UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
Pró-Reitoria de Pesquisa e Pós-Graduação
Departamento de Matemática Pura e Aplicada - CCENS

RELATÓRIO DE INICIAÇÃO CIENTÍFICA

Códigos de grupo: construções, exemplos e análise via GAP

Discente: *Gabriel de Souza Cruz*
Orientador: *Prof. Dr. Victor do Nascimento Martins (DMPA - UFES)*

SETEMBRO/2024

SUMÁRIO

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
Pró-Reitoria de Pesquisa e Pós-Graduação
Departamento de Matemática Pura e Aplicada - CCENS

RESUMO

CÓDIGOS DE GRUPO: CONSTRUÇÕES, EXEMPLOS E ANÁLISE VIA GAP

Este trabalho possui o intuito de apresentar elementos primordiais da teoria de códigos de grupo, trazendo as principais definições, teoremas e exemplos, trabalhando diversos elementos teóricos, de cunho algébrico, que fundamentam tal teoria. No escopo deste trabalho abordamos, de forma incisiva, os códigos corretores de erros, dentre eles, temos os códigos lineares, duais, cíclicos, dentre outros. Por fim, estudamos teorias de álgebras de grupo, que fundamentam os aspectos dos códigos de grupo, discutindo a possibilidade de utilização do software algébrico GAP como um agente contribuinte para o estudo de tal teoria algébrica aplicada.

Palavras-chave: Códigos Corretores de Erros; Álgebras de Grupo; Códigos de Grupo; GAP.

INTRODUÇÃO

No aspecto geral, as teorias de álgebra abstrata foram fundamentadas por expoentes como P. Ruffini, L. Euler, C.F. Gauss, dentre outros. Em meados do século XIX referenciais como A. Cauchy, N.A. Abel, E. Galois desenvolveram diversos resultados importantes relacionados as teorias de diversos objetos algébricos matemáticos, trabalhando avanços em pesquisas nas estruturas de grupo e de anéis. No século XX começou-se a firmar uma área de estudo na álgebra, denominada como teoria de anéis de grupos, sendo alicerçada em estruturas algébricas canônicas, que são as de grupo e de anéis, onde por mais que A. Cayley tenha trazido o primeiro anel de grupo em seus trabalhos, somente no século XX tal teoria começou a ser explorada e serem obtidos resultados da natureza dessa álgebra. Temos que um anel de grupo é uma estrutura híbrida, definida como um módulo livremente gerado sobre um grupo com coeficientes em um anel associativo com unidade.

Diante do avanço das teorias algébricas, e em particular, da teoria de anéis de grupo, uma nova teoria matemática aplicada começou a ser desenvolvida por C.E. Shannon, do laboratório Bell, denominada por teoria dos códigos corretores de erros, que é configurada como uma teoria matemática de comunicação, sendo exposta ao mundo em 1948, através da publicação de seu trabalho.

Os códigos corretores de erros estão presentes em diversos aspectos de nosso cotidiano, pois os mesmos estão presentes em atividades como a de assistir um programa de televisão, ouvir uma música, enviar mensagens digitais, conectar-se a internet. Um exemplo característico de determinados códigos é o de números com códigos verificadores, que são os números vinculados as contas bancárias, CPF. Em tais são fornecidos alguns dígitos adicionais que permitem detectar erros.

Em linhas gerais, o estudo de tal teoria está ligada a aspectos de transmissão/armazenamento

de mensagens eletrônicas, onde tal mensagem será transformada em sinal digital, através de uma codificação para ser transmitida ou armazenada. Entretanto, nesse processo a mensagem pode receber corrompimento ou adulteração, em prol de reduzir tal interferência, são desenvolvidos códigos e esses são aplicados nas palavras a serem enviadas, de modo que, mesmo sofrendo interferências no processo de envio das mensagens, tais códigos estão munidos (algebricamente) com ferramentas que permitem com que as mensagens que chegaram ao destinatário possam ser as mesmas que, de fato, foram enviadas, ou seja, os códigos consigam corrigir os erros oriundos da transmissão para que haja decodificação das palavras e essas estejam certas.

Dividimos este trabalho em três capítulos. No primeiro apresentamos os fatos básicos da teoria de códigos corretores de erros. Especialmente as definições e resultados de natureza algébrica. O segundo capítulo é dedicado ao estudo da estrutura de anéis de grupo. Para isso, foi necessário apresentar um breve resumo da teoria de módulos. Por fim, nosso último capítulo é dedicado ao objetivo central deste trabalho que é a apresentação dos códigos de grupo.

CAPÍTULO 1

CÓDIGOS CORRETORES DE ERROS COM ESTRUTURA CÍCLICA

Os códigos corretores de erros são fundamentais na teoria da informação e nas comunicações digitais, garantindo a confiabilidade da transmissão de dados em canais ruidosos. Entre as várias classes de códigos, os códigos com estrutura cíclica destacam-se por suas propriedades algébricas e eficiência computacional. Neste capítulo, exploraremos inicialmente os códigos lineares, com foco especial nos códigos cíclicos, que formam uma subclasse importante e amplamente aplicada. Discutiremos também a métrica de Hamming, que mede a distância entre palavras de código, e os códigos duais, que permitem a análise da estrutura algébrica dos códigos.

Como literatura básica e introdutória para estudo da teoria indicamos [4]. Além disso, conceitos algébricos serão necessários para uma boa compreensão do texto, então sugerimos uma breve revisão das estruturas algébricas básicas apresentadas em [3].

1.1 Introdução

Um código corretor de erro é uma maneira organizada de se acrescentar um dado para cada informação que será transmitida ou recebida, de modo que permita detectar e corrigir erros no processo de recuperação da informação. Traremos um exemplo para tornar mais palpável e consolidada essa ideia.

Exemplo 1.1 *Suponhamos que exista um robô que se desloca sobre um tabuleiro quadriculado trididmensional e por isso abaixa e levanta cada braço separadamente. Note que o robô pode movimentar-se de oito maneiras distintas, sendo elas: Leste, Oeste, Norte, Sul,*

Direito-cima, Direito-baixo, Esquerdo-cima, Esquerdo-baixo, onde as palavras Direito e esquerdo representam os braços do robô.

Podemos descrever uma codificação para representar tais movimentações possíveis, sendo ela denominada como ***código fonte****, onde tal código será descrito através de coordenadas* $\{0,1\} \times \{0,1\} \times \{0,1\}$

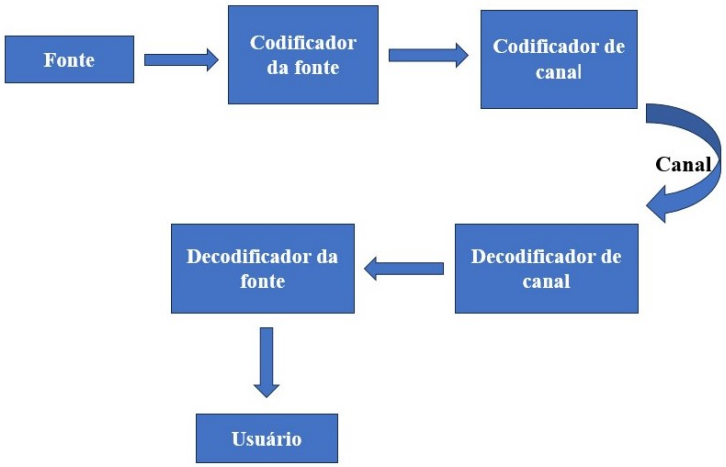
$$\begin{gathered} \textit{Leste} \mapsto 000 \\ \textit{Oeste} \mapsto 010 \\ \textit{Norte} \mapsto 100 \\ \textit{Sul} \mapsto 110 \\ \textit{Direito-cima} \mapsto 101 \\ \textit{Direito-baixo} \mapsto 001 \\ \textit{esquerdo-cima} \mapsto 011 \\ \textit{Esquerdo-baixo} \mapsto 111 \end{gathered}$$

Os códigos corretores de erros visam determinar maneiras de corrigir eventuais quebras ou interferências que possam acometer a mensagem enviada. Com intuito de minimizar tal perspectiva são introduzidas redundâncias, que é uma maneira de recodificar as mensagens e que permita a correção de erros com maior confiabilidade através do algoritmo. Esse novo código gerado a partir do código fonte aliado as redundâncias recebe o nome de ***código de canal****, denotaremos tal código por* P*, onde* $P \subset A^7$*, com* $A = \{0,1\}$*.*

$$\begin{gathered} \textit{Leste} \mapsto 0000000 \\ \textit{Oeste} \mapsto 0101010 \\ \textit{Norte} \mapsto 1001001 \\ \textit{Sul} \mapsto 1101101 \\ \textit{Direito-cima} \mapsto 1010101 \\ \textit{Direito-baixo} \mapsto 0011111 \\ \textit{esquerdo-cima} \mapsto 0110110 \\ \textit{Esquerdo-baixo} \mapsto 1111011 \end{gathered}$$

Note que se ao enviarmos a palavra ***0101010*** *houvesse alguma danificação na mensagem e o receptor obtivesse a palavra* ***0101011*** *teríamos que comparar as palavras que pertencem ao código com a recebida, nesse processo é possível detectar o erro e, sequencialmente, podemos corrigí-lo, averiguando que a palavra* ***0101010*** *é, precisamente, a mensagem enviada.*

Esse processo de correção e organização de códigos pode ser esquematizado da seguinte maneira:



Observação 1.1 *O estudo relacionado a códigos corretores de erros no escopo do trabalho está voltado na transformação do código fonte em código canal e também na detecção, correção de erros e decodificação de mensagens recebidas do código canal para o código fonte.*

Observação 1.2 *o estudo sobre códigos corretores contidos no presente trabalho estarão fundamentados nos* ***canais simétricos****, que satisfazem duas propriedades*

i) Todos os símbolos transmitidos possuem a mnesma probabilidade (pequena) de serem recebidos errados;

ii) Se um símbolo é recebido errado, a probabilidade de ser qualquer um dos outros é a mesma.

1.1.1 Métrica de Hamming

Primeiramente, para construirmos um código corretor de erros escolhe-se um conjunto finito A que é denominado **alfabeto** e o número de elementos de A, que é representado por $|A|$ será denotado como q.

Um **código corretor de erros** é um subconjunto próprio qualquer de A^n para algum natural n.

Agora abordaremos uma forma organizada de medir a distância entre os elementos de A^n, que chamaremos de palavras.

Definição 1.1 (Distância de Hamming) *Dados dois elementos $u, v \in A^n$, a Distância de Hamming entre u e v é definida como*

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

Um fato importante a ser destacado é que a Distância de Hamming satisfazendo as três propriedades listadas na proposição abaixo a caracterizam como uma métrica, sendo denominada, portanto, como **Métrica de Hamming**.

Proposição 1.1 *Dados u, v , y* $\in A^n$*, então*

1) ***Positividade****:* $d(u, v) \geq 0$ *e temos* $d(u, v) = 0$ *se e só se* $u = v$*;*

2) ***Simetria****:* $d(u,v) = d(v, u)$*;*

3) ***Desigualdade Triangular****:* $d(u, v) \leq d(u, y) + d(y, v)$*.*

Demonstração: Presente em [4]. ∎

Traremos agora duas definições fundamentais para estudo de códigos corretores de erros, que são as de **disco** e **esfera**.

