Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Departamento de Matemática

Mariana de Almeida Nery Coutinho

Corpos Finitos e Códigos Corretores de Erros

Juiz de Fora
2014

Mariana de Almeida Nery Coutinho

Corpos Finitos e Códigos Corretores de Erros

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática da Universidade Federal de Juiz de Fora, como parte integrante dos requisitos necessários para obtenção do grau de Bacharel em Matemática.

Orientadora: Beatriz Casulari da Motta Ribeiro

Juiz de Fora

2014

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

Coutinho, Mariana de Almeida Nery.
Corpos Finitos e Códigos Corretores de Erros / Mariana de Almeida Nery Coutinho. – 2014.
73 f. : il.

Orientadora: Beatriz Casulari da Motta Ribeiro
Trabalho de Conclusão de Curso (Graduação) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas, Departamento de Matemática, 2014.

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

Mariana de Almeida Nery Coutinho

Corpos Finitos e Códigos Corretores de Erros

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática da Universidade Federal de Juiz de Fora, como parte integrante dos requisitos necessários para obtenção do grau de Bacharel em Matemática.

Aprovado em 04 de novembro de 2014

BANCA EXAMINADORA

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

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

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

AGRADECIMENTOS

À Deus em primeiro lugar.

Aos meus pais e irmão, pelo incentivo incessante e por terem sido os meus primeiros professores. Aos meus avós, tios e primos, por todo o apoio.

À professora e orientadora Beatriz Casulari da Motta Ribeiro, por ter me proporcionado as primeiras oportunidades de estudar e conhecer a Álgebra, desde a Introdução à Teoria dos Números até os Corpos Finitos; pela alegria com que explicava cada tópico em suas aulas e horários de atendimento; e especialmente, pela amizade, apoio e incentivo durante todo esse período.

À professora Flaviana Andrea Ribeiro, por ter me ensinado boa parte do que hoje sei sobre Álgebra, motivando, a cada aula, o meu interesse por essa área e auxiliando, nesta fase, com a avaliação e correção deste trabalho.

Ao professor Frederico Sercio Feitosa, por ter aceitado o convite para fazer parte da banca que avaliou este trabalho, colaborando para o resultado final aqui apresentado.

A cada um dos meus professores da graduação, por tudo que ensinaram e contribuíram para o meu crescimento acadêmico e pessoal. Em especial, agradeço aos professores Regis Castijos Alves Soares Junior, Orestes Piermatei Filho e Lucy Tiemi Takahashi que, além das aulas, me incentivaram e apoiaram na escolha do curso de Matemática; ao professor André Arbex Hallack, por ter me apresentado os primeiros ideais e anéis, bem como por ser o responsável, juntamente com a professora Lucy, por praticamente toda a minha base de Álgebra Linear, disciplina essa que foi fundamental para eu pudesse enxergar que realmente gostava de Matemática; aos professores Olimpio Hiroshi Miyagaki e Fábio Rodrigues Pereira, por terem contribuído para que eu gostasse um pouquinho mais de Análise; e aos professores Luis Fernando Crocco Afonso e Laercio José dos Santos, por terem despertado o meu interesse pela Geometria e sobretudo pelo apoio e incentivo.

Ao professor Maikel Yusat Ballester Furones, pela enorme contribuição para a minha formação acadêmica e pessoal enquanto sua aluna de Iniciação Científica.

Ao amigo Bruno Marques, pelo apoio incondicional.

Ao amigo Eli Vilela, pelas conversas sobre Matemática e diversos outros assuntos.

A todos os meus amigos da graduação, pelo importante papel que representaram para que esse momento se concretizasse. Em especial, agradeço à Adriele, à Janaína e ao Leandro, amigos que estiveram sempre ao meu lado compartilhando momentos de alegria e estudo, bem como me ajudando nos momentos mais difíceis; à Sandra, pela amizade e pelo exemplo que foi para mim durante todos esses anos; ao Gladston, pela enorme companhia durante as aulas de Álgebra Linear, por todas as risadas e por toda a ajuda no momento em que decidi cursar Matemática; ao Weslley, pela amizade e pela ajuda, juntamente com a Sandra, para que diversos problemas pudessem ser resolvidos.

A todos os meus amigos do mestrado, em especial à Eliza, pela companhia e amizade ao longo dos últimos dois anos; à Yulia, ao Vladimir, ao Julio, ao Carlos, à Lívia, à Taís e ao Erasmo, pelos momentos de estudo e descontração; ao Eduardo e ao Pavel, por toda a ajuda com os problemas de Geometria Diferencial e Medida e Integração; ao Juan, pela amizade, companhia, pelas conversas sobre o Peru, além da ajuda e explicações nas aulas de Álgebra; ao Oscar, por todo o apoio; ao Santiago, por toda a ajuda e companhia, bem como por todas as conversas e explicações de espanhol; e à Gisele, pelo grande exemplo.

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

À Propesq - UFJF, pelas bolsas de Iniciação Científica.

RESUMO

Neste trabalho, estamos interessados em estudar duas estruturas algébricas especiais, os Corpos Finitos e os Códigos Corretores de Erros, onde a primeira é a base sobre a qual boa parte da Teoria dos Códigos está desenvolvida.

O nosso estudo dos Códigos Corretores de Erros está centrado numa classe especial destes, os chamados códigos lineares, dos quais apresentamos os Códigos Cíclicos, BCH e de Goppa Clássicos.

Palavras-chave: Álgebra Abstrata. Corpos Finitos. Códigos Corretores de Erros.

ABSTRACT

In this work, we are interested in studying two special algebraic structures, the Finite Fields and the Error-Correcting Codes, where the first is the basis on which much of the Coding Theory is developed.

Our study of the Error-Correcting Codes focuses on a special class of these, the so-called linear codes, of which are presented Cyclic, BCH and Classical Goppa Codes.

Key-words: Abstract Algebra. Finite Fields. Error-Correcting Codes.

SUMÁRIO

1 INTRODUÇÃO

A detecção e correção de erros presentes em informações que circulam por intermédio dos mais diversos meios é um dos desafios inerentes à vida em sociedade. Nesse sentido, surge na década de 1940, no Laboratório Bell de Tecnologia, com os trabalhos de Richard W. Hamming e C. E. Shannon, a Teoria dos Códigos, que possui como objetivo a elaboração de mecanismos capazes de permitir uma transmissão confiável de dados através de canais sujeitos a interferências, também denominadas ruídos.

Algumas áreas da Álgebra Abstrata tiveram um papel importante para o desenvolvimento da Teoria dos Códigos, dentre as quais é possível destacar a Teoria dos Corpos Finitos, a teoria de anéis de polinômios sobre esses corpos, a Geometria Algébrica e a Teoria de Grupos.

O presente trabalho tem por objetivo apresentar alguns elementos da Teoria dos Corpos Finitos e da Teoria dos Códigos Corretores de Erro, com destaque para os códigos lineares. Como exemplos destes últimos, exibiremos os Códigos Cíclicos, introduzidos por E. Prange, no período de 1957 a 1959, e W. W. Peterson em 1961; os Códigos BCH, desenvolvidos inicialmente por Alexis Hocquenghem e, de forma independente, por Raj Chandra Bose e Dwijendra Kumar Ray-Chaudhuri, por volta de 1960; e os Códigos de Goppa Clássicos, desenvolvidos V. D. Goppa em 1970, como uma generalização dos Códigos BCH.

No Capítulo 2, apresentaremos os fundamentos algébricos, destacando definições e resultados necessários para o desenvolvimento do texto.

No Capítulo 3, exibiremos alguns dos principais resultados referentes à Teoria dos Corpos Finitos, incluindo aqueles que são importantes para o desenvolvimento da Teoria dos Códigos Corretores de Erro.

No Capítulo 4, faremos uma introdução aos Códigos Corretores de Erros, apresentando na seção 4.1 os elementos gerais dessa teoria e na seção 4.2 os códigos lineares. Além disso, na seção 4.3, exibiremos os Códigos Cíclicos, na seção 4.4, os códigos BCH, e por último, na seção 4.5, os chamados Códigos de Goppa Clássicos.

2 FUNDAMENTOS ALGÉBRICOS

O objetivo principal deste capítulo é estabelecer alguns tópicos estudados em Álgebra Abstrata e que serão úteis para o desenvolvimento e melhor compreensão do restante do texto.

2.1 UM POUCO SOBRE EXTENSÕES DE CORPOS

Nesta seção, apresentaremos resultados de extensões de corpos, que se aplicam não somente aos conjuntos que objetivamos aqui estudar, os corpos finitos, mas também aos corpos de uma forma geral. Lembramos, para isso, que um corpo é um anel comutativo com unidade no qual todo elemento não nulo possui inverso.

Definição 2.1.1. Sejam F e K corpos. Dizemos que F é uma extensão de K se K for um subcorpo de F, isto é, $K \subset F$, $(K, +)$ é subgrupo de $(F, +)$ e $(K \setminus \{0\}, \cdot)$ é subgrupo de $(F \setminus \{0\}, \cdot)$.

Observação 2.1.2. Se F é uma extensão do corpo K, então as operações

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

fazem de F um espaço vetorial sobre K.

Desse modo, chegamos à seguinte definição para uma extensão F de K.

Definição 2.1.3. Chamamos de grau da extensão a dimensão de F como espaço vetorial sobre K. Tal dimensão será denotada por $[F : K]$.

Definição 2.1.4. Dizemos que F é uma extensão finita de K se $[F : K] < +\infty$. Caso contrário, dizemos que F é uma extensão infinita de K.

Teorema 2.1.5. *Sejam K um corpo, F uma extensão finita de K e L uma extensão finita de F. Então L é uma extensão finita de K, com*

$$[L : K] = [L : F][F : K].$$

Demonstração. Coloquemos $m = [L : F]$, $n = [F : K]$ e sejam $\{\alpha_1, ..., \alpha_m\}$ e $\{\beta_1, ..., \beta_n\}$ bases do espaço vetorial L sobre F e do espaço vetorial F sobre K, respectivamente. Então todo $\alpha \in L$ é uma combinação linear do tipo $\alpha = \gamma_1\alpha_1 + ... + \gamma_m\alpha_m$, onde $\gamma_i \in F$, $\forall\, i = 1, ..., m$. Agora, escrevendo cada $\gamma_i \in F$ como combinação linear dos termos da base $\{\beta_1, ..., \beta_n\}$, obtemos a seguinte expressão:

$$\alpha = \sum_{i=1}^{m} \gamma_i\alpha_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} r_{ij}\beta_j \right) \alpha_i = \sum_{i=1}^{m} \sum_{j=1}^{n} r_{ij}\beta_j\alpha_i$$

onde $r_{ij} \in K$. Para concluirmos a demonstração, basta mostrar que os elementos $\beta_j\alpha_i$, com $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, são linearmente independentes sobre K. Dessa forma, suponhamos que

$$\sum_{i=1}^{m} \sum_{j=1}^{n} s_{ij}\beta_j\alpha_i = 0$$

com $s_{ij} \in K$. Então,

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n} s_{ij}\beta_j \right) \alpha_i = 0$$

e pela independência linear dos elementos α_i sobre F, temos que

$$\sum_{j=1}^{n} s_{ij}\beta_j = 0.$$

Do mesmo modo, pela independência linear dos elementos β_j sobre K, temos que $s_{ij} = 0$, $\forall\, i = 1, ..., m$, $\forall\, j = 1, ..., n$. ■

Definição 2.1.6. Sejam F um corpo e $X \subset F$ um subconjunto qualquer. O subcorpo gerado por X é a interseção de todos os subcorpos de F que contêm X. Se K for um subcorpo de F e $X \subset F$, então o subcorpo gerado por $K \cup X$ é dito corpo obtido de K adjuntando X e será denotado por $K(X)$.

Se o subconjunto X de F for finito, digamos $X = \{\alpha_1, ..., \alpha_n\}$, então escreveremos $K(X) = K(\alpha_1, ..., \alpha_n)$.

Definição 2.1.7. Dizemos que um corpo F é uma extensão simples do corpo K se existir $\alpha \in F$ tal que $F = K(\alpha)$. Neste caso, α é chamado elemento definidor de F sobre K.

Definição 2.1.8. Seja F uma extensão do corpo K. Dizemos que $u \in F$ é algébrico sobre K se existir $p(x) \in K[x] \setminus \{0\}$ tal que $p(u) = 0$. Caso contrário, dizemos que u é transcendente sobre K.

Definição 2.1.9. Dizemos que o corpo F é uma extensão algébrica do corpo K se $u \in F$ for algébrico sobre K, para todo $u \in F$. Se pelo menos um elemento de F for transcendente sobre K, dizemos que F é uma extensão transcendental (ou transcendente) de K.

Como exemplo, temos que:

a) $i \in \mathbb{C}$ é algébrico sobre $\mathbb{Q}$. De fato, $g(i) = 0$, onde $g(x) = x^2 + 1 \in \mathbb{Q}[x]$;

b) $\mathbb{C}$ é uma extensão algébrica de $\mathbb{R}$. Com efeito, dado $\alpha = a + ib \in \mathbb{C}$, a, $b \in \mathbb{R}$, temos que $\alpha - a = ib \Rightarrow \alpha^2 - 2a\alpha + a^2 = -b^2 \Rightarrow \alpha^2 - 2a\alpha + a^2 + b^2 = 0$. Assim $g(x) = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$ é tal que $g(\alpha) = 0$;

c) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$ é uma extensão algébrica de $\mathbb{Q}$. De fato, dado $\alpha = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, a, $b \in \mathbb{Q}$, temos que $\alpha - a = b\sqrt{2} \Rightarrow \alpha^2 - 2a\alpha + a^2 = 2b^2 \Rightarrow \alpha^2 - 2a\alpha + a^2 - 2b^2 = 0$. Assim $g(x) = x^2 - 2ax + a^2 - 2b^2 \in \mathbb{Q}[x]$ á tal que $g(\alpha) = 0$.

Definição 2.1.10. Sejam $\alpha \in F$ um elemento algébrico sobre K. O polinômio $m(x) \in K[x]$ mônico de menor grau tal que $m(\alpha) = 0$ é chamado polinômio mínimo de α e denotado por $irr(\alpha, K)$.

Segue da definição 2.1.10 que o polinômio minimal $irr(\alpha, K)$ é o único polinômio mônico irredutível que anula α. Além disso, se $q(x) \in K[x]$ for tal que $q(\alpha) = 0$, então $irr(\alpha, K)|q(x)$.

Teorema 2.1.11. *Sejam F uma extensão do corpo K e $\alpha \in F$. Então α é algébrico sobre K se, e somente se, $K(\alpha)$ for uma extensão finita de K.*

Demonstração. Consideremos o homomorfismo

$$\begin{array}{rccc} \varphi: & K[x] & \to & K(\alpha) \\ & f(x) & \mapsto & f(\alpha) \end{array}$$

que tem por imagem o conjunto

$$Im(\varphi) = K[\alpha] = \{f(\alpha);\ f \in K[x]\}$$

e por núcleo o conjunto

$$Ker(\varphi) = \{f(x) \in K[x];\ f(\alpha) = 0\}.$$

Primeiramente, suponhamos α algébrico sobre K. Temos então que $Ker(\varphi) \neq \{0\}$ (por definição). Ainda, $K(\alpha)$ corpo $\Rightarrow$ $K(\alpha)$ domínio de integridade $\Rightarrow$ $Ker(\varphi)$ é um ideal primo. Sendo $K[x]$ um domínio euclidiano, temos que $K[x]$ é um domínio de ideais principais. Dessa forma, $Ker(\varphi) = \langle m(x) \rangle$ é um ideal maximal, onde $m(x) \in K[x]$ é irredutível. Pelo 1º Teorema de Isomorfismos de Anéis, temos $\dfrac{K[x]}{Ker(\varphi)} = Im(\varphi) = K[\alpha]$. Como $Ker(\varphi)$ é um ideal maximal, temos que $\dfrac{K[x]}{Ker(\varphi)}$ é um corpo. Logo $K[\alpha]$ é um corpo (contendo K e α). Da definição de $K(\alpha)$ e da inclusão $K[\alpha] \subset K(\alpha)$, temos que $K[\alpha] = K(\alpha)$.
Mostremos agora que $B = \{1, \alpha, ..., \alpha^{n-1}\}$ é uma base de $K[\alpha] = K(\alpha)$ sobre K, onde $n = gr(m(x))$. Com efeito, dado, $a \in K[\alpha]$, existe $p(x) \in K[x]$ tal que $a = p(\alpha)$. Sendo $(K[x], gr)$ um domínio euclidiano, temos que existem $q(x)$, $r(x) \in K[x]$ tais que $p(x) = q(x)m(x) + r(x)$, com $r(x) = 0$ ou $gr(r(x)) < gr(m(x)) = n$. Daí, $a = p(\alpha) = r(\alpha)$, onde $r(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$, $a_i \in K$, isto é, $a = p(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$, mostrando que B gera $K[\alpha]$ sobre K. Ainda, se $b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1} = 0$, então $p(x) = b_0 + b_1x + ... + b_{n-1}x^{n-1}$ é tal que $p(\alpha) = 0$, com $p(x) = 0$ ou $gr(p(x)) \leqslant n - 1 < n = gr(m(x))$. Mas se o segundo caso ocorresse, teríamos uma contradição com a minimalidade do grau de $m(x)$ (gerador de $Ker(\varphi)$). Portanto, $p(x) = 0$, o que nos dá que $b_0 = ... = b_{n-1} = 0$, isto é, B é um conjunto L. I. sobre K.
Dessa forma, concluímos que $K(\alpha) = K[\alpha]$ é uma extensão finita.

Por outro lado, se $[K(\alpha) : K] = n < +\infty$, então qualquer subconjunto de $K(\alpha)$ com mais de n elementos é L. D.. Daí, $\{1, \alpha, ..., \alpha^n\}$ é L. D. sobre K, donde existem elementos a_0, ..., $a_n \in K$, não todos nulos, tais que $a_0 + a_1\alpha + ... + a_n\alpha^n = 0$. Logo α é raiz de $p(x) = a_0 + a_1x + ... + a_nx^n$, o que nos dá que α é algébrico sobre K. ■

Teorema 2.1.12. *Toda extensão finita de um corpo K é algébrica sobre K.*

Demonstração. Seja L uma extensão finita de K e coloquemos $m = [L : K]$. Dado $\alpha \in L$, os $m + 1$ elementos $1, \alpha, ..., \alpha^m$ devem ser L. D. sobre K e assim, é possível obtermos uma combinação linear $a_0+a_1\alpha+...+a_m\alpha^m = 0$, com $a_i \in K$, $\forall\, i = 1, ..., m$ e com $a_i \neq 0$ para algum $i \in \{1, ..., m\}$. Assim, se $p(x) = a_m x^m + ... + a_1 x + a_0$, temos que $p(\alpha) = 0$, isto é, α é algébrico sobre K. ■

Exemplo 2.1.13. Seja $K \supset \mathbb{Q}$ tal que $[K : \mathbb{Q}] = m$ e seja $p(x) \in \mathbb{Q}[x]$ um polinômio irredutível sobre $\mathbb{Q}$ de grau n. Se $mdc(m, n) = 1$, então $p(x)$ é um polinômio irredutível sobre K.

Demonstração. Seja $\alpha \in \mathbb{C}$ uma raiz de $p(x)$. Sabendo que $\mathbb{Q}[\alpha] \subset K[\alpha]$ e colocando $[K[\alpha] : K] = r$ e $[K[\alpha] : \mathbb{Q}[\alpha]] = s$, temos que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$ e $[K[\alpha] : K] = r = n$. De fato, pelo teorema 2.1.5, segue que $[K[\alpha] : \mathbb{Q}[\alpha]][\mathbb{Q}[\alpha] : \mathbb{Q}] = [K[\alpha] : \mathbb{Q}] = [K[\alpha] : K][K : \mathbb{Q}]$, isto é, $sn = rm$. Como $mdc(m, n) = 1$, segue que $n|r$. Mas $r \leqslant n$ (pois podemos enxergar o polinômio mínimo de α sobre $\mathbb{Q}$ em $K[x]$, de forma que o polinômio mínimo de α sobre K divide o polinômio mínimo de α sobre $\mathbb{Q}$) e, portanto, $n = r$, o que resulta em $p(x)$ irredutível sobre K. ■

2.2 CORPO DE DECOMPOSIÇÃO

Definição 2.2.1. Sejam K é um corpo e $f(x) \in K[x]$. Dizemos que $f(x)$ se fatora em $K[x]$ 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, ..., $\alpha_n \in K$.

