobre Geometria, aumentando a cada conversa o meu interesse por esta área.

Ao professor Laércio José dos Santos, pelos ensinamentos aprendidos durante a pandemia e, principalmente, por ter me propiciado as belíssimas elucidações e visões que hoje tenho sobre Álgebra Linear, motivando meu interesse por essa área. Além disso, por me ajudar na organização e no planejamento da minha trajetória acadêmica.

À professora Ana Tércia Monteiro de Oliveira, pelo apoio dado, e pela primeira oportunidade de bolsa da graduação. Também, pelas conversas e por me motivar a seguir meus estudos no Bacharelado em Matemática, sendo sempre uma fonte de inspiração.

À professora Tatiana Aparecida Gouveia pelo apoio, ensinamentos e con-

versas praticados, principalmente, no final do curso de graduação. Sua ajuda foi essencial para chegar onde hoje estou.

Ao professor Luís Fernando Crocco Afonso, pelas excelentes aulas sobre Geometria e por todos os ensinamentos.

À todos os docentes do ICE, em especial aos docentes do Departamento de Matemática, pela contribuição em todo meu processo de enriquecimento matemático.

Aos membros da banca examinadora, Beatriz Casulari da Motta Ribeiro, Flaviana Andréa Ribeiro e Frederico Sercio Feitosa, pelas excepcionais contribuições e avaliações.

Aos colegas e amigos de faculdade, por tornarem minha trajetória mais leve e divertida. Em especial, agradeço aos meus amigos Thayonara, Vinícius Sangi Gustavo Dutra, Gabriel, Sheucíer e Thiago Evangelista por me proporcionarem tantos momentos inesquecíveis de alegria, estudos e tristezas compartilhados. Além disso, pelos ensinamentos aprendidos e frutos colhidos durante essa trajetória.

Aos amigos Thayonara e Vinícius, pela amizade, pelo apoio incondicional, por me acompanharem nesses anos e pelas conversas em nosso grupo.

Ao Gustavo Dutra, por ter sido meu companheiro e parceiro de graduação, meu amigo dentro e fora da faculdade, e por ter entendido minhas indecisões durante essa caminhada.

À Sheucíer, por me apoiar, me aconselhar e por me abrigar em sua casa nas noites de rolês.

Ao Thiago Evangelista, pelas conversar e por me ajudar no finalzinho de graduação.

Agradeço também, à Letianne, à Larissa, ao Heitor, ao Gustavo Roque, ao Yago, à Milena, ao Walter, à Camila, à Vanessa, ao Scheffer, ao Paulo, ao Luca e ao Daniel de Souza, por me acompanharem e me apoiarem nessa jornada.

À Universidade Federal de Juiz de Fora e ao Departamento de Matemática.

À PROPP - UFJF, pelas bolsas de Iniciação Científica.

"É das hipóteses mais simples que mais devemos desconfiar, porque são aquelas que têm mais possibilidades de passar despercebidas" - Henri Poincaré

RESUMO

Ao longo do presente trabalho, estaremos interessados no estudo dos Corpos Finitos e dos Códigos Corretores de Erros, especialmente os lineares, de modo que, a primeira estrutura serve como a base sobre a qual desenvolveremos a teoria sobre códigos. Ademais, estudaremos uma classe especial de códigos corretores de erros lineares, chamada códigos cíclicos. Por fim, apresentaremos uma interessante aplicação da subclasse de códigos cíclicos chamada códigos BCH em sequências de DNA.

Palavras-chave: Corpos Finitos. Códigos Corretores de Erros. Sequências de DNA.

ABSTRACT

Throughout this work, we will be interested in the study of Finite Fields and Error Correcting Codes, specially the linear ones, so that the first structure serves as the basis on which we will develop the code theory. Furthermore, we will study some special class of linear error correcting codes, the so-called cyclic codes. Finally, we will present an interesting application of a subclass of cyclic codes called BCH codes in DNA sequences.

Keywords: Finite Fiels. Error Correcting Codes.DNA sequences.

SUMÁRIO

1 INTRODUÇÃO

A Teoria de Códigos é um campo de estudo que é atualmente muito ativo, tanto do ponto de vista teórico quanto tecnológico. Nos mais diversos meios (internet, celulares, TVs, pen drives) circulam informações que carregam consigo possíveis erros feitos na transmissão. De forma geral, os códigos corretores de erros tem como objetivo a correção de erros que ocorrem durante a transmissão ou armazenamento da informação, e estão presentes na comunicação via satélite, nas comunicações internas de um computador e no armazenamento de dados. Essa Teoria surge na década de 1940, no Laboratório Bell de Tecnologia, com os trabalhos de Richard W. Hamming e C. E. Shannon, com objetivo de elaborar mecanismos capazes de permitir uma transmissão confiável de dados através de canais sujeitos a interferências, também denominadas ruídos.

A teoria se baseia no seguinte cenário: buscamos transmitir uma mensagem, a qual denominamos palavra, que consiste numa sequência finita de símbolos, onde tais símbolos são elementos de um alfabeto (um conjunto) finito. Chamamos cada um desses elementos de letras. Por exemplo, tomando como alfabeto o conjunto $\mathbb{Z}_2 = \{0, 1\}$, uma palavra pode ser descrita como um número binário.

No caso dos códigos que estudaremos nesse trabalho, os métodos para melhorar a confiabilidade da transmissão estão intrinsecamente ligados às propriedades dos corpos finitos. Uma ideia básica na teoria da codificação algébrica é transmitir informação extra junto com a mensagem que se quer comunicar, isto é, estende-se a sequência de símbolos da mensagem para uma sequência mais longa de forma sistemática, adicionando as chamadas redundâncias. Logo, um código corretor de erros é essencialmente, uma maneira organizada de acrescentar algum dado a cada informação que se queira transmitir ou armazenar, de forma que permita, ao recuperar a informação, detectar e corrigir erros presentes na transmissão da informação.

No Capítulo 2, nosso objetivo é fazer uma introdução à Teoria de Corpos Finitos, demonstrando a existência dessa estrutura algébrica. Para isso, serão necessárias definições e resultados sobre corpos em geral e sobre polinômios em uma variável com coeficientes em um corpo.

Já no Capítulo 3, dedicaremos à apresentação dos conceitos básicos da Teoria de Códigos, como uma introdução ao assunto. Definiremos o que são os códigos corretores de erros, a métrica de Hamming e os parâmetros de um código.

No Capítulo 4, destinaremos nosso estudo à uma classe especial de códigos, denominados códigos lineares, que consiste na classe de códigos mais utilizada na prática. Também, destinaremos este capítulo a determinação dos parâmetros dessa classe de códigos e aos algoritmos gerais de correção de erros, vendo, em especial, a decodificação por síndrome.

Apresentaremos, no Capítulo 5, uma classe particular de códigos lineares, denominada por códigos cíclicos. A importância desse tipo de código consiste em seus algoritmos de implementação muito eficientes, que se baseiam em operações com polinômios.

No Capítulo 6, resolveremos parcialmente um dos problemas teóricos de trabalhar com códigos, que é a fatoração de polinômios sobre um corpo finito. Apresentaremos uma maneira sistemática de proceder com a fatoração de polinômios do tipo $x^n - 1$, com $n \in \mathbb{N}$ sobre $\mathbb{F}_q[x]$, onde q é potência de algum número primo.

No Capítulo 7, estudaremos os códigos BCH, que são uma classe de códigos cíclicos, utilizando para isso os cosets ciclotômicos, estudados no capítulo anterior. Veremos uma maneira direta de codificar uma mensagem nesse tipo de código e, também, uma forma de decodificação por síndrome.

Por fim, no Capítulo 8, baseado no artigo [2] e na tese [3], apresentaremos uma aplicação dos códigos BCH às sequências de DNA, sigla que identifica, em inglês, o ácido desoxirribonucléico (portador dos genes dentro das células). Nos sistemas de comunicação, os códigos corretores de erros são utilizados sempre que se deseja transmitir ou armazenar informação que possa ser corrigida caso haja algum tipo de erro na transmissão. O sistema biológico também armazena e transmite a informação através do código genético. Assim, faz sentido pensar em uma analogia entre sistemas de informação e o biológico. Esse é um problema que constitui objeto de pesquisa desde os anos 1980 e que tem sido de particular interesse, por exemplo, por suas aplicações teóricas na compreensão de anomalias genéticas e até mesmo práticas no sentido de economizar insumos laboratoriais.

2 CORPOS FINITOS

O objetivo desse capítulo é demonstrar, para qualquer potência q de um primo, a existência e unicidade (a menos de isomorfismo) de um corpo finito com q elementos. Para tal, precisaremos de algumas definições e resultados sobre corpos e extensões de corpos, que listaremos conforme forem sendo necessárias. Para mais informações sobre o assunto, indicamos [5] e [6].

Definição 2.1. *Um* ***corpo*** $\mathbb{K}$ *é um anel comutativo com unidade e tal que todo elemento não nulo é inversível.*

Sejam A um anel, $a \in A$ e $m \in \mathbb{Z}$. Definimos $m \cdot a$ como sendo o elemento de A dado

$$m \cdot a = \begin{cases} \underbrace{a + a + \cdots + a}_{m \text{ vezes}}, & \text{se } m > 0 \\ 0, & \text{se } m = 0 \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{m \text{ vezes}}, & \text{se } m < 0 \end{cases} . \tag{2.1}$$

Definição 2.2. *A* ***característica*** c *de um corpo é definida como o menor inteiro positivo tal que* $c \cdot 1 = 0$*. Se não existir tal* c*, dizemos que a característica do corpo é* ***zero****. Denotaremos por* $\text{char}(\mathbb{K})$ *a característica do corpo* $\mathbb{K}$*.*

Proposição 2.3. *Se* $\mathbb{K}$ *é um corpo, então* $\text{char}(\mathbb{K}) = 0$ *ou* $\text{char}(\mathbb{K}) = p$*, com* p *primo.*

Demonstração. Suponhamos $\text{char}(\mathbb{K}) = c \neq 0$. Seja p um divisor primo de c. Então, $0 = c \cdot 1 = (p \cdot 1)(c/p \cdot 1)$. Como $\mathbb{K}$ é um corpo, devemos ter $p \cdot 1 = 0$ ou $c/p \cdot 1 = 0$, contrariando a minimalidade de $\text{char}(\mathbb{K}) = c$. Dessa forma, c tem que ser primo. ■

Definição 2.4. *Um corpo com um número finito de elementos é dito um* ***corpo finito****.*

Proposição 2.5. *Se* $\mathbb{K}$ *é um corpo finito, então* $\text{char}(\mathbb{K})$ *é um número primo.*

Demonstração. Seja $\mathbb{K}$ um corpo finito. Consideremos $1 \cdot 1$, $2 \cdot 1$, $3 \cdot 1, \ldots$ os múltiplos da unidade de $\mathbb{K}$. Por hipótese, $\mathbb{K}$ possui um numero finito de elementos distintos, donde, existem $m, n \in \mathbb{Z}$ tais que $1 \leq m < n$ e $m \cdot 1 = n \cdot 1$, isto é, $(n-m) \cdot 1 = 0$. Logo, $\mathbb{K}$ possui característica positiva. Portanto, pelo Lema 2.3, $\mathbb{K}$ deve ter característica prima. ■

Definição 2.6. *Um* ***subcorpo*** $\mathbb{K}$ *de um corpo* $\mathbb{F}$ *é um subconjunto* $\mathbb{K} \subset \mathbb{F}$ *que é ele próprio um corpo com as operações de* $\mathbb{F}$*. Dizemos que um corpo* $\mathbb{F}$ *é um* ***corpo primo*** *quando este não contém nenhum subcorpo próprio. Dado um corpo* $\mathbb{F}$*, a interseção de todos seus subcorpos é dito* ***subcorpo primo*** *de* $\mathbb{F}$ *(é possível provar que de fato é subcorpo).*

Como exemplo de corpo finito com p elementos, onde p é um número primo, temos o corpo dos inteiros módulo p, $\mathbb{Z}_p := \mathbb{Z}/\langle p \rangle$. Dado um número primo p, seja $\mathbb{F}_p = \{0, 1, \ldots, p-1\} \subset \mathbb{Z}$. Consideremos a aplicação

$$\begin{array}{rccc} \varphi : \mathbb{Z}_p & \to & \mathbb{F}_p \\ \overline{a} & \mapsto & a \end{array}, \tag{2.2}$$

onde $a \in \{0, 1, \ldots, p-1\}$. Então $\mathbb{F}_p$, com a estrutura de corpo induzida por φ, é um corpo finito, chamado ***corpo de Galois*** de ordem p.

Perceba que, se p é primo e $\mathbb{K}$ é um subcorpo de um corpo finito $\mathbb{F}_p$, então $\mathbb{K}$ deve conter os elementos 0 e 1 e assim deve também conter todos os demais elementos de $\mathbb{F}_p$, já que a adição é uma operação fechada em $\mathbb{K}$. Dessa forma, o corpo finito $\mathbb{F}_p$, onde p é um número primo, é um corpo primo. É possível provar que o subcorpo primo de qualquer corpo finito de característica p é isomorfo a $\mathbb{F}_p$.

Definição 2.7. *Sejam* $\mathbb{F}$ *e* $\mathbb{K}$ *corpos. Dizemos que* $\mathbb{F}$ *é uma* ***extensão*** *de* $\mathbb{K}$ *se* $\mathbb{K}$ *for um subcorpo de* $\mathbb{F}$*.*

Sendo $\mathbb{F}$ uma extensão do corpo $\mathbb{K}$, as operações

$$\begin{array}{rccc} + : & \mathbb{F} \times \mathbb{F} & \to & \mathbb{F} \\ & (u, v) & \mapsto & u + v \end{array} \quad \text{e} \quad \begin{array}{rccc} \cdot : & \mathbb{K} \times \mathbb{F} & \to & \mathbb{F} \\ & (\lambda, u) & \mapsto & \lambda \cdot u \end{array} \tag{2.3}$$

fazem de $\mathbb{F}$ um espaço vetorial sobre $\mathbb{K}$.

Definição 2.8. *Chamamos de* ***grau da extensão*** *a dimensão de* $\mathbb{F}$ *como espaço vetorial sobre* $\mathbb{K}$*. Tal dimensão será denotada por* $[\mathbb{F} : \mathbb{K}]$*. Dizemos que* $\mathbb{F}$ *é uma* ***extensão finita*** *de* $\mathbb{K}$ *se* $[\mathbb{F} : \mathbb{K}] < +\infty$*. Caso contrário, dizemos que* $\mathbb{F}$ *é uma* ***extensão infinita*** *de* $\mathbb{K}$*.*

Lema 2.9. *Seja* $\mathbb{F}$ *um corpo finito contendo um subcorpo* $\mathbb{K}$ *com* q *elementos. Então* $\mathbb{F}$ *possui* q^m *elementos, onde* $m = [\mathbb{F} : \mathbb{K}]$*.*

Demonstração. Sabendo que $\mathbb{F}$ pode ser visto como um espaço vetorial sobre $\mathbb{K}$, então a dimensão do espaço vetorial $\mathbb{F}$ sobre o corpo $\mathbb{K}$ é finita, uma vez que $\mathbb{F}$ é um corpo finito. Tomando $m = [\mathbb{F} : \mathbb{K}]$, segue que $\mathbb{F}$ possui uma base $\{b_1, b_2, \ldots, b_m\}$ sobre $\mathbb{K}$ constituída por m elementos. Assim, todo elemento de $\mathbb{F}$ pode ser escrito de forma única como $a_1b_1 + a_2b_2 + \cdots + a_mb_m$, com $a_i \in \mathbb{K}$, para cada $i \in \{1, 2, \ldots, m\}$. Para concluir a demonstração, basta notar que, como $\mathbb{K}$ possui q elementos, $\mathbb{F}$ possui exatamente q^m elementos. ■

Como consequência do Lema 2.9, um corpo finito $\mathbb{F}$ possui p^n elementos, onde $p = \text{char}(\mathbb{F})$ e n é a dimensão de $\mathbb{F}$ quando visto como um espaço vetorial sobre o seu corpo primo, já que esse é isomorfo a $\mathbb{F}_p$.

Proposição 2.10. *Seja* $\mathbb{F}$ *um corpo finito de característica* p *e seja* $q = p^n$*,* $n \in \mathbb{N}$*. Se* a*,* $b \in \mathbb{F}$*, temos que* $(a \pm b)^q = a^q \pm b^q$*.*

Demonstração. Pelo Binômio de Newton temos que

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

Ainda é possível mostrar que $p \mid \binom{p}{i}$, para cada $i \in \{1, \ldots, p-1\}$. Logo

$$(a \pm b)^p = a^p \pm b^p.$$

O restante da prova segue por indução, notando que $(a \pm b)^{p^r} = ((a \pm b)^{p^{r-1}})^p$. ■

Proposição 2.11. *Se* $\mathbb{F}$ *é um corpo finito com* q *elementos, então* $a^q = a$*, para todo* $a \in \mathbb{F}$*.*

Demonstração. Se $a = 0$, então a igualdade $a^q = a$ é satisfeita. Por outro lado, os elementos não nulos de $\mathbb{F}$ formam um grupo multiplicativo de ordem $q - 1$. Assim, $a^{q-1} = 1$, para todo $a \in \mathbb{F} \setminus \{0\}$. Multiplicando ambos os lados da igualdade anterior por a, teremos também $a^q = a$, para todo $a \in \mathbb{F} \setminus \{0\}$, o que conclui a demonstração. ■

Definição 2.12. *Sejam $\mathbb{K}$ é um corpo e $f(x) \in \mathbb{K}[x]$. Dizemos que $f(x)$ se **fatora** em $\mathbb{K}[x]$ se $f(x)$ pode ser escrito como o produto de fatores lineares*

$$f(x) = c(x - \alpha_1)...(x - \alpha_n),$$

com c, α_1, ..., $\alpha_n \in \mathbb{K}$.

Nas condições da Definição 2.12, os zeros de $f(x)$ em $\mathbb{K}$ são exatamente os elementos α_1, ..., α_n. Ademais, se $\mathbb{F}$ é uma extensão de $\mathbb{K}$, então $f(x)$ também pertence a $\mathbb{F}[x]$. Dessa forma, faz sentido falarmos na fatoração de $f(x)$ em $\mathbb{F}[x]$.

Definição 2.13. *Sejam $\mathbb{K}$ um corpo e Σ uma extensão de $\mathbb{K}$. Dizemos que Σ é um **corpo de decomposição** para o polinômio $f(x) \in \mathbb{K}[x]$ quando a seguintes condições são satsifeitas:*

i) $f(x)$ se fatora em $\Sigma[x]$;

ii) Se $\mathbb{K} \subset \Sigma' \subset \Sigma$ e $f(x)$ se fatora em $\Sigma'[x]$, então $\Sigma = \Sigma'$, ou seja, Σ é o menor corpo que contém $\mathbb{K}$ e todas as raízes de $f(x)$.

É possível provar (veja Teorema 3.2, capítulo V de [7]) que se $\mathbb{K}$ é um corpo qualquer e $f(x) \in \mathbb{K}[x]$, então existe um corpo de decomposição de $f(x)$ sobre $\mathbb{K}$. Além disso, tal corpo é único no sentido do seguinte resultado:

Teorema 2.14. *Sejam $i : \mathbb{K} \to \mathbb{K}'$ um isomorfismo entre corpos. Definimos a aplicação $\hat{i} : \mathbb{K}[x] \to \mathbb{K}'[x]$ dada por*

$$\hat{i}(a_0 + a_1x + ... + a_nx^n) = i(a_0) + i(a_1)x + ... + i(a_n)x^n\,. \tag{2.4}$$

Sejam Σ um corpo de decomposição de $f(x) \in \mathbb{K}[x]$ e Σ' um corpo de decomposição de $\hat{i}(f(x))$ sobre $\mathbb{K}'$. Então existe um isomorfismo $j : \Sigma \to \Sigma'$ tal que $j|_{\mathbb{K}} = i$.

Demonstração. Ver Teorema 3.8, capítulo V de [7]. ■

Proposição 2.15. *Se $\mathbb{F}$ é um corpo finito com q elementos e $\mathbb{K}$ é um subcorpo de $\mathbb{F}$, então o polinômio $x^q - x \in \mathbb{K}[x]$ é fatorado em $\mathbb{F}[x]$ na forma*

$$x^q - x = \prod_{a \in \mathbb{F}} (x - a) \tag{2.5}$$

e $\mathbb{F}$ é o corpo de decomposição de $x^q - x$ sobre $\mathbb{K}$.

Demonstração. O polinômio $x^q - x$ de grau q possui no máximo q raízes em $\mathbb{F}$. Ainda, pela Proposição 2.11, segue que todos os elementos de $\mathbb{F}$ são raízes de $x^q - x$. Assim, o polinômio $x^q - x$ fatora-se em $\mathbb{F}$ e não pode fatorar-se em nenhum corpo menor, o que nos diz que $\mathbb{F}$ é o corpo de decomposição do polinômio $x^q - x$. ■

Teorema 2.16 (Existência e Unicidade de Corpos Finitos)**.** *Para todo primo p e para todo inteiro positivo n existe um corpo finito com p^n elementos. Além disso, todo corpo finito com $q = p^n$ elementos é isomorfo ao corpo de decomposição do polinômio $x^q - x$ sobre $\mathbb{F}_p$.*

Demonstração. (Existência) Para $q = p^n$, consideremos o polinômio $x^q - x \in \mathbb{F}_p[x]$ e seja $\mathbb{F}$ o corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Esse polinômio possui q raízes distintas em $\mathbb{F}$, já que a sua derivada é $qx^{q-1} - 1 = -1 \neq 0$ em $\mathbb{F}_p[x]$. Seja

$$S = \{a \in \mathbb{F}; a^q - a = 0\}.$$

Então S é um subcorpo de $\mathbb{F}$ pois:

- S contém os elementos 0 e 1;
- a, $b \in S$ implica em $(a - b)^q = a^q - b^q = a - b$ e assim $a - b \in S$;
- Dados a, $b \in S$, $b \neq 0$, então $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$ e assim $ab^{-1} \in S$.

Por outro lado, $x^q - x$ deve se decompor em S já que S contém todas a suas raízes. Logo, $\mathbb{F} = S$ e como S contém q elementos, segue que $\mathbb{F}$ é um corpo finito com q elementos.
(Unicidade) Seja $\mathbb{F}$ um corpo finito com $q = p^n$ elementos. Então $\mathbb{F}$ possui

característica p e assim contém $\mathbb{F}_p$ como um subcorpo. Pela Proposição 2.11, $\mathbb{F}$ é o corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. O resultado segue então da unicidade dos corpos de decomposição. ■

Os corpos finitos são utilizados nas construções da maioria dos códigos corretores de erros que conhecemos. Estes corpos são denotados por $GF(q)$ ou $\mathbb{F}_q$, onde $q \geq 2$ é o número de elementos do corpo, uma potência da característica. Ao longo deste trabalho utilizaremos a segunda notação.

Exemplo 2.17. O corpo finito $\mathbb{F}_{2^2}$ pode ser visto como o corpo de decomposição de $x^4 - x$ sobre $\mathbb{F}_2$. Temos:

$$x^4 - x = x(x-1)(x^2 + x + 1)$$

Veja que essa é de fato a fatoração em irredutíveis de $x^4 - x$ sobre $\mathbb{F}_2$, já que $x^2 + x + 1$ tem grau 2 e não tem raízes em $\mathbb{F}_2$. Assim:

$$\mathbb{F}_4 = \mathbb{F}_2[\alpha] = \{0, 1, \alpha, \alpha^2 \,|\, \alpha^2 + \alpha + 1 = 0\} = \{0, 1, \alpha, \alpha + 1 \,|\, \alpha^2 + \alpha + 1 = 0\}$$

onde a última igualdade segue de $\alpha^2 + \alpha + 1 = 0 \Rightarrow \alpha^2 = \alpha + 1$. Aqui, lembramos que soma e produto de elementos devem levar em conta a característica 2 e que $\alpha^2 + \alpha + 1 = 0$. Assim:

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

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Apesar da nossa escolha, pela garantia da existência e unicidade, de definir corpos finitos como corpos de decomposição de certos polinômios, existe outra forma de enxergá-los que é mais prática para certos cálculos.

Dados um anel comutativo R e um ideal I de R, podemos definir uma relação de equivalência entre elementos de R: $a \equiv b \pmod{I}$ se e somente se $a - b \in I$. As classes de equivalência formam o anel comutativo R/I com adição

e multiplicação induzidos por R (Teorema 2 da Seção III.3 de [5]). Ainda, esse anel R/I é um corpo caso I seja maximal (sempre que exista J ideal de R com $I \subset J \subset R$, então $I = J$ ou $J = R$), veja o Teorema 3 da Seção III.3 de [5]. Quando K é um corpo, podemos provar que os ideais maximais de $K[x]$ são aqueles gerados por polinômios irredutíveis sobre K (veja o Teorema 4 da seção IV.4 de [5]).

Assim, fixados um número primo p e um inteiro positivo n, seja $f(x) \in \mathbb{F}_p[x]$ um polinômio irredutível de grau n. Podemos construir então $\mathbb{F}_p[x]/\langle f(x)\rangle$, que é um corpo finito com p^n elementos. De fato, se $g(x) \in \mathbb{F}_p[x]$, então existem $q(x), r(x) \in \mathbb{F}_p[x]$ tais que $g(x) = f(x)q(x) + r(x)$ com $r(x) = 0$ ou de grau menor que o grau de $f(x)$. Assim, em $\mathbb{F}_p[x]/\langle f(x)\rangle$, temos $\overline{g(x)} = \overline{r(x)}$, o que significa que os elementos de $\mathbb{F}_p[x]/\langle f(x)\rangle$ podem ser identificados com os polinômios de grau no máximo $n-1$ e coeficientes em $\mathbb{F}_p$, que são exatamente p^n. Assim, pelo Teorema 2.16, podemos considerar $\mathbb{F}_{p^n}$ como $\mathbb{F}_p[x]/\langle f(x)\rangle$. A questão aqui é que estamos supondo que para quaisquer n inteiro positivo e p primo existe um polinômio irredutível de grau n em $\mathbb{F}_p[x]$. Essa suposição é verdadeira: é possível provar que se $I(n)$ é o número de polinômios mônicos irredutíveis de grau n em $\mathbb{F}_p[x]$, então

$$p^n = \sum_{d|n} d\ I(d)\,. \tag{2.6}$$

Para referência desses resultados, veja a Proposição 11 e o Teorema 2 do capítulo IV de [6].

Exemplo 2.18. O $\mathbb{F}_{2^2}$ pode ser construído como $\mathbb{F}_2/\langle x^2+x+1\rangle$, já que x^2+x+1 é irredutível em $\mathbb{F}_2[x]$. Nesse caso:

$$\mathbb{F}_4 = \mathbb{F}_2/\langle x^2+x+1\rangle = \{a\alpha+b \,|\, a,b \in \mathbb{F}_2 \text{ e } \alpha^2+\alpha+1=0\} = \{0,1,\alpha,\alpha+1 \,|\, \alpha^2+\alpha+1=0\}$$

Exemplo 2.19. O polinômio $x^3-x+1 \in \mathbb{F}_3$ é irredutível sobre $\mathbb{F}_3$. Então:

$$\mathbb{F}_{27} = \mathbb{F}_3/\langle x^3-x+1\rangle = \{a\alpha^2+b\alpha+c \,|\, a,b,c \in \mathbb{F}_3 \text{ e } \alpha^3-\alpha+1=0\}$$

Veja que então podemos encontrar todos os elementos de $\mathbb{F}_{27}$ variando $a, b, c \in \mathbb{F}_3$. Fazendo isso e usando $\alpha^3 - \alpha + 1 = 0$, obtemos os seguintes elementos de $\mathbb{F}_{27}$:

0	$\alpha^8 = -\alpha^2 - 1$	$\alpha^{17} = -\alpha^2 + \alpha$
1	$\alpha^9 = \alpha + 1$	$\alpha^{18} = \alpha^2 - \alpha + 1$
α	$\alpha^{10} = \alpha^2 + \alpha$	$\alpha^{19} = -\alpha^2 - \alpha - 1$
α^2	$\alpha^{11} = \alpha^2 + \alpha - 1$	$\alpha^{20} = -\alpha^2 + \alpha + 1$
$\alpha^3 = \alpha - 1$	$\alpha^{12} = \alpha^2 - 1$	$\alpha^{21} = \alpha^2 + 1$
$\alpha^4 = \alpha^2 - \alpha$	$\alpha^{13} = -1$	$\alpha^{22} = -\alpha - 1$
$\alpha^5 = -\alpha^2 + \alpha - 1$	$\alpha^{14} = -\alpha$	$\alpha^{23} = -\alpha^2 - \alpha$
$\alpha^6 = \alpha^2 + \alpha + 1$	$\alpha^{15} = -\alpha^2$	$\alpha^{24} = -\alpha^2 - \alpha + 1$
$\alpha^7 = \alpha^2 - \alpha - 1$	$\alpha^{16} = -\alpha + 1$	$\alpha^{25} = -\alpha^2 + 1$

Veja que $\alpha^{26} = -\alpha^3 + \alpha = -\alpha + 1 + \alpha = 1$. Assim, o elemento α está nas condições da Definição 2.20, dada a seguir.

Observe ainda que a escrita do elementos como potência de α ajuda na operação de produto, por exemplo: $\alpha^7\alpha^{13} = \alpha^{20} = -\alpha^2 + \alpha + 1$.

Definição 2.20. *Um elemento α de um corpo finito $\mathbb{F}_q$ é chamado* ***elemento primitivo*** *se*

$$\mathbb{F}_q^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}, \tag{2.7}$$

isto é, a ordem de α é igual a $q - 1$.

É possível provar que os subcorpos de $\mathbb{F}_{q^m}$ são exatamente os corpos $\mathbb{F}_{q^n}$ com n um divisor de m (veja a proposição 1 da seção 7.1 de [6]). Nesse cenário, temos:

Definição 2.21. *Sejam $\alpha \in \mathbb{F}_{q^m}$ e $f(x) \in \mathbb{F}_q[x]$ um polinômio mônico. Dizemos que f é um* ***polinômio mínimo*** *para α sobre $\mathbb{F}_q$ quando α é uma raiz de f e f é irredutível sobre $\mathbb{F}_q[x]$.*

Observação 2.22. Como na teoria de corpos em geral, o polinômio mínimo em $\mathbb{F}_q[x]$ de $\alpha \in \mathbb{F}_{q^m}$ é o polinômio mônico de menor grau que tem α como raiz.

Definição 2.23. *Sejam $\alpha \in \mathbb{F}_{q^m}$ e $f(x) \in \mathbb{F}_q[x]$ um polinômio mônico. Se α é um elemento primitivo de $\mathbb{F}_{q^m}$, e f é um polinômio mínimo para α sobre $\mathbb{F}_q$, dizemos que f é um* ***polinômio primitivo****.*

Veja que nem todo polinômio mônico irredutível sobre $\mathbb{F}_q$ é um polinômio primitivo. Por exemplo, em $\mathbb{F}_{2^4}$, seja α tal que $\alpha^4 + \alpha + 1 = 0$. Então, α é um elemento primitivo (ou seja, que gera $\mathbb{F}_{2^4}^*$). De fato:

É possível verificar, por exemplo, que α^2 e α^4 também são primitivos, mas α^3 e α^5 não. Por exemplo, $x^4 + x^3 + x^2 + x + 1$ é irredutível, mas não é primitivo. É possível provar que o polinômio primitivo de um elemento de $\mathbb{F}_{p^m}$ tem grau m (veja a propriedade M5 da seção 4.3 de [10]). Em geral, não é fácil listar todos os polinômios primitivos de certo grau em um anel $\mathbb{F}_q[x]$, porém para corpos pequenos há listas, como em [9].

3 CÓDIGOS CORRETORES DE ERROS

Este capítulo é dedicado a apresentação dos conceitos básicos da teoria de Códigos Corretores de Erros, podendo servir como uma introdução ao assunto. Aqui, vamos definir o que são os códigos corretores de erros, a métrica de Hamming e os parâmetros de um código.

3.1 O que é um Código

- $\mathcal{A}$ um ***alfabeto***;
- ***Letras*** são os elementos de $\mathcal{A}$;
- $\mathcal{A}^n$ denota que $\mathcal{A}$ é um alfabeto cuja maior palavra tem ***comprimento*** n;
- ***Palavras*** são os elementos de $\mathcal{A}^n$;
- Os elementos de $\mathcal{A}^n$ poderão ser representados por $a_1 \cdots a_n$ em vez de $(a_1, \ldots, a_n)$.

Façamos um exemplo para ilustrar os princípios dessa teoria. Suponhamos que temos um robô que se move sobre um tabuleiro quadriculado, de modo que, ao darmos um dos comandos (Leste, Oeste, Norte ou Sul), o robô se desloca do centro de uma casa para o centro da casa adjunta indicada pelo comando.

Os quatro comandos acima descritos podem ser codificados como elementos de $\{0,1\} \times \{0,1\}$, como segue-se:

$$\mathcal{C}_1 = \begin{cases} \text{Leste} \mapsto 00 \\ \text{Oeste} \mapsto 01 \\ \text{Norte} \mapsto 10 \\ \text{Sul} \mapsto 11 \end{cases} . \tag{3.1}$$

O código do lado direito é chamado de ***código da fonte***.

Suponhamos, que esses pares ordenados devam ser transmitidos via radio e que o sinal no caminho sofra interferências. Imaginemos que a mensagem 00 possa,

na chegada, ser recebida como 01, o que faria com que o robô, em vez de ir para Leste, fosse para Oeste. Desse modo, o erro ocorrido durante a transmissão não seria percebido. Esse problema ocorre por conta da "proximidade"[1] das palavras. Para diminuir a possibilidade de que casos como esse ocorram, o que se faz é recodificar as palavras, de modo a introduzir ***redundâncias*** (acrescentar mais letras) que permitam detectar e corrigir erros.

Por exemplo, modificar o nosso código da seguinte forma:

$$\mathcal{C}_2 = \begin{cases} \text{Leste} \mapsto 000 \\ \text{Oeste} \mapsto 010 \\ \text{Norte} \mapsto 101 \\ \text{Sul} \mapsto 111 \end{cases} . \tag{3.2}$$

Nessa recodificação, as duas primeiras posições reproduzem o código da fonte, enquanto que as três posições restantes são redundâncias introduzidas. O novo código introduzido na recodificação é chamado de ***código de canal***. Agora, caso haja erro em uma letra, será possível saber que a informação estará errada, pois a palavra recebida não pertencerá ao código. No entanto, não será possível descobrir qual era a mensagem correta. Por exemplo, ao receber a mensagem 011, é possível perceber que a mensagem está errada. Porém, não há maneiras de saber se a mensagem correta era 010 ou 111. Logo, esse código detecta erros, mas não os corrige. Isso acontece porque as palavras do código ainda estão muito próximas. Isso pode ser corrigido com mais redundâncias.

Por exemplo:

$$\mathcal{C}_3 = \begin{cases} \text{Leste} \mapsto 00000 \\ \text{Oeste} \mapsto 01011 \\ \text{Norte} \mapsto 10110 \\ \text{Sul} \mapsto 11101 \end{cases} . \tag{3.3}$$

Agora, caso haja erro em uma letra, será possível não somente detectar, mas também corrigir erros. De fato, basta escolhermos no código a palavra que tem apenas uma letra diferente da recebida. Por exemplo, suponhamos que se tenha

[1] Ainda vamos definir matematicamente o que significa essa terminologia.

introduzido um erro ao transmitirmos a palavra 10110, de modo que a mensagem recebida seja 11110. Comparando essa mensagem com as demais palavras do código, notamos que não lhe pertence e, portanto, detectamos erros. A palavra do código mais próxima da referida mensagem (a que tem menor número de letras diferentes) é 10110, que é precisamente a palavra transmitida

O procedimento acima pode ser esquematizado como mostra a Figura 1.

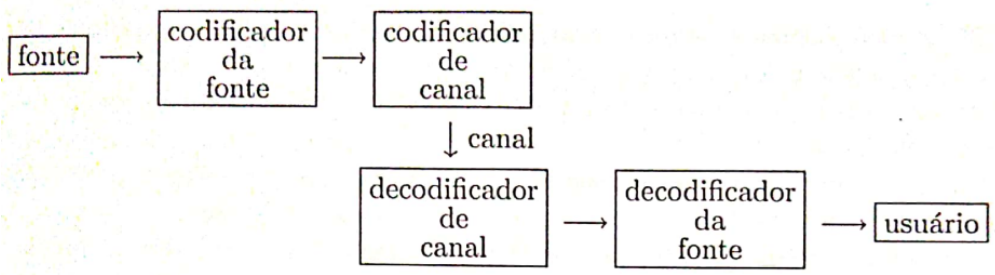

Figura 1 – Procedimento da codificação. Fonte [6].

O nosso estudo consiste em transformar o código da fonte em código de canal, em detectar e corrigir erros na recepção e em decodificar o código de canal em código da fonte.

3.2 Métrica de Hamming

Seja $\mathbb{N} = \{1, 2, 3, \ldots\}$ o conjunto dos números naturais.

Agora, vamos definir os elementos necessários para a construção de um código corretor de erros.

Definição 3.1. *Um conjunto finito $\mathcal{A} = \{a_1, a_2, \ldots, a_q\}$, com $q \in \mathbb{N}$, será dito um* ***alfabeto****. Os elementos $a_i \in \mathcal{A}$, onde $i \in \{1, 2, \ldots, q\}$, são chamados de* ***letras****. O* ***número de elementos*** *de $\mathcal{A}$, será denotado por $|\mathcal{A}|$ e simbolizado por q. A sequência $a_{k_1}a_{k_2}\cdots a_{k_j}$ ou $(a_{k_1}, a_{k_2} \ldots, a_{k_j})$, com $a_{k_i} \in \mathcal{A}$ para cada $i \in \{1, 2, \ldots, j\}$, é denominada por* ***palavra*** *do código $\mathcal{A}$. O* ***comprimento de uma palavra*** *é o número de letras que a forma. Além disso, $\mathcal{A}^n$ denota que $\mathcal{A}$ é um alfabeto cuja* ***maior palavra*** *tem comprimento n.*

Definição 3.2. *Um* ***código corretor de erros*** $\mathcal{C}$ *é um subconjunto próprio qualquer de* $\mathcal{A}^n$*, para algum* $n \in \mathbb{N}$*.*

Pelos exemplos que demos na seção anterior, compreendemos que a detecção e correção de erros depende da distância entre as palavras. Agora, buscamos uma maneira matemática para podermos comparar a proximidade entre palavras. Para isso, introduziremos a noção de distância e então, apresentaremos um modo de medir a distância entre palavras.

Definição 3.3. *Seja* M *um conjunto não vazio. Uma* ***métrica*** *(ou* ***distância*** *ou* ***função analítica****) em* M *é uma função*

$$\begin{aligned} d : M \times M &\to \mathbb{R}_+ \\ (x, y) &\mapsto d(x, y) \in \mathbb{R}_+ \end{aligned}$$

que associa a cada par ordenado $(x, y) \in M \times M$ *um número real positivo* $d(x, y)$*, de modo que, dados* $x, y, z \in M$ *as seguintes condições são satisfeitas:*

(d1) $d(x, x) = 0$*.*

(d2) Se $x \neq y$*, então* $d(x, y) > 0$*.*

(d3) $d(x, y) = d(y, x)$*.*

(d4) $d(x, z) \leqslant d(x, y) + d(y, z)$*.*

Definição 3.4. *Dados dois elementos* $u, v \in \mathcal{A}^n$*, a* ***distância de Hamming*** *entre* u *e* v *é dada por*

$$d(u, v) = |\{i;\ u_i \neq v_i,\ i \leqslant i \leqslant n\}|. \tag{3.4}$$

Em outras palavras, a distância de Hamming entre u e v é definida como o número de coordenadas distintas entre u e v.

Exemplo 3.5. Considere $\mathcal{A} = \{0, 1\} \times \{0, 1\} \times \{0, 1\} = \{0, 1\}^3$. Queremos encontrar, para cada par de elementos $u, v \in \mathcal{A}^3$, a distância de Hamming entre u

e v. Temos:

$$\begin{array}{llll} d(000,000) = 0; & d(001,000) = 1; & d(011,000) = 2; & d(111,000) = 3; \\ d(000,001) = 1; & d(001,001) = 0; & d(011,001) = 1; & d(111,001) = 2; \\ d(000,011) = 2; & d(001,011) = 1; & d(011,011) = 0; & d(111,011) = 1; \\ d(000,111) = 3; & d(001,001) = 2; & d(011,111) = 1; & d(111,111) = 0. \end{array}$$

Mostraremos na seguinte proposição que a distância de Hamming realmente pode ser vista como uma distância.

Proposição 3.6. *Dados $u, v, w \in \mathcal{A}^n$, valem as seguintes propriedades:*

i) Positividade: $d(u,v) \geqslant 0$, valendo a igualdade se, e somente se, $u = v$.

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

iii) Desigualdade Triangular: $d(u,v) \leqslant d(u,w) + d(w,v)$.

Demonstração. Comecemos com as duas primeiras propriedades, que são provadas mais diretamente. Claramente, pela forma em que definimos a distância de Hamming, temos $d(u,v) \geqslant 0$. Ademais:

$$\begin{aligned} d(u,v) = 0 &\Leftrightarrow |\{i;\ u_i \neq v_i,\ i \leqslant i \leqslant n\}| = 0 \\ &\Leftrightarrow \nexists i;\ u_i \neq v_i \\ &\Leftrightarrow u_i = v_i, \forall i = 1, \ldots, n \\ &\Leftrightarrow u = v. \end{aligned}$$

Também:

$$\begin{aligned} d(u,v) &= |\{i;\ u_i \neq v_i,\ i \leqslant i \leqslant n\}| \\ &= |\{i;\ v_i \neq u_i,\ i \leqslant i \leqslant n\}| \\ &= d(v,u). \end{aligned}$$

Por fim, demonstraremos a terceira propriedade, cuja demonstração não é totalmente trivial.

A contribuição das i-ésimas coordenadas de u e v para $d(u,v)$ é igual a:

$$\begin{cases} 0, & \text{se } u_i = v_i \\ 1, & \text{se } u_i \neq v_i \end{cases},$$

Por outro lado, a contribuição das i-ésimas coordenadas para $d(u,w) + d(w,v)$ é

$$\begin{cases} 0, & \text{se } u_i = w_i \text{ e } w_i = v_i \\ 1, & \text{se } u_i = w_i \text{ e } w_i \neq v_i, \text{ ou } u_i \neq w_i \text{ e } w_i = v_i \\ 2, & \text{se } u_i \neq w_i \text{ e } w_i \neq v_i \end{cases}.$$

Analisemos cada caso:

- Se a contribuição das i-ésimas coordenadas de de u e v a $d(u,v)$ for 0, então segue que a contribuição das i-ésimas coordenadas a $d(u,v)$ será menor ou igual a das i-ésimas coordenadas a $d(u,w) + d(w,v)$.
- Se a contribuição das i-ésimas coordenadas de u e v a $d(u,v)$ for 1, isto é, $u_i \neq v_i$, não teremos $u_i = w_i$ e $w_i = v_i$, simultaneamente. Por conseguinte, a contribuição das i-ésimas coordenadas a $d(u,w) + d(w,v)$ é maior ou igual a 1, que é a contribuição das i-ésimas coordenadas a $d(u,v)$.

Portanto, provamos as três propriedades. ■

Observação 3.7. As propriedades que provamos na Proposição 3.6, estão dentro das condições da Definição 3.3. Por conta disso, a distância de Hamming entre elementos de $\mathcal{A}^n$ é também chamada de ***métrica de Hamming***.

Dados um elemento $a \in \mathcal{A}^n$ e um número real $t \geqslant 0$, definimos o ***disco*** e a ***esfera*** de centro a e raio t como sendo, respectivamente, os conjuntos

$$D(a,t) = \{u \in \mathcal{A}^n;\ d(u,a) \leqslant t\}, \tag{3.5}$$

$$S(a,t) = \{u \in \mathcal{A}^n;\ d(u,a) = t\}. \tag{3.6}$$

Estes conjunto são finitos e o próximo lema nos fornecerá as suas cardinalidades.

Antes de enunciar o próximo lema, ao longo do texto usaremos a notação usual para a combinação de elementos, dois a dois, ou seja,

$$\binom{n}{i} = \frac{n!}{i!(n-i)!} \tag{3.7}$$

e denotaremos por $|B|$ o número de elementos de um conjunto finito B.

Lema 3.8. *Para todo $a \in \mathcal{A}^n$ e todo número natural $r > 0$, temos que*

$$|D(a,r)| = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i. \tag{3.8}$$

Demonstração. Seja $u \in S(a,r)$. Suponhamos $u = (u_1, \ldots, u_n)$ e $a = (a_1, \ldots, a_n)$. Temos:

$$d(u,a) = 0 \;\; \Leftrightarrow \;\; |\{i;\ u_i \neq a_i,\ i \leqslant i \leqslant n\}| = t, \text{ com } t \in \{0, \ldots n\}.$$

■

Note que, a cardinalidade de $D(a,r)$ depende apenas n (tamanho da maior palavra em $\mathcal{A}$), q (número de elementos de $\mathcal{A}$) e r (raio do disco ou esfera).

Definição 3.9. *Seja $\mathcal{C} \subset \mathcal{A}^n$ um código. A **distância mínima** de $\mathcal{C}$ é o número*

$$d = \min\{d(u,v);\ u,v \in \mathcal{C} \text{ e } u \neq v\}. \tag{3.9}$$

Exemplo 3.10. Considerando $\mathcal{C}$ o código robô, temos $d = 3$. De fato, sabemos que as palavras de $\mathcal{C}$ são: $00000, 01011, 10110, 11101$. Desta forma:

$$\begin{aligned}
d(00000, 01011) &= 3,\\
d(00000, 10110) &= 3,\\
d(00000, 11101) &= 4,\\
d(01011, 10110) &= 4,\\
d(01011, 11101) &= 3,\\
d(10110, 11101) &= 3.
\end{aligned}$$

Logo, $d = 3$.

A princípio, para calcular d é necessário $\binom{M}{2}$ distâncias, onde M é o número de palavras no códio. Isto tem grande custo computacional. Veremos mais adiante como pode-se calcular d de modo mais econômico em códigos, com alguma estrutura algébrica adicional.

Dado um código $\mathcal{C} \subset \mathcal{A}^n$, com distância mínima d, defini-se

$$\kappa = \left[\frac{d-1}{2}\right], \tag{3.10}$$

onde $[t]$ representa a ***parte inteira*** de $t \in \mathbb{R}$.

Lema 3.11. *Seja $\mathcal{C} \subset \mathcal{A}^n$ um código com distância mínima d. Se c e c' são palavras distintas de $\mathcal{C}$, então*

$$D(c,\kappa) \cap D(c',\kappa) = \varnothing. \tag{3.11}$$

Demonstração. De fato, suponhamos, por absurdo , que existisse $x \in D(c,\kappa) \cap D(c',\kappa)$. Desta forma, teríamos $d(x,c) \leqslant \kappa$ e $d(x,c') \leqslant \kappa$, donde seguiria

$$\begin{aligned} d(c,c') &\overset{\text{desigualdade triangular}}{\leqslant} && d(c,x) + d(x,c') \\ &\overset{\text{simetria}}{=} && \underbrace{d(x,c)}_{\leqslant\kappa} + \underbrace{d(x,c')}_{\leqslant\kappa} \\ &= && 2\kappa \\ &\leqslant && d-1. \end{aligned}$$

Absurdo, pois $d(c,c') \geqslant d$, já que d é a distância mínima de $\mathcal{C}$. ■

A principal importância da distância mínima d de um código pode ser observada a seguir.

Teorema 3.12. *Seja $\mathcal{C}$ um código com distância mínima d. Então $\mathcal{C}$ pode corrigir até $\kappa = \left[\frac{d-1}{2}\right]$ erros e detectar até $d-1$ erros.*

Demonstração. Se ao transmitirmos uma palavra c do código cometemos t erros, com $t \leqslant \kappa$, recebendo a palavra r, então $d(r,c) = t \leqslant \kappa$; enquanto que, pelo Lema 2, a distância de r a qualquer outra palavra do código e maior do que κ. Isso determina c univocamente a partir de r.

Por outro lado, dada uma palavra do código, podemos nela introduzir até $d-1$ erros sem encontrar outra palavra do código. ■

Exemplo 3.13. No código robô, como $d = 3$, então pelo Teorema 3.12, podemos corrigir até

$$\kappa = \left[\frac{d-1}{2}\right] = \left[\frac{3-1}{2}\right] = \left[\frac{2}{2}\right] = [1] = 1 \text{ erros}$$

e detectar até $d - 1 = 3 - 1 = 2$ erros.

Observação 3.14. Note que, pelo Teorema 3.12, temos que quanto maior for a distância mínima d de um determinado código, maior será sua capacidade de detecção e correção de erros. Logo, é importante poder encontrar d ou pelo menos uma cota inferior para d.

O Teorema 3.12 também permite traçarmos uma estratégia para detecção e correção de erros. De fato, sejam $\mathcal{C} \subset \mathcal{A}^n$ um código com distância mínima d e $\kappa = \left[\frac{d-1}{2}\right]$.

Quando o receptor recebe uma palavra r, uma, e somente uma, das seguintes afirmações é verificada:

1. Existe $c \in \mathcal{C}$ tal que $r \in D(c, \kappa)$, isto é, $d(r, c) \leqslant \kappa$. Neste caso, substitui-se r por c.

2. Não existe $c \in \mathcal{C}$ tal que $r \in D(c, \kappa)$, isto é, $d(r, c) > \kappa$, para todo $c \in C$. Neste caso, não é possível decodificar r com uma boa margem de segurança.

Observe que em 1. não se pode ter certeza absoluta de que c tenha sido a palavra transmitida, pois poderíamos ter cometido mais do que κ erros, afastando assim r da palavra transmitida e aproximando-a a outra palavra do código. Esta questão deve ser encarada em termos probabilísticos.

Um código $\mathcal{C}$ sobre um alfabeto $\mathcal{A}$ possui três ***parâmetros*** fundamentais $[n, M, d]$, que são, respectivamente, o seu comprimento (isto é, n corresponde ao espaço ambiente $\mathcal{A}^n$ onde $\mathcal{C}$ encontra-se), o seu número de elementos e sua distância mínima. Interessam os códigos para os quais M e d são relativamente grandes a n. Dados três inteiros positivos arbitrários n, M e d, nem sempre existe um código que

tenha parâmetros $[n, M, d]$, pois há uma interdependência complexa entre estes três números, e um dos problemas fundamentais da Teoria de Códigos é o de estudá-la.

4 CÓDIGOS LINEARES

4.1 Códigos Lineares

A classes de códigos mais utilizada na prática é a chamada classe de códigos lineares, à qual estamos estudando neste trabalho.

Aqui, nosso alfabeto será um corpo finito $\mathbb{F}_q$ com q elementos. Dessa forma, para cada número natural n, temos $\mathbb{F}_q^n$ um espaço vetorial sobre $\mathbb{F}_q$ de dimensão n.

Definição 4.1. *Um código $\mathcal{C} \subset \mathbb{F}_q^n$ é dito um* ***código linear*** *se for um subespaço vetorial de $\mathbb{F}_q^n$.*

Exemplo 4.2. Seja $\mathcal{C} = \{00000, 01011, 10110, 11101.\}$ o código robô.

Considerando como alfabeto o Corpo de Galois $\mathcal{A} = \mathbb{F}_2 = \{0, 1\}$, então $\mathcal{C}$ é um subespaço vetorial de $\mathbb{F}_2^5$, que é imagem da transformação linear

$$\begin{array}{rccc} T: & \mathbb{F}_2^2 & \to & \mathbb{F}_2^5 \\ & (x_1, x_2) & \mapsto & (x_1, x_2, x_1, x_1 + x_2, x_2) \end{array}$$

Como um código linear qualquer é definido como um subespaço de um espaço vetorial de dimensão finita, segue que todo código linear é, por definição, um espaço vetorial de dimensão finita.

Considere k a dimensão do código linear $\mathcal{C}$. Seja $\mathcal{B} = \{v_1, v_2, \ldots, v_k\}$ uma base de $\mathcal{C}$. Então, dado um elemento $v \in \mathcal{C}$, escrevemos v de forma única na forma

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k,$$

com $a_i \in \mathbb{F}_q$, para $i = 1, 2, \ldots, k$. Assim

$$M = |\mathcal{C}| = q^k, \tag{4.1}$$

donde,

$$\dim_{\mathbb{F}_q} \mathcal{C} = k = \log_q q^k = \log_q M. \tag{4.2}$$

Definição 4.3. *Dado $x \in \mathbb{F}_q^n$, definimos o* ***peso*** *de x como o número inteiro*

$$\omega(x) = |\{i;\ x_i \neq 0\}|. \tag{4.3}$$

Perceba que, se d é a métrica de Hamming, então

$$\omega(x) = d(x, 0). \tag{4.4}$$

Definição 4.4. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear. Definimos o* ***peso*** *de $\mathcal{C}$ como o inteiro*

$$\omega(\mathcal{C}) = \min\{\omega(x);\ x \in \mathcal{C} \setminus \{0\}\}. \tag{4.5}$$

Proposição 4.5. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear com distância mínima d. Então, as seguintes afirmações são válidas:*

1. *Para todos $x, y \in \mathbb{F}_q^n$ vale $d(x, y) = \omega(x - y)$;*
2. *$d = \omega(\mathcal{C})$.*

Demonstração. Dados $x, y \in \mathbb{F}_q^n$, sabemos que a distância de Hamming é definida como

$$d(x, y) = |\{i;\ x_i \neq y_i,\ 1 \leq i \leq n\}|. \tag{4.6}$$

Além disso, sendo $x = (x_1, x_2, \ldots, x_n)$ e $y = (y_1, y_2, \ldots, y_n)$, então

$$x - y = (x_1, x_2, \ldots, x_n) - (y_1, y_2, \ldots, y_n) = (x_1 - y_1, x_2 - y_2, \ldots, x_n - y_n).$$

Assim:

$$\begin{aligned} \omega(x - y) &= d(x - y, 0) \\ &= |\{i;\ x_i - y_i \neq 0,\ 1 \leq i \leq n\}| \\ &= |\{i;\ x_i \neq y_i,\ 1 \leq i \leq n\}| \\ &= d(x, y). \end{aligned}$$

Logo, $d(x, y) = \omega(x - y)$, para todos $x, y \in \mathbb{F}_q^n$.

Agora, para todo par de elementos x, y em $\mathcal{C}$, com $x \neq y$, temos $x - y \in \mathcal{C} \setminus \{0\}$. Tome $z = x - y \in \mathcal{C} \setminus \{0\}$. Então, pelo que acabamos de provar,

$d(x,y) = \omega(x-y) = \omega(z)$. Consequentemente:

$$\begin{aligned} d &= \min\{d(x,y);\ x,y \in \mathcal{C} \text{ e } x \neq y\} \\ &= \min\{d(x,y);\ x,y \in \mathcal{C} \text{ e } x-y \neq 0\} \\ &= \min\{d(x,y);\ x-y \in \mathcal{C} \setminus \{0\}\} \\ &= \min\{\omega(z);\ z \in \mathcal{C} \setminus \{0\}\} \\ &= \omega(\mathcal{C}). \end{aligned}$$

Portanto, $d = \omega(\mathcal{C})$, como queríamos demonstrar. ■

Note que, pela Proposição 4.5, em códigos lineares com M elementos, podemos calcular a distância mínima d a partir de $M-1$ cálculos de distância, em vez dos $\binom{M}{2} = \dfrac{M!}{2(M-2)!}$ cálculos anteriormente requeridos. Na prática, em códigos grandes, esse método de cálculo de d é inviável por representar um custo computacional muito elevado. Dessa forma, queremos desenvolver outros métodos para determinarmos a distância mínima de um código.

Em virtude do item 2 da Proposição 4.5, a distância mínima de um código linear $\mathcal{C}$ será também chamada de ***peso do código*** $\mathcal{C}$. Em Álgebra Linear, conhecemos essencialmente duas maneiras para descrevermos subespaços vetoriais $\mathcal{C}$ de um espaço vetorial $\mathbb{F}_q^n$. São eles:

- Descrevermos o subespaço $\mathcal{C}$ como imagem de uma transformação linear;
- Descrevermos o subespaço $\mathcal{C}$ como o núcleo de uma transformação linear.

Primeiramente, observemos como se obtém a representação de $\mathcal{C}$ como imagem.

Escolhemos uma base $\mathcal{B} = \{v_1, v_2, \ldots, v_k\}$ de $\mathcal{C}$ e consideramos a transformação linear

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \to & \mathbb{F}_q^n \\ & x = (x_1, x_2, \ldots, x_k) & \mapsto & x_1v_1 + x_2v_2 + \cdots + x_kv_k \end{array} \tag{4.7}$$

Então T é uma transformação linear injetora.

De fato:

- T é linear:

  Sejam $x = (x_1, x_2, \ldots, x_k)$ e $y = (y_1, y_2, \ldots, y_k)$ em $\mathbb{F}_q^k$ e $a \in \mathbb{F}_q$. Temos:

$$\begin{aligned}
T(x + ay) &= T(x_1 + ay_1, x_2 + ay_2, \ldots, x_k + ay_k) \\
&= (x_1 + ay_1)v_1 + (x_2 + ay_2)v_2 + \cdots + (x_k + ay_k)v_k \\
&= x_1v_1 + ay_1v_1 + x_2v_2 + ay_2v_2 + \cdots + x_kv_k + ay_kv_k \\
&= x_1v_1 + a(y_1v_1) + x_2v_2 + a(y_2v_2) + \cdots + x_kv_k + a(y_kv_k) \\
&= x_1v_1 + x_2v_2 + \cdots x_kv_k + a(y_1v_1) + a(y_2v_2) + \cdots a(y_kv_k) \\
&= x_1v_1 + x_2v_2 + \cdots x_kv_k + a(y_1v_1 + y_2v_2 + \cdots + y_kv_k) \\
&= T(x_1, x_2, \ldots, x_k) + aT(y_1, y_2, \ldots, y_k) \\
&= T(x) + aT(y).
\end{aligned}$$

- T é injetora:

  Sejam $x = (x_1, x_2, \ldots, x_k)$ e $y = (y_1, y_2, \ldots, y_k)$ em $\mathbb{F}_q^k$. Então:

$$\begin{aligned}
T(x) = T(y) &\Rightarrow T(x_1, x_2, \ldots, x_k) = T(y_1, y_2, \ldots, y_k) \\
&\Rightarrow x_1v_1 + x_2v_2 + \cdots + x_kv_k = y_1v_1 + y_2v_2 + \cdots + y_kv_k \\
&\Rightarrow x_1v_1 + x_2v_2 + \cdots + x_kv_k - (y_1v_1 + y_2v_2 + \cdots + y_kv_k) = 0 \\
&\Rightarrow x_1v_1 + x_2v_2 + \cdots + x_kv_k - y_1v_1 - y_2v_2 - \cdots - y_kv_k = 0 \\
&\Rightarrow (x_1 - y_1)v_1 + (x_2 - y_2)v_2 + \cdots + (x_k - y_k)v_k \\
&\overset{\mathcal{B} \text{ é base de } \mathcal{C}}{\Rightarrow} x_1 - y_1 = 0,\ x_2 - y_2 = 0,\ \ldots,\ x_k - y_k = 0 \\
&\Rightarrow x_1 = y_1,\ x_2 = y_2,\ \ldots,\ x_k = y_k \\
&\Rightarrow x = y.
\end{aligned}$$

  Ademais, a imagem de T é C, isto é, $Im(T) = \mathcal{C}$.

