Revista Eletrônica Paulista de Matemática

ISSN 2316-9664
v. 23, n. 1, jul. 2023
Artigo de Iniciação Científica

Corpos finitos: códigos cíclicos e BCH binário

Finite Field: cyclic code and binary BCH code

Ariely da Silva Camargo
Faculdade de Engenharia Mecânica
Universidade Federal de Uberlândia
ariely.camargo@ufu.br

Ana Paula Tremura Galves
Faculdade de Matemática
Universidade Federal de Uberlândia
ana.galves@ufu.br

Resumo

Com a transmissão de informações realizadas por meio digitais, foi importante criar mecanismos que assegurassem que as informações recebidas correspondiam as enviadas. A fim de assegurar essa transmissão, foram criados códigos corretores e detectores de erros, os quais, atualmente, são indispensáveis na transmissão de informações digitais. Neste sentido, os códigos cíclicos, como o de Reed Somolon (RS) e de Bose–Chaudhuri–Hocquenghem (Código BCH) são utilizados nessas transmissões. Desse modo, o artigo busca exemplificar os processos de codificação e decodificação de um código BCH binário. Para isso, inicialmente, serão abordados conceitos de Álgebra Abstrata, como grupos e polinômios, bem como mostrada a construção de um corpo finito. Após isso, serão apresentados os códigos BCH binário, mostrando sua definição e exemplo da decodificação de uma informação recebida.
Palavras-chave: Códigos cíclicos. Código BCH binário. Corpos finitos. Álgebra abstrata.

Abstract

Because of the increasing use of data trasmission, it was important to create methods to ensure that the information received was equivalent to the information sended. In this context it was created Error-control codes that are used to detect and correct errors that can occur during data transmission. These are now indispensable in the transmission of digital information. In this circumstances, the cyclic codes, such as the Reed Solomon (RS) and the Bose-Chaudhuri-Hocquenghem (BCH code) are used to transmit data. In this sense, the paper aims to show an example of encoding and decoding process. For that, the paper will present concepts of Abstract Algebra, such as group and polynomials. Besides, the article will show the construction of a finite field. After that, the paper will present the binary BCH code, exhibiting its definition and an example of a decoding of a message received.
Keywords: Cyclic Code. BCH Code. Finite Field. Abstract Algebra.

Artigo recebido em mar. 2023 e aceito em jul. 2023

1 Introdução

A revolução tecnológica iniciada no século XX trouxe a possibilidade de se comunicar utilizando meios digitais. Para tornar possível essa comunicação foi necessário desenvolver maneiras de assegurar a transmissão das informações. Essas mensagens passam por canais de comunicação, como fios e ondas eletromagnéticas, sujeitos a distorções elétricas ou magnéticas.

É preciso, então, assegurar que os dados recebidos sejam iguais aos enviados. Nesse contexto, surgem os códigos detectores e corretores de erros. Os códigos detectores de erros identificam um erro e impedem que a informação seja repassada. Já os códigos corretores de erros tem o intuito de descobrir possíveis erros e corrigi-los, fazendo com que a mensagem planejada seja determinada, ainda que certa quantidade de erros tenha acontecido.

Em 1948, o matemático Claude Elwood Shannon estabeleceu bases teóricas para projetar sistemas de comunicação que sejam codificados com uma probabilidade de erro tão pequena quanto a menor capacidade do canal de transmissão da informação. Mais informações sobre a teoria de Shannon pode ser encontrada em Shannon (1948). Além disso, na década de 1940 foi criado o Código de Hamming, um dos primeiros códigos corretores de erros que se tem registro. Tal código é baseado na adição de dígitos de paridade e podem detectar até dois e corrigir até um erro. No entanto, com o desenvolvimento da comunicação digital houve a necessidade de criar códigos mais eficientes que o de Hamming. Neste sentido, desenvolveu-se a classe de códigos cíclicos, a qual inclui o Código de Bose–Chaudhuri–Hocquenghem (Código BCH) e o Código de Reed Solomon (Código RS). O código RS, por exemplo, foi utilizado pela NASA durante missões espaciais.

Assim, devido a importância dos códigos corretores e detectores de erro, esse trabalho tem como objetivo apresentar a teoria dos Códigos Ciclícos do Código BCH binário. Para isso, inicialmente, são apresentados definições e resultados importantes sobre corpos, espaços vetoriais e polinômios. Após isso, é exibido a construção de um corpo finito. Por fim, foi definido Código BCH e apresentado um exemplo.

2 Codificação

A codificação é um campo de estudo relacionado a transmissão de mensagem. Na transmissão de informações, há uma fonte de mensagens, um meio em que a mensagem é transmitida e um usuário que recebe e, geralmente, interpreta a mensagem. No entanto, é importante destacar que no meio de transmissão das informações, erros podem ocorrer, fazendo com que uma informação diferente da planejada chegue ao receptor.

Nesse contexto, considere uma mensagem m que é preciso enviar. Ao invés de enviá-la e deixá-la sujeita a erros, associa-se, a m uma palavra código c. O processo que associa uma mensagem a uma palavra código através de uma bijeção é chamado de codificação. Esse processo pode ser feito através da multiplicação da mensagem por matrizes ou polinômios, por exemplo.

A palavra código c será enviada pelo canal de comunicação e estará sujeita a erros. Assim, a informação r que chega ao receptor pode conter erros. O processo de decodificação irá verificar se erros ocorreram, detectando ou corrigindo tal erro. Caso a correção seja possível, será obtida a palavra código c enviada. Como c e m foram associadas por uma bijeção será possível encontrar a mensagem original m.

O processo de decodificação geralmente usa o método do vizinho mais próximo. Neste método se r é a informação recebida, então é procurada a palavra código c com a maior quantidade de dígitos iguais a r.

É importante ressaltar que existe uma quantidade máxima de erros que determinado código corrige.

Os códigos corretores de erro tem o intuito de descobrir possíveis erros e corrigi-los, fazendo com que a mensagem planejada seja determinada, ainda que certa quantidade de erros tenha acontecido.

Esse trabalho estuda códigos cíclicos. No estudo desses códigos, usa-se conceitos da Álgebra Linear e Abstrata como grupos, anéis, corpos e espaços vetoriais. Tais conceitos são definidos na próxima seção.

3 Conceitos preliminares

Na modelagem de códigos corretores e detectores de erros, faz-se necessário o entendimento de grupos, anéis, ideais, corpos e polinômios. Isso porque tais conceitos serão utilizados na teoria dos códigos. Assim, a compreensão desses conceitos é indispensável no entendimento de códigos cíclicos e códigos BCH binários, os quais serão tratados nas seções subsequentes.

3.1 Grupos, anéis, ideais e corpos

Definição 1 (Grupo) *Seja $(G,+)$ um conjunto G não vazio sobre o qual foi definido uma operação de adição. $(G,+)$ será chamado de grupo aditivo se as seguintes condições 1, 2 e 3 forem satisfeitas. Além disso, $(G,+)$ será chamado de grupo abeliano se a condição 4 abaixo for satisfeita.*

1. *Se $a,b,c \in G$ então $a+(b+c)=(a+b)+c$. (Propriedade associativa da adição.)*
2. *Existe um elemento $0_G \in G$ tal que $a+0_G=a$, para todo $a \in G$. O elemento 0_G é chamado elemento neutro de G.*
3. *Para todo $a \in G$, existe $a' \in G$ tal que $a+a'=0_G$. Esse elemento é indicado por $-a$ e é chamado oposto de a.*
4. *Se $a,b \in G$, então $a+b=b+a$. (Propriedade comutativa da adição.)*

Definição 2 (Anel) *Seja $(A,+,.)$ um conjunto A não vazio, sobre o qual foram definidas uma operação de adição e uma operação de multiplicação. $(A,+,.)$ será chamado de anel se as condições da Definição 1 e também as seguintes condições forem satisfeitas.*

1. *A multiplicação goza da propriedade associativa, isto é, se $a,b,c \in A$ então $a.(b.c)=(a.b).c$.*
2. *Se $a,b,c \in A$ então $a.(b+c)=a.b+a.c$ e $(a+b).c=a.c+b.c$, isto é, a multiplicação é distributiva em relação à adição.*

Além disso, $(A,+,.)$ será chamado de anel comutativo se a multiplicação é comutativa, isto é, se $a,b \in A$, então $a.b=b.a$.

Definição 3 (Subanel) *Seja $(A,+,.)$ um anel e L um subconjunto não vazio de A. Diz se que L é um subanel de A se $(L,+,.)$ também é um anel, em que a adição e multiplicação consideradas são as mesmas de A, porém restritas aos elementos de L.*

Definição 4 (Ideal) *Seja* $(A, +, .)$ *um anel comutativo. Um subconjunto não vazio* $I \subset A$ *será chamado ideal em A se, para quaisquer* $x, y \in I$ *e* $a \in A$*, tem-se* $x - y \in I$ *e* $a.x \in I$*.*

Definição 5 (Conjunto das classes laterais) *Seja* $(G, +)$ *um grupo, H um subgrupo de G e* $a \in G$*. O conjunto indicado e definido por* $a + H = \{a + h \mid h \in H\}$ *é chamado de classe lateral à direita módulo H definida por a.*

O conjunto das classes laterais à direita módulo H é o conjunto $G/H = \{a + H \mid a \in G\}$*.*

Se for definida a operação de multiplicação sobre G de forma que $(G, +, .)$ seja um anel, pode-se definir uma operação de multiplicação sobre G/H de forma que ele também seja um anel. O Teorema 6 apresenta essa operação bem como a condição que H deve obedecer.

Teorema 6 (Teorema 14.2, (3)) *Seja* $(A, +, .)$ *um anel e J um subanel de A. O conjunto* $A/J = \{a + J \mid a \in A\}$ *é um anel sob as operações* $(s + J) + (t + J) = (s + t) + J$ *e* $(s + J).(t + J) = (s.t) + J$ *se, e somente se, J é um ideal.*

Definição 7 (Conjunto gerado) *Seja* $(A, +, .)$ *um anel comutativo e* $a_1, a_2, ..., a_n \in A$*, define-se o seguinte subconjunto de A:* $< a_1, a_2, ..., a_n >= \{x_1.a_1 + x_2.a_2 + ... + x_n.a_n \mid x_1, x_2, ..., x_n \in A\}$*.*

Proposição 8 *Seja* $(A, +, .)$ *um anel comutativo e* $a_1, a_2, ..., a_n \in A$*, o subconjunto* $< a_1, a_2, ..., a_n >$ *é um ideal em A.*

A demonstração da Proposição 8 pode ser encontrada em Domingues e Iezzi (2003) na página 257.

Definição 9 (Corpo) *Seja Q um conjunto não vazio, Q recebe o nome de corpo se as seguintes condições são satisfeitas:*

1. $(Q, +)$ *é um grupo e a adição é comutativa.*
2. $(Q - \{0\}, .)$ *é um grupo e a multiplicação é comutativa, onde* 0 *é o elemento neutro da adição.*
3. *A multiplicação é distributiva em relação à adição.*

Obviamente, percebe-se que todo corpo é um anel. Um exemplo de corpo infinito é $\mathbb{R}$ com as operações usuais.

Há também corpos finitos, indicados por $GF(q)$, em que q é o número de elementos do corpo. Exemplo disso é $GF(2)$, cujo conjunto é $GF(2) = \{0, 1\}$ e têm as seguintes tábuas de operações.

Tabela 1: Tábua da adição em GF(2)

+	0	1
0	0	1
1	1	0

Tabela 2: Tábua da multiplicação em GF(2)

.	0	1
0	0	0
1	0	1

Definição 10 (Extensão de um corpo) *Um corpo F é uma extensão de um corpo Q se as seguintes condições forem verificadas:*

1. $Q \subset F$

2. *As operações de F restritas aos elementos de Q são as operações definidas em Q.*

Na próxima subseção serão definidos alguns conceitos acerca de corpos finitos, utilizados nos códigos cíclicos.