Definição 1.2 *Dado um elemento* $a \in A^n$ *e um número* $t \geq 0$*, definimos o* ***disco*** *e a* ***esfera*** *de centro em a e raio t como sendo, respectivamente, os conjuntos*

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

Vamos apresentar a maneira de se exprimir a cardinalidade do disco e da esfera, que são conjuntos finitos. Para isso enunciamos a seguinte observação:

Observação 1.3 *Usaremos a notação usual acerca das combinatórias*

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

e denotaremos por $|B|$ *o número de elementos do conjunto* B*.*

Lema 1.1 *Para todo* $a \in A^n$ *e todo número natural* $r > 0$*, temos que*

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

Demonstração: Primeiramente, observemos que

$$|S(a, r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i;$$

e para cada coordenada da palavra c existem $(q-1)$ elementos distintos do alfabeto A, e a potência i é justificada pelo número de coodenadas da palavra que podem ser variadas. Observe que como as palavras pertencem a A^n então as i's entradas distintas podem ocorrer nas n's coordenadas da palavra, ou seja,configurando-se uma combinação entre tais fatores.

Note que

$$S(a,i) \cap S(a,j) = \varnothing \text{ se } i \neq j;$$
$$\text{e}$$
$$\bigcup S(a,i) = D(a,r), \text{ onde } 0 \leq i \leq r;$$

e daí segue de imediato o que queríamos mostrar. ■

Observação 1.4 *A cardinalidade de $D(a,c)$ depende apenas de n, q, r.*

Definição 1.3 *Seja C um código. A* ***distância mínima de C*** *é o número*

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

Exemplo 1.2 *Ao analisarmos código canal do robô (presente no Exemplo 1.1) temos que, comparando as palavras duas a duas, obteremos $d = 3$.*

Definição 1.4 *Dado um código C com distância mínima d, definimos o número*

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

onde $[t]$ representa a parte inteira de um número real t.

Lema 1.2 *Seja C um código com distância mínima d. Se c e c' são palavras distintas de C, então*

$$D(c,k) \cap D(c',k) = \varnothing.$$

Demonstração: Presente em [4]. ■

O próximo teorema justificará a importância de encontrarmos a distância mínima de um código.

Teorema 1.1 *Seja C um código com distância mínima d. Então C pode detectar até $d-1$ erros e corrigir $k = \left[\frac{d-1}{2}\right]$ erros.*

Demonstração: Se ao transmitirmos uma palavra c do código cometemos t erros com $t \leq k$, recebendo a palavra r, então $d(r, c) = t \leq k$, e pelo Lema 1.2, a distância de r para qualquer outra palavra do código é maior do que k. Isso determina c univocamente a partir de r, ou seja, corrigi-se a palavra recebida e substituindo-a por c.

Por outro lado, dada uma palavra do código, podemos nela introduzir até $d - 1$ erros sem encontrar outra palavra do código, e assim, a detecção do erro será possível. ■

Definição 1.5 *Seja $C \subset A^n$ um código com distância mínima d e seja $k = \left[\frac{d-1}{2}\right]$. o código será dito* ***perfeito*** *se*

$$\bigcup_{c \in C} D(c, k) = A^n$$

Um código C sobre um alfabeto A possui três parâmetros fundamentais $[n, m, d]$, que são, respectivamente, n como o seu comprimento (o número n corresponde ao espaço ambiente A^n onde C se encontra, M que representa o número de elementos e d a sua distância mínima. Os códigos interessantes de serem estudados são os que possuem M e d grandes, em relação a n, mas nem sempre há códigos que envolvam os três parâmetros, pois há uma interdependência complexa entre tais valores.

1.2 Códigos lineares

Consideremos $\mathbf{K}$ um corpo finito com q elementos determinado cmo alfabeto. Temos então para cada número natural n um $\mathbf{K}$-espaço vetorial $\mathbf{K^n}$ de dimensão n.

Definição 1.6 *Um código $C \subset \mathbf{K^n}$ será chamado de* ***código linear*** *se for um subespaço vetorial próprio de $\mathbf{K^n}$*

Observação 1.5 *Todo código linear é por definição um espaço vetorial de dimensão finita.*

Seja k a dimensão do código C e seja $v_1, v_2, ..., v_k$ uma de suas bases, portanto, qualquer elemento de C é descrito de forma única, tal como:

$$\lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_k v_k;$$

Onde $\lambda_i, i = 1, 2, ..., k$, são elementos do corpo $\mathbf{K}$. Segue que

$$M = |C| = q^k,$$

e também

$$dim_k C = k = log_q q^k = log_q M$$

Definição 1.7 *Dado $x \in \mathbf{K^n}$ define-se o* ***peso*** *de x como sendo o número inteiro*

$$w(x) := |\{i; x_i \neq 0\}|$$

Observe que

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

onde d representa a métrica de Hamming.

Definição 1.8 *O* ***peso*** *de um código linear C é o inteiro*

$$w(C) := min\{w(x); x \in C - \{0\}\}.$$

Proposição 1.2 *Seja $C \subset \mathbf{K^n}$ um código linear com distância mínima d. Temos que*

i) $\forall x, y \in \boldsymbol{K}^n$, $d(x, y) = w(x - y)$;

ii) $d = w(C)$.

Demonstração:

i) Segue de imediato das definições da métrica de Hamming e da de peso de um código;

ii) segfue do fato de que para todo par de elementos x, y em C tais que $x \neq y$ tem-se $x - y = z \in C - \{0\}$ e $d(x - y) = w(z)$.

■

Observe que a proposição acima nos mostra que, em códigos lineares com M elementos podemos calcular a distância mínima d a partir de "$M - 1$" cálculos de distâncias.

Pelo item ii) da proposição anterior a distância mínima de um código linear C será denominada também como **peso do código C**.

Utilizaremos resultados de álgebra linear para descrever duas formas de determinar subespaços vetoriais C de um espaço vetorial $\mathbf{K}^n$, uma como imagem e outra como núcleo de transformações lineares.

Primeiramente, descreveremos como obter a representação de C como Imagem. Tomando uma base $v_1, v_2, ..., v_k$ de C e considerando a aplicação linear abaixo

$$T: \quad \mathbf{K^k} \quad \rightarrow \quad \mathbf{K^n}$$

$$x = (x_1, x_2, ..., x_n) \mapsto x_1v_1 + x_2v_2 + ... + x_nv_n$$

Temos que T é uma transformação linear injetora, tal que a imagem de T é C.

Essa é a forma paramétrica do subespaço C, pois oe elementos de C são parametrizados pelos elementos x de $\mathbf{K}^n$ através da transformação T. Entretanto é difícil decidir se um dado elemento v de $\mathbf{K}^n$ pertence ou não à C, pois, para tal é necessário resolver um sistema que possui n equações nas k incógnitas $x_1, ..., x_k$ abaixo

$$x_1v_1 + x_2v_2 + ... + x_kv_k = v$$

E computacionalmente tal solução possui, de forma geral, um custo elevado. Contrapondo a tal fato iremos descrever um código C através do núcleo de uma transformação linear. Tome um subespaço $C^{'}$ de $\mathbf{K}^n$, complementar de C, ou seja,

$$C \bigoplus C' = \mathbf{K}^n$$

Considere a aplicação linear

$$H : C \bigoplus C' \rightarrow \mathbf{K^{n-k}}$$

$$u \oplus v \quad \mapsto \quad v$$

tal que o núcleo é precisamente C. Computacionalmente é mais simples verificar se um elemento $v \in \mathbf{K^n}$ pertence ou não á C, para isso, basta verificar se $H(v)$ é ou não o vetor nulo de $\mathbf{K^{n-k}}$, que tem um custo pequeno.

Exemplo 1.3 *Considere o corpo finito com três elementos* $\mathbf{F_3} = \{0, 1, 2\}$*, e seja* $C \subset \mathbf{F_3^4}$ *o código gerado pelos vetores* $v_1 = 1011$ *e* $v_2 = 0112$.

Esse código possui 9 elementos ($q^k = 3^2$)*, pois tem dimensão 2 sobre um corpo de três elementos. Uma representação paramétrica de C é dada por*

$$x_1v_1 + x_2v_2$$

ao variar x_1, x_2 *em* $\mathbf{F_3}$*. O código C pode ser representado como núcleo da transformação linear*

$$\begin{array}{ccccc} H : & \mathbf{F_3^4} & \rightarrow & \mathbf{F_3^2} \\ & (x_1, ..., x_4) & \mapsto & (2x_1 + 2x_2 + x_3, 2x_1 + x_2 + x_4) \end{array}$$

Definição 1.9 *Seja* $\mathbf{K}$ *um corpo finito. Dois códigos lineares* C *e* $C^{'}$ *são* ***linearmente equivalentes*** *se existir uma isometria linear* $T : K^n \rightarrow \mathbf{K^n}$ *tal que* $T(C) = C^{'}$

A partir de alguns resultados de àlgebra linear descritos em [4] temos que dois códigos lineares C e $C^{'}$ em $\mathbf{K}^n$ são linearmente equivalentes se e só se existem uma permutação π de $\{1, 2, ..., n\}$ e elementos $c_1, c_2, ..., c_n$ de $\mathbf{K} - \{0\}$ tais que

$$C^{'} = \{(c_1x_{\pi(1)}, ..., c_nx_{\pi(n)}); (x_1, ..., x_n \in C)\}$$

Do fato mencionado anteriormente discorre uma segunda definição acerca de códigos lineares linearmente equivalentes

Definição 1.10 *Dois códigos lineares são linearmente equivalentes se e só se cada um deles pode ser obtido do outro mediante uma sequência de operações do tipo:*

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

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

1.2.1 Matriz geradora de um código

Sejam $\mathbf{K}$ um corpo finito com q elementose $C \subset \mathbf{K}^n$ um código linear. Denominaremos como *parâmetro do código linear* C a terna de inteiros (n, k, d), onde k é a dimensão de C sobre o corpo $\mathbf{K}$ e d representa a distância minima de C. Observe que o número de elementos M de C é igaual a q^k.

Seja $\mathbf{B} = \{v_1, ..., v_k\}$ uma base ordenada de C e considere a matriz G, cujas linhas são os vetores $v_i = \{v_{i1}, ..., v_{in}\}, i = 1, ..., k$, ou seja,

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

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

Considere a transformação linear definida por

$$\begin{aligned} T: \quad & K^k \to K^n \\ & x \mapsto xG \end{aligned}$$

Se $x = \{x_1, ..., x_k\}$, temos que

$$T(x) = xG = x_1v_1 + ... + x_kv_k,$$

logo $T(\mathbf{k}^{\mathbf{k}}) = C$. Pode-se considerar $\mathbf{K}^{\mathbf{k}}$ como sendo o código da fonte, C, o código de canal e a transfromação T, uma codificação.

Note que a matriz G não é univocamente determinada, visto que ela depende da escolha da base de $\mathbf{B}$. Lembremos de resultados da teoria de espaços vetoriais que nos garantem que uma base de um espaço vetorial pode ser obtida uma da outra através de operações do tipo:

i) Permutação de dois elementos da base;

ii) multiplicação de um elemento da base por um escalar não nulo;

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

Do resultado acima segue que duas matrizes geradoras de um mesmo código C podem ser obtidas uma da outra por uma sequência de operações do tipo:

I) Permutação de duas linhas;

II) Multiplicação de uma linha por um escalar não nulo;

III) Adição de um múltiplo escalar de uma linha a outra.

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

$$\begin{aligned} T: \quad \mathbf{K^k} &\to \mathbf{K^n} \\ x &\mapsto xG \end{aligned}$$

Definição 1.11 *Diz-se que uma matriz geradora G de um código C está na forma padrão se tivermos*

$$G = (Id_k|A),$$

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

Algo importante que deve ser salientado é que dado um código C, nem sempre é possível achar uma matriz geradora de C na forma padrão. Por exemplo, o código em $\mathbb{F}_2^5$ de matriz geradora

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

nunca poderá ter uma matriz geradora na forma padrão, pois não consegue-se obtê-la utilizando uma das operações descritas anteriormente.

Entretanto, efetuando também as permutações das colunas de G, pode-se obter a matriz

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

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

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

C1) permutação de duas colunas;

C2) multiplicação de uma coluna por um escalar não nulo;

obtemos uma matriz G' de um código C'.

Observação 1.6 *Note que efetuar as operações acima numa base de C implica efetuá-las em todas as palavras de C.*

Permitindo-se a utilização de operações do tipo C1 conseguimos ter o seguinte resultado:

Teorema 1.2 *Dado um código C, existe um único código equivalente C' com matriz geradora na forma padrão.*

Demonstração: Presente em [4] ∎

1.2.2 Códigos Duais

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

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

Tal operação possui as propriedades usuais de um produto interno, isto é, simetria

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

e bilinearidade

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

para todo $\lambda \in \mathbf{K}$

Seja $C \subset \mathbf{K}^n$ um código linear, define-se

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

Lema 1.3 *Se $C \in \mathbf{K}^n$ é um código linear com matriz geradora G, então*

i) $C^{\perp}$ é um subespaço vetorial de $\boldsymbol{k}^n$;

ii) $x \in C^{\perp} \Longleftrightarrow Gx^t = 0$

Demonstração:

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

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

e portanto $u + \lambda v \in C^{\perp}$.

ii) $x \in C^{\perp}$ se, e só se x é ortogonal a todos os elementos de C se, e só se x é ortogonal a todos os elementos de uma base de C, que é equivalente dizer que $Gx^t = 0$, pois as linhas de G são uma base de C.

■

Observação 1.7 *O subespaço vetorial $C^{\perp}$ de k^n, ortogonal a C, é também um código linear que será chamado de* ***código dual*** *de C.*

Proposição 1.3 *Seja $C \subset \mathbf{K}^n$ um código de dimensão k com matriz geradora $G = (Id_k|A)$, na forma padrão. Então*

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

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

Demonstração:

i) Pelo lema 1, $x = (x_1, ..., x_n)$ pertence a $C^{\perp}$ se, e só se $Gx^t = 0$. Como G está na forma padrão, temos que

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

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

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

■

Vamos recordar as definições de algumas isometrias lineares básicas de $\mathbf{K}^n$

$$T_{\phi}: \quad \mathbf{K^n} \quad \rightarrow \quad \mathbf{K^n}$$

$$(x_1, ..., x_n) \mapsto (x_{\phi(1)}, ..., x_{\phi(n)}),$$

onde ϕ é uma permutação de $\{1, ..., n\}$, e

$$T_c^j : \quad \mathbf{K^n} \quad \rightarrow \quad \mathbf{K^n}$$

$$(x_1, ..., x_j, ..., x_n) \mapsto (x_1, ..., cx_j, ..., x_n),$$

onde $c \in \mathbf{K}^*$ e $j = 1, ..., n$.

O seguinte lema diz como se relaciona a dualidade com a equivalência de códigos lineares

Lema 1.4 *Seja C um código linear em $\mathbf{K^n}$. Para toda permutação ϕ de $\{1, ..., n\}$, para todo $c \in K^*$ e para todo $j = 1, ..., n$ temos que*

i) $(T_\phi(C))^\perp = T_\phi(C^\perp)$;

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

Proposição 1.4 *Sejam C e D dois códigos lineares em $\mathbf{K}^n$. Se C e D são linearmente equivalentes, então $C^\perp$ e $D^\perp$ são linearmente equivalentes.*

Demonstração: Se C e D são linearmente equivalentes existem uma permutação ϕ de $\{1, ..., n\}$ e elementos $c_1, ..., c_n \in \mathbf{K}$ tais que

$$D = T_\phi \circ T_{c_1}^1 \circ ... \circ T_{c_n}^n(C).$$

Levando em consideração o resultado do lema anterior temos

$$D^\perp = (T_\phi \circ T_{c_1}^1 \circ ... \circ T_{c_n}^n(C))^\perp = T_\phi \circ T_{c_1^{-1}}^1 \circ ... \circ T_{c_n^{-1}}^n(C^\perp).$$

■

Corolário 1.1 *Se D é um código linear em $\mathbf{K}^n$ de dimensão k, então $D^\perp$ é um código de dimensão $n - k$.*

Demonstração: Presente em [4]. ■

Lema 1.5 *Suponha que C seja um código de dimensão k em $\mathbf{K}^n$ com matriz geradora G. Uma matriz H de ordem $(n - k) \times n$, com coeficientes em $\mathbf{K}$ e com linhas linearmente independentes, é uma matriz geradora de $C^\perp$ se, e só se*

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

Demonstração: As linhas de H geram um subespaço vetorial de $\mathbf{K^n}$ de dimensão$n-k$, portanto, igual 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

$$(G \cdot H_{ij}^t) = \langle g_i, h_j \rangle .$$

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

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

■

Corolário 1.2 $(C^{\perp})^{\perp} = C$

Demonstração: Presente em [4]. ■

Proposição 1.5 *Seja C um código linear e suponhamos que H seja uma matriz geradora de $C^{\perp}$. Temos então que*

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

Demonstração: Pelo Lema 1.3 (ii) e o Corolário 1.2,

$$v \in C \Longleftrightarrow v \in (C^{\perp})^{\perp} \Longleftrightarrow Hv^t = 0.$$

■

A proposição acima nos permite caracterizar os elementos de um código C por uma condição de anulamento.

A matriz geradora H de $C^{\perp}$ é chamada de **matriz teste de paridade** de C.

Definição 1.12 *Dados um código C com matriz teste de paridade H e um vetor $v \in \mathbf{K}^n$, chamamo o vetor hv^t de **síndrome** de $\boldsymbol{v}$.*

Proposição 1.6 *Seja H a matriz teste de paridade de um código C. Temos que o peso de C é maior do que ou igual a s se, e só se quaisquer $s-1$ colunas de H são linearmente independentes.*

Demonstração: Suponhamos que cada conjunto de $s-1$ colunas de H é linearmente independente. 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

$$0 = H \cdot e^t = \sum c_i h^i.$$

Visto que $w(c)$ é o número de componentes não nulas de c, segue que se $w(c) \leq s-1$ teríamos uma combinação nula de um número t, com $1 \leq t \leq s-1$, de colunas de H, o que é contraditório. Logo, $w(c) \geq s$, e portanto, $w(C) \geq s$.

Por outro lado, suponhamos que $w(C) \geq s$. Suponhamos também, por absurdo, que H tenha $s-1$ colunas linearmente dependentes, digamos $h^{i_1},...,h^{i_{s-1}}$. Logo, existiriam $c_{i_1},...,c_{i_{s-1}}$, no corpo, nem todos nulos, tais que

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

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

Teorema 1.3 *Seja H a matriz teste de paridade de um código C. Temos que o peso de C é igual a s se, e só se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

Demonstração: Presente em [4]. ■

Corolário 1.3 *Cota de Sigleton: Os parâmetros (n,k,d) de um código linear satisfazem a desigualdade*

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

Demonstração: Se H é uma matriz teste de paridade, ela tem posto $n-k$. Como, pelo Teorema 1.3, $d-1$ é menor ou igual ao posto de H, segue a desigualdade. ■

Definição 1.13 *Um código será chamado de **MDS** (Maximum Distance Separable) se valer a igualdade $d=n-k+1$.*

1.2.3 Exemplos de Códigos

Exemplo 1.4 *(Códigos de Hamming)*
Um código de Hamming de ordem m sobre $\mathbf{F}_2$ é um código com matriz teste de paridade H_m de ordem $m \times n$, cujas colunas são os elementos de $\mathbf{F}_2^m - \{0\}$ numa ordem qualquer.

O exemplo acima que traz a definição de H_m determina o código C a menos de equivalência.

Temos portanto, que o comprimento de um código de Hamming de ordem m é $n = 2^m - 1$, e sua dimensão é $k = n - m = 2^m - m - 1$.

Proposição 1.7 *Todo código de Hamming é perfeito.*

Demonstração: A priori, temos que distância mínima de um código de Hamming é $d = 3$, daí $k = \left[\frac{d-1}{2}\right] = 1$. Dado c em $\mathbf{F}_2^n$. Temos que

$$|D(c,1)| = 1 + n.$$

Portanto,

$$|\bigcup_{c\in C} D(c,1)| = [1+n]2^k = [1+2^m-1]2^{n-m} = 2^n,$$

e consequentemente,

$$\bigcup_{c\in C} D(c,1) = \mathbf{F}_2^n.$$

■

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

Exemplo 1.5 ***O código do Mariner 9***
O código usado na nave espacial mariner 9 é um membro particular de uma família de códigos R(1,m) definidos sobre $\mathbf{F}_2$. *Estes códigos são denominados de Códigos de Reed-Muller de primeira ordem.*

Considere todos os elementos de $\mathbf{F}_2^m$ *e arrume-os como vetores colunas de uma matriz* $A_m, m \times 2^m$, *de modo que o bloco* $m \times 2^m - 1$ *a esquerda dessa matriz seja a matriz* H_m *como descrita no exemplo 1.5, e que a última coluna à direita seja o vetor zero de* $\mathbf{F}_2^m$, *isto é*

$$A_m = (H_m, 0).$$

Construímos a matriz G com $(m+1)$ *linhas e* 2^m *colunas, de tal modo que nas entradas de sua primeira linha sejam todas iguais a 1 e, logo abaixo, a matriz* A_m *como bloco, ou seja,*

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

A seguinte proposição traz quais são os paramêtros dos códigos $R(1,m)$ cuja matriz geradora seja a matriz G.

Proposição 1.8 *Os parâmetros do código R(1,m) são* $(2^m, m+1, 2^{m-1})$

Demonstração: A princípio temos que o comprimento do código é 2^m, pois a matriz G tem 2^m colunas. Como a matriz G tem $m+1$ linhas linearmente independentes devido ao bloco H_m e pelo fato da primeira linha ser linearmente independente das demais, segue que a dimensão de $R(1,m)$ e $m+1$.

Vamos mostrar que a distância mínima de tal código é 2^{m-1}. Note que, exceto a palavra $u = 1...1$, as demais palavras do código possuem peso 2^{m-1}, isto é, metade das componentes são constituídas de zero e a outra metade, de uns.

Seja $c = v_{i_1} + ... + v_{i_r}$ uma palavra qualquer de $R(1,m)$ onde os $v_{i_j}, j = 1, ..., m$ são vetores linha da matriz G. Suponhamos que nenhum desses vetores é o vetor 11...1. Considere a matriz

$$B = \begin{pmatrix} v_{i_j} \\ ... \\ v_{i_r} \end{pmatrix}.$$

A matriz B possui 2^r colunas distintas correspondentes aos vetores de $\mathbf{F}_2^r$, cada uma repetida 2^{m-r} vezes. Portanto, a matriz A possui metade das colunas de peso par e metade de peso ímpar. Consequentemente, o vetor c possui metade de suas componenetes iguais a zero e metade igual a um, o que prova que o peso de c é 2^{m-1}. Se um dos somandos de c, digamos v_{i_1}, é igual ao vetor 11...1, pelo fato já estabelecidode que o vetor $v_{i_2} + ... + v_{i_r}$ tem metade de suas componentes igual a 1 e metade igual a zero, segue que o mesmo ocorre para c. ■

Observação 1.8 *O código do Mariner 9 corresponde ao caso* $m = 5$*, portanto trata-se do código* $R(1,5)$ *cujos parâmetros são* $(32, 6, 16)$*. Logo,* $k = 7$*.*

1.2.4 Decodificação

Denomina-se **Decodificação** o procedimento de detecção e correção de erros num determinado código. O método de decodificação abordado na pesquisa pautada na referência [4] é um aperfeiçoamento do método inventado por D. Slepian do laboratório Bell na década de 60.

Definição 1.14 *O vetor erro* $\boldsymbol{e}$ *trata-se da diferença entre o vetor recebido* $\boldsymbol{r}$ *e o vetor transmitido* $\boldsymbol{c}$*, ou seja,*

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

Observação 1.9 *O peso do vetor erro corresponde ao número de erros cometidos numa palavra entre a transmissão e a recepção.*

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

$$He^t = H(r^t - c^t) = Hr^t - He^t = Hr^t.$$

Portanto, a palavra recebida e o vetor erro possuem a mesma síndrome.
Denotaremos por h^i a i-ésima coluna de H. Se $e = (\alpha_1 ... \alpha_n)$, então

$$\sum_{i=1}^{n} \alpha_i h^i = Het = Hr^t.$$

Lema 1.6 *Seja C um código linear em $\mathbf{K}^n$ com capacidade de correção k. Se $\boldsymbol{r} \in \mathbf{K}^n$ e $c \in C$ são tais que $d(c, r) \leq k$, então existe um único vetor $\boldsymbol{e}$ com $w(\boldsymbol{e}) \leq k$, cuja síndrome é igual a síndrome de $\boldsymbol{r}$ e tal que $\boldsymbol{c} = \boldsymbol{r} - \boldsymbol{e}$*

Demonstração: Observe que $\mathbf{e} = \mathbf{r} - \mathbf{c}$ possui a propriedade do lema, pois $w(\mathbf{e}) = d(c, r) \leq k$. Para provarmos a unicidade, suponhamos que $\mathbf{e} = (\alpha_1 ... \alpha_n)$ e $e^{'} = (\alpha_1^{'} ... \alpha_n^{'})$ sejam tais que $w(\mathbf{e}) \leq k$ e $w(e') \leq k$ e tenham mesma síndrome que $\mathbf{r}$. Então, se H é uma matriz teste de paridade de C, temos

$$He^t = H(e')^t \Longrightarrow \sum_{i=1}^{n} \alpha_i h^i = \sum_{i=1}^{n} \alpha_i^{'} h^i,$$

O que nos dá uma relação de dependência linear entre $2k(\leq d-1)$ colunas de H. Como quaisquer $d-1$ colunas de H são linearmente indepenetes, temos que $\alpha_1 = \alpha_i$, para todo i, logo $\mathbf{e} = e^{'}$. ■

Exemplo 1.6 *(Determinação de $\boldsymbol{e}$ quando $w(\boldsymbol{e}) \leq 1$)*
Suponhamos que o código C tenha distância mínima $d \geq 3$ e que o vetor erro $\boldsymbol{e}$, introduzido entre a palavra transmitida $\boldsymbol{c}$ e a palavra recebida $\boldsymbol{r}$, seja tal que $w(\boldsymbol{e}) \leq 1$. Isto é, o canal introduziu no máximo um erro.

Se $He^t = 0$, então $r \in C$ e toma-se $c = r$.

Suponhamos $He^t \neq 0$, então $w(\boldsymbol{e}) = 1$, e portanto, $\boldsymbol{e}$ tem apenas uma coordenada não nula. Nesse caso, consideremos que $\boldsymbol{e} = (0, ..., \alpha, ..., 0)$ com $\alpha \neq 0$ na i-ésima posição. Logo,

$$He^t = \alpha h^i,$$

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

$$Het = Hr^t = \alpha h^i,$$

podemos determinar $\boldsymbol{e}$ como sendo o vetor com todas as componenetes nulas exceto a i-ésima componente, que é α.

Agora, estabeleremos o **algoritmo de decodificação em códigos corretores de um erro**

A priori, considere H a matriz teste de paridade do código C e seja $\mathbf{r}$ um vetor recebido e supondo $d \geq 3$.

i) Calcule Hr^t;

ii) Se $Hr^t = 0$, aceite $\mathbf{r}$ como sendo a palavra transmitida;

iii) Se $Hr^t = s^t \neq 0$, compare s^t com as colunas de H;

iv) Se existirem i e α tais que $s^t = \alpha h^i$, para $\alpha \in K$, então $\mathbf{e}$ é a n-upla com α na posição i e zeros nas outras posições. Corrija $\mathbf{r}$ pondo $\mathbf{c} = \mathbf{r} - \mathbf{e}$;

v) Se o contrário de (iv) ocorrer, então mais de um erro foi cometido.

Seja $C \subset K^n$ um código corretor de erros com matriz teste de paridade H. Sejam d a distância mínima de C e $k = \left[\frac{d-1}{2}\right]$.

Definição 1.15 *Seja $v \in \mathbf{K^n}$, cada conjunto da forma*

$$v + C = \{v + c : c \in C\}$$

*é denominado de **classe lateral de v segundo c**.*

Lema 1.7 *Os vetores $\boldsymbol{u}$ e $\boldsymbol{v}$ de $\mathbf{k^n}$ tem a mesma síndrome se, e só se, $\boldsymbol{u} \in \boldsymbol{v+C}$.*

Demonstração: $Hu^t = Hv^t \iff H(u-v)^t = 0 \iff u - v \in C \iff u \in v + C$. ∎

Proposição 1.9 *Seja C um $(n,k)-$código linear. Temos que:*

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

ii) $(v + C) \cap (v' + C) \neq \varnothing \Longrightarrow v + C = v' + C$;

iii) $\bigcup_{v \in K^n} (v + C) = K^N$;

iv) $|(v + c)| = |C| = q^k$.

Definição 1.16 *Um vetor de peso mínimo numa classe lateral é chamado de **elemento líder** dessa classe.*

Proposição 1.10 *Seja C um código linear em K^n com distância mínima d. Se u inK^n é tal que*

$$w(u) \leq \left[\frac{d-1}{2}\right] = k,$$

então u é o único elemento líder de sua classe.

Demonstração: Suponhamos que $u, v \in \mathbf{K}^n$ com $w(u) \leq \left[\frac{d-1}{2}\right]$ e $w(v) \leq \left[\frac{d-1}{2}\right]$.

Se $u - v \in C$ então

$$w(u-v) \leq w(u) + w(v) \leq \left[\frac{d-1}{2}\right] + \left[\frac{d-1}{2}\right] \leq d-1$$

logo, $u - v = o$ e portanto, $u = v$. ■

Observação 1.10 *Para achar líderes das classes, selecionamos todos os elementos u tais que $w(u) \leq \left[\frac{d-1}{2}\right]$. Cada um desses elementos é líder de uma, e somente uma classe.*

Nessa última parte do capítulo discutiremos um algorítmo de correção de mensagens que tenham sofrido um número de erros menor ou igual a capacidade de correção do código, que é $k = \left[\frac{d-1}{2}\right]$.

Preparação: Determine todos os elementos u de $\mathbf{K}^n$ tal que $w(u) \leq k$. Em seguida, calcule as síndromes desses elementos e coloque tais dados numa tabela. Seja r uma palavra recebida.

O Algoritmo da Decodificação

i) Calcule a síndrome $s^t = Hr^t$;

ii) Se s está na tabela, seja l o líder da classe determinada por s, troque r por $r - l$;

iii) Se s não está na tabela, então na mensagem recebida foram cometidos mais do que k erros.

Justificativa: Dado r, sejam c e e, respectivamente, a mensagem transmitida e o vetor erro. Como $He^t = Hr^t$, temos que a classe lateral onde e se encontra está determinada pela síndrome de r. Se $w(e) \leq k$, temos que e é o único elemento líder l de sua classe, portanto, é conhecido e se encontra na tabela e pelo lema 1.6 $c = r - e = r - l$ é determinado.

1.2.5 Códigos cíclicos

Os códigos cíclicos são muito utilizados nas aplicações por formarem uma classe de códigos linearesque possui bons algorítmos de codificação e de decodificação. Sugerimos a leitura dos capitulos 2 e 3 da referência [4] ou uma consulta a [3] para melhor compreensão de elementos de estruturas algébricas abordadas no escopo do trabalho. Considere $\mathbf{K}$ um corpo finito. Representaremos as coordenadas de $\mathbf{K^n}$ por $(x_0, ..., x_{n-1})$.

Definição 1.17 *Um código linear $C \subset \mathbf{K^n}$ será chamado de **código cíclico** se para todo $c = (c_0, ..., c_{n-1})$ pertencente a C, o vetor $(c_{n-1}, c_0, ..., c_{n-2})$ pertence a C.*

Equivalentemente, o código linear C será um código cíclico se, dada a permutação π de $\{0, ..., n-1\}$ definida por

$$\pi_(i)\begin{cases} i-1, & se \quad i \geq 1; \\ n-1 & se \quad i = 0; \end{cases}$$

e sendo

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

temos que $T_\pi \in C, \forall c \in C$, isto é, $T_\pi(C) \subset C$.

Exemplo 1.7 *Seja $v \in \mathbf{K^n}$. O espaço vetorial*

$$\langle v \rangle = Kv + KT_\pi(v) + ... + KT_\pi^{n-1}(v)$$

é um código cíclico, observe que $T_\pi^n = Id$.

As questões imediatas que surgem em tal contexto são:

i) Como podem ser descritos todos os códigos cíclicos de $\mathbf{K}^n$?

ii) Qantos são os códigos cíclicos de dimensão k em $\mathbf{K^n}$?

iii) Todo código cíclico é da forma $\langle v \rangle$ para algum v?

iv) Como calcular o peso de um código cíclico?

Algo que vale salientar é que a (iv) pergunta é uma parte de uma questão em aberto, as demais são discutidas na referência [4] base do escopo desse trabalho.

As técnicas para lidar com códigos cíclicos consiste no enriquecimento da estrutura de espaço vetorial de K^n, como será descrito:
Defina R_n como sendo o anel das classes residuais em $\mathbf{K}[x]$ módulo $x^n - 1$, isto é

$$R_n = \mathbf{K}[x]_{(x^n-1)}.$$

um elemento de de R_n, é um conjunto da forma:

$$[f(x)] = \{f(x) + g(x)(x^n - 1), g(x) \in \mathbf{K}[x]\};$$

a adição e multiplicação em R_n são definidas, respectivamente por

$$[f_1(x)] + [f_2(x)] = [f_1(x) + f_2(x)]$$

e

$$[f_1(x)].[f_2(x)] = [f_1(x).f_2(x)]$$

A multiplicação em R_n por escalares $\lambda \in \mathbf{K}$ é definida por

$$\lambda[f(x)] = [\lambda f(x)],$$

Observe que R_n com tais propriedades é um $\mathbf{K}-$espaço vetorial de dimensão n com base $1, [x], ..., [x^{n-1}]$ e é isomorfo a K^n através da transformação linear

$$\begin{array}{ccccc} v: & & K^n & \to & R_n \\ & & (a_o, ..., a_{n-1}) & \mapsto & [a_0 + a_1 x + ... + a_{n-1}x^{n-1}]. \end{array}$$

Observação 1.11 *O isomorfismo descrito acima é extremante vantajoso para se estudar qualquer código linear $C \subset \mathbf{K^n}$ por R_n possuir estrutura de espaço vetorial, e também uma estrutura adicional de anel.*

Agora, nosso objetivo é determinar matrizes geradoras e matrizes teste de paridade de códigos cíclicos em R_n. Note que a ação de T_π em $\mathbf{K^n}$ traduz-se, por meio de v, na multiplicação por $[x]$ em R_n.

tomando $c = (c_0, ..., c_{n-1})$ temos

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

e

$$v(T_\pi(c)) = [c_{n-1} + c_0 x + ... + c_{n-2}x^{n-1} = [x][c_0 + c_1 x + ... + c_{n-1}x^{n-1} = [x]v.$$

Lema 1.8 *Seja V um subespaço vetorial de R_n. Então, V é um ideal de R_n se, e só se V é fechado pela multiplicação por $[x]$.*

Demonstração: Suponhamos que V seja um ideal de R_n. da definição de ideal segue que $[x][f(x)] \in V, \forall [f(x)] \in V$.

Por outro lado, suponhamos que V seja fechado pela multiplicação em $[x]$. É suficiente mostrar que $[g(x)][f(x)] \in V, \forall [g(x)] \in R_n$ e todo $[f(x)] \in V$.

Seja$[f(x)] \in V$. Como V é um subespaço de R_n, então $a[f(x)] \in V, \forall a \in \mathbf{K}$.

Por hipótese,

$$[xf(x)] = [x][f(x)] \in V.$$

Indutivamente, temos que para todo $m \in \mathbf{N}$

$$[x^m f(x)] = [x^m][f(x)] \in V.$$

Escrevendo $[g(x)] = [a_0 + a_1x + ... + a_{n-1}x^{n-1}]$, temos que

$$[g(x)][f(x)] = [g(x)f(x)] = [(a_0 + a_1x + ... + a_{n-1}x^{n-1}] = \\ a_0[f(x)] + a_1[x][f(x)] + ... + a_{n-1}[x^{n-1}][f(x)] \in V,$$

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

Teorema 1.4 *Um subespaço C de* $\mathbf{K^n}$ *é um código cíclico se, e só se* $v(C)$ *é um ideal de* R_n

Para alguns próximos resultados considere a proposição abaixo:

Proposição 1.11 *Um código C em* $\mathbf{K^n}$ *é cíclico se, e só se* $v(C) = I([g(x)])$*, onde* $g(x) \in \mathbf{K[x]}$ *é um divisor de* $x^n - 1$.

Seja $p = car(K)$. Se $n = mp^s$ com m e p primos entre si, temos que

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

Como $(x^m - 1) = mx^{m-1} \neq 0$, o polinômio x^{m-1} não possui fator não constante em comum com a sua derivada, portanto, não possui múltiplo algum. Com isso,

$$x^m - 1 = f_1...f_r,$$

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

$$x^n - 1 = f_1^{p^s}...f_r^{p^s}.$$

Segue então que o polinômio $x^n - 1$ possui exatamente $(p^s + 1)^r$ divisores mônicos.
Note que R_n não é um domínio de integridade, pois por exemplo

$$[x - 1].[x^{n-1} + x^{n-2} + ... + x + 1] = [x^n - 1] = [0].$$

Observe que $g(x)$ denotará sempre um divisor de $x^n - 1$, colocaremos

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

Teorema 1.5 *Seja $I = I([g(x)])$, onde $g(x)$ é um divisor de $x^n - 1$ de grau s. Temos que $[g(x)], [xg(x)], [x^2g(x)], ..., [x^{n-s-1}g(x)]$ é uma base de I como espaço vetorial sobre* $\mathbf{K}$.

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

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

Logo,

$$[g(x)][a_0 + a_1x + ... + a_{n-s-1}x^{n-s-1}] = [0].$$

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

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

Daí, segue que

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

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

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

$$f(x) \equiv d(x).g(x) \quad mod \quad (x^n - 1).$$

Pelo algorítmo 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,

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

e portanto,

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

Consequentemente,

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

■

Corolário 1.4 *Dado um código C cíclico, existe $v \in C$ tal que $C = \langle v \rangle$.*

Corolário 1.5 *Seja $g(x) = g_0 + g_1x + ... + g_nx^s$ um divisor de $x^n - 1$ de grau s. Se $I = I([g(x)])$, então*

$$dim_k I = n - s,$$

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

$$G = \begin{pmatrix} v^{-1}([g(x)]) \\ v^{-1}([xg(x)]) \\ ... \\ v^{-1}(x^{n-s-1}[g(x)]) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & ... & g_s & 0 & ... & 0 \\ 0 & g_0 & g_1 & ... & g_s & ... & 0 \\ ... & ... & ... & ... & ... & ... & ... \\ 0 & ... & 0 & g_0 & ... & ... & g_s \end{pmatrix}.$$

Demonstração: As demonstrações dos corolários acima estão presente em [4]. ■

Definição 1.18 *Dado um polinômio $h(x) = h_0 + h_1x + ... + h_tx_t$ que divide $X^n - 1$, tem-se que o **polinômio recíproco** de $h(x)$ é*

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

é também um divisor de $x^n - 1$.

Teorema 1.6 *Seja $C = v^{-1}(I)$ um código cíclico, onde $I = I([g(x)])$, com $g(x)$ um divisor de $x^n - 1$ de grau s. Então $C^\perp$ é cíclico e $C^\perp = v^{-1}(J)$, onde $J = I([h^*(x)])$.*

Demonstração: Tomemos $g(x) = g_0 + g_1x + ... + g_sx^s$ e $h(x) = h_0 + h_1x + ... + h_{n-s}x^{n-s}$
Note que $\text{gr}(h(x)) = n - s$, portanto $h_{n-s} \neq 0$.
Sejam

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

e

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

Observe que as linhas de H são linearmente independentes.
Seja $\{e_1, ..., e_n\}$ a base canônica de $\mathbf{K^n}$. A i-ésima linha de G é

$$G_i = g_0e_1 + g_1e_{i+1} + ... + g_se_{i+s}, \quad 1 \leq i \leq n - s,$$

e a j-ésima coluna de H^t é

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

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

$$g_{j-i}h_{n-s} + g_{j-i-1}h_{n-s-1} + ... + g_{n-s}h_{j-i}, \quad j - i = 0, ..., s - 1.$$

Mas a soma acima é precisamente igual ao coeficiente de $x^{n-s+j-i}$ no produto $g(x) \cdot h(x) = x^n - 1$. Como $1 \leq n - s + j - i \leq n - 1$, temos que esse coeficiente é igual a zero. O caso para $j \leq i$ é análogo. Portanto, $G \cdot H^t = 0$ de modo que H é uma matriz geradora de $C^{\perp}$.

Observe que

$$H = \begin{pmatrix} v^{-1}([h^*(x)]) \\ v^{-1}([xh^*(x)]) \\ ... \\ v^{-1}(x^{n-s-1}[h^*(x)]), \end{pmatrix}$$

e com isso temos que $C^{\perp} = v^{-1}(j)$, onde $J = I([h^*(x)])$. ■

Corolário 1.6 *A matriz teste de paridade de $C = v^{-1}(I)$, em que $I = I([g(x)])$, é dada por*

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

onde

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

Demonstração: Provado no teorema 1.6 ■

1.2.5.1 Decodificação em Códigos Cíclicos

Seja $C \subset \mathbf{K}^n$ um código cíclico. Neste trecho do trabalho mostraremos como determina-se uma matriz geradora de C na forma padrão $(R|Id)$ e abordaremos um algorítmo de codificação para tais códigos. Além do mais, será mostrado como se determina a síndrome em códigos cíclicos.

Seja

$$\begin{array}{rccc} \gamma: & \mathbf{K}^s & \to & \mathbf{K}[x]_{s-1} \subset \mathbf{K}[x] \\ & (a_o, ..., a_{s-1}) & \mapsto & \displaystyle\sum_{i=0}^{s-1} a_i x^i \end{array}$$

o isomorfismo de $\mathbf{K}$- espaços vetoriais, onde $\mathbf{K}[\mathbf{x}]_{\mathbf{s-1}}$ é o espaço vetorial dos polinômios de grau menor ou igual a $s-1$. Tal isomorfismo será importante para o estudo dos próximos resultados.

Teorema 1.7 *Seja $C \subset \mathbf{K}^n$ um código cíclico. Suponhamos que $C = v^{-1}(I)$, onde ($I = I([g(x)]$, cpm $g(x)$ um divisor de $x^n - 1$. Seja R a matriz $(n-s) \times x$ cuja i-ésima linha é*

$$R_i = -\gamma^{-1}(r_i(x)), \qquad 1 \leq i \leq n-s,$$

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

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

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

Portanto, $[x^{s-1+i} - r_i(x)]$ pertence a I e é fácil ver que tasi vetores para $i = 1, 2, ..., n-s$ são linearmente independentes sobre $\mathbf{K}$, como $v^{-1}([x^{s-1+i} - r_i(x)] = e_{s-1+i} - \gamma^{-1}(r_i(x))$, temos que a matriz

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

é uma matriz geradora de C ∎

Falaremos agora sobre o algoritmo de codificação. Os elementos de C podem ser considerados como codificação do código da fonte $\mathbf{K}_{n-s}$ conforme será descrito abaixo.

Dado $(a_1, ..., a_{n-s}) \in \mathbf{K}^{n-s}$, esse vetor ppde ser codificado como elementos de C como se segue:

$$(a_1, ..., a_{n-s})(R|Id_{n-s}) = (b_0, ..., b_{s-1}, a_1, ..., a_{n-s}),$$

onde

$$(b_0, ..., b_{s-1}) = -a_{-1}\gamma^{-1}(r_1(x) - ... - a_{n-s}\gamma^{-1}(r_{n-s}(x)) =$$
$$-\gamma^{-1}(a_1 r_1(x) + ... + a_{n-s}r_{n-s}(x)) =$$
$$-\gamma(\sum_{i=1}^{n-s} a_i r_i(x))$$

Exemplo 1.8 *Considere o polinômio $x^7 - 1$, sobre $\mathbf{F}$. A fatoração $x^7 - 1$ é dada por*

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

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

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

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

Logo, pelo teorema anterior (1.7), temos que uma matriz geradora de C é dada por

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

Suponhamos que seja dado o vetor $(a_1, a_2, a_3, a_4) \in \mathbf{F}_2^7$, do código da fonte, então, de acordo com o que foi discutido anteriormente, a codificação desse vetor é dada por

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

onde b_0, b_1, b_2 são os coeficientes do polinômio

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

Portanto, a codificação de (a_1, a_2, a_3, a_4) é

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

O teorema seguinte permitirá calcular algébricamente a síndrome de um vetor relativamente a uma matriz teste de paridade num código cíclico, sem que seja necessário o produto vetorial pela matriz referenciada.

Teorema 1.8 *Seja $C \subset \mathbf{K}^n$ um código cíclico gerado por um polinômio mônico $g(x)$ de grau s e com matriz geradora na forma padrão $(R|Id_{n-s})$ e matriz teste de paridade $H = (Id_s| - R^t)$. Se $y = (y_0...., y_{n-1}) \in \mathbf{K}^n$, então a síndrome de y com relação a matriz H é dada por*

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

onde $r(x)$ é o resto da divisão de $y_0 + y_1x + ... + y_{n-1}x^{n-1}$ por $g(x)$.

Demonstração: A síndrome de y é o vetor

$$(Id_s| - R^t)y^t =$$
$$(\gamma^{-1}(1), \gamma^{-1}(x), ..., \gamma^{-1}(x^{s-1}), \gamma^{-1}(r_1(x)), ..., \gamma^{-1}(r_{n-s}(x)))y^t =$$
$$\gamma^{-1}(t_0 + y_1x + ... + y_{s-1}x^{s-1} + y_sr_1(x) + ... + y_{n-1}r_{n-s}(x))$$

Segue que

$$r(x) = y_0 + y_1x + ... + y_{s-1}x^{s-1} + y_sr_1x + ... + y_{n-1}r_{n-s}(x)$$

é o resto da divisão de $y_0 + y_1x + ... + y_{n-1}x^{n-1}$ por $g(x)$. ■

Exemplo 1.9 *Considerando o código do exemplo anteior (1.9). A matriz teste de paridade associada a G é a matriz*

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

dado o vetor $(1101001) \in \mathbf{F}_2^8$, *a sua síndrome relativa a H é dada por* $\gamma^{-1}(r(x))$, *onde $r(x)$ é o resto da divisão de* $1 + x + x^3 + x^6$ *por* $g(x) = 1 + x + x^3$. *Portanto,* $r(x) = x2 + 1$, *e consequentemente, a síndrome é* (101).

CAPÍTULO 2

ÁLGEBRAS DE GRUPO

Neste capítulo, vamos apresentar, sem demonstrações, os conceitos básicos da teoria de anéis de grupos. Para isso, necessitaremos tratar rapidamente da teoria de módulos que é, por si só, uma importante área de pesquisa em matemática e é repleta de importantes resultados, como o Teorema de Wedderburn-Artin. Porém, nosso foco aqui, é dar o máximo de elementos possíveis sobre a álgebras de grupo para que os utilizemos na compreensão dos códigos de grupo. Para mais detalhes sobre módulos ou anéis de grupo, inclusive para as demonstrações omitidas aqui, sugerimos [5].

2.1 Módulos

Seja $\mathbf{R}$ um anel com unidade 1. Diz-se que um conjunto não zazio M é um **módulo a esquerda sobre R** ou simplesmente, **R**-módulo a esquerda se temos definida em M uma operação, que denotaremos por $+$ e uma lei de composição externa, tal que a cada par $(a, m) \in \mathbf{R} \times M$ associa um elemento $am \in M$, onde para quaiquer $a, b \in \mathbf{R}$ e $m, n, p \in M$ tenhamos tais propriedades satisfeitas:

i) $(m + n) + p = m + (n + p)$;

ii) Existe um elemento "0" tal que $0 + m = m + 0 = m$;

iii) Existe um elemento $-m$" tal que $-m + m = 0$;

iv) $m + n = n + m$;

v) $(a + b)m = am + bm$;

vi) $a(m + n) = am + an$;

vii) $a(bm) = (ab)m$;

viii) Existe 1 tal que $1m = m$;

Analogamente, define-se R**-módulo a direita**, realizando a lei de composição externa com os elementos do anel R à direita.

Seja I um ideal a esquerda de um anel R. Então I admite uma estrutura de $\mathbf{R}$-módulo, com soma induzida pela soma de $\mathbf{R}$ e a aplicação $\mathbf{R} \times I$ dada pela multiplicação, a esquerda, por elementos de $\mathbf{R}$. Assim temos que um anel $\mathbf{R}$ é sempre um módulo sobre si mesmo, para denotar tal aspecto, denotamos ${}_{\mathbf{R}}\mathbf{R}$ e $\mathbf{R}_{\mathbf{R}}$, os módulos à esquerda e à direita, respectivamente.

Definição 2.1 *Seja* $\boldsymbol{R}$ *um anel comutativo. Um* $\boldsymbol{R}$*-módulo* M *é denominado uma* $\boldsymbol{R}$***-álgebra*** *se existe uma multiplicação, definida em* M*, tal que, com essa multiplicação e a adição definida em* M *tal seja um anel.*

Definição 2.2 *Seja* M *um* $\boldsymbol{R}$*-módulo e* N *um subconjunto de* M*. Dizemos que* N *é um* $\boldsymbol{R}$*-Submódulo de* M *se:*

i) $N \neq \varnothing$*;*

ii) $m - n \in N, \forall m, n \in N$*;*

iii) Para todo $r \in \mathbf{R}$ *e para todo* $n \in N$ *temos* $rn \in N$*.*

Todo $\mathbf{R}$-módulo M possui, pelo menos, dois súbmódulos, que são $\{0\}$ e M, que são denominados *submódulos triviais*, os demais submódulos que não são os triviais, são denominados *submódulos próprios.*

Uma aplicação $f : M \to N$ é denominada *homomorfismo de* $\boldsymbol{R}$*-módulos* se

i) $f(m + p) = f(m) + f(p); \forall m, p \in M$;

ii) $f(am) = f(a)f(m) = af(m); \forall a \in \mathbf{R}$ e $\forall m \in M$.

Se o $\mathbf{R}$-homomorfismo por injetivo é chamado $\boldsymbol{R}$*-monomorfismo*, e se for sobrejetivo é denominado $\boldsymbol{R}$*-epimorfismo.*

Alguns resultados imediatos são que o $ker(f)$ e $im(f)$ são submódulos de M e N, respectivamente. Além do mais, f é um $\mathbf{R}$-epimorfismo se, e só se, $Im(f) = N$, e também, f é um $\mathbf{R}$-monomorfismo se, e só se, $ker(f) = \{0\}$.

Da mesma maneira que é definido para Anéis, o *módulo quociente* é o conjunto tal que

$$\frac{M}{N} = \{m + N : m \in M\},$$

onde M é um $\mathbf{R}$-módulo e N um submódulo de M.

Teorema 2.1 *Teorema de homomorfismo para módulos*

Sejam M e N dois $\boldsymbol{R}$-módulos, $f : M \to N$ um $\boldsymbol{R}$-homomorfismo, $j : M \to \frac{M}{ker(f)}$ a projeção canônica ao quociente e $Im(f) \to N$ a inclusão. Então existe uma única aplicação

$$f^* : \frac{M}{ker(f)} \to Im(f)$$

tal que

i) $f = i \circ f^* \circ j$;

ii) F^* *é um* $\boldsymbol{R}$*-isomorfismo.*

Definição 2.3 *Seja $\{M\}_{i\in I}$ uma família de $\boldsymbol{R}$-módulos, onde I é o conjunto de índices. Uma família $(m_i)_{i\in I} \in M$ é dita quase nula se $m_i = 0$, exceto para algum número finito de índices.*

Usaremos a proposição em seguida para definirmos *soma direta* na estrutura de módulos, que será análoga a comumente vista em espaços vetoriais.

Proposição 2.1 *Seja $\{M_i\}_{i\in I}$ uma família de $\boldsymbol{R}$-submódulos de um $\boldsymbol{R}$-módulo M. As seguintes afirmações são equivalentes:*

i) Todo elemento $m \in M$ se escreve de único modo, na forma $m = \sum_{i\in I} m_i$, onde $m_i \in M_i$ para todo $i \in I$ e a família $(m_i)_{i\in I}$ é quase nula;

ii) $M = \sum_{i\in I} M_i$ *e se,* $m_i = 0$ *com* $M_i \in M_i$ *então* $m_i = 0$ *para todo* $i \in I$;

iii) $M = \sum_{i\in I} M_i$ *e* $M_j \cap (\sum_{i\neq j} M_i) = \{0\}$, *para todo* $j \in I$.

Um $\mathbf{R}$-módulo M é dito *soma direta* de uma família $\{M_i\}_{i\in I}$ de submódulos se alguma das condições anteriores for satisfeita.

Para indicar que M é soma direta dos submódulos $\{M_i\}_{i\in I}$ usaremos o símbolo

$$M = \bigoplus_{i\in I} M_i$$

Observação 2.1 *Um submódulo N de um $\boldsymbol{R}$-módulo M é dito somando direto se existe um outro $\boldsymbol{R}$-módulo T tal que*

$$M = N \oplus T.$$

2.1.1 Módulos semissimples

Um **R**-módulo M é chamado é denominado *semissimples* se todo submódulo de M é um somando direto. Equivalentemente temos que M é semissimples se, e só se, M é uma soma direta de submódulos simples.

Teorema 2.2 *Seja* $\boldsymbol{R}$ *um anel. As seguintes condições são equivalentes:*

i) Todo $\boldsymbol{R}$*-módulo é semissimples;*

ii) $\boldsymbol{R}$ *é um anel semissimples;*

iii) $\boldsymbol{R}$ *é uma soma direta de um número finito de ideais minimais à esquerda;*

dada uma decomposição de um anel semissimples **R** como uma soma direta de ideais minimais à esquerda, reordenando caso necessário, podemos agrupar os ideais a esquerda isomosrfos juntos.

$$R = L_{11} \oplus ... \oplus L_{1r_1} \oplus L_{21} \oplus ... \oplus L_{2r_2} \oplus ... \oplus L_{s1} \oplus ... \oplus L_{sr_s}$$

Com a notação acima $L_{ij} \simeq L_{ik}$ e $L_{ij}L_{kh} = \{0\}$, se $i \neq k$. Sabe-se também que todo ideal minimal a esquerda de **R** é isomorfo a um dos ideais na decomposição de **R** descrita acima.

Teorema 2.3 *Com a notação acima, seja* A_i *a soma de todos os ideais a esquerda isomorfos a* L_{i1}, $1 \leq i \leq s$. *Então:*

i) Cada A_i *é um ideal bilateral minimal de* $\boldsymbol{R}$*;*

ii) $A_iA_j = \{0\}$ *se* $i \neq j$*;*

iii) $\boldsymbol{R} = \bigoplus_{i-1}^{s} A_i$ *como anel, onde* s *é o número de classes isomórficas de ideais a esquerda minimais de* $\boldsymbol{R}$*.*

Corolário 2.1 *Os ideais* A_i *com* $1 \leq i \leq s$ *definidos acima são anéis simples, isto é, seus únicos ideais bilaterais são os triviais.*

2.2 Anéis de grupo

Seja G um grupo e **R** um anel com unidade. Construíremos um **R**-módulo onde os elementos de G são uma base e usaremos as operações de G e **R** uma estrutura de anel sobre esse módulo.

Seja $\mathbf{R}G$ o conjunto de todas as combinações lineares da forma

$$\alpha = \sum_{g \in G} a_g g,$$

em que $a_g \in \mathbf{R}$ e $a_g = 0$, para quase todo $g \in G$. Dado $\alpha \in G$ definimos o *suporte* de α como o subconjunto de elementos de G que, de fato, aparecem na expressão de α, ou seja

$$supp(\alpha) = \{g \in G : a_g \neq 0\}.$$

Da definição segue que dados $\alpha, \beta \in RG$ se $\alpha = \beta$, então $a_g = b_g$, para todo $g \in G$.

Define-se uma adição e uma multiplicação para $\mathbf{R}G$ no intuito de que tal possua uma estrutura de anel.

$$\alpha + \beta = \sum_{g \in G} a_g g + b_g g = \sum_{g \in G} (a_g + b_g) g$$

$$\alpha.\beta = \sum_{g \in G} a_g g.b_g g = \sum_{g \in G} (a_g.b_g) g$$

Assim, $\mathbf{R}G$ é um anel com as operações descritas acima. Na verdade, $\mathbf{R}G$ é um anel com unidade $1 = \sum_{g \in G} u_g g$, onde o coeficiente correspondente aunidade do gruo é 1 e $u_g = 0$, para todos os outros elementos de G.

Também podemos definir em $\mathbf{R}G$ a multiplicação de elementos de $\mathbf{R}G$ por elementos λ de $\mathbf{R}$ da seguinte forma:

$$\lambda\alpha = \lambda \sum_{g \in G} a_g g = \sum_{g \in G} (\lambda a_g) g$$

Definidas essas três operações acima, temos que $\mathbf{R}G$ é um $\mathbf{R}$-módulo e se $\mathbf{R}G$ for um anel comutativo então $\mathbf{R}G$ é uma $\mathbf{R}$-álgebra.

O conjunto $\mathbf{R}G$ com as operações definidas acima é denominado **anel de grupo** de G sobre $\mathbf{R}$. Se $\mathbf{R}$ for comutativo então $\mathbf{R}G$ é chamado de **álgebra de grupo** de G sobre $\mathbf{R}$.

Proposição 2.2 *Seja $f : G \to H$ um homomorfismo de grupos. Existe um único Homomorfismo de anéis $f^* : \boldsymbol{R}G \to \boldsymbol{R}H$ tal que $f^*(g) = f(g)$, para todo $g \in G$. Se $\boldsymbol{R}$ é um anel comutativo, então f^* é um homorfismo de $\boldsymbol{R}$-álgebras. E se f é epimorfismo (monomorfismo) então f^* é epimorfismo (monomorfismo).*

Observe que se $H = \{1\}$, então a proposição anterior mostra que a aplicação $G \to \{1\}$ induz a um homomorfismo de anéis $e : \mathbf{R}G \to R$ tal que

$$e(\alpha) = e(\sum_{g \in G} a_g g) = \sum_{g \in G} a_g.$$

Definição 2.4 *O homomorfismo e anterior é denominado **aplicação de aumento** de $\boldsymbol{R}G$, e seu núcleo, denotado por $\triangle(G)$ é chamdo **ideal de aumento** de $\boldsymbol{R}G$.*

Note que se $\alpha = (\sum_{g\in G} a_g g)$ pertence a $\triangle(G)$, então

$$e(\alpha) = e(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g = 0.$$

Assim

$$\alpha = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g(g-1).$$

Proposição 2.3 *O conjunto* $\{g-1 : g \in G; g \neq 1\}$ *é uma base de* $\triangle(G)$ *sobre* R*, isto é,*

$$\triangle(G) = \{\sum_{g\in G} a_g(g-1) : g \in G; g \neq 1; a_g \in \boldsymbol{R}\}.$$

2.2.1 Ideais de aumento

Dados um grupo G e um anel $\mathbf{R}$ denotamos por $S(G)$ o conjunto de todos os subgrupos de G e por $I(\mathbf{R}G)$ o conjunto de todos os ideais a esquerda de $\mathbf{R}G$.

Seja $H \in S(G)$ um subgrupo. Denotamos por $\triangle_g(G,H)$ o ideal a esquerda de $\mathbf{R}G$ gerado por $\{h-1 : h \in H\}$, isto é

$$\triangle_g(G,H) = \{\sum_{h\in H} \alpha_h(h-1) : \alpha_h \in \mathbf{R}\}.$$

Quando estivermos trabalhando com um anel $\mathbf{R}$ fixo, denotaremos por $\triangle(G,H)$.

Lema 2.1 *Seja* H *um subgrupo de um grupo* G *e seja* S *um conjunto de geradores de* H*. O conjunto* $\{s-1 : s \in S\}$ *é um conjunto de geradores de* $\triangle(G,H)$ *como um ideal a esquerda de* $\boldsymbol{R}G$*.*

Para melhor descrevermos $\triangle_R(G,H)$ denotaremos por $\phi = \{q_i\}_{i\in I}$ um conjunto completo de representantes de classes a esquerda de H em G. Escolhemos para representante da classe H em ϕ o elemento identidade de G. Assim, todo elemento $g \in G$ pode ser escrito de única forma como $g = q_i h_j$, onde $q_i \in \phi$ e $h_j \in H$.

Proposição 2.4 *O conjunto* $B_H = \{q(h-1) : q \in \phi; h \in H; h \neq 1\}$ *é uma base de* $\triangle_R(G,H)$ *sobre* $\boldsymbol{R}$*.*

Se H é um subgrupo normal de G então o homomorfismo canônico $w : G \to G|H$ pode ser estendido ao epimorfismo $w^* : \mathbf{R}G \to \mathbf{R}(G|H)$ tal que

$$w^*(\alpha) = w^*(\sum_{g\in G} a(g)g) = \sum_{g\in G} a(g)w(g).$$

Corolário 2.2 *Seja* H *um subgrupo normal de* G*. Então* $\triangle(G,H)$ *é um ideal bilateral de* $\boldsymbol{R}G$ *e*

$$\frac{\boldsymbol{R}G}{\triangle(G,H)} \simeq \boldsymbol{R}(G|H)$$

2.2.2 Semissimplicidade

Definição 2.5 *Seja X um subconjunto de um anel de grupo $\boldsymbol{R}G$. O* ***anulador à esquerda*** *de X é o conjunto*

$$Ann_l = \{\alpha \in \boldsymbol{R}G : \alpha x = 0; \forall x \in X\}.$$

analogamente, temos o **anulador à direita** de X

$$Ann_r = \{\alpha \in \mathbf{R}G : x\alpha = 0; \forall x \in X\}$$

Dados um anel de grupo $\mathbf{R}G$ e um subconjunto finito X do grupo G. Denotaremos por $X^{'}$ o seguinte elemento de $\mathbf{R}G$:

$$X^{'} = \sum_{x \in X} x.$$

Lema 2.2 *Seja H um subgrupo de G e $\boldsymbol{R}$ um anel. O $Ann_r(\triangle(G,H)) \neq \varnothing$ se, e só se H é finito. Neste caso, temos $Ann_R(\triangle(G,H)) = H^{'} * \boldsymbol{R}G$. Além disso, se H é um subgrupo normal de G então o elemento $H^{'}$ é central em $\boldsymbol{R}G$ e temos*

$$Ann_r(\triangle(G,H)) = Ann_l(\triangle(G,H)) = \boldsymbol{R}G * H$$

Lema 2.3 *Seja I um ideal bilateral de um anel $\boldsymbol{R}$. Suponha que exista um ideal à esquerda J tal que $\boldsymbol{R} = I \oplus J$, como $\boldsymbol{R}$-módulos à esquerda. Então $J \subset Ann_r(I)$.*

Lema 2.4 *Se o ideal de aumento $\triangle(G) = \triangle(G,G)$ é um somando direto de $\boldsymbol{R}G$, como um $\boldsymbol{R}G$-módulo, então G é finito e $|G|$ é invertível em $\boldsymbol{R}$.*

Teorema 2.4 ***(Teorema de Maschke)*** *Seja G um grupo, o anel de grupo $\boldsymbol{R}G$ é semissimples se, e só se valem as seguintes condições:*

i) $\boldsymbol{R}$ *é um anel semissimples;*

ii) G é um grupo finito;

iii) $|G|$ é invertível em $\boldsymbol{R}$.

Corolário 2.3 *Seja G e $\mathbf{K}$ um corpo finito. Então $\mathbf{K}G$ é semissimples se, e só se, $car(\mathbf{K}) \nmid |G|$.*

CAPÍTULO 3

CÓDIGOS DE GRUPO

Baseados, especialmente no estudo desenvolvido em [2], iremos apresentar neste capítulo, um pouco sobre os códigos de grupo. Que são códigos que possuem como base a estrutra de álghebras de grupo.

Um **código de grupo** (à esquerda) de comprimento n é um código linear que é imagem de um ideal (à esquerda) de uma álgebra de grupo via um isomorfismo

$$\mathbf{K}G \to \mathbf{K}^n$$

que aplica G na base canônica de $\mathbf{K}^n$.

Definição 3.1 *Se G é um grupo de ordem n e $C \subset \mathbf{K}^n$ é um código linear então C é um G-código (à esquerda) se existe uma bijeção entre a base canônica de $\mathbf{K}^n$ e G que se estende a um isomorfismo $\mathbf{K}^n \to \mathbf{K}G$ que aplica C em um ideal (à esquerda) de $\mathbf{K}G$.*

Logo, um código de grupo (à esquerda) é, na verdade, um código linear que é um G-código (à esquerda) para algum grupo G. Mediante a tal aspecto, o código a ser estudado está relacionado ao grupo que será abordado, para darmos continuação a nossa pesquisa, trabalharemos com os grupos cíclicos, ou seja, estudaremos, a partir de agora, os **códigos de grupos cíclicos**.

3.1 Códigos de grupos cíclicos

Sejam $\mathbf{K}$ um corpo e $G = \{1, a, ..., a^{n-1}\}$ um grupo cíclico de ordem n, tal que $car(\mathbf{K}) \nmid |G|$. Observe que a álgebra de grupo $\mathbf{K}G$ de G sobre $\mathbf{K}$ é um $\mathbf{K}$-espaço vetorial de dimensão n, assim, isomorfo a $\mathbf{K}^n$.

Consideremos o seguinte isomorfismo linear:

$$\varphi : \qquad K^n \qquad \to \qquad \mathbf{K}G$$

$$(c_o, ..., c_{n-1}) \mapsto c_0 + c_1 a + ... + c_{n-1}a^{n-1}.$$

Graças ao isomorfismo acima, temos que cada palavra de um códico $C \subset \mathbf{K}^n$ está relacionada a um elemento de anel de grupo $\mathbf{K}G$. Além do mais, se $c = (c_o, ..., c_{n-1}) \in C$, temos que o peso de C é $w(c) = |supp(\varphi(c))|$.

Considere o epimorfismo:

$$\theta : \qquad K[x] \to \mathbf{K}G$$

$$f(x) \mapsto f(a)$$

Como resultado de homomorfismo de anéis, temos que

$$\mathbf{K}G \simeq \frac{\mathbf{K}[\mathbf{x}]}{Ker(\theta)}$$

Proposição 3.1 $Ker(\theta) =< x^n - 1 >$

Demonstração: Note que dado $q(x) \in (x^n - 1)$, temos $q(x) = f(x)(x^n - 1)$, onde $f(x) \in \mathbf{K}[x]$. Segue que $\theta(q(x)) = q(a) = f(a)(a^n - 1) = f(a)0 = 0$, isto é, $(x^n - 1) \in ker(f)$.

Por outro lado, seja $f(x) \in ker(\theta)$. Pelo algorítmo da divisão existem $q(x)$ e $r(x) \in \mathbf{K}[x]$ tais que

$$f(x) = q(x)(x^n - 1) + r(x),$$

onde

$r(x) = b_0 + b_1 a + ... + b_{n-1}a^{n-1}$.

Assim,

$$f(a) = q(a)(a^n - 1) + r(a),$$

como $f(x) \in ker(\theta)$ e $(a^n - 1) - 0$ segue que $r(a) = 0$, logo
$b_0 + b_1 x + ... + b_{n-1}x^{n-1} = 0$, e como $\{1, a, ..., a^{n-1}\}$ é uma base de $\mathbf{K}G$ então $r(x) = 0$.

Portanto, $f(x) = q(x)(x^n - 1) \Leftrightarrow f(x) \in (x^n - 1)$. ■

Observe que com o resultado obtido anteriormente e com elementos já estudados temos:

$$\mathbf{K}G \simeq \frac{\mathbf{K}[\mathbf{x}]}{Ker(\theta)} = \frac{\mathbf{K}[x]}{< x^n - 1 >} = \mathbf{R}_n$$

Proposição 3.2 *Seja $G =< a >$ um grupo cíclico de ordem n gerado por a. Todo ideal de $\mathbf{K}G$ é da forma $\mathbf{K}Gf(a)$, onde $f(x)$ é um divisor de $(x^n - 1)$.*

Demonstração: Lembremos que os ideais de R_n são gerados por $f(x) \in \mathbf{K}[x]$, onde $f(x)$ é um divisor de $(x^n - 1)$. E como $\mathbf{K}G$ é isomorfo a R_n, o resultado segue de imediato. ∎

Diante disso, temos que um código $C \in \mathbf{K}^n$ é cíclico se, e só se, $\varphi(C)$ é da forma $\mathbf{K}Gf(a)$, onde $f(x) \in \mathbf{K}[x]$ é um divisor de $(x^n - 1)$.

Observação 3.1 *Qaundo $g(x)$ for um divisor de (x^n-1), denotaremos por $h(x)$ o quociente*

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

Definição 3.2 *Seja $\varphi(C) = \mathbf{K}Gg(a)$ um código cíclico. Denominamos $g(a)$ por **gerador principal** de C.*

Podem haver vários geradores para $\varphi(C)$, entretanto estamos interessados no que é oriundo da fatoração do polinômio $(x^n - 1)$. Considerando, por abuso de notação $C =< g(a) >$ e $\alpha \in C$ temos que $\alpha = k(a)g(a)$, onde $k(a) \in \mathbf{K}G$ e $g(x) \in \mathbf{K}[x]$.

Proposição 3.3 *Um elemento $g(a)$ pertence a $\mathbf{K}Gg(a)$ se, e só se, $f(a)h(a) = 0$ em $\mathbf{K}G$.*

Demonstração: Seja$f(a) \in \mathbf{K}Gf(a)$. Assim, $f(a) = \lambda(a)g(a)$, onde $\lambda(a) \in \mathbf{K}G$. Logo, $f(a)h(a) = \lambda(a)g(a)h(a)$, ou seja, $f(a)h(a) = \lambda(a)(a^n - 1) = 0$.

Por outro lado, suponha $f(a)h(a) = 0$ pertencentes a $\mathbf{K}G$. Como $g(x), h(x)$ são relativamente primos, existem $r(x), s(x) \in \mathbf{K}[x]$ tais que

$$r(x)g(x) + s(x)h(x) = 1;$$

Daí,

$$r(a)g(a) + s(a)h(a) = 1 \Longrightarrow f(a)r(a)g(a) + f(a)s(a)h(a) = f(a)$$

Como G é um grupo cíclico, $\mathbf{K}$ é um corpo e , por hipótese, $f(a)g(a) = 0$ então

$$f(a)r(a)g(a) = f(a)s(a)h(a) = 0;$$

Portanto, $f(a) \in \mathbf{K}G$ ∎

Observação 3.2 *O elemento $h(a)$ recebe o nome de **elemento de teste** do código $C =< g(a) >$.*

3.2 Matriz geradora e Matriz teste de paridade

No escopo do presente trabalho já determinou-se matriz geradora e a matriz teste de paridade para códigos cíclicos sobre o corpo $\mathbf{k}^n$, mediante a isomorfismos determinares tais matrizes em $\mathbf{K}G$, relaconando $\mathbf{K}^n$ com $\mathbf{K}G$.

Teorema 3.1 *Seja* $\mathbf{K}Gg(a)$ *onde* $g(x) = g_0 + g_1x + ... + g_sx^s$ *é um divisor de* $(x^n - 1)$ *de grau s. Então* $B = \{g(a), ag(a), ..., a_{n-s-1}g(a)\}$ *é uma base de I como espaço vetorial sobre* $\mathbf{K}$*, a dimensão de I é* $n - s$ *e do código* $C = \varphi^{-1}(I)$ *possui matriz geradora*

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

Demonstração:

Segue do teorema (1.5) e também, pelo fato de $R_n \simeq \mathbf{K}G$. ■

Observação 3.3 *Lembremos que dado um polinômio* $p(x) = p_0 + p_1x^1 + ... + p_tx^t$*, denominamos o polinômio* $p^*(x)$ *por* ***polinômio recíproco*** *de* $p(x)$*, onde*

$$p^* = x^t f(x^{-1}) = p_t + p_{t-1}x + ... + p_0x^t.$$

3.3 Utilização do GAP no Estudo de Códigos de Grupo

O software GAP é um recurso computacional (software) livre, que pode ser instalado direto de sua página inicial $www.gap-system.org$, e que é voltado para o estudo de álgebra cujo intuito é o de facilitar a pesquisa e o ensino de teorias relacionadas com contextos mais abstratos, de modo que os algoritmos do programa efetuem cálculos que por muitas vezes são trabalhosos e possibilitem a visualização de diversas estruturas.

O GAP (Groups, Algorithms, and Programming) é uma poderosa ferramenta computacional voltada para a manipulação de estruturas algébricas, especialmente grupos, e tem se mostrado extremamente útil no estudo de códigos corretores de erros, especificamente no contexto de códigos de grupo. A teoria algébrica de códigos corretores de erros utiliza estruturas como grupos finitos para criar e analisar códigos que são capazes de detectar e corrigir erros em transmissões de dados.

No estudo de códigos de grupo, o GAP permite a construção de grupos e seus subgrupos, além de possibilitar operações com anéis, módulos e espaços vetoriais, elementos essenciais para a teoria dos códigos. O software oferece funcionalidades para verificar propriedades estruturais de grupos e realizar cálculos que seriam inviáveis de serem realizados manualmente, especialmente quando se lida com grupos de alta ordem.

Entre as aplicações do GAP para códigos de grupo, destacam-se:

- Construção e análise de exemplos de códigos de grupo: Utilizando os grupos finitos e seus subgrupos, o GAP pode ser utilizado para construir códigos lineares baseados em grupos e estudar suas propriedades, como peso, distância mínima e dimensão.
- Análise da estrutura do grupo: GAP oferece ferramentas para determinar geradores, relações e decomposições de grupos, o que é essencial para a construção de códigos com boas propriedades corretoras de erros.
- Verificação de propriedades de códigos: O GAP pode calcular parâmetros importantes, como a distância mínima entre palavras-código, determinando a eficiência e a capacidade de correção de erros do código construído.

Assim, o GAP é uma ferramenta fundamental para pesquisadores na área de teoria algébrica dos códigos, permitindo a exploração de códigos de grupo de maneira sistemática e eficiente.

Neste trabalho, nos baseamos nos estudos feitos em [1] para compreender um pouco das funcionalidades do GAP e especialmente suas aplicações na teoria de grupos. A estrutura de grupos, em especial dos grupos finitos, é fundamental no estudo dos códigos de grupo. Foi possível apenas nos familiarizar com o software e compreender comandos práticos envolvendo grupos, porém se abriram diversas perspectivas de novas pesquisas envolvendo o GAP e a teoria de códigos, já que o software pode facilitar consideravelmente muitos cálculos.

CONSIDERAÇÕES FINAIS

No presente trabalho abordamos diversos aspectos que envolvem a teoria matemática de comunicação, tendo como objeto principal os códigos corretores de erros, e dentro desse universo abordamos os principais códigos que envolvem tal teoria, como os códigos lineares, códigos duais, códigos cíclicos. Além do mais, realizamos alguns estudos acerca de álgebras de grupo, especificamente, abordando os assuntos de módulos e anéis de grupo, e com tal bagagem teórica, pode-se realizar o estudo básico acerca dos códigos de grupo, trabalhando fundamentos de um código de grupo específco, que são os códigos de grupos cíclicos.

O software GAP mostrou-se como uma ferramenta bastante útil para aprofundamento em pesquisas de códigos de grupos cíclicos, visto que tal teoria está fundamentada na estrutura algébica de anéis de grupo, onde o software comporta e possibilita estudo sobre tal ente matemático, uma vez que o GAP possui inúmeras ferramentas prontas em sua biblioteca que abordam tópicos de tal teoria e, além do mais, nele é possível implementar comandos que corroborem para se estudar tais entes matemáticos. Logo, por mais que não se tenha trabalhado, de forma incisiva, no software, claramente ele pode ser encarado como uma ferramenta catalisadora para resultados em pesquisas mais aprofundadas acerca da teoria algébrica dos anéis de grupo.

Portanto, o projeto atendeu a proposta de veicular elementos substanciais para a compreensão das teorias que fundamentam os códigos de grupo, contendo uma projeção organizacional voