UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Faculdade de Matemática
Av. João Naves de Àvila, 2121, Bloco 1F - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: +55 (34) 3239-4158/4156/4126 - www.famat.ufu.br - famat@ufu.br

ATA DE DEFESA - GRADUAÇÃO

Curso de Graduação em:	Matemática				
Defesa de:	Trabalho de Conclusão de Curso 2 (FAMAT31804)				
Data:	30/11/2023	Hora de início:	10h00min	Hora de encerramento:	11h30min
Matrícula do Discente:	11811MAT038				
Nome do Discente:	Wanderson Gustavo Jacó de Resende				
Título do Trabalho:	**Elementos da Teoria dos Códigos Corretores de Erros**				
A carga horária curricular foi cumprida integralmente?	(x) Sim ( ) Não				

Reuniu-se na Sala 1F119, Campus Santa Mônica, da Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Curso de Graduação em Matemática, assim composta pelos Professores: Prof. Dr. Cícero Fernandes de Carvalho – FAMAT/UFU, Prof. Dr. Josimar Joao Ramirez Aguirre- FAMAT/UFU e o Prof. Dr. Victor Gonzalo Lopez Neumann – FAMAT/UFU, orientador do candidato.

Iniciando os trabalhos, o presidente da mesa, Prof. Dr. Victor Gonzalo Lopez Neumann, apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao discente a palavra, para a exposição do seu trabalho. A duração da apresentação do discente e o tempo de arguição e resposta foram conforme as normas do curso.

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

(x) Aprovado ( ) Reprovado

Nota: 90

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

Documento assinado eletronicamente por **Josimar João Ramirez Aguirre**, **Professor(a) do Magistério Superior**, em 30/11/2023, às 12:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Cícero Fernandes de Carvalho**, **Professor(a) do Magistério Superior**, em 30/11/2023, às 12:42, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann**, **Professor(a) do Magistério Superior**, em 30/11/2023, às 14:35, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5007155** e o código CRC **C605CC42**.

Referência: Processo nº 23117.080371/2023-50 SEI nº 5007155

Universidade Federal de Uberlândia
Faculdade de Matemática

Bacharelado em Matemática

ELEMENTOS DA TEORIA DOS CÓDIGOS CORRETORES DE ERROS

Wanderson Gustavo Jacó de Resende

Uberlândia-MG
2023

Wanderson Gustavo Jacó de Resende

ELEMENTOS DA TEORIA DOS CÓDIGOS CORRETORES DE ERROS

Trabalho de conclusão de curso apresentado à Coordenação do Curso de Bacharelado em Matemática como requisito parcial para obtenção do grau de Bacharel em Matemática.

Orientador: Prof. Dr. Cícero Fernandes de Carvalho

Uberlândia-MG

2023

Universidade Federal de Uberlândia
Faculdade de Matemática

Coordenação do Curso de Bacharelado em Matemática

A banca examinadora, conforme abaixo assinado, certifica a adequação deste trabalho de conclusão de curso para obtenção do grau de Bacharel em Matemática.

Uberlândia, ____ de _____ de 20____

BANCA EXAMINADORA

_____

Prof. Dr. Cícero Fernandes de Carvalho

_____

Prof. Dr. Josimar Joao Ramirez Aguirre

_____

Prof. Dr. Victor Gonzalo Lopez Neumann

Uberlândia-MG

2023

Agradecimentos

Agradeço primeiramente a Deus, por permitir-me completar essa etapa tão importante na minha vida.

À minha mãe e pai que sempre fizeram de tudo para que eu pudesse me dedicar integralmente aos estudos.

Ao meu irmão, familiares e amigos, pelo constante apoio, motivação e por sempre acreditarem no meu potencial.

À Universidade Federal de Uberlândia, por proporcionar um estudo gratuito e de qualidade.

Aos docentes da Faculdade de Matemática, por compartilharem um pouco de seu conhecimento e experiência.

Ao meu orientador Cícero Carvalho pela paciência, pelos ensinamentos passados e por acreditar no meu potencial.

Ao professor Victor Gonzalo por se encarregar como orientador na defesa do meu TCC e pela presença na banca.

Ao professor Josimar Ramirez por fazer parte da banca examinadora e pelos ensinamentos ao longo da graduação.

Ao Bashara por estar sempre presente na graduação durante os melhores e piores momentos, por sempre me fortalecer e por tornar esse ciclo da minha vida algo satisfatório.

Resumo

Neste trabalho desenvolveremos um estudo na área da Álgebra Abstrata focado na Teoria dos Códigos Corretores de Erros, que essencialmente estuda a criação de codificadores e decodificadores de informações cada vez mais precisos em relação a erros ocorridos durante a transmissão e a recepção de dados das diversas maneiras possíveis.

Palavras-chave: Álgebra Abstrata, Teoria de Códigos, codificação, decodificação, corpos finitos.

Abstract

In this work, we will develop a study in the field of Abstract Algebra focused on the Theory of Error-Correcting Codes. This theory essentially explores the creation of increasingly precise encoders and decoders for information in relation to errors that may occur during the transmission and reception of data from many different means.

Keywords: Abstract Algebra, code theory, codification, decoding, finite fields.

Sumário

1. Introdução

Os Códigos Corretores de Erros são utilizados para transmitir ou armazenar informações de modo confiável. O seu uso ocorre quando são identificados erros durante uma transmissão, causados por alguma interferência no canal utilizado, fazendo com que o receptor não consiga identificar a mensagem original que lhe foi enviada, ou então, quando não for possível recuperar uma informação armazenada em algum meio de armazenamento de dados.

Tal ferramenta está presente, também, em comunicações via satélite, comunicações internas de um computador, navegações pela internet, entre várias outras situações.

A teoria sobre códigos corretores de erros nasceu em 1948, fundada pelo matemático C. E. Shannon, foi bastante desenvolvida pelos matemáticos da época e, a partir dos anos 70, despertou o interesse de engenheiros que ajudaram a continuar no desenvolvimento da mesma. Hoje, sempre que se deseja transmitir dados com confiabilidade, os códigos corretores são utilizados.

Neste trabalho, exploramos aplicações para conceitos abstratos bastante conhecidos na matemática, tendo como objetivo final e principal definir e dar propriedades de códigos lineares, e em particular, de códigos cíclicos. Iremos também estudar os resultados iniciais de codificação e decodificação dos códigos lineares, e cíclicos em particular.

No primeiro capítulo abordaremos conceitos de Álgebra necessários para o entendimento do tema, tais como: homomorfismo, característica de um corpo finito, potências da característica de um corpo finito, a existência de polinômios irredutíveis e por fim a classificação dos corpos finitos culminando na unicidade dos corpos finitos.

No Segundo capítulo iremos introduzir o que são os códigos lineares, iremos definir a matriz geradora de um código para que possamos estudar mais afundo a questão de codificação e decodificação desses códigos.

Por fim, no terceiro capítulo iremos abordar o conceito de códigos cíclicos e como funciona a sua codificação e decodificação.

Esta monografia se baseia numa leitura do livro "Códigos Corretores de Erros", dos autores Abramo Hefez e Maria Lúcia T.Villela, que a referência principal deste trabalho (v. [2]). Para conceitos de Álgebra Comutativa, utilizamos o livro clássico (v. [1]).

2. CORPOS FINITOS

Iniciaremos o nosso estudo com a apresentação de alguns conceitos importantes para o desenvolvimento e classificação de corpos finitos que serão de extrema importância para o entendimento de códigos lineares e cíclicos mais adiantes.

2.1 CARACTERÍSTICAS DE UM CORPO

Neste trabalho iremos trabalhar com o fato de que todo anel mencionado será um anel comutativo com unidade.

Definição 2.1. *(Homomorfismo) Sejam A e B dois anéis (ou corpos). Uma função $f : A \to B$ será chamada homomorfismo se, para todos os elementos a e b em A, vale que*

$$\begin{aligned} &(i) \quad f(a+b) = f(a) + f(b), \\ &(ii) \quad f(a \cdot b) = f(a) \cdot f(b), \\ &(iii) \quad f(1) = 1. \end{aligned}$$

Proposição 2.2. *Seja $f : A \to B$ um homomorfismo entre os anéis A e B e sejam $a,b \in A$. Temos que*

i) $f(0) = 0$.

ii) $f(-a) = -f(a)$.

iii) $f(a-b) = f(a) - f(b)$.

iv) Se $a \in A$ é *invertível*, então $f(a)$ é *invertível* e $f(a^{-1}) = (f(a))^{-1}$.

v) Se f é *bijetora*, então a função f^{-1}, *inversa* de f, é um homomorfismo.

vi) Se A e B são corpos, então f é injetora e $f(A)$ é um subcorpo de B.

Demonstração. i) Temos que $f(0) = f(0+0) = f(0) + f(0)$, portanto, cancelando $f(0)$ nos extremos dessa igualdade, obtemos que $0 = f(0)$.

ii) Temos que $0 = f(0) = f(a + (-a)) = f(a) + f(-a)$. Somando -$f(a)$ aos extremos da igualdade anterior, obtemos que $-f(a) = f(-a)$.

iii) A partir de (ii) e usando que $a - b = a + (-b)$ obtemos o resultado.

iv) Usando que a é invertível, temos que $(f(a))^{-1} = f(a^{-1})$, pois

$$1 = f(1) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1}).$$

v) Se f é um homomorfismo bijetor, segue que $f^{-1}(1) = 1$, pois, $f(1) = 1$, por definição. Sejam $c, d \in B$, $a = f^{-1}(c)$ e $b = f^{-1}(d)$, temos que

$$f^{-1}(c + d) = f^{-1}(f(a) + f(b)) = f^{-1}(f(a + b)) = a + b = f^{-1}(c) + f^{-1}(d)$$

e

$$f^{-1}(c \cdot d) = f^{-1}(f(a) \cdot f(b)) = f^{-1}(f(a \cdot b)) = a \cdot b = f^{-1}(c) \cdot f^{-1}(d).$$

vi) Vamos supor que A e B sejam corpos. Se $f(a) = f(b)$, por (iii), segue que $f(a - b) = f(a) - f(b) = 0$. Se $a \neq b$, então $a - b$ seria invertível. Por (iv), $f(a - b)$ seria invertível, e portanto, não nulo; chegando em um absurdo. Assim sendo, $a = b$ e, portanto, f é injetora. Para provar que $f(A)$ é um subcorpo de B, temos que dados $a, b \in A$ $f(a)+f(b) = f(a+b)$ e $f(a)f(b) = f(a \cdot b)$, no qual $f(A)$ é subanel de B. Mas, se $a \neq 0$, temos $f(a)f(a^{-1}) = f(a \cdot a^{-1}) = f(1) = 1$. Logo, $f(a)$ é invertível e $f(a)^{-1} = f(a^{-1})$ e portanto, $f(A)$ é subcorpo de B.

□

Nesse trabalho denotamos por $\mathbb{N}$ o conjunto dos inteiros positivos.

Definição 2.3. *Um homomorfismo bijetor de corpos será chamado de isomorfismo. Dois corpos serão ditos isomorfos se existir um isomorfismo entre eles.*

Definição 2.4. *Seja K um corpo finito com elemento unidade 1. Considere o seguinte conjunto*

$$\Lambda_K = \{n \in \mathbb{N}; n1 := \underbrace{1 + \cdots + 1}_{n \text{ vezes}} = 0\} \subset \mathbb{N}.$$

Proposição 2.5. *Λ_K é um conjunto não vazio.*

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

Definição 2.6. *Define se a característica de um corpo finito K, como sendo o inteiro positivo*

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

Se um corpo F é subcorpo de um corpo K, então $car(K) = car(F)$, pois $\Lambda_F = \Lambda_K$. Temos também que K é um espaço vetorial sobre F.

Proposição 2.7. *Seja K um corpo finito, então $car(K)$ é um número primo.*

Demonstração. Seja $m = car(k)$ e suponhamos que m não seja primo. Logo, existem m_1 e m_2, inteiros positivos maiores do que 1 e menores do que m, tais que $m = m_1 \cdot m_2$. Então,

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

Temos que K é corpo e como todo corpo é um domínio de integridade, chegamos que $m_1 1 = 0$ ou $m_2 1 = 0$, ou seja, uma contradição. Logo, m é um inteiro positivo primo. □

Dado um elemento $a \in K$ e um inteiro m definimos $m \cdot a := 0$, se $m = 0$, $m \cdot a := a + \cdots + a$, onde temos m parcelas na soma, se $m > 0$ e, se $m \langle 0$ definimos $m \cdot a = -((-m) \cdot a)$.