Definição 11 *Seja Q um corpo e $\alpha \in Q$, a ordem de α é o menor inteiro positivo n tal que $\alpha^n = 1$.*

Definição 12 (Elemento primitivo) *Considere o corpo finito $GF(q)$. Um elemento não nulo $\alpha \in GF(q)$ é primitivo se a ordem de α é $q - 1$.*

Definição 13 (Espaço vetorial) *Seja V um conjunto não vazio e Q um corpo. Define-se uma operação de adição sobre V e uma operação de produto de um elemento de Q por um elemento de V. Sejam $u, v \in V$ e $\mu, \lambda \in Q$. Se essas operações satisfazem as seguintes condições, V será chamado de espaço vetorial sobre o corpo Q.*

1. $u + v = v + u$, $\forall u, v \in V$;
2. $u + (v + w) = (u + v) + w$, $\forall u, v, w \in V$;
3. *Existe elemento* $0 \in V$ *tal que* $0 + v = v$;
4. *Para cada* $v \in V$ *existe* $-v \in V$ *tal que* $v + (-v) = 0$;
5. $\mu(\lambda v) = (\mu\lambda)v, \forall \mu, \lambda \in Q, v \in V$;
6. $(\mu + \lambda).u = \mu u + \lambda u, \forall \mu, \lambda \in Q, u \in V$;
7. $\mu(u + v) = \mu u + \mu v, \forall u, v \in V \mu \in Q$;
8. $1u = u, \forall u \in V$.

Definição 14 (Subespaço vetorial) *Seja V um espaço vetorial e U um subconjunto não vazio de V. Se U é um espaço vetorial de V quando as operações de V são restritas a U, então U é chamado de subespaço vetorial de V.*

3.2 Polinômios

No estudo de códigos cíclicos, é necessário construir corpos finitos, como será visto na Seção 4. Neste sentido, na construção desses corpos, faz-se necessário o uso de polinômios para dar sentido a operação de adição sobre corpos finitos.

Definição 15 (Polinômio sobre um anel comutativo) *Seja $(A, +, .)$ um anel comutativo. O conjunto*

$$A[x] = \{a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \mid a_i \in A \text{ e } n \text{ é um inteiro não negativo}\}$$

é chamado de conjunto dos polinômios sobre A na indeterminada x.

Com a adição e multiplicação sobre esse conjunto definidas de maneira usual, semelhante aos polinômios sobre o conjunto dos números reais, $A[x]$ é um anel.

Definição 16 (Polinômio mônico) *Seja Q um corpo. Um polinômio $p(x) \in Q[x]$ é chamado de mônico se o coeficiente do termo de maior grau for $1 \in Q$.*

Definição 17 (Polinômio irredutível) *Seja Q um corpo. Um polinômio $p(x)$ sobre Q é dito irredutível se:*

1. *grau $p(x) \geq 1$*
2. *Sempre que $p(x) = g(x).h(x)$, onde $g, h \in Q[x]$, então ou $g(x)$ é um polinômio constante ou $h(x)$ é um polinômio constante.*

Proposição 18 (Teorema 5.1, (2)) *Todo polinômio irredutível de grau m em $GF(2)$ divide $x^{2^m-1}+1$.*

Definição 19 (Polinômio primitivo) *Um polinômio irredutível $p(x)$ de grau m é dito primitivo se o menor inteiro positivo n para o qual $p(x)$ divide $x^n + 1$ é $n = 2m + 1$.*

Definição 20 (Polinômio minimal) *Considere um elemento $\alpha \in GF(2^m)$, extensão de $GF(2)$. O polinômio $\Phi_\alpha(x) \in GF(2)[x]$ é polinômio minimal de α com respeito a $GF(2)$ se:*

1. *$\Phi_\alpha(\alpha) = 0$*
2. *$\Phi_\alpha(\alpha)$ é o polinômio de menor grau em $GF(2)[x]$ em que o item 1 é verificado.*

Como será visto é importante calcular o polinômio minimal de dado elemento. Para isso utiliza-se o Teorema 21. Na Seção 4 será calculado o polinômio minimal de um elemento $\alpha \in GF(2^m)$.

Teorema 21 (Teorema 2.1.8, (6)) *Seja Φ_α o polinômio minimal de $\alpha \in GF(2^m)$. Seja e o menor inteiro tal que $\alpha^{2^e} = \alpha$, então*

$$\Phi_\alpha = \prod_{i=0}^{e-1} (x + \alpha^{2^i})$$

4 Código Cíclico

As definições a seguir auxiliam no tratamento formal de códigos.

Definição 22 (Conjunto das mensagens) *Seja Q um corpo . O conjunto $M = Q^m$ é um espaço vetorial chamado neste trabalho de espaço das mensagens. Os elementos de M são chamados de mensagens.*

Definição 23 (Código linear) *Seja $U = Q^n$ um espaço vetorial sobre um corpo Q. Um código linear é um subespaço vetorial $C \subset U$. Os elementos de C são chamados de palavras códigos.*

Nas Definições 22 e 23, tem-se que $m < n$, pois o espaço das mensagens M deve ter menos entradas que os espaço das palavras códigos C.

Definição 24 (Distância de Hamming entre dois vetores) *Seja $U = Q^n$ um espaço vetorial. O peso do vetor $u \in U$, $w(u)$, é o número de coordenadas não nulas de u. A distância de Hamming entre dois vetores $v_1, v_2 \in U$, indicada por $d_H(v_1, v_2)$, é $w(v_1 - v_2)$.*

Definição 25 (Distância mínima de Hamming em um código linear) *A distância mínima de Hamming $d(C)$ de um Código Linear C é a **menor** distância de Hamming entre duas palavras códigos distintas, isto é, $d(C) = min\{d_H(c_1, c_2) | c_1, c_2 \in C \, e \, c_1 \neq c_2\}$*

Perceba que $d_H(c_1, c_2) = w(c_1 - c_2)$, logo $d(C)$ é igual ao peso da palavra código de C não nula com o menor peso.

Com essas definições, a seguinte proposição pode ser provada:

Proposição 26 *Seja $d(C) = 2t + 1$ a distância mínima de Hamming de um código linear C. O processo de decodificação pelo método do vizinho mais próximo, visto na Seção 2, pode corrigir no máximo t erros.*

Demonstração. Suponha que na transmissão de mensagens a palavra código $c \in C$ tenha sido enviada e o vetor r tenha sido recebido. Suponha também que ocorreram e erros, com $0 \leq e \leq t$. Assim, $d_H(c, r) \leq t$. Seja $v \in C, v \neq c$. Como $d(C) = 2t + 1$, então $d_H(v, c) \geq 2t + 1$. Assim, $2t + 1 \leq d_H(v, c) \leq d_H(v, r) + d_H(c, r) \leq d_H(v, r) + t$. Logo $2t + 1 \leq d_H(v, r) + t \Leftrightarrow t + 1 \leq d_H(v, r)$. ■

Observe, então que c é a palavra código mais próxima de r. Isso porque toda palavra código diferente de c tem $d_H(v, r) \geq t + 1$. Além disso, se ocorreram mais do que t erros, existirá $v \neq c$ em que $d_H(v, r) < d_H(v, c)$ e, portanto, o processo de decodificação não consideraria a palavra mais próxima.