Nas condições da definição 2.2.1, temos que os zeros de $f(x)$ em K são exatamente os elementos α_1, ..., α_n. Além disso, se F é uma extensão de K, então $f(x)$ também pertence a $F[x]$. Dessa forma, faz sentido falarmos na fatoração de $f(x)$ em $F[x]$, significando que $f(x)$ é o produto de fatores lineares com coeficientes em F.

Definição 2.2.2. Sejam K um corpo e Σ uma extensão de K. Então Σ é um corpo de decomposição para o polinômio $f(x) \in K[x]$ se:

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

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

Lema 2.2.3. *Sejam K um corpo e $f(x) \in K[x]$ irredutível. Então existem um corpo F e $\alpha \in F$ tais que $K \subset F$ e $f(\alpha) = 0$. Além disso $[F : K] = gr(f(x))$.*

Demonstração. Consideremos o anel $F = \dfrac{K[x]}{\langle f(x)\rangle}$. Como K é um corpo, $K[x]$ é um domínio euclidiano e dessa forma um domínio de ideais principais. Logo $f(x)$ ser irredutível implica que $\langle f(x)\rangle$ é um ideal maximal, o que nos dá que $F = \dfrac{K[x]}{\langle f(x)\rangle}$ é um corpo. Os elementos de F são as classes $\overline{h(x)} = h(x) + \langle f(x)\rangle$, com $h(x) \in K[x]$. Para todo $a \in K \subset K[x]$ (esta inclusão é um homomorfismo injetor que identifica $a \in K$ com o polinômio constante $a(x) = a \in K[x]$), é possível construir a classe $\overline{a}$ e se $b \in K$, $b \neq a$, então $\overline{a} \neq \overline{b}$, já que $f(x)$ possui grau positivo por não ser invertível. A aplicação $a \mapsto \overline{a}$ fornece um isomorfismo de K sobre um subcorpo K_1 de F, de modo que F pode ser visto como uma extensão de K.
Dado $h(x) = a_0 + a_1x + ... + a_mx^m \in K[x]$, temos que

$$\begin{aligned}\overline{h(x)} &= \overline{a_0 + a_1x + ... + a_mx^m} \\ &= \overline{a_0} + \overline{a_1x} + ... + \overline{a_mx}^m \\ &= a_0 + a_1\overline{x} + ... + a_m\overline{x}^m\end{aligned}$$

onde a última igualdade segue da identificação $a \mapsto \overline{a}$. Dessa forma, todo elemento de F pode ser escrito como um polinômio com coeficientes em K aplicado ao elemento $\overline{x}$. Como todo corpo que contém K e $\overline{x}$ deve conter elementos da forma $h(\overline{x})$, $h(x) \in K[x]$, temos que $F \subset K(\overline{x}) = K[\overline{x}]$, o que nos dá que $F = K(\overline{x}) = K[\overline{x}]$ pela definição de $K(\overline{x})$. Ainda, se $f(x) = b_0 + b_1x + ... + b_nx^n$, então

$$f(\overline{x}) = b_0 + b_1\overline{x} + ... + b_n\overline{x}^n = \overline{b_0 + b_1x + ... + b_nx^n} = \overline{f(x)} = \overline{0}\,.$$

Portanto, $\overline{x}$ é uma raiz de $f(x)$ em F e assim $\overline{x}$ é um elemento algébrico sobre K. Por último, $(1/b_n)f(x) = irr(\overline{x}, K)$ nos dá que $[F : K] = n$. ∎

Corolário 2.2.4. *Se $f(x) \in K[x] \setminus K$, onde K é um corpo, então existe uma extensão finita F de K onde $f(x)$ possui uma raiz. Além disso, $[F : K] \leqslant gr(f(x))$.*

Demonstração. Seja $p(x)$ um fator irredutível de $f(x)$ (tal fator sempre existe pois K ser corpo $\Rightarrow K[x]$ é domínio euclidiano $\Rightarrow K[x]$ é domínio de fatoração única). Qualquer raiz de $p(x)$ é uma raiz de $f(x)$. Pelo lema 2.2.3, existe uma extensão F de K, com $[F : K] = gr(p(x)) \leqslant gr(f(x))$, onde $p(x)$, e consequentemente, $f(x)$ possui uma raiz. ■

Lema 2.2.5. *Sejam K um corpo e $f(x) \in K[x] \setminus K$, com $gr(f(x)) = n$. Então existe uma extensão F de K, com $[F : K] \leqslant n!$, onde $f(x)$ possui n raízes (contadas com multiplicidade).*

Demonstração. Pelo corolário 2.2.4, existe uma extensão F_0 de K com $[F_0 : K] \leqslant n$ em que $f(x)$ possui uma raiz α. Assim, em $F_0[x]$, $f(x)$ fatora-se como $f(x) = (x - \alpha)q(x)$, onde $gr(q(x)) = n - 1$. Por indução matemática, existe uma extensão F de F_0 de grau no máximo $(n - 1)!$ na qual $q(x)$ possui $n - 1$ raízes. Já que as raízes de $f(x)$ são α ou as raízes de $q(x)$, temos que F contém todas as n raízes de $f(x)$. Além disso, $[F : K] = [F : F_0][F_0 : K] \leqslant (n - 1)! \times n = n!$. Portanto, o resultado segue. ■

Teorema 2.2.6. *Se K é um corpo qualquer e $f(x) \in K[x]$, então existe um corpo de decomposição de $f(x)$ sobre K.*

Demonstração. A demonstração deste teorema está feita nos lemas 2.2.3 e 2.2.5, notando-se que o corpo F construído é o menor corpo que contém K e todas as raízes de $f(x)$. Com efeito, $F = K(\sigma_1, ..., \sigma_n)$, onde $\sigma_1, ..., \sigma_n$ são todas as raízes (não necessariamente distintas) de $f(x)$. ■

Seja $i : K \to F$ um homomorfismo injetor entre corpos. Definimos a aplicação $\hat{i} : K[x] \to F[x]$ dada por

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

Desse modo, $\hat{i}$ é um homomorfismo injetor e, mais ainda, se i for um isomorfismo, $\hat{i}$ também será.

Temos a unicidade do corpo de decomposição de um polinômio $f(x)$ sobre um corpo K no sentido do teorema a seguir, cuja demonstração pode ser encontrada em [4].

Teorema 2.2.7. *Sejam $i : K \to K'$ um isomorfismo entre corpos. Sejam Σ um corpo de decomposição de $f(x) \in K[x]$ e Σ' um corpo de decomposição de $\hat{i}(f(x))$ sobre K'. Então existe um isomorfismo $j : \Sigma \to \Sigma'$ tal que $j|_K = i$. Em outras palavras, as extensões Σ e Σ' são isomorfas.*

Como consequência do teorema 2.2.7, temos que corpos isomorfos possuem corpos de decomposição isomorfos.

3 CORPOS FINITOS

O principal objetivo deste capítulo é realizar uma introdução aos corpos finitos, apresentando algumas das suas propriedades mais importantes, entre elas as que se referem às extensões de corpos.

3.1 PRIMEIRAS DEFINIÇÕES E PROPRIEDADES

Definição 3.1.1. Seja A um anel. Definimos, para cada $n \in \mathbb{Z}$ e para cada $a \in A$,

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

Definição 3.1.2. Seja A um anel. A característica de A, denotada por $char(A)$, é o menor inteiro positivo n tal que $n \cdot a = 0$, $\forall\, a \in A$. Se não existir tal inteiro, dizemos que a característica de A é zero.

Proposição 3.1.3. *Seja $(A, +, \times)$ um anel com unidade.*

a) Se $n \cdot 1 \neq 0$, $\forall\, n \in \mathbb{N}$, então $char(A) = 0$.

b) Se existir $n \in \mathbb{N}$ tal que $n \cdot 1 = 0$, então $char(A) = min\{n \in \mathbb{N};\, n \cdot 1 = 0\}$.

Demonstração. a) Como não existe $n \in \mathbb{N}$ tal que $n \cdot 1 = 0$, temos que não existe $n \in \mathbb{N}$ tal que $n \cdot a = 0$, $\forall\, a \in A$. Logo $char(A) = 0$.
b) Seja $n = min\{n \in \mathbb{N};\, n \cdot 1 = 0\}$. Então, para todo $a \in A$ temos, de $a = 1 \times a$, que $n \cdot a = n \cdot (1 \times a) = \underbrace{1 \times a + \ldots + 1 \times a}_{n} = \underbrace{(1 + \ldots + 1)}_{n} \times a = (n \cdot 1) \times a = 0 \times a = 0$.
Como o n considerado é mínimo no conjunto $\{n \in \mathbb{N};\, n \cdot 1 = 0\}$, temos que ter $n = char(A)$. ■

Proposição 3.1.4. *Seja $A \neq \{0\}$ um domínio de integridade. Então $char(A) = 0$ ou $char(A) = p$, onde p é um número primo.*

Demonstração. Se $char(A) = 0$, então nada há para mostrar. Caso contrário, como $A \neq \{0\}$, existe um elemento não nulo em A, de modo que $char(A) \geqslant 2$. Se $char(A)$ não for um número primo, então é possível escrever $char(A) = m \cdot n$, com $m, n \in \mathbb{Z}$, $1 < m$, $n < char(A)$. Logo $0 = char(A) \cdot 1 = (m \cdot n) \cdot 1 = (m \cdot 1) \times (n \cdot 1)$. Como A não possui divisores de zero, temos que $m \cdot 1 = 0$ ou $n \cdot 1 = 0$, o que é uma contradição pela proposição 3.1.3. ■

Corolário 3.1.5. *Todo corpo finito possui característica prima.*

Demonstração. Pela proposição 3.1.3 basta mostrarmos que todo corpo finito possui característica positiva. Para isso, seja K um corpo finito e consideremos os múltiplos 1, $2 \cdot 1$, $3 \cdot 1$, ... da unidade de K. Como K possui somente um número finito de elementos distintos, temos que existem inteiros m, $n \in \mathbb{Z}$ tais que $1 \leqslant m < n$ e $m \cdot 1 = n \cdot 1$, ou seja, $(n - m) \cdot 1 = 0$ e assim K possui característica positiva. ■

Como exemplo de corpo finito com p elementos, onde p é um número primo, temos o corpo $\mathbb{Z}_p := \mathbb{Z}/\langle p \rangle$. Dado um número primo p, sejam $\mathbb{F}_p$ o subconjunto $\{0, 1, ..., p-1\}$ dos inteiros e $\varphi : \mathbb{Z}_p \to \mathbb{F}_p$ a aplicação definida por $\varphi(\overline{a}) = a$, para $a = 0, 1, ..., p-1$. Então $\mathbb{F}_p$, com a estrutura de corpo induzida por φ, é um corpo finito, chamado corpo de Galois de ordem p.

Se K é um subcorpo de um corpo finito $\mathbb{F}_p$, sendo p um número primo, então 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 K.

Definição 3.1.6. Sejam F um corpo e K um subcorpo de F, com $K \neq F$. Então K é dito um subcorpo próprio de F.

Definição 3.1.7. Dizemos que um corpo F é primo quando este não contém nenhum subcorpo próprio.

Pelo argumento acima, temos que o corpo finito $\mathbb{F}_p$, onde p é um número primo, é um corpo primo. Um outro exemplo de corpo primo é o corpo $\mathbb{Q}$ dos números racionais.

O corpo $\mathbb{F}_p$, onde p é um número primo, ainda desempenha um importante papel na teoria dos corpos. Com efeito, todo corpo finito de característica p contém

uma "cópia" de $\mathbb{F}_p$, uma vez que o seu subcorpo primo é isomorfo a $\mathbb{F}_p$, conforme a proposição 3.1.8 a seguir.

Proposição 3.1.8. *O subcorpo primo de um corpo F de característica p, onde p é um número primo, é isomorfo à $\mathbb{F}_p$.*

Demonstração. Consideremos a aplicação $\varphi : \mathbb{Z}_p \to F$ dada por $\varphi(\overline{n}) = n \cdot 1$. Em primeiro lugar essa aplicação está bem definida. Com efeito, se $\overline{n} = \overline{m}$ em $\mathbb{Z}_p$, onde m e n são dois inteiros, então existe $\lambda \in \mathbb{Z}$ tal que $n = m + \lambda p$, de modo que $n \cdot 1 = (m + \lambda p) \cdot 1 = m \cdot 1 + (\lambda p) \cdot 1 = m \cdot 1 + \lambda \cdot (p \cdot 1) = m \cdot 1$. Além disso, a função φ é um homomorfismo. Logo, sendo $\mathbb{Z}_p$ e F corpos, temos que φ é um homomorfismo injetor e assim $\varphi(\mathbb{Z}_p)$ é um subcorpo de F isomorfo $\mathbb{Z}_p$. Como qualquer subcorpo de F contém 0 e 1, temos que qualquer subcorpo também irá conter $\varphi(\mathbb{Z}_p)$. Logo $\varphi(\mathbb{Z}_p)$ é o subcorpo primo de F e é isomorfo a $\mathbb{F}_p$. ■

Finalizamos essa seção apresentando um interessante resultado aritmético da teoria dos corpos finitos, que pode ser demonstrado utilizando o Binômio de Newton.

Proposição 3.1.9. *Seja F um corpo finito de característica p e seja $q = p^n$, $n \in \mathbb{N}$. Se a, $b \in F$, temos que $(a \pm b)^q = a^q \pm b^q$.*

Ainda, aplicando-se o princípio da indução e a proposição 3.1.9, temos:

Corolário 3.1.10. *Sejam F um corpo finito de característica p e a_0, ..., a_n elementos de F. Se $q = p^r$, para algum r inteiro positivo, então $(a_0 + ... + a_n)^q = a_0^q + ... + a_n^q$. Além disso, se $p(x) = a_0 + a_1 x + ... + a_n x^n$, então $p(x)^q = a_0^q + a_1^q x^q + ... + a_n^q x^{nq}$.*

3.2 CARACTERIZAÇÃO DOS CORPOS FINITOS

Lema 3.2.1. *Seja F um corpo finito contendo um subcorpo K com q elementos. Então F possui q^m elementos, onde $m = [F : K]$.*

Demonstração. Sabendo que F pode ser visto como um espaço vetorial sobre K, temos que a dimensão do espaço vetorial F sobre o corpo K é finita, uma vez que

F é um corpo finito. Colocando $m = [F : K]$, temos que F possui uma base sobre K constituída por m elementos b_1, b_2, ..., b_m. Assim, todo elemento de F pode ser escrito de forma única como $a_1b_1 + a_2b_2 + ... + a_mb_m$, onde a_1, a_2, ..., $a_m \in K$. Para concluir a demonstração, basta notar que, como K possui q elementos, F possui exatamente q^m elementos. ■

Teorema 3.2.2. *Seja F um corpo finito. Então F possui p^n elementos, onde $p = char(F)$ e n é a dimensão de F quando visto como um espaço vetorial sobre o seu corpo primo.*

Demonstração. Como F é finito, sua característica é um número primo p. Logo, o subcorpo primo K de F é isomorfo a $\mathbb{F}_p$ e assim contém p elementos. O restante da prova segue diretamente do lema 3.2.1. ■

Proposição 3.2.3. *Se F é um corpo finito com q elementos, então, para todo $a \in F$, temos que $a^q = a$.*

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

Proposição 3.2.4. *Se F é um corpo finito com q elementos e K é um subcorpo de F, então o polinômio $x^q - x \in K[x]$ é fatorado em $F[x]$ na forma*

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

e F é um corpo de decomposição de $x^q - x$ sobre K.

Demonstração. O polinômio $x^q - x$ de grau q possui no máximo q raízes em F. Ainda, pelo proposição 3.2.3, temos que todos os elementos de F são raízes de $x^q - x$. Assim, o polinômio $x^q - x$ fatora-se em F e não pode fatorar-se em nenhum corpo menor, o que nos diz que F é um corpo de decomposição do polinômio $x^q - x$. ■

Na sequência, será apresentado o teorema de existência e unicidade dos corpos finitos. Para tal, serão fornecidas duas demonstrações, uma teórica e outra mais construtiva. Para a primeira forma de demonstração, utilizaremos os resultados até aqui desenvolvidos. Já para a segunda, serão necessários os resultados e definições a seguir.

Proposição 3.2.5. *Seja K um corpo finito com q elementos e seja $f(x) \in K[x]$ um polinômio mônico irredutível de grau d. Consideremos o corpo $F = K[x]/\langle f(x)\rangle$. Então temos que:*

a) $\overline{1}$, $\overline{x}$, $\overline{x^2}$, ..., $\overline{x^{d-1}}$ *formam uma base de F sobre K.*

b) $\overline{x}^{q^d} = \overline{x}$ *em F.*

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

d) Os elementos $\overline{x}$, $\overline{x}^q$, ..., $\overline{x}^{q^{d-1}}$ *de F são distintos e são as raízes de $f(x)$.*

Demonstração. a) Dado $\overline{p(x)} \in F$, temos que existem polinômios $q(x)$, $r(x)$ em $K[x]$ tais que $p(x) = q(x)f(x) + r(x)$, onde $r(x) = 0$ ou $gr(r(x)) < d$. Assim $\overline{p(x)} = \overline{r(x)}$. Como $r(x) = a_0 + a_1x + ... + a_{d-1}x^{d-1}$, segue que

$$\overline{p(x)} = \overline{a_0 + a_1x + ... + a_{d-1}x^{d-1}} = a_0 + a_1\overline{x} + ... + a_{d-1}\overline{x^{d-1}}$$

o que mostra que $\{\overline{1}, \overline{x}, \overline{x^2}, ..., \overline{x^{d-1}}\}$ gera F sobre K. Agora, suponhamos que $a_0 + a_1\overline{x} + ... + a_{d-1}\overline{x^{d-1}} = \overline{0}$. Então $\overline{a_0 + a_1x + ... + a_{d-1}x^{d-1}} = \overline{0}$, de forma que $f(x)|(a_0 + a_1x + ... + a_{d-1}x^{d-1})$. Como $gr(f(x)) = d$, isso só ocorre se $a_0 + a_1x + ... + a_{d-1}x^{d-1} = 0$, ou seja, se $a_0 = a_1 = ... = a_{d-1} = 0$, de forma que $\overline{1}$, $\overline{x}$, $\overline{x^2}$, ..., $\overline{x^{d-1}}$ é linearmente independente sobre K, o que conclui a demonstração.

b) Temos que F é um corpo finito com q^d elementos. Assim, pela proposição 3.2.3, temos que $\overline{x}^{q^d} = \overline{x}$.

c) Segue do item b.

d) Consideremos o polinômio $g(y) = (y - \overline{x})(y - \overline{x}^q)...(y - \overline{x}^{q^{d-1}}) \in F[y]$. Temos do item b) que

$$\begin{aligned} g(y^q) &= (y^q - \overline{x})(y^q - \overline{x}^q) \dots (y^q - \overline{x}^{q^{d-1}}) \\ &= (y^q - \overline{x}^{q^d})(y^q - \overline{x}^q) \dots (y^q - \overline{x}^{q^{d-1}}) \\ &= ((y - \overline{x}^{q^{d-1}})(y - \overline{x}) \dots (y - \overline{x}^{q^{d-2}}))^q = (g(y))^q \,. \end{aligned}$$

Assim, se $g(y) = b_0 + b_1 y + ... + b_d y^d$, temos que $b_i = b_i^q$, para todo $i = 0$, ..., d. Pela proposição 3.2.4, temos que os coeficientes de $g(y)$ pertencem a K, ou seja, $g(y) \in K[y]$. Como $f(y)$ e $g(y)$ possuem a raiz $\overline{x}$ em comum na extensão F de K, temos que o seu mdc em $F[y]$ é não constante e pertence a $K[y]$ (ver observação 3.2.6 a seguir). Como $f(y)$ é irredutível e mônico, então coincide com o *mdc* de $f(y)$ e $g(y)$, de forma que $f(y)$ divide $g(y)$. Sendo $f(y)$ e $g(y)$ polinômios mônicos de mesmo grau, devemos ter $f(y) = g(y)$. Ainda, Pelo item c) dessa proposição, sabemos que $f(y) = g(y)$ divide $y^{q^d} - y$ em $K[y]$, onde o último polinômio não possui fatores múltiplos em nenhuma extensão de K. Logo as raízes $\overline{x}$, $\overline{x}^q$, ..., $\overline{x}^{q^{d-1}}$ são duas a duas distintas, o que completa a demonstração.

■

Observação 3.2.6. Essa observação visa fornecer uma explicação para uma das passagens da demonstração da proposição 3.2.5. Sejam K um corpo e F uma extensão de K. Em virtude da unicidade do quociente e do resto na divisão de polinômios em $F[x]$, temos que dados dois polinômios $f(x)$, $g(x) \in K[x]$, o quociente e o resto de sua divisão em $F[x]$ são os mesmos que em $K[x]$. Com isso, pelo Algoritmo de Euclides temos que o mdc de $f(x)$ e $g(x)$ em $F[x]$ coincide com o mdc desses polinômios em $K[x]$.

Corolário 3.2.7. *Sejam K um corpo finito com q elementos e $f(x) \in K[x]$ um polinômio irredutível de grau d. Então $d = min\{j \in \mathbb{N}; \overline{x}^{q^j} = \overline{x}\}$, onde $\overline{x} \in K[x]/\langle f(x) \rangle$.*

Demonstração. Segue do item d) da proposição 3.2.5. ■

Lema 3.2.8. *Seja K um corpo qualquer. Dados m, n inteiros positivos, temos que $mdc(x^m - 1, x^n - 1) = x^{mdc(m,n)} - 1$.*

Demonstração. Se $m = n$, então o máximo divisor comum é o polinômio $x^m - 1$. Caso contrário, suponhamos, sem perda de generalidade, que $m < n$. Pelo algoritmo da divisão em $\mathbb{Z}$, temos que $n = mq + r$, onde $0 \leqslant r < m$. Já pelo algoritmo da divisão em $K[x]$, temos que

$$x^n - 1 = (x^m - 1)(x^{n-m} + x^{n-2m} + ... + x^{n-qm}) + x^r - 1\,. \tag{3.1}$$

Consideremos agora o Algoritmo de Euclides para o cálculo do mdc de m e n:

$$\begin{aligned} n &= mq_1 + r_1 \\ m &= r_1q_2 + r_2 \\ &\vdots \\ r_{s-1} &= r_sq_s + r_{s+1} \end{aligned}$$

onde $r_{s+1} = 0$. Dessa forma $mdc(m,\, n) = r_s$. Utilizando as igualdades anteriores, temos que

$$\begin{aligned} x^n - 1 &= (x^m - 1)Q_1(x) + x^{r_1} - 1 \\ x^m - 1 &= (x^{r_1} - 1)Q_2(x) + x^{r_2} - 1 \\ &\vdots \\ x^{r_{s-1}} - 1 &= (x^{r_s} - 1)Q_{s+1} + x^{r_{s+1}} - 1 \end{aligned}$$

onde $Q_i(x)$, $i = 1,\, ...,\, s + 1$, são polinômios como na equação (3.1). Logo

$$mdc(x^m - 1,\, x^n - 1) = x^{r_s} - 1 = x^{mdc(m,\, n)} - 1.$$

■

Corolário 3.2.9. *Seja K um corpo qualquer. Dados m, n, q inteiros positivos, temos que $mdc(x^{q^n} - x,\, x^{q^m} - x) = x^{q^{mdc(m,\, n)}} - x$.*

Demonstração. Com efeito, pelo resultado anterior.

$$\begin{aligned} mdc(x^{q^n} - x,\, x^{q^m} - x) &= x\ mdc(x^{q^n - 1} - 1,\, x^{q^m - 1} - 1) \\ &= x(x^{mdc(q^n - 1,\, q^m - 1)} - 1) \\ &= x(x^{q^{mdc(n,m)} - 1} - 1) = x^{q^{mdc(n,\, m)}} - x. \end{aligned}$$

■

Lema 3.2.10. *Sejam m, n, q inteiros positivos. Então $(x^{q^m}-x)|(x^{q^n}-x)$ se, e somente se, $m|n$.*

Demonstração. De fato, temos as seguintes equivalências:

$$\begin{aligned}(x^{q^m}-x)|(x^{q^n}-x) &\Leftrightarrow mdc(x^{q^m}-x,\, x^{q^n}-x) = x^{q^m}-x\\ &\Leftrightarrow x^{q^{mdc(m,\,n)}}-x = x^{q^m}-x\\ &\Leftrightarrow mdc(m,\,n) = m\\ &\Leftrightarrow m|n.\end{aligned}$$

■

Proposição 3.2.11. *Seja K um corpo finito com q elementos e 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 $K[x]$.*

Demonstração. Seja $f(x) \in K[x]$ um polinômio mônico irredutível de grau d. Como $x^{q^n}-x$ não possui fatores múltiplos (pelo mesmo argumento apresentado na demonstração da proposição 3.2.5), basta provar que $f(x)$ divide $x^{q^n}-x$ se, e somente se, d divide n.

Suponhamos que $f(x)|(x^{q^n}-x)$. Pela proposição 3.2.5, temos

$$f(x)|mdc(x^{q^n}-x,\, x^{q^d}-x)\,.$$

Como $mdc(x^{q^n}-x,\, x^{q^d}-x) = x^{q^e}-x$, onde $e = mdc(n,d) \leqslant d$, temos que $\overline{x}^{q^e} = \overline{x}$, o que pelo corolário 3.2.7 só é possível se $e \geqslant d$. Dessa forma, temos que $d = e = mdc(n,d)$, donde $d|n$. Reciprocamente, se $d|n$, temos que $(x^{q^d}-x)|(x^{q^n}-x)$. Como $f(x)$ divide $x^{q^d}-x$ pela proposição 3.2.5, segue que $f(x)|(x^{q^n}-x)$. ■

Definição 3.2.12. Seja K um corpo finito. Definimos $I(n)$ como sendo o número de polinômios mônicos irredutíveis de grau n em $K[x]$.

Corolário 3.2.13. *Seja K um corpo finito com q elementos. Então, temos que $q^n = \sum_{d|n} d\ I(d)$.*

Demonstração. Basta comparar os graus dos polinômios na igualdade

$$x^{q^n} - x = \prod_{d|n} G_d(x).$$

■

Teorema 3.2.14. *Seja K um corpo finito com q elementos. Para cada número natural n existe pelo menos um polinômio irredutível de grau n em $K[x]$.*

Demonstração. Para $n = 1$, temos que $I(1) = q > 0$, pois existem q possibilidades para o coeficiente b em x+b e estes são exatamente os polinômios mônicos irredutíveis de grau 1. Para $n = 2$, temos que $q^2 = I(1) + 2I(2)$, donde $I(2) = \dfrac{q^2 - q}{2} = \dfrac{q(q-1)}{2} > 0$. Suponhamos agora $n > 2$. Sejam $1 = d_1 < ... < d_s < n$, com $s \geqslant 1$, os divisores de n. Se K possuir q elementos, temos que

$$\begin{aligned} q^n &= \sum_{d|n} d\ I(d) = \sum_{i=1}^{s} d_i\ I(d_i) + n\ I(n) \\ &\leqslant \sum_{i=1}^{s} (\sum_{e|d_i} e\ I(e)) + n\ I(n) \\ &= \sum_{i=1}^{s} q^{d_i} + n\ I(n) \\ &< \sum_{i=0}^{d_s} q^i + n\ I(n) \\ &= \frac{q^{d_s+1} - 1}{q-1} + n\ I(n) < q^{d_s+1} + n\ I(n)\,. \end{aligned}$$

Isso nos dá que $nI(n) > q^n - q^{d_s+1}$. Como d_s divide n e $d_s < n$, temos que $n = \lambda\ d_s$, com $\lambda > 1$. Logo $d_s = n/\lambda \leqslant n/2$ e $q^{d_s+1} \leqslant q^{n/2+1}$. Daí,

$$n\ I(n) > q^n - q^{n/2+1} = q^n(1 - q^{-n/2+1})$$

de forma que $I(n) > 0$. ■

Teorema 3.2.15 (Existência e Unicidade de Corpos Finitos - Primeira Forma)**.** *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 F um corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Esse polinômio possui q raízes distintas em F, já que a sua derivada é $qx^{q-1} - 1 = -1 \neq 0$ em $\mathbb{F}_p[x]$. Seja $S = \{a \in F; a^q - a = 0\}$. Então S é um subcorpo de F pois:

a) S contém os elementos 0 e 1;

b) a, $b \in S$ implica em $(a-b)^q = a^q - b^q = a - b$ e assim $a - b \in S$;

c) Dados a, $b \in S$, $b \neq 0$, temos que $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$ 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. Portanto $F = S$ e como S contém q elementos, F é um corpo finito com q elementos.
(Unicidade) Seja F um corpo finito com $q = p^n$ elementos. Então F possui característica p e assim contém $\mathbb{F}_p$ como um subcorpo. Pelo proposição 3.2.3, F é um corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. O resultado segue então da unicidade dos corpos de decomposição apresentado no capítulo 1. ■

Teorema 3.2.16 (Existência e Unicidade de Corpos Finitos - Segunda Forma)**.** *Para todo primo p e para todo inteiro positivo n existe um corpo finito com p^n elementos. Ainda, dois corpos finitos com o mesmo número de elementos são isomorfos.*

Demonstração. (Existência) Para todo número primo p e todo inteiro positivo n, existe, pelo teorema 3.2.14, um polinômio irredutível $f(x) \in \mathbb{F}_p$ de grau n. Logo o corpo $\mathbb{F}_p/\langle f(x)\rangle$ é um corpo finito com p^n elementos.
(Unicidade) Seja F um corpo finito com p^n elementos. Então a característica de F é p e F contém um subcorpo isomorfo a $\mathbb{F}_p$ (proposição 3.1.8). Assim, F é um espaço vetorial de dimensão n sobre $\mathbb{F}_p$. Como F é um corpo finito com p^n elementos, temos pela proposição 3.2.4 que todos os elementos de F são raízes do polinômio $x^{p^n} - x$. Seja $f(x) \in \mathbb{F}_p[x]$ um polinômio mônico e irredutível de grau n, cuja existência está garantida pelo teorema 3.2.14. Ainda, pela proposição 3.2.5 c), temos que $f(x)|(x^{p^n} - x)$ em $\mathbb{F}_p[x]$. Logo, existe $\beta \in F$ tal que $f(\beta) = 0$. Os elementos 1, β, β^2, ..., β^{n-1} são linearmente independentes

sobre $\mathbb{F}_p$, pois, caso contrário, existiria um polinômio não nulo $r(x) \in \mathbb{F}_p[x]$ de grau menor do que o grau de $f(x)$ tal que $r(\beta) = 0$. Pela observação 3.2.6, temos que $mdc(f(x), r(x)) \neq 1$ em $\mathbb{F}_p[x]$. Como $f(x)$ é irredutível, teríamos que ter $f(x)|r(x)$, o que não é possível pois $gr(r(x)) < gr(f(x)) = n$. Assim $\{1, \beta, \beta^2, ..., \beta^{n-1}\}$ forma uma base de F sobre $\mathbb{F}_p$. Sabemos também pela proposição 3.2.5 a) que $\{\overline{1}, \overline{x}, \overline{x^2}, ..., \overline{x^{n-1}}\}$ é uma base de $\mathbb{F}_p[x]/\langle f(x)\rangle$ sobre $\mathbb{F}_p$. Definindo $\varphi : \mathbb{F}_p[x]/\langle f(x)\rangle \to F$ pondo $\varphi(\overline{a_0 + a_1x + ... + a_{n-1}x^{n-1}}) = a_0 + a_1\beta + ... + a_{n-1}\beta^{n-1}$, temos que φ está bem definida. Com efeito, se $\overline{a_0 + a_1x + ... + a_{n-1}x^{n-1}} = \overline{b_0 + b_1x + ... + b_{n-1}x^{n-1}}$, então, para algum $g(x) \in \mathbb{F}_p[x]$, temos que $a_0 + a_1x + ... + a_{n-1}x^{n-1} - (b_0 + b_1x + ... + b_{n-1}x^{n-1}) = f(x)g(x)$, de modo que $(a_0 + a_1\beta + ... + a_{n-1}\beta^{n-1}) - (b_0 + b_1\beta + ... + b_{n-1}\beta^{n-1}) = f(\beta)g(\beta) = 0$, ou seja, $a_0 + a_1\beta + ... + a_{n-1}\beta^{n-1} = b_0 + b_1\beta + ... + b_{n-1}\beta^{n-1}$. Ainda, por construção, φ é sobrejetora. Para completarmos a prova, resta-nos mostrar que φ preserva a adição e a multiplicação. Pela lei de formação da função φ é possível perceber que ela preserva a adição. Agora, dados $\overline{u(x)}$, $\overline{v(x)} \in \mathbb{F}_p[x]/\langle f(x)\rangle$, $u(x)$, $v(x) \in \mathbb{F}_p[x]$, existem $q(x)$, $r(x) \in \mathbb{F}_p[x]$ tais que $u(x)v(x) = f(x)q(x) + r(x)$, com $r(x) = 0$ ou $gr(r(x)) < n$. Logo, $\overline{u(x)v(x)} = \overline{r(x)}$ e $u(\beta)v(\beta) = r(\beta)$, o que mostra que $\varphi(\overline{u(x)v(x)}) = r(\beta) = u(\beta)v(\beta) = \varphi(\overline{u(x)})\varphi(\overline{v(x)})$. ■

Terminamos essa seção com a definição de elemento primitivo de um corpo finito.

Definição 3.2.17. Um elemento α de um corpo finito $\mathbb{F}_q$ é chamado elemento primitivo se $\mathbb{F}_q^* = \{1, \alpha, \alpha^2, ..., \alpha^{q-2}\}$, ou seja, a ordem de α é igual a $q - 1$.

É possível provar que todo corpo finito possui pelo menos um elemento primitivo. Uma demonstração deste resultado pode ser encontrada nas referências [1] e [7].

3.3 EXTENSÕES DE CORPOS FINITOS

Proposição 3.3.1. *Seja p um número primo. Um corpo F com p^n elementos contém um subcorpo K com p^m elementos se, e somente se, $m|n$. Nesse caso, existe*

um único subcorpo com a referida propriedade, e seus elementos são as raízes em F do polinômio $x^{p^m} - x$.

Demonstração. Suponhamos que F e K sejam corpos com p^n e p^m elementos, respectivamente. Sabemos que os elementos de F são raízes do polinômio $x^{p^n} - x$, enquanto os elementos de K são raízes do polinômio $x^{p^m} - x$. Daí temos que $K \subset F$ se, e somente se, $(x^{p^m} - x)|(x^{p^n} - x)$, o que, pelo lema 3.2.10, ocorre se, e somente se, $m|n$. ■

Corolário 3.3.2. *Seja q uma potência inteira de um número primo p e sejam m, n inteiros positivos. O corpo $\mathbb{F}_{q^n}$ contém um subcorpo isomorfo a $\mathbb{F}_{q^m}$ se, e somente se, $m|n$. Neste caso, tal subcorpo é único e seus elementos são as raízes de $x^{q^m} - x$ em $\mathbb{F}_{q^m}$.*

Demonstração. Escrevamos $q = p^r$. Então $q^n = p^{rn}$ e $q^m = p^{rm}$. Como $rm|rn$ se, e somente se, $m|n$, temos que o resultado segue da proposição 3.3.1. ■

Proposição 3.3.3. *Sejam F um corpo finito, K um subcorpo de F e $\beta \in F$.*

a) Se $m = gr(irr(\beta, K))$, então $1, \beta, ..., \beta^{m-1}$ é uma base de $K(\beta)$ sobre K. Em particular, $[K(\beta) : K] = m$.

b) Se K possui q elementos, então $\beta^{q^m} = \beta$ e $\beta^{q^i} \neq \beta^{q^j}$ para $i, j = 0, ..., m-1$, $i \neq j$. Além disso, $irr(\beta, K) = (x - \beta)(x - \beta^q)...(x - \beta^{q^{m-1}})$.

c) Existe $\alpha \in F$ tal que $F = K(\alpha)$.

Demonstração. a) Essa prova encontra-se na demonstração do teorema 2.1.11.

b) A demonstração desse item pode ser encontrada na referência [7].

c) Se α é um elemento primitivo de F, então $F = K(\alpha)$. ■

3.4 RAÍZES DA UNIDADE

Definição 3.4.1. Uma raiz n-ésima da unidade num corpo F é uma raiz em F do polinômio $x^n - 1$.

Proposição 3.4.2. *Sejam F um corpo finito com q elementos e n um inteiro positivo que divide $q-1$. Então existe um elemento $\gamma \in F$ tal que*

$$x^n - 1 = (x-1)(x-\gamma)(x-\gamma^2)...(x-\gamma^{n-1}),$$

onde 1, γ, γ^2, ..., γ^{n-1} são dois a dois distintos.

Demonstração. Seja α um elemento primitivo de F. Logo $\alpha^{q-1} = 1$ e $\alpha^m \neq 1$ para todo $0 < m < q-1$. Se $n = 1$, nada temos para provar. Suponhamos agora $n \geqslant 2$. Escrevendo $\gamma = \alpha^{\frac{q-1}{n}} \in F$, temos que 1, γ, γ^2, ..., γ^{n-1} são raízes de $x^n - 1$. Ainda, essas raízes são duas a duas distintas, pois caso contrário, se $\gamma^i = \gamma^j$ para algum par de inteiros (i, j) tais que $0 \leqslant i < j \leqslant n-1$, então $\alpha^{(j-i)\frac{q-1}{n}} = \gamma^{j-i} = 1$, o que é uma contradição, pois $(j-i)\dfrac{q-1}{n} < q-1$. Isso conclui a demonstração. ■

Corolário 3.4.3. *Seja K um corpo finito com q elementos e n um inteiro positivo tal que $mdc(n, q) = 1$. Então existem uma extensão F de K e um elemento $\gamma \in F$ tais que $x^n - 1 = (x-1)(x-\gamma)(x-\gamma^2)...(x-\gamma^{n-1})$, com 1, γ, γ^2, ..., γ^{n-1} dois a dois distintos.*

Demonstração. Se $n = 1$, nada temos para provar. Suponhamos agora que $n \geqslant 2$. Como $mdc(n, q) = 1$, temos que $\overline{q}$ é invertível em $\mathbb{Z}_n$. Sendo $\mathbb{Z}_n$ finito, então no conjunto $\{\overline{q}, \overline{q}^2, \overline{q}^3, ...\}$ há certas repetições. Sejam dessa forma i, j tais que $\overline{q}^i = \overline{q}^j$ e $j > i$. Como $\overline{q}$ é invertível, temos que $\overline{q}^{-i} = (\overline{q}^{-1})^i \in \mathbb{Z}_n$. Portanto $d = j - i$ é tal que $\overline{q}^d = 1$. Seja m um inteiro positivo tal que $\overline{q}^m = 1$. Então existe uma extensão de K com q^m elementos. Assim $n|(q^m - 1)$, de modo que o resultado segue pela proposição 3.4.2. ■

Observação 3.4.4. Se no corolário 3.4.3 considerarmos m o menor inteiro positivo que satisfaz $\overline{q}^m = 1$, então o corpo $\mathbb{F}_{q^m}$ será o menor corpo onde $x^n - 1$ se fatora.

Definição 3.4.5. Nas condições da observação 3.4.4, denominados o corpo $\mathbb{F}_{q^m}$ de corpo de raízes de $x^n - 1$.

Observação 3.4.6. Se n e a característica p de K não são primos entre si, podemos escrever $n = n'p^r$, onde $mdc(n', p) = 1$. Assim, $x^n - 1 = (x^{n'} - 1)^{p^r}$, de forma que α é uma raiz n-ésima da unidade se, e somente se, α é uma raiz n'-ésima da

unidade. Aplicando o corolário 3.4.3, é possível garantir que existe uma extensão F de K e um elemento $\gamma \in F$, raiz n'-ésima da unidade tal que $x^n - 1 = (x^{n'} - 1)^{p^r} = [(x-1)(x-\gamma)...(\gamma^{n'-1})]^{p^r}$, com 1, γ, γ^2, ..., $\gamma^{n'-1}$ raízes n'-ésimas da unidade duas a duas distintas.

Definição 3.4.7. Uma raiz n-ésima da unidade que não é raiz m-ésima da unidade para nenhum $m < n$ será chamada raiz n-ésima primitiva da unidade.

4 CÓDIGOS CORRETORES DE ERROS

Neste capítulo apresentaremos alguns elementos da teoria dos códigos corretores de erros. Denotaremos por $\mathbb{F}_q$ o corpo finito com q elementos.

4.1 INTRODUÇÃO AOS CÓDIGOS CORRETORES DE ERROS

Vejamos que um idioma é um exemplo familiar de um código corretor de erros. Seja A o conjunto de todas as letras do alfabeto da língua inglesa acrescido do espaço em branco. Uma palavra desse idioma pode ser considerada como um elemento do conjunto A^{45}, onde 45 é o tamanho da palavra mais longa existente na língua inglesa. Nesse caso, estamos inserindo as letras dessa palavra nas primeiras entradas da 45-upla e completando o restante com espaços em branco. Denotando por I o conjunto de todas as palavras dessa língua, o fato desse conjunto ser um subconjunto próprio de A^{45} faz, de certa forma, que I seja um código detector e corretor de erros. Para ilustrar tal fato, suponhamos que ao tentar escrever uma palavra escrevamos "machematics". Uma vez que essa palavra não pertence a I, é possível detectar a ocorrência de um erro e, como a palavra que "mais se assemelha" a essa é "mathematics", é possível corrigir o erro cometido. Vale ainda ressaltar que esse exemplo de código não é muito eficaz. De fato, se pretendêssemos escrever "let" e por algum motivo essa palavra fosse escrita como "get" ou "set", não haveria possibilidade de detectarmos o erro. A razão disso é que nesse código existem muitas palavras "próximas" uma das outras.

A figura a seguir apresenta os elementos da teoria estudada.

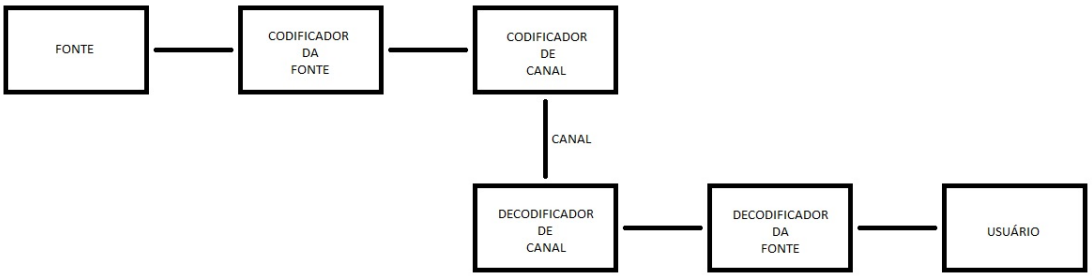

Figura 1 – Mecanismo dos códigos corretores de erros

O exemplo a seguir facilitará a compreensão dos elementos apresentados na figura 1.

Exemplo 4.1.1. Consideremos a peça torre sobre um tabuleiro de xadrez e suponhamos que seja possível controlarmos o movimento dessa peça eletronicamente, de forma que ao fornecermos um dos comandos Norte, Sul, Leste ou Oeste, a peça se desloque para a casa adjacente indicada pelo comando. Os quatro comandos acima poderiam ser codificados como os elementos de $\mathbb{F}_2^2$ da seguinte forma:

$$Norte \mapsto (0,\, 0) \;\; Sul \mapsto (1,\, 0)$$

$$Leste \mapsto (0,\, 1) \;\; Oeste \mapsto (1,\, 1).$$

O código anterior é denominado código da fonte. Suponhamos agora que esses pares ordenados devam ser transmitidos via ondas de rádio e que o sinal no caminho possa sofrer interferências, de forma que seja possível enviarmos a palavra $(0, 0)$ e recebermos a palavra $(0, 1)$. Neste caso, buscamos recodificar as palavras, de modo a introduzir redundâncias que permitam detectar e corrigir possíveis erros. Podemos, por exemplo, recodificar as palavras anteriores da seguinte forma:

$$(0,\, 0) \mapsto (0,\, 0,\, 0,\, 0,\, 0) \;\; (1,\, 0) \mapsto (1,\, 0,\, 0,\, 1,\, 0)$$

$$(0,\, 1) \mapsto (0,\, 1,\, 0,\, 0,\, 1) \;\; (1,\, 1) \mapsto (1,\, 1,\, 0,\, 1,\, 1).$$

Nessa recodificação as duas primeiras posições reproduzem o código da fonte e as demais posições são as redundâncias introduzidas. Esse novo código é denominado código de canal. Como exemplo temos os canais de radiofrequência, os canais de microondas, cabos, fitas magnéticas e os discos de armazenamento.

O objetivo das próximas seções será apresentar alguns elementos teóricos da detecção e correção de erros e da transformação de códigos da fonte em códigos de canal.

4.1.1 Métrica de Hamming

Definição 4.1.2. Um alfabeto A é um conjunto com um número finito de elementos.

Até o início da seção 4.2, A irá denotar um alfabeto e a cardinalidade de A, denotada por $|A|$, será simbolizada por q.

Definição 4.1.3. Um código corretor de erros é um subconjunto próprio de A^n, para algum número natural n.

Queremos agora atribuir um sentido matemático para a proximidade das palavras de um código. Para isso, consideremos a seguinte definição:

Definição 4.1.4. Dados dois elementos $u = (u_1, ..., u_n)$ e $v = (v_1, ..., v_n)$ em A^n, a distância de Hamming entre u e v é definida como

$$d(u, v) = |\{i;\, u_i \neq v_i,\, 1 \leqslant i \leqslant n\}|,$$

onde $|B|$ denota a cardinalidade do conjunto B.

A partir de agora, $d(u, v)$ irá denotar a distância de Hamming entre u e v.

Exemplo 4.1.5. Consideremos o alfabeto como sendo o conjunto $\mathbb{F}_2$ e consideremos, na notação da definição 4.1.4, $n = 5$. Se considerarmos o código de canal do exemplo 4.1.1, temos que

$$d((1, 0, 0, 1, 0), (0, 1, 0, 0, 1)) = 4$$

e

$$d((0, 0, 0, 0, 0), (0, 1, 0, 0, 1)) = 2.$$

Proposição 4.1.6. *A distância de Hamming é uma métrica.*

Demonstração. Com efeito, seja $n \in \mathbb{N}$. Se $d : A^n \times A^n \to \mathbb{R}$ é a distância de Hamming, então d satisfaz:

a) Positividade: $d(u, v) \geqslant 0$, $\forall\, u, v \in A^n$
   A cardinalidade de um conjunto é sempre um número inteiro não negativo.

b) Simetria: $d(u, v) = d(v, u)$, $\forall\, u, v \in A^n$
   De fato, $d(u, v) = |\{i;\, u_i \neq v_i,\, 1 \leqslant i \leqslant n\}| = |\{i;\, v_i \neq u_i,\, 1 \leqslant i \leqslant n\}| = d(v, u)$.

c) Desigualdade Triangular: $d(u,\, v) \leqslant d(u,\, w) + d(w,\, v),\ \forall\, u,\, v,\, w \in A^n$
De fato, dados $u,\, v \in A^n$, a contribuição das i-ésimas coordenadas para $d(u,\, v)$ é igual a zero, se $u_i = v_i$, e igual a um, se $u_i \neq v_i$. Assim, dado $w \in A^n$, se a contribuição das i-ésimas coordenadas para $d(u,\, v)$ for zero, teremos que essa contribuição é sempre menor ou igual às contribuições das i-ésimas coordenadas para $d(u,\, w) + d(w,\, v)\,(= 0,\, 1,\, 2)$. Se a contribuição das i-ésimas coordenadas para $d(u,\, v)$ é um, temos que $u_i \neq v_i$, de modo que não é possível termos $u_i = w_i$ e $v_i = w_i$, o que nos dá que a contribuição das i-ésimas coordenadas para $d(u,\, w) + d(w,\, v)$ é sempre maior ou igual a um, que é a contribuição das i-ésimas coordenadas para $d(u,\, w) + d(w,\, v)$.

■

Observação 4.1.7. Em virtude da proposição 4.1.6, temos que a distância de Hamming é muitas vezes também chamada métrica de Hamming.

Definição 4.1.8. Sejam $n \in \mathbb{N}$, $a \in A^n$ e $t \geq 0$, $t \in \mathbb{R}$. Definimos o disco e a esfera de centro a e raio t como sendo, respectivamente, os conjuntos

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

e

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

Lema 4.1.9. *Para todo $a \in A^n$ e para todo número natural $r > 0$, temos que* $|D(a,\, r)| = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i$.

Demonstração. Mostremos inicialmente que $|S(a,\, i)| = \binom{n}{i}(q-1)^i$. Com efeito, $S(a,\, i) = \{u \in A^n;\, d(u,\, a) = i\}$ implica que se $u \in S(a,\, i)$, então u possui i entradas que são distintas das respectivas entradas de a. Assim, para determinarmos o número de elementos de $S(a,\, i)$, pelo princípio multiplicativo, basta conhecer o número de possibilidades de se escolher i entradas entre n e multiplicar pelo número de possibilidades de se preencher essas i entradas de modo a garantir que todas sejam distintas das respectivas entradas em A. Isso nos dá o resultado desejado. Ainda, $S(a,\, i) \cap S(a,\, j) = \emptyset$, se $i \neq j$. Logo $|D(a,\, r)| = \sum_{i=0}^{r} |S(a,\, i)| = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i$. ■

Definição 4.1.10. Seja C um código. A distância mínima de C é o número

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

Exemplo 4.1.11. Se considerarmos o código de canal do exemplo 4.1.1, é possível perceber que a distância mínima é 2.

Definição 4.1.12. Dado um código C com distância mínima d, define-se $\kappa = \left[\frac{d-1}{2}\right]$, onde $[t]$ representa a parte inteira do número real t.

Lema 4.1.13. *Seja C um código com distância mínima d. Se c e c' são palavras distintas de C, então $D(c, \kappa) \cap D(c', \kappa) = \emptyset$.*

Demonstração. Suponhamos que exista x tal que $x \in D(c, \kappa) \cap D(c', \kappa)$. Então $d(x, c) \leqslant \kappa$ e $d(x, c') \leqslant \kappa$, o que resulta em $d(c, c') \leqslant d(c, x) + d(x, c') \leqslant 2\kappa \leqslant d-1$. Mas isto é uma contradição, pois a distância mínima do código é d. ■

Teorema 4.1.14. *Seja C um código com distância mínima d. Então 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 $d(r, c) \leqslant \kappa$. Pelo lema 4.1.13, temos que a distância de r a qualquer outra palavra de C é maior do que κ. Isso determina c univocamente a partir de r. Sendo a distância mínima do código igual a d, podemos introduzir até $d-1$ erros sem encontrar outra palavra do código (pois assim a palavra r recebida terá distância para c menor ou igual a $d-1$ e, portanto, não irá pertencer ao código). ■

Exemplo 4.1.15. No código do exemplo 4.1.1, como $d = 2$, temos que é possível detectar até 1 erro, mas não é possível corrigir erros.

Definição 4.1.16. Sejam $C \subset A^n$ um código com distância mínima d e $\kappa = \left[\frac{d-1}{2}\right]$. O código C será dito perfeito se $\bigcup_{c \in C} D(c, \kappa) = A^n$.

Observação 4.1.17. Um código C sobre A possui três parâmetros fundamentais $[n, M, d]$ que são, respectivamente, o seu comprimento, o seu número de elementos e a sua distância mínima.

4.1.2 Equivalência de Códigos

Definição 4.1.18. Seja $n \in \mathbb{N}$. Dizemos que uma função $F : A^n \to A^n$ é uma isometria de A^n se ela preserva distâncias de Hamming, isto é, se $d(F(x), F(y)) = d(x, y)$, $\forall\, x, y \in A^n$.

Proposição 4.1.19. *Toda isometria de A^n é uma aplicação bijetora.*

Demonstração. Seja $F : A^n \to A^n$ uma isometria. Dados $x, y \in A^n$ tais que $F(x) = F(y)$, temos que, $d(F(x), F(y)) = d(F(x), F(x)) = 0$. Mas F é uma isometria e assim $d(x, y) = d(F(x), F(y)) = 0$, de forma que $x = y$. Logo F é injetora. Como A^n é finito, segue que F é sobrejetora. Portanto, F é uma bijeção. ■

Proposição 4.1.20. *Sejam F e G isometrias de A^n e $I : A^n \to A^n$ a função identidade. Então:*

a) I é uma isometria de A^n.

b) F^{-1} é uma isometria de A^n.

c) $F \circ G$ é uma isometria de A^n.

Demonstração. a) Segue diretamente da definição da função identidade.
b) Sendo F uma isometria temos que F é uma bijeção e dessa forma possui uma inversa F^{-1}. Assim, dados $x, y \in A^n$ temos que

$$d(F^{-1}(x), F^{-1}(y)) = d(F(F^{-1}(x)), F(F^{-1}(y))) = d(x, y).$$

c) Dados $x, y \in A^n$, temos que

$$d(F \circ G(x), F \circ G(y)) = d(F(G(x)), F(G(y))) = d(G(x), G(y)) = d(x, y)$$

pois F e G são isometrias. ■

Definição 4.1.21. Sejam C e $C' \subset A^n$ códigos. Dizemos que o código C é equivalente a C' se existir uma isometria F de A^n tal que $F(C) = C'$.

Proposição 4.1.22. *A equivalência de códigos é uma relação de equivalência.*

Demonstração. Com efeito:

a) A equivalência de códigos é uma relação reflexiva.
Pela letra a) da proposição 4.1.20, todo código C é equivalente a si mesmo, pois $I(C) = C$, onde I é a aplicação identidade.

b) A equivalência de códigos é uma relação simétrica.
De fato, pela letra b) da proposição 4.1.20, temos que se F é uma isometria, então F^{-1} é uma isometria. Assim, se C e C' são códigos de A^n tais que Cé equivalente a C', então existe F isometria tal que $F(C) = C'$, de forma $F^{-1}(C') = C$, ou seja, C' é equivalente a C.

c) A equivalência de códigos é uma relação transitiva.
De fato, utilizando a letra c) da proposição 4.1.20, temos que se C, C', C'' são códigos de A^n tais que C é equivalente a C' e C' é equivalente a C'', então existem isometrias F e G satisfazendo $F(C) = C'$ e $G(C') = C''$, de modo que $G \circ F(C) = G(F(C)) = C''$, ou seja, C é equivalente a C''.

■

Observação 4.1.23. Decorre da definição que dois códigos equivalentes possuem os mesmos parâmetros.

Exemplo 4.1.24. Apresentaremos aqui dois exemplos importantes de isometrias.

a) Se $f : A \to A$ é uma bijeção e i é um número inteiro tal que $1 \leqslant i \leqslant n$, então a aplicação $T_f^i : A^n \to A^n$, dada por

$$T_f^i(a_1, ..., a_n) = (a_1, ..., a_{i-1}, f(a_i), a_{i+1}, ..., a_n),$$

é uma isometria.
Com efeito, sejam $u, v \in A^n$ tais que $u = (u_1, ..., u_n)$ e $v = (v_1, ..., v_n)$. Então

$$d(T_f^i(u), T_f^i(v)) =$$
$$d((u_1, ..., u_{i-1}, f(u_i), u_{i+1}, ..., u_n), (v_1, ..., v_{i-1}, f(v_i), v_{i+1}, ..., v_n)).$$

Como f é uma bijeção, se $f(u_i) = f(v_i)$, então $u_i = v_i$. Como f é uma função, se $f(u_i) \neq f(v_i)$, então $u_i \neq v_i$. Logo a contribuição de $f(u_i)$ e $f(v_i)$ para $d(T_f^i(u), T_f^i(v))$ é a mesma que seria obtida se substituíssemos $f(u_i)$ por u_i e $f(v_i)$ por v_i. Portanto

$$d(T_f^i(u), T_f^i(v)) = d((u_1, ..., u_n), (v_1, ..., v_n)) = d(u, v).$$

b) Sejam $I_n := \{1, ..., n\}$ e $\pi : I_n \to I_n$ uma bijeção (π é chamada uma permutação). A aplicação permutação de coordenadas, $T_\pi : A^n \to A^n$, dada por $T_\pi(a_1, ..., a_n) = (a_{\pi(1)}, ..., a_{\pi(n)})$, é uma isometria.
De fato, sejam $u, v \in A^n$, $u = (u_1, ..., u_n)$ e $v = (v_1, ..., v_n)$. Então

$$\begin{aligned} d(T_\pi(u), T_\pi(v)) &= d((u_{\pi(1)}, ..., u_{\pi(n)}), (v_{\pi(1)}, ..., v_{\pi(n)})) \\ &= |\{\pi(i); u_{\pi(i)} \neq v_{\pi(i)}, 1 \leqslant i \leqslant n\}| \end{aligned}$$

Como π é uma bijeção, temos que

$$\begin{aligned} \{\pi(i); u_{\pi(i)} \neq v_{\pi(i)}, 1 \leqslant i \leqslant n\} &= \{j; j = \pi(i), u_{\pi(i)} \neq v_{\pi(i)}, 1 \leqslant i \leqslant n\} \\ &= \{j; u_j \neq v_j, 1 \leqslant j \leqslant n\}. \end{aligned}$$

Logo $d(T_\pi(u), T_\pi(v)) = d(u, v)$.

Teorema 4.1.25. *Seja $F : A^n \to A^n$ uma isometria. Então existem uma permutação π de I_n e bijeções f_i de A, $i = 1, ..., n$, tais que $F = T_\pi \circ T_{f_1}^1 \circ ... \circ T_{f_n}^n$.*

Demonstração. Essa demonstração pode ser encontrada na referência [7]. ■

Corolário 4.1.26. *Sejam C e C' dois códigos de A^n. Temos que C e C' são equivalentes se, e somente se, existem uma permutação π de I_n e bijeções $f_1, ..., f_n$ de A tais que $C' = \{(f_{\pi(1)}(x_{\pi(1)}), ..., f_{\pi(n)}(x_{\pi(n)})); (x_1, ..., x_n) \in C\}$.*

O corolário 4.1.26 motiva o resultado a seguir.

Proposição 4.1.27. *Dois códigos de comprimento n sobre um alfabeto A são equivalentes se, e somente se, um deles pode ser obtido do outro mediante uma sequência de operações do tipo:*

a) Substituição das letras numa dada posição fixa em todas as palavras do código por meio de uma bijeção de A.

b) Permutação das posições das letras em todas as palavras do código, mediante uma permutação fixa de I_n.

4.2 CÓDIGOS LINEARES

4.2.1 **Primeiras Definições e Propriedades**

Consideraremos a partir de agora o nosso alfabeto como sendo o corpo finito $\mathbb{F}_q$. Assim, para cada número natural n, obtemos um espaço vetorial $\mathbb{F}_q^n$ sobre $\mathbb{F}_q$ de dimensão n.

Definição 4.2.1. Dizemos que um código $C \subset \mathbb{F}_q^n$ é linear se C for um subespaço vetorial de $\mathbb{F}_q^n$.

Exemplo 4.2.2. O código apresentado no exemplo 4.1.1 é um código linear. Com efeito, o alfabeto neste exemplo é o corpo $\mathbb{F}_2$ e o código é o subespaço vetorial de $\mathbb{F}_2^5$ imagem da transformação linear $T : \mathbb{F}_2^2 \to \mathbb{F}_2^5$ dada por

$$T(x_1, x_2) = (x_1, x_2, 0, x_1, x_2).$$

Observação 4.2.3. Iremos relacionar agora o número de elementos de um código linear C sobre $\mathbb{F}_q$ com a dimensão k desse código. Para isso, seja $\{v_1, ..., v_k\}$ uma base de C sobre $\mathbb{F}_q$. Então todos os elementos de C são da forma $\lambda_1 v_1 + ... + \lambda_k v_k$, onde $\lambda_i \in \mathbb{F}_q$, $\forall\, i = 1, ..., k$, de modo que C possui q^k elementos. Dessa forma, temos que $k = log_q M$, onde $M := |C| = q^k$.

Definição 4.2.4. Dado $x \in \mathbb{F}_q^n$, temos que o peso de x é, por definição, o número inteiro $\omega(x) := |\{i;\, x_i \neq 0,\, 1 \leqslant i \leqslant n\}|$.

Observação 4.2.5. Com base na definição 4.2.4, temos que $\omega(x) = d(x, 0)$.

Definição 4.2.6. Dado $C \subset \mathbb{F}_q^n$ um código linear, define-se o peso de C como sendo $\omega(C) := min\{\omega(x); x \in C \setminus \{0\}\}$.