Proposição 2.8. *Seja K um corpo finito com $car(K) = p$. Se para $m \in \mathbb{Z}$ e $a \in K$ tem se que $ma = 0$, então m é um múltiplo de p ou $a = 0$.*

Demonstração. Suponhamos que $ma = 0$, isto é, $(m1) \cdot a = 0$. Como K é um corpo, temos que $m1 = 0$ ou $a = 0$. Agora, basta mostrar que, se $m1 = 0$, então m é um múltiplo de p. De fato, suponhamos que $m1 = 0$. Usando o algoritmo da divisão, temos que $m = \lambda p + r$, onde $0 \leq r < p$. Logo,

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

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

Teorema 2.9. *Seja K um corpo finito com $car(K) = p$, onde p é um número primo. Então, K contém um subcorpo isomorfo a $\mathbb{Z}_p$. Em particular, K tem p^n elementos para algum número natural n.*

Demonstração. Considere a seguinte aplicação

$$\begin{aligned} \varphi : \mathbb{Z}_p &\longrightarrow K \\ [n] &\longmapsto n1 \end{aligned}$$

Preliminarmente devemos mostrar que essa definição está bem definida em nosso ambiente. De fato, se $[n] = [m]$, no qual m e n são dois inteiros, então existe um inteiro λ tal que $n = m + \lambda p$. Logo,

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

Agora, pela Proposição 2.2(vi), temos que $\varphi(\mathbb{Z}_p)$ é um subcorpo de K, isomorfo a $\mathbb{Z}_p$. Consequentemente, temos que K é um espaço vetorial sobre $\mathbb{Z}_p$ e como K é finito, segue que tem dimensão finita sobre $\mathbb{Z}_p$. Agora, seja $\alpha_1, \ldots, \alpha_n$ uma base de K sobre $\mathbb{Z}_p$. Então, todo elemento de K se escreve de modo único da seguinte forma

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

com os $\lambda_i \in \mathbb{Z}_p$, com $i = 1, \ldots, n$. Contando esses elementos, segue que $|K| = p^n$.

□

2.2 Potências da Característica

Neste trabalho iremos definir K como sendo um corpo finito de característica p e seja $q = p^r$, para algum inteiro positivo r.

Proposição 2.10. *Se $a, b \in K$, temos que*

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

Demonstração. Usando o Binômio de Newton, temos que

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

Como $p|\binom{p}{i}$, para $i = 1, \ldots, p-1$, temos

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

Assim sendo, a prova segue por meio de indução matemática, observando que

$$(a \pm b)^{p^r} = ((a \pm b)^{p^{r-1}})^p = (a^{p^{r-1}} \pm b^{p^{r-1}})^p = a^{p^r} \pm b^{p^r}.$$

□

Observação 2.11. *Utilizando o método da indução finita pode-se generalizar a proposição acima e mostrar que dados $a_1, \ldots, a_n$ num corpo finito K, de característica p, e dada uma potência q de p, temos que*

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

A partir disso, é fácil verificar que se $P(X) = a_0 + a_1X + \cdots + a_nX^n \in K[X]$, então

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

Colorário 2.12. *A aplicação f_q é um isomorfismo de corpos, onde*

$$\begin{aligned} f_q : K &\longrightarrow K \\ x &\longmapsto x^q \end{aligned}$$

Demonstração. Já sabemos que

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

e usando a Proposição 2.10,

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

Como $f_q(1) = 1$, segue que f_q é um homomorfismo. Agora, usando a Proposição 2.2(vi), temos f_q é injetora e, como K é finito, segue que f_q é bijetora. Portanto f_q é um isomorfismo. □

Colorário 2.13. *Sejam F um corpo de característica $p > 0$ e q uma potência inteira de p. O conjunto $K = \{\alpha \in F; \alpha^q - \alpha = 0\}$ é um subcorpo de F.*

Demonstração. Basta mostrar que se $\alpha, \beta \in K$, onde $\beta \neq 0$, então $\alpha - \beta$ e $\frac{\alpha}{\beta}$ estão em K. Agora usando a Proposição 2.10 temos que o resultado segue de imediato. Portanto, K é subcorpo de F. □

Proposição 2.14. *Sejam $P(X) \in K[X]$ e K um corpo finito de característica p. Temos que $P'(X) = 0$ se, somente se, existe um polinômio $Q(X) \in K[X]$ tal que $P(X) = Q(X)^p$.*

Demonstração. Se $P(X) = a_0 + a_1X + \cdots + a_iX^i + \cdots + a_nX^n$ é tal que $P'(X) = 0$, segue que $ia_i = 0$ para todo $i = 1, \ldots, n$. Consequentemente, pela Proposição 2.8, temos que i é um múltiplo de p sempre que $a_i \neq 0$, ou seja,

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

Escolhendo $b_i \in K$ tal que $b_i^p = a_{ip}$, o que é possível tomando $q = p$ no Corolário 2.12, o resultado segue se tomamos $Q(X) = b_0 + b_1X + b_2X^2 + \cdots + b_sX^s$

A recíproca segue imediatamente das regras de derivação de potências de polinômios. □

Proposição 2.15. *O polinômio $F(X) = X^q - X$ não possui fatores irredutíveis múltiplos em $K[X]$.*

Demonstração. Pelo fato de $F'(X) = qX^{q-1} - 1 = -1$, temos que $F(X)$ e $F'(X)$ são primos entre si. Suponha, por absurdo, que exista um fator irredutível $G(X)$ de $F(X)$ tal que $F(X) = G(X)^2H(X)$. Então teríamos que $F'(X) = 2G(X)H(X) + G(X)^2H'(X)$, e logo $G(X)$ seria fator de $F'(X)$, em contradição com o fato de $F(X)$ e $F'(X)$ serem primos entre si. □

Lema 2.16. *Para todo $\alpha \in K^*$, onde $K^* = K \setminus \{0\}$, temos que*

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

Demonstração. Seja $\alpha \in K^*$ e considere a aplicação

$$\begin{aligned} \varphi_\alpha : K^* &\longrightarrow K^* \\ a &\longmapsto \alpha a \end{aligned}$$

É imediato verificar que φ_α é injetora, como K^* é finito, temos que φ_α é bijetora. Se $K^* = \{a_1, \ldots, a_{q-1}\}$, temos então que

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

consequentemente,

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

Portanto,

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

□

Uma importante consequência do resultado anterior é a seguinte.

Colorário 2.17. *Para todo $\alpha \in K$ e para todo $i \in \mathbb{N}$, temos que $\alpha^{q^i} = \alpha$.*

Demonstração. Do lema anterior temos que $\alpha^q = \alpha$ para todo $\alpha \in K$. O resultado do corolário segue usando indução. □

Colorário 2.18. *Seja F uma extensão de K. Então os elementos de K são os elementos de F que são raízes de $X^q - X = 0$, enquanto que os elementos do subcorpo $\mathbb{Z}_p$ de F são as raízes do polinômio $X^p - X = 0$*

Demonstração. Pelo corolário anterior, temos que os elementos de K são raízes do polinômio $X^q - X$. Porém esse polinômio, tendo grau q, tem no máximo q raízes, logo, as suas raízes são todos os elementos de K. A demonstração da segunda afirmação é análoga à primeira considerando $\mathbb{Z}_p$ ao invés de K. □

Definição 2.19. *A ordem de $\alpha \in K^*$ é o inteiro positivo*

$$ord\ \alpha = min\{n \in \mathbb{N}; \alpha^n = 1\}.$$

Proposição 2.20. *Seja $\alpha \in K^*$. Se para algum inteiro positivo m temos que $\alpha^m = 1$, então ord $\alpha \mid m$. Em particular, ord $\alpha \mid (q-1)$.*

Demonstração. Usando o algoritmo da divisão, temos $m = (\text{ord } \alpha)s + r$, para alguns inteiros $s \geq 0$ e $0 \leq r \langle \text{ord } \alpha$. Portanto,

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

o que, pela minimalidade de ord α, implica que $r = 0$; logo, ord $\alpha \mid m$. Por último, usando o Lema 2.16, temos que $\alpha^{q-1} = 1$. Portanto, pelo que acabamos de provar, ord $\alpha \mid (q-1)$. □

Proposição 2.21. *Sejam α e β elementos de K tais que $MDC(ord\ \alpha, ord\ \beta) = 1$. Então ord $\alpha\beta =$ ord $\alpha \cdot$ ord β.*

Demonstração. Considere $m = \text{ord}\ \alpha$ e $n = \text{ord}\ \beta$. Temos então que

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

Em contrapartida, se $(\alpha\beta)^t = 1$, então

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

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

Portanto, pela proposição anterior, temos que $n \mid tm$ e $m \mid tn$. Como $MDC(m,n) = 1$, segue que $m \mid t$ e $n \mid t$. Novamente usando o fato de que $MDC(m,n) = 1$, segue que $mn \mid t$, provando que $mn = min\{t > 0; (\alpha\beta)^t = 1\}$; concluindo assim que ord $\alpha\beta = mn$. □

Proposição 2.22. *Sejam $\alpha \in K^*$ e $i \in \mathbb{N}$. Suponhamos que ord $\alpha = m$, então*

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

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

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

Ou seja, t é o menor inteiro positivo tal que $m \mid it$; dito de outra forma, it é o menor múltiplo simultaneamente de m e de i. Logo, $it = MMC(m,i)$, ou seja,

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

□

2.3 POLINÔMIOS IRREDUTÍVEIS

Nesta seção iremos apresentar dois teoremas e um corolário de suma importância para que possamos no final enunciar e demonstrar o teorema central dessa seção que nos assegurá a existência de polinômios irredutíveis de qualquer grau com coeficientes num corpo finito arbitrário.

Proposição 2.23. *Seja $f(X)$ um polinômio mônico irredutível em $K[X]$, de grau d. Considere o corpo $F = K[X]/(f(X))$. Temos que*

i) $1, [X], [X^2], \ldots, [X^{d-1}]$ *formam uma base de F sobre K.*

ii) $[X]^{q^d} = [X]$ *em F.*

iii) $f(X)$ *divide* $X^{q^d} - X$ *em $K[X]$.*

iv) Os elementos $[X], [X]^q, \ldots, [X]^{q^{d-1}}$ *de* F *são distintos e são as raízes de* $f(X)$ *em* F.

Antes de demonstrarmos essa proposição vamos nos atentar a seguinte observação:

Observação 2.24. *Seja* F *uma extensão de um corpo* K. *Por causa da unicidade do quociente e do resto na divisão de polinômios em* $F[X]$ *temos que dados dois polinômios* $f(X)$ *e* $g(X)$ *com coeficientes em* K, *o quociente e o resto de sua divisão em* $F[X]$ *são os mesmos que em* $K[X]$. *A partir disso, e pelo Algoritmo de Euclides temos que o* $MDC(f(X), g(X))$, *como polinômios em* $F[X]$, *se encontra em* $K[X]$ *e coincide com o máximo divisor comum de* $f(X)$ *e* $g(X)$, *como polinômios em* $K[X]$.

Agora, vamos para a demonstração da proposição anterior.

Demonstração. i) Dado $g(X) \in K[X]$, fazendo a divisão euclidiana de $g(X)$ por $f(X)$, encontramos $q(X), r(X) \in K[X]$ tais que $g(X) = q(X)f(X)+r(X)$, com $r(X) = \sum_{i=0}^{d-1} a_i X^i$. Tomando as classes na expressão de $g(X)$ vemos que as classes $[X^i]$, com $i = 0, \ldots, d-1$ geram F como K-espaço vetorial. E se $\sum_{i=0}^{d-1} a_i[X^i] = [0]$ então $f(X) \mid \sum_{i=0}^{d-1} a_i X^i$ o que só é possível se $a_i = 0$ para todo $i = 0, \ldots, d-1$. Isso mostra que $\{1, [X], [X^2], \ldots, [X^{d-1}]\}$ é uma base para F como K-espaço vetorial.

ii) Temos que F é um corpo finito com q^d elementos, logo, pelo Corolário 2.17, temos que $[X]^{q^d} = [X]$.

iii) Imediato de (ii).

iv) Considere o polinômio

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

Temos de (ii) que

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

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

$$((Y - [X]^{q^{d-1}})(Y - [X]) \cdots (Y - [X]^{q^{d-2}}))^q = (g(Y))^q.$$

Assim, $g(Y^q) = (g(Y))^q$ e portanto se $g(Y) = b_0 + b_1 Y + \cdots + b_{d-1}Y^{d-1} + Y^d$, temos que $b_i^q = b_i$ para todo $i = 0, \ldots, d-1$. Sendo assim, pelo Corolário 2.18, segue que $g(Y) \in K[Y]$.