Nesta seção serão estudados códigos cíclicos em geral. Nas próximas seções, no entanto, será detalhado acerca dos códigos cíclicos BCH binário.

Definição 27 *Seja C um código linear tal que $C \subset Q^n$, em que Q é um corpo qualquer. Esse código linear é chamado de código linear cíclico sobre Q se a seguinte condição é satisfeita: Se $c = (c_0, c_1, ..., c_{n-1}) \in C$, então $c' = (c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C$.*

Pode-se associar cada palavra código $c = (c_0, c_1, ..., c_{n-1})$ com um polinômio $c(x)$ com coeficientes em Q, $c(x) = c_0 + c_1 x + c_2 x^2 + ... + c_{n-1} . x^{n-1}$. O polinômio $c(x)$ é chamado de polinômio código.

Para melhor análise, vale-se definir o conjunto dos polinômios códigos de C.

Definição 28 *Seja C um código cíclico, o conjunto*

$$I(C) = \{c(x) = c_0 + c_1 x + c_2 x^2 + ... + c_{n-1} . x^{n-1} | (c_0, c_1, ..., c_{n-1}) \in C\}$$

é chamado conjunto dos polinômios códigos de C.

Assim, ao invés de se trabalhar com o subespaço vetorial C, trabalha-se de forma equivalente com o conjunto $I(C)$. Portanto, é válido estudar as operações e propriedades sobre $I(C)$.

Como C é um código cíclico se $c, c' \in C$ em que $c = (c_0, c_1, ..., c_{n-1})$ e $c' = (c_{n-1}, c_0, c_1, ..., c_{n-2})$, então $c + c' = (c_0 + c'_0, c_1 + c'_1, ..., c_{n-1} + c'_{n-1}) \in C$. Assim, é preciso que uma operação de adição

seja definida sobre $I(C)$ de forma $c(x) + c'(x) \in I(C)$. A operação de adição usual sobre $Q[x]$ garante esse resultado.

Ademais, $c = (c_0, c_1, ..., c_{n-1}) \in C$, então $c' = (c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C$ é equivalente a dizer que se $c(x) = c_0 + c_1x + c_2x^2 + ... + c_{n-1}.x^{n-1} \in I(C)$, então $c'(x) = c_{n-1} + c_0x + c_1x^2 + c_2x^3 + ... + +c_{n-2}x^{n-1} \in I(C)$.

No entanto, considerando a multiplicação em $Q[x]$, $xc(x) = c_0x + c_1x^2 + c_2x^3 + ... + c_{n-2}x^{n-1} + +c_{n-1}x^n$. Perceba com isso que $c'(x)$ é o resto da divisão de $xc(x)$ por $x^n - 1$.

Isso motiva a utilização da classe de equivalência

$$Q[x]/< x^n - 1 >= \{q(x) + p(x).(x^n - 1), \text{ em que } q(x), p(x) \in Q[x]\}.$$

De acordo com o Teorema 6, $Q[x]/< x^n - 1 >$ é um anel. Além disso, pode-se provar que I(C) é um conjunto de polinômios códigos se, e somente se, é um ideal em $Q[x]/< x^n - 1 >$.

Proposição 29 *Considere um código cíclico linear C sobre o corpo Q cujo conjunto de polinômios associado seja $I(C)$. Com isso, $I(C)$ é um conjunto de polinômios códigos se, e somente se, é um ideal em $Q[x]/< x^n - 1 >$.*

Demonstração. Seja C um código cíclico linear sobre o corpo Q, então o conjunto de polinômios associados $I(C) \in Q[x]/< x^n - 1 >$, uma vez que os elementos de $I(C)$ tem grau menor que n. Pela Definição 4, para provar que $I(C)$ é um ideal basta mostrar que

1. $c(x) - d(x) \in I(C)$ sempre que $c(x), d(x) \in I(C)$;
2. $m(x).c(x) \in I(C)$ sempre que $m(x) \in Q[x]/< x^n - 1 >$ e $c(x) \in I(C)$.

A condição 1 é verificada pois como C é um código linear, a palavra código $c - d \in C$, logo seu polinômio associado $c(x) - d(x) \in I(C)$ pela Definição 28.

Sejam $m(x) = m_0 + m_1x + m_2x^2 + ... + m_{n-1}.x^{n-1} \in Q[x]/< x^n - 1 >\in Q[x]/< x^n - 1 >$ e $c(x) \in I(C)$, então $m(x)c(x) = m_0c(x) + m_1xc(x) + ... + m_{n-1}.x^{n-1}c(x)$.

Por outro lado, $xc(x) \in I(C)$, pois $xc(x)$ corresponde a palavra código $c' = (c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C$ pela Definição 27. É fácil perceber que, utilizando o mesmo argumento, tem-se que $x^ic(x) \in I(C)$ para todo i inteiro positivo.

Dessa forma, $m(x)c(x) = m_0c(x) + m_1xc(x) + ... + m_{n-1}.x^{n-1}c(x) \in I(C)$ pelo argumento anterior e pelo item 1.

Agora, seja $I(C)$ um ideal em $Q[x]/< x^n - 1 >$. Pela Definição 4, tem-se que $c(x) - d(x) \in I$ o que implica que $c - d \in C$. Além disso, por essa mesma definição, $q.c(x) \in I$, o que implica que $qc \in C$. Assim C é um código linear. Ademais, pelo item 2, $x.c(x) \in I(C)$ o que implica que $c' \in C$. Assim, C é um código linear cíclico. ■

É possível provar que o ideal $I(C)$ tem um único polinômio gerador mônico, isto é, uma maneira de se encontrar todos os elementos do código. Isso é provado no Teorema 30 a seguir.