Proposição 4.2.7. *Seja $C \subset \mathbb{F}_q^n$ um código linear com distância mínima d. Então:*

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

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

Demonstração. a) Com efeito, temos que

$$d(x,\, y) = |\{i;\, x_i \neq y_i\}| = |\{i;\, x_i - y_i \neq 0\}| = \omega(x - y).$$

b) Tal afirmação segue do fato de que para todo par de elementos x, y em C com $x \neq y$, tem-se $z = x - y \in C \setminus \{0\}$ e $d(x,\, y) = \omega(z)$. ■

Observação 4.2.8. Em virtude da proposição 4.2.7, temos que, em códigos lineares, a distância mínima será muitas vezes também denominada de peso do código linear.

Exemplo 4.2.9. Descrição de um código linear como núcleo e como imagem de uma transformação linear

a) Representação de um código linear C como imagem de uma transformação linear (ou forma paramétrica do subespaço C).

   Seja $\{v_1,\, ...,\, v_k\}$ uma base de C. Consideremos $T : \mathbb{F}_q^k \to \mathbb{F}_q^n$ dada por $T(x_1,\, ...,\, x_k) = x_1v_1 + ... + x_kv_k$. Temos que T é uma transformação linear injetora. Além disso, $C = Im(T)$. Dessa forma, fornecer um código $C \in \mathbb{F}_q^n$ de dimensão k é equivalente a dar uma transformação linear injetora $T : \mathbb{F}_q^k \to \mathbb{F}_q^n$ e definir $C = Im(T)$.

b) Representação de C como núcleo de uma transformação linear.

   Sejam C' um subespaço de $\mathbb{F}_q^n$ tal que $C \oplus C' = \mathbb{F}_q^n$ e $\{v_1,\, ...,\, v_{n-k}\}$ uma base de C'. Dado $v \in C'$, podemos escrever v como $v = y_1v_1 + ... + y_{n-k}v_{n-k}$. Consideremos $H : C \oplus C' \to \mathbb{F}_q^{n-k}$ dada por

$$T(u + v) = T(u + y_1v_1 + ... + y_{n-k}v_{n-k}) = (y_1,\, ...,\, y_{n-k})\,.$$

   Temos então que H é uma transformação linear cujo núcleo é C.

Definição 4.2.10. Sejam C e C' dois códigos lineares em $\mathbb{F}_q^n$. Dizemos que C e C' são linearmente equivalentes se existir um isometria linear $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ tal que $T(C) = C'$.

Observação 4.2.11. Se π é uma permutação de I_n, então a aplicação $T_\pi : A^n \to A^n$, dada por, $T_\pi(a_1, ..., a_n) = (a_{\pi(1)}, ..., a_{\pi(n)})$ é linear. Temos também que se $f_i : \mathbb{F}_q \to \mathbb{F}_q$, $i = 1, ..., n$, são bijeções e $T_f^i : A^n \to A^n$, $i = 1, ..., n$, são aplicações dadas por $T_f^i(a_1, ..., a_n) = (a_1, ..., a_{i-1}, f(a_i), a_{i+1}, ..., a_n)$, então $T_\pi \circ T_{f_1}^1 \circ ... \circ T_{f_n}^n$ é linear se, e somente se, cada f_i é linear. Ainda, temos que uma função $f : \mathbb{F}_q \to \mathbb{F}_q$ é linear se, e somente se, existe um elemento $c \in \mathbb{F}_q$ tal que $f(x) = cx$, $\forall\, x \in \mathbb{F}_q$. Das observações anteriores e do corolário 4.1.26 temos que dois códigos lineares C e C' são linearmente equivalentes se, e somente se, existem uma permutação π de I_n e elementos $c_1, ..., c_n \in \mathbb{F}_q$ tais que $C' = \{(c_1 x_{\pi(1)}, ..., c_n x_{\pi(n)});\ (x_1, ..., x_n) \in C\}$.

A observação 4.2.11 nos leva ao resultado a seguir.

Proposição 4.2.12. *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:*

a) Multiplicação dos elementos numa dada posição fixa por um escalar não nulo em todas as palavras.

b) Permutação das posições de todas as palavras do código, mediante uma permutação fixa de I_n.

4.2.2 Matriz Geradora de um Código

Definição 4.2.13. Seja $C \subset \mathbb{F}_q^n$ um código linear. Chamaremos de parâmetros do código linear C à terna (n, k, d), onde k é a dimensão de C sobre $\mathbb{F}_q$ e d representa a distância mínima de C.

Definição 4.2.14. Seja $C \subset \mathbb{F}_q^n$ um código linear. Se $B = \{v_1, ..., v_k\}$ é uma base ordenada de C, consideremos a matriz

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

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

Observação 4.2.15. Sejam $C \subset \mathbb{F}_q^n$ um código linear e G a matriz geradora de C associada à base ordenada $B = \{v_1, ..., v_k\}$. Seja $T : \mathbb{F}_q^k \to \mathbb{F}_q^n$ a transformação linear injetora dada por $T(x) = xG$. Então $T(\mathbb{F}_q^k) = C$, de modo que é possível considerar, de acordo com o que foi introduzido no exemplo 4.1.1, $\mathbb{F}_q^k$ como sendo o código da fonte, C o código de canal e T uma codificação. Reciprocamente, é possível construirmos códigos a partir de matrizes cujas linhas sejam linearmente independentes. De fato, se G é uma matriz que satisfaz essas condições, é possível definirmos um código como sendo a imagem da transformação linear $T : \mathbb{F}_q^k \to \mathbb{F}_q^n$ dada por $T(x) = xG$.

Observação 4.2.16. Como duas bases de um certo espaço vetorial podem ser obtidos uma da outra através de uma sequência de operações do tipo:

- Permutação de dois elementos da base;
- Multiplicação de um elemento da base por um escalar não nulo;
- Substituição de um elemento da base por ele mesmo somado com um múltiplo escalar de outro vetor da base

temos que duas matrizes geradoras de um código linear C podem ser obtidas uma da outra por uma sequência de operações do tipo:

- Permutação de duas linhas da matriz;
- Multiplicação de uma linha por um escalar não nulo;
- Substituição de uma linha por ela mesma somada com um múltiplo escalar de outra linha.

Exemplo 4.2.17. Consideremos $K = \mathbb{F}_2$ e seja

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

Se $T : \mathbb{F}_2^3 \to \mathbb{F}_2^5$ for dada por $T(x) = xG$, é possível obtermos um código C definindo $C := T(\mathbb{F}_2^3)$. Assim, temos, por exemplo, que $T(1, 1, 0) = (1, 1, 1, 1, 1)$. Suponhamos agora que tenha sido dada a palavra (0, 1, 0, 1, 0) do código de canal e pretendemos encontrar a respectiva palavra do código da fonte. Para isso, temos que resolver o sistema $xG = (0, 1, 0, 1, 0)$, ou seja,

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

cuja solução é dada por $x_1 = x_3 = 0$ e $x_2 = 1$. Esse sistema de equações é um sistema simples de ser resolvido, fato que não ocorre de uma forma geral. Contudo, realizando uma sequência de operações do tipo indicado na observação 4.2.16, é possível encontrarmos a matriz

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

geradora do mesmo código C. Com essa nova matriz, para determinarmos os vetores do código da fonte olhando apenas para os vetores do código de canal, basta considerarmos as três primeiras entradas dos vetores dos códigos da fonte.

Definição 4.2.18. Dizemos que uma matriz geradora G de um código $C \subset \mathbb{F}_q^n$ de dimensão k está na forma padrão se $G = (Id_k|A)$, onde Id_k é matriz identidade $k \times k$ e A é uma matriz de ordem $k \times (n - k)$.

Observação 4.2.19. Fixado um código linear C, nem sempre é possível encontrarmos uma matriz geradora para este código que esteja na forma padrão. Como exemplo desse fato, temos o código em $\mathbb{F}_2^5$ de matriz geradora dada por

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

Contudo, quando permutamos também as colunas da matriz anterior, é possível obtermos a matriz

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

que é a matriz geradora de um código C' equivalente a C.

A observação acima nos mostra que, se além das operações apresentadas na observação 4.2.16, acrescentarmos

- Permutação de duas colunas;
- Multiplicação de uma coluna por um escalar não nulo.

é possível obter o seguinte resultado.

Teorema 4.2.20. *Dado um código C, existe um código equivalente C' com matriz geradora na forma padrão.*

Demonstração. A ideia dessa demonstração foi apresentada na observação 4.2.19. Uma prova formal deste resultado pode ser encontrada na referência [7]. ■

4.2.3 Códigos Duais

Definição 4.2.21. Sejam $u = (u_1, ..., u_n)$ e $v = (v_1, ..., v_n)$ elementos de $\mathbb{F}_q^n$. Definimos o produto interno de u e v como sendo $\langle u, v\rangle = u_1v_1 + ... + u_nv_n$.

Observação 4.2.22. A operação definida acima possui as propriedades usuais de produto interno, isto é, é uma operação simétrica e bilinear.

Definição 4.2.23. Seja $C \subset \mathbb{F}_q^n$ um código linear. Definimos

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

Lema 4.2.24. *Seja $C \subset \mathbb{F}_q^n$ um código linear com matriz geradora G. Então*

a) $C^{\perp}$ *é um subespaço vetorial de* $\mathbb{F}_q^n$*;*

b) $x \in C^{\perp} \Leftrightarrow Gx^t = 0$.

Demonstração. a) Em primeiro lugar, $C^{\perp} \neq \emptyset$, pois a n-upla com todas as entradas nulas pertence a $C^{\perp}$. Sejam agora u, $v \in C^{\perp}$, $x \in C$ e $\lambda \in \mathbb{F}_q$. Então

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

o que mostra que $u + \lambda v \in C^{\perp}$. Portanto $C^{\perp}$ é um subespaço vetorial de $\mathbb{F}_q^n$.
b) ($\Rightarrow$) Seja $x \in C^{\perp}$. Então, para todo $u \in C$, $\langle u,\, x\rangle = 0$. Em particular, para todas as linhas de G, v_1, ..., v_k, que constituem uma base de C, temos que $\langle v_i,\, x\rangle = 0$, $i \in \{1,\, ...,\, k\}$. Logo,

$$Gx^t = \begin{bmatrix} \langle v_1,\, x\rangle \\ \vdots \\ \langle v_k,\, x\rangle \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

($\Leftarrow$) Se $Gx^t = 0$, então x é ortogonal a todos os elementos de uma base de C. Pela bilinearidade do produto interno, temos que x é ortogonal a todos os elementos de C. Logo $x \in C^{\perp}$. ■

O lema 4.2.24 nos diz que o conjunto $C^{\perp}$ é também um código linear.

Definição 4.2.25. Seja $C \subset \mathbb{F}_q^n$ um código linear. Então o código linear $C^{\perp}$ é chamado código dual de C.

Proposição 4.2.26. *Seja* $C \subset \mathbb{F}_q^n$ *um código de dimensão* k *com matriz geradora* $G = (Id_k|A)$ *na forma padrão. Então*

a) $dim(C^{\perp}) = n - k$.

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

Demonstração. a) Pelo lema 4.2.24, $x = (x_1,\, ...,\, x_n) \in C^{\perp}$ se, e somente se, $Gx^t = 0$. Ainda

$$(Id_k|A)x^t = 0 \Leftrightarrow \begin{bmatrix} x_1 & + & a_{k+1}^{(1)}x_{k+1} & + & ... & + & a_n^{(1)}x_n \\ & & & \vdots & & & \\ x_k & + & a_{k+1}^{(k)}x_{k+1} & + & ... & + & a_n^{(k)}x_n \end{bmatrix} = 0$$

$$\Leftrightarrow \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} + A \begin{bmatrix} x_{k+1} \\ \vdots \\ x_n \end{bmatrix} = 0$$

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

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

b) Como as linhas de H são linearmente independentes em virtude do bloco Id_{n-k}, temos que essas geram um subespaço de dimensão $n-k$. Ainda, as linhas de H são ortogonais às linhas de G, de forma que o espaço gerado pelas linhas de H está contido em $C^\perp$. Agora, uma vez que esses subespaços têm a mesma dimensão, eles coincidem, o que mostra que $H = (-A^t|Id_{n-k})$ é uma matriz geradora de $C^\perp$. ■

Lema 4.2.27. *Seja C um código linear em $\mathbb{F}_q^n$. Para toda permutação σ de $\{1, ..., n\}$, para todo $\lambda \in \mathbb{F}_q \setminus \{0\}$ e para todo $j = 1, ..., n$, temos que*

a) $(T_\sigma(C))^\perp = T_\sigma(C^\perp)$;

b) $(T_\lambda^j(C))^\perp = T_{\lambda^{-1}}^j(C^\perp)$.

Demonstração. a) Seja $c = (c_1, ..., c_n) \in (T_\sigma(C))^\perp$. Então, dado $u_\sigma \in T_\sigma(C)$, temos que $u_\sigma = (u_{\sigma(1)}, ..., u_{\sigma(n)})$, onde $u = (u_1, ..., u_n) \in C$, de modo que $\langle c, u_\sigma \rangle = 0$. Mas dessa forma, $c_{\sigma^{-1}} = (c_{\sigma^{-1}(1)}, ..., c_{\sigma^{-1}(n)}) \in C^\perp$, pois

$$\langle c, u_\sigma \rangle = 0 \Rightarrow \langle c_{\sigma^{-1}}, u_{\sigma^{-1}\circ\sigma} \rangle = \langle c_{\sigma^{-1}}, u \rangle = 0\,,$$

onde $u \in C$ é fixo, mas arbitrário. Logo, concluimos que $c = T_\sigma(c_{\sigma^{-1}}) \in T_\sigma(C^\perp)$. Reciprocamente, dado $c_\sigma \in T_\sigma(C^\perp)$, temos que $c_\sigma = (c_{\sigma(1)}, ..., c_{\sigma(n)})$, sendo

que $c = (c_1, ..., c_n) \in C^{\perp}$. Daí, dado $u_\sigma = (u_{\sigma(1)}, ..., u_{\sigma(n)}) \in T_\sigma(C)$, onde $u = (u_1, ..., u_n) \in C$, temos que $\langle c_\sigma, u_\sigma \rangle = \langle c, u \rangle = 0$.

b) Seja $c = (c_1, ..., c_n) \in (T^j_\lambda(C))^{\perp}$. Então, dado $u_\lambda \in T^j_\lambda(C)$, temos que $u_\lambda = (u_1, ..., u_{j-1}, \lambda u_j, u_{j+1}, ..., u_n)$, onde $u = (u_1, ..., u_n) \in C$, de modo que $\langle c, u_\lambda \rangle = 0$. Mas dessa forma, $c_\lambda = (c_1, ..., c_{j-1}, \lambda c_j, c_{j+1}, ..., c_n) \in C^{\perp}$, pois $\langle c_\lambda, u \rangle = \langle c, u_\lambda \rangle = 0$. Concluimos que $c = T^j_{\lambda^{-1}}(c_\lambda) \in T^j_{\lambda^{-1}}(C^{\perp})$, pois u é arbitrário. Reciprocamente, dado $c_{\lambda^{-1}} \in T^j_{\lambda^{-1}}(C^{\perp})$, temos que

$$c_{\lambda^{-1}} = (c_1, ..., c_{j-1}, \lambda^{-1} c_j, c_{j+1}, ..., c_n),$$

onde $c = (c_1, ..., c_n) \in C^{\perp}$. Dado $u_\lambda = (u_1, ..., u_{j-1}, \lambda u_j, u_{j-1}, ..., u_n) \in T^j_\lambda(C)$, onde $u = (u_1, ..., u_n) \in C$, temos que $\langle c_{\lambda^{-1}}, u_\lambda \rangle = \langle c, u \rangle = 0$. ■

Proposição 4.2.28. *Sejam C e D dois códigos lineares em $\mathbb{F}_q^n$. Se C e D são linearmente equivalentes, então $C^{\perp}$ e $D^{\perp}$ são linearmente equivalentes.*

Demonstração. Se C e D são códigos linearmente equivalentes, então existem uma permutação σ de $\{1, ..., n\}$ e $c_1, ..., c_n \in \mathbb{F}_q \setminus \{0\}$ tais que $D = T_\sigma \circ T^1_{c_1} \circ ... \circ T^n_{c_n}(C)$. Daí, pelo lema 4.2.27 temos que o resultado segue, pois

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

■

Corolário 4.2.29. *Seja D um código linear em $\mathbb{F}_q^n$ de dimensão k. Então $D^{\perp}$ é um código de dimensão $n - k$.*

Demonstração. Pelo teorema 4.2.20, o código D é equivalente a um código C, também de dimensão k, com matriz geradora na forma padrão e, portanto, pela proposição 4.2.26, segue que $dim(C^{\perp}) = n - k$. Pela proposição 4.2.28, temos que $D^{\perp}$ é equivalente a $C^{\perp}$, e, dessa forma, também tem dimensão $n - k$. ■

Lema 4.2.30. *Suponhamos que C seja um código de dimensão k em $\mathbb{F}_q^n$ com matriz geradora G. Uma matriz H de ordem $(n - k) \times n$ com coeficientes em $\mathbb{F}_q$ e com linhas linearmente independentes é uma matriz geradora de $C^{\perp}$ se, e somente se, $GH^t = 0$.*

Demonstração. Com efeito, as linhas de H geram um subespaço vetorial de $\mathbb{F}_q^n$ de dimensão $n-k$, que é a dimensão de $C^\perp$. Por outro lado, representando por h_1, ..., h_{n-k} e por g_1, ..., g_k, respectivamente, as linhas de H e de G, temos que $(GH^t)_{ij} = \langle g_i, h_j \rangle$. Portanto, $GH^t = 0$ 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 $GH^t = 0$ se, e somente se, $C^\perp$ é gerado pelas linhas de H. ■

Corolário 4.2.31. *Seja C um código linear. Então $(C^\perp)^\perp = C$.*

Demonstração. Sejam C e H, respectivamente, as matrizes geradoras de C e $C^\perp$. Logo $GH^t = 0$. Assim $0 = (GH^t)^t = (H^t)^t G^t = HG^t$. Isso mostra que G é a matriz geradora de $(C^\perp)^\perp$, donde segue o resultado. ■

Proposição 4.2.32. *Seja C um código linear e suponhamos que H seja uma matriz geradora de $C^\perp$. Temos dessa forma que $v \in C$ se, e somente se, $Hv^t = 0$.*

Demonstração. De fato, pelo lema 4.2.24, temos que $v \in C = (C^\perp)^\perp$ se, e somente se, $Hv^t = 0$. ■

Definição 4.2.33. Seja C um código linear. A matriz H geradora de $C^\perp$ é chamada de matriz teste de paridade de C.

Definição 4.2.34. Dados um código linear C com matriz teste de paridade H e um vetor $v \in \mathbb{F}_q^n$, chamamos o vetor Hv^t de síndrome de v.

Exemplo 4.2.35. Seja C o código sobre $\mathbb{F}_2$ com matriz geradora

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

Como G está na forma padrão, temos, pela proposição 4.2.26, que a matriz teste de paridade H é dada por

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

Sejam $u = (1, 0, 0, 1, 1, 0)$ e $v = (0, 0, 0, 1, 1, 0) \in \mathbb{F}_2^6$. Então

$$Hu^t = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad e \quad Hv^t = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix},$$

fato que nos dá que $u \in C$, mas $v \notin C$.

Proposição 4.2.36. *Seja H uma matriz teste de paridade de um código C. Temos que o peso de C é maior ou igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes.*

Demonstração. ($\Rightarrow$) Suponhamos que $\omega(C) \geqslant s$ e que H tenha $s-1$ colunas linearmente dependentes, a saber h^{i_1}, h^{i_2}, ..., $h^{i_{s-1}}$. Daí, existiriam c_{i_1}, c_{i_2}, ..., $c_{i_{s-1}} \in \mathbb{F}_q$ não todos nulos tais que

$$c_{i_1}h^{i_1} + c_{i_2}h^{i_2} + ... + c_{i_{s-1}}h^{i_{s-1}} = 0.$$

Portanto $(0, ..., c_{i_1}, ..., c_{i_{s-1}}, ...) \in C$ e consequentemente $\omega(C) \leqslant s-1 < s$, o que seria uma contradição. Portanto quaisquer $s-1$ colunas de H devem ser linearmente independentes.
($\Leftarrow$) Seja $c = (c_1, ..., c_n)$ uma palavra não nula de C e sejam h^1, ..., h^n as colunas de H. Como $Hc^t = 0$, temos que $0 = Hc^t = \sum_{i=1}^{n} c_i h^i$. Sabendo que $\omega(c)$ é o número de componentes não nulas de c, segue que se $\omega(c) \leqslant s-1$, teríamos pela igualdade anterior uma combinação linear nula de um número t de colunas de H, com $1 \leqslant t \leqslant s-1$, o que é uma contradição. Logo $\omega(c) \geqslant s$ e, portanto, $\omega(C) \geqslant s$. ■

Teorema 4.2.37. *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. ($\Rightarrow$) Supondo $\omega(C) = s$, temos, pela proposição 4.2.36, que todo conjunto de $s-1$ colunas de H é linearmente independente. Por outro lado, devem existir s colunas linearmente dependentes, pois caso contrário, pela mesma proposição citada acima teríamos $\omega(C) \geqslant s+1$.
($\Leftarrow$) Pela proposição 4.2.36, temos que $\omega(C) \geqslant s$. Mas $\omega(C)$ não pode ser maior do que s, pois neste caso, novamente pela proposição 4.2.36, teríamos que quaisquer s colunas de H são linearmente independentes, o que é uma contradição. ■

Corolário 4.2.38 (Cota de Singleton)**.** *Os parâmetros* (n, k, d) *de um código linear satisfazem à desigualdade* $d \leqslant n-k+1$.