Como $f(Y), g(Y) \in K[Y]$ possuem uma raiz em comum na extensão F de K, segue que o seu máximo divisor comum em $F[Y]$ é não constante e pertence a $K[Y]$(Observação 2.24). Como $f(Y)$ é irredutível e mônico, ele coincide com o $MDC(f(Y), g(Y))$, logo, $f(Y)$ divide $g(Y)$. Agora, como $f(Y)$ e $g(Y)$ são polinômios mônicos de mesmo grau, eles devem ser iguais.

Agora sabemos de (iii) que $g(Y) = f(Y)$ divide $Y^{q^d} - Y$, que, pela Proposição 2.15, não tem fatores múltiplos na extensão F de K, logo, as raízes $[X], [X]^q, \ldots, [X]^{q^{d-1}}$ de $g(Y)$ são duas a duas distintas, provando o que foi enunciado.

□

Observação 2.25. *Note que com a proposição anterior fica provado que, se* $[X] \in K[X]/(f(X))$ *com* $f(X) \in K[X]$ *irredutível de grau* d*, então*

$$d = \min\{j \in \mathbb{N}; [X]^{q^j} = \overline{X}\}. \tag{2.1}$$

Proposição 2.26. *Seja* n *um inteiro positivo. Em* $K[X]$ *temos a seguinte igualdade:*

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

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

Demonstração. Seja $f(X) \in K[X]$ um polinômio mônico irredutível de grau d. Como $X^{q^n} - X$ não possui fatores múltiplos (lembre-se da Proposição 2.15), então nos resta provar a seguinte asserção:

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

Vamos supor inicialmente que $f(X) \mid (X^{q^n} - X)$. Como $f(X) \mid (X^{q^n} - X)$(Pela Proposição 2.23 (iii)), segue que $f(X)$ divide $MDC(X^{q^n} - X, X^{q^d} - X)$; logo, pelo Exemplo 3.2 do livro ([2]), $f(X) \mid (X^{q^e} - X)$, onde $e = MDC(n, d) \leq d$. Posto isso, $[X]^{q^e} = [X]$, o que pela Proposição 2.23 (iv) só é possível se $e \geq d$. Verifica-se, então, que $d = e = MDC(n, d)$, e portanto, $d \mid n$.

Reciprocamente, se d divide n, temos que $(X^{q^d} - X) \mid (X^{q^n} - X)$ (veja Problema 3.2.4 do livro ([2])). Como $f(X) \mid (X^{q^d} - X)$ (pela Proposição 2.23 (iii)), segue que $f(X) \mid (X^{q^n} - X)$. □

Colorário 2.27. *Seja* $I(n)$ *o número de polinômios mônicos irredutíveis de grau* n *em* $K[X]$*. Temos que*

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

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

Observação 2.28. *A fórmula do corolário acima nos permite calcular recursivamente o valor de* $I(n)$ *num corpo finito qualquer.*

Teorema 2.29. *Seja* K *um corpo finito qualquer. Para cada número natural* n*, existe pelo menos um polinômio irredutível de grau* n *em* $K[X]$*.*

Demonstração. Para $n = 1$, o resultado é direto, pois o polinômio X é irredutível. Agora, suponhamos que $n > 1$. Sejam $1 = d_1 < \cdots < d_s < n$, com $s \geq 1$, os divisores de n.

Escrevendo $q = |K|$ e usando duas vezes o corolário acima, temos que

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

$$\sum_{i=1}^{s}(\sum_{d|d_i} dI(d)) + nI(n) = \sum_{i=1}^{s} q^{d_i} + nI(n) < \sum_{i=0}^{d_s} q^i + nI(n) =$$

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

Portanto,

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

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

$$nI(n) > q^n - q^{\frac{n}{2}+1} = q^n(1 - q^{-\frac{n}{2}+1}), \tag{2.2}$$

acarretando em $I(n) > 0$. □

2.4 Classificação dos Corpos Finitos

Teorema 2.30 (Existência de Corpos Finitos)**.** *Para todos os números inteiros positivos p e n, com p primo, existe um corpo com p^n elementos.*

Demonstração. Pelo Teorema 2.29, existe, para todo primo positivo p e todo inteiro positivo n um polinômio irredutível $f(X) \in \mathbb{Z}_p[X]$ de grau n. Logo, o corpo $K = \mathbb{Z}_p[X]/(f(X))$ é um dos corpos procurados, pois tem p^n elementos. □

Exemplo 2.31. *Consideremos o problema de construir um corpo com $19.683 = 3^9$ elementos. Isso pode ser realizado determinando um polinômio de grau 9 irredutível sobre $\mathbb{F}_3$, o que é uma tarefa de dificuldade considerável. No entanto, se considerarmos o polinômio $X^3 - X - 1$, este é irredutível em $\mathbb{F}_3[X]$, pois em $\mathbb{F}_3$ esse polinômio não tem raízes (note que $\alpha^3 - \alpha = 0$ para todo $\alpha \in \mathbb{F}_3$). Portanto, $K = \mathbb{F}_3[X]/(X^3 - X - 1)$ é um corpo com $3^3 = 27$ elementos. Para construir um corpo F com $19.683 = 27^3$ elementos, basta achar um polinômio irredutível $p(Y)$ de grau 3 em $K[Y]$ e tomar $F = K[Y]/(p(Y))$. Para isso, considere a função*

$$\begin{aligned} \varphi : K &\longrightarrow K \\ \beta &\longmapsto \beta^3 - \beta \end{aligned}$$

É fácil verificar que φ é uma aplicação $\mathbb{F}_3$-linear, cujo núcleo é $\mathbb{F}_3$. Portanto, φ não é injetora e, consequentemente, não é sobrejetora. Se tomarmos $\gamma \in K \setminus Im(\varphi)$, então certamente o polinômio $p(Y) = Y^3 - Y - \gamma$ não terá raízes em K e, portanto, será irredutível em $k[Y]$. Vamos então determinar $Im(\varphi)$.

Usando as relações abaixo,

1. $\overline{X^6 - X^2} = \overline{2X + 1}$,
2. $\overline{X^3 - X} = \overline{1}$,
3. $\overline{X^6 + X^2} = \overline{-X^2 - X + 1}$,
4. $\overline{X^3 + X} = \overline{2X + 1}$.

Podemos escrever os elementos de K na tabela a seguir. Esses elementos tem, em cada linha, a mesma imagem por φ, que é indicada na última coluna da direita.

α	α	α	$\varphi(\alpha)$
$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{X}$	$\overline{X+1}$	$\overline{X+2}$	$\overline{1}$
$\overline{2X}$	$\overline{2X+1}$	$\overline{2X+2}$	$\overline{2}$
$\overline{X^2}$	$\overline{X^2+1}$	$\overline{X^2+2}$	$\overline{2X+1}$
$\overline{X^2+X}$	$\overline{X^2+X+1}$	$\overline{X^2+X+2}$	$\overline{2X+2}$
$\overline{X^2+2X}$	$\overline{X^2+2X+1}$	$\overline{X^2+2X+2}$	$\overline{2X}$
$\overline{2X^2}$	$\overline{2X^2+1}$	$\overline{2X^2+2}$	$\overline{X+2}$
$\overline{2X^2+X}$	$\overline{2X^2+X+1}$	$\overline{2X^2+X+2}$	$\overline{X}$
$\overline{2X^2+2X}$	$\overline{2X^2+2X+1}$	$\overline{2X^2+2X+2}$	$\overline{X+1}$

Portanto, o polinômio $p(Y) = Y^3 - Y - \overline{X^2}$ não tem raízes em K, sendo assim irredutível em $K[Y]$.

Teorema 2.32 (Unicidade dos Corpos Finitos)**.** *Dois corpos finitos com o mesmo número de elementos são isomorfos.*

Demonstração. Seja L um corpo finito com p^n elementos, logo, a característica de L é p e ele contém um corpo isomorfo a $\mathbb{Z}_p$ (de acordo com o Teorema 2.9). Logo, L é um espaço vetorial sobre $\mathbb{Z}_p$ de dimensão n.

Como L é um corpo finito com p^n elementos, sabemos que a equação $X^{p^n} - X$ tem todas as suas raízes em L e todos os elementos de L são as raízes desse polinômio. (usando o Corolário 2.18)

Seja $f(X) \in \mathbb{Z}_p[X]$ um polinômio mônico irredutível de grau n, cuja existência está garantida pelo Teorema 2.29. Agora, pela Proposição 2.23(iii), sabemos que $f(X)$ divide $X^{p^n} - X$ em $\mathbb{Z}_p[X]$, logo, existe β em L tal que $f(\beta) = 0$. Os elementos $1, \beta, \beta^2, \ldots, \beta^{n-1}$ de L são linearmente independentes sobre $\mathbb{Z}_p$, pois, caso contrário, existiria um polinômio não nulo $r(X) \in \mathbb{Z}_p[X]$ de grau menor do que o grau de $f(X)$ tal que $r(\beta) = 0$.

Pela Observação 2.24, seguiria que $MDC(f(X), r(X)) \neq 1$; e como $f(X)$ é irredutível, teríamos $f(X) \mid r(X)$, o que é irreal, pois $gr(r(X)) \langle n$. Logo, tais elementos formam uma base de L sobre $\mathbb{Z}_p$. Também é de nosso conhecimento, que pela Proposição 2.23(i), que $1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{n-1}$ é uma base de $\mathbb{Z}_p[X]/(f(X))$ sobre $\mathbb{Z}_p$.

Definindo

$$\begin{aligned} \varphi : \mathbb{Z}_p[X]/(f(X)) &\longrightarrow L \\ \overline{a_0 + \cdots + a_{n-1}X^{n-1}} &\longmapsto a_0 + \cdots + a_{n-1}\beta^{n-1} \end{aligned}$$

temos que φ está bem definida, pois, se

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

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

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

Portanto,

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

o que prova que

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

Além disso, φ é sobrejetora e é aditiva, pois $\{1, \beta, \ldots, \beta^{n-1}\}$ é L.I e a dimensão de L sobre $\mathbb{Z}_p$ é n, ou seja,

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

Para mostrarmos que φ é um isomorfismo, basta provarmos que é multiplicativa, ou seja,

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

já que $\varphi([1]) = 1$ e todo homomorfismo de corpos é injetor. Sejam $u = \overline{u(X)}$ e $v = \overline{v(X)}$, em $\mathbb{Z}_p[X]/(f(X))$, onde $u(X)$ e $v(X)$ são polinômios em $\mathbb{Z}_p[X]$. Usando o algoritmo da divisão de polinômios, escrevemos

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

onde $r(X)$ é zero ou é um polinômio de grau menor ou igual a $n - 1$. Logo, temos que

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

provando assim que

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

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

3. CÓDIGOS LINEARES

Denotaremos por K um corpo finito com q elementos. Temos, então, para cada número natural n, um K-espaço vetorial K^n de dimensão n.

Definição 3.1. *Um código linear $C \subset K^n$ é um subespaço vetorial de K^n*

Dizemos que $C \subset K^n$ tem comprimento n.

Definição 3.2. *Dados $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n) \in K^n$, a **distância de Hamming** entre x e y é definida como*

$$d(x, y) = \#\{i; x_i \neq y_i, \text{ onde } i \in \{1, \ldots, n\}\}$$

Proposição 3.3. *Dados $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)$ e $z = (z_1, \ldots, z_n) \in K^n$, valem as seguintes propriedades:*

- $d(x, y) \geq 0$ *e* $d(x, y) = 0$ *se, e somente se,* $x = y$.
- $d(x, y) = d(y, x)$.
- $d(x, z) \leq d(x, y) + d(y, z)$.

Demonstração. Vamos demonstrar a terceira propriedade, pois a primeira e a segunda são triviais. No caso em que $x_i = z_i$ a contribuição para $d(x, z)$ é zero; no caso em que $x_i \neq z_i$ não podemos ter $x_i = y_i$ e $z_i = y_i$, logo a contribuição das i-ésimas coordenadas para a soma $d(x, y) + d(y, z)$ é pelo menos 1. Assim, vale a desigualdade. □

O resultado acima mostra que a distância de Hamming satisfaz as propriedades de uma métrica, por isso é também chamada de métrica de Hamming.