Teorema 30 *Seja $I(C)$ um código cíclico, então*

1. *existe um único polinômio mônico $g(x) \in I(C)$ de grau mínimo;*
2. *I(C) é um ideal gerado pelo polinômio mônico de grau mínimo;*

3. *O polinômio gerador mônico divide* $x^n - 1$.

Demonstração.

1. Obviamente é possível encontrar um polinômio $h(x)$ tal que $h(x) = h_0 + h_1x + h_2x^2 + ... + +h_r.x^r$, em que $h_r \neq 0$ e r seja o menor grau. Para encontrar um polinômio mônico basta tomar $h'(x) = (h_r)^{-1}.h(x)$. Agora, deve-se provar que $h'(x)$ é único. Para isso tome um polinômio $j(x) = j_0 + j_1x + j_2x^2 + ... + j_r.x^r$, $j_r \neq 0$ de grau r. Multiplique-o por j_r^{-1}, obtendo o polinômio $j'(x)$ que é mínimo de grau r. Devemos provar que $j'(x) = h'(x)$. Para isso, lembre-se que $I(C)$ é um ideal, logo $j'(x) - h'(x) \in I(C)$, como esse polinômio não pode ter grau menor ou igual a $r - 1$, já que foi suposto que r era o menor grau encontrado em $I(C)$, então $j'(x) - h'(x) = 0$ e, portanto, $j'(x) = h'(x)$.

2. Seja $g(x)$ o polinômio mônico de grau mínimo em $I(C)$ e $f(x) \in I(C)$. É preciso provar que $f(x) = m(x).g(x) + < x^n - 1 >, m(x) \in Q[x]$. Na verdade basta mostrar que em $Q[x]$, $f(x) = = m(x).g(x)$. Usando o algoritmo da divisão euclidiana, tem-se que $f(x) = m(x).g(x)+r(x)$, em que grau(r) ¡ grau(g). Como $I(C)$ é um ideal, $f(x), g(x) \in I(C)$, então $f(x) - m(x)g(x) = r(x) \in I(C)$. No entanto, por hipótese $g(x)$ é um polinômio de menor grau, logo o grau de $r(x)$ não pode ser menor que o de $g(x)$. Assim $r(x) = 0$.

3. Suponha que o polinômio mônico de grau mínimo $g(x)$ em $I(C)$ não seja um divisor de $x^n - 1$. Então, $x^n - 1 = m(x)g(x) + r(x)$, em que $r(x)$ não é o polinômio nulo e grau(r) ¡ grau(g). Isolando $r(x)$ tem-se que $x^n - 1 - m(x)g(x) = r(x)$. Mas $r(x) = x^n - 1 - m(x)g(x) = -m(x).g(x)$ em $Q[x]/< x^n - 1 >$. Assim, $r(x) \in Q[x]/< x^n - 1 >$. No entanto, pelo algoritmo da divisão euclidiana grau (r)¡ grau (g), um absurdo pois pela hipótese inicial não existe elemento em $I(C)$ de grau menor que o de $g(x)$. Assim, $g(x)$ é um divisor de $x^n - 1$. ■

É evidente que um polinômio gerador mônico gera um único código cíclico. Além disso, pelo item 1. do Teorema 30 um código cíclico não pode ser gerado por dois polinômios mônicos distintos de menor grau $h(x)$ e $g(x)$.

De fato, como $g(x)$ gera o código $I(C)$ e $h(x) \in I(C)$ então $h(x) = g(x).m(x), m(x) \in Q[x]$. Sabe-se que na verdade, $h(x) = g(x)m(x) + p(x).(x^n - 1), p(x) \in Q[x]$, como $g(x)$ divide $x^n - 1$, tem-se que $h(x) = g(x)m(x) + p(x).g(x)t(x)$ para conveniente $t(x) \in Q[x]$. Logo, $h(x) = = g(x)(m(x) + p(x)t(x))$. Assim, pode-se afirmar que o grau de $h(x)$ é maior que o de $g(x)$ ou que $h(x) = m(x)g(x)$, em que $m(x)$ é um polinômio constante. No entanto, ambos os casos são absurdos, o primeiro contraria o fato de $h(x)$ ter grau mínimo em $I(C)$, já o segundo contraria o fato de $h(x)$ ser mônico. Dessa forma, pode-se concluir que $g(x)$ é o único polinômio mônico de grau mínimo gerador de $I(C)$.

Assim, há uma correspondência biunívoca entre os ideais $I(C)$ em $Q[x]/< x^n - 1 >$ e os divisores mônicos de $x^n - 1$.

5 Construção de corpos finitos

Pelo Teorema 30, percebe-se que para construir um código cíclico é necessário encontrar, primeiramente, um divisor mônico de $x^n - 1$.

Encontrar divisores, em $Q[x]$, de um polinômio pode ser trabalhoso e algumas vezes impossível. No entanto, a teoria relacionada aos corpos finitos permite sempre encontrar um divisor de dado polinômio criando extensões de determinados corpos.

Na próxima subseção será explicado como construir uma extensão do corpo $GF(2)$.

5.1 Construindo corpos a partir de $GF(2)$

Para construir uma extensão F de $GF(2)$, considere primeiramente um elemento $\alpha \in F$. Impõe-se que a operação de multiplicação em F tem as seguintes propriedades:

$$0.\alpha^j = \alpha^j.0 = 0 \quad 1.\alpha^j = \alpha^j.1 = \alpha^j \quad \alpha^i.\alpha^j = \alpha^{i+j},$$

com $i, j \in \{1, 2, 3, 4, ...\}$. Logo, $F = \{0, 1, \alpha, \alpha^2, \alpha^3, ..., \alpha^i, ...\}$. A fim de limitar o número de elementos de F, tome $p(x)$ de grau m um polinômio irredutível sobre $GF(2)$. Considere que, em F, $p(\alpha) = 0$. Como $p(x)$ divide $x^{2m-1} + 1$, tem-se que $x^{2m-1} + 1 = p(x).q(x)$, como $q(x) \in GF(2)[x]$. Logo $\alpha^{2m-1} + 1 = p(\alpha).q(\alpha) \iff \alpha^{2m-1} + 1 = 0 \iff \alpha^{2m-1} = 1$. Com isso, $F = \{0, 1, \alpha, \alpha^2, \alpha^3, ..., \alpha^i, ...\} = \{0, 1, \alpha, \alpha^2, ...\alpha^{2^{m-2}}\}$.

Suponha agora uma operação de adição entre dois elementos indicada por $\alpha^i + \alpha^j$, suponha que é válida a distributiva da multiplicação em relação a adição. Portanto, $\alpha^i + \alpha^j = \alpha^i(1 + \alpha^j)$. Para dar significado a $(1 + \alpha^j)$ pode-se associar cada elemento de F com um polinômio com coeficientes em $GF(2)$ de grau menor ou igual a $m - 1$.

$\alpha^l = a_{l0} + a_{l1}\alpha + a_{l2}\alpha^2 + ... + a_{l,m-1}\alpha^{m-1}$. Com isso, $(1 + \alpha^l) = (1 + a_{l0}) + a_{l1}\alpha + a_{l2}\alpha^2 + ... + +a_{l,m-1}\alpha^{m-1}$.

Com as operações definidas dessa maneira, pode-se provar que F é uma extensão de $GF(2)$.

Apesar de $(1 + \alpha^l)$ estar definido é preciso encontrar $\alpha^k \in F$ tal que $(1 + \alpha^l) = \alpha^k$, em que l, k não são necessariamente iguais a i e j. Para isso, utiliza-se que $p(\alpha) = 0$ e $\alpha^{2m-1} + 1 = 0$. Com essas duas informações, monta-se uma Tabela de Operações.

Exemplo 31 *Construa a extensão $F = GF(2^4) = GF(16)$ e sua Tabela de Operações.*
Resolução. Primeiramente, é preciso encontrar um polinômio irredutível sobre $GF(2)$ de grau 4. Perceba que $p(x) = x^4 - x - 1$ é irredutível sobre $GF(2)$. Impondo que um elemento $\alpha \in GF(2^m)$ seja tal que $p(\alpha) = 0$, afirma-se que $\alpha^4 - \alpha - 1 = 0 \iff \alpha^4 = \alpha + 1$. Para ser possível fazer a adição é necessário encontrar os valores de $\alpha^i + 1$ para $1 \leq i$. No entanto, primeiramente é preciso representar cada elemento α^i na forma polinomial.

Por exemplo, $\alpha^5 = \alpha^4.\alpha = (\alpha + 1).\alpha = \alpha^2 + \alpha$, $\alpha^6 = \alpha^5.\alpha = (\alpha^2 + \alpha).\alpha = \alpha^3 + \alpha^2$,
$\alpha^7 = \alpha^6.\alpha = (\alpha^3 + \alpha^2).\alpha = \alpha^4 + \alpha^3 = \alpha + 1 + \alpha^3 = \alpha^3 + \alpha + 1$.

Com esse mesmo raciocínio constrói-se a Tabela 3 a seguir.

Exemplo 32 *Encontre o polinômio minimal de $\alpha^3 \in GF(2^4)$, em que α é o elemento primitivo de $GF(2^4)$.*
Resolução. Pelo Teorema 21 é preciso, primeiramente, encontrar o menor número inteiro e tal que $(\alpha^3)^{2^e} = \alpha^3$. Usando propriedades exponencial, tem-se que $(\alpha^3)^{2^e} = \alpha^3 \iff (\alpha^{2^e})^3 = \alpha^3 \iff (\alpha^{2^e}) = \alpha$. Essa última igualdade ocorre quando $e = 4$. Agora, basta fazer o produto

$$\Phi_{\alpha^3} = \prod_{i=0}^{3}(x + (\alpha^3)^{2^i}) = (x + (\alpha^3)^{2^0}).(x + (\alpha^3)^{2^1}).(x + (\alpha^3)^{2^2}).(x + (\alpha^3)^{2^3}) =$$

$$= (x + (\alpha^3)^1).(x + (\alpha^3)^2).(x + (\alpha^3)^4).(x + (\alpha^3)^8).$$

Tabela 3: Forma exponencial e polinomial de GF (16)

Forma exponencial	Forma polinomial
α	α
α^2	α^2
α^3	α^3
α^4	$\alpha+1$
α^5	$\alpha^2+\alpha$
α^6	$\alpha^3+\alpha^2$
α^7	$\alpha^3+\alpha+1$
α^8	α^2+1
α^9	$\alpha^3+\alpha$
α^{10}	$\alpha^2+\alpha+1$
α^{11}	$\alpha^3+\alpha^2+\alpha$
α^{12}	$\alpha^3+\alpha^2+\alpha+1$
α^{13}	$\alpha^3+\alpha^2+1$
α^{14}	α^3+1
α^{15}	1

Tabela 4: Forma exponencial e valores de α^i+1 em GF (16)

α^i+1	Forma exponencial
$\alpha+1$	α^4
α^2+1	α^8
α^3+1	α^{14}
α^4+1	α
α^5+1	α^{10}
α^6+1	α^{13}
α^7+1	α^9
α^8+1	α^2
α^9+1	α^7
$\alpha^{10}+1$	α^5
$\alpha^{11}+1$	α^{12}
$\alpha^{12}+1$	α^{11}
$\alpha^{13}+1$	α^6
$\alpha^{14}+1$	α^3
$\alpha^{15}+1$	0

Usando $\alpha^{16}=\alpha$ e a Tabela 3 , tem-se

$$\Phi_{\alpha^3}=x^4+x^3+x^2+x+1.$$

5.2 As raízes de x^n-1

O seguinte Teorema aliado a subseção anterior, permitem que códigos cíclicos sejam construídos.

Teorema 33 (Teorema B.1, (5)) *Os 2^m-1 elementos não nulos de $GF(2^m)$ formam todas as raízes de $x^{2^m-1}+1$ em $GF(2^m)[x]$.*

Assim, a extensão de $GF(2)$, que é $GF(2^m)$, é o menor corpo em que x^n+1, com $n=2^m-1$, será fatorado como produto de fatores lineares.

Com essa fatoração, o processo de encontrar um polinômio gerador é simplificado. De fato, para encontrar um polinômio gerador g(x) é preciso multiplicar os fatores de maneira que g(x) tenha coeficientes em GF(2).

Nos códigos BCH binários, os polinômios mínimos e o gerador são encontrados e definidos de maneira a se ter a distância mínima de Hamming do código definida. Assim, a partir da distância mínima que se deseja para o código, define-se o polinômio gerador.

6 Códigos BCH binários

Para saber a quantidade de erros que um código linear cíclico C consegue detectar e corrigir

é necessário saber a distância mínima de Hamming deste código C. Assim, como dito esse trabalho exibe um tipo de código cíclico, os códigos BCH binários.

O Teorema 34 permite a posterior definição de código BCH binário.

Teorema 34 (Teorema 4.3.3, (1)) *Considere o corpo $GF(2)$, n um número natural maior do que 1 e $GF(2^m)$ uma extensão de $GF(2)$, na qual $x^n - 1$ pode ser fatorado em fatores lineares. Sejam α o elemento primitivo de $GF(2^m)$, $\Phi_{\alpha^i}(x)$ o polinômio mínimo de α^i e C um código cíclico com seguinte polinômio gerador*

$$g(x) = mmc\{\Phi_\alpha(x), \Phi_{\alpha^2}(x), ..., \Phi_{\alpha^{\delta-1}}(x)\}$$

em que $\delta \leq n$. Assim, a distância mínima d de Hamming de C é $d \geq \delta$ e sua dimensão k é $k \geq n - m(\delta - 1)$, com m a dimensão do espaço vetorial $GF(2^m)$ sobre o corpo $GF(2)$.

Pelo Teorema 34, pode-se definir um código cíclico com n coordenadas e que corrige t erros. Além disso, o número de dígitos k das mensagens é dado pela seguinte inequação $k \geq n - m.t$, em que m satisfaz $x^{2m} - 1 = n$.

Definição 35 *Seja α um elemento primitivo em $GF(2^m)$ e seja $\Phi_{\alpha^i}(x)$ o polinômio minimal de α^i. Então, o código BCH cuja distância é $d = 2t + 1$ é um código cíclico gerado pelo polinômio $g(x) \in GF(2)[x]$ dado por*

$$g(x) = mmc\{\Phi_\alpha(x), \Phi_{\alpha^2}(x), ..., \Phi_{\alpha^{2t}}(x)\}.$$

Exemplo 36 *Suponha que é desejado construir um código cíclico que corrige $t = 2$ erros e que cada palavra código tenha $n = 15$ dígitos. Dessa maneira, pela Definição 35 esse código terá como polinômio gerador:*

$$g(x) = mmc\{\Phi_\alpha(x), \Phi_{\alpha^2}(x), ..., \Phi_{\alpha^{2t}}(x)\} = mmc\{\Phi_\alpha(x), \Phi_{\alpha^2}(x), \Phi_{\alpha^3}(x), \Phi_{\alpha^4}(x)\}.$$

Usando o Teorema 21, encontra-se os polinômios minimais de maneira similar ao feito no Exemplo 32.

$\Phi_{\alpha^1}(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8)$;
$\Phi_{\alpha^2}(x) = (x+\alpha^2)(x+(\alpha^2)^2)(x+(\alpha^2)^4)(x+(\alpha^2)^8) = (x+\alpha^2)(x+\alpha^4)(x+\alpha^8)(x+\alpha) = \Phi_{\alpha^1}(x)$;
$\Phi_{\alpha^3}(x) = x^4 + x^3 + x^2 + x + 1$, *como encontrado no Exemplo 32;*
$\Phi_{\alpha^4}(x) = (x+\alpha^4)(x+(\alpha^4)^2)(x+(\alpha^4)^4)(x+(\alpha^4)^8) = (x+\alpha^4)(x+\alpha^8)(x+\alpha)(x+\alpha^2) = \Phi_{\alpha^1}(x)$.

Além disso, tem-se que $(x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8) = x^4+x+1$, usando a Tabela de Operações.
Assim, $g(x) = (x^4 + x + 1).(x^4 + x^3 + x^2 + x + 1) = x^8 + x^7 + x^6 + x^4 + 1$.
Com isso, o número de dígitos das mensagens será $15 - 8 = 7$.
Portanto, o polinômio $g(x) = (x^4 + x + 1).(x^4 + x^3 + x^2 + x + 1) = x^8 + x^7 + x^6 + x^4 + 1$ gera o código cíclico com 15 dígitos e que codifica mensagens de 7 dígitos, o qual será denotado por $C(15, 7)$.

7 Codificação e decodificação

A codificação das mensagens em palavras códigos pode ser feita de maneira similar aos códigos de Hamming ou usando o polinômio gerador mônico. Já a decodificação também consiste em, primeiramente, multiplicar a palavra recebida pela matriz de controle e, juntamente com a dimensão mínima do código, encontrar o erro.

7.1 Decodificação

Seja $r(x)$ um polinômio recebido, pelo Algoritmo da Divisão Euclidiana $r(x) = m(x).g(x) + +s(x)$ em que $g(x)$ é o polinômio mônico que gera $I(C)$ e $m(x) \in GF(2)[x]/< x^n - 1 >$. Pelo Teorema 30, $r(x) \in I(C) \iff s(x) = 0$.

Pela Definição 35, α^i para $1 \leq i \leq 2t$ é uma raiz de $g(x)$ em $GF(2^m)[x]$, em que t é o número de erros que o código cíclico BCH corrige. Logo, $r(\alpha^i) = m(\alpha^i).g(\alpha^i) + s(\alpha^i) = s(\alpha^i)$.

Dessa forma, $g(x) = (x-\alpha^i).p_i(x)$ com $p_i(x) \in GF(2^m)[x]$. Como $c(x) = m(x).g(x)$, $\forall\, c(x) \in I(C)$, então $c(x) = m(x)(x - \alpha^i).p_i(x)$. Assim, $c(x) \in I(C)$ se, e somente se, α^i divide $c(x)$, para $1 \leq i \leq 2t$.

Seja $r(x) = r_0 + r_1x + r_2x^2 + ... + r_{n-1}.x^{n-1}$ o polinômio recebido, então $r(x) \in I(C) \iff r(\alpha^i) = r_0 + r_1\alpha^i + r_2(\alpha^i)^2 + ... + r_{n-1}.(\alpha^i)^{n-1} = 0$.

Como, $r(x) = c(x) + e(x)$, em que $c(x) \in I(C)$ e $e(x)$ é o polinômio erro, tem-se que $s(\alpha^i) = = r(\alpha^i) = c(\alpha^i) + e(\alpha^i) = e(\alpha^i)$.

Suponha que ocorreram $b < t$ erros nas posições $j_1, j_2, ..., j_b$ em uma palavra código enviada. Assim, $e(x) = x^{j_1} + x^{j_2} + x^{j_3} + ... + x^{j_b}$. Dessa forma, $e(\alpha^i) = (\alpha^i)^{j_1} + (\alpha^i)^{j_2} + (\alpha^i)^{j_3} + ... + (\alpha^i)^{j_b}$, para $1 \leq i \leq 2t$. Dessa maneira, para encontrar o erro e(x) basta resolver esse Sistema com 2t equações, encontrando $\alpha^{j_1}, \alpha^{j_2}, \alpha^{j_3}, ..., \alpha^{j_b}$.

Na próxima seção será mostrado um exemplo particular da resolução de uma decodificação.

7.2 Exemplo de decodificação

Considere o código cíclico C(15,7), BCH binário, do Exemplo 36, cujo polinômio gerador é $g(x) = x^8 + x^7 + x^6 + x^4 + 1$ e que corrige no máximo dois erros. Será mostrado um processo de decodificação de um vetor recebido.

Suponha que se tenha recebido o vetor $r = [1\,1\,0\,1\,1\,1\,1\,0\,1\,0\,0\,0\,1\,1\,0\,0]$.

Passando para a forma polinomial, tem-se $r(x) = 1 + x + x^3 + x^4 + x^5 + x^6 + x^8 + x^{12} + x^{13}$.

Seja α o elemento primitivo de $GF(2)$, pelo resultado anterior, tem-se que o erro $e(x) = 0 \iff e(\alpha^i) = r(\alpha^i) = 0$.

Após fazer cálculos e usar a Tabela de operações, tem-se que $r(\alpha) = \alpha^8; r(\alpha^2) = \alpha; r(\alpha^3) = \alpha^{14}; r(\alpha^4) = \alpha^2$.

Como esse código corrige dois erros, supõem-se que os erros ocorreram nas posições j_1 e j_2.

$$\begin{cases} \alpha^8 = \alpha^{j_1} + \alpha^{j_2} \\ \alpha = (\alpha^{j_1})^2 + (\alpha^{j_2})^2 \\ \alpha^{14} = (\alpha^{j_1})^3 + (\alpha^{j_2})^3 \\ \alpha^2 = (\alpha^{j_1})^4 + (\alpha^{j_2})^4 \end{cases} \tag{1}$$

É preciso encontrar uma solução para o Sistema (1). Perceba que se $\alpha^{j_1} = \alpha^{j_2}$, então $\alpha^{j_1} + \alpha^{j_2} = = \alpha^{j_1} + \alpha^{j_1} = 0$. Portanto, $\alpha^{j_1} \neq \alpha^{j_2}$.

Para resolver esse sistema pode-se encontrar o polinômio localizador, como apresentado por Souza (2012).

No entanto, como o Sistema (1) é pequeno é possível resolvê-lo por inspeção utilizando a Tabela de operações. Após algumas análises percebe-se que a^{10} e α satisfazem o Sistema (1).

Dessa maneira, conclui-se que os erros ocorreram nas posições 2 e 11, logo $\vec{e} = [0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0]$ e a palavra código enviada é $\vec{r} + \vec{e} = \vec{c} = [1\,0\,0\,1\,1\,1\,1\,0\,1\,0\,1\,0\,1\,1\,0\,0]$.

Para decodificar o vetor $\vec{c}$ basta fazer uma divisão de polinômios em $GF(2)[x]$.

De fato, como $c(x) = m(x).g(x)$, em que $m(x)$ é a mensagem codificada e $g(x)$ o polinômio gerador. Pode-se obter que $\frac{c(x)}{g(x)} = x^5+x^3+1$. Portanto, o vetor mensagem enviado foi [1 0 0 1 0 1 0].

8 Conclusões

Com esse trabalho foi possível exibir uma aplicação da Álgebra Abstrata, em particular o estudo de Corpos Finitos. Isso porque com o intuito de apresentar como os códigos cíclicos são definidos, foi necessário o estudo de polinômios e corpos finitos, por exemplo. De fato, para encontrar um divisor mônico de x^n-1 e, consequentemente, criar um código cíclico, foi necessário construir um corpo finito a partir do corpo GF(2). Além disso, o trabalho exibiu um caso particular dos códigos cíclicos, o código BCH binário. Neste sentido, foi mostrado um exemplo de decodificação de uma mensagem recebida. Como já discutido, códigos cíclicos são extremamente utilizados na transmissão de dados. É importante, assim, entender a teoria matemática que apoia o desenvolvimento desses códigos, a fim de propor códigos mais eficientes e seguros.

9 Bibliografia

[1] ADAMS, S. S. **Introduction to algebraic coding theory**. 2. ed. [Needham]: Cornell University. 2008.

[2] BIAZZI, R. N. **Polinômios irredutíveis:** critérios e aplicações. 2014. 74 f. Dissertação (Mestrado Profissional em Matemática) - Instituto de Geociências e Ciências Exatas, Universidade Estadual Paulista "Júlio de Mesquita Filho", Rio Claro, 2014.

[3] CASTIÑEIRA MOREIRA, J.; FARREL, P. G. **Essentials of error-control coding**. West Sussex: John Wiley & Sons, c2006. *E-book*.

[4] GALLIAN, J. A. **Contemporary abstract algebra**. 7th ed. Belmont: Brooks/Cole Cengage Learning. 2010.

[5] DOMINGUES, H. H.; IEZZI, G. **Álgebra moderna**. 4. ed. São Paulo: Atual, 2003.

[6] OLIVEIRA, A. N. **Códigos BCH aplicados no processo de análise de fenômenos mutacionais**. 2020. 87 f. Dissertação (Mestrado em Estatística Aplicada e Biometria) - Universidade Federal de Alfenas, Alfenas, 2020.

[7] SHANNON, C. E. The mathematical theory of communication. **The Bell System Technical Journal**, v. 27, n. 4, p. 623-656, out. 1948.

[8] SOUZA, T. A. **Álgebra de corpos finitos aplicada à teoria da codificação:** estudo do codificador BCH. 2012. 80 f. Trabalho de Conclusão de Curso (Bacharelado em Matemática) - Universidade Federal da Paraíba, João Pessoa, 2012.