Demonstração. Se H é uma matriz teste de paridade, então ela tem posto $n-k$. Pelo teorema 4.2.37, temos que se a distância mínima de C é d, então quaisquer $d-1$ colunas de H devem ser linearmente independentes e devem existir d colunas de H linearmente dependentes. Como posto de H é $n-k$, temos que existe pelo menos um grupo de $n-k$ colunas de H linearmente independentes e que qualquer quantidade maior de colunas é linearmente dependente. Assim, 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. Dessa forma, temos que $d-1 \leqslant n-k$, de modo que o resultado segue. ■

4.3 CÓDIGOS CÍCLICOS

4.3.1 Primeiras Definições e Propriedades

Representaremos a partir de agora um elemento em $\mathbb{F}_q^n$ por $(x_0, ..., x_{n-1})$.

Definição 4.3.1. Um código linear $C \subset \mathbb{F}_q^n$ será chamado de código cíclico se, para todo $c = (c_0, ..., c_{n-1}) \in C$, o vetor $(c_{n-1}, c_0, ..., c_{n-2}) \in C$.

Observação 4.3.2. Com base no que já foi visto até aqui, um código linear $C \subset \mathbb{F}_q^n$ será um código cíclico se dada a permutação π de $\{0, ..., n-1\}$ de lei de formação

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

tivermos

$$T_\pi(c_0, ..., c_{n-1}) = (c_{\pi(0)}, c_{\pi(1)}, ..., c_{\pi(n-1)}) = (c_{n-1}, c_0, ..., c_{n-2}) \in C$$

para todo $(c_0, ..., c_{n-1}) \in C$, ou seja, $T_\pi(C) \subset C$.

Exemplo 4.3.3. Seja $v \in \mathbb{F}_q^n$. O espaço vetorial

$$\langle v \rangle = \{a_0 v + a_1 T_\pi(v) + ... + a_{n-1} T_\pi^{n-1}(v);\ a_i \in \mathbb{F}_q,\ \forall\, i = 0, ..., n-1\}$$

é um código linear cíclico, notando-se que $T_\pi^n = Id$.

Definição 4.3.4. Denotaremos por R_n o anel das classes residuais de $\mathbb{F}_q[x]$ módulo o polinômio $x^n - 1$, isto é, $R_n = \dfrac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$.

Observação 4.3.5. De acordo com a definição 4.3.4, temos que um elemento $\overline{f(x)} \in R_n$ é da forma $\overline{f(x)} = \{f(x) + g(x)(x^n - 1);\ g(x) \in \mathbb{F}_q[x]\}$. Podemos atribuir a R_n uma estrutura adicional de espaço vetorial sobre $\mathbb{F}_q$ definindo a multiplicação por escalar por $\lambda\overline{f(x)} = \overline{\lambda f(x)}$. Neste caso, a dimensão de R_n sobre $\mathbb{F}_q$ é n e $\{1, \overline{x}, ..., \overline{x^{n-1}}\}$ é uma base de R_n sobre $\mathbb{F}_q$. Logo, $\mathbb{F}_q^n$ é isomorfo a R_n através da transformação linear $\nu : \mathbb{F}_q^n \to R_n$ dada por

$$\nu(a_0, a_1, ..., a_{n-1}) = \overline{a_0 + a_1 x + ... + a_{n-1} x^{n-1}}\,.$$

Temos dessa forma que todo código linear $C \subset \mathbb{F}_q^n$ pode ser transportado para R_n mediante o isomorfismo ν e neste espaço estudado. A vantagem desse processo é que em R_n temos uma estrutura, além da de espaço vetorial, de anel.

4.3.2 Códigos Cíclicos

Iremos nessa seção caracterizar os códigos cíclicos em R_n. Para isso consideraremos T_π e ν as aplicações definidas como na seção 4.3.1.

Observação 4.3.6. A transformação linear T_π pode ser traduzida em R_n da seguinte forma: se $c = (c_0, ..., c_{n-1}) \in \mathbb{F}_q^n$, então $T_\pi(c) = (c_{n-1}, c_0, ..., c_{n-2})$ e $\nu(T_\pi(c)) = \overline{c_{n-1} + c_0 x + ... + c_{n-2} x^{n-1}} = \overline{x} \cdot \overline{c_0 + c_1 x + ... + c_{n-1} x^{n-1}} = \overline{x} \cdot \nu(c)$.

Lema 4.3.7. *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. Se V é um ideal, então V já é, em particular, fechado para a multiplicação por $\overline{x}$. Reciprocamente, suponhamos que V seja fechado para a multiplicação por $\overline{x}$. Como V é um subespaço vetorial, basta mostrarmos que $\overline{f(x)} \cdot \overline{g(x)} \in V$ para todos $\overline{f(x)} \in R_n$ e $\overline{g(x)} \in V$. Com efeito, se $g(x) \in V$, sendo V um subespaço vetorial, temos que $a \cdot \overline{g(x)} \in V$, para todo $a \in \mathbb{F}_q$. Como por hipótese $\overline{x} \cdot \overline{g(x)} = \overline{xg(x)} \in V$, segue, por indução, para todo $n \in \mathbb{N}$, $\overline{x^n} \cdot \overline{g(x)} = \overline{x^n g(x)} \in V$. Logo, escrevendo $\overline{f(x)} = \overline{a_0 + a_1 x + ... + a_{n-1}x^{n-1}}$,

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

■

A observação 4.3.6 e o lema 4.3.7, demonstram o teorema a seguir.

Teorema 4.3.8. *Um subespaço $C \subset \mathbb{F}_q^n$ é um código cíclico se, e somente se, $\nu(C)$ é um ideal de R_n.*

Observação 4.3.9. Como $\mathbb{F}_q[x]$ é um domínio de ideais principais, temos que R_n também o será, de forma que $C \subset \mathbb{F}_q^n$ é um código cíclico se, e somente se, $\nu(C) = \langle \overline{g(x)} \rangle$, onde $g(x) | (x^n - 1)$.

Observação 4.3.10. Pelo corolário 3.1.10, temos que se $p = char(\mathbb{F}_q)$ e $n = mp^s$, com $mdc(m,\, p) = 1$, então $x^n - 1 = (x^m - 1)^{p^s}$. Como a derivada de $x^m - 1$ é $mx^{m-1} \neq 0$, o polinômio $x^m - 1$ não tem fator em comum não constante com a sua derivada, de forma que $x^m - 1$ não possui fator múltiplo algum. Logo, $x^m - 1 = f_1 ... f_r$, onde os f_i são polinômios mônicos, irredutíveis e dois a dois distintos, de modo que a decomposição de $x^n - 1$ em fatores irredutíveis é $f_1^{p^s} ... f_r^{p^s}$. Assim, $x^n - 1$ possui $(p^s + 1)^r$ divisores mônicos. Sabendo que existe uma bijeção entre os ideais de R_n e os divisores mônicos de $x^n - 1$, temos que R_n possui exatamente $(p^s + 1)^r$ ideais. Em particular, se $mdc(n,\, p) = 1$, então $p^s = 1$, de forma que R_n possui 2^r ideais.

Observação 4.3.11. É importante notarmos que R_n não é um domínio de integridade. Com efeito, $(\overline{x - 1})(\overline{x^{n-1} + x^{n-2} + ... + x + 1}) = \overline{x^n - 1} = \overline{0}$.

Para os resultados a seguir, $g(x)$ é um divisor de $x^n - 1$ e $h(x) = \dfrac{x^n - 1}{g(x)}$.

Teorema 4.3.12. *Seja* $I = \langle \overline{g(x)} \rangle \subset R_n$, *onde* $gr(g(x)) = s$. *Então*

$$\{\overline{g(x)}, \overline{xg(x)}, \overline{x^2g(x)}, ..., \overline{x^{n-s-1}g(x)}\}$$

é uma base de I *sobre* $\mathbb{F}_q$.

Demonstração. Em primeiro lugar, o conjunto

$$\{\overline{g(x)}, \overline{xg(x)}, \overline{x^2g(x)}, ..., \overline{x^{n-s-1}g(x)}\}$$

é um conjunto linearmente independente. Com efeito, se

$$a_0 \cdot \overline{g(x)} + a_1 \cdot \overline{xg(x)} + a_2 \cdot \overline{x^2g(x)} + ... + a_{n-s-1} \cdot \overline{x^{n-s-1}g(x)} = \overline{0},$$

então $(\overline{g(x)})(\overline{a_0 + a_1x + ... + a_{n-s-1}x^{n-s-1}}) = \overline{0}$. Logo, para algum $d(x) \in \mathbb{F}_q[x]$, temos que $g(x)(a_0 + a_1x + a_2x^2 + ... + a_{n-s-1}x^{n-s-1}) = d(x)(x^n - 1)$, ou seja, $a_0 + a_1x + a_2x^2 + ... + a_{n-s-1}x^{n-s-1} = d(x)h(x)$. Como o grau de $h(x)$ é $n - s$ e $n - s > n - s - 1$, teremos que $a_0 + a_1x + a_2x^2 + ... + a_{n-s-1}x^{n-s-1} = 0$, de modo que $a_0 = a_1 = a_2 = ... = a_{n-s-1} = 0$.

Resta-nos agora mostrar que

$$\{\overline{g(x)}, \overline{xg(x)}, \overline{x^2g(x)}, ..., \overline{x^{n-s-1}g(x)}\}$$

é um conjunto de geradores de I. Com efeito, se $\overline{f(x)} \in I$, então $\overline{f(x)} = \overline{d(x)} \cdot \overline{g(x)}$, de forma $f(x) \equiv d(x)g(x)\, mod\, (x^n - 1)$. Pelo algoritmo da divisão temos que $d(x) = c(x)h(x) + r(x)$, com $r(x) = a_0 + a_1x + ... + a_{n-s-1}x^{n-s-1}$. Logo,

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

e

$$f(x) \equiv c(x)(x^n - 1) + r(x)g(x) \equiv r(x)g(x)\, mod\, (x^n - 1).$$

Portanto,

$$\overline{f(x)} = a_0 \cdot \overline{g(x)} + a_1 \cdot \overline{xg(x)} + a_2 \cdot \overline{x^2g(x)} + ... + a_{n-s-1} \cdot \overline{x^{n-s-1}g(x)}.$$

■

Corolário 4.3.13. *Dado um código cíclico* C, *existe* $v \in C$ *tal que* $C = \langle v \rangle$.

Demonstração. Seja $I = \nu(C)$. Logo, I é gerado com um espaço vetorial sobre $\mathbb{F}_q$ por $\overline{g(x)}$, $\overline{xg(x)}$, ..., $\overline{x^{n-s-1}g(x)}$, onde $g(x)$ é um divisor de $x^n - 1$ de grau s. Daí, se $v = \nu^{-1}(\overline{g(x)})$, então temos que C é gerado por v, $T_\pi(v)$, ..., $T_\pi^{n-s-1}(v)$, ou seja, $C = \langle v \rangle$. ■

Corolário 4.3.14. *Seja $g(x) = g_0 + g_1x + ... + g_sx^s$. Se $I = \langle \overline{g(x)} \rangle$, então a dimensão de I sobre $\mathbb{F}_q$ é igual a $n - s$ e o código $C = \nu^{-1}(I)$ tem matriz geradora*

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

Definição 4.3.15. Sejam K um corpo e $f(x) \in K[x]$ um polinômio de grau n. Define-se o polinômio recíproco de $f(x)$ como sendo o polinômio $f^*(x) = x^n f(\frac{1}{x})$.

Lema 4.3.16. *Sejam K um corpo, $f(x) = a_0 + a_1x + ... + a_nx^n \in K[x]$ um polinômio mônico de grau n e $f^*(x)$ o polinômio recíproco de $f(x)$. Então*

a) $f^*(x) = a_n + a_{n-1}x + ... + a_1x^{n-1} + a_0x^n$, de forma que $f^*(x) \in K[x]$.

b) Se $g(x) \in K[x]$ é tal que $g(x)|f(x)$, então $g^*(x)|f^*(x)$. Como consequência, se $g(x)|(x^n - 1)$, então $g^*(x)|(x^n - 1)$.

Demonstração. a) Temos que $f\left(\frac{1}{x}\right) = a_0 + a_1\frac{1}{x} + ... + a_n\left(\frac{1}{x}\right)^n = a_0 + a_1\frac{1}{x} + ... + a_n\frac{1}{x^n}$, de forma que $f^*(x) = x^n f\left(\frac{1}{x}\right) = a_0x^n + a_1x^{n-1} + ... + a_n$.

b) Seja $g(x) \in K[x]$ tal que $g(x)|f(x)$. Então, existe $h(x) \in K[x]$ tal que $gr(h(x)) = n - gr(g(x))$ e $f(x) = g(x)h(x)$, de modo que $f\left(\frac{1}{x}\right) = g\left(\frac{1}{x}\right)h\left(\frac{1}{x}\right)$. Logo

$$f^*(x) = x^n f\left(\frac{1}{x}\right) = x^n g\left(\frac{1}{x}\right) h\left(\frac{1}{x}\right) = x^{gr(g(x))} g\left(\frac{1}{x}\right) x^{gr(h(x))} h\left(\frac{1}{x}\right),$$

onde

$$x^{gr(g(x))} g\left(\frac{1}{x}\right) x^{gr(h(x))} h\left(\frac{1}{x}\right) = g^*(x)h^*(x),$$

o que nos dá que $g^*(x)|f^*(x)$. Em particular, se $f(x) = x^n - 1$ e $g(x)|f(x)$, então $g^*(x)|f^*(x)$. Mas como $f^*(x) = -f(x)$, temos que $g^*(x)|f(x)$.

■

Observação 4.3.17. Para o caso específico em que estamos estudando, temos que se $x^n - 1 \in \mathbb{F}_q[x]$ e $g(x)$ é um polinômio que divide $x^n - 1$, isto é, $g(x)$ é o polinômio gerador de algum código cíclico C, então $g^*(x)$ também divide $x^n - 1$, de modo que $g^*(x)$ é o polinômio gerador de algum código cíclico.

Teorema 4.3.18. *Seja $C = \nu^{-1}(I)$ um código cíclico, onde $I = \langle\overline{g(x)}\rangle$ e $g(x)$ é um divisor de $x^n - 1$ de grau s. Se $h(x) = \dfrac{x^n - 1}{g(x)}$, então $C^\perp$ é um código cíclico tal que $C^\perp = \nu^{-1}(J)$, onde $J = \langle\overline{h^*(x)}\rangle$.*

Demonstração. Escrevamos

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

Como $gr(h(x)) = n - s$, temos que $h_{n-s} \neq 0$. Sejam

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

e

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

Como $h_{n-s} \neq 0$, temos que as linhas de H são linearmente independentes. Seja $\{e_1, ..., e_n\}$ a base canônica de $\mathbb{F}_q^n$. A i-ésima linha de G é $G_i = g_0e_i + ... + g_se_{i+s}$, $1 \leqslant i \leqslant n - s$, e a j-ésima coluna de H^t é $H_j = h_{n-s}e_j + ... + h_0e_{j+n-s}$, para $1 \leqslant j \leqslant s$. Suponhamos que $i \leqslant j$. O produto interno de G_i por H_j é dado por

$g_{j-i}h_{n-s} + g_{j-i-1}h_{n-s-1} + ... + g_{n-s}h_{j-i}$, com $0 \leqslant j - i \leqslant s - 1$. Mas essa soma é precisamente o coeficiente de $x^{n-s+j-i}$ no produto $g(x)h(x) = x^n - 1$. Já que $1 \leqslant n - s + j - i \leqslant n - 1$, temos que esse coeficiente é igual a zero. O caso de $j \leqslant i$ pode ser provado de forma análoga. Fica então provado que $GH^t = 0$, donde pelo lema 4.2.30 segue que H é uma matriz geradora de $C^{\perp}$. Agora, notemos que

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

Daí, pelo teorema 4.3.12, temos que $C^{\perp} = \nu^{-1}(J)$, onde $J = \langle\overline{h^*(x)}\rangle$. ■

Corolário 4.3.19. *A matriz teste de paridade de $C = \nu^{-1}(I)$, onde $I = \langle\overline{g(x)}\rangle$, é dada por*

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

onde $\dfrac{x^n - 1}{g(x)} = h_0 + h_1x + ... + h_{n-s}x^{n-s}$.

4.3.3 Códigos Cíclicos Definidos por Anulamento

Seja dado um código cíclico $C \subset \mathbb{F}_q^n$, onde $mdc(n, q) = 1$. Sabemos que C pode ser visto como um ideal $\nu(C) = \langle\overline{g(x)}\rangle$ no anel R_n, onde $g(x) \in \mathbb{F}_q[x]$ divide $x^n - 1$. Seja F um corpo finito que contém $\mathbb{F}_q$ e sobre o qual o polinômio $x^n - 1$ se fatora em fatores lineares mônicos distintos (ver corolário 3.4.3). Sejam α_1, ..., α_r as raízes de $g(x)$ em F que são, portanto, duas a duas distintas.

Proposição 4.3.20. *Com as notações e condições apresentadas no início dessa seção, temos que*

$$\nu(C) = \langle\overline{g(x)}\rangle = \{\overline{f(x)} \in R_n;\ f(\alpha_1) = ... = f(\alpha_r) = 0\}.$$

Demonstração. Temos que $\overline{f(x)} \in \langle \overline{g(x)} \rangle$ se, e somente se, existe $c(x) \in \mathbb{F}_q[x]$ tal que $\overline{f(x)} = \overline{g(x)} \cdot \overline{c(x)}$, de forma $(x^n - 1)d(x) = f(x) - c(x)g(x)$ e, chamando $h(x) = \dfrac{x^n - 1}{g(x)}$, $f(x) = (c(x) + d(x)h(x))g(x)$. Assim, $\overline{f(x)} \in \langle \overline{g(x)} \rangle$ se, e somente se, existe $c'(x) \in \mathbb{F}_q[x]$ tal que $c'(x)g(x) = f(x)$, o que é equivalente à condição $f(\alpha_i) = 0$, para todo $i = 1, ..., r$. Isso mostra o resultado. ■

Observação 4.3.21. Pela proposição 4.3.20, temos que

$$\nu(C) = \langle \overline{g(x)} \rangle = \langle \overline{mmc(irr(\alpha_1, \mathbb{F}_q), ..., irr(\alpha_r, \mathbb{F}_q))} \rangle.$$

Observação 4.3.22. Com a proposição 4.3.20 podemos determinar a matriz teste de paridade de um código cíclico C de forma mais simplificada. De fato, seja $f(x) = \sum_{j=0}^{n-1} a_j x^j \in \mathbb{F}_q[x]$. Então $\overline{f(x)}$ é um elemento de $\langle \overline{g(x)} \rangle$ se, e somente se, $f(\alpha_i) = \sum_{j=0}^{n-1} a_j \alpha_i^j = 0$ $(*)$, para todo $i = 1, ..., r$. Pode-se então descrever o código cíclico C definido pelo polinômio $g(x)$ como sendo o conjunto dos elementos $a = (a_0, ..., a_{n-1}) \in \mathbb{F}_q^n$ tais que $a_0 + a_1\alpha_i + a_2\alpha_i^2 + ... + a_{n-1}\alpha_i^{n-1} = 0$, para todo $i = 1, ..., r$, ou seja, o conjunto dos elementos $a = (a_0, ..., a_{n-1}) \in \mathbb{F}_q^n$ tais que $\tilde{H}a^t = 0$, onde

$$\tilde{H} = \begin{bmatrix} \alpha_1^0 & \alpha_1^1 & ... & \alpha_1^{n-1} \\ \alpha_2^0 & \alpha_2^1 & ... & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots \\ \alpha_r^0 & \alpha_r^1 & ... & \alpha_r^{n-1} \end{bmatrix}.$$

A matriz apresentada acima não é a matriz teste de paridade de C, uma vez que as suas entradas estão em F e não em $\mathbb{F}_q$. Com o intuito de determinar a matriz teste de paridade de C, olhemos para F com espaço vetorial sobre $\mathbb{F}_q$ de dimensão finita d. Dessa forma, podemos representar os elementos $\alpha_i^j \in F$ como vetores colunas $\langle \alpha_i^j \rangle \in \mathbb{F}_q^d$, de modo que $(*)$ é equivalente a $0 = \left\langle \sum_{j=0}^{n-1} a_j \alpha_i^j \right\rangle = \sum_{j=0}^{n-1} \alpha_j \langle \alpha_i^j \rangle$. Definindo a matriz

$$H' = \begin{bmatrix} \langle \alpha_1^0 \rangle & \langle \alpha_1^1 \rangle & ... & \langle \alpha_1^{n-1} \rangle \\ \langle \alpha_2^0 \rangle & \langle \alpha_2^1 \rangle & ... & \langle \alpha_2^{n-1} \rangle \\ \vdots & \vdots & & \vdots \\ \langle \alpha_r^0 \rangle & \langle \alpha_r^1 \rangle & ... & \langle \alpha_r^{n-1} \rangle \end{bmatrix},$$

temos que $a \in C$ se, e somente se, $H'a^t = 0$.

Como as linhas de H' não são necessariamente linearmente independentes, escolhemos um conjunto maximal de linhas linearmente independentes, de modo que obtemos uma matriz teste de paridade H do código C.

Notemos ainda que o número máximo de colunas linearmente independentes de H é o mesmo que o de H' e coincide com o de $\tilde{H}$. Assim, a distância mínima de C pode ser determinada calculando o maior número d tal que quaisquer $d-1$ colunas de $\tilde{H}$ são linearmente independentes.

4.4 CÓDIGOS BCH

Teorema 4.4.1 (Bose - Chaudhuri - Hocquenghem)**.** *Sejam $\mathbb{F}_q$ um corpo finito com q elementos e $n \in \mathbb{N}$ tal que $mdc(n, q) = 1$. Seja F um corpo onde $x^n - 1$ se decompõe em fatores lineares e seja $\gamma \in F$ uma raiz n-ésima primitiva da unidade. Seja C um código cíclico com polinômio gerador*

$$g(x) = mmc(irr(\gamma^a, \mathbb{F}_q), ..., irr(\gamma^{a+\delta-2}, \mathbb{F}_q)),$$

com $a \geqslant 0$ e $\delta \leqslant n$. Então, a distância mínima de C é pelo menos δ e a dimensão de C sobre $\mathbb{F}_q$ é pelo menos $n - m(\delta - 1)$, onde m é a dimensão de F sobre $\mathbb{F}_q$.

Demonstração. A demonstração deste resultado pode ser encontrada em [7]. ■

Definição 4.4.2. Os códigos cíclicos com a forma apresentada no teorema 4.4.1 são denominados códigos BCH. O número δ é dito peso estimado do código BCH.

Definição 4.4.3. Sejam $\mathbb{F}_q$ um corpo finito com q elementos, $n \in \mathbb{N}$ tal que $mdc(n, q) = 1$ e F uma extensão de $\mathbb{F}_q$ que contém uma raiz n-ésima primitiva da unidade γ. Então definimos

$$C_{\mathbb{F}_q}(n, \delta) = \left\{ (a_0, ..., a_{n-1}) \in \mathbb{F}_q^n; \sum_{i=0}^{n-1} a_i \gamma^{ij} = 0, j = 1, ..., \delta - 1 \right\},$$

ou seja, o código BCH definido pelo polinômio

$$g(x) = mmc(irr(\gamma, \mathbb{F}_q), ..., irr(\gamma^{\delta-1}, \mathbb{F}_q)).$$

Observação 4.4.4. Notemos que se $\delta < \delta'$, então $C_{\mathbb{F}_q}(n, \delta') \subset C_{\mathbb{F}_q}(n, \delta)$.

Teorema 4.4.5. *Sejam $\mathbb{F}_q$ um corpo finito com q elementos, $n \in \mathbb{N}$ tal que $mdc(n, q) = 1$, e F uma extensão de $\mathbb{F}_q$ que contém uma raiz n-ésima primitiva da unidade γ. Então $(a_0, ..., a_{n-1}) \in C_{\mathbb{F}_q}(n, \delta)$ se, somente se,*

$$\sum_{j=0}^{n-1} a_j \gamma^{j(\delta-1)} \frac{x^{\delta-1} - \gamma^{-j(\delta-1)}}{x - \gamma^{-j}} = 0.$$

Demonstração. Por definição, temos que $(a_0, ..., a_{n-1}) \in C_{\mathbb{F}_q}(n, \delta)$ se, e somente se, $\sum_{i=1}^{\delta-1} \left(\sum_{j=0}^{n-1} a_j \gamma^{ij} \right) x^i = 0$. Reescrevendo a identidade acima, obtemos

$$0 = \sum_{i=1}^{\delta-1} \left(\sum_{j=0}^{n-1} a_j \gamma^{ij} \right) x^i = x \left(\sum_{i=1}^{\delta-1} \left(\sum_{j=0}^{n-1} a_j \gamma^{ij} \right) x^{i-1} \right) = x \left(\sum_{k=0}^{\delta-2} \left(\sum_{j=0}^{n-1} a_j \gamma^{(k+1)j} \right) x^k \right)$$

donde

$$\begin{aligned} 0 &= \sum_{k=0}^{\delta-2} \left(\sum_{j=0}^{n-1} a_j \gamma^{(k+1)j} \right) x^k \\ &= \sum_{j=0}^{n-1} a_j \gamma^{j(\delta-1)} \left(\sum_{k=0}^{\delta-2} \gamma^{-j(\delta-k-2)} x^k \right) \\ &= \sum_{j=0}^{n-1} a_j \gamma^{j(\delta-1)} \frac{x^{\delta-1} - \gamma^{-j(\delta-1)}}{x - \gamma^{-j}}. \end{aligned}$$

■

4.4.1 Polinômios q-Lineares

Definição 4.4.6. Um polinômio q-linear sobre $\mathbb{F}_{q^m}$ é um polinômio mônico da forma

$$L(x) = \sum_{i=0}^{r} l_i x^{q^i} \in \mathbb{F}_{q^m}[x].$$

Exemplo 4.4.7. Os polinômios x^q e $x^{q^2} + x^q + x$ são exemplos de polinômios q-lineares sobre $\mathbb{F}_{q^m}$.

Observação 4.4.8. Todo polinômio q-linear sobre $\mathbb{F}_{q^m}$ induz a transformação linear $L : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$, dada por $L(x) = \sum_{i=0}^{r} l_i x^{q^i}$, sobre $\mathbb{F}_q$. Com efeito,

$$\begin{aligned} L(\alpha x + y) &= \sum_{i=0}^{r} l_i(\alpha x + y)^{q^i} \\ &= \sum_{i=0}^{r} l_i((\alpha x)^{q^i} + y^{q^i}) \\ &= \sum_{i=0}^{r} l_i(\alpha^{q^i} x^{q^i}) + l_i(y^{q^i}) \\ &= \sum_{i=0}^{r} l_i(\alpha x^{q^i}) + \sum_{i=0}^{r} l_i(y^{q^i}) \\ &= \alpha \sum_{i=0}^{r} l_i(x^{q^i}) + \sum_{i=0}^{r} l_i(y^{q^i}) \\ &= \alpha L(x) + L(y) \end{aligned}$$

para todos x, $y \in \mathbb{F}_{q^m}$ e $\alpha \in \mathbb{F}_q$. Dessa forma, as raízes de um polinômio q-linear constituem um subespaço vetorial de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$, pois o conjunto dessas raízes é o núcleo da transformação linear apresentada acima.

Lema 4.4.9. *Seja V um subespaço vetorial de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Então, o polinômio $L(x) = \prod_{\beta \in V} (x - \beta)$ é mônico, q-linear sobre $\mathbb{F}_{q^m}$ e de grau q^h, onde h é a dimensão de V sobre $\mathbb{F}_q$.*

Demonstração. A demonstração deste resultado pode ser encontrada em [7]. ■

4.4.2 Peso de um Código BCH Primitivo

Definição 4.4.10. Um código BCH em $\mathbb{F}_q^n$, onde $n = q^m - 1$ para algum $m \in \mathbb{N}$, será chamado código primitivo.

Observação 4.4.11. Notemos que em códigos primitivos temos $mdc(n, q) = 1$.

Nesta seção, daremos uma estimativa melhor do que o peso estimado para a distância mínima de um código BCH primitivo.

Definição 4.4.12. Sejam $\mathbb{F}_q$ um corpo finito com q elementos, $n \in \mathbb{N}$ tal que $mdc(n,\, q) = 1$ e F uma extensão de $\mathbb{F}_q$ que contém uma raiz n-ésima primitiva da unidade γ. Seja $a \in \mathbb{F}_q$ um vetor de peso ω e sejam a_{i_1}, ..., a_{i_ω} as suas coordenadas não nulas. Definimos o polinômio localizador de a como sendo

$$l_a(x) = \prod_{j=1}^{\omega}(1 - \gamma^{i_j}x) \in F[x].$$

Observação 4.4.13. Nas condições da definição 4.4.12, temos que o grau do polinômio $l_a(x)$ é $\omega(a)$ e os zeros desse polinômio são raízes da unidade por serem inversos de raízes da unidade.

Lema 4.4.14. *Sejam $\mathbb{F}_q$ um corpo finito com q elementos, n um inteiro positivo tal que $mdc(n, q) = 1$ e F uma extensão de $\mathbb{F}_q$ que contém uma raiz n-ésima primitiva da unidade γ. Seja $l(x) = \sum_{j=0}^{\omega} l_j x^j \in F[x]$ de grau ω. Então $l(x)$ é o polinômio localizador de uma palavra de coordenadas iguais a 0 e 1 de peso ω de $C_{\mathbb{F}_q}(n,\, \delta)$ se, e somente se, são verificadas ambas as condições a seguir:*

a) As raízes de $l(x)$ são raízes n-ésimas da unidade distintas.

b) $l_j = 0$ para todo $j \leqslant \delta - 1$ e j não divisível por p.

Demonstração. A demonstração desse resultado pode ser encontrada em [7]. ■

Proposição 4.4.15. *Seja $C = C_{\mathbb{F}_q}(n,\, \delta)$ um código BCH. Suponhamos que $n = q^m - 1$, para algum $m \in \mathbb{N}$, e que $\delta = q^h - 1$, para algum inteiro h, com $h < m$. Então C tem peso $d = \delta$.*

Demonstração. Se γ um elemento primitivo de $F = \mathbb{F}_{q^m}$ então

$$F^* = \{1,\, \gamma,\, \gamma^2,\, ...,\, \gamma^{n-1}\}$$

e γ é uma raiz n-ésima primitiva da unidade em F. Como pelo teorema 4.4.1 temos que $d \geqslant \delta$, segue que para concluirmos a demonstração basta exibirmos

um elemento $a \in C$ de peso δ. Seja V um subespaço vetorial de F sobre $\mathbb{F}_q$ de dimensão h e consideremos o polinômio $L(x) = \prod_{\beta \in V} (x - \beta)$. Pelo lema 4.4.9, temos que $L(x)$ é um polinômio q-linear de grau q^h e, portanto,

$$L(x) = x^{q^h} + c_{h-1}x^{q^{h-1}} + ... + c_0 x.$$

Notemos que $c_0 \neq 0$, uma vez que $L(x)$ tem $x = 0$ como raiz de multiplicidade 1 (pois cada elemento de V é raiz de multiplicidade 1 de $L(x)$). Consideremos o polinômio recíproco de $L(x)$,

$$L^*(x) = x^{q^h} L(x^{-1}) = 1 + c_{h-1}x^{q^h - q^{h-1}} + ... + c_0 x^{q^h - 1}.$$

Esse polinômio de grau $q^h - 1$ satisfaz às condições a) e b) do lema 4.4.14. De fato, para todo $0 \leqslant i \leqslant h-1$, temos que $p = char(\mathbb{F}_q) | (q^h - q^{h-i})$, o que mostra que $L^*(x)$ satisfaz a condição b) do lema 4.4.14. Ainda, como as raízes de $L(x)$ são raízes n-ésimas da unidade, temos pelo lema 4.3.16 que as raízes de $L^*(x)$ também o são, o que mostra que $L^*(x)$ satisfaz o item a) do lema 4.4.14. Portanto, por esse mesmo resultado, existe uma palavra $a \in C$ de peso δ, cujo polinômio localizador é o polinômio $L^*(x)$. Assim, temos $d = \delta$. ■

Teorema 4.4.16. *Seja $C = C_{\mathbb{F}_q}(n, \delta)$ um código BCH primitivo. Então C tem peso d no máximo igual a $q\delta - 1$.*

Demonstração. Seja h o inteiro positivo tal que $q^{h-1} \leqslant \delta < q^h - 1$. Como os códigos BCH são encaixados, temos que C contém um código C' com peso estimado $q^h - 1$. Pela proposição 4.4.15, temos que o peso de C' é $q^h - 1$. Portanto $d \leqslant q^h - 1 \leqslant q\delta - 1$. ■

4.4.3 Polinômio Gerador de um Código BCH

Seja C um código BCH sobre o corpo $\mathbb{F}_q$ definido pelas raízes n-ésimas da unidade γ^a, ..., $\gamma^{a+\delta-2}$, onde γ é uma raiz n-ésima primitiva da unidade, numa extensão F de $\mathbb{F}_q$. Para determinar

$$g(x) = mmc(irr(\gamma^a, \mathbb{F}_q), ..., irr(\gamma^{a+\delta-2}, \mathbb{F}_q))$$

é preciso determinar os polinômios $irr(\gamma^j, \mathbb{F}_q)$ para qualquer valor de j. Pela proposição 3.3.3, temos que

$$irr(\gamma^j, \mathbb{F}_q) = (x - \gamma^j)(x - (\gamma^j)^q)...(x - (\gamma^j)^{q^{d_j - 1}}),$$

onde d_j é o menor inteiro positivo tal que $(\gamma^j)^{q^{d_j}} = \gamma^j$, isto é, d_j é o menor inteiro positivo tal que $jq^{d_j} \equiv j \, mod \, n$. Portanto, a determinação de $irr(\gamma^j, \mathbb{F}_q)$ passa pela determinação do conjunto

$$C_j = \{\overline{jq^t} \in \mathbb{Z}_n;\, t \in \mathbb{Z},\, t \geqslant 0\},$$

cujos elementos são os expoentes a que devemos elevar γ para achar todas as raízes de $irr(\gamma^j, \mathbb{F}_q)$.

Proposição 4.4.17. *Os conjuntos C_i satisfazem:*

a) Se $C_i \bigcap C_j \neq \emptyset$, então $C_i = C_j$.

b) A união de todos os C_j é igual a $\mathbb{Z}_n$.

Demonstração. a) Se $C_i \bigcap C_j \neq \emptyset$, então existem r e s inteiros não negativos tais que $\overline{iq^r} = \overline{jq^s}$. Dessa forma, supondo $r \geqslant s$, temos que $\overline{iq^{r-s}} = \overline{j}$, pois $mdc(n, q) = 1$. Isso nos dá que $C_j \subset C_i$. Por outro lado, pelo teorema de Euler, temos que $\overline{q^{\varphi(n)}} = \overline{1}$, onde φ é a função de Euler. Multiplicando a igualdade $\overline{iq^{r-s}} = \overline{j}$ por $\overline{q^t}$, onde t é tal que $t + (r - s) = k\varphi(n)$, para algum $k \in \mathbb{N}$, obtemos $\overline{jq^t} = \overline{iq^{r-s}q^t} = \overline{iq^{t+(r-s)}} = \overline{iq^{k\varphi(n)}} = \overline{i(q^{\varphi(n)})^k} = \overline{i}$, o que nos dá que $C_i \subset C_j$. Portanto $C_i = C_j$.
b) Como cada C_j está contido em $\mathbb{Z}_n$, temos que a sua união também está. Por outro lado, $\overline{m} \in C_m$, para todo $m \in \mathbb{Z}$, fato que mostra a outra inclusão. ■

Definição 4.4.18. O conjunto $C_j = \{\overline{jq^t} \in \mathbb{Z}_n;\, t \in \mathbb{Z},\, t \geqslant 0\}$ é chamado de classe de ciclotomia de j módulo n.

Exemplo 4.4.19. Consideremos $n = 20$ e $q = 3$. O menor inteiro positivo m tal que $2^m \equiv 1 \, mod \, 20$ é $m = 4$. Seja α um elemento primitivo de $\mathbb{F}_{81}$. Então $\gamma = \alpha^4$

é uma raiz 20-ésima primitiva da unidade em $\mathbb{F}_{81}$. As classes de ciclotomia módulo 20 são

$$\begin{aligned} C_0 &= \{\overline{0}\} \\ C_1 &= \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\} \\ C_2 &= \{\overline{2}, \overline{6}, \overline{14}, \overline{18}\} \\ \\ C_4 &= \{\overline{4}, \overline{8}, \overline{12}, \overline{16}\} \\ C_5 &= \{\overline{5}, \overline{15}\} \\ C_{10} &= \{\overline{10}\} \\ C_{11} &= \{\overline{11}, \overline{13}, \overline{17}, \overline{19}\}. \end{aligned}$$

Ainda, $d_1 = 4$, $d_2 = 4$, $d_4 = 4$, $d_5 = 2$, $d_{10} = 1$, $d_{11} = 4$, de modo que

$$\begin{aligned} irr(\gamma, \mathbb{F}_3) = irr(\gamma^3, \mathbb{F}_3) &= irr(\gamma^7, \mathbb{F}_3) = irr(\gamma^9, \mathbb{F}_3) \\ &= (x-\gamma)(x-\gamma^3)(x-\gamma^{3^2})(x-\gamma^{3^3}) \\ &= (x-\gamma)(x-\gamma^3)(x-\gamma^9)(x-\gamma^{27}) \\ &= (x-\gamma)(x-\gamma^3)(x-\gamma^7)(x-\gamma^9) \end{aligned}$$

$$\begin{aligned} irr(\gamma^2, \mathbb{F}_3) = irr(\gamma^6, \mathbb{F}_3) &= irr(\gamma^{14}, \mathbb{F}_3) = irr(\gamma^{18}, \mathbb{F}_3) \\ &= (x-\gamma^2)(x-\gamma^{2(3)})(x-\gamma^{2(3^2)})(x-\gamma^{2(3^3)}) \\ &= (x-\gamma^2)(x-\gamma^6)(x-\gamma^{18})(x-\gamma^{54}) \\ &= (x-\gamma^2)(x-\gamma^6)(x-\gamma^{14})(x-\gamma^{18}) \end{aligned}$$

$$\begin{aligned} irr(\gamma^4, \mathbb{F}_3) = irr(\gamma^8, \mathbb{F}_3) &= irr(\gamma^{12}, \mathbb{F}_3) = irr(\gamma^{16}, \mathbb{F}_3) \\ &= (x-\gamma^4)(x-\gamma^{4(3)})(x-\gamma^{4(3^2)})(x-\gamma^{4(3^3)}) \\ &= (x-\gamma^4)(x-\gamma^{12})(x-\gamma^{36})(x-\gamma^{108}) \\ &= (x-\gamma^4)(x-\gamma^8)(x-\gamma^{12})(x-\gamma^{16}) \end{aligned}$$

$$\begin{aligned} irr(\gamma^5, \mathbb{F}_3) = irr(\gamma^{15}, \mathbb{F}_3) &= (x-\gamma^5)(x-\gamma^{5(3)}) \\ &= (x-\gamma^5)(x-\gamma^{15}) \end{aligned}$$

$$irr(\gamma^{10}, \mathbb{F}_3) \;=\; (x - \gamma^{10})$$

e

$$\begin{aligned} irr(\gamma^{11}, \mathbb{F}_3) = irr(\gamma^{13}, \mathbb{F}_3) &= irr(\gamma^{17}, \mathbb{F}_3) = irr(\gamma^{19}, \mathbb{F}_3) \\ &= (x - \gamma^{11})(x - \gamma^{11(3)})(x - \gamma^{11(3^2)})(x - \gamma^{11(3^3)}) \\ &= (x - \gamma^{11})(x - \gamma^{33})(x - \gamma^{99})(x - \gamma^{297}) \\ &= (x - \gamma^{11})(x - \gamma^{13})(x - \gamma^{17})(x - \gamma^{19}) \end{aligned}$$

Assim, por exemplo, o código BCH gerado pelo polinômio

$$\begin{aligned} g(x) &= mmc(irr(\gamma, \mathbb{F}_3), irr(\gamma^2, \mathbb{F}_3), irr(\gamma^3, \mathbb{F}_3), irr(\gamma^4, \mathbb{F}_3), irr(\gamma^5, \mathbb{F}_3)) \\ &= irr(\gamma, \mathbb{F}_3) \cdot irr(\gamma^2, \mathbb{F}_3) \cdot irr(\gamma^4, \mathbb{F}_3) \cdot irr(\gamma^5, \mathbb{F}_3) \end{aligned}$$

é o código $C_{\mathbb{F}_3}(20, 6)$, que tem distância mínima $d \geqslant 6$.

4.5 CÓDIGOS DE GOPPA CLÁSSICOS

Com auxílio do teorema 4.4.5, é possível definirmos os códigos BCH de uma forma que pode ser generalizada e cuja generalização nos fornece os chamados códigos de Goppa clássicos.

Definição 4.5.1. Seja F um corpo finito, extensão do corpo $\mathbb{F}_q$. Sejam $\varphi(x) \in F[x]$ e $L = \{\alpha_0, ..., \alpha_{n-1}\} \subset F$, com $\alpha_i \neq \alpha_j$, se $i \neq j$, e $\varphi(\alpha_i) \neq 0$, para todo $i = 0, ..., n-1$. Definimos

$$\Gamma_{\mathbb{F}_q}(L, \varphi) = \left\{ (c_0, ..., c_{n-1}) \in \mathbb{F}_q^n; \sum_{i=0}^{n-1} c_i \varphi(\alpha_i)^{-1} \frac{\varphi(x) - \varphi(\alpha_i)}{x - \alpha_i} = 0 \right\}.$$

Observação 4.5.2. Nas condições da definição 4.5.1, temos que $\Gamma_{\mathbb{F}_q}(L, \varphi)$ é um subespaço vetorial de $\mathbb{F}_q^n$ e, dessa forma, um código linear.

Definição 4.5.3. O conjunto apresentado na definição 4.5.1 é chamado código de Goppa clássico sobre $\mathbb{F}_q$.

Exemplo 4.5.4. Se considerarmos $\mathbb{F}_q$, F, n e γ como na seção 4.4, se

$$(\alpha_0, ..., \alpha_{n-1}) = (1, \gamma^{-1}, ..., \gamma^{-(n-1)})$$

e se $\varphi(x) = x^{\delta-1}$, então pelo teorema 4.4.5, $\Gamma_{\mathbb{F}_q}(L, \varphi)$ é o código BCH que corresponde às raízes da unidade γ, ..., $\gamma^{\delta-1}$, ou seja, é o código cíclico que está associado ao polinômio

$$g(x) = mmc(irr(\gamma, \mathbb{F}_q), ..., irr(\gamma^{\delta-1}, \mathbb{F}_q)).$$

4.5.1 Matrizes Teste de Paridade para Códigos de Goppa Clássicos

Pretendemos nesta seção encontrar a matriz $\tilde{H}$ que determina por condições de anulamento o código $\Gamma_{\mathbb{F}_q}(L, \varphi)$.

Seja

$$\varphi(x) = \sum_{j=0}^{\delta} \varphi_j x^j,$$

com $\varphi_\delta \neq 0$. Então

$$\begin{aligned}
\frac{\varphi(x) - \varphi(\alpha)}{x - \alpha} &= \sum_{j=0}^{\delta} \varphi_j \frac{x^j - \alpha^j}{x - \alpha} \\
&= 0 + \sum_{j=1}^{\delta} \varphi_j \frac{x^j - \alpha^j}{x - \alpha} \\
&= \varphi_1 + \varphi_2(x + \alpha) + \varphi_3(x^2 + x\alpha + \alpha^2) + ... + \\
&+ \varphi_\delta(x^{\delta-1} + x^{\delta-2}\alpha + ... + x\alpha^{\delta-2} + \alpha^{\delta-1}) \\
&= (\varphi_1 + \varphi_2\alpha + \varphi_3\alpha^2 + ... + \varphi_\delta\alpha^{\delta-1})x^0 + \\
&+ (\varphi_2 + \varphi_3\alpha + \varphi 4\alpha^2 + ... + \varphi_\delta\alpha^{\delta-1})x^1 + ... + (\varphi_\delta)x^{\delta-1} \\
&= \sum_{t=0}^{\delta-1} \left(\sum_{j=t+1}^{\delta} \varphi_j \alpha^{j-1-t} \right) x^t.
\end{aligned}$$

Portanto, $(c_0, ..., c_{n-1}) \in \Gamma_{\mathbb{F}_q}(L, \varphi)$ se, e somente se,

$$\begin{aligned} 0 &= \sum_{i=0}^{n-1} c_i \varphi(\alpha_i)^{-1} \frac{\varphi(x) - \varphi(\alpha_i)}{x - \alpha_i} \\ &= \sum_{i=0}^{n-1} c_i \varphi(\alpha_i)^{-1} \sum_{t=0}^{\delta-1} \left(\sum_{j=t+1}^{\delta} \varphi_j \alpha_i^{j-1-t} \right) x^t \\ &= \sum_{t=0}^{\delta-1} \left(\sum_{i=0}^{n-1} \left(\varphi(\alpha_i)^{-1} \sum_{j=t+1}^{\delta} \varphi_j \alpha_i^{j-1-t} \right) c_i \right) x^t, \end{aligned}$$

o que ocorre se, e somente se,

$$\sum_{i=0}^{n-1} \left(\varphi(\alpha_i)^{-1} \sum_{j=t+1}^{\delta} \varphi_j \alpha_i^{j-1-t} \right) c_i = 0,$$

para todo $0 \leqslant t \leqslant \delta - 1$. Dessa forma, escrevendo

$$B = \begin{bmatrix} \varphi(\alpha_0)^{-1}\varphi_\delta & \dots & \varphi(\alpha_{n-1})^{-1}\varphi_\delta \\ \varphi(\alpha_0)^{-1}(\varphi_{\delta-1} + \varphi_\delta \alpha_0) & \dots & \varphi(\alpha_{n-1})^{-1}(\varphi_{\delta-1} + \varphi_\delta \alpha_{n-1}) \\ \vdots & & \vdots \\ \varphi(\alpha_0)^{-1} \sum_{j=1}^{\delta} \varphi_j \alpha_0^{j-1} & \dots & \varphi(\alpha_{n-1})^{-1} \sum_{j=1}^{\delta} \varphi_j \alpha_{n-1}^{j-1} \end{bmatrix},$$

temos que $c \in \Gamma_{\mathbb{F}_q}(L, \varphi)$ se, e somente se, $Bc^t = 0$. Como $\varphi_\delta \neq 0$, após realizarmos uma sequência de operações elementares sobre as linhas de B, obtemos a matriz

$$\tilde{H} = \begin{bmatrix} \varphi(\alpha_0)^{-1} & \dots & \varphi(\alpha_{n-1})^{-1} \\ \varphi(\alpha_0)^{-1}\alpha_0 & \dots & \varphi(\alpha_{n-1})^{-1}\alpha_{n-1} \\ \vdots & & \vdots \\ \varphi(\alpha_0)^{-1}\alpha_0^{\delta-1} & \dots & \varphi(\alpha_{n-1})^{-1}\alpha_{n-1}^{\delta-1} \end{bmatrix},$$

de modo que $c \in \Gamma_{\mathbb{F}_q}(L, \varphi)$ se, e somente se, $\tilde{H}c^t = 0$.

Se $F = \mathbb{F}_q$, então $\tilde{H}$ é uma matriz teste de paridade de $\Gamma_{\mathbb{F}_q}(L, \varphi)$, de modo que se chamarmos $\Lambda_{\mathbb{F}_q}(L, \varphi)$ o código gerado pela matriz $\tilde{H}$, temos que $\Lambda_{\mathbb{F}_q}(L, \varphi) = (\Gamma_{\mathbb{F}_q}(L, \varphi))^{\perp}$.

Caso contrário, cada elemento da matriz $\tilde{H}$ pode ser escrito como um vetor coluna de comprimento m com entradas em $\mathbb{F}_q$, olhando F como um espaço vetorial de dimensão m sobre $\mathbb{F}_q$. Assim, é possível obter uma matriz H' tal que $c \in \Gamma_{\mathbb{F}_q}(L, \varphi)$ se, e somente se, $H'c^t = 0$. Uma vez que as linhas de H' não necessariamente linearmente independentes, H' pode ainda não ser a matriz teste de paridade de $\Gamma_{\mathbb{F}_q}(L, \varphi)$. Contudo, tomando um conjunto maximal de linhas linearmente independentes, obtemos a matriz teste de paridade H de $\Gamma_{\mathbb{F}_q}(L, \varphi)$.

Teorema 4.5.5. *Seja F uma extensão do corpo $\mathbb{F}_q$, tal que a dimensão de F sobre $\mathbb{F}_q$ é m. Sejam $\varphi(x) \in F[x]$, com $gr(\varphi) = \delta$, e $L = \{\alpha_0, ..., \alpha_{n-1}\} \subset F$, com $\alpha_i \neq \alpha_j$, se $i \neq j$, e $\varphi(\alpha_i) \neq 0$, para todo $i = 0, ..., n-1$. Então $\Gamma_{\mathbb{F}_q}(L, \varphi)$ é um código de dimensão $k \geqslant n - m\delta$ e com distância mínima $d \geqslant \delta + 1$.*

Demonstração. A demonstração deste resultado é análoga a do teorema 4.4.1, que pode ser encontrada na referência [7]. ■

4.5.2 Matriz Geradora de um Código de Goppa

Definição 4.5.6. Escreveremos $\sum_{i=0}^{n-1} \frac{c_i}{x - \alpha_i} \equiv 0 \, mod \, \varphi(x)$ quando existirem polinômios $a(x)$ e $b(x)$ primos entre si tais que $\varphi(x) | a(x)$ e $\sum_{i=0}^{n-1} \frac{c_i}{x - \alpha_i} = \frac{a(x)}{b(x)}$.

Proposição 4.5.7. *Seja F uma extensão do corpo $\mathbb{F}_q$. Sejam $\varphi(x) \in F[x]$, com $gr(\varphi) = \delta$ e $L = \{\alpha_0, ..., \alpha_{n-1}\} \subset F$, com $\alpha_i \neq \alpha_j$, se $i \neq j$, e $\varphi(\alpha_i) \neq 0$, para todo $i = 0, ..., n-1$. Então temos que*

$$\Gamma_{\mathbb{F}_q}(L, \varphi) = \left\{ (c_0, ..., c_{n-1}) \in \mathbb{F}_q^n; \sum_{i=0}^{n-1} \frac{c_i}{x - \alpha_i} \equiv 0 \, mod \, \varphi(x) \right\}.$$

Demonstração. Notemos que

$$\frac{1}{x - \alpha_i} \equiv \frac{-1}{\varphi(\alpha_i)} \left(\frac{\varphi(x) - \varphi(\alpha_i)}{x - \alpha_i} \right) \, mod \, \varphi(x).$$

Se $C = \left\{ (c_0, ..., c_{n-1}) \in \mathbb{F}_q^n; \sum_{i=0}^{n-1} \frac{c_i}{x - \alpha_i} \equiv 0 \, mod \, \varphi(x) \right\}$ e $c = (c_0, ..., c_{n-1})$, então

$$\begin{aligned} c \in C &\Leftrightarrow \sum_{i=0}^{n-1} \frac{c_i}{x-\alpha_i} \equiv 0 \, mod \, \varphi(x) \\ &\Leftrightarrow \sum_{i=0}^{n-1} \frac{-c_i}{\varphi(\alpha_i)} \left(\frac{\varphi(x)-\varphi(\alpha_i)}{x-\alpha_i} \right) \equiv 0 \, mod \, \varphi(x) \\ &\Leftrightarrow \sum_{i=0}^{n-1} \frac{-c_i}{\varphi(\alpha_i)} \left(\frac{\varphi(x)-\varphi(\alpha_i)}{x-\alpha_i} \right) = 0 \\ &\Leftrightarrow c \in \Gamma_{\mathbb{F}_q}(L, \varphi), \end{aligned}$$

onde a penúltima equivalência decorre do grau de $f(x) = \sum_{i=0}^{n-1} \frac{-c_i}{\varphi(\alpha_i)} \left(\frac{\varphi(x)-\varphi(\alpha_i)}{x-\alpha_i} \right)$ ser menor do que o grau de $\varphi(x)$. ■

Proposição 4.5.8. *Uma matriz geradora do código* $\Gamma_{\mathbb{F}_q}(L, \varphi)$ *é*

$$\begin{bmatrix} \frac{\varphi(\alpha_0)}{h'(\alpha_0)} & \cdots & \frac{\varphi(\alpha_{n-1})}{h'(\alpha_{n-1})} \\ \frac{\varphi(\alpha_0)}{h'(\alpha_0)}\alpha_0 & \cdots & \frac{\varphi(\alpha_{n-1})}{h'(\alpha_{n-1})}\alpha_{n-1} \\ \vdots & & \vdots \\ \frac{\varphi(\alpha_0)}{h'(\alpha_0)}\alpha_0^{n-1-\delta} & \cdots & \frac{\varphi(\alpha_{n-1})}{h'(\alpha_{n-1})}\alpha_{n-1}^{n-1-\delta} \end{bmatrix},$$

onde $h(x) = \prod_{j=0}^{n-1}(x-\alpha_j)$.

Demonstração. Em primeiro lugar, temos que $c = (c_0, ..., c_{n-1}) \in \Gamma_{\mathbb{F}_q}(L, \varphi)$ se, e somente se, existe $b(x) \in F[x]$ tal que $\sum_{i=0}^{n-1} \frac{c_i}{x-\alpha_i} = \frac{b(x)\varphi(x)}{h(x)}$, conforme está explicado na observação 4.5.9. Portanto, para determinar um elemento $c \in \Gamma_{\mathbb{F}_q}(L, \varphi)$, precisamos apenas encontrar $b(x) \in F[x]$ que satisfaça a última igualdade. Assim, temos que

$$b(x)\varphi(x) = h(x) \sum_{i=0}^{n-1} \frac{c_i}{x-\alpha_i} = \sum_{i=0}^{n-1} c_i \prod_{k \neq i}(x-\alpha_k).$$

Sabemos também que $h'(x) = \sum_{i=0}^{n-1} \prod_{k \neq i} (x - \alpha_k)$, de modo que

$$h'(\alpha_j) = \sum_{i=0}^{n-1} \prod_{k \neq i} (\alpha_j - \alpha_k) = \prod_{k \neq j} (\alpha_j - \alpha_k).$$

Logo, para cada $j = 0, ..., n-1$,

$$b(\alpha_j)\varphi(\alpha_j) = \sum_{i=0}^{n-1} c_i \prod_{k \neq i} (\alpha_j - \alpha_k) = c_j \prod_{k \neq j} (\alpha_j - \alpha_k) = c_j h'(\alpha_j).$$

Sabendo que $gr(b(x)) \leqslant n-1-\delta$, é possível escrevermos $b(x) = \sum_{i=0}^{n-1-\delta} b_i x^i$. Portanto, para cada $j = 0, ..., n-1$, temos que $\frac{c_j h'(\alpha_j)}{\varphi(\alpha_j)} = b(\alpha_j) = \sum_{i=0}^{n-1-\delta} b_i \alpha_j^i$. Assim,

$$c_j = \frac{\varphi(\alpha_j)}{h'(\alpha_j)} \sum_{i=0}^{n-1-\delta} b_i \alpha_j^i = \sum_{i=0}^{n-1-\delta} b_i \frac{\varphi(\alpha_j)\alpha_j^i}{h'(\alpha_j)}.$$

Dessa forma, $c \in \Gamma_{\mathbb{F}_q}(L, \varphi)$ se, e somente se, existe $(b_0, ..., b_{n-1-\delta}) \in F^{n-\delta}$ tal que

$$c = (b_0, ..., b_{n-1-\delta}) \begin{bmatrix} \frac{\varphi(\alpha_0)}{h'(\alpha_0)} & \cdots & \frac{\varphi(\alpha_{n-1})}{h'(\alpha_{n-1})} \\ \frac{\varphi(\alpha_0)}{h'(\alpha_0)}\alpha_0 & \cdots & \frac{\varphi(\alpha_{n-1})}{h'(\alpha_{n-1})}\alpha_{n-1} \\ \vdots & & \vdots \\ \frac{\varphi(\alpha_0)}{h'(\alpha_0)}\alpha_0^{n-1-\delta} & \cdots & \frac{\varphi(\alpha_{n-1})}{h'(\alpha_{n-1})}\alpha_{n-1}^{n-1-\delta} \end{bmatrix}.$$

■

Observação 4.5.9. Pretendemos aqui fornecer uma explicação para a primeira equivalência apresentada na demonstração da proposição 4.5.8. Para isso, consideremos as hipóteses da mesma. Dado $c = (c_0, ..., c_{n-1}) \in \mathbb{F}_q^n$, podemos escrever $\sum_{i=0}^{n-1} \frac{c_i}{x - \alpha_i} = \frac{P(x)}{h(x)}$. Assim

$$
\begin{aligned}
c \in \Gamma_{\mathbb{F}_q}(L,\, \varphi) \quad &\Rightarrow \quad \frac{P(x)}{h(x)} = \frac{a(x)}{b(x)}, \text{ onde } \varphi(x)|a(x) \text{ e } mdc(a(x),\, b(x)) = 1 \\
&\Rightarrow \quad P(x)b(x) = a(x)h(x), \text{ com } \varphi(x)|a(x) \text{ e } mdc(a(x),\, b(x)) = 1 \\
&\Rightarrow \quad \varphi(x)|P(x) \\
&\Rightarrow \quad P(x) = \varphi(x)Q(x).
\end{aligned}
$$

Por outro lado, se existe $b(x)$ tal que $\dfrac{b(x)\varphi(x)}{h(x)} = \displaystyle\sum_{i=0}^{n-1} \frac{c_i}{x - \alpha_i}$, como $mdc(\varphi(x), h(x)) = 1$, pois α_i não é raiz de $\varphi(x)$ para nenhum i, temos que é possível simplificar o quociente $\dfrac{b(x)}{h(x)}$ de forma a obter uma expressão tal que $\dfrac{b(x)}{h(x)} = \dfrac{b'(x)}{h'(x)}$, com $mdc(b'(x),\, h'(x)) = 1$. Isso nos dá uma expressão que satisfaz a definição 4.5.6.

REFERÊNCIAS

[1] GARCIA, A. L. P.; LEQUAIN, Y. A. E. *Elementos de álgebra*. 6. ed. Rio de Janeiro: IMPA, 2012.

[2] GONÇALVES, A. *Introdução à Álgebra*. 5. ed. Rio de Janeiro: IMPA, 2011.

[3] HUNGERFORD, T. W. *Algebra*. New York: Springer-Verlag, 1974.

[4] STEWART, I. *Galois Theory*. 3. ed. Chapman and Hall, 2003.

[5] HUCZYNSKA, S.; NEUNHÖFFER, M. *Finite Fields*. Disponível em `http://www.math.rwth-aachen.de/~Max.Neunhoeffer/Teaching/ff2013/ff2013.pdf`. Acesso em: 19 ago. 2014.

[6] LIDL, R.; NIEDERREITER, H. *Introduction to Finite Fields and their Applications*. Cambridge: Cambridge University Press, 1986.

[7] HEFEZ, A.; VILLELA, M. L. T. *Códigos Corretores de Erros*. 2. ed. Rio de Janeiro: IMPA, 2008.

[8] HUFFMAN, W. C.; PLESS, V. *Fundamentals of Error-Correcting Codes*. Cambridge: Cambridge University Press, 2003.

[9] MILES, C. P. *Breve introdução à Teoria dos Códigos Corretores de Erros*. Disponível em `http://www.sbm.org.br/docs/coloquios/NE-1.04.pdf`. Acesso em: 30 set. 2014.