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

$$\delta(C) := \min\{d(x, y); x, y \in C \text{ e } x \neq y\}$$

Definição 3.5. *Dado $x = (x_1, \ldots, x_n) \in K^n$, define-se o peso de x como sendo o número inteiro*

$$\omega(x) := \#\{i; x_i \neq 0\}.$$

Ou seja, temos que

$$\omega(x) = d(x, 0),$$

onde d representa a métrica de Hamming.

Definição 3.6. *O peso de um código linear C é o inteiro*

$$\omega(C) := min\{\omega(x); x \in C\backslash\{0\}\}.$$

Proposição 3.7. *Seja $C \subset K^n$ um código linear com distância mínima d. Temos que*

i) $\forall x, y \in K^n$, $d(x, y) = \omega(x - y)$.

ii) $d = \omega(C)$.

Demonstração. O item (i) segue imediatamente das definições da métrica de Hamming e da de peso de um código. O item (ii) decorre do fato que, para todo par de elementos x, y em C com $x \neq y$, tem se $z = x - y \in C\backslash\{0\}$ e $d(x, y) = \omega(z)$. □

Vejamos que a proposição acima nos mostra que, em códigos lineares com M elementos, podemos calcular a distância mínima d a partir de $M - 1$ cálculos de distâncias, em vez dos $\binom{M}{2}$ cálculos em princípio requeridos. Na prática, em códigos grandes, esse método para cálculo de d é inviável por representar um custo computacional muito elevado, teremos, portanto, que desenvolver outros métodos para determinar a distância mínima de um código.

Pela Proposição 3.7(ii) , a distância mínima de um código linear C será também chamada de peso do código C. Em álgebra linear, conhecem-se essencialmente duas maneiras de se descrever subespaços vetoriais C de um espaço vetorial K^n, uma como imagem, e outra como núcleo de transformações lineares.

Primeiramente vamos mostrar como se obtém a representação de C como imagem. Devemos escolher uma base $v_1, v_2, \ldots, v_k$ de C e considere a aplicação linear

$$T : K^k \longrightarrow K^n$$
$$x = (x_1, \ldots, x_k) \longmapsto x_1v_1 + x_2v_2 + \cdots + x_kv_k$$

Temos que T é uma transformação linear injetora (pois o conjunto $\{v_1, v_2, \ldots, v_k\}$ é linearmente independente sobre K), e imagem de T é C, ou seja,

$$Im(T) = C.$$

Portanto, dar um código $C \subset K^n$ de dimensão k é equivalente a dar uma transformação linear injetora

$$T : K^k \longrightarrow K^n$$

e definir $C = Im(T)$. Essa é a forma paramétrica do subespaço C, pois os elementos de C são parametrizados pelos elementos x de K^k através de T, o que torna fácil gerar todos os elementos de C. Note que nessa representação é difícil decidir se um dado elemento v de K^n pertence ou não a C, pois, para tal, é necessário resolver todo o sistema de n equações nas k

incógnitas $x_1, x_2, \ldots, x_k$ abaixo

$$x_1v_1 + x_2v_2 + \cdots + x_kv_k = v, \tag{3.1}$$

essa resolução, em geral, representa um custo computacional muito elevado.

A outra maneira de descrevermos um código C é através do núcleo de uma transformação linear. Sendo assim, tome um subespaço C' de K^n complementar de C, ou seja,

$$C \oplus C' = K^n, \tag{3.2}$$

e considere a aplicação linear

$$\begin{aligned} H : C \oplus C' &\longrightarrow K^{n-k} \\ u \oplus v &\longmapsto v \end{aligned} \tag{3.3}$$

cujo núcleo é precisamente C. Computacionalmente, é muito mais simples determinar se um certo elemento $v \in K^n$ pertence ou não a C; para isto, basta verificar se $H(v)$ é ou não o vetor nulo de K^{n-k}, o que tem um custo computacional bem pequeno.

Exemplo 3.8. *Considere o corpo finito com três elementos $\mathbb{F}_3 = \{0, 1, 2\}$ e seja $C \subset \mathbb{F}_3^4$ o código gerado pelos vetores $v_1 = (1, 0, 1, 1)$ e $v_2 = (0, 1, 1, 2)$. Esse código possui $9 = 3^2$) elementos, pois tem dimensão dois sobre um corpo com três elementos. Uma representação paramétrica de C é dada por*

$$x_1v_1 + x_2v_2$$

ao variar x_1 e x_2 em $\mathbb{F}_3$. O código C pode ser representado como núcleo da transformação linear

$$\begin{aligned} H : \mathbb{F}_3^4 &\longrightarrow \mathbb{F}_3^2 \\ (x_1, \ldots, x_4) &\longmapsto (2x_1 + 2x_2 + x_3, 2x_1 + x_2 + x_4) \end{aligned}$$

Definição 3.9. *Seja K um corpo finito. Dois códigos lineares C e C' são linearmente equivalentes se existir um isomorfismo de K-espaços vetoriais $T : K^n \longrightarrow K^n$, que preserve o peso das palavras (i.e. $\omega(x) = \omega(T(x))$) e tal que $T(C) = C'$. Um tal isomorfismo é chamado de isometria linear.*

Observação 3.10. *De acordo com os problemas 1.6, 1.7 e 1.9 do capítulo 5 do livro ([2]) temos os seguintes resultados:*

1. *Sejam K um corpo e π uma permutação de $\{1, \ldots, n\}$. Temos que $T_\pi : K^n \longrightarrow K^n$ dada por $T_\pi(x) = (x_{\pi(1)}, \ldots, x_{\pi(n)})$ é uma isometria linear.*

2. *Seja K um corpo e π uma permutação de $\{1, \ldots, n\}$ e $f_i : K \longrightarrow K$, $i = 1, \ldots, n$, bijeções. Temos que $T_\pi \circ T_{f_1}^1 \circ \cdots \circ T_{f_n}^n$ é linear se, e somente se, cada f_i é linear.*

3. *Seja K um corpo. Temos que uma função $f : K \longrightarrow K$ é linear se, e somente se, existe um elemento $c \in K$ tal que $f(x) = cx$, $\forall x \in K$.*

Levando em consideração a observação acima e tudo que já vimos até aqui, segue que dois códigos lineares C e C' em K^n são linearmente equivalentes se, e somente se, existem uma permutação π de $1, \cdots, n$ e elementos $c_1, \cdots, c_n$ de $K\backslash\{0\}$ tais que

$$C' = \{(c_1 x_{\pi(1)}, \cdots, c_n x_{\pi(n)}); (x_1, \cdots, x_n \in C)\}.$$

Ou seja, 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:

i) Multiplicação dos elementos numa dada posição fixa por um escalar não nulo em todos os elementos do código.

ii) Permutação das posições de todas os elementos do código, mediante uma permutação fixa de $\{1, 2, \ldots, n\}$.

3.1 Matriz Geradora de um Código

Sejam K o corpo finito com q elementos e $C \in K^n$ um código linear. Chamaremos de parâmetros do código linear C à terna de inteiros (n, k, d), onde k é a dimensão de C sobre K, e d representa a distância mínima de C, que é também igual ao peso $\omega(C)$ do código C. Note que o número de elementos M de C é igual a q^k.

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

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

A matriz G é chamada de *matriz geradora* de C associada à base $\mathcal{B}$. Agora, considere a transformação linear definida por

$$\begin{aligned} T : K^k &\longrightarrow K^n \\ x &\longmapsto xG \end{aligned} \tag{3.4}$$

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

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

logo $T(K^k) = C$. Tecnicamente dizemos que K^k é o código fonte, C é o código de canal e a transformação T, é uma codificação.

Note que a matriz G não é univocamente determinada por C, pois ela depende da escolha da base $\mathcal{B}$. Relembre, ainda, 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; ou
- substituição de um elemento da base por ele mesmo somado com um múltiplo escalar de outro vetor da base.

Segue, então, que duas matrizes geradoras de um mesmo código 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 outra.

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 dada por (3.4).

Exemplo 3.11. *Tome $K = \mathbb{F}_2$ e seja*

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

Considerando a transformação linear

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

obtemos um código C em $\mathbb{F}_2^5$, imagem de T. A palavra 101 do código fonte, por exemplo, é codificada como 01010.

Suponhamos agora que seja dada a palavra 10101 do código, e que gostaríamos de decodificá-la, ou seja, achar a palavra x de $\mathbb{F}_2^3$ da qual ela se origina por meio de T. Teríamos então, que resolver o sistema:

$$(x_1\ x_2\ x_3)G = (10101)$$

ou seja,

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

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

Esse sistema particular de equações foi fácil de se resolver, mas, em geral, dada uma matriz G *mais complexa, a resolução do sistema de equações associado pode ser bem complicada e trabalhosa.*

Observe, entretanto, que, efetuando operações sobre as linhas de G *do tipo (1), (2) e (3), podemos colocar* G *na forma*

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

Note que

$$xG' = (x_1 \ x_2 \ x_3 \ x_2 \ x_3)$$

e, portanto, o vetor x *tomando apenas as três primeiras componentes do vetor a ser decodificado. Logo, a palavra (10101) é facilmente decodificada como (101).*

Definição 3.12. *Diremos que uma matriz geradora* G *de um código* C *está na forma padrão se tivermos*

$$G = (Id_k \mid A),$$

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

Dado um código C, nem sempre é possível achar uma matriz geradora de C na forma padrão. Por exemplo, o código em $\mathbb{F}_2^5$ com as duas primeiras colunas nulas e as demais não nulas nunca poderá ter uma matriz geradora na forma padrão, mas efetuando as permutações nas colunas dessa matriz é possível chegar em outra matriz geradora na forma padrão equivalente a primeira.

De modo mais geral, efetuando também sequências de operações sobre a matriz geradora G de um código linear C, do tipo:

(C1) permutação de duas colunas,

(C2) multiplicação de uma coluna por um escalar não nulo,

obtemos uma matriz G' de um código C' equivalente a C.(Note que as operações acima numa base C implica efetuá-la em todas as palavras de C).

Permitindo-se, também, a utilização de operações do tipo $(C1)$ acima, temos o seguinte resultado:

Teorema 3.13. *Dado um código* C*, existe um código equivalente* C' *com matriz geradora na forma padrão.*

Demonstração. Seja G uma matriz geradora de C. Mostraremos que com uma sequência de operações do tipo $(L1), (L2), (L3)$ e $(C1)$ podemos colocar G na forma padrão.

Suponhamos que

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

Como a primeira linha de G não é nula (os vetores linhas de G são linearmente independentes), por meio de $(C1)$, podemos supor $g_{11} \neq 0$. Agora, multiplicando a primeira linha por g_{11}^{-1}, podemos pôr 1 no lugar de g_{11} (usando a operação $(L2)$).

Somando à segunda, terceira e assim por diante linhas, respectivamente, a primeira linha multiplicada respectivamente por $(-1)g_{21}, (-1)g_{31}$, etc, (usando as operações $(L3)$), obtemos a seguinte matriz

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

Agora, na segunda linha dessa matriz, temos certamente um elemento não nulo que, por meio de uma operação $(C1)$, pode ser colocado na segunda linha e segunda coluna. Multiplicando a segunda linha pelo inverso desse elemento, a matriz se transforma em

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

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

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

e assim sucessivamente, até encontrarmos uma matriz na forma padrão

$$G' = (Id_k \mid A).$$

□

3.2 Códigos Duais

Definição 3.14. *Sejam $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n)$ elementos de K^n, define-se o produto interno de u e v como sendo*

$$\langle u, v\rangle = u_1v_1 + \cdots + u_nv_n.$$

Essa operação possui as propriedades usuais de um produto interno, ou seja, é simétrica

$$\langle u, v\rangle = \langle v, u\rangle$$

e bilinear

$$\langle u + \lambda w, v\rangle = \langle u, v\rangle + \lambda\langle w, v\rangle$$

para todo $\lambda \in K$.

Definição 3.15. *Seja $C \subset K^n$ um código linear, definimos o conjunto $C^\perp$ como sendo*

$$C^\perp = \{v \in K^n; \langle v, u\rangle = 0,\ \forall u \in C\}.$$

Quando $\langle u, v\rangle = 0$ dizemos que u e v são ortogonais.

Lema 3.16. *Se $C \subset K^n$ é um código linear, com matriz geradora G, então*

i) $C^\perp$ é um subespaço vetorial de K^n

ii) $x \in C^\perp \iff Gx^t = 0$.

Demonstração. i) Sejam dados $u, v \in C^\perp$ e $\lambda \in K$. Temos, para todo $x \in C$, que

$$\langle u + \lambda v, x\rangle = \langle u, x\rangle + \lambda\langle v, x\rangle = 0,$$

e, portanto, $u + \lambda v \in C^\perp$, provando que $C^\perp$ é um subespaço vetorial de K^n.

ii) $x \in C^\perp$ se, e somente se, x é ortogonal a todos os elementos de C. Isso equivale a x ser ortogonal a todos elementos de uma base de C, o que é equivalente a dizer que $Gx^t = 0$, pois as linhas de G formam uma base de C.

□

O subespaço vetorial $C^\perp$ de K^n é um código linear que será chamado de *código dual* de C, e dizemos que $C^\perp$ é ortogonal a C.

Proposição 3.17. *Seja $C \subset K^n$ um código de dimensão k com matriz geradora $G = (Id_k \mid A)$ na forma padrão. Então*

i) $dim\ C^{\perp} = n - k$;

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

Demonstração. i) Pelo lema anterior, $x = (x_1, \ldots, x_n)$ pertence a $C^{\perp}$ se, e somente se, $Gx^t = 0$. Como G está na forma padrão, isso equivale a ter

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

Portanto, $C^{\perp}$ possui q^{n-k} elementos, que são justamente as possíveis escolhas arbitrárias de $x_{k+1}, \ldots, x_n$. Logo, $C^{\perp}$ tem dimensão $n - k$.

ii) É claro ver que as linhas de H são linearmente independentes (principalmente por conta do bloco Id_{n-k}), portanto, geram um subespaço vetorial de dimensão $n - k$. Como as linhas de H são ortogonais às linhas de G, temos que o espaço gerado pelas linhas de H está contido em $C^{\perp}$; e como esses dois subespaços têm a mesma dimensão, eles coincidem, provando assim que $H = (-A^t \mid Id_{n-k})$ é uma matriz geradora de $C^{\perp}$.

□

Lema 3.18. *Seja* C *um código linear em* K^n. *Para toda permutação* σ *de* $\{1, \ldots, n\}$, *para todo* $c \in K^*$ *e para todo* $j = 1, \ldots, n$, *definindo*

$$T_c^j : K^n \longrightarrow K^n$$
$$(x_1, \cdots, x_j, \cdots, x_n) \longmapsto (x_1, \cdots, cx_j, \cdots, x_n)$$

temos que

i) $(T_\sigma(C))^{\perp} = T_\sigma(C^{\perp})$

ii) $(T_c^j(C))^{\perp} = T_{c^{-1}}^j(C^{\perp})$.

Demonstração. Segue diretamente das definições. □

Antes de continuarmos com a equivalência linear de dois códigos, vamos enunciar um teorema e o seu corolário que serão de extrema importância para o nosso estudo.

Definição 3.19. *Sejam* C *um código linear em* K^n *e* n *um número natural. Diremos que uma função* $F : K^n \longrightarrow K^n$ *é uma isometria de* K^n *se ela preserva distâncias de Hamming. Em símbolos,*

$$d(F(x), F(y)) = d(x, y); \quad \forall x, y \in K^n.$$

Teorema 3.20. *Seja $F : K^n \to K^n$ uma isometria, então existem uma permutação π de $\{1, \ldots, n\}$ e bijeções f_i de A, $i = 1, \ldots, n$, tais que*

$$F = T_\pi \circ T^1_{f_1} \circ \cdots \circ T^n_{f^n}.$$

Demonstração. A demonstração desse teorema se encontra no Apêndice 2 do livro ([2]). □

Colorário 3.21. *Sejam C e C' dois códigos lineares em K^n. Temos que C e C' são linearmente equivalentes se, e somente se, existem uma permutação π de $\{1, \ldots, n\}$ e bijeções $f_1, \ldots, f_n$ de K tais que*

$$C' = \{(f_{\pi(1)}(x_{\pi(1)}), \ldots, f_{\pi(n)}(x_{\pi(n)})); \ (x_1, \ldots, x_n) \in C\}.$$

Proposição 3.22. *Sejam C e D dois códigos lineares em K^n. Se C e D são linearmente equivalentes, então $C^\perp$ e $D^\perp$ são linearmente equivalentes.*

Demonstração. Se C e D são linearmente equivalentes, pelo corolário anterior e pelo que já sabemos de códigos linearmente equivalentes, existem uma permutação σ de $\{1, \ldots, n\}$ e elementos $c_1, \ldots, c_n \in K^*$ tais que

$$D = T_\sigma \circ T^1_{c_1} \circ \cdots \circ T^n_{c_n}(C).$$

Desse ponto, levando em consideração o Lema 3.18, segue o resultado, pois

$$D^\perp = (T_\sigma \circ T^1_{c_1} \circ \cdots \circ T^n_{c_n}(C))^\perp = T_\sigma \circ T^1_{c_1^{-1}} \circ \cdots \circ T^n_{c_n^{-1}}(C^\perp).$$

□

Colorário 3.23. *Se D é um código linear em K^n de dimensão k, então $D^\perp$ é um código de dimensão $n - k$.*

Demonstração. Pelo Teorema 3.13, o código D é linearmente equivalente a um código C, também de dimensão k, com matriz geradora na forma padrão e, portanto, pela Proposição 3.17, segue que $\dim C^\perp = n - k$. Pela proposição anterior, temos que $D^\perp$ é equivalente a $C^\perp$ e, portanto, também tem dimensão $n - k$. □

Lema 3.24. *Suponha que C seja um código de dimensão k em K^n com matriz geradora G. Uma matriz H de ordem $(n-k) \times n$, com coeficientes em K e com linhas linearmente independentes, é uma matriz geradora de $C^\perp$ se, e somente se,*

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

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

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

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

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

□

Colorário 3.25. *Temos que* $(C^\perp)^\perp = C$.

Demonstração. Sejam G e H respectivamente matrizes geradoras de C e $C^\perp$. Logo, $G \cdot H^t = 0$. Tomando transpostas nessa última igualdade, temos que $H \cdot G^t = 0$, por consequência, G é uma matriz geradora de $(C^\perp)^\perp$, dado isso seguimos com o resultado. □

Proposição 3.26. *Seja C um código linear e suponhamos que H seja uma matriz geradora de $C^\perp$. Temos então que*

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

Demonstração. Temos, pelo corolário anterior Lema 3.16(ii), $v \in C$ se, e somente se, $v \in (C^\perp)^\perp$, o que equivale a $Hv^t = 0$. □

A proposição acima nos permite caracterizar os elementos de um código C por uma condição de anulamento. A matriz geradora H de $C^\perp$ é chamada de *matriz teste de paridade de C*.

Observe que, para verificar se um determinado valor de v em K^n pertence ou não a um código C com matriz geradora G, é necessário verificar se o sistema de n equações com k incógnitas $x = (x_1, \ldots, x_k)$, dado por

$$xG = v,$$

admite solução. Em geral, essa questão requer um custo operacional elevado para ser respondida. No entanto, trabalhando com uma matriz teste de paridade de H, a solução pode ser encontrada bem mais rapidamente. Basta verificar se é nulo o vetor Hv^t, o que pode ser feito com um circuito simples.

Dados um código C com matriz teste de paridade H e um vetor $v \in K^n$, chamamos o vetor Hv^t de *síndrome de v*.

Proposição 3.27. *Seja H a matriz teste de paridade de um código C. Temos que o peso de C é maior do que ou igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes.*

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

$$0 = H \cdot c^t = \sum c_i h^i. \tag{3.5}$$

Visto que $\omega(c)$ é o número de componentes não nulas de c, segue que se $\omega(c) \leq s-1$, teríamos por (3.5) uma combinação nula de um número t, com $1 \leq t \leq s-1$, de colunas de H, o que é contraditório. Portanto, $\omega(c) \geq s$ e, sendo assim, $\omega(C) \geq s$.

[$\Longrightarrow$] Reciprocamente, suponhamos que $\omega(C) \geq s$. Suponhamos também, por absurdo, que H tenha $s-1$ colunas linearmente dependentes, digamos $h^{i_1}, h^{i_2}, \ldots, h^{i_{s-1}}$. Logo, existiriam $c_{i_1,\ldots,c_{i_{s-1}}}$, no corpo, nem todos nulos, tais que

$$c_{i_1} h^{i_1} + \cdots + c_{i_{s-1}} h^{i_{s-1}} = 0. \tag{3.6}$$

Portanto, $c = (0, \ldots, c_{i_1}, 0, \ldots, c_{i_{s-1}}, 0, \ldots, 0 = 0) \in C$ e consequentemente, $\omega(c) \leq s-1 < s$, o que seria um absurdo. □

Teorema 3.28. *Seja H a matriz teste de paridade de um código C. Temos que o peso de C é igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

Demonstração. Suponhamos que $\omega(C) = s$, logo, todo conjunto de $s-1$ colunas de H é linearmente independente. Por outro lado, existem s colunas de H linearmente dependentes, pois, caso contrário, pela proposição anterior, teríamos $\omega(C) \geq s+1$.

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

Colorário 3.29 (Cota de Singleton)**.** *Os parâmetros (n, k, d) de um código linear satisfazem à desigualdade*

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

Demonstração. Se H é uma matriz teste de paridade, então ela tem posto $n-k$. Como, pelo teorema anterior, $d-1$ é menor ou igual ao posto de H, segue a desigualdade. □

Observação 3.30. *Um código será chamado de MDS(Maximum Distance Separable) se valer a igualdade $d = n - k + 1$.*

3.3 Código de Hamming

Construir códigos com distância mínima pelo menos três é muito simples. Basta construir uma matriz H tal que quaisquer duas colunas sejam linearmente independentes, e, para isso, importa que nenhuma coluna de H seja nula e que nenhuma seja múltipla da outra (agora, quando o código é binário, essa condição pode ser substituída por nenhuma coluna é igual a outra).

Nesta seção vamos apresentar um código chamado de código de Hamming.

Definição 3.31. *Um código de Hamming de ordem m sobre $\mathbb{F}_2$ é um código com matriz de paridade H_m de ordem $m \times n$, cujas colunas são as m-uplas de $\mathbb{F}_2^m \setminus \{0\}$ numa ordem qualquer.*

A definição acima de H_m determina o código C a menos de equivalência.

Temos, portanto, que o comprimento de um código de Hamming de ordem m é o número de m-uplas em $\mathbb{F}_2^m \setminus \{0\}$, a saber $n = 2^m - 1$. Observe que o posto de H (ou seja, a dimensão de $C^\perp$) é m, pois após uma reordenação das colunas é possível obter a matriz Id_k nas primeiras k colunas, assim a dimensão de C vai ser $k = n - m = 2^m - m - 1$.

Verificamos facilmente, usando a Proposição 3.17, que a distância mínima $d = 3$, pois em H_m é fácil achar três colunas linearmente dependentes.

Como exemplo numérico, considere a matriz de um código de Hamming correspondente a $m = 3$.

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Verifica-se facilmente que um código de Hamming de ordem m é MDS se, e só se, $m = 2$.

3.4 DECODIFICAÇÃO

Chama-se *decodificação* ao procedimento de detecção e correção de erros num determinado código. O método geral de decodificação para códigos lineares que desenvolvemos nessa seção é um aperfeiçoamento de um método inventado por D. Slepian do Laboratório Bell em Murray Hill, New Jersey na década de 60. O método original de Slepian tinha um custo computacional bem elevado e os aperfeiçoamentos visaram reduzir esse custo.

Inicialmente, define-se o vetor erro $\mathbf{e}$ como sendo a diferença entre o vetor recebido $\mathbf{r}$ e o vetor transmitido $\mathbf{c}$, isto é,

$$\mathbf{e} = \mathbf{r} - \mathbf{c}$$

Por exemplo, se, num determinado código sobre $\mathbb{F}_2$, tenhamos transmitido a palavra (010011) e a palavra recebida tenha sido (101011), então

$$\mathbf{e} = (101011) - (010011) = (111000).$$

Note que o peso do vetor erro corresponde ao número de erros cometidos numa palavra entre a transmissão e a recepção.