Portanto, dar um código linear $\mathcal{C} \subset \mathbb{F}_q^n$ de dimensão k é equivalente a dar uma transformação linear injetora

$$T : \mathbb{F}_q^k \to \mathbb{F}_q^n$$

e definir $\mathcal{C} = \Im(T)$. Essa é a ***forma paramétrica*** do subespaço $\mathcal{C}$. Esta nomenclatura decorre do fato de que todo elemento de $\mathcal{C}$ é parametrizado pelos x

de $\mathbb{F}_q^k$ através da transformação linear T, o que torna fácil gerar todos os elementos de $\mathcal{C}$. Note que nessa representação é, porém, difícil decidir se um elemento $v = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ pertence ou não a $\mathcal{C}$, pois, para tal, é necessário resolver o sistema de n equações e k incógnitas $a_i, a_2, \ldots, a_k$ abaixo[1]

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k = (x_1, x_2, \ldots, x_n).$$

A resolução de tal sistema, em geral, tem um custo computacional muito elevado.

A outra maneira de descrevermos um código $\mathcal{C}$ é através do núcleo de uma transformação linear. Com este propósito, tome $\mathcal{C}'$ um subespaço de $\mathbb{F}_q^n$ complementar de $\mathcal{C}$, isto é,

$$\mathcal{C} \oplus \mathcal{C}' = \mathbb{F}_q^n, \tag{4.8}$$

e considere a aplicação linear

$$\begin{array}{rccc} H: & \mathcal{C} \oplus \mathcal{C}' & \to & \mathbb{F}_q^{n-k} \\ & u \oplus v & \mapsto & v \end{array} \tag{4.9}$$

Então, $\mathcal{C}$ é o núcleo da transformação linear H. De fato:

$$\begin{aligned} \ker(H) &= \{u \oplus v \in \mathcal{C} \oplus \mathcal{C}';\ H(u \oplus v) = 0\} \\ &= \{u \oplus v \in \mathcal{C} \oplus \mathcal{C}';\ v = 0\} \\ &= \{u \oplus 0;\ u \in \mathcal{C}\} \\ &= \{u;\ u \in \mathcal{C}\} \\ &= \mathcal{C}. \end{aligned}$$

Computacionalmente, é muito mais simples determinar se um certo elemento $v \in \mathbb{F}_q^n$ pertence ou não a $\mathcal{C}$, pois, para isso, basta verificar se $H(v)$ é ou não o vetor nulo de $\mathbb{F}_q^{n-k}$, o que tem um custo computacional bem pequeno.

Exemplo 4.6. Consideremos o corpo finito com três elementos $\mathbb{F}_3 = \{0, 1, 2\}$ e seja $\mathcal{C} = \text{ger}\{(1, 0, 1, 1), (0, 1, 1, 2)\} \subset \mathbb{F}_3^4$. Denotemos $v_1 = (1, 0, 1, 1)$ e $v_2 = (0, 1, 1, 2)$. Esse código possui

$$q^k = 3^2 = 9 \text{ elementos.},$$

[1] Lembre que, $v_i \in \mathbb{F}_q^n$ para cada $i \in \{1, 2, \ldots, k\}$.

pois tem dimensão 2 sobre um corpo com 3 elementos. Os elementos de $\mathcal{C}$ são:

$$\begin{aligned}
u_1 &= (0,0,0,0)\\
u_2 &= v_1 = (1,0,1,1)\\
u_3 &= v_2 = (0,1,1,2)\\
u_4 &= 2\cdot(1,0,11) = (2,0,2,2)\\
u_5 &= 2\cdot(0,1,1,2) = (0,2,24) = (0,2,2,1)\\
u_6 &= 1\cdot(1,0,1,1) + 1\cdot(0,1,1,2) = (1,0,1,1) + (0,1,1,2) = (1,1,2,3) = (1,1,2,0)\\
u_7 &= 1\cdot(1,0,1,1) + 2\cdot(0,1,1,2) = (1,0,1,1) + (0,2,2,4) = (1,0,1,1) + (0,2,2,1)\\
&= (1,2,3,2) = (1,2,0,2)\\
u_8 &= 2\cdot(1,0,1,1) + 1\cdot(0,1,1,2) = (2,0,2,2) + (0,1,1,2) = (2,1,3,4) = (2,1,0,1)\\
u_9 &= 2\cdot(1,0,1,1) + 2\cdot(0,1,1,2) = (2,0,2,2) + (0,2,2,1) = (2,2,4,3) = (2,2,1,0)
\end{aligned}$$

Logo,

$$\mathcal{C} = \begin{cases} (0,0,0,0), (1,0,1,1), (0,1,1,2) \\ (2,0,2,2), (0,2,2,1), (1,1,2,0) \\ (1,2,0,2), (2,1,0,1), (2,2,1,0) \end{cases}.$$

Uma representação paramétrica de C é dada por

$$a_1 v_1 + a_2 v_2$$

ao variar a_1 e a_2 em $\mathbb{F}_3$. Agora, vamos obter $\mathcal{C}$ como núcleo de uma transformação linear H. O código $\mathcal{C}$ pode ser representado como núcleo da transformação linear

$$\begin{array}{rccc} H: & \mathbb{F}_3^4 & \to & \mathbb{F}_3^2 \\ & (x_1,x_2,x_3,x_4) & \mapsto & (2x_1+2x_2+x_3, 2x_1+x_2+x_4) \end{array}$$

De fato:

$$\begin{aligned}
\ker(H) &= \{(x_1,x_2,x_2,x_4) \in \mathbb{F}_3^4;\ H(x_1,x_2,x_2,x_4) = (0,0)\}\\
&= \{(x_1,x_2,x_3,x_4) \in \mathbb{F}_3^4;\ (2x_1+2x_2+x_3, 2x_1+x_2+x_4) = (0,0)\}.
\end{aligned}$$

Assim, temos:

$$\begin{cases} 2x_1+2x_2+x_3 = 0 \\ 2x_1+x_2+x_4 = 0 \end{cases}$$

Matricialmente:

$$\begin{bmatrix} 2 & 2 & 1 & 0 & \vdots & 0 \\ 2 & 1 & 0 & 1 & \vdots & 0 \end{bmatrix} \underline{2L_1 \to L_1} \sim \begin{bmatrix} 1 & 1 & 2 & 0 & \vdots & 0 \\ 2 & 1 & 0 & 1 & \vdots & 0 \end{bmatrix} \underline{L_2 + L_1 \to L_2}$$

$$\sim \begin{bmatrix} 1 & 1 & 2 & 0 & \vdots & 0 \\ 0 & 2 & 2 & 1 & \vdots & 0 \end{bmatrix} \underline{L_1 + L_2 \to L_1} \sim \begin{bmatrix} 1 & 0 & 1 & 1 & \vdots & 0 \\ 0 & 2 & 2 & 1 & \vdots & 0 \end{bmatrix} \underline{2L_2 \to L_2}$$

$$\sim \begin{bmatrix} 1 & 0 & 1 & 1 & \vdots & 0 \\ 0 & 1 & 1 & 2 & \vdots & 0 \end{bmatrix}$$

Logo,

$$\begin{aligned} \ker(H) &= \{(x_1, x_2, x_3, x_4) \in \mathbb{F}_3^4;\ (2x_1 + 2x_2 + x_3, 2x_1 + x_2 + x_4) = (0, 0)\} \\ &= \text{ger}\{(1, 0, 1, 1), (0, 1, 1, 2)\} \\ &= \mathcal{C}, \end{aligned}$$

como queríamos.

Note que o código $\mathcal{C}$ também pode ser obtido como núcleo da transformação linear

$$\begin{array}{rccc} H': & \mathbb{F}_3^4 & \to & \mathbb{F}_3^2 \\ & (x_1, x_2, x_3, x_4) & \mapsto & (x_1 + x_3 + x_4, x_2 + x_3 + 2x_4) \end{array},$$

o que nos mostra que não há garantias quanto a unicidade da transformação linear cujo núcleo gera um determinado código linear.

Exemplo 4.7. Dada a transformação linear

$$\begin{array}{rccc} T: & \mathbb{F}_2^6 & \to & \mathbb{K}^n \\ & (x_1, x_2, x_3, x_4, x_5, x_6) & \mapsto & (x_1 + x_4, x_1 + x_2 + x_3 + x_5, x_1 + x_2 + x_6) \end{array},$$

defina $\mathcal{C}$ como sendo o núcleo de T. Determine se $(1, 0, 0, 1, 1, 1)$ e $(0, 1, 0, 1, 0, 1)$ pertencem ou não a $\mathcal{C}$.

Temos:

$$\begin{aligned} \ker(T) &= \{(x_1, x_2, x_2, x_4, x_5, x_6) \in \mathbb{F}_2^6;\ T(x_1, x_2, x_2, x_4, x_5, x_6) = (0, 0, 0)\} \\ &= \{(x_1, x_2, x_3, x_4, x_5, x_6) \in \mathbb{F}_2^6;\ (x_1 + x_4, x_1 + x_2 + x_3 + x_5, x_1 + x_2 + x_6) = (0, 0, 0)\} \end{aligned}$$

Assim, temos:

$$\begin{cases} x_1 + x_4 = 0 \\ x_1 + x_2 + x_3 + x_5 = 0 \\ x_1 + x_2 + x_6 = 0 \end{cases}$$

Matricialmente:

$$\left[\begin{array}{cccccc|c} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{array}\right] \begin{array}{l} L_2 + L_3 \to L_2 \\ L_3 + L_1 \to L_3 \end{array} \sim \left[\begin{array}{cccccc|c} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right] \underline{L_3 \leftrightarrow L_2}$$

$$\sim \left[\begin{array}{cccccc|c} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right]$$

Logo,

$$\begin{aligned} \ker(T) &= \{(x_1, x_2, x_3, x_4, x_5, x_6) \in \mathbb{F}_2^6;\ (x_1 + x_4, x_1 + x_2 + x_3 + x_5, x_1 + x_2 + x_6) = (0, 0, 0)\} \\ &= \text{ger}\{(1, 0, 0, 1, 0, 0), (0, 1, 0, 1, 0, 1), (0, 0, 1, 0, 1, 1)\} \\ &= \mathcal{C}. \end{aligned}$$

Suponha $x_1, x_2, x_3 \in \mathbb{F}_2$ tais que

$$x_1(1, 0, 0, 1, 0, 0) + x_2(0, 1, 0, 1, 0, 1) + x_3(0, 0, 1, 0, 1, 1) = (1, 0, 0, 1, 1, 1)$$

$$\Leftrightarrow\ (x_1, x_2, x_3, x_1 + x_2, x_3, x_2 + x_3) = (1, 0, 0, 1, 1, 1)$$

Assim, temos:

$$\begin{cases} x_1 = 1 \\ x_2 = 0 \\ x_3 = 0 \\ x_1 + x_2 = 1 \\ x_3 = 1 \\ x_2 + x_3 = 1 \end{cases}, \quad \text{isto é,} \quad \begin{cases} x_3 = 0 \\ x_3 = 1 \end{cases}$$

o que é um absurdo. Logo, $(1, 0, 0, 1, 1, 1)$ não pertence a $\mathcal{C}$.

Por outro lado, $(0,1,0,1,0,1)$ pertence a $\mathcal{C}$, pois

$$(0,1,0,1,0,1) = 0(1,0,0,1,0,0) + 1(0,1,0,1,0,1) + 0(0,0,1,0,1,1).$$

Definição 4.8. *Seja $\mathbb{F}_q$ um corpo finito. Dois códigos lineares $\mathcal{C}$ e $\mathcal{C}'$ são ditos* ***linearmente equivalentes*** *se existir uma isometria linear (ou seja, uma transformação linear que preserva distâncias) $T : \mathbb{K}^n \to \mathbb{K}^n$ tal que $T(\mathcal{C}) = \mathcal{C}'$.*

É possível provar que dois códigos lineares $\mathcal{C}$ e $\mathcal{C}'$ em $\mathbb{F}_q^n$ são linearmente equivalentes se, e somente se, existe uma permutação π de $\{1, 2, \ldots, n\}$ e elementos $c_1, c_2, \ldots, c_n$ de $\mathbb{F}_q \setminus \{0\}$ tais que

$$\mathcal{C}' = \{(c_1 x_{\pi(1)}, c_2 x_{\pi(2)}, \ldots, c_n x_{\pi(n)});\ (x_1, x_2, \ldots, x_n) \in C\}. \tag{4.10}$$

Daí, decorre o resultado abaixo, o qual é usualmente utilizado em textos sobre códigos como definição de códigos lineares equivalentes.

Dois códigos lineares são linearmente equivalentes se, e somente se, cada um deles pode ser obtido do outro mediante uma sequência de operações do tipo:

1. Multiplicação dos elementos numa dada posição fixa por um escalar não nulo em todas as palavras.
2. Permutação das posições de todas as palavras do código, mediante uma permutação fixa de $\{1, 2, \ldots, n\}$.

4.2 Matriz geradora de um código

Sejam $\mathbb{F}_q$ o corpo finito com q elementos e $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear. Chamaremos de ***parâmetros do código linear*** $\mathcal{C}$ a terna $[n, k, d]_q$, onde:

- n é o comprimento do código;
- k é a dimensão de $\mathcal{C}$ como subespaço vetorial sobre $\mathbb{F}_q$;
- d é a distância mínima de $\mathcal{C}$, que é também igual ao peso $\omega(\mathcal{C})$ do códio $\mathcal{C}$.

Perceba que o número de elementos de $\mathcal{C}$ é igual a $M = q^k$.

Definição 4.9. *Seja $\mathcal{B} = \{v_1, v_2, \ldots, v_k\}$ uma base ordenada de $\mathcal{C}$ e considere a matriz G, cujas linhas são os vetores $v_i = (v_{i1}, v_{i2}, \ldots, v_{ik})$, $i \in \{1, 2, \ldots, k\}$ da base, isto é,*

$$G = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix} = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{bmatrix}. \tag{4.11}$$

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

Exemplo 4.10. Considere $\mathcal{C}$ o código linear sobre $\mathbb{F}_2$ gerado pela matriz

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

Podemos perceber que comprimento do código é 7, a dimensão é 4. As palavras de $\mathcal{C}$ e seus respectivos pesos são:

- $c_0 = (0,0,0,0,0,0,0)$
  $\Rightarrow\ \omega(c_0) = 0$;
- $c_1 = (1,0,0,0,1,1,1)$
  $\Rightarrow \omega(c_1) = 3$;
- $c_2 = (0,1,0,0,1,1,0)$
  $\Rightarrow\ \omega(c_2) = 3$;
- $c_3 = (0,0,1,0,1,0,1)$
  $\Rightarrow\ \omega(c_3) = 3$;
- $c_4 = (0,0,0,1,0,1,1)$
  $\Rightarrow\ \omega(c_4) = 3$;
- $c_5 = c_1 + c_2 = (0,1,1,0,0,1,1)$
  $\Rightarrow\ \omega(c_5) = 4$;
- $c_6 = c_1 + c_3 = (0,0,1,1,1,1,0)$;
  $\Rightarrow\ \omega(c_6) = 4$;
- $c_7 = c_1 + c_4 = (1,0,0,1,1,0,0)$
  $\Rightarrow\ \omega(c_7) = 3$;
- $c_8 = c_2 + c_3 = (0,0,1,1,1,1,0)$
  $\Rightarrow\ \omega(c_8) = 4$;
- $c_9 = c_2 + c_4 = (0,1,0,1,1,0,1)$
  $\Rightarrow\ \omega(c_9) = 4$;

- $c_{10} = c_1+c_2+c_3 = (0,1,1,1,0,0,0)$
  $\Rightarrow\ \omega(c_{10}) = 3.$
- $c_{11} = c_1+c_2+c_4 = (0,1,1,1,0,0,0)$
  $\Rightarrow \omega(c_{11}) = 3;$
- $c_{12} = c_2+c_3+c_4 = (0,0,1,0,1,0,1)$
  $\Rightarrow\ \omega(c_{12}) = 3;$
- $c_{13} = c_1 + c_2 + c_3 + c_4 = (0,1,1,0,0,1,1)$
  $\Rightarrow\ \omega(c_{13}) = 4.$

Logo, a distância mínima de $\mathcal{C}$ é $d = 3$ (pois é o peso mínimo de uma palavra não nula do código). Portanto, $[7,4,3]_2$ são os parâmetros de $\mathcal{C}$.

Nesse caso, se queremos, por exemplo, codificar (1, 0, 0, 1), temos:

$$\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 1\\ 0 & 1 & 0 & 0 & 1 & 1 & 0\\ 0 & 0 & 1 & 0 & 1 & 0 & 1\\ 0 & 0 & 0 & 1 & 0 & 1 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 1 & 1 & 0 & 0\end{bmatrix}.$$

Ou seja, ao codificar a mensagem $(1,0,0,1)$ receberíamos a mensagem $(1,0,0,1,1,0,0)$.

Considere a transformação linear

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \to & \mathbb{F}_q^n \\ & x & \mapsto & xG \end{array}, \tag{4.12}$$

Se $x = (x_1, x_2, \ldots, x_k)$, então

$$T(x) \ = \ xG \ = \ x_1v_1 + x_2v_2 + \cdots + x_kv_k. \tag{4.13}$$

Logo, $T(\mathbb{K}^k) = \mathcal{C}$. Podemos, então, considerar $\mathbb{F}_q^k$ como sendo o código da fonte, $\mathcal{C}$, o código de canal e a transformação T, uma codificação.

Note que a matriz G não é univocamente determinada por $\mathcal{C}$, pois ela depende da escolha da base $\mathcal{B}$. Lembremos que, uma base de um espaço vetorial pode ser obtida de uma outra qualquer através de sequências de operações do tipo:

- Permutação de dois elementos da base;
- Multiplicação de um elemento da base por um escalar não nulo;

- Substituição de um vetor da base por ele mesmo somado com um múltiplo escalar de outro vetor da base.

Segue, então, que duas matrizes de um mesmo código $\mathcal{C}$ podem ser obtidas uma da outra por uma sequência de operações do tipo:

(L1) Permutação de duas linhas;

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

(L3) Adição de um múltiplo escalar de uma linha a outro.

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

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \to & \mathbb{F}_q^n \\ & x & \mapsto & xG \end{array},$$

Exemplo 4.11. Sejam $\mathbb{F}_2$ e

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

Considerando a transformação linear

$$\begin{array}{rccc} T: & \mathbb{F}_2^3 & \to & \mathbb{F}_2^5 \\ & x & \mapsto & xG \end{array},$$

obtemos um código $\mathcal{C}$ em $\mathbb{F}_2^5$, imagem de T. A palavra $c_1 = (1, 0, 1)$ do código da fonte, por exemplo, é codificada como $(0, 1, 0, 1, 0)$, pois

$$c_1G = \begin{bmatrix} 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1\cdot 1 + 0\cdot 1 + 1\cdot 1 \\ 1\cdot 0 + 0\cdot 1 + 1\cdot 1 \\ 1\cdot 1 + 0\cdot 0 + 1\cdot 1 \\ 1\cdot 0 + 0\cdot 1 + 1\cdot 1 \\ 1\cdot 1 + 0\cdot 0 + 1\cdot 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ 2 \\ 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Suponhamos agora que seja dada a palavra $(1,0,1,0,1)$ do código, e que gostaríamos de decodificá-la, isto é, achar a palavra $x=(x_1,x_2,x_3)$ de $\mathbb{F}_2^3$ da qual ela se origina por meio de T. Teríamos, então, que resolver o sistema:

$$(x_1,x_2,x_3)G=(1,0,1,0,1),$$

ou seja:

$$\begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}\begin{bmatrix} 1&0&1&0&1\\ 1&1&0&1&0\\ 1&1&1&1&1 \end{bmatrix}=\begin{bmatrix}1\\0\\1\\0\\1\end{bmatrix} \Leftrightarrow \begin{bmatrix} x_1+x_2+x_3\\ x_2+x_3\\ x_1+x_3\\ x_2+x_3\\ x_1+x_3 \end{bmatrix}=\begin{bmatrix}1\\0\\1\\0\\1\end{bmatrix}$$

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

$$\sim \left[\begin{array}{ccc|c} 1&1&1&1\\ 0&1&1&0\\ 1&0&1&1 \end{array}\right] \underline{\quad L_1+L_2\to L_1\quad} \sim \left[\begin{array}{ccc|c} 1&0&0&1\\ 0&1&1&0\\ 1&0&1&1 \end{array}\right] \underline{\quad L_3+L_1\to L_3\quad}$$

$$\sim \left[\begin{array}{ccc|c} 1&0&0&1\\ 0&1&1&0\\ 0&0&1&0 \end{array}\right] \underline{\quad L_2+L_3\to L_2\quad} \sim \left[\begin{array}{ccc|c} 1&0&0&1\\ 0&1&0&0\\ 0&0&1&0 \end{array}\right].$$

Logo, a solução do sistema é $x_1=1$, $x_2=0$ e $x_3=0$.

Esse sistema particular de equações não foi trabalhoso de se resolver, mas, em geral, dada uma matiz G mais complexa, a resolução do sistema de equações assocado pode ser muito trabalhosa.

Notemos que, efetuando operações sobre as linhas de G, obtemos:

$$\begin{bmatrix} 1&0&1&0&1\\ 1&1&0&1&0\\ 1&1&1&1&1 \end{bmatrix} \begin{matrix} L_2+L_1\to L_2\\ L_3+L_2\to L_3 \end{matrix} \sim \begin{bmatrix} 1&0&1&0&1\\ 0&1&1&1&1\\ 0&0&1&0&1 \end{bmatrix} \begin{matrix} L_1+L_3\to L_1\\ L_2+L_3\to L_2 \end{matrix}$$

$$\sim \; G' \; = \; \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Dessa forma

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

e, portanto, obtém-se o vetor x tomando apenas as três primeiras componentes do vetor a ser decodificado. Logo, a palavra $(1, 0, 1, 0, 1)$ é facilmente decodificada como $(1, 0, 1)$.

Definição 4.12. *Dizemos que uma matriz geradora G de um código linear $\mathcal{C}$ está na* ***forma padrão*** *quando*

$$G = [Id_k|A], \tag{4.14}$$

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

Dado um código $\mathcal{C}$, nem sempre é possível encontrar uma matriz geradora de $\mathcal{C}$ na forma padrão, conforme podemos observar no seguinte exemplo:

Exemplo 4.13. Considere sobre $\mathbb{F}_2^5$ o código $\mathcal{C}$ de matriz geradora

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

Então, por mais que operações sejam efetuadas sobre as linhas de G, nunca será possível colocar G na forma padrão.

No entanto, efetuando também permutações sobre as colunas de G, temos:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad \begin{matrix} C_1 \leftrightarrow C_3 \\ C_2 \leftrightarrow C_4 \end{matrix} \quad \sim \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

que é a matriz geradora na forma padrão de um código $\mathcal{C}'$ equivalente ao código $\mathcal{C}$.

Mais geralmente, dado um código linear $C \subset \mathbb{K}^n$ de matriz geradora G, se além de considerarmos as operações sobre as linhas de G, considerarmos as operações

(C1) Permutação de duas colunas;

(C2) Multiplicação de uma coluna por um escalar não nulo;

obtemos uma matriz G' geradora de um código $\mathcal{C}'$ que é equivalente ao código $\mathcal{C}$ inicialmente dado. Com essas operações sobre as linhas e colunas de uma matriz geradora, obtemos o seguinte resultado:

Teorema 4.14. *Dado um código linear $\mathcal{C}$, existe um código $\mathcal{C}'$ equivalente a $\mathcal{C}$ com matriz geradora na forma padrão.*

Demonstração. Seja G uma matriz geradora do código $\mathcal{C} \subset \mathbb{F}_q^n$. Suponhamos $\dim \mathcal{C} = k$ e consideremos

$$G = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}.$$

Lembremos que, as linhas de G são formadas por vetores base de $\mathcal{C}$. Em particular, as linhas de G são linearmente independentes.

Utilizando a operação (C1), podemos supor, sem perda de generalidade, que $g_{11} \neq 0$. Então, utilizando a operação (L2), obtemos:

$$G = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix} \quad \underline{\frac{1}{g_{11}} L_1 \to L_1} \quad \sim \quad \begin{bmatrix} 1 & g_{12}/g_{11} & \cdots & g_{1n}/g_{11} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}$$

Agora, utilizando a operação (L3):

$$\begin{bmatrix} 1 & g_{12}/g_{11} & \cdots & g_{1n}/g_{11} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix} \quad \begin{array}{c} L_2 + (-1)g_{21}L_1 \to L_2 \\ L_3 + (-1)g_{31}L_1 \to L_3 \\ \vdots \\ L_k + (-1)g_{k1}L_1 \to L_k \end{array} \quad \sim \quad \begin{bmatrix} 1 & b_{12} & \cdots & b_{1n} \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{k2} & \cdots & b_{kn} \end{bmatrix}$$

Agora, na segunda linha da matriz

$$\begin{bmatrix} 1 & b_{12} & \cdots & b_{1n} \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{k2} & \cdots & b_{kn} \end{bmatrix},$$

temos um elemento não nulo que, utilizando a operação (C1), pode ser colocando na segunda linha e segunda coluna da matriz acima. Dessa forma, multiplicando a segunda linha pelo inverso desse elemento, obtemos a matriz

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

Novamente, usando operações (L3), obtemos:

$$\begin{bmatrix} 1 & c_{12} & c_{13} & \cdots & c_{1n} \\ 0 & 1 & c_{23} & \cdots & c_{2n} \\ 0 & c_{32} & c_{33} & \cdots & c_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & c_{k2} & c_{k3} & \cdots & c_{kn} \end{bmatrix} \begin{array}{l} L_1 + (-1)c_{12}L_2 \to L_1 \\ L_3 + (-1)c_{32}L_2 \to L_3 \\ L_4 + (-1)c_{42}L_2 \to L_4 \\ \vdots \\ L_k + (-1)c_{k2}L_2 \to L_k \end{array} \sim \begin{bmatrix} 1 & 0 & d_{13} & \cdots & d_{1n} \\ 0 & 1 & d_{23} & \cdots & d_{2n} \\ 0 & 0 & d_{33} & \cdots & d_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & d_{k3} & \cdots & d_{kn} \end{bmatrix}.$$

Logo, procedendo analogamente, obtemos uma matriz na forma padrão

$$G' = [Id_k|A].$$

■

Exemplo 4.15. Dado o código $\mathcal{C}$ definido sobre $\mathbb{F}_2$ pela matriz geradora

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

vamos determinar um código $\mathcal{C}'$ equivalente a $\mathcal{C}$, com matiz geradora na forma padrão.

Temos:

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{matrix} \\ L_2 + L_1 \to L_2 \\ L_3 + L_1 \to L_3 \\ \\ \end{matrix} \sim \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{matrix} \\ \\ C_2 \leftrightarrow C_5 \\ C_3 \leftrightarrow C_7 \\ \end{matrix}$$

$$\sim \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \underline{L_2 + L_4 \to L_2} \sim \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Logo, o código $\mathcal{C}'$ definido sobre $\mathbb{F}_2$ pela matriz geradora

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

é equivalente a $\mathcal{C}$, com matriz geradora G' na forma padrão.

4.3 Matriz teste de paridade

Aqui, veremos uma outra maneira de definir um código linear, agora como a solução de um sistema linear de equações.

Definição 4.16. *Uma* ***matriz teste de paridade*** *para um código linear $\mathcal{C} \subset \mathbb{F}_q^n$ é uma matriz H $m \times n$ com entradas em $\mathbb{F}_q$ tal que*

$$\mathcal{C} = \{u \in \mathbb{F}_q^n;\ uH^t = 0\}, \tag{4.15}$$

onde H^t é a transposta da matriz H.

Proposição 4.17. *Seja $\mathcal{C}$ um código linear com matriz teste de paridade H. Se todo conjunto com $d-1$ colunas de H é linearmente independente e existem d colunas linearmente dependentes, então a distância mínima de $\mathcal{C}$ é d.*

Demonstração. Seja u uma palavra do código $\mathcal{C}$. Seja D o conjunto das coordenadas não nulas de u. Então, $|D| = \omega(u)$. Seja h_i a i-ésima coluna de H. Como H é uma matriz teste de paridade para $\mathcal{C}$, temos:

$$uH^t = 0 \ \Rightarrow \ \sum_{i \in D} u_i h_i = 0.$$

Assim, existe uma combinação linear de $|D|$ colunas de H que são linearmente dependentes. Logo, pela Proposição 4.5, existe uma combinação linear de $|D| = d$ colunas de H que são linearmente dependentes. ■

Exemplo 4.18. Seja $\mathbb{F}_2$ o alfabeto.

Consideremos o código $\mathcal{C}$ do Exemplo 4.10, gerado pela matriz

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

O conjunto

$$\mathcal{B} = \{1000111, 0100110, 0010101, 0001011\}$$

é uma base de C. Ou seja, dado $v \in C$, v é escrito de forma única como

$$v = (x_1, x_2, x_3, x_4, x_1 + x_2 + x_3, x_1 + x_2 + x_4, x_1 + x_3 + x_4),$$

onde $x_i \in \mathbb{F}_2$, $i \in \{1, 2, 3, 4\}$.

A matriz

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

é a matriz teste de paridade para o código $\mathcal{C}$.

De fato, seja $u \in \mathbb{F}_2^7$. Temos:

$$uH^t = 0 \;\Leftrightarrow\; \begin{bmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & u_7 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$$

$$\Leftrightarrow \quad \begin{bmatrix} u_1 + u_2 + u_3 + u_5 & u_1 + u_2 + u_4 + u_6 & u_1 + u_3 + u_4 + u_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$$

$$\Leftrightarrow \quad \begin{cases} u_1 + u_2 + u_3 + u_5 = 0 \\ u_1 + u_2 + u_4 + u_6 = 0 \\ u_1 + u_3 + u_4 + u_7 = 0 \end{cases} \quad \Leftrightarrow \quad \begin{cases} u_1 = u_1 \\ u_2 = u_2 \\ u_3 = u_3 \\ u_4 = u_4 \\ u_5 = u_1 + u_2 + u_3 \\ u_6 = u_1 + u_2 + u_4 \\ u_7 = u_1 + u_3 + u_4 \end{cases}$$

Ou seja, $u = (u_1, u_2, u_3, u_4, u_1 + u_2 + u_3, u_1 + u_2 + u_4, u_1 + u_3 + u_4)$. Portanto, $\mathcal{C} = \{u \in \mathbb{F}_2^7;\ uH^t = 0\}$, isto é, H é a matriz teste de paridade para $\mathcal{C}$.

Olhando para a matriz H, vemos que toda dupla de colunas é LI e que há um conjunto de exatamente 3 colunas LDs (por exemplo, a primeira coluna é a soma da segunda coluna e da sétima coluna). Logo, de fato, pela Proposição 4.17 a distância mínima é 3.

Proposição 4.19. *Seja G uma matriz geradora de um código linear $\mathcal{C}$ de dimensão k. Uma matriz $m \times n$ H é uma matriz teste de paridade para $\mathcal{C}$ se, e somente se, $GH^t = 0$ e o posto de H é $n - k$.*

Demonstração. Tome H uma matriz $m \times n$ que seja uma matriz teste de paridade para $\mathcal{C}$. Sendo G uma matriz teste de paridade para $\mathcal{C}$, todas as linhas de G são

palavras do código $\mathcal{C}$. Então, se u é uma linha de G, $uH^t = 0$, donde $GH^t = 0$. Logo, a dimensão k do código $\mathcal{C}$ é $n - \text{posto}(H)$, ou seja, o posto de H é $n - k$.

Reciprocamente, suponhamos que $GH^t = 0$ e que o posto de H é $n - k$. Sendo G uma matriz geradora, uma palavra do $u \in \mathcal{C}$ se escreve como uma combinação linear das linhas de G, donde $uH^t = 0$. Como o posto de H é $n - k$, a dimensão do núcleo (à esquerda) é k, que é a dimensão de $\mathcal{C}$, logo $\mathcal{C}$ é todo o núcleo. ■

Corolário 4.20 (Cota de Singleton)**.** *Os parâmetros $[n, k, d]_q$ de um código linear satisfazem a desigualdade*

$$d \leq n - k + 1. \tag{4.16}$$

Demonstração. Seja H é uma matriz teste de paridade do código $\mathcal{C}$. Então, pela Proposição 4.19, a matriz H tem posto $n - k$. Pela Proposição 4.17, se a distância mínima de $\mathcal{C}$ é d, então quaisquer $d - 1$ colunas de H devem ser linearmente independentes e devem existir d colunas de H linearmente dependentes. Ademais, como posto$(H) = n - k$, existe pelo menos um grupo de $n - k$ colunas de H linearmente independentes e qualquer quantidade maior de colunas é linearmente dependente. Logo, podemos ter $d - 1 = n - k$, se quaisquer $n - k$ colunas de H forem linearmente independentes, ou $d - 1 < n - k$ se existir um grupo de $n - k$ colunas de H linearmente dependentes. Por conseguinte, temos que $d - 1 \leq n - k$, isto é, $d \leq n - k + 1$, como queríamos. ■

Proposição 4.21. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código de dimensão k com matriz geradora $G = [Id_k|A]$ na forma padrão. Então, $H = [-A^t|Id_{n-k}]$ é uma matriz teste de paridade para $\mathcal{C}$.*

Demonstração. Provar que $H = [-A^t|Id_{n-k}]$ é uma matriz teste de paridade para $\mathcal{C}$ é provar que e o produto interno da $i-$ésima linha de $G = (g_{ij})$ com a $\ell-$linha de $H = (h_{\ell j})$ é 0. Para $j \leq k$, temos $g_{ij} = 0$, a menos que $i = j$ ($g_{ij} = 0$). Para $j \geq k + 1$, temos $h_{\ell j} = 0$, a menos que $\ell = j - k$ ($h_{\ell \ell+k} = 1$). Portanto:

$$\sum_{j=1}^{n} g_{ij}h_{\ell j} = \sum_{j=1}^{k} g_{ij}h_{\ell j} + \sum_{j=k+1}^{n} g_{ij}h_{\ell j} = h_{\ell i} + g_{i,\ell+k} = -a_{i\ell} + a_{i\ell} = 0.$$

■

Exemplo 4.22. Considere o código linear $\mathcal{C}$ sobre $\mathbb{F}_5$ gerado pela matriz

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 2 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 2 & 1 & 1 \end{bmatrix}.$$

Perceba que G está na forma padrão, $n = 6$ e $k = 3$. Além disso,

$$A = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} \Rightarrow -A^t = \begin{bmatrix} -1 & -1 & -2 \\ -1 & -2 & -1 \\ -2 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 4 & 4 & 3 \\ 4 & 3 & 4 \\ 3 & 4 & 4 \end{bmatrix}$$

Logo, pela Proposição 4.21,

$$H = [-A^t | Id_{n-k}] = \begin{bmatrix} 4 & 4 & 3 & 1 & 0 & 0 \\ 4 & 3 & 4 & 0 & 1 & 0 \\ 3 & 4 & 4 & 0 & 0 & 1 \end{bmatrix}$$

é uma matriz teste de paridade para $\mathcal{C}$.

4.4 Decodificação por síndrome

Dada uma matriz geradora G de um código linear $\mathcal{C}$, e dado $v \in \mathcal{C}$, podemos codificar este vetor da seguinte forma:

$$v \mapsto vG. \tag{4.17}$$

Além disso, se a matriz geradora está na forma padrão $G = [Id_k|A]$, podemos codificar anexando as $n - k$ coordenadas de vA a v.

Agora, para fazer o caminho inverso, isto é, para decodificar uma mensagem, precisamos de um trabalho é um pouco mais árduo. Para decodificar escolhendo o vetor mais próximo no código, devemos encontrar uma palavra do código de comprimento n que está mais próxima a n-upla recebida. Para um código sem estrutura óbvia, isso só pode ser feito calculando a distância entre cada palavra do código e a n-upla recebida, o que pode ser bem trabalhoso.

Vamos ver então um algoritmo de decodificação que explora a linearidade dos códigos lineares.

Definição 4.23. *Seja $\mathcal{C}$ um código linear com matriz teste de paridade H. Dado um vetor $v \in \mathbb{F}_q^n$, definimos a* ***síndrome*** *de v como sendo o vetor $s(v) = vH^t$.*

Quando uma mensagem c é transmitida e um vetor v é recebido, a diferença entre os dois vetores é chamada ***erro*** e denotada por e. Dessa forma:

$$v = c + e. \tag{4.18}$$

Se H é uma matriz teste de paridade para o código linear $\mathcal{C}$, então, como $C = \{v \in \mathbb{F}_q^n;\ vH^t = 0\}$, temos:

$$\begin{aligned} s(v) &= vH^t \overset{v=c+e}{=} (c+e)H^t \\ &= cH^t + eH^t \\ &= 0 + eH^t, \quad \text{pois } c \in C \\ &= eH^t \\ &= s(e), \end{aligned}$$

ou seja, a síndrome de v é a mesma do vetor erro. Ademais,

$$s(v) = 0 \ \Leftrightarrow\ vH^t = 0 \ \Leftrightarrow\ v \in \mathcal{C}. \tag{4.19}$$

Exemplo 4.24. Considere o código linear do Exemplo 4.22, vimos que

$$H = \begin{bmatrix} 4 & 4 & 3 & 1 & 0 & 0 \\ 4 & 3 & 4 & 0 & 1 & 0 \\ 3 & 4 & 4 & 0 & 0 & 1 \end{bmatrix}$$

é uma matriz teste de paridade para $\mathcal{C}$. Sejam $u = (1,0,0,1,1,2)$ e $v = (1,0,0,1,1,0)$ vetores de $\mathbb{F}_5^6$. Então:

$$uH^t = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 4 & 4 & 3 \\ 4 & 3 & 4 \\ 3 & 4 & 4 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 5 & 5 & 5 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$$

$$vH^t = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 4 & 4 & 3 \\ 4 & 3 & 4 \\ 3 & 4 & 4 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 5 & 5 & 3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 3 \end{bmatrix}$$

Logo, pela expressão (4.19), segue que $u \in \mathcal{C}$ e $v \notin \mathcal{C}$.

Se $\omega(e) \leq 1$, então a síndrome $s(v) = s(e) = eH^t$ é só um múltiplo escalar de uma coluna de H.

Isso nos dá um algoritmo de decodificação simples para códigos lineares que corrijam 1 erro. Primeiro, calculamos a síndrome de v. Assim, temos dois casos:

- $s(v) = 0$.

  Neste caso, $v \in \mathcal{C}$, e então não houve erro na transmissão.

- $s(v) \neq 0$.

  Neste caso, procure a coluna de H que é um múltiplo escalar de $s(v)$. Se essa coluna não existir, então houve mais de um erro e o código não será capaz de corrigir. Agora, se $s(v) = \lambda \cdot$ coluna j, para algum $\lambda \in \mathbb{N}$, então, para corrigir o erro, basta somar a v o vetor com $-\lambda$ na j-ésima posição e 0 nas demais posições para corrigir o erro.

Exemplo 4.25. Seja $\mathcal{C}$ o código $[5, 3, d]_3$ de matriz de teste de paridade

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Seja $c = (1, 0, 1, 2, 0)$. Então

$$cH^t = \begin{bmatrix} 1 & 0 & 1 & 2 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 0 & 3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}.$$

Então, $c \in \mathcal{C}$. Suponhamos que, em vez de c, recebemos $v = (1, 0, 1, 1, 0)$. Calculando a síndrome de v:

$$s(v) = vH^t = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 2 \end{bmatrix}.$$

Com isso, $s(v) = (2, 0, 2) = 2(1, 0, 1)$, que é um múltiplo da quarta coluna da matriz H. Logo, para corrigirmos o erro, usando a decodificação por síndrome, fazemos:

$$v + (0, 0, 0, -2.0,) = (1, 0, 1, -1, 0) = (1, 0, 1, 2, 0).$$

Exemplo 4.26. Seja $\mathcal{C}$ o código $[6, 3, d]_5$ com matriz teste de paridade

$$H = \begin{bmatrix} 4 & 4 & 3 & 1 & 0 & 0 \\ 4 & 3 & 4 & 0 & 1 & 0 \\ 3 & 4 & 4 & 0 & 0 & 1 \end{bmatrix}$$

Suponhamos que recebemos $v = (0, 2, 3, 4, 3, 2)$. Vamos decodificar v usando síndrome. Temos:

$$s(v) = vH^t = \begin{bmatrix} 0 & 2 & 3 & 4 & 3 & 2 \end{bmatrix} \begin{bmatrix} 4 & 4 & 3 \\ 4 & 3 & 4 \\ 3 & 4 & 4 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 21 & 21 & 22 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 2 \end{bmatrix}$$

Com isso, $s(v) = (1, 1, 2) = (16, 16, 12) = 4(4, 4, 3)$, que é um múltiplo da primeira coluna da matriz H. Logo, para corrigir o erro fazemos:

$$v + (-4, 0, 0, 0, 0, 0) = (-4, 2, 3, 4, 3, 2) = (1, 2, 3, 4, 3, 2).$$

Exemplo 4.27. A matriz

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

gera um código $[8, 4, 4]_3$. Assim, como G está na forma padrão, pela Proposição 4.21, a matriz

$$H = \begin{bmatrix} 0 & -1 & -1 & -1 & 1 & 0 & 0 & 0 \\ -1 & 0 & -1 & -1 & 0 & 1 & 0 & 0 \\ -1 & -1 & 0 & -1 & 0 & 0 & 1 & 0 \\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 2 & 2 & 1 & 0 & 0 & 0 \\ 2 & 0 & 2 & 2 & 0 & 1 & 0 & 0 \\ 2 & 2 & 0 & 2 & 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

é uma matriz teste de paridade para $\mathcal{C}$. Suponhamos que uma palavra $u \in \mathcal{C}$ tenha sido enviada e o vetor $v = (1, 0, 1, 0, 0, 1, 0, 2)$ tenha sido recebido. Para decodificarmos essa mensagem usando síndrome, calculamos

$$s(v) = vH^t = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 0 & 2 & 2 & 2 \\ 2 & 0 & 2 & 2 \\ 2 & 2 & 0 & 2 \\ 2 & 2 & 2 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 5 & 2 & 6 \end{bmatrix} = \begin{bmatrix} 2 & 2 & 2 & 0 \end{bmatrix}$$

que é a quarta coluna de H. Assim, para corrigir o erro, tomamos $e = (0, 0, 0, 1, 0, 0, 0, 0)$ e, assim, a palavra correta é

$$v - e = (1, 0, 1, -1, 0, 1, 0, 2) = (1, 0, 1, 2, 0, 1, 0, 2) = (1, 0, 1, 2)G.$$

O processo visto nos exemplos anteriores é bem útil quando temos apenas 1 erro na mensagem transmitida. Todavia, quando tivermos mais de 1 erro, esse processo não irá funcionar. Dessa forma, buscaremos agora modificar esse processo para podermos utilizar a decodificação por síndrome em mais casos.

Definição 4.28. *Seja $\mathcal{C}$ um código linear. Diremos que dois vetores x e y são* ***equivalentes*** *com respeito a $\mathcal{C}$ se, e somente se, $x - y \in \mathcal{C}$.*

A relação

$$x \sim y \;\Leftrightarrow\; x - y \in \mathcal{C}.$$

é uma relação de equivalência. De fato, temos:

- $\sim$ é reflexiva.

  Como $\mathcal{C}$ é um subespaço vetorial, $x - x = 0$ pertence a $\mathcal{C}$. Logo, $x \sim x$.

- $\sim$ é simétrica.

  Suponha $x \sim y$. Então, $x - y \in \mathcal{C}$. Daí, como $\mathcal{C}$ é subespaço, $-(x - y) \in \mathcal{C}$, isto é, $y - x \in C$. Logo, $x \sim y$.

- $\sim$ é transitiva.

  Sejam $x \sim y$ e $y \sim z$. Então, $x - y \in \mathcal{C}$ e $y - z \in \mathcal{C}$. Como $\mathcal{C}$ é linear, segue que $x - z = (x - y) + (y - z) \in \mathcal{C}$. Logo, $x \sim z$.

As classes de equivalência dessa relação serão chamadas de cosets de $\mathcal{C}$, como veremos na definição abaixo.

Definição 4.29. *Sejam $\mathcal{C}$ um código linear e x um vetor de $\mathcal{C}$. Definimos o* ***coset*** *de x como sendo o conjunto*

$$\overline{x} = \{y \in \mathcal{C};\ x - y \in \mathcal{C}\}.$$

Dessa forma, um coset é o conjunto de todos os vetores com a mesma síndrome. Simbolicamente:

$$\overline{x} = \{y \in \mathcal{C};\ s(y) = s(v)\}. \tag{4.20}$$

Com efeito, suponha $y \in \overline{x}$, isto é, $x - y \in \mathcal{C}$. Tome $c = x - y$. Então, $x = c + y$. Temos:

$$s(x) = xH^t = (c + y)H^t = cH^t + yH^t,$$

e como $c \in \mathcal{C}$, temos $cH^t = 0$. Logo, $s(x) = yH^t = s(y)$. Por outro lado, suponha $s(x) = s(y)$, ou seja, $xH^t = yH^t$. Então, $(x - y)H^t = 0$ e, consequentemente, $x - y \in \mathcal{C}$. Logo, $y \in \overline{x}$. Portanto, $\overline{x} = \{y \in \mathcal{C};\ s(y) = s(v)\}$.

Exemplo 4.30. Seja $\mathcal{C}$ o código linear $[5, 2, d]_2$ gerado pela matriz

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

Como G está na forma padrão, pela Proposição 4.21, a matriz teste de paridade de $\mathcal{C}$ é

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

Como $00000, 10101, 01110 \in \mathcal{C}$ segue que $s(00000) = s(10101) = s(01110) = 0000$. Além disso, $10101 + 01110 = 11211 = 11011 \in \mathcal{C}$ e, consequentemente, $s(11011) = 000$.

Considere o vetor 00001. Temos:

$$\begin{aligned} 10101 - 00001 &= 10100 \\ 01110 - 00001 &= 01111 \\ 11011 - 00001 &= 11010. \end{aligned}$$

Ademais:

$$s(00001) = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} = 001.$$

Logo, $s(00001) = s(10100) = s(01111) = s(11010) = 001$. Procedendo analogamente:

- 00010:

  10101 - 00010 = 10111;

  01110 - 00010 = 01100;

  11011 - 00010 = 11001.

- 00100:

  10101 - 00100 = 10001;

  01110 - 00100 = 01010;

  11011 - 00100 = 11111.

- 01000:

  10101 - 01000 = 11101;

  01110 - 01000 = 00110;

  11011 - 01000 = 10011.

- 10000:

  10101 - 10000 = 00101;

  01110 - 10000 = 11110;

  11011 - 10000 = 01011.

- 11000:

  10101 - 11000 = 01101;

  01110 - 11000 = 10110;

  11011 - 11000 = 00011.

- 10010:

  10101 - 10010 = 00111;

  01110 - 10010 = 11100;

  11011 - 10010 = 01001.

A seguir, podemos ver os cosets com as síndromes:

Cosets				Síndrome
00000	10101	01110	11011	000
00001	10100	01111	11010	001
00100	10001	01010	11111	100
01000	11101	00110	10011	110
10000	00101	11110	01011	101
11000	01101	10110	00011	011
10010	00111	11100	01001	111

Tabela 1 – Tabela de cosets e síndromes dos vetores de $\mathcal{C}$.

Em cada coset, o vetor escrito na primeira coluna tem peso mínimo entre os vetores daquele coset. Tal vetor é chamado o ***líder*** (quando há mais de um vetor com o mesmo peso, escolhemos arbitrariamente).

Na proposição a seguir veremos em quais hipóteses há garantias da unicidade do coset.

Proposição 4.31. *Seja $\mathcal{C}$ um código linear com distância mínima d. Se x é um vetor de peso $\omega(x) \leq \left[\frac{d-1}{2}\right]$, então x é o único elemento de seu coset com peso mínimo e, então, é o líder do coset.*

Demonstração. Suponhamos, por contradição, que y seja um elemento do coset de x tal que $\omega(y) = \omega(x)$. Então:

$$\omega(x-y) \leq \omega(x) + \omega(y) = 2\omega(x) \leq 2\left[\frac{d-1}{2}\right] \leq d-1,$$

o que é uma contradição com a distância mínima d de C, a menos que $x - y = 0$. Logo, $x = y$. ■

Exemplo 4.32. Consideremos $\mathcal{C}$ o código linear do Exemplo 4.30. Observando a matriz geradora de $\mathcal{C}$, vemos que as palavras de $\mathcal{C}$ e seus respectivos pesos são:

- $c_0 = 00000 \ \Rightarrow \ \omega(c_0) = 0$;
- $c_1 = 10101 \ \Rightarrow \ \omega(c_1) = 3$;
- $c_2 = 01110 \ \Rightarrow \omega(c_2) = 3$;
- $c_3 = c_1 + c_2 = 11211 = 11011 \ \Rightarrow \ \omega(c_3) = 4$.

Logo, o peso mínimo de $\mathcal{C}$ é $\omega(\mathcal{C}) = 3$ e, pela Proposição 4.5, segue que a $d = \omega(\mathcal{C}) = 3$ é distância mínima de $\mathcal{C}$. Logo, pela Proposição 4.31, as palavras com peso menor ou igual a 1 são líderes de seus cosets. Observando a Tabela 1, vemos que isso ocorre em suas 6 primeiras linhas.

Em suma:

Quando um vetor v é recebido em uma transmissão, procuramos o coset em que ele está (calculando a síndrome) e então subtraímos de v o líder do coset.

Exemplo 4.33. Voltemos ao código do Exemplo 4.30. Suponhamos recebida a mensagem $u = 11101$. A síndrome de u é $s(u) = 111$ e, pela Tabela 1, o líder do coset de u é $\ell = 01000$ (apenas um erro). Assim, corrigimos u por

$$u - \ell = 11101 - 01000 = 10101.$$

Agora, se a mensagem recebida for $v = 11100$, vemos que v tem síndrome $s(v) = 111$ e, novamente pela Tabela 1, o líder de seu coset é $\ell = 10010$. Vimos no Exemplo 4.32 que esse código tem distância mínima $d = 3$. Então, pelo Teorema 3.12, $\mathcal{C}$ tem a capacidade de corrigir até

$$\kappa = \left[\frac{d-1}{2}\right] = 1$$

erro. Assim, nesse caso, estaremos corrigindo 2 erros, mas não temos garantia de que essa correção estará correta. De fato, o líder do coset foi escolhido como 100010 mas poderia ter sido 01001. Todavia, como ambos estão a uma mesma distância de v, então não teríamos como ter certeza de qual era a correta.

5 CÓDIGOS CÍCLICOS

Definição 5.1. *Dizemos que um $[n, k, d]_q$ código linear $\mathcal{C}$ é* ***cíclico*** *se para todo $(c_1, c_2, \ldots, c_n) \in \mathcal{C}$, o vetor $(c_n, c_1, \ldots, c_{n-1})$ também está em $\mathcal{C}$.*

O vetor $(c_n, c_1, \ldots, c_{n-1})$ é chamado vetor ***shift*** de $(c_1, c_2, \ldots, c_n)$. Quando fizermos shifts de palavras, denotaremos por $\mapsto$. Por exemplo, se $u = (0, 2, 3)$,

$$u \ \mapsto \ (3, 0, 2)$$

nos diz que, $(3, 0, 2)$ é o shift de u.

Exemplo 5.2. Considere o código linear sobre $\mathbb{F}_2$ dado pela matriz geradora

$$G = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix},$$

Então,

$$\mathcal{C} = \{(0,0,0), (1,1,0), (0,1,1), (1,0,1)\}.$$

Esse é um código cíclico. De fato:

$$\begin{aligned} C_0 = (0,0,0) &\ \mapsto \ (0,0,0) \ \mapsto \ C_0; \\ C_1 = (1,1,0) &\ \mapsto \ (0,1,1) \ \mapsto \ C_2; \\ C_2 = (0,1,1) &\ \mapsto \ (1,0,1) \ \mapsto \ C_3; \\ C_3 = (1,0,1) &\ \mapsto \ (1,1,0) \ \mapsto \ C_1. \end{aligned}$$

Exemplo 5.3. Considere o $[7, 3, d]_2$ código linear gerado pela matriz

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

Se C_1, C_2, C_3 são as linhas de G, então, as palavras não nulas de C são:

$$\begin{aligned} C_0 &= (0,0,0,0,0,0,0); \\ C_1 &= (1,0,1,1,1,0,0); \end{aligned}$$

$$C_2 = (0,1,0,1,1,1,0);$$
$$C_3 = (0,0,1,0,1,1,1);$$
$$C_4 = C_1 + C_2 = (1,1,1,2,2,1,0) = (1,1,1,0,0,1,0);$$
$$C_5 = C_1 + C_3 = (1,0,2,1,2,1,1) = (1,0,0,1,0,1,1);$$
$$C_6 = C_2 + C_3 = (0,1,1,1,2,2,1) = (0,1,1,1,0,0,1);$$
$$C_7 = C_1 + C_2 + C_3 = (1,1,2,2,3,2,1) = (1,1,0,0,1,0,1).$$

Esse é um código cíclico, pois, temos:

$$\begin{aligned}
C_0 &\mapsto (0,0,0,0,0,0,0) \mapsto C_0;\\
C_1 &\mapsto (0,1,0,1,1,1,0) \mapsto C_2;\\
C_2 &\mapsto (0,0,1,0,1,1,1) \mapsto C_3;\\
C_3 &\mapsto (1,0,0,1,0,1,1) \mapsto C_5;\\
C_4 &\mapsto (0,1,1,1,0,0,1) \mapsto C_6;\\
C_5 &\mapsto (1,1,0,0,1,0,1) \mapsto C_7;\\
C_6 &\mapsto (1,0,1,1,1,0,0) \mapsto C_1;\\
C_7 &\mapsto (1,1,1,0,0,1,0) \mapsto C_4.
\end{aligned}$$

Exemplo 5.4. Considere o $[4,2,d]_3$ código linear $\mathcal{C}$ gerado pela matriz.

$$G = \begin{bmatrix} 1 & 0 & 2 & 0 \\ 1 & 1 & 2 & 2 \end{bmatrix}.$$

Se C_1 e C_2 são as linhas de G, então, as 9 palavras de $\mathcal{C}$ são:

$$\begin{aligned}
C_0 &= (0,0,0,0) \\
C_1 &= (1,0,2,0) \\
C_2 &= (1,1,2,2) \\
2C_1 &= (2,0,4,0) = (2,0,1,0) \\
2C_2 &= (2,2,4,4) = (2,2,1,1) \\
C_1+C_2 &= (2,1,4,2) = (2,1,1,2) \\
C_1+2C_2 &= (3,2,3,1) = (0,2,0,1) \\
2C_1+C_2 &= (3,1,3,2) = (0,1,0,2) \\
2C_1+2C_2 &= (4,2,2,1) = (1,2,2,1)
\end{aligned}$$

Calculando os shifts:

$$\begin{aligned}
C_0 &\mapsto (0,0,0,0) \mapsto C_0 \\
C_1 &\mapsto (0,1,0,2) \mapsto 2C_1+C_2 \\
C_2 &\mapsto (2,1,1,2) \mapsto C_1+C_2 \\
2C_1 &\mapsto (0,2,0,1) \mapsto C_1+2C_2 \\
2C_2 &\mapsto (1,2,2,1) \mapsto 2C_1+2C_2 \\
C_1+C_2 &\mapsto (2,2,1,1) \mapsto 2C_2 \\
C_1+2C_2 &\mapsto (1,0,2,0) \mapsto C_1 \\
2C_1+C_2 &\mapsto (2,0,1,0) \mapsto 2C_1 \\
2C_1+2C_2 &\mapsto (1,1,2,2) \mapsto C_2
\end{aligned}$$

Logo, para todo vetor no código temos que seus shifts também pertencem ao código. Portanto, $\mathcal{C}$ e um código cíclico.

Agora, vamos enxergar os códigos cíclicos através de polinômios com coeficientes em $\mathbb{F}_q$.

Definição 5.5. *Seja $a = (a_0, a_1, \ldots, a_{n-1})$ uma palavra de um $[n,k,d]_q$ código linear $\mathcal{C}$. Definimos o* ***polinômio associado*** *a $a \in \mathcal{C}$ como*

$$a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x]. \tag{5.1}$$

Exemplo 5.6. Sendo $\mathcal{C}$ o código do Exemplo 5.4, consideremos $2C_1 = C_3$, $2C_2 = C_4$, $C_1 + C_2 = C_5$, $C_1 + 2C_2 = C_6$, $2C_1 + C_2 = C_7$ e $2C_1 + 2C_2 = C_8$. Assim, para cada palavra do código, determinemos o polinômio associado:

$$\begin{aligned}
C_0 = (0,0,0,0) &\longleftrightarrow C_0(x) = 0;\\
C_1 = (1,0,2,0) &\longleftrightarrow C_1(x) = 1 + 2x^2;\\
C_2 = (1,1,2,2) &\longleftrightarrow C_2(x) = 1 + x + 2x^2 + 2x^3;\\
C_3 = (2,0,1,0) &\longleftrightarrow C_3(x) = 2 + x^2;\\
C_4 = (2,2,1,1) &\longleftrightarrow C_4(x) = 2 + 2x + x^2 + x^3;\\
C_5 = (2,1,1,2) &\longleftrightarrow C_5(x) = 2 + x + x^2 + 2x^3;\\
C_6 = (0,2,0,1) &\longleftrightarrow C_6(x) = 2x + x^3;\\
C_7 = (0,1,0,2) &\longleftrightarrow C_7(x) = x + 2x^3;\\
C_8 = (1,2,2,1) &\longleftrightarrow C_8(x) = 1 + 2x + 2x^2 + x^3.
\end{aligned}$$

Teorema 5.7. *Fixe um inteiro $n > 1$. Seja $g(x) \in \mathbb{F}_q[x]$ um divisor de $x^n - 1$ de grau $n - k$ para algum $0 \leq k \leq n$. Seja*

$$\mathcal{P}_g\{g(x)\alpha(x) \pmod{x^n - 1};\ \alpha(x) \in \mathbb{F}_q[x],\ \deg(\alpha(x)) < k\}. \tag{5.2}$$

Todo polinômio $f(x) \in \mathcal{P}_g$ pode ser escrito como

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x]. \tag{5.3}$$

O conjunto dos distintos vetores $(a_0, a_1, \ldots, a_{n-1})$ obtidos de $f(x) \in \mathcal{P}_g$ formam um $[n, k, d]_q$ código cíclico.

Demonstração. Seja $\mathcal{C}$ o código gerado. Primeiramente, toda palavra de C está associada a um polinômio $g(x)\alpha(x)$, onde

$$\alpha(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} \in \mathbb{F}_q[x]$$

é tal que $\deg(\alpha(x)) < k$.

Sejam $u_1, u_2 \in \mathcal{C}$ que estão associadas ao polinômios $g(x)\alpha_1(x)$ e $g(x)\alpha_2(x)$, com $\deg(\alpha_1(x)), \deg(\alpha_2(x)) < k$. Então:

$$u_1 + u_2 \ \leftrightarrow\ g(x)\alpha_1(x) + g(x)\alpha_2(x) = g(x)[\alpha_1(x) + \alpha_2(x)].$$

Como a soma de polinômios de grau menor que k é um polinômio de grau menor que k, segue que $u_1 + u_2 \in \mathcal{C}$. Assim, a soma de palavras é ainda uma palavra do código.

Vamos provar que $\mathcal{C}$ é um código cíclico. Seja $u = (a_0, a_1, \ldots, a_{n-1})$ uma palavra de $\mathcal{C}$ e

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathcal{P}_g.$$

seu polinômio associado. Então:

$$\begin{aligned} xf(x) &= x(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) \\ &= a_0 x + a_1 x^2 + \cdots + a_{n-1}x^n \\ &= a_0 x + a_1 x^2 + \cdots + a_{n-1}x^n + a_{n-1} - a_{n-1} \\ &= a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1}(x^n - 1) \\ &= h(x) + a_{n-1}(x^n - 1), \end{aligned}$$

onde $h(x) = a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1}$. Ou seja, $h(x)$ é o polinômio associado a palavra $v = (a_{n-1}, a_0, a_1, \ldots, a_{n-2})$, que é o shift de u. Como $xf(x)$ e $x^n - 1$ são divisíveis por $g(x)$, segue que $h(x)$ também é divisível por $g(x)$. Logo, $h(x) \in \mathcal{P}_g$ e $\mathcal{C}$ é cíclico. ■

Na proposição a seguir provaremos que todo código cíclico pode ser obtido como no Teorema 5.7 a partir de um polinômio $g(x)$ que divide $x^n - 1$.

Teorema 5.8. *Seja $\mathcal{C}$ um código cíclico. Então, existe um único polinômio mônico $g(x)$ de grau mínimo em $\mathcal{C}$ de forma que $g(x)$ divide $x^n - 1$ e o código $\mathcal{C}$ pode ser gerado usando $g(x)$ como no Teorema 5.7.*

Demonstração. Suponhamos, por contradição, que existam dois polinômios distintos $g_1(x)$ e $g_2(x)$ de grau mínimo em C. Então, $g_1(x) - g_2(x)$ tem grau menor ainda, o que contradiz a minimalidade dos graus de $g_1(x)$ e $g_2(x)$.

Seja $g(x)$ um polinômio mônico de grau mínimo em $\mathcal{C}$. Suponhamos, por contradição, que $g(x)$ não divide $x^n - 1$. Assim, existem $q(x), r(x) \in \mathbb{F}_q[x]$ tais que

$$x^n - 1 = g(x)q(x) + r(x), \quad \deg(r(x)) < \deg(g(x))$$

Logo, $r(x)$ também seria um polinômio do código $\mathcal{C}$ tal que seu grau é menor que o mínimo, o que nos dá uma contradição.

Portanto, existe um único polinômio mônico $g(x)$ de grau mínimo em $\mathcal{C}$ de forma que $g(x)$ divide $x^n - 1$ e $g(x)$ está nas condições do Teorema 5.7. ■

Exemplo 5.9. Sejam $n = 3$ e $q = 2$. Perceba que, $g(x) = x - 1$ divide $x^3 - 1$. Podemos escrever

$$g(x) = x - 1 = x + 1 \in \mathbb{F}_2[x].$$

Vamos entender o conjunto $\mathcal{P}_g$, definido na expressão (5.2). Para isso, vamos listar todos os possíveis $g(x)\alpha(x) \pmod{x^3 - 1}$, com $\deg(\alpha(x)) \leq 2$. Veja que

$$\alpha(x) \in \{0, 1, x, 1 + x, x^2, 1 + x^2, 1 + x + x^2\}$$

Lembrando que $x^3 \equiv 1 \pmod{x^3 - 1}$ segue que:

$$\begin{gathered}
(1 + x)0 \equiv 0 \pmod{x^3 - 1}; \\
(1 + x)1 \equiv 1 + x \pmod{x^3 - 1}; \\
(1 + x)x \equiv x + x^2 \pmod{x^3 - 1}; \\
(1 + x)(1 + x) = 1 + 2x + x^2 \equiv 1 + x^2 \pmod{x^3 - 1}; \\
(1 + x)x^2 = x^2 + x^3 \equiv 1 + x^2 \pmod{x^3 - 1}; \\
(1 + x)(1 + x^2) = 1 + x^2 + x + x^3 \equiv x + x^2 \pmod{x^3 - 1}; \\
(1 + x)(x + x^2) = 1 + x^2 + x^2 + x^3 \equiv 1 + x \pmod{x^3 - 1}; \\
(1 + x)(1 + x + x^2) = 1 + x + x^2 + x + x^2 + x^3 \equiv 0 \pmod{x^3 - 1}.
\end{gathered}$$

Logo,

$$\mathcal{P}_g = \{0, 1 + x, 1 + x^2, x + x^2\}.$$

Os vetores associados aos polinômios de $\mathcal{P}_g$ são:

- $0 \longleftrightarrow (0, 0, 0)$;
- $1 + x \longleftrightarrow (1, 1, 0)$;
- $1 + x + x^2 \longleftrightarrow (1, 1, 1)$;
- $x + x^2 \longleftrightarrow (0, 1, 1)$.

Logo, encontramos o código cíclico do Exemplo 5.2.

Exemplo 5.10. Sejam $n = 3$ e $q = 2$. Tomemos $g(x) = x^2 + x + 1$ que também divide $x^3 - 1$ em $\mathbb{F}_2[x]$. Vamos entender o conjunto $\mathcal{P}_g$, definido na expressão (5.2). Para isso, vamos listar todos os possíveis $g(x)\alpha(x) \pmod{x^3 - 1}$, com $\deg(\alpha(x)) \leq k$. Como, $k = 3 - \deg(g(x)) = 1$, assim, para formar $\mathcal{P}_g$, há apenas 4 polinômios de grau 0 ou 1. Ou seja,

$$\alpha(x) \in \{0, 1, x, 1 + x\}.$$

Temos:

$$(1 + x + x^2)0 \equiv 0 \pmod{x^3 - 1};$$
$$(1 + x + x^2)1 \equiv 1 + x + x^2 \pmod{x^3 - 1};$$
$$(1 + x + x^2)x = x + x^2 + x^3 \equiv 1 + x + x^2 \pmod{x^3 - 1};$$
$$(1 + x + x^2)(1 + x) = 1 + x + x^2 + x + x^2 + x^3 \equiv 0 \pmod{x^3 - 1};$$

Logo,

$$\mathcal{P}_g = \{0, 1 + x + x^2\}.$$

Os vetores associados aos polinômios de $\mathcal{P}_g$ são:

- $0 \longleftrightarrow (0, 0, 0)$;
- $1 + x + x^2 \longleftrightarrow (1, 1, 1)$.

Obtemos então o código $C = \{(0, 0, 0), (1, 1, 1)\}$.

Exemplo 5.11. Sobre $\mathbb{F}_2[x]$, o polinômio $x^7 - 1$ se fatora como

$$x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Então, há 8 códigos cíclicos de comprimento 7 sobre $\mathbb{F}_2$, a saber:

1. $\mathcal{C} = \langle 0 \rangle$;
2. $\mathcal{C} = \langle 1 \rangle = \mathbb{F}_2^7$;
3. $\mathcal{C} = \langle 1 + x \rangle$ que tem dimensão 6;

4. $\mathcal{C} = \langle 1 + x + x^3 \rangle$ que tem dimensão 4;

5. $\mathcal{C} = \langle 1 + x^2 + x^3 \rangle$ que tem dimensão 4;

6. $\mathcal{C} = \langle (1 + x)(1 + x + x^3) \rangle$ que tem dimensão 3;

7. $\mathcal{C} = \langle (1 + x)(1 + x^2 + x^3) \rangle$ que tem dimensão 3;

8. $\mathcal{C} = \langle (1 + x + x^3)(1 + x^2 + x^3) \rangle$ que tem dimensão 6.

A aplicação

$$\begin{array}{rccc} \varphi : & \mathbb{F}_q^n & \to & \mathbb{F}_q[x]/\langle x^n - 1 \rangle \\ & (a_0, a_1, \ldots, a_{n-1}) & \mapsto & a_0 + a_1 x + \cdot + a_{n-1} x^{n-1} \end{array} \tag{5.4}$$

é uma bijeção entre os vetores de $\mathbb{F}_q^n$ e os polinômios de $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$, onde escrevemos x no lugar de $\overline{x}$ por simplicidade. De fato, dado $(a_0, a_1, \ldots, a_n) \in F_q^n$, então como o grau de $\overline{a_0 + a_1 x + \cdot + a_{n-1} x^{n-1}}$ é menor que n, então pode ser identificado com o próprio $a_0 + a_1 x + \cdot + a_{n-1} x^{n-1}$. Por outro lado, um polinômio em $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ necessariamente tem grau menor que n e, assim, seus coeficientes formam um vetor $(a_0, a_1 \ldots, a_n) \in \mathbb{F}_q^n$.

Lema 5.12. *Um subespaço vetorial V de $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ é um ideal de $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ se, e somente se, $x \cdot f \in V$ para todo $f \in V$.*

Demonstração. A ida decorre diretamente da definição de ideal.

Reciprocamente, suponhamos que $x \cdot f \in V$, para todo $f \in V$. Como V é um subespaço vetorial, basta mostrarmos que $f(x) \cdot g(x) \in V$, para todos $f(x) \in \mathbb{F}_q[x]/\langle x^n - 1 \rangle$ e $g(x) \in V$. Com efeito, se $g(x) \in V$, como V é subespaço vetorial, então $a \cdot g(x) \in V$, para todo $a \in \mathbb{F}_q$. Por hipótese, $xg(x) \in V$, utilizando o fato de que V é um subespaço vetorial, segue, por indução, que $x^i g(x) \in V$, para todo $i \in \mathbb{N}$. Portanto, $g(x)f(x) \in V$. ■

Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código cíclico. Assim, se $(c_1, c_2, \ldots, c_n) \in \mathcal{C}$, então $(c_n, c_1, \ldots, c_{n-1}) \in \mathcal{C}$. Consequentemente,

$$g(x) = c_1 + c_2 x + \cdots + c_n x^{n-1}$$

e

$$\begin{aligned} xg(x) &= c_1x + c_2x^2 + \cdots c_nx^n \\ &- c_1x + c_2x^2 + \cdots + c_n \end{aligned}$$

pertencem ambos a um ideal $I \subset \mathbb{F}_q[x]/\langle x^n - 1\rangle$. Por conseguinte, há uma bijeção entre os códigos cíclicos de $\mathbb{F}_q^n$ e os ideais de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.

Suponhamos que, $MDC(n, q) = 1$, de modo que, o polinômio $x^n - 1$ não tenha raízes múltiplas. Assim, como o anel $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ é principal, se I é um ideal de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ segue que

$$I = \langle g(x)\rangle = \{fg;\ f \in \mathbb{F}_q[x]/\langle x^n - 1\rangle\}, \tag{5.5}$$

onde $g(x)$ é mônico de grau mínimo no ideal I e I é um ideal principal. Logo, podemos dizer que os códigos cíclicos estão em bijeção com ideais gerados por $g(x)$, isto é, $\langle g(x)\rangle$.

Exemplo 5.13. Consideremos o código do Exemplo 5.3. Calculemos os associados às palavras do código:

$$\begin{aligned} C_0 = (0,0,0,0,0,0,0) &\longleftrightarrow 0; \\ C_1 = (1,0,1,1,1,0,0) &\longleftrightarrow 1 + x^2 + x^3 + x^4; \\ C_2 = (0,1,0,1,1,1,0 &\longleftrightarrow x + x^3 + x^4 + x^5; \\ C_3 = (0,0,1,0,1,1,1) &\longleftrightarrow x^2 + x^4 + x^5 + x^6; \\ C_4 = (1,1,1,0,0,1,0) &\longleftrightarrow 1 + x + x^2 + x^5; \\ C_5 = (1,0,0,1,0,1,1) &\longleftrightarrow 1 + x^3 + x^5 + x^6; \\ C_6 = (0,1,1,1,0,0,1) &\longleftrightarrow x + x^2 + x^3 + x^6; \\ C_7 = (1,1,0,0,1,0,1) &\longleftrightarrow 1 + x + x^4 + x^6. \end{aligned}$$

Então, a palavra $C_1 = (1,0,1,1,1,0,0)$ vista como polinômio é $g(x) = 1+x^2+x^3+x^4$ e este polinômio é mônico de menor grau dentre os associados às palavras do código. Portanto, $g(x) = 1 + x^2 + x^3 + x^4$ é o polinômio gerador do código, isto é, $C = \langle g\rangle$. Ademais, $\langle 1 + x^2 + x^3 + x^4\rangle$ é um ideal de $\mathbb{F}_2[x]/\langle x^7 - 1\rangle$.

Exemplo 5.14. Consideremos o código do Exemplo 5.6. Então, a palavra $C_3 = (2,0,1,0)$ vista como polinômio é $g(x) = 2 + x^2$ e este polinômio é mônico de

menor grau dentre os associados às palavras do código. Portanto, $g(x) = 2 + x^2$ é o polinômio gerador do código, isto é, $C = \langle g \rangle$. Além disso, $\langle 2 + x^2 \rangle$ é um ideal de $\mathbb{F}_3[x]/\langle x^4 - 1 \rangle$.

Lema 5.15. *Seja $\mathcal{C} = \langle g \rangle$ um código cíclico de comprimento n. Valem:*

1. *$g(x)$ divide $x^n - 1$;*
2. $\dim(c) = n - \deg(g)$.

Demonstração.

1. Suponhamos, por contradição que $g(x)$ não divide $x^n - 1$. Então existem $a(x)$ e $b(x)$ tais que

$$a(x)g(x) + b(x)(x^n - 1) = \ MDC(g(x), x^n - 1).$$

   Este MDC tem grau menor que o de g e está no ideal

$$I = \langle g(x) \rangle \subset \mathbb{F}_q[x]/\langle x^n - 1 \rangle,$$

   o que contradiz a minimalidade do grau de g em I. Logo, $g(x)$ divide $x^n - 1$.

2. Os polinômios $x^j g(x)$, para $j \in \{1, 2, \ldots, n - \deg(g) - 1\}$ são linearmente independentes em $I = \langle g \rangle$. Assim, a dimensão de C é pelo menos $n - \deg(g)$. Vamos mostrar que esses polinômios geram I.

   De fato, se $f(x) \in I$, então $f(x) = d(x)g(x)$ em $\mathbb{F}_q[x]/\langle g(x) \rangle$, de modo que, $f(x) \equiv d(x)g(x) \pmod{x^n - 1}$.

   Seja $h(x) \in \mathbb{F}_q[x]$ tal que $h(x)g(x) - x^n - 1$. Pelo algoritmo da divisão, temos

$$d(x) = c(x)h(x) + r(x)$$

   em $\mathbb{F}_q[x]$, onde

$$r(x) = a_0 + a_1 x + \cdots + a_{n-\deg(g)-1} x^{n-\deg(g)-1}.$$

   Assim,

$$f(x) \equiv d(x)g(x) \equiv c(x)h(x)g(x) + r(x)g(x) \pmod{x^n - 1}$$

e

$$f(x) \equiv c(x)(^n-1) + r(x)g(x) \equiv r(x)g(g) \pmod{x^n - 1}.$$

Logo, em $\mathbb{F}_q[x]/\langle x^n - 1\rangle$

$$f(x) = a_0 g(x) + a_1 x g(x) + a_2 x^2 g(x) + \cdots + a_{n-\deg(g)-1} x^{n-\deg(g)-1} g(x).$$

Daí: $\dim(C) = n - \deg(g)$.

■

Seja $\mathcal{C}$ um $[n, k, d]_q$ código cíclico gerado pelo polinômio

$$g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}. \tag{5.6}$$

Então, pelo Lema 5.15

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & \cdots & g_{n-k} & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \cdots & \cdots & 0 & g_0 & g_1 & \cdots & \cdots & g_{n-k} \end{bmatrix} = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix} \tag{5.7}$$

é uma matriz geradora para $\mathcal{C}$.

Agora, seja $h(x) \in \mathbb{F}_q[x]$ tal que $g(x)h(x) = x^n - 1$. Note que

$$\deg(h) = n - \deg(g) = n - (n - k) = k. \tag{5.8}$$

Se

$$h(x) = h_0 + h_1 x + \cdots + h_k x^k, \tag{5.9}$$

considere o polinômio recíproco $\overleftarrow{h}(x) = x^k h(x^{-1})$, isto é,

$$\begin{aligned} \overleftarrow{h}(x) &= x^k h(x^{-1}) \\ &= x^k (h_0 + h_1 x^{-1} + h_2 (x^{-1})^2 + \cdots + h_k (x^{-1})^k \\ &= x^k \left(h_0 + \frac{h_1}{x} + \frac{h_2}{x^2} + \cdots + \frac{h_k}{x^k} \right) \\ &= h_0 x^k + h_1 x^{k-1} + h_2 x^{k-2} + \cdots + h_{k-1} x + h_k \\ &= h_k + h_{k-1} x + \cdots + h_2 x^{k-2} + h_1 x^{k-1} + h_0 x^k. \end{aligned} \tag{5.10}$$

Então

$$H = \begin{bmatrix} h_k & h_{k-1} & \cdots & \cdots & h_0 & 0 & \cdots & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & \cdots & h_0 & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots & \\ 0 & \cdots & \cdots & 0 & h_k & h_{k-1} & \cdots & \cdots & h_0 \end{bmatrix} = \begin{bmatrix} \overleftarrow{h}(x) \\ x\overleftarrow{h}(x) \\ \vdots \\ x^{n-k-1}\overleftarrow{h}(x) \end{bmatrix} \tag{5.11}$$

é uma matriz teste de paridade para $\mathcal{C}$.

De fato, o produto interno $\langle G_i, H_j \rangle$ da i-ésima linha de G com a j-ésima linha de H é o coeficiente de x^{k-i+j} no produto $g(x)h(x)$, onde $i \in \{1, 2, \ldots, k\}$ e $j \in \{1, 2, \ldots, n-k\}$. Como $g(x)h(x) = x^n - 1$ e $1 \leq k - i + j \leq n - 1$, segue que $\langle G_i, H_j \rangle = 0$. Ainda, H tem $n - k$ linhas linearmente independentes, isto é, posto$(h) = n - k$.

Exemplo 5.16. Voltemos ao código do Exemplo 5.3. Temos $C = \langle g \rangle$, onde

$$g(x) = 1 + x^2 + x^3 + x^4.$$

Então como $C \subset \mathbb{F}_2$ é um código de comprimento $n = 7$ temos

$$k = n - \deg(g) = 7 - 4 = 3,$$

isto é, $\mathcal{C}$ é um $[7, 3, d]_2$ código. Como

$$h(x) = \frac{x^7 - 1}{x^4 + x^3 + x^2 + 1},$$

logo,

$$h(x) = 1 + x^2 + x^3 \quad \text{e} \quad \overleftarrow{h}(x) = x^3 + x^2 + 1.$$

As matrizes geradora e teste de paridade são então:

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \end{bmatrix}$$

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \overleftarrow{h}(x) \\ x\overleftarrow{h}(x) \\ x^2\overleftarrow{h}(x) \\ x^3\overleftarrow{h}(x) \end{bmatrix}.$$

Segue ainda das observações sobre as matrizes geradora e teste de paridade o seguinte resultado:

Teorema 5.17. *Seja $\mathcal{C} = \langle G \rangle$ um código cíclico de comprimento n e dimensão k. O código dual $\mathcal{C}^{\perp}$ é o código cíclico, onde $g(x)h(x) = x^n - 1$ e $\overleftarrow{h}(x) = x^k h(x^{-1})$.*

Exemplo 5.18. Seja $x^{11} - 1$ em $\mathbb{F}_3[x]$. Temos:

$$x^{11} - 1 = (x-1)(x^5 - x^3 + x^2 - x - 1)(x^5 + x^4 - x^3 + x^2 - 1).$$

Vamos considerar o código cíclico $\mathcal{C} = \langle g \rangle$, onde $g(x) = -1 - x + x^2 - x^3 + x^5$. Então, C tem comprimento $n = 11$ e dimensão $k = n - \deg(g) = 11 - 5 = 6$. Assim a matriz geradora de $\mathcal{C}$ é:

$$G = \begin{bmatrix} -1 & -1 & 1 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 1 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 & -1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & -1 & 1 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 & 1 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & -1 & 1 & -1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ x^3 g(x) \\ x^4 g(x) \\ x^5 g(x) \end{bmatrix}.$$

Seja $h(x)$ tal que $g(x)h(x) = x^{11} - 1$, ou seja,

$$\begin{aligned} h(x) &= (x-1)(x^5 + x^4 - x^3 + x^2 - 1) \\ &= x^6 + x^5 - x^4 + x^3 - x - x^5 - x^4 + x^3 - x^2 + 1 \\ &= x^6 - 2x^4 + 2x^3 - x^2 - x + 1 \\ &= 1 - x - x^2 - x^3 - x^4 + x^6. \end{aligned}$$

Então:

$$\begin{aligned} \overleftarrow{h}(x) &= x^6 h(x^{-1}) \\ &= x^6(x^{-6} + x^{-4} - x^{-3} - x^{-2} - x^{-1} + 1) \\ &= x^6 - x^5 - x^4 - x^3 - x^2 + 1. \end{aligned}$$

Logo, o código dual de $\mathcal{C}$ é $\mathcal{C}^{\perp} = \langle \overleftarrow{h} \rangle$ de comprimento $n = 11$ e dimensão $k = n - \deg(\overleftarrow{h}) = 11 - 6 = 5$. Ademais, a matriz geradora de $\mathcal{C}^{\perp}$ é:

$$G = \begin{bmatrix} 1 & -1 & -1 & -1 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 & -1 & -1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & -1 & -1 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & -1 & -1 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & -1 & -1 & -1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \overleftarrow{h}(x) \\ x\overleftarrow{h}(x) \\ x^2\overleftarrow{h}(x) \\ x^3\overleftarrow{h}(x) \\ x^4\overleftarrow{h}(x) \end{bmatrix}.$$

Perceba que, a matriz geradora de $\mathcal{C}^{\perp}$ é a matriz teste de paridade de $\mathcal{C}$.

6 FATORAÇÃO DE POLINÔMIOS CICLOTÔMICOS

Vimos que, para os códigos cíclicos, é útil saber fatorar polinômios do tipo $x^n - 1$, onde $n \in \mathbb{N}$. Aqui, estudaremos alguns casos especiais disso.

Seja $q = p^h$, com p primo. Sabemos que $x^{q-1} - 1$ se fatora em fatores lineares distintos em $\mathbb{F}_q[x]$.

Lema 6.1. *O polinômio $x^{q-1}-1$ se fatora em $F_p[x]$ em fatores irredutíveis distintos cujos graus são divisores de h.*

Demonstração. Seja $\alpha \in \mathbb{F}_q^*$, α uma raiz de $x^{q-1} - 1$. Vamos mostrar que α é raiz de um polinômio $f(x) \in \mathbb{F}_p[x]$ de grau r. Seja $\mathbb{F}_p(\alpha)$ o menor corpo que contém $\mathbb{F}_p$ e α. Então, a extensão $\mathbb{F}_p(\alpha)$ sobre $\mathbb{F}_p$ é um subcorpo de $\mathbb{F}_q$ que é um espaço vetorial sobre $\mathbb{F}_p$. Ademais, tal extensão tem grau $r = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ e $\mathbb{F}_p(\alpha)$ é gerado por $1, \alpha, \alpha^2, \ldots, \alpha^{r-1}$. Então, existem $a_0, a_1, \ldots, a_r \in \mathbb{F}_p$ tais que

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_r\alpha^r = 0,$$

donde, α é raiz de um polinômio em $\mathbb{F}_p[x]$ de grau r.

Agora, vamos mostrar que $r \mid h$, Com efeito, seja $\beta \in \mathbb{F}_p(\alpha) \subset \mathbb{F}_q$. Como $\beta \in \mathbb{F}_p(\alpha)$ segue que $\beta^{p^r} = \beta$. Também, como $\beta \in \mathbb{F}_q$, temos $\beta^q = \beta$, isto é, $\beta^{p^h} = \beta$. Assim, pela arbitrariedade de $\beta \in \mathbb{F}_p(\alpha)$, segue que $(x^{p^r} - x) \mid (x^q - x)$, isto é, $(x^{p^r} - x) \mid (x^{p^h} - x)$ Logo, $r \mid h$.

Portanto, $x^{q-1} - 1$ se fatora em $F_p[x]$ em fatores irredutíveis distintos cujos graus são divisores de h, como queríamos. ■

Exemplo 6.2. Vamos fatorar $x^8 - x$ em $\mathbb{F}_2[x]$.

Temos:

$$x^8 = x = x(x^7 - 1).$$

Temos também, $q = 8 = p^h = 2^3$. Agora, pelo Lema 6.1, $x^7 - 1 = x^{2^3-1} - 1$ se fatora em $\mathbb{F}_2[x]$ como produto de polinômios irredutíveis de graus que dividem 3. Sabemos que 1 e 3 são os únicos divisores de 3.

Ademais, 1 é a única raiz de $x^7 - 1$ em $\mathbb{F}_2$. Então, o único polinômio de grau 1 dessa fatoração é $x - 1$ e escrevemos

$$x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1).$$

Agora, basta encontrarmos os polinômios irredutíveis distintos de grau 3 que multiplicados dão o polinômio $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ de grau 6. Em $\mathbb{F}_2[x]$, há 8 polinômios de grau 3. São eles:

$$x^3;$$
$$x^3 + 1;$$
$$x^3 + x + 1;$$
$$x^3 + x^2 + x + 1;$$
$$x^3 + x;$$
$$x^3 + x^2 + x;$$
$$x^3 + x^2;$$
$$x^3 + x^2 + 1.$$

Os que tem termo independente nulo tem 0 como raiz, então não são irredutíveis. Restam 4:

$$x^3 + 1;$$
$$x^3 + x + 1;$$
$$x^3 + x^2 + x + 1;$$
$$x^3 + x^2 + 1.$$

Como os polinômios com um número par de termos, tem 1 como raiz, segue que

$$x^8 - x = x(x - 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Exemplo 6.3. Vamos fatorar $x^9 - x$ em $\mathbb{F}_3[x]$.

Temos, $x^9 - x = x(x^8 - 1)$ e, pelo Lema 6.1, os fatores irredutíveis de $x^8 - 1 = x^{3^2-1} - 1$ em $\mathbb{F}_3[x]$ têm grau divisor de 2, ou seja, grau 1 ou grau 2.

Como ± 1 são as raízes de $x^8 - 1$ em $\mathbb{F}_3$, os fatores de grau 1 são $x + 1$ e $x - 1$.

Faltam 3 fatores de grau 2. A menos de sinal, há 9 polinômios de grau 2 em $\mathbb{F}_3[x]$, sendo 6 dele com termo independente não nulo. São eles:

- $x^2 + 1$;
- $x^2 + x - 1$;
- $x^2 - x + 1$;
- $x^2 - 1$;
- $x^2 + x + 1$;
- $x^2 - x - 1$.

Agora, os únicos que não tem -1 ou 1 como raiz são: $x^2 + 1$, $x^2 + x - 1$ e $x^2 - x - 1$. Portanto:

$$x^9 - x = x(x + 1)(x - 1)(x^2 + 1)(x^2 + x - 1)(x^2 - x - 1).$$

Exemplo 6.4. O polinômio $x^{q-1} - 1$ se fatora como

$$x^{q-1} - 1 = (x^{(q-1)/2} - 1)(x^{(q-1)/2} + 1),$$

quando q é ímpar. As raízes do primeiro polinômio são os quadrados não nulos de $\mathbb{F}_q$ e as raízes do segundo polinômio são os não-quadrados.

Suponha agora que queremos fatorar $x^n - 1$ em $\mathbb{F}_q[x]$.

Se $MDC(n, q) = \ell > 1$, então $\binom{\ell}{j} = 0$, para cada $j \in \{1, 2, \ldots, \ell - 1\}$ e assim, como $MDC(n/\ell, q) = 1$, segue que

$$x^n - 1 = (x^{n/\ell} - 1)^\ell. \tag{6.1}$$

Isso significa que basta sabermos fatorar $x^m - 1$, com $MDC(m, q) = 1$ e, assim, podemos fatorar todos $x^n - 1$.

Vamos procurar uma extensão de $\mathbb{F}_q$ que contenha as n-ésimas raízes da unidade procurando o menor h tal que $n \mid q^h - 1$, isto é, determinando a ordem de q em $\mathbb{Z}_n$ como grupo multiplicativo.

Definição 6.5. *Um elemento $\xi \in \mathbb{F}_{q^h}$ é dito uma* ***raiz n-ésima da unidade****, quando ξ é raiz de $x^n - 1$ em $\mathbb{F}_{q^h}$. Dizemos que um elemento $\xi \in \mathbb{F}_{q^h}$ é uma* ***raiz primitiva da unidade*** *se $\{1, \xi, \ldots, \xi^{n-1}\}$ é o conjunto das n-ésimas raízes da unidade.*

Lema 6.6. *Um polinômio* $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_t) \in \mathbb{F}_q[x]$ *se, e somente se,* $\{\alpha_1, \alpha_2, \ldots, \alpha_t\} = \{\alpha_1^q, \alpha_2^q, \ldots, \alpha_t^q\}$.

Demonstração. Consideremos

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_t) = a_0 + a_1x + \cdots + a_tx^t.$$

Queremos provar que $f(x) \in \mathbb{F}_q[x]$. Para isso, basta provarmos que $a_i \in \mathbb{F}_q$, para cada $i \in \{0, 1, \ldots, t\}$, ou seja, que $a_i = a_i^q$, para todo $i \in \{0, 1, \ldots, t\}$. Temos:

$$\begin{aligned}(f(x))^q &= [(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_t)]^q \\ &= (x-\alpha_1)^q(x-\alpha_2)^q\cdots(x-\alpha_t)^q \\ &= (x^q-\alpha_1)^q(x^q-\alpha_2^q)\cdots(x^q-\alpha_t^q).\end{aligned}$$

Por outro lado,

$$\begin{aligned}(f(x))^q &= (a_0 + a_1x + \cdots + a_tx^t)^q \\ &= a_0^q + a_1^qx^q + \cdots + a_t^qx_t^q, \quad \text{pois } q \text{ é potência da característica.}\end{aligned}$$

Logo,

$$a_0^q + a_1^qx + \cdots + a_t^q = x = (x-\alpha_1^q)(x-\alpha_1^q)\cdots(x-\alpha_t^q).$$

Portanto, para cada $i \in \{0, 1, \ldots, t\}$:

$$\begin{aligned}a_i = a_i^q &\Leftrightarrow (x-\alpha_1^q)(x-\alpha_1^q)\cdots(x-\alpha_t^q) = (x-\alpha_1)(x-\alpha_1)\cdots(x-\alpha_t) \\ &\Leftrightarrow \{\alpha_1, \alpha_2, \ldots, \alpha_t\} = \{\alpha_1^q, \alpha_2^q, \ldots, \alpha_t^q\}.\end{aligned}$$

■

Teorema 6.7. *Suponha* $MDC(n, q) = 1$ *e seja* $\xi \in \mathbb{F}_{q^h}$ *uma raiz primitiva da unidade de ordem n. Os fatores irredutíveis de* $x^n - 1$ *em* $\mathbb{F}_q[x]$ *são*

$$(x-\xi^n)(x-\xi^{nq})\cdots(x-\xi^{nq^{d-1}}), \tag{6.2}$$

para $r \in \{0, 1, \ldots, n-1\}$, *onde d é o menor inteiro positivo tal que* $rq^d \equiv r \pmod{n}$.

Demonstração. Por hipótese, $rq^d \equiv r \pmod{n}$, assim

$$(\xi^{rq^{d-1}})^q = \xi^{rq^d} = \xi^r.$$

Então, pelo Lema 6.6,

$$g(x) = (x - \xi^n)(x - \xi^{nq}) \cdots (x - \xi^{nq^{d-1}}) \in \mathbb{F}_q[x].$$

Seja dado arbitrariamente $f(x) \in \mathbb{F}_q[x]$, $f(x) = a_0 + a_1 x + \cdots + a_m x^m$. Em particular, $a_i \in \mathbb{F}_q$, isto é, $a_i^q = a_i$, para cada $i \in \{1, 2, \ldots, m\}$. Se α é uma raiz de f, então

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_m\alpha^m = 0.$$

Elevando a q:

$$\begin{aligned} 0 &= (a_0 + a_1\alpha + \cdots + a_m\alpha^m)^q \\ &= a_0^q + a_1^q\alpha^q + \cdots + a_m^q\alpha^{mq} \\ &= a_0 + a_1\alpha^q + \cdots + a_m\alpha^{mq} \\ &= f(\alpha^q). \end{aligned}$$

Logo, α^q é raiz de f.

Vamos mostrar que $g(x)$ é o polinômio em $\mathbb{F}_q[x]$ mônico de menor grau tal que ξ^r é raiz. De fato, se $h(x)$ é tal que $h(\xi^r) = 0$, então:

$$\begin{aligned} h(\xi^r) = 0 &\Rightarrow h(\xi^{rq}) = 0 \\ &\Rightarrow h(\xi^{rq^2}) = 0 \\ &\cdots \end{aligned}$$

Consequentemente, o grau de h não pode ser menor que o grau de g. Logo, $g(x)$ é irredutível em $\mathbb{F}_q[x]$. Como todas as raízes de $g(x)$ são as raízes de $x^n - 1$, pois ξ é raiz primitiva da unidade de ordem n, segue o resultado. ■

Vamos entender melhor o que nos diz o Teorema 6.7.

Para cada $r \in \{0, 1, \ldots, n-1\}$ calculamos

$$\{r, rq, rq^2, \ldots, rq^{d-1}\} \tag{6.3}$$

fazendo cada elemento módulo n. O conjunto da expressão (6.3) é chamado ***coset ciclotômico***. Um coset ciclotômico de tamanho d corresponde e a um fator irredutível de $x^n - 1$ de grau d sobre $\mathbb{F}_q$. A união disjunta de cosets ciclotômicos é

$$\{0, 1, \ldots, n-1\}. \tag{6.4}$$

Agora veremos exemplos de como isso ajuda na fatoração.

Exemplo 6.8. Vamos fatorar $x^{12} - 1$ em $\mathbb{F}_{17}[x]$.

Primeiramente, vamos calcular os cosets ciclotômicos módulo $n = 12$.

Para $r = 0$ o coset é $\{0\}$.

Agora, para $r = 1$, temos

$$1 \times 17 \equiv 5 \pmod{12},$$

então 1 e 5 estão no mesmo coset. Ainda, temos:

$$\underbrace{1 \times 17^2}_{289} \equiv 5^2 \equiv 1 \pmod{5}.$$

Logo, $d_1 = 2$ e o coset é apenas $\{1, 5\}$.

Para $r = 2$, temos

$$2 \times 17 \equiv 2 \times 5 \equiv 10 \pmod{12},$$

donde, 2 e 10 estão no mesmo coset. Ainda,

$$2 \times 17^2 \equiv \underbrace{2 \times 5^2}_{50} \equiv 2 \pmod{12},$$

ou seja, $d_2 = 2$ e o coset de 2 é $\{2, 10\}$.

Para $r = 3$, temos

$$3 \times 17 \equiv \underbrace{3 \times 5}_{15} \equiv 3 \pmod{12},$$

donde, $d_3 = 1$ e o coset de 3 é $\{3\}$.

Para $r = 4$, temos

$$4 \times 17 \equiv \underbrace{4 \times 5}_{20} \equiv 8 \pmod{12}.$$

Ademais:

$$4 \times 17^2 \equiv \underbrace{4 \times 5^2}_{100} \equiv 2 \pmod{12},$$

donde, $d_4 = 2$ e o coset de 4 é $\{4, 8\}$.

Como $r = 5$ aparece no coset de $\{1\}$, calculemos o coset de $r = 6$. Temos:

$$6 \times 17 \equiv \underbrace{6 \times 5}_{30} \equiv 6 \pmod{12},$$

daí: $d_6 = 1$ e o coset de 6 é $\{6\}$.

Para $r = 7$, temos:

$$7 \times 17 \equiv \underbrace{7 \times 5}_{35} \equiv 11 \pmod{12}.$$

Temos também:

$$7 \times 17^2 \equiv \underbrace{7 \times 5^2}_{175} \equiv 7 \pmod{12}.$$

Logo, $d_7 = 2$ e o coset de 7 é $\{7, 11\}$.

Agora, como 10 aparece no coset de 2 e 11 aparece no coset de 7, resta, somente, calcularmos o coset de 9. Temos:

$$9 \times 17 \equiv \underbrace{9 \times 5}_{45} \equiv 9 \pmod{12}.$$

Logo, $d_9 = 1$ e o coset de 9 é $\{9\}$.

Então, os cosets ciclotômicos módulo 12 são:

$$\begin{aligned}
r = 0 : &\quad \{0\};\\
r = 1 : &\quad \{1, 5\};\\
r = 2 : &\quad \{2, 10\};\\
r = 3 : &\quad \{3\};\\
r = 4 : &\quad \{4, 8\};\\
r = 6 : &\quad \{6\};\\
r = 7 : &\quad \{7, 11\};\\
r = 9 : &\quad \{9\}.
\end{aligned}$$

Assim, na fatoração há 4 fatores de grau 2 e 4 de grau 1. Notamos que

$$x^{12} - 1 = (x^6 - 1)(x^6 + 1)$$

e

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x + 1)(x - 1)(x^2 + x + 1)(x^2 - x + 1). \qquad (6.5)$$

Faltam dois fatores de grau 1 e dois de grau 2, que estão na fatoração de $x^6 + 1$. Veja que, em $\mathbb{F}_{17}$, temos $4^2 = 16 = -1$, donde $4 = -4^{-1}$ e, assim, $-4^{-6} = -4^6 = 1$. Isso significa que

$$x^6 + 1 = -\left(\left(\frac{x}{4}\right)^6 - 1\right) \text{ em } \mathbb{F}_{17}[x].$$

Assim, podemos fatorar $x^6 + 1$ substituindo x por $x/4$ em (6.5):

$$\begin{aligned} x^6 + 1 &= -(x/4 - 1)((x/4)^2 + x + 1)(x/4 + 1)((x/4)^2 - x + 1) \\ &= (x - 4)(x^2 + 4x - 1)(x + 4)(x^2 - 4x - 1). \end{aligned}$$

Portanto, a fatoração de $x^{12} - 1$ em $\mathbb{F}_{17}[x]$ é:

$$x^{12}-1 = (x+1)(x-1)(x^2+x+1)(x^2-x+1)(x-4)(x^2+4x-1)(x+4)(x^2-4x-1).$$

Exemplo 6.9. Vamos fatorar o polinômio $x^{11} - 1$ sobre $\mathbb{F}_3[x]$. Para isso, vamos calcular os cosets ciclotômicos módulo 11.

Para $r = 0$, o coset é $\{0\}$.

Para $r = 1$, temos:

$$\begin{aligned} 1 \times 3 &\equiv 3 \pmod{11}; \\ 1 \times 3^2 &\equiv 9 \pmod{11}; \\ \underbrace{1 \times 3^3}_{27} &\equiv 6 \pmod{11}; \\ \underbrace{1 \times 3^4}_{81} &\equiv 4 \pmod{11}; \\ \underbrace{1 \times 3^5}_{243} &\equiv 1 \pmod{11}. \end{aligned}$$

Logo, $d_1 = 5$ e coset de 1 é $\{1, 3, 4, 6, 9\}$.

Para $r = 2$, temos:

$$\begin{aligned}
\underbrace{2 \times 3}_{6} &\equiv 5 \pmod{11};\\
\underbrace{2 \times 3^2}_{18} &\equiv 7 \pmod{11};\\
\underbrace{2 \times 3^3}_{54} &\equiv 10 \pmod{11};\\
\underbrace{2 \times 3^4}_{162} &\equiv 8 \pmod{11};\\
\underbrace{2 \times 3^5}_{486} &\equiv 2 \pmod{11}.
\end{aligned}$$

Assim, $d_2 = 5$ e o coset de 2 é $\{2, 5, 7, 8, 10\}$.

Logo, os cosets ciclotômicos são:

$$\{0\}, \{1, 3, 9, 5, 4\}, \{2, 6, 7, 10, 8\}.$$

Ou seja, a fatoração que buscamos têm 2 polinômios de grau 5 que podem ser vistos usando uma 11-raiz da unidade $\xi \in \mathbb{F}_{3^5}$ como:

$$f(x) = (x - \xi)(x - \xi^3)(x - \xi^9)(x - \xi^5)(x - \xi^4).$$

e

$$g(x) = (x - \xi^2)(x - \xi^6)(x - \xi^7)(x - \xi^{10})(x - \xi^8).$$

Observe que ambos polinômios tem termo independente $\xi^{22} = -1$ e que as raízes de f e de g são recíprocas (ξ e ξ^{10}, ξ^3 e ξ^8, ξ^9 e ξ^2, ξ^5 e ξ^6, ξ^4 e ξ^7). Dessa forma, se

$$f(x) = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x - 1,$$

$$g(x) = x^5 - a_1x^4 - a_2x^3 - a_3x^2 - a_4x - 1.$$

Assim, variando os coeficientes encontramos:

$$x^{11} - 1 = (x - 1)(x^5 - x^3 + x^2 - x - 1)(x^5 + x^4 - x^3 + x^2 - 1).$$

7 CÓDIGOS BCH

Seja α uma raiz primitiva da unidade em $\mathbb{F}_{q^m}$. Os ***códigos BCH*** são uma classe de códigos cíclicos em que escolhemos α de modo que

$$\alpha, \alpha^2, \ldots, \alpha^{d_0-1} \tag{7.1}$$

são raízes de um polinômio de grau pequeno (no sentido de minimalidade) $g(x) \in \mathbb{F}_q[x]$, para algum $d_0 < n$ fixado. Isso nos permite limitar inferiormente a distância mínima do código $\langle g(x) \rangle$. Quanto menor for o grau do polinômio g, maior será a dimensão do código.

Suponhamos que $g(x) \in \mathbb{F}_q[x]$ seja um polinômio de grau mínimo tal que $g(\alpha^k) = 0$ para $j \in \{1, 2, \ldots, d_0 - 1\}$. O código $\langle g(x) \rangle$ é chamado código BCH devido a seus criadores Bose, Ray-Chaudhuri e Hocquenghem, que introduziram essa família de códigos cíclicos. O parâmetro d_0 é chamado ***distância mínima prescrita*** devido ao seguinte resultado:

Teorema 7.1. *A dimensão do código BCH $\langle g \rangle$ é pelo menos $n - m(d_0 - 1)$ e a distância mínima é pelo menos d_0.*

Demonstração. Seja $j \in \{1, 2, \ldots, d_0 - 1\}$. O polinômio

$$f_j(x) = (x - \alpha^j)(x - \alpha^{jq}) \cdots (x - \alpha^{jq^{m-1}})$$

pertence a $\mathbb{F}_q[x]$. Ainda, $f(\alpha^j) = 0$ e $\deg(f) = m$. Então $\prod f_j$ é um polinômio de grau $(d_0 - 1)m$ em $\mathbb{F}_q[x]$ que se anula em α^j para todo $j \in \{1, 2, \ldots, d_0 - 1\}$. Temos:

$$\begin{aligned} \deg(g) \leq (d_0 - 1)m &\Rightarrow -\deg(g) \geq -m(d_0 - 1) \\ &\Rightarrow \dim(\langle g \rangle) = n - \deg(g) \geq n - m(d_0 - 1). \end{aligned}$$

Agora, suponhamos que exista $h \in \langle g \rangle$ tal que $\omega(h) \leq d_0 - 1$. Assim, tomemos

$$h(x) = b_1 x^{k_1} + b_2 x^{k_2} + \cdots + b_{d_0-1} x^{d_0-1}.$$

Como $h \in \langle g \rangle$, então $h(\alpha^j) = 0$, para todo $j \in \{1, 2, \ldots, d_0 - 1\}$. Ou seja,

$$\underbrace{\begin{bmatrix} \alpha^{k_1} & \alpha^{k_2} & \cdots & \alpha^{k_{d_0-1}} \\ \alpha^{2k_1} & \alpha^{2k_2} & \cdots & \alpha^{2k_{d_0-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(d_0-1)k_1} & \alpha^{(d_0-1)k_2} & \cdots & \alpha^{(d_0-1)k_{d_0-1}} \end{bmatrix}}_{A} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{d_0-1} \end{bmatrix} = 0.$$

Como o determinante da matriz A é

$$\det(A) = \prod_{i \neq j} (\alpha^{k_i} - \alpha^{k_j}) \neq 0,$$

a única solução do sistema é $h(x) = 0$. Logo, o peso mínimo de uma palavra não-nula do código $\langle g \rangle$ é pelo menos d_0 e segue a conclusão sobre a distância mínima. ■

Exemplo 7.2. Seja α uma raiz primitiva da unidade de ordem 31 em $\mathbb{F}_{32} = \mathbb{F}_{2^5}$. Obtemos a fatoração de $x^{31} - 1$ sobre $\mathbb{F}_2$ considerando os cosets ciclotômicos módulo 31, temos:

- Para $r = 1$:

$$\begin{aligned} 1 \times 2 &\equiv 2 \pmod{31}; \\ \underbrace{1 \times 2^2}_{4} &\equiv 4 \pmod{31}; \\ \underbrace{1 \times 2^3}_{8} &\equiv 8 \pmod{31}; \\ \underbrace{1 \times 2^4}_{16} &\equiv 16 \pmod{31}; \\ \underbrace{1 \times 2^5}_{32} &\equiv 1 \pmod{31}. \end{aligned}$$

  Assim, $d_1 = 5$ e o coset de 1 é $\{1, 2, 4, 8, 16\}$.

- Para $r = 3$:

$$\begin{aligned}
\underbrace{3 \times 2}_{6} &\equiv 6 \pmod{31};\\
\underbrace{3 \times 2^2}_{12} &\equiv 12 \pmod{31};\\
\underbrace{3 \times 2^3}_{24} &\equiv 24 \pmod{31};\\
\underbrace{3 \times 2^4}_{48} &\equiv 17 \pmod{31};\\
\underbrace{3 \times 2^5}_{96} &\equiv 3 \pmod{31}.
\end{aligned}$$

  Assim, $d_3 = 5$ e o coset de 3 é $\{3, 6, 12, 24, 17\}$.

- Para $r = 5$:

$$\begin{aligned}
\underbrace{5 \times 2}_{10} &\equiv 10 \pmod{31};\\
\underbrace{5 \times 2^2}_{20} &\equiv 20 \pmod{31};\\
\underbrace{5 \times 2^3}_{40} &\equiv 9 \pmod{31};\\
\underbrace{5 \times 2^4}_{80} &\equiv 18 \pmod{31};\\
\underbrace{5 \times 2^5}_{160} &\equiv 5 \pmod{31}.
\end{aligned}$$

  Assim, $d_5 = 5$ e o coset de 5 é $\{5, 10, 20, 9, 18\}$.

- Para $r = 7$:

$$\begin{aligned}
\underbrace{7 \times 2}_{14} &\equiv 14 \pmod{31};\\
\underbrace{7 \times 2^2}_{28} &\equiv 28 \pmod{31};\\
\underbrace{7 \times 2^3}_{56} &\equiv 25 \pmod{31};\\
\underbrace{7 \times 2^4}_{112} &\equiv 19 \pmod{31};\\
\underbrace{7 \times 2^5}_{224} &\equiv 7 \pmod{31}.
\end{aligned}$$

Assim, $d_7 = 5$ e o coset de 7 é $\{7, 14, 28, 25, 19\}$.

- Para $r = 11$:

$$\begin{aligned}
\underbrace{11 \times 2}_{22} &\equiv 22 \pmod{31};\\
\underbrace{11 \times 2^2}_{44} &\equiv 13 \pmod{31};\\
\underbrace{11 \times 2^3}_{88} &\equiv 26 \pmod{31};\\
\underbrace{11 \times 2^4}_{176} &\equiv 21 \pmod{31};\\
\underbrace{11 \times 2^5}_{352} &\equiv 11 \pmod{31}.
\end{aligned}$$

Assim, $d_{11} = 5$ e o coset é $\{11, 22, 13, 26, 21\}$.

- Para $r = 15$:

$$\begin{aligned}
\underbrace{15 \times 2}_{30} &\equiv 30 \pmod{31};\\
\underbrace{15 \times 2^2}_{60} &\equiv 29 \pmod{31};\\
\underbrace{15 \times 2^3}_{120} &\equiv 27 \pmod{31};\\
\underbrace{15 \times 2^4}_{240} &\equiv 23 \pmod{31};\\
\underbrace{15 \times 2^5}_{480} &\equiv 15 \pmod{31};
\end{aligned}$$

Assim, $d_{15} = 5$ e o coset de 15 é $\{15, 30, 29, 27, 23\}$.

Logo, os cosets ciclotômicos módulo 31 são:

$$\{1, 2, 4, 8, 16\}, \{3, 6, 12, 24, 17\}, \{5, 10, 20, 9, 18\}$$
$$\{7, 14, 28, 25, 19\}, \{11, 22, 13, 26, 21\}, \{15, 30, 29, 27, 23\}.$$

O i-ésimo coset ciclotômico nos dá um polinômio $f_i(x) \in \mathbb{F}_2[x]$ tal que $f_i(\alpha^j) = 0$, para cada j do coset. Assim, temos:

$$\begin{aligned}
f_1(x) &= (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^{16});\\
f_2(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^{24})(x-\alpha^{17});\\
f_3(x) &= (x-\alpha^5)(x-\alpha^{10})(x-\alpha^{20})(x-\alpha^9)(x-\alpha^{18});\\
f_4(x) &= (x-\alpha^7)(x-\alpha^{14})(x-\alpha^{28})(x-\alpha^{25});\\
f_5(x) &= (x-\alpha^{11})(x-\alpha^{22})(x-\alpha^{13})(x-\alpha^{26})(x-\alpha^{21});\\
f_6(x) &= (x-\alpha^{15})(x-\alpha^{30})(x-\alpha^{29})(x-\alpha^{27})(x-\alpha^{23}).
\end{aligned}$$

Seja $g_1(x) = f_1(x)f_2(x)f_3(x)$. O código cíclico $\langle g_1\rangle$ tem dimensão $n = 31 - \deg(g_1) = 31 - 15 = 16$. Os cosets ciclotômicos envolvidos são:

$$\{1,2,4,8,16\}, \{3,6,12,24,17\}, \{5,10,20,9,18\}$$

Como $1,2,3,4,5,6$ estão em tais cosets, então $g_1(\alpha^j) = 0$, para cada $j \in \{1,2,3,4,5,6\}$. Então, $d_0 - 1 = 6$, ou seja, $d_0 = 7$. Logo, pelo Teorema 7.1, o código $\mathcal{C} = \langle g_1\rangle$ tem distância mínima $d \geq \underbrace{7}_{d_0}$, donde, seus parâmetros são $[31, 16, \geq 7]_2$. Na verdade, consegue-se provar que $d = 7$.

Agora, consideremos $g_2(x) = f_1(x)f_2(x)f_3(x)f_4(x)$. O código cíclico $\langle g_2\rangle$ tem dimensão $n = 31 - \deg(g_2) = 31 - 20 = 11$. Os cosets ciclotômicos envolvidos são:

$$\{1,2,4,8,16\}, \{3,6,12,24,17\}, \{5,10,20,9,18\}, \{7,14,28,25,19\}.$$

Como $1,2,3,4,5,6,7,8,9,10$ estão em tais cosets, então $g_2(\alpha^j) = 0$, para cada $j \in \{1,2,3,4,5,6,7,8,9,10\}$. Então, $d_0 - 1 = 10$, ou seja, $d_0 = 11$. Portanto, pelo Teorema 7.1, o código $\mathcal{C} = \langle g_2\rangle$ tem distância mínima $d \geq 11$, donde, seus parâmetros são $[31, 11, \geq 11]_2$.

Exemplo 7.3. Seja $\mathbb{F}_9 = \mathbb{F}_3[x]/\langle x^2 + x - 1\rangle$.

Se α é uma raiz de $x^2 + x - 1$, então ele é um gerador de $\mathbb{F}_9 \setminus \{0\}$.

Com efeito, sendo α uma raiz de x^2+x-1, então $\alpha^2+\alpha-1=0$, isto é, $\alpha^2=-\alpha+1$. Temos:

$$\begin{aligned}
\alpha^3 &= \alpha\alpha^2=\alpha(-\alpha+1)=-\alpha^2+\alpha=-(-\alpha+1)+\alpha=2\alpha-1=-\alpha-1;\\
\alpha^4 &= \alpha\alpha^3=\alpha(-\alpha-1)=-\alpha^2-\alpha=-(-\alpha+1)-\alpha=-1;\\
\alpha^5 &= \alpha\alpha^4=\alpha(-1)=-\alpha;\\
\alpha^6 &= \alpha\alpha^5=\alpha(-\alpha)=-\alpha^2=-(-\alpha+1)=\alpha-1;\\
\alpha^7 &= \alpha\alpha^6=\alpha(\alpha-1)=\alpha^2-\alpha=(-\alpha+1)-\alpha=-2\alpha+1=\alpha+1;\\
\alpha^8 &= \alpha\alpha^7=\alpha(\alpha+1)=\alpha^2+\alpha=(-\alpha+1)+\alpha=1.
\end{aligned}$$

Então, α é uma raiz primitiva da unidade de ordem 8 e

$$\mathbb{F}_9\setminus\{0\}=\langle\alpha\rangle=\{\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8\}.$$

Ainda, fatorando o polinômio x^8-1 em $\mathbb{F}_3$, temos:

$$x^8-1=(x+1)(x-1)(x^2+1)(x^2-x-1)(x^2+x-1).$$

Como α é gerador, cada potência de α é raiz de algum dos polinômios da fatoração obtida. De fato:

- α:

  Como $\alpha^2=-\alpha+1$, temos $\alpha^2+\alpha-1=0$. Logo, α é raiz de x^2+x-1.

- α^2:

  Como $\alpha^4=1$, temos $(\alpha^2)^2-1=0$. Logo, α^2 é raiz de x^2+1.

- α^3:

  Como $\alpha^6=\alpha-1$ e $\alpha^3=-\alpha-1$, temos

  $$\underbrace{\alpha^6}_{(\alpha^3)^2}+\alpha^3-1=\alpha-1-\alpha-1-1=0.$$

  Logo, α^3 é raiz de x^2+x-1.

- α^4:

  Como $\alpha^4=-1$, ou seja, $\alpha^4+1=0$, segue que α^4 é raiz de $x+1$.

- α^5:

  Temos:

$$\underbrace{\alpha^{10}}_{(\alpha^5)^2} + \alpha^5 - 1 = -\alpha + 1 - \alpha - 1 = 0.$$

  Logo, α^5 é raiz de $x^2 + x - 1$.

- α^6:

  Temos:

$$\underbrace{\alpha^{12}}_{(\alpha^6)^2} + 1 = -1 + 1 = 0.$$

  Logo, α^6 é raiz de $x^2 + 1$.

- α^7:

  Temos:

$$\underbrace{\alpha^{14}}_{(\alpha^7)^2} - \alpha^7 - 1 = \alpha - 1 - (\alpha - 1) - 1 = 0.$$

  Logo, α^7 é raiz de $x^2 - x - 1$.

- α^8:

  Como $\alpha^8 = 1$, isto é, $\alpha^8 - 1 = 0$, segue que, α^8 é raiz de $x - 1$.

  Seja

$$g(x) = (\underbrace{x+1}_{f_1(x)})(\underbrace{x^2+1}_{f_2(x)})(\underbrace{x^2+x-1}_{f_3(x)}) = x^5 - x^4 + x^3 + x^2 - 1.$$

O código cíclico $\langle g \rangle$ tem dimensão $n = 8 - \deg(g) = 8 - 5 = 3$. Os cosets ciclotômicos envolvidos são:

$$\{4\}, \{2, 6\}, \{1, 3\}.$$

Como 1,2,3,4 estão em tais cosets, então $g(\alpha^j) = 0$, para cada $j \in \{1, 2, 3, 4\}$. Então, $d_0 - 1 = 4$, isto é, $d_0 = 5$. Portanto, pelo Teorema 7.1, o código $\mathcal{C} = \langle g \rangle$ tem parâmetros $[8, 3, d]_9$, onde $d \geq 5$.

Observação 7.4. Nos exemplos 7.2 e 7.3, usamos a fatoração de $x^{q^m-1}-1$ como vista no capítulo 6 para produzir os polinômios geradores dos códigos BCH. Apesar da escolha de não termos explicitado, os polinômios escolhidos são, de fato, os polinômios mínimos das potências das raízes (de fato, são irredutíveis e mônicos). Utilizando isso, é possível provar que o polinômio gerador do código BCH relacionado às potências $\alpha, \alpha^2, \ldots, \alpha^{d_0-1}$ de uma raiz da unidade $\alpha \in \mathbb{F}_{q^m}$ é:

$$g(x) = MMC\{p_1(x), \ldots, p_{d_0-1}(x)\}$$

onde $p_i(x)$ é o polinômio mínimo de α^i sobre $\mathbb{F}_q$ (Teorema 2 da seção 7.4 de [6]).

Visto que um código BCH é um código cíclidadco gerado por um polinômio $g(x)$, então é formado por múltiplos do polinômio $g(x)$. Dessa fora, o jeito mais direto de codificar uma mensagem é, em forma de polinômio, multiplicá-lo pelo gerador. Vejamos um exemplo:

Exemplo 7.5. Consideremos o código BCH com parâmetros $[31, 21, d]_2$ gerado pelo polinômio

$$g(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1.$$

Suponhamos que queremos codificar a mensagem 101101110111101111101. O polinômio associado à essa mensagem é

$$p(x) = x^{20}+x^{18}+x^{17}+x^{15}+x^{14}+x^{13}+x^{11}+x^{10}+x^9+x^8+x^6+x^5+x^4+x^3+x^2+1.$$

Efetuando a multiplicação $p(x)g(x)$ módulo 2, temos:

$$\begin{aligned}
s(x) &= p(x)g(x) \\
&= (x^{20}+x^{18}+x^{17}+x^{15}+x^{14}+x^{13}+x^{11}+x^{10}+x^9+x^8+x^6+x^5+ \\
&+ x^4+x^3+x^2+1)(x^{10}+x^9+x^8+x^6+x^5+x^3+1) \\
&= (x^{30}+x^{29}+x^{28}+x^{26}+x^{25}+x^{23}+x^{20})+(x^{28}+x^{27}+x^{26}+x^{24}+x^{23}+x^{21}+x^{18})+ \\
&+ (x^{27}+x^{26}+x^{25}+x^{23}+x^{22}+x^{20}+x^{17})+(x^{25}+x^{24}+x^{23}+x^{21}+x^{20}+x^{18}+x^{15})+ \\
&+ (x^{24}+x^{23}+x^{22}+x^{20}+x^{19}+x^{17}+x^{14})+(x^{23}+x^{22}+x^{21}+x^{19}+x^{18}+x^{16}+x^{13})+ \\
&+ (x^{21}+x^{20}+x^{19}+x^{17}+x^{16}+x^{14}+x^{11})+(x^{20}+x^{19}+x^{18}+x^{16}+x^{15}+x^{13}+x^{10})+ \\
&+ (x^{19}+x^{18}+x^{17}+x^{15}+x^{14}+x^{12}+x^9)+(x^{18}+x^{17}+x^{16}+x^{14}+x^{13}+x^{11}+x^8)+ \\
&+ (x^{16}+x^{15}+x^{14}+x^{12}+x^{11}+x^9+x^6)+(x^{15}+x^{14}+x^{13}+x^{11}+x^{10}+x^8+x^5)+ \\
&+ (x^{14}+x^{13}+x^{12}+x^{10}+x^9+x^7+x^4)+(x^{13}+x^{12}+x^{11}+x^9+x^8+x^6+x^3)+ \\
&+ (x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^2)+(x^{10}+x^9+x^8+x^6+x^5+x^3+1) \\
&= x^{30}+x^{29}+2x^{28}+2x^{27}+3x^{26}+3x^{25}+3x^{24}+6x^{23}+3x^{22}+4x^{21}+6x^{20}+ \\
&+ 5x^{19}+6x^{18}+5x^{17}+5x^{16}+5x^{15}+7x^{14}+6x^{13}+45x^{12}+6x^{11}+5x^{10}+ \\
&+ 5x^9+5x^8+2x^7+3x^6+3x^5+x^4+2x^3+x^2+0x+1 \\
&= x^{30}+x^{29}+x^{26}+x^{25}+x^{24}+x^{22}+x^{19}+x^{17}+x^{16}+x^{15} \\
&+ x^{14}+x^{12}+x^{10}+x^9+x^8+x^6+x^5+x^4+x^2+1.
\end{aligned}$$

Logo, a mensagem a ser transmitida é 1100111010010111101011101110101.

Agora, quanto à decodificação, trabalharemos com síndrome, conforme vimos anteriormente. Veremos como fazer isso no seguinte exemplo:

Exemplo 7.6. Seja $\mathbb{F}_{2^4} = \mathbb{F}_2/\langle x^4+x+1\rangle$.

Seja ξ uma raiz de x^4+x+1. Então, ξ é uma raiz primitiva da unidade de ordem 15 (gera $\mathbb{F}_{16}\setminus\{0\}$). De fato, sendo ξ uma raiz de x^4+x+1, então $\xi^4+\xi+1=0$, isto é, $\xi^4=\xi+1$. Temos:

i	ξ^i
0	1
1	ξ
2	ξ^2
3	ξ^3
4	$\xi^4 = \xi + 1$
5	$\xi^5 = \xi(\xi + 1) = \xi^2 + \xi$
6	$\xi^6 = \xi(\xi^2 + \xi) = \xi^3 + \xi^2$
7	$\xi^7 = \xi(\xi^3 + \xi^2) = \xi^4 + \xi^3 = \xi^3 + \xi + 1$
8	$\xi^8 = \xi(\xi^3 + \xi + 1) = \xi^4 + \xi^2 + \xi = \xi + 1 + \xi^2 + \xi = \xi^2 + 1$
9	$\xi^9 = \xi(\xi^2 + 1) = \xi^3 + \xi$
10	$\xi^{10} = \xi(\xi^3 + \xi) = \xi^4 + \xi^2 = \xi^2 + \xi + 1$
11	$\xi^{11} = \xi(\xi^2 + \xi + 1) = \xi^3 + \xi^2 + \xi$
12	$\xi^{12} = \xi(\xi^3 + \xi^2 + \xi) = \xi^4 + \xi^3 + \xi^2 = \xi^3 + \xi^2 + \xi + 1$
13	$\xi^{13} = \xi(\xi^3 + \xi^2 + \xi + 1) = \xi^4 + \xi^3 + \xi^2 + \xi = \xi^3 + \xi^2 + 1$
14	$\xi^{14} = \xi(\xi^3 + \xi^2 + 1) = \xi^4 + \xi^3 + \xi = \xi^3 + 1$
15	$\xi^{15} = \xi(\xi^3 + 1) = \xi^4 + \xi = 1$

Tabela 2 – Potências da raiz ξ de $x^4 + x + 1$.

Logo, ξ é uma raiz primitiva da unidade de ordem 15 e

$$\mathbb{F}_9 \setminus \{0\} = \langle \xi \rangle = \{1, \xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^6, \xi^7, \xi^8, \xi^9, \xi^{10}, \xi^{11}, \xi^{12}, \xi^{13}, \xi^{14}\}.$$

Ainda, a fatoração de $x^{15} - 1$ é da forma:

$$x^{15} - 1 = (x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1).$$

Seja

$$g(x) = (\underbrace{x^4 + x + 1}_{f_1(x)})(\underbrace{x^4 + x^3 + x^2 + x + 1}_{f_2(x)}).$$

O polinômio $g(x)$ gera um código BCH de comprimento $n = 15$ (lembre que $g(x)$ é formado por fatores de $x^{15} - 1$), dimensão $n - \deg(g) = 15 - 8 = 7$. Note que as raízes de $f_1(x)$ e $f_2(x)$ são ξ, ξ^2, ξ^4, ξ^8 e ξ^3, ξ^6, ξ^9, ξ^{12}, respectivamente. Assim, como $g(x)$ tem como raízes consecutivas ξ, ξ^2, ξ^3 e ξ^4, segue, pelo Teorema 7.1, que $\langle g \rangle$ tem distância mínima prescrita $d_0 = 4 + 1 = 5$. Logo, o código $\mathcal{C} = \langle g \rangle$ tem parâmetros $[15, 7, d \geq 5]_2$ e assim, pelo Teorema 3.12, $\mathcal{C}$ pode corrigir até $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor = 2$ erros.

Suponhamos que recebemos a palavra $y = (y_0, y_1, \ldots, y_{14})$ que está a uma distância menor do que ou igual a 2 de uma palavra do código. Queremos encontrar a palavra $c \in \mathcal{C}$ tal que $y = c + e$, com $\omega(e) \leq 2$. Suponhamos $\omega(e) = 2$ e que os erros nas posições i_1 e i_2. O que podemos afirmar?

Sejam $y(x) = \sum y_i x^i$, $c(x) = \sum c_i x^i$ e $e(x) = x^{i_1} + x^{i_2}$, os polinômios associados às palavras y, c e e, respectivamente. O único polinômio que conhecemos é $y(x)$. Sabemos ainda que $y(\alpha) = e(\alpha)$ e $c(\alpha) = 0$, isto é, conhecemos as síndromes $s_i := y(\xi^i)$, para cada $i \in \{1, 2, 3, 4, 6, 8, 9, 12\}$ (pois, $c(x)$ é um múltiplo de $g(x)$). Sejam $a = \xi^{i_1}$ e $b = \xi^{i_2}$. Temos:

$$\begin{aligned} e(\xi) = s_1 &\Rightarrow a + b = s_1 \\ e(\xi^2) = s_2 &\Rightarrow a^2 + b^2 = s_2 \\ e(\xi^3) = s_3 &\Rightarrow a^3 + b^3 = s_3 \\ e(\xi^4) = s_4 &\Rightarrow a^4 + b^4 = s_4 \end{aligned}$$

Veremos que essas 4 igualdades são suficientes para determinarmos as posições dos erros. De fato, devemos encontrar $a \neq b$ em $\mathbb{F}_{2^k} = \mathbb{F}_2(\xi)$ satisfazendo tais igualdades. Perceba que basta encontrarmos ab pois, nesse caso, teremos a fatoração do polinômio

$$z^2 - (a + b)z + ab = (a - z)(b - z)$$

e assim revela a e b. Ainda, temos:

$$\begin{aligned} s_1^3 &= (a + b)^3 \\ &= (a^2 + b^2)(a + b) \\ &= a^3 + b^3 + ab(a + b) \\ &= s_3 + abs_1 \end{aligned}$$

Como $s_1 \neq 0$, temos

$$ab = s_1^3 - \frac{s_3}{s_1} = s_2 - \frac{s_3}{s_1},$$

já que estamos em característica 2.

Suponhamos que recebemos a mensagem $y = (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$. Então, o polinômio associado à essa palavra é $y(x) = x^4 + x^6 + x^7 + x^8 + x^{13}$.

Temos:

$$\begin{aligned}
s_1 &= y(\xi) = \xi^4+\xi^6+\xi^7+\xi^8+\xi^{13} \\
&= (\xi+1)+(\xi^3+\xi^2)+(\xi^3+\xi+1)+(\xi^2+1)+(\xi^3+\xi^2+1) \\
&= 3\xi^3+3\xi^2+2\xi+4 = \xi^3+\xi^2 \\
&= \xi^6. \\
s_2 &= y(\xi^2) = x^8+x^{12}+x^{14}+x^{16}+x^{26} \\
&= (\xi^2+1)+(\xi^3+\xi^2+\xi+1)+(\xi^3+1)+\xi+(\xi^3+\xi^2+\xi) \\
&= 3\xi^3+3\xi^2+3\xi+3 = \xi^3+\xi^2+\xi+1 \\
&= \xi^{12}. \\
s_3 &= y(\xi^3) = x^{12}+x^{18}+x^{21}+x^{24}+x^{39} \\
&= (\xi^3+\xi^2+\xi+1)+\xi^3+(\xi^3+\xi^2)+(\xi^3+\xi)+(\xi^3+\xi) \\
&= 5\xi^3+2\xi^2+3\xi+1 = \xi^3+\xi+1 \\
&= \xi^7. \\
s_4 &= y(\xi^4) = \xi^{16}+\xi^{24}+\xi^{28}+\xi^{32}+\xi^{52} \\
&= \xi+(\xi^3+\xi)+(\xi^3+\xi^2+1)+\xi^2+(\xi^3+\xi+1) \\
&= 3\xi^3+2\xi^2+3\xi+2 = \xi^3+\xi \\
&= \xi^9.
\end{aligned}$$

Além disso,

$$a+b = s_1 = \xi^6 = \xi^3+\xi^2.$$

$$ab = s_2 - \frac{s_3}{s_1} = \xi^{12} - \frac{\xi^7}{\xi^6} = \xi^{12}-\xi.$$

Assim, o polinômio a ser fatorado é:

$$\begin{aligned}
z^2+(\xi^3+\xi^2)z+(\xi^{12}-\xi) &= z^2+\xi^6 z+(\xi^3+\xi^2+1) \\
&= z^2+\xi^6 z+\xi^{13}.
\end{aligned}$$

Uma forma de fazer isso é procurar as raízes entre ξ^i que são $\xi^0 = 1$ e ξ^{13}. Assim, concluímos que a palavra recebida teve erro nas posições 0 e 13, donde a palavra do código mais próxima é

$$\begin{aligned}
c &= (0,0,0,0,1,0,1,1,1,0,0,0,0,1,0)-(1,0,0,0,0,0,0,0,0,0,0,0,0,1,0) \\
&= (1,0,0,0,1,0,1,1,1,0,0,0,0,0,0)
\end{aligned}$$

Dado $x \in \mathbb{Z}$, definimos:

$$\lfloor x \rfloor = \max\{m \in \mathbb{Z};\ m \leq x\} \quad \text{e} \quad \lceil x \rceil = \max\{n \in \mathbb{Z};\ n \geq x\} \tag{7.2}$$

Agora, mais geralmente, o algoritmo de decodificação consiste, resumidamente, no seguinte:

Suponha que o polinômio gerador código tenha raízes consecutivas $\xi, \xi^2, \ldots \xi^{d_0-1}$. Então, podemos corrigir no máximo $\left\lfloor \dfrac{d_0-1}{2} \right\rfloor$ erros. Se a palavra recebida for y, encontramos o polinômio associado $y(x)$, calculamos as síndromes $s_1 = y(\xi), s_2 = y(\xi^2), \ldots, s_{2t} = y(\xi^{2t})$. Se os erros estão nas posições $i_1, i_2, \ldots, i_t$, escrevendo $a_k = \xi^{i_k}$, para cada $k \in \{1, 2, \ldots, t\}$, obtemos as relações

$$\begin{aligned} a_1 + a_2 + \cdots + a_t &= s_1 \\ a_1^2 + a_2^2 + \cdots + a_t^2 &= s_2 \\ &\vdots \\ a_1^t + a_2^t + \cdots + a_t^t &= s_t, \end{aligned}$$

e podemos trabalhar com as relações de Newton entre os coeficientes de $L(z) = (z - a_1)(z - a_2)\cdots(z - a_t)$.

8 SEQUÊNCIAS DE DNA E CÓDIGOS BCH

Neste capítulo teremos como objetivo aplicar a teoria que vimos sobre códigos BCH à sequências de DNA. As referências principais são [2] e [3].

8.1 Um pouco de biologia celular

Nesta seção, faremos uma breve apresentação de alguns conceitos sobre o DNA, com o objetivo de compreender o processo de geração de proteínas, realizado no sistema biológico.

A ***célula*** é a unidade da básica vida em todas as formas de organismos vivos, da mais simples bactéria ao mais complexo animal. Assim como os humanos, cada célula que forma nosso corpo deve crescer, reproduzir-se, processar informações, responder a estímulos e realizar uma série de reações químicas. Os seres humanos e os outros ***organismos multicelulares*** (que possuem mais de uma célula) são compostos por bilhões ou trilhões de células organizadas em estruturas complexas, mas outros organismos consistem de uma única célula, os denominados ***organismos unicelulares***. Mesmo os organismos unicelulares simples exibem todas as propriedades características da vida, indicando que a célula é a unidade fundamental. Há dois tipos de células - procarióticas e eucarióticas.

As ***células procarióticas*** consistem de um único compartimento fechado, que é delimitado por uma membrana plasmática; essas células não possuem um núcleo definido e apresentam uma organização interna relativamente simples. Um exemplo de organismo que apresenta célula procariótica é a bactéria, que é um organismo unicelular dos mais abundantes na natureza.

As ***células eucarióticas***, diferentemente das células procarióticas, contêm um núcleo definido delimitado por membrana e uma grande quantidade de membranas internas que delimitam outros compartimentos, as organelas. O ***núcleo*** é uma estrutura presente em todas as células eucarióticas que é responsável por controlar todas as atividades celulares e armazenar informação genética. A região da célula existente entre a membrana plasmática e o núcleo é o ***citoplasma***, o qual compreende o ***citosol*** e as ***organelas***. Os eucariotos, organismos que que

apresentam célula(s) eucariótica(s), englobam todos os membros dos reinos animal e vegetal, incluindo os fungos, que ocorrem sob formas multicelulares (bolores e cogumelos) e unicelulares (leveduras), e os protozoários, que são exclusivamente unicelulares.

Muito do conteúdo celular consiste de um meio aquoso adicionado de pequenas moléculas (por exemplo, açúcares simples, aminoácidos, vitaminas) e íons (por exemplo, sódio, cloreto e íons cálcio). Uma das mais conhecidas entre as moléculas pequenas é o ***trifosfato de adenosina*** (***ATP***), que estoca energia química facilmente disponível em duas de suas ligações químicas. As ***mitocôndrias*** são organelas celulares relacionadas com o processo de respiração celular gerando grande quantidade de ATP.

Certas moléculas pequenas, chamadas ***monômeros***, presentes na célula podem se unir para a formação de ***polímeros*** (qualquer molécula grande composta de unidades, monômeros), pela repetição de um único tipo de reação de ligação química. As células produzem três tipos de grandes polímeros, denominados ***macromoléculas***: as proteínas, os polissacarídeos e os ácidos nucleicos.

As ***proteínas*** são polímeros lineares contendo de dezenas a vários milhares de aminoácidos, de maneira que as proteínas dão estrutura às células e realizam grande parte das tarefas celulares. São responsáveis pelas mais variadas funções no nosso organismo, desde o transporte de nutrientes e metabólitos à catálise de reações biológicas. São, no entanto, relativamente simples: sua composição consiste nas repetições de 20 unidades básicas, as quais denominamos por ***aminoácidos***.

Os ***polissacarídeos*** são polímeros lineares ou ramificados de monossacarídeos (açúcares), como a glicose, ligados por meio de ligações glicosídicas.

Os ***ácidos nucleicos*** são polímeros lineares que contêm de centenas a milhões de nucleotídeos, consistindo em macromoléculas que contém a informação que determina a sequência de aminoácidos. Consequentemente, os ácidos nucleicos contém a estrutura e a função de todas as proteínas de uma célula as quais fazem parte das estruturas celulares e alinham os aminoácidos de forma correta, quando uma cadeia polipeptídica está sendo sintetizada e catalisam uma série de reações químicas fundamentais nas células, inclusive a formação das pontes peptídicas entre os aminoácidos, durante a síntese de proteínas.

Os ácidos nucleicos contêm as informações para a produção das proteínas no local e momento adequados. A informação referente a como, quando e onde deve ser produzido cada tipo de proteína está contida no material genético. Dois tipos de ácidos nucleicos quimicamente semelhantes, o ***DNA*** (ácido desoxirribonucleico) e o ***RNA*** (ácido ribonucleico), são as principais moléculas que carregam as informação das células. Denominaremos por ***nucleotídeos***, os monômeros que formam o DNA e o RNA que têm uma estrutura comum: um grupo fosfato ligado por uma ligação fosfodiéster a uma pentose (uma molécula de açúcar com cinco carbonos) que, por sua vez, está ligada a um anel cuja estrutura contém nitrogênio e carbono, a qual normalmente é conhecida como "base". No RNA, a pentose é a ribose, e no DNA, é a desoxirribose.

Uma ***sequência de DNA*** é a estrutura primária de uma molécula de DNA representada por uma série de nucleotídeos.

8.2 Motivação para o uso de códigos corretores de erros

Em um sistema de comunicação digital, a informação é transportada de um transmissor para um receptor por uma sequência de bits passando por um canal de transmissão. Nas células eucarióticas, existe entre outros processos biológicos o transporte de proteínas (P) para organelas onde uma informação genética no núcleo se move para o citosol através de intermediários de mRNA (RNA mensageiro), que é posteriormente traduzido em uma proteína precursora contendo uma extensão N-terminal (extremidade da proteína que possui um grupo amino livre) que funciona como uma sequência de direcionamento (TS) direcionando a proteína para a organela correspondente. As sequências internas (IS) em algumas proteínas precursoras têm a finalidade de sinalizar para os compartimentos submitocondriais corretos de uma organela. Assim, pode-se conceber que um código corretor de erros usado na transmissão de dados através de um canal de ruídos possa ser aplicado à geração de sequências de DNA (como proteínas, sequências de direcionamento e sequências internas) em células eucarióticas ou procarióticas. Nesse caso, os conceitos da teoria de códigos podem ser usados adequadamente para modelar os processos de transcrição e tradução.

Levando em consideração essas semelhanças e premissas, os autores de [2]

propuseram um algoritmo capaz de reproduzir sequências de DNA, associadas a regiões codificadoras de genes, como palavras de códigos corretores de erros. Mesmo que anteriormente vários estudos tenham sido realizados para associar sequências de DNA com palavras de códigos corretores de erros, nenhum sucesso parece ter sido alcançado até o momento. Uma questão sempre colocada na maioria dos trabalhos relacionados à codificação genômica é:

Existe alguma forma de códigos corretores de erros serem associados à estrutura das sequências de DNA?

Aqui, veremos, seguindo [2], uma resposta positiva para esta pergunta, mostrando que existem sequências de DNA que podem ser identificadas como palavras de códigos BCH sobre corpos finitos. Este resultado permite o uso de simulações computacionais eficientes na análise de processos biológicos como polimorfismos e mutações (erros espontâneos durante a replicação do DNA provocando alterações na sequência dos nucleotídeos) e, por conseguinte, reduzindo o tempo e os materiais gastos em experimentos laboratoriais.

8.3 Procedimento para geração de sequência de DNA

Embora o código genético tenha um alfabeto próprio, é desejável, como já vimos, que o alfabeto de um código corretor de erros tenha certa estrutura algébrica. Em geral, a identificação de uma estrutura algébrica com o alfabeto genético é um problema em aberto. Aqui, vamos usar $\mathbb{F}_4$ como o alfabeto e, como o código genético deve ser convertido para o alfabeto, e vice-versa, segue-se que essa conversão deve levar em consideração todos os possibilidades de associar os elementos do conjunto $N = \{A, C, G, T\}$, onde A é adenina, C é citosina, G é guanina e T é timina, com os elementos do conjunto $\mathbb{F}_4 = \{0, 1, a, a^2 = b\}$. Chamamos esta associação de ***rotulagem***, tendo 24 permutações envolvidas.

O objetivo dessa rotulagem é determinar qual permutação corresponde à palavra-código com a sequência de DNA fornecida. Em seguida, a fim de corresponder o comprimento da sequência de DNA ao comprimento da palavra-código, devemos encontrar o grau da extensão, denotado por r, usando a igualdade $n = 4^r - 1$, onde n é o comprimento da sequência de DNA.

Consideraremos, então, C um código BCH com parâmetros $[n, k, d_H]_4$ sobre $\mathbb{F}_{4^r}$, com $n = 4^r - 1$. Vamos relacionar a notação utilizada no capítulo 7 com as terminologias biológicas:

- n é o comprimento das palavras do código, ou seja, o comprimento das sequências de DNA;
- k é a dimensão do código como um subespaço vetorial de $\mathbb{F}_4^r$, isto é, o comprimento da sequência de informação de entrada responsável por gerar a sequência de DNA.

Lembramos, ainda, que d_H é a distância mínima do código e que r é o grau do polinômio primitivo da extensão $\mathbb{F}_{4^r}|\mathbb{F}_4$.

Agora, como gerar o código BCH? Para cada valor de r (o grau da extensão), há muitos polinômios primitivos $p(x)$ a serem considerados e existe um polinômio gerador $g(x)$ do código BCH que corresponde a cada $p(x)$. A complexidade computacional adicional na solução deste problema vem do fato de que quanto maior o grau da extensão, maior o número de $p(x)$ a serem considerados na construção do código. Por exemplo, se $n = 63$, então $r = 3$ e, usando a expressão 2.6, o número $I(3)$ de polinômios mônicos irredutíveis de grau 3 sobre $\mathbb{F}_4$ satisfaz:

$$4^3 = 4 + 3T(3) \Rightarrow I(3) = 20\,.$$

Nem todo polinômio mônico irredutível é um polinômio primitivo. Para cada um dos $p(x)$ que sejam, devemos encontrar a extensão de $\mathbb{F}_4[x]/\langle p(x)\rangle$ correspondente, o grupo de unidades da extensão e, usando o elemento primitivo, devemos construir o polinômio gerador $g(x)$ do código BCH.

Ainda, sabendo que o número de palavras do código geradas cresce exponencialmente com a dimensão do código, em vez de gerar todas as palavras do código e comparar com a sequência de DNA, as 24 permutações são aplicadas àquela sequência de DNA, e essas sequências são consideradas como "possíveis palavras-código" v. Então, para determinar quais são, de fato, palavras-código, a relação $vH^t = 0$ é utilizada. No caso em que temos $vH^t = 0$, a palavra está no código. Caso contrário, devemos verificar o que aconteceria se em cada posição

tivéssemos um (dos três outros possíveis) nucleotídeo diferente em cada posição na sequência de DNA, para cada permutação, e novamente usamos a relação vH^t para verificar se v é uma palavra do código.

8.4 O algoritmo

Dados de entradas:

1. $seq :=$ sequência de DNA original em nucleotídeos (NCBI);
2. n;
3. $d_H = 2t + 1$.

O algoritmo a seguir nos fornece uma identificação de sequências de DNA utilizando a construção de códigos BCH sobre $\mathbb{F}_{4^r}$, $r \in \mathbb{N}$.

Passo 1) Escolher o alfabeto do código;

Passo 2) Determinar em qual corpo finito irá trabalhar;

Passo 3) Encontrar todos os polinômios primitivos com o mesmo grau r da extensão e escolher um $p(x)$ dentre esses polinômios;

Passo 4) Determinar a extensão $\mathbb{F}_{4^r}$ do corpo finito $\mathbb{F}_4$;

Podemos obter o corpo $\mathbb{F}_{4^r}$ através do quociente de $F_4[x]$ por um ideal gerado por qualquer um dos polinômios primitivos escolhido no Passo 2). Dessa forma, escolhido um $p(x)$ de grau r, temos:

$$\begin{aligned} \mathbb{F}_{4^r}[x] &= \mathbb{F}_4[x]/\langle p(x)\rangle \\ &= \{a_0 + a_1x + a_2x^2 + \cdots + a_{r-1}x^{r-1};\ a_i \in \mathbb{F}_4,\ i = 1\ldots, r-1\}. \end{aligned}$$

Passo 5) Encontrar o grupo das unidades para o código BCH;

Encontrar o grupo das unidades de $\mathbb{F}_{4^r}$, significa encontrar um gerador de $\mathbb{F}_{4^r} \setminus \{0\}$, isto é, um elemento primitivo que gera $\mathbb{F}_{4^r} \setminus \{0\}$. Lembrando que, tal elemento primitivo é uma raiz primitiva da unidade de ordem $4^r - 1$. Neste caso, o comprimento da sequência de DNA é igual a $4^r - 1$.

Passo 6) Determinar o polinômio gerador $g(x)$ e a matriz G teste de paridade do código $\mathcal{C}$.

Depois de ter realizado os passos anteriores, podemos agora construir códigos BCH de comprimento n sobre $\mathbb{F}_4$, considerando que a distância mínima d_H do código, é no máximo, igual ao comprimento do código, isto é, $d_H \leq n$. O algoritmo irá analisar todos os valores possíveis para d_H. Lembrando que a distância está relacionada com a capacidade de correção de erros através da relação $d_H \leq 2\kappa + 1$ (vide Teorema 3.12), onde κ denota a quantidade de erros que o código será capaz de corrigir no processo de decodificação. Para encontrarmos $g(x)$, basta seguirmos os seguintes passos:

i) Encontrar as raízes dos polinômios minimais $m_i(x)$, $i \in \{1, 2, \ldots, n-1\}$;
Sendo α um elemento primitivo de $\mathbb{F}_{4^r}$, para cada $i \in \{1, 2, \ldots, n-1\}$, o polinômio minimal $m_i(x)$ tem como raízes os elementos do conjunto

$$\left\{\alpha^i, (\alpha^i)^4, (\alpha^i)^{4^2}, (\alpha^i)^{4^3}, \ldots, (\alpha^i)^{4^{r/2-1} \pmod n}\right\}.$$

ii) Encontrar os $m_i(x)$, para todo $i \in \{1, 2, \ldots, n-1\}$;
Os minimais são encontrados da seguinte forma:

$$m_i(x) = (x-\alpha^i)(x-(\alpha^i)^4)(x-(\alpha^i)^{4^2})(x-(\alpha^i)^{4^3}) \cdots (x-(\alpha^i)^{4^{r/2-1} \pmod n}).$$

iii) Para cada valor de κ tal que $d_H \geq 2\kappa + 1$, encontrar os polinômios geradores;
O polinômio gerador para cada valor de κ é dado por

$$g(x) = \ mmc\{m_1(x), m_2(x), \ldots, m_{n-1}(x)\},$$

formado pelos polinômios minimais que são diferentes entre si e que possuem raízes $\alpha, \alpha^2, \ldots, \alpha^{2t}$.

Passo 7) Determinar o polinômio gerador $h(x)$ da matriz teste de paridade H do código;

O polinômio gerador da matriz teste de paridade H é obtido através da relação:

$$h(x) = \frac{x^n - 1}{g(x)},$$

onde $g(x)$ é o polinômio gerador encontrado no Passo 6).

Passo 8) Determinar a matriz G geradora do código $\mathcal{C}$ e encontrar sua transposta G^t;

Lembremos que, sendo $\mathcal{C}$ um $[4^r-1, k, d_H]_{4^r}$ código BCH, supondo que $\mathcal{C}$ é um código cíclico gerado pelo polinômio $g(x) = g_0 + g_1x + \cdots + g_{4^r-1-k}x^{4^r-1-k}$, então, pelo Lema 5.15

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & \cdots & g_{4^r-1-k} & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & g_{4^r-1-k} & 0 & \cdots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \cdots & \cdots & 0 & g_0 & g_1 & \cdots & \cdots & g_{4^r-1-k} \end{bmatrix} = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix}$$

é uma matriz geradora para $\mathcal{C}$.

Passo 9) Determinar H e calcular sua transposta H^t;

Se $h(x) = h_0 + h_1x + \cdots + h_kx^k$, considerando $\overleftarrow{h}(x)$ o polinômio recíproco, então

$$H = \begin{bmatrix} h_k & h_{k-1} & \cdots & \cdots & h_0 & 0 & \cdots & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & \cdots & h_0 & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots & \\ 0 & \cdots & \cdots & 0 & h_k & h_{k-1} & \cdots & \cdots & h_0 \end{bmatrix} = \begin{bmatrix} \overleftarrow{h}(x) \\ x\overleftarrow{h}(x) \\ \vdots \\ x^{4^r-1-k-1}\overleftarrow{h}(x) \end{bmatrix}$$

é uma matriz teste de paridade para $\mathcal{C}$.

Passo 10) Rotular a *seq* utilizando o Passo 1);

Passo 11) Verificar se a *seq* é uma palavra do código de acordo com os padrões de erros estabelecidos: $D(a,b) = 0$, $D(a,b) = 1$, $D(a,b) = 2$;

Para determinarmos quais são, de fato, palavras do código, utilizaremos a relação

$$vH^t = 0. \tag{8.1}$$

No caso em que temos $vHt = 0$, a palavra está no código e assim ocorrem $D(a,b) = 0$ nucleotídeo de diferença. Ainda, utilizando a relação (8.1), vamos determinar quais das sequências de DNA apresentando os padrões de erros $D(a,b) = 1$ e $D(a,b) = 2$ nucleotídeos de diferença da sequência de DNA do NCBI, respectivamente, são palavras-código dos códigos $[n, k, d_H]_{4^r}$.

Passo 12) Comparar todas as palavras do código que foram armazenadas no Passo 11) com a *seq* e explicitar onde os erros ocorreram;

Neste passo, todas as palavras-código armazenadas no passo 11) estão rotuladas na forma do alfabeto do código, $\mathbb{F}_4 = \{0, 1, a, b\}$, e serão convertidas em nucleotídeos usando o rotulamento do alfabeto do código genético $N = \{A, C, G, T\}$. Feito o rotulamento, as palavras-código são comparadas, uma-a-uma, com a sequência de DNA do NCBI mostrando onde os nucleotídeos diferem, e armazena os resultados.

Passo 13) Voltar para o Passo 6) e determinar outro $g(x)$;

Neste passo, determinamos outro valor da distância mínima d_H e utilizamos o mesmo procedimento, apresentado no Passo 6), para determinar o polinômio gerador relativo a esta distância.

Passo 14) Repetir do Passo 7) ao Passo 11) para o $g(x)$ encontrado do Passo 13), até que esgotem-se todas as possibilidades de $g(x)$;

Neste passo, o algoritmo determina todas as palavras-código encontradas com 0, 1 e 2 nucleotídeos de diferença através de todos os polinômios geradores relativos à distância mínima $1 \leq d_H \leq n$ e armazena os resultados.

Passo 15) Voltar ao Passo 3) e escolher um outro $p(x)$, e, então, repetir do Passo 4) ao Passo 14), até esgotar todos os $p(x)$ do Passo 3);

Passo 16) Fim.

8.5 Um exemplo

Agora, vamos descrever a construção do código BCH primitivo com parâmetros $[63, k, d_h = 3]_{4^r}$ sobre $\mathbb{F}_{4^r}$ capaz de gerar e reproduzir sequências de DNA com comprimento $n = 4^3 - 1 = 63$, com 1 nucleotídeo diferindo da sequência original.

Passo 1) Escolher o alfabeto do código:

Utilizaremos como alfabeto o corpo finito $\mathbb{F}_4 = \{0, 1, a, a^2 = b\}$, que está relacionado ao conjunto de nucleotídeos $N = \{A, C, G, T\}$, onde:

- A - bases adenina;
- C - citosina;
- G - guanina;
- T - timina.

Passo 2) Determinar em qual corpo finito irá trabalhar;

Como, neste exemplo, vamos estudar a construção de um código BCH primitivo com comprimento $n = 63$, segue que $r = 3$ é o grau polinômio primitivo utilizado na construção do corpo finito $\mathbb{F}_4$.

Passo 3) Encontrar todos os polinômios primitivos com o mesmo grau r da extensão e escolher um $p(x)$ dentre esses polinômios:

Temos:

$p_{01}(x) = x^3 + x^2 + ax + b$	$p_{02}(x) = x^3 + x^2 + bx + a$	$p_{03}(x) = x^3 + ax^2 + bx + a$
$p_{04}(x) = x^3 + bx^2 + ax + b$	$p_{05}(x) = x^3 + ax^2 + ax + a$	$p_{06}(x) = x^3 + x^2 + x + b$
$p_{07}(x) = x^3 + bx^2 + bx + b$	$p_{08}(x) = x^3 + bx^2 + x + a$	$p_{09}(x) = x^3 + x^2 + x + a$
$p_{10}(x) = x^3 + x^2 + bx + a$	$p_{11}(x) = x^3 + ax^2 + x + b$	$p_{12}(x) = x^3 + bx^2 + ax + a$

Tabela 3 – Polinômios primitivos da extensão de Galois de grau $r = 3$.

Neste exemplo, utilizaremos o polinômio $p_{05}(x) = x^3 + ax^2 + ax + a$, da Tabela 3, para realizarmos o Passo 4).

Passo 4) Determinar a extensão $\mathbb{F}_{4^r}$ do corpo finito $\mathbb{F}_4$:

Considerando $p(x)$ como sendo o polinômio $p_{05}(x) = x^3 + ax^2 + ax + a$ do Passo 3), podemos construir $\mathbb{F}_{4^3}$ da seguinte forma:

$$\begin{aligned} \mathbb{F}_{4^3}[x] &= \mathbb{F}_4/\langle x^3 + ax^2 + ax + a\rangle \\ &= \{a_0 + a_1x + a_2x^2;\ a_0, a_1, a_2 \in \mathbb{F}_4,\ x^3 + ax^2 + ax + a = 0\}. \end{aligned}$$

Passo 5) Encontrar o grupo das unidades para o código BCH primitivo;

Seja $\xi \in \mathbb{F}_{4^3}$ uma raiz do polinômio primitivo $p(x) = x^3 + ax^2 + ax + a$. Vamos mostrar que ξ é uma raiz primitiva da unidade de ordem 63. De fato:

$$\begin{aligned} p(\xi) = 0 &\Rightarrow \xi^3 + a\xi^2 + a\xi + a = 0 \\ &\Rightarrow \xi^3 = -a\xi^2 - a\xi - a \\ &\Rightarrow \xi^3 = a\xi^2 + a\xi + a. \end{aligned}$$

Lembrando que $\mathbb{F}_4 = \{0, 1, a, a^2 = b\}$, então:

$$a^2 = a + 1 = b \;\Rightarrow\; a + b = 1.$$

Vamos calcular as potências de ξ:

$$\begin{aligned} \xi^0 &= 1 \\ \xi^1 &= \xi \\ \xi^2 &= \xi^2 \\ \xi^3 &= a + a\xi + a\xi^2 \\ \xi^4 &= a\xi^3 + a\xi^2 + a\xi = a^2\xi^2 + a^2\xi + a^2 + a\xi^2 + a\xi \\ &= b + \xi + \xi^2 \\ \xi^5 &= \xi^3 + \xi + b\xi = a + a\xi + a\xi^2 + \xi + b\xi \\ &= a + \xi + b\xi^2 \\ \xi^6 &= b\xi^3 + \xi^2 + a\xi = ba\xi^2 + ba\xi + ba + \xi^2 + a\xi \\ &= \xi^2 + \xi + 1 + \xi^2 + a\xi \\ &= 1 + b\xi \\ &\vdots \end{aligned}$$

Continuando o processo, obtemos $\mathbb{F}_{64} = \langle \xi \rangle$. Os resultados das potências estão resumidos na tabela 4.

(ξ^0, ξ^1, ξ^2)	(ξ^0, ξ^1, ξ^2)	(ξ^0, ξ^1, ξ^2)	(ξ^0, ξ^1, ξ^2)
$0 \longleftrightarrow (0,0,0)$	$\xi^0 \longleftrightarrow (1,0,0)$	$\xi^1 \longleftrightarrow (0,1,0)$	$\xi^2 \longleftrightarrow (0,1,0)$
$\xi^3 \longleftrightarrow (a,a,a)$	$\xi^4 \longleftrightarrow (b,1,1)$	$\xi^5 \longleftrightarrow (a,1,b)$	$\xi^6 \longleftrightarrow (1,b,0)$
$\xi^7 \longleftrightarrow (0,1,b)$	$\xi^8 \longleftrightarrow (1,1,0)$	$\xi^9 \longleftrightarrow (0,1,1)$	$\xi^{10} \longleftrightarrow (a,a,b)$
$\xi^{11} \longleftrightarrow (1,b,b)$	$\xi^{12} \longleftrightarrow (1,0,a)$	$\xi^{13} \longleftrightarrow (b,a,b)$	$\xi^{14} \longleftrightarrow (1,a,b)$
$\xi^{15} \longleftrightarrow (1,0,b)$	$\xi^{16} \longleftrightarrow (1,0,1)$	$\xi^{17} \longleftrightarrow (a,b,a)$	$\xi^{18} \longleftrightarrow (b,1,0)$
$\xi^{19} \longleftrightarrow (0,b,1)$	$\xi^{20} \longleftrightarrow (a,a,1)$	$\xi^{21} \longleftrightarrow (a,0,0)$	$\xi^{22} \longleftrightarrow (0,a,0)$
$\xi^{23} \longleftrightarrow (0,0,a)$	$\xi^{24} \longleftrightarrow (b,b,b)$	$\xi^{25} \longleftrightarrow (1,a,a)$	$\xi^{26} \longleftrightarrow (b,a,1)$
$\xi^{27} \longleftrightarrow (a,1,0)$	$\xi^{28} \longleftrightarrow (0,a,1)$	$\xi^{29} \longleftrightarrow (a,a,0)$	$\xi^{30} \longleftrightarrow (0,a,a)$
$\xi^{31} \longleftrightarrow (b,b,1)$	$\xi^{32} \longleftrightarrow (a,1,1)$	$\xi^{33} \longleftrightarrow (a,0,b)$	$\xi^{34} \longleftrightarrow (1,b,1)$
$\xi^{35} \longleftrightarrow (a,b,1)$	$\xi^{36} \longleftrightarrow (a,0,1)$	$\xi^{37} \longleftrightarrow (a,0,a)$	$\xi^{38} \longleftrightarrow (b,1,b)$
$\xi^{39} \longleftrightarrow (1,a,0)$	$\xi^{40} \longleftrightarrow (0,1,a)$	$\xi^{41} \longleftrightarrow (b,b,a)$	$\xi^{42} \longleftrightarrow (b,0,0)$
$\xi^{43} \longleftrightarrow (0,b,0)$	$\xi^{44} \longleftrightarrow (0,0,b)$	$\xi^{45} \longleftrightarrow (1,1,1)$	$\xi^{46} \longleftrightarrow (a,b,b)$
$\xi^{47} \longleftrightarrow (1,b,a)$	$\xi^{48} \longleftrightarrow (b,a,0)$	$\xi^{49} \longleftrightarrow (0,b,a)$	$\xi^{50} \longleftrightarrow (b,b,0)$
$\xi^{51} \longleftrightarrow (0,b,b)$	$\xi^{52} \longleftrightarrow (1,1,a)$	$\xi^{53} \longleftrightarrow (b,a,a)$	$\xi^{54} \longleftrightarrow (b,0,1)$
$\xi^{55} \longleftrightarrow (a,1,a)$	$\xi^{56} \longleftrightarrow (b,1,a)$	$\xi^{57} \longleftrightarrow (b,0,a)$	$\xi^{58} \longleftrightarrow (b,0,b)$
$\xi^{59} \longleftrightarrow (1,a,1)$	$\xi^{60} \longleftrightarrow (a,b,0)$	$\xi^{61} \longleftrightarrow (0,a,b)$	$\xi^{62} \longleftrightarrow (1,1,b)$
$\xi^{63} \longleftrightarrow (1,0,0)$			

Tabela 4 – Elementos de $\mathbb{F}_{64}$.

Passo 6) Determinar o polinômio gerador $g(x)$ da matriz G teste de paridade do código:

Considerando que a distância mínima do código é $d_H = 3$, então o polinômio gerador é dado por:

$$g(x) = \ mmc\{m_1(x), m_2(x)\}.$$

Assim, só precisamos dos minimais $m_1(x)$ e $m_2(x)$. As raízes dos minimais são:

$$m_1(x): \left\{\xi^1, (\xi^1)^4, (\xi^1)^{4^2}, \ldots, (\xi^1)^{4^{3/2-1} \pmod{63}}\right\} = \{\xi^1, (\xi^1)^4, (\xi^1)^{4^2}\} = \{\xi, \xi^4, \xi^{16}\}.$$

$$m_2(x): \left\{\xi^2, (\xi^2)^4, (\xi^2)^{4^2}, \ldots, (\xi^2)^{4^{3/2-1} \pmod{63}}\right\} = \{\xi^2, (\xi^1)^4, (\xi^2)^{4^2}\} = \{\xi^2, \xi^8, \xi^{32}\}.$$

Logo, os minimais são:

$$\begin{aligned} m_1(x) &= (x-\xi)(x-\xi^4)(x-\xi^{16}) = x^3 + ax^2 + ax + a \\ m_2(x) &= (x-\xi^2)(x-\xi^8)(x-\xi^{32}) = x^3 + bx^2 + bx + b. \end{aligned}$$

Portanto, o polinômio gerador é dado por:

$$\begin{aligned} g(x) &= mmc\{m_1(x), m_2(x)\} \\ &= x^6 + x^5 + x^3 + x^2 + 1. \end{aligned}$$

O polinômio $g(x)$ gera um código BCH de dimensão $n - \deg(g) = 63 - 6 = 57$. Ou seja, o código $\mathcal{C} = \langle g(x) \rangle$ tem parâmetros $[65, 57, 3]_{4^3}$.

Passo 7) Determinar o polinômio gerador $h(x)$ da matriz teste de paridade H do código:

Temos:

$$\begin{aligned} h(x) &= \frac{x^{63} - 1}{x^6 + x^5 + x^3 + x^2 + 1} \\ &= x^{57} + x^{56} + x^{55} + x^{50} + x^{47} + x^{43} + x^{42} + x^{40} + x^{39} + x^{36} + x^{34} + x^{33} + \\ &+ x^{31} + x^{29} + x^{28} + x^{27} + x^{25} + x^{24} + x^{23} + x^{22} + x^{19} + x^{18} + x^{14} + x^{12} + \\ &+ x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1 \end{aligned}$$

Passo 8) Determinar a matriz G geradora do código $\mathcal{C}$ e encontrar sua transposta G^t:

Reescrevendo $g(x) = x^6 + x^5 + x^3 + x^2 + 1$ na forma

$$g(x) = 1 + 0x + x^2 + x^3 + 0x^4 + x^5 + x^6$$

a matriz geradora do código $\mathcal{C}$ é uma matriz 57×63 dada por:

$$G = \begin{bmatrix} 101101100000000000000000000000000000000000000000000000000000000 \\ 010110110000000000000000000000000000000000000000000000000000000 \\ 001011011000000000000000000000000000000000000000000000000000000 \\ 000101101100000000000000000000000000000000000000000000000000000 \\ \vdots \\ 000000000000000000000000000000000000000000000000000001011011000 \\ 000000000000000000000000000000000000000000000000000000101101100 \\ 000000000000000000000000000000000000000000000000000000010110110 \\ 000000000000000000000000000000000000000000000000000000001011011 \end{bmatrix},$$

ou seja,

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ x^3g(x) \\ \vdots \\ x^{53}g(x) \\ x^{54}g(x) \\ x^{55}g(x) \\ x^{56}g(x) \end{bmatrix}.$$

A matriz G^t é 63×57 determinada como sendo a troca da linha pela coluna da matriz G.

Passo 9) Determinar H e calcular sua transposta H^t:

Sendo

$$\begin{aligned} h(x) &= 1 + 0x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + 0x^8 + 0x^9 + x^{10} \\ &+ 0x^{11} + x^{12} + 0x^{13} + x^{14} + 0x^{15} + 0x^{16} + 0x^{17} + x^{18} + x^{19} + 0x^{20} \\ &+ 0x^{21} + x^{22} + x^{23} + x^{24} + x^{25} + 0x^{26} + x^{27} + x^{28} + x^{29} + 0x^{30} \\ &+ 0x^{31} + 0x^{32} + 0x^{33} + x^{34} + 0x^{35} + x^{36} + 0x^{37} + 0x^{38} + x^{39} + x^{40} \\ &+ 0x^{41} + x^{42} + x^{43} + 0x^{44} + 0x^{45} + 0x^{46} + x^{47} + 0x^{48} + 0x^{49} + 0x^{50} \\ &+ 0x^{51} + 0x^{52} + 0x^{53} + 0x^{54} + x^{55} + x^{56} + x^{57}, \end{aligned}$$

o polinômio recíproco é

$$\begin{aligned} \overleftarrow{h}(x) &= x^{57} + x^{56} + x^{55} + x^{50} + x^{47} + x^{43} + x^{42} + x^{40} + x^{39} + x^{36} + x^{34} + x^{33} + \\ &+ x^{31} + x^{29} + x^{28} + x^{27} + x^{25} + x^{24} + x^{23} + x^{22} + x^{19} + x^{18} + x^{14} + x^{12} + \\ &+ x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1 \end{aligned}$$

e a matriz teste de paridade de $\mathcal{C}$ é

$$H = \begin{bmatrix} 111000000010001101100101000011101111001100010101001111110100000 \\ 011100000001000110110010100001110111100110001010100111111010000 \\ 001110000000100011011001010000111011110011000101010011111101000 \\ 000111000000010001101100101000011101111001100010101001111110100 \\ 000011100000001000110110010100001110111100110001010100111111010 \\ 000001110000000100011011001010000111011110011000101010011111101 \end{bmatrix}$$

A matriz H^t com dimensão 63×6 é determinada pela troca da linha pela coluna da matriz H acima.

Passo 10) Rotular a *seq* utilizando o Passo 1);

Neste exemplo, analisaremos se o código BCH sobre F_{64} é capaz de reproduzir a sequência de DNA correspondente à sequência de direcionamento (SD) de certa proteína mitocondrial (não vamos entrar em detalhes biológicos aqui). Este passo determina as 24 permutações entre o alfabeto do código genético $N = \{A, C, G, T/U\}$ e o alfabeto do código BCH $\mathbb{F}_4 = \{0, 1, a, b\}$. Uma vez que a aplicação $N \to \mathbb{F}_4$ não é conhecida, a SD deve ser rotulada de acordo com as 24 permutações apresentadas abaixo:

$N \to \mathbb{F}_4$	$N \to \mathbb{F}_4$	$N \to \mathbb{F}_4$
01^{o} - $(A, C, G, T) = (0, 1, b, a)$	09^{o} - $(A, C, G, T) = (0, 1, a, b)$	17^{o} - $(A, C, G, T) = (0, a, 1, b)$
02^{o} - $(A, C, G, T) = (0, b, 1, a)$	10^{o} - $(A, C, G, T) = (0, b, a, 1)$	18^{o} - $(A, C, G, T) = (0, a, b, 1)$
03^{o} - $(A, C, G, T) = (1, 0, a, b)$	11^{o} - $(A, C, G, T) = (1, 0, b, a)$	19^{o} - $(A, C, G, T) = (1, b, 0, a)$
04^{o} - $(A, C, G, T) = (1, a, 0, b)$	12^{o} - $(A, C, G, T) = (1, a, b, 0)$	20^{o} - $(A, C, G, T) = (1, b, a, 0)$
05^{o} - $(A, C, G, T) = (a, 1, b, 0)$	13^{o} - $(A, C, G, T) = (a, 1, 0, b)$	21^{o} - $(A, C, G, T) = (a, 0, 1, b)$
06^{o} - $(A, C, G, T) = (a, b, 1, 0)$	14^{o} - $(A, C, G, T) = (a, b, 0, 1)$	22^{o} - $(A, C, G, T) = (a, 0, b, 1)$
07^{o} - $(A, C, G, T) = (b, 0, a, 1)$	15^{o} - $(A, C, G, T) = (b, 0, 1, a)$	23^{o} - $(A, C, G, T) = (b, 1, 0, a)$
08^{o} - $(A, C, G, T) = (b, a, 0, 1)$	16^{o} - $(A, C, G, T) = (b, a, 1, 0)$	24^{o} - $(A, C, G, T) = (b, 1, a, 0)$

Tabela 5 – 24 permutações para $\mathbb{F}_4$.

Consideremos a seguinte sequência:

ATGTTCAGGCACTCTTCTCGACTCCTAGCTCGCGCCACCACAATGGGGTGGCGTCGCCCCTTC

Cada uma das linhas da matriz abaixo utiliza uma das permutações 1 a 24 da Tabela 5 para rotular a sequência considerada:

$$P = \begin{bmatrix}
0abaa10bb101a1aa1a1b01a11a0b1a1b1b110110100abbbbabb1ba1b1111aa1 \\
0a1aab011b0babaabab10babba01bab1b1bb0bb0b00a1111a11b1ab1bbbbaab \\
1babb01aa010b0bb0b0a10b00b1a0b0a0a001001011baaaabaa0ab0a0000bb0 \\
1b0bba100a1ababbaba01abaab10aba0a0aa1aa1a11b0000b00a0ba0aaaabba \\
a0b001abb1a10100101ba10110ab101b1b11a11a1aa0bbbb0bb1b01b1111001 \\
a0100ba11bab0b00b0b1ab0bb0a1b0b1b1bbabbabaa01111011b10b1bbb00b \\
b1a110baa0b01011010ab01001ba010a0a00b00b0bb1aaaa1aa0a10a0000110 \\
b1011ab00aba1a11a1a0ba1aa1b0a1a0a0aabaababb10000100a01a0aaaa11a \\
0babb10aa101b1bb1b1a01b11b0a1b1a1a110110100baaaabaa1ab1a1111bb1 \\
01a11b0aab0b1b11b1ba0b1bb10ab1bababb0bb0b001aaaa1aaba1babbbb11b \\
1abaa01bb010a0aa0a0b10a00a1b0a0b0b001001011abbbbabb0ba0b0000aa0 \\
10b00a1bba1a0a00a0ab1a0aa01ba0ababaa1aa1a110bbbb0bbab0abaaaa00a \\
ab0bb1a001a1b1bb1b10a1b11ba01b101011a11a1aab0000b0010b101111bb1 \\
a1011ba00bab1b11b1b0ab1bb1a0b1b0b0bbabbabaa10000100b01b0bbbb11b \\
ba1aa0b110b0a0aa0a01b0a00ab10a010100b00b0bba1111a1101a010000aa0 \\
b0100ab11aba0a00a0a1ba0aa0b1a0a1a1aabaababb01111011a10a1aaaa00a \\
0b1bba011a0ababbaba10abaab01aba1a1aa0aa0a00b1111b11a1ba1aaaabba \\
01b11a0bba0a1a11a1ab0a1aa10ba1ababaa0aa0a001bbbb1bbab1abaaaa11a \\
1a0aab100b1babaabab01babba10bab0b0bb1bb1b11a0000a00b0ab0bbbbaab \\
10a00b1aab1b0b00b0ba1b0bb01ab0bababb1bb1b110aaaa0aaba0babbbb00b \\
ab1bb0a110a0b0bb0b01a0b00ba10b010100a00a0aab1111b1101b010000bb0 \\
a1b110abb0a01011010ba01001ab010b0b00a00a0aa1bbbb1bb0b10b0000110 \\
ba0aa1b001b1a1aa1a10b1a11ab01a101011b11b1bba0000a0010a101111aa1 \\
b0a001baa1b10100101ab10110ba101a1a11b11b1bb0aaaa0aa1a01a1111001
\end{bmatrix}.$$

Passo 11) Verificar se a *seq* é uma palavra do código de acordo com os padrões de erros estabelecidos: $D(a,b) = 0,\ D(a,b) = 1,\ D(a,b) = 2$;

a) $D(a,b) = 1$ nucleotídeo de diferença:

Neste caso, consideramos as 3 outras possibilidades de nucleotídeos em cada posição na sequência de DNA para cada permutação, resultando

em um total de 3 possibilidades de nucleotídeo em cada posição, multiplicados pelo comprimento da sequência n e pelas 24 possibilidades de permutações. Ou seja,

$$3 \times 63 \times 24 = 4536 \text{ possibilidades}$$

para cada sequência de DNA, então usamos a expressão 8.1. As palavras-código encontradas são armazenadas.

b) Para analisarmos este caso nos 24 casos de permutação, consideramos todas as combinações simples tomados 2 a 2 dos n nucleotídeos de comprimento da sequência, isto é, $C_{n,m} = \frac{n!}{m!(n-m)!}$. Então, sendo $n = 63$ e $m = 2$

$$C_{63,2} = \frac{63!}{2!(63-2)!} = 1953 \times 9 = 17577 \text{ possibilidades.}$$

de palavra-código para cada caso de permutação de cada sequência de DNA analisada. As palavras-código encontradas também são armazenadas.

Passo 12) Comparar todas as palavras do código que foram armazenadas no Passo 11) com a *seq* e explicitar onde os erros ocorreram;

Passo 13) Voltar para o Passo 6) e determinar outro $g(x)$;

Passo 14) Repetir do Passo 7) ao Passo 11) para o $g(x)$ encontrado do Passo 13), até que esgotem-se todas as possibilidades de $g(x)$;

Neste passo, o algoritmo determina todas as palavras-código encontradas com 0, 1 e 2 nucleotídeos de diferença através de todos os polinômios geradores relativos à distância mínima $1 \leq d_H \leq 63$ e armazena os resultados.

Passo 15) Voltar ao Passo 3) e escolher um outro $p(x)$, e, então, repetir do Passo 4) ao Passo 14), até esgotar todos os $p(x)$ do Passo 3);

Passo 16) Fim.

8.6 Resultados

No trabalho de Faria [3], o algoritmo foi aplicado com o padrão de distância de 1 nucleotídeo, obtendo 24 palavras-cóodigo que correspondem às 24 permutações apresentadas na tabela 5. As palavras-código são diferentes em termos do alfabeto $\mathbb{F}_4$ do código, porém são as mesmas em relação ao alfabeto $N = \{A, C, G, T\}$, o que significa que resultam em uma única sequência de DNA. Assim, é suficiente considerar o caso com o polinômio primitivo $p_{05}(x) = x^3 + ax^2 + ax + a$ e o gerador $g(x) = x^6 + x^5 + x^3 + x^2 + 1$ como no exemplo feito na seção 8.5. A sequência de DNA gerada está na figura abaixo.

$p_{05}(x) = x^3+ax^2+ax+a$ - $g_{05}(x) = x^6+x^5+x^3+x^2+1$

```
aaO:  M   F   R   H   S   S   R   L   L   A   R   A   T   T   M   G   W   R   R   P   F
ntO: ATG TTC AGG CAC TCT TCT CGA CTC CTA GCT CGC GCC ACC ACA ATG GGG TGG CGT CGC CCC TTC
RtO: 0ba bb1 0aa 101 b1b b1b 1a0 1b1 1b0 a1b 1a1 a11 011 010 0ba aaa baa 1ab 1a1 111 bb1
RtG: 0ba bb1 0aa 101 b1b b1b 1a0 1b1 1b0 a1b 1a1 a11 011 010 0ba aaa ba0 1ab 1a1 111 bb1
ntG: ATG TTC AGG CAC TCT TCT CGA CTC CTA GCT CGC GCC ACC ACA ATG GGG TGA CGT CGC CCC TTC
aaG:  M   F   R   H   S   S   R   L   L   A   R   A   T   T   M   G  sto  R   R   P   F
```

Figura 2 – Sequência de DNA (com um nucleotídeo diferente) gerada pelo código BCH $\langle x^6 + x^5 + x^3 + x^2 + 1 \rangle$, onde aaO = aminoácidos originais; ntO = nucleotídeos originais; RtO = rotulamento original; RtG = rotulamento gerado; ntG = nucleotídeos gerados; aaG = aminoácidos gerados. Fonte: [3].

Veja que o nucleotídeo diferente está destacado e gera um aminoácido errado. No contexto biológico, essa incompatibilidade é conhecida como polimorfismo de nucleotídeo único (SNP). Assim, uma possível interpretação é que ou a palavra do código gerada por um código BCH é um SNP em relação à sequência de DNA original correspondente ou vice-versa. No entanto, como essa incompatibilidade está dentro da capacidade de correção de erros do código, segue-se que é possível encontrar a posição e a magnitude a serem adicionadas nessa posição para reproduzir totalmente a sequência de DNA original.

9 CONCLUSÃO

O presente trabalho teve como principal objetivo explorar a Teoria de Códigos Corretores de Erros sobre corpos finitos, estudando algumas classes especiais de códigos. A saber: códigos lineares (classe de códigos mais utilizada na prática), códigos cíclicos e códigos BCH. Para atingirmos tal objetivo, exploramos a construção de corpos finitos, definimos a métrica de Hamming (métrica que utilizamos para medir a distância entre as palavras) e os parâmetros de um código. Também, aprendemos a codificar e decodificar mensagens.

Um outro objetivo deste trabalho foi apresentar uma interessante teoria desenvolvida sobre os códigos BCH em sequências de DNA. Para isso, apresentamos um algoritmo, que além de identificar uma possível estrutura algébrica para a construção de códigos corretores de erros, reproduzimos uma sequências de DNA gerada por um código BCH, possibilitando a realização de simulações computacionais eficientes de acordo com a aplicação de interesse.

Vale ressaltarmos que, da mesma forma que estudamos os códigos sobre a estrutura de corpos, uma possibilidade de estudo futuro seria estudarmos essa teoria sobre a estrutura de anéis, o que pode ser encontrado em [3].

REFERÊNCIAS

1 COUTINHO, M. de A. N., **Corpos Finitos e Códigos Corretores de Erros**, Trabalho de Conclusão de Curso do Bacharelado em Matemática. Universidade Federal de Juiz de Fora, 2014. Disponível em: https://www2.ufjf.br/matematica//files/2014/02/TCC_Mariana.pdf. Acesso em: 3 jan. 2023.

2 FARIA, L.; ROCHA, A.S.L.; KLEINSCHMIDT, J.; PALAZZO, R.; SILVA-FILHO, M., **DNA sequences generated by BCH codes over GF(4)**. Electronics Letters. 46 (3). pp. 203 - 204, 2010. Disponível em: https://doi.org/10.1049/el.2010.3397. Acesso em 4 jan. 2023.

3 FARIA, L., **Existências de códigos corretores de erros e protocolos de comunicação em sequências de DNA**. Tese de Doutorado em Engenharia Elétrica - Universidade Estadual de Campinas, São Paulo, 2011. Disponível em: https://repositorio.unicamp.br/acervo/detalhe/807840. Acesso em: 4 jan. 2023.

4 FARIA, L.; ROCHA, A.; KLEINSCHMIDT, J.; SILVA-FILHO, M., BIM, E. , et al. **Is a Genome a Codeword of an Error-Correcting Code?**. PLOS ONE 7(5): e36644, 2012. Disponível em: https://doi.org/10.1371/journal.pone.0036644. Acesso em 4 jan. 2023.

5 GONÇALVES, A. **Introdução à Álgebra**. 5. ed. Rio de Janeiro: IMPA, 2011

6 HEFEZ, A.; VILLELA, M. L. T. **Códigos Corretores de Erros**. 2. ed. Rio de Janeiro: IMPA, 2008.

7 HUNGERFORD, T. **Algebra**. Springer Science & Business Media, 2012.

8 LIDL, R.; NIEDERREITER, H. **Introduction to finite fields and their applications**. Cambridge university press, 1994.

9 LIDL, R.; NIEDERREITER, H.. **Finite fields**. Cambridge university press, 1997.

10 MACWILLIAMS, F.; SLOANE, N., **The theory of error correcting codes**. Elsevier, 1977.

11 MILIES, C. P. **Breve introdução à teoria dos códigos corretores de erros**. Colóquio de Matemática da Região Centro-Oeste, SBM, p. 22, 2009. Disponível em: http://www.kurims.kyotou.ac.jp/EMIS/journals/em/docs/coloquios/NE-1.04.pdf. Acesso em: 30 set. 2022.

12 MOTTA, B. **Tópicos em Álgebra II: Códigos Corretores de Erros**. Notas de aula. Juiz de Fora: UFJF, 2022.

13 SERCIO, F. **Álgebra IV** Notas de aula. Juiz de Fora: UFJF, 2021.

14 VENTURA, J. **Notas de Combinatória e Teoria de Códigos**, 2014. Disponível em: `https://www.math.tecnico.ulisboa.pt/~jventura/CTC/NotasCTC.pdf`. Acesso em: 29 dez. 2022.