Seja H a matriz teste de paridade do código. Como $Hc^t = 0$, temos que

$$H\mathbf{e}^t = H(\mathbf{r}^t - \mathbf{c}^t) = H\mathbf{r}^t - H\mathbf{c}^T = H\mathbf{r}^t.$$

Portanto, a palavra recebida e o vetor erro têm a mesma síndrome.

Denotaremos por h^i a i-ésima coluna de H. Se $\mathbf{e} = (\alpha_1, \ldots, \alpha_n)$, então

$$\sum_{i=1}^{n} \alpha_i h^i = H\mathbf{e}^t = H\mathbf{r}^t.$$

Definição 3.32. *Seja C um código com distância mínima d. A capacidade de correção de C é o inteiro definido como*

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

A importância desse conceito aparece no seguinte resultado.

Lema 3.33. *Seja C um código linear em K^n com capacidade de correção κ. Se $\boldsymbol{r} \in K^n$ e $\boldsymbol{c} \in C$ são tais que $d(\boldsymbol{c}, \boldsymbol{r}) \leq \kappa$, então existe um único vetor $\boldsymbol{e}$ com $\omega(\boldsymbol{e}) \leq \kappa$, cuja síndrome é igual à síndrome de $\boldsymbol{r}$. Além disso, $\boldsymbol{c} = \boldsymbol{r} - \boldsymbol{e}$.*

Demonstração. De fato, $\mathbf{e} = \mathbf{r} - \mathbf{c}$ tem a propriedade do lema, já que $\omega(\mathbf{e}) = d(\mathbf{c}, \mathbf{r}) \leq \kappa$. Para provar a unicidade, suponhamos que $\mathbf{e} = (\alpha_1 \cdots \alpha_n)$ e $\mathbf{e}' = (\alpha_1' \cdots \alpha_n')$ sejam tais que $\omega(\mathbf{e}) \leq \kappa$ e $\omega(\mathbf{e}') \leq \kappa$ e tenham mesma síndrome que $\mathbf{r}$. Então, se H é uma matriz teste de paridade de C, temos

$$H\mathbf{e}^t = H\mathbf{e}'^t \Longrightarrow \sum_{i=1}^{n} \alpha_i h^i = \sum_{i=1}^{n} \alpha_i' h^i, \tag{3.7}$$

o que nos dá uma relação de dependência linear entre $2\kappa (\leq d-1)$ colunas de H. Como quaisquer $d-1$ colunas de H são linearmente independentes (veja o Teorema 3.28), temos que $\alpha_i = \alpha_i'$, para todo i, logo $\mathbf{e} = \mathbf{e}'$ □

O problema que se coloca, então, é de como determinar esse único vetor $\mathbf{e}$ a partir de $H\mathbf{r}^t$.

Exemplo 3.34. *Determinação de $\boldsymbol{e}$ quando $\omega(\boldsymbol{e}) \leq 1$.*

Suponhamos que o código C tenha distância mínima $d \geq 3$ e que o vetor erro $\boldsymbol{e}$, introduzido entre a palavra transmitida $\boldsymbol{c}$ e a palavra recebida $\boldsymbol{r}$, seja tal que $\omega(\boldsymbol{e}) \leq 1$. Isto é, o canal introduziu no máximo um erro. Se $H\boldsymbol{e}^t = 0$, então $\boldsymbol{r} \in C$ e se toma $\boldsymbol{c} = \boldsymbol{r}$. Suponhamos que $H\boldsymbol{e}^t \neq 0$, então $\omega(\boldsymbol{e}) = 1$ e, portanto, $\boldsymbol{e}$ tem apenas uma coordenada não nula. Nesse caso, consideremos que $\boldsymbol{e} = (0, \ldots, \alpha, \ldots, 0)$ com $\alpha \neq 0$ na i-ésima posição. Logo,

$$H\boldsymbol{e}^t = \alpha h^i,$$

onde h^i é a i-ésima coluna de H. Portanto, não conhecendo $\boldsymbol{e}$, mas conhecendo

$$H\boldsymbol{e}^t = H\boldsymbol{r}^t = \alpha h^i,$$

podemos determinar $\boldsymbol{e}$ como sendo o vetor com todas as componentes nulas exceto i-ésima componente que é α. Note que i acima é bem determinado, pois $d \geq 3$.

Com isso, a seguir estabelecemos o algoritmo de decodificação em códigos corretores de um erro.

Seja H a matriz teste de paridade do código C e seja $\mathbf{r}$ um vetor recebido.
(Suponha $d \geq 3$).
(i) Calcule $H\mathbf{r}^t$.
(ii) Se $H\mathbf{r}^t = 0$, aceite $\mathbf{r}$ como sendo a palavra transmitida.
(iii) Se $H\mathbf{r}^t = s^t \neq 0$, compare s^t com as colunas de H.
(iv) Se existirem i e α que $s^t = \alpha h^i$, para $\alpha \in K$, então $\mathbf{e}$ é a n-upla
com α na posição i e zeros nas outras posições. Corrija $\mathbf{r}$ pondo $\mathbf{c} = \mathbf{r} - \mathbf{e}$.
(v) Se o contrário de (iv) ocorrer, então mais de um erro foi comitido.

Esse algoritmo pode ser aperfeiçoado para o caso dos códigos de Hamming como segue.

Ordene os vetores colunas de H_m do seguinte modo: se $v \in \mathbb{F}_2^m \ \{0\}$, então, $v = (v_1, \ldots, v_m)$ com $v_i = 0, 1$. Coloque o vetor v em H_m na coluna de ordem

$$i = v_1 + v_2 2^1 + v_3 2^2 + \cdots + v_m 2^{m-1}.$$

Note que, na condição (iv) em códigos binários, α é necessariamente igual a 1. Suponhamos, agora, que $H_m\mathbf{r}^t \neq 0$. Logo $H_m\mathbf{r}^t = s^t$ é a coluna de H_m de ordem

$$j = s_1 + s_2 2 + s_3 2^2 + \cdots + s_m 2^{m-1}$$

e, portanto, o vetor erro correspondente é

$$\mathbf{e} = \mathbf{e}_j = (0, \ldots 0, 1, 0, \ldots, 0)$$

com 1 na j-ésima componente.

Exemplo 3.35. *No código de Hamming de ordem 3, tomemos a matriz teste de paridade*

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Se $r = (1010011)$, *então*

$$H_3 \boldsymbol{r}^t = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix};$$

logo, $j = 1 + 2 = 3$ *e, portanto,* $\boldsymbol{e} = (0010000)$ *e* $\boldsymbol{c} = (1000011)$.

Voltemos para o caso geral. Seja $C \subset K^n$ um código corretor de erros com matriz de paridade H. Sejam d a distância mínima de C e $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$. Recorde que $\mathbf{e}$ e $\mathbf{r}$ têm a mesma síndrome e, se $\omega(\mathbf{e}) = d(\mathbf{r} - \mathbf{c}) < \kappa$, então $\mathbf{e}$ é univocamente determinado por $\mathbf{r}$.

Seja $v \in K^n$. Defina

$$v + C = \{v + \mathbf{c}; \mathbf{c} \in C\}.$$

Lema 3.36. *Os vetores u e v de K^n têm a mesma síndrome se, e somente se, $u \in v + C$.*

Demonstração. Temos o seguinte: $[Hu^t = Hv^t] \iff H(u-v)^t = 0 \iff u - v \in C \iff u \in v + C$. □

É fácil verificar que os conjuntos $v + C$ têm as propriedades abaixo enunciadas.

Proposição 3.37. *Seja C um (n,k)-código linear. Temos que*

i) $v + C = v' + C \Leftrightarrow v - v' \in C$;

ii) $(v + C) \cap (v' + C) \neq \emptyset \Rightarrow v + C = v' + C$

iii) $\cup_{v \in K^n}(v + C) = K^n$

iv) $\mid (v + C) \mid = \mid C \mid = q^k$.

Demonstração. i) Temos

$$v + C = v' + C \Leftrightarrow v \in v' + C \text{ e } v' \in v + C \Leftrightarrow$$

$$v = v' + c' \text{ e } v' = v + c, \text{ com } c, c' \in C \Leftrightarrow$$

$$v - v' = c' \in C \text{ e } v' - v = c \in C$$

A demostração de (ii),(iii) e (iv) saem diretamente da definição e cálculos de teoria de conjuntos como feito em (i). □

Cada conjunto da forma $v + C$ é chamado de *classe lateral de v* segundo C. Note que

$$v + C = C \iff v \in C.$$

Segue imediatamente de (ii) - (iv) da proposição acima que o número de classes laterais segundo C é

$$\frac{q^n}{q^k} = q^{n-k}.$$

Exemplo 3.38. *Seja C o (4,2)-código gerado sobre $\mathbb{F}_2$, pela matriz*

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

Logo,

$$C = \{0000, 1011, 0101, 1110\},$$

e as classes laterais segundo C são

$$\begin{aligned} 0000+C &= \{0000, 1011, 0101, 1110\}. \\ 1000+C &= \{1000, 0011, 1101, 0110\}. \\ 0100+C &= \{0100, 1111, 0001, 1010\}. \\ 0010+C &= \{0010, 1001, 0111, 1100\}. \end{aligned}$$

Observação 3.39. *Observe que o Lema 3.36 nos estabelece uma correspondência 1 a 1 entre as classes laterais e síndromes. Todos os elementos de uma classe lateral têm a mesma síndrome, e elementos de classes laterais distintas possuem síndromes distintas.*

Definição 3.40. *Um vetor de peso mínimo numa classe lateral é chamado de elemento líder dessa classe.*

Observação 3.41. *No código do exemplo anterior, temos que:*

- *0000 é líder de C;*
- *1000 é líder de $1000+C$;*
- *0100 e 0001 são líderes de $0100+C$ e*
- *0010 é líder de $0010+C$.*

Proposição 3.42. *Seja C um código linear em K^n com distância mínima d. Se $u \in K^n$ é tal que*

$$\omega(u) \leq \left\lfloor \frac{d-1}{2} \right\rfloor = \kappa,$$

então u é o único elemento líder da sua classe.

Demonstração. Suponhamos que $u, v \in K^n$ com $\omega(u) \leq \lfloor \frac{d-1}{2} \rfloor$ e $\omega(v) \leq \lfloor \frac{d-1}{2} \rfloor$. Se $u - v \in C$, então:

$$\omega(u-v) \leq \omega(u) + \omega(v) \leq \left\lfloor \frac{d-1}{2} \right\rfloor + \left\lfloor \frac{d-1}{2} \right\rfloor \leq d-1;$$

logo, $u - v = 0$ e, portanto, $u = v$. □

Observação 3.43. *Para achar líderes de classes, selecionamos todos os elementos u tais que $\omega(u) \leq \lfloor \frac{d-1}{2} \rfloor$. Cada um desses elementos é líder de uma e somente uma classe. Esses líderes são todos aqueles de peso $\leq \lfloor \frac{d-1}{2} \rfloor$, os outros líderes não serão considerados.*

Para finalizar essa seção vamos discutir um algoritmo de correção de mensagens que tenham sofrido um número de erros menor ou igual à capacidade de correção do código, que é $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Inicialmente, antes de desenvolvermos o Algoritmo da Decodificação temos que determinar todos os elementos u de K^n, tal que $\omega(u) \leq \kappa$. Em seguida, devemos calcular as síndromes desses elementos e colocá-los numa tabela. Após disso, podemos começar com o Algoritmo.

Seja **r** uma palavra recebida, temos:

O Algoritmo de Decodificação

(1) Calcule a síndrome $s^t = H\mathbf{r}^t$.

(2) Se s está na tabela, seja l o elemento líder da classe determinada por s; troque $\mathbf{r}$ por $\mathbf{r}$ - l.

(3) Se s não está na tabela, então na mensagem recebida foram cometidos mais do que κ erros.

Justificativa: Dado $\mathbf{r}$, sejam $\mathbf{c}$ e $\mathbf{e}$, respectivamente, a mensagem transmitida e o vetor erro. Como $H\mathbf{e}^t = H\mathbf{r}^t$, temos que a classe lateral onde $\mathbf{e}$ se encontra está determinada pela síndrome de $\mathbf{r}$. Se $\omega(\mathbf{e}) \leq \kappa$, temos que $\mathbf{e}$ é o único elemento líder l de sua classe e, portanto, é conhecido e se encontra na tabela. Consequentemente, pelo Lema 3.33, $\mathbf{c} = \mathbf{r} - \mathbf{e} = \mathbf{r} - l$ é determinado.

Exemplo 3.44. *Considere o (6,3)-código linear definido sobre $\mathbb{F}_2$ com matriz teste de paridade*

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

Nesse caso, temos $d = 3$ e, portanto, $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor = 1$.

Os vetores de peso ≤ 1 com as suas respectivas síndromes estão relacionados na tabela abaixo

líder	*síndrome*
000000	000
000001	101
000010	011
000100	110
001000	001
010000	010
100000	100

Agora, suponhamos que a palavra recebida seja

(a) $\boldsymbol{r} = (100011)$. *Logo,* $H\boldsymbol{r}^t = (010)^t$ *e, portanto,* $\boldsymbol{e} = (010000)$. *Consequentemente,* $\boldsymbol{c} = \boldsymbol{r} - \boldsymbol{e} = (110011)$.

(b) $\boldsymbol{r} = (111111)$. *Logo,* $H\boldsymbol{r}^t = (111)^t$, *que não se encontra na tabela. Sendo assim, foi cometido mais do que um único erro na mensagem* $\boldsymbol{r}$.

4. Códigos Cíclicos

Temos que os códigos cíclicos são bastante utilizados nas aplicações por formarem uma classe de códigos lineares que possui bons algoritmos de codificação e decodificação.

Seja K um corpo finito. No que se segue, representaremos as coordenadas de K^n por $(x_0, \ldots, x_{n-1})$.

4.1 Introdução

Definição 4.1. *Um código linear $C \in K^n$ será chamado de código cíclico se, para todo $c = (c_0, \ldots, c_{n-1})$ que pertence a C, o vetor $(c_{n-1}, c_0, \ldots, c_{n-2})$ pertence a C.*

Ou seja, o código linear C será cíclico se, dada a permutação π de $\{0, \ldots, n-1\}$ definida por

$$\pi(i) = \begin{cases} i+1, & \text{se } 0 \leq i < n-1 \\ 0, & \text{se } i = n-1, \end{cases}$$

e sendo

$$T_\pi(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, \ldots, c_{n-2}),$$

temos que $T_\pi(\mathbf{c}) \in C$ para todo $\mathbf{c} \in C$; em outras palavras, $T_\pi(C) \subset C$.

Exemplo 4.2. *Seja $v \in K^n$. O espaço vetorial*

$$\langle v \rangle = \langle v + T_\pi(v) + \cdots + T_\pi^{n-1}(v) \rangle$$

é claramente um código cíclico (note que $T_\pi^n = id$). Em particular, o código $C = \langle 0 \rangle = \{0\}$ é cíclico.

Como exemplo numérico considere $K = \mathbb{F}_2$ e seja $v = (1011) \in K^4$. Temos que

$$\langle v \rangle \ = \langle 1011 + 1101 + 1110 + 0111 \rangle \text{ é cíclico.}$$

A técnica para lidar com os códigos cíclicos consiste em enriquecer a estrutura de espaço vetorial de K^n. Para fazer esse enriquecimento, devemos primeiramente definir R_n como sendo o anel das classes residuais em $K[X]$ módulo $x^n - 1$, ou seja,

$$R_n = K[X]/(x^n - 1).$$

Relembre também que R_n munido da multiplicação por escalares $\lambda \in K$, definida por

$$\lambda\overline{f(x)} = \overline{\lambda f(x)},$$

é um K-espaço vetorial de dimensão n com base $1, \bar{x}, \ldots, \overline{x^{n-1}}$ (a demostração desse fato é a mesma da Proposição 2.23(i), apesar de $x^n - 1$ não ser irredutível) e, como tal, é isomorfo a K^n através da seguinte transformação linear

$$\begin{aligned} \nu : K^n &\longrightarrow R_n \\ (a_0, \ldots, a_{n-1}) &\longmapsto \overline{a_0, +a_1 x, \ldots, a_{n-1}x^{n-1}}. \end{aligned}$$

Temos, então, que todo código linear $C \subset K^n$ pode ser transportado para R_n mediante o isomorfismo acima ν. A vantagem de se utilizar essa transformação linear é que sua imagem nos dá uma estrutura adicional de anel, chamada de *ideal*.

Neste trabalho vamos levar em consideração que o leitor já saiba o básico da teoria de ideais, mas iremos enfatizar o seguinte resultado

Proposição 4.3. *Seja $P(x) \in K[X]$. Todo ideal de $K[X]/P(x)$ é da forma $(\overline{F(x)})$, onde $F(x)$ é um divisor de $P(x)$.*

Demonstração. Seja I um ideal de $K[X]/P(x)$. Considere o conjunto

$$J = \{G(x) \in K[X]; \overline{G(x)} \in I\}.$$

Primeiramente vamos provar que J é um ideal de $K[X]$. De fato, se $G_1(x)$ e $G_2(x)$ estão em J, então $\overline{G_1(x)}$ e $\overline{G_2(x)}$ estão em I. Portanto,

$$\overline{G_1(x) + G_2(x)} = \overline{G_1} + \overline{G_2} \in I,$$

e consequentemente, $G_1 + G_2 \in J$.

Por outro lado, se $G(x) \in J$ e $H(x) \in K[X]$, temos que $\overline{G(x)} \in I$ e, portanto, $\overline{G(x)H(x)} = \overline{G(x)}\ \overline{H(x)} \in I$. Logo, $G(x)H(x) \in J$.

Sendo $J \neq \{0\}$, pois $P(x) \in J$, temos que existe $F(x) \in K[X]/\{0\}$ tal que $J = (F(x))$.

Agora, como $P(x) \in J = (F(x))$, segue que $P(x)$ é um múltiplo de $F(x)$, em outras palavras, $F(x)$ é um divisor de $P(x)$.

Veja agora que $I = \{\overline{G(x)}; G(x) \in J\}$, e como $J = (F(x))$, temos que

$$I = \{\overline{H(x)}\ \overline{F(x)}; \overline{H(x)} \in K[X]/P(x)\} = (\overline{F(x)}).$$

□

4.2 CÓDIGOS CÍCLICOS

O objetivo desta seção é determinar matrizes geradoras e matrizes teste de paridade para códigos cíclicos. Para tal, vamos caracterizar os códigos cíclicos em R_n.

Inicialmente, note que a ação de T_π em K^n traduz-se, por meio de ν, na multiplicação por $\overline{x}$ em R_n.

De fato, tomando $c = (c_0, \ldots, c_{n-1})$, temos

$$T_\pi(c) = (c_{n-1}, c_0, \ldots, c_{n-2})$$

e

$$\nu(T_\pi(c)) = \overline{c_{n-1} + c_0 x + \cdots + c_{n-2}x^{n-1}} = \overline{x}\ \overline{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}} = \overline{x}\nu(c).$$

Lema 4.4. *Seja V um subespaço vetorial de R_n. Então, V é um ideal de R_n se, e somente se, V é fechado pela multiplicação por $\overline{x}$.*

Demonstração. Suponhamos que V seja um ideal de R_n. Da definição de ideal, segue que $\overline{x}\ \overline{f(x)} \in V$ para todo $\overline{f(x)} \in V$.

Reciprocamente, suponhamos que V seja fechado pela multiplicação por $\overline{x}$. É suficiente mostrar que $\overline{g(x)}\ \overline{f(x)} \in V$ para todo $\overline{g(x)} \in R_n$ e todo $\overline{f(x)} \in V$.

Seja $\overline{f(x)} \in V$. Como V é um subespaço de R_n, é claro que $a\overline{f(x)} \in V$, para todo $a \in K$. Como por hipótese,

$$\overline{xf(x)} = \overline{x}\ \overline{f(x)} \in V,$$

então

$$\overline{x^2 f(x)} = \overline{x}\ \overline{xf(x)} \in V.$$

Indutivamente, obtemos, para todo $m \in \mathbb{N}$, que

$$\overline{x^m f(x)} = \overline{x^m}\ \overline{f(x)} \in V.$$

Agora, escrevendo $\overline{g(x)} = \overline{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}}$, temos que

$$\overline{g(x)}\ \overline{f(x)} = \overline{g(x)f(x)} = \overline{(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1})f(x)} = a_0\overline{f(x)} + a_1\overline{x}\ \overline{f(x)} + \cdots + a_{n-1}\overline{x^{n-1}}\ \overline{f(x)} \in V,$$

pois V é um subespaço e cada parcela da última expressão pertence a V. □

Com o lema que acabamos de enunciar e provar, juntamente com as observações anteriores ao lema, temos o resultado a seguir.

Teorema 4.5. *Um subespaço C de K^n é um código cíclico se, e somente se, $\nu(C)$ é um ideal de R_n.*

Portanto, pela Proposição4.3 temos que um código C em K^n é cíclico se, e somente se, $\nu(C) = I\overline{g(X)}$, onde $g(x) \in K[X]$ é um divisor de $x^n - 1$.

Seja $p =$ card (K). Se $n = mp^s$ com m e p primos entre si, temos pela Observação 4.2 da referência ([2]), que

$$X^n - 1 = (X^m - 1)^{p^s}.$$

Como $(X^m - 1)' = mX^{m-1} \neq 0$, o polinômio $x^m - 1$ não tem fator não constante em comum com a sua derivada, portanto, não possui fator múltiplo algum (Proposição 3.7 da referência ([2])). Consequentemente,

$$X^m - 1 = f_1 \cdots f_r,$$

onde os f_i são polinômios mônicos, irredutíveis e dois a dois distintos. Logo, a decomposição em fatores irredutíveis de $X^n - 1$ é

$$X^n - 1 = f_1^{p^s} \cdots f_r^{p^s}.$$

Temos então que o polinômio $x^n - 1$ tem exatamente $(p^s + 1)^r$ divisores mônicos. Temos então, em vista do problema 2.5 da referência ([2]), que R_n possui precisamente $(p^s+1)^r$ ideais. Em particular, se $MDC(n, p) = 1$, segue que R_n tem precisamente 2^r ideais.

Note que R_n não é um domínio de integridade, pois temos, por exemplo,

$$\overline{x-1} \cdot \overline{x^{n-1} + x^{n-2} + \cdots + x + 1} = \overline{x^n - 1} = \overline{0}.$$

No que segue, $g(x)$ denotará sempre um divisor de $x^n - 1$, e escreveremos

$$h(x) = \frac{x^n - 1}{g(x)}.$$

Teorema 4.6. *Seja $I = (\overline{g(x)})$, onde $g(x)$ é um divisor de $x^n - 1$ de grau s. Temos que $\overline{g(x)}, \overline{xg(x)}, \overline{x^2g(x)}, \ldots, \overline{x^{n-s-1}g(x)}$ é uma base de I como espaço vetorial sobre K.*

Demonstração. Os elementos acima são linearmente independentes. De fato, suponhamos que

$$a_0\overline{g(x)} + a_1\overline{xg(x)} + \cdots + a_{n-s-1}\overline{x^{n-s-1}g(x)} = \overline{0}.$$

Logo,

$$\overline{g(x)}\ \overline{a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1}} = \overline{0}.$$

Portanto, para algum $d(x) \in K[X]$, temos que

$$g(x)(a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1}) = d(x) \cdot (x^n - 1).$$

Daí, segue que

$$a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1} = d(x) \cdot h(x)$$

Como o grau de $h(x)$ é $n - s$, devemos ter $a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1} = 0$, e consequentemente, $a_0 = a_1 = \cdots = a_{n-s-1} = 0$.

Os elementos acima geram I sobre K. De fato, se $\overline{f(x)} \in I$, temos que

$$f(x) \equiv d(x) \cdot g(x) \bmod(x^n - 1).$$

Pelo algoritmo da divisão, temos que $d(x) = c(x) \cdot h(x) + r(x)$, com $r(x) = a_0 + a_1 x + \cdots + a_{n-s-1}x^{n-s-1}$. Logo,

$$f(x) \equiv d(x) \cdot g(x) \equiv c(x) \cdot h(x) \cdot g(x) + r(x) \cdot g(x) \bmod(x^n - 1),$$

e portanto,

$$f(x) \equiv c(x)(x^n - 1) + r(x) \cdot g(x) \equiv r(x) \cdot g(x) \bmod(x^n - 1)$$

Consequentemente e por fim,

$$\overline{f(x)} = a_0\overline{g(x)} + a_1\overline{xg(x)} + \cdots + a_{n-s-1}\overline{x^{n-s-1}g(x)}.$$

□

Colorário 4.7. *Dado um código cíclico C, existe $v \in C$ tal que $C = \langle v \rangle$.*

Demonstração. Seja $I = \nu(C)$. Logo, I é gerado como K-espaço vetorial por $\overline{g(x)}, \overline{xg(x)}, \overline{x^2g(x)}, \ldots, \overline{x^{n-s-1}g(x)}$, onde $g(x)$ é um divisor de $x^n - 1$ de grau s. Portanto, colocando $v = \nu^{-1}(\overline{g(x)})$, temos que C é gerado por $v, T_\pi(v), \ldots, T_\pi^{n-s-1}(v)$ e, portanto, $C = \langle v \rangle$. □

Colorário 4.8. *Seja $g(x) = g_0 + g_1x + \cdots + g_sx^s$ um divisor de $x^n - 1$ de grau s. Se $I = (\overline{g(x)})$, então*

$$dim_K I = n - s,$$

e o código $C = \nu^{-1}(I)$ tem matriz geradora

$$G = \begin{pmatrix} \nu^{-1}(\overline{g(x)}) \\ \nu^{-1}(\overline{xg(x)}) \\ \vdots \\ \nu^{-1}(\overline{x^{n-s-1}g(x)}) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_s & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_s & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & g_0 & \cdots & \cdots & g_s \end{pmatrix}.$$

Observação 4.9. *Dado um polinômio $h(x) = h_0 + h_1x + \cdots + h_tx^t$ que divide $x^n - 1$, temos do problema 3.1.2 da referência ([2]), que o polinômio recíproco de $h(x)$,*

$$h^*(x) = x^t h(1/x) = h_t + h_{t-1}x + \cdots + h_0x^t,$$

é também um divisor de $x^n - 1$, e portanto, é o polinômio gerador de algum código cíclico que identificaremos adiante.

Teorema 4.10. *Seja $C = \nu^{-1}(I)$ um código cíclico, onde $I = (\overline{g(x)})$, com $g(x)$ um divisor de $x^n - 1$ de grau s. Então $C^\perp$ é cíclico e $C^\perp = \nu^{-1}(J)$, onde $J = (\overline{h^*(x)})$.*

Demonstração. Ponhamos

$$g(x) = g_0 + g_1x + \cdots + g_sx^s \quad \text{e} \quad h(x) = h_0 + h_1x + \cdots + h_{n-s}x^{n-s}.$$

Note que $\mathrm{gr}(h(x)) = n - s$, e portanto, $h_{n-s} \neq 0$.

Sejam

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_s & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_s & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & g_0 & \cdots & \cdots & g_s \end{pmatrix}.$$

e

$$H = \begin{pmatrix} h_{n-s} & h_{n-s-1} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_{n-s} & h_{n-s-1} & \cdots & h_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & h_{n-s} & \cdots & \cdots & h_0 \end{pmatrix}.$$

É claro que as linhas de H são linearmente independentes.

Seja $\{e_1, \ldots, e_n\}$ a base canônica de K^n. A i-ésima linha de G é

$$G_i = g_0e_i + g_1e_{i+1} + \cdots + g_se_{i+s}, \quad 1 \leq i \leq n - s,$$

e a j-ésima linha de H é

$$H_j = h_{n-s}e_j + h_{n-s-1}e_{j+1} + \cdots + h_0e_{j+n-s}, \quad 1 \leq j \leq s.$$

Suponhamos que $i \leq j$. O produto interno de G_i por H_j é dado por

$$g_{j-i}h_{n-s} + g_{j-i+1}h_{n-s-1} + \cdots + g_{n-s}h_{j-i},$$

onde $j - i = 0, \ldots, s - 1$.

Mas a soma acima é precisamente igual ao coeficiente de $x^{n-s+j-i}$ no produto $g(x) \cdot h(x) = x^n - 1$. Como $1 < n - s + j - i \leq n - 1$, temos que esse coeficiente é igual a zero. O caso $j < i$ é análogo.

Então, temos provado que $G \cdot H^t = 0$, e portanto, pelo Lema 3.24, segue que H é uma matriz geradora de $C^\perp$. Observe, agora, que

$$H = \begin{pmatrix} \nu^{-1}(\overline{h^*(x)}) \\ \nu^{-1}(\overline{xh^*(x)}) \\ \vdots \\ \nu^{-1}(\overline{x^{n-s-1}h^*(x)}) \end{pmatrix},$$

e portanto, pelo Teorema 4.6, temos que $C^\perp = \nu^{-1}(J)$, onde $J = (\overline{h^*(x)})$. □

Colorário 4.11. *A matriz teste de paridade de $C = \nu^{-1}(I)$, em que $I = (\overline{g(x)})$, é dada por*

$$H = \begin{pmatrix} h_{n-s} & h_{n-s-1} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_{n-s} & h_{n-s-1} & \cdots & h_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & h_{n-s} & \cdots & \cdots & h_0 \end{pmatrix},$$

onde

$$\frac{x^n - 1}{g(x)} = h_0 + h_1 x + \cdots + h_{n-s}x^{n-s}.$$

Demonstração. Na verdade, esse corolário foi provado no teorema anterior. □

4.3 Decodificação em Códigos Cíclicos

Seja $C \subset K^n$ um código cíclico. Mostraremos, nesta seção, como determinar uma matriz geradora de C na forma padrão já vista antes $(R \mid Id)$ e discutiremos um algoritmo de codificação para esses códigos. No final da seção, mostraremos como se determina a síndrome nos códigos cíclicos.

Seja

$$\begin{aligned} \mu : \quad K^s \quad &\longrightarrow K[X]_{s-1} \subset K[X] \\ (a_0, \ldots, a_{s-1}) &\longmapsto \sum_{i=0}^{s-1} a_i x^i \end{aligned}$$

o isomorfismo de K-espaços vetoriais, onde $K[X]_{s-1}$ é o espaço vetorial dos polinômios de grau menor ou igual a $s-1$. Esse isomorfismo será de grande utilidade nos resultado a seguir.

Teorema 4.12. *Seja $C \subset K^n$ um código cíclico. Suponhamos que $C = \nu^{-1}(I)$, onde $I = (\overline{g(x)})$, com $g(x)$ um divisor de $X^n - 1$ de grau s. Seja R a matriz $(n-s) \times s$ cuja i-ésima linha é*

$$R_i = -\mu^{-1}(r_i(x)), \quad 1 \leq i \leq n-1,$$

onde $r_i(x)$ é o resto da divisão de x^{s-1+i} por $g(x)$. Então, $(R \mid Id_{n-s})$ é uma matriz geradora de C.

Demonstração. Sejam $q_i(x)$ e $r_i(x)$ o quociente e o resto da divisão de x^{s-1+i} por $g(x)$. Logo,

$$x^{s-1+i} = g(x)q_i(x) + r_i(x), \text{ com } r_i(x) = 0 \text{ ou } \mathrm{gr}(r_i(x)) \leq s-1.$$

Portanto, $\overline{x^{s-1+i} - r_i(x)}$ pertence a I, e é claro que esses vetores para $i = 1, \ldots, n-s$ são linearmente independentes sobre K. Como $\nu^{-1}(\overline{x^{s-1+i} - r_i(x)}) = e_{s-1+i} - \mu^{-1}(r_i(x))$, temos que a matriz

$$\begin{pmatrix} -\mu^{-1}(r_1(x)) & 1 & 0 & \cdots & 0 \\ -\mu^{-1}(r_2(x)) & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ -\mu^{-1}(r_{n-s}(x)) & 0 & 0 & \cdots & 1 \end{pmatrix}$$

é uma matriz geradora de C. □

Vamos agora, discutir o algoritmo de codificação de códigos cíclicos.

Os elementos de C podem ser considerados como codificação do código da fonte K^{n-s} conforme descrevemos abaixo.

Dado $(a_1, \ldots, a_{n-s}) \in K^{n-s}$, esse vetor pode ser codificado como elemento de C como a seguir:

$$(a_1, \ldots, a_{n-s})(R \mid Id_{n-s}) = (b_0, \ldots, b_{s-1}, a_1, \ldots, a_{n-s}),$$

onde

$$(b_0, \ldots, b_{s-1}) = -a_1\mu^{-1}(r_1(x)) - \cdots - a_{n-s}\mu^{-1}(r_{n-s}(x)) =$$

$$-\mu^{-1}(a_1r_1(x) + \cdots + a_{n-s}r_{n-s}(x)) =$$

$$-\mu^{-1}\left(\sum_{i=1}^{n-s} a_i r_i(x)\right).$$

Exemplo 4.13. *Considere o polinômio $x^7 - 1$ sobre $\mathbb{F}_2$. A fatoração de $x^7 - 1$ é dada por*

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

Vamos considerar o código $C \subset \mathbb{F}_2^7$ gerado pelo polinômio $g(x) = 1 + x + x^3$. A dimensão de C é 4. Agora, determinaremos uma matriz geradora desse código na forma padrão:

$$x^3 = (x^3 + x + 1) + (x + 1)$$

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

$$x^5 = (x^3 + x + 1)(x^2 + 1) + (x^2 + +x + 1)$$

$$x^6 = (x^3 + x + 1)(x^3 + x + 1) + (x^2 + 1)$$

Logo, pelo teorema anterior, temos que uma matriz geradora de C é dada por

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

Suponhamos que seja dado o vetor $(a_1, a_2, a_3, a_4) \in \mathbb{F}_2^4$, *do código da fonte, então, de acordo com a discussão acima, a codificação desse vetor é dada por*

$$(b_0, b_1, b_2, a_1, a_2, a_3, a_4),$$

onde b_0, b_1 *e* b_2 *são os coeficientes do polinômio. Analisemos:*

$$a_1(x+1) + a_2(x^2+x) + a_3(x^2+x+1) + a_4(x^2+1) =$$

$$a_1 + a_3 + a_4 + (a_1 + a_2 + a_3)x + (a_2 + a_3 + a_4)x^2.$$

Temos portanto, que a codificação de (a_1, a_2, a_3, a_4) *é*

$$(a_1 + a_3 + a_4, a_1 + a_2 + a_3, a_2 + a_3 + a_4 + a_1, a_2, a_3, a_4)$$

O próximo teorema nos permitirá calcular algebricamente a síndrome de um vetor relativamente a uma matriz teste de paridade num código cíclico, sem que seja necessário efetuarmos o produto matricial pela referida matriz.

Teorema 4.14. *Seja* $C \subset K^n$ *um código cíclico gerado por um polinômio mônico* $g(x)$ *de grau* s *com matriz geradora na forma padrão* $(R \mid Id_{n-s})$ *e matriz teste de paridade* $H = (Id_s \mid -R^t)$. *Se* $v = (v_0, \ldots, v_{n-1}) \in K^n$, *então a síndrome de* v *com relação à matriz* H *é dada por*

$$\mu^{-1}(r(x)),$$

onde $r(x)$ *é o resto da divisão de* $v_0 + v_1x + \cdots + v_{n-1}x^{n-1}$ *por* $g(x)$.

Demonstração. A síndrome de v é o vetor

$$(Id_s \mid -R^t)v^t =$$

$$(\mu^{-1}(1), \mu^{-1}(x), \ldots, \mu^{-1}(x^{s-1}), \mu^{-1}(r_1(x)), \ldots, \mu^{-1}(r_{n-s}(x)))v^t =$$

$$\mu^{-1}(v_0 + v_1x + \cdots + v_{s-1}x^{s-1} + v_sr_1(x) + \cdots + v_{n-1}r_{n-s}(x)),$$

o que implica o resultado que queríamos provar, visto que

$$r(x) = v_0 + v_1x + \cdots + v_{s-1}x^{s-1} + v_sr_1(x) + \cdots + v_{n-1}r_{n-s}(x)$$

é o resto da divisão de $v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}$ por $g(x)$. □

Exemplo 4.15. *Considere o código do exemplo anterior. A matriz teste de paridade associada a G' é a matriz*

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

Dado o vetor $(1101001) \in \mathbb{F}_2^8$*, a sua síndrome relativa a H é dada por $\mu^{-1}(r(x))$, onde $r(x)$ é o resto da divisão de $1 + x + x^3 + x^6$ por $g(x) = 1 + x + x^3$. Portanto, $r(x) = x^2 + 1$, e consequentemente, a síndrome é* (101).

Referências Bibliográficas

[1] Atiyah, M. F. e MacDonald, I. G.: *Introduction to commutative algebra.* Addison-Wesley-Longman, 1969.

[2] Hefez, A. e Villela, M. L. T.: *Códigos Corretores de Erros.* IMPA, 2ª ed., 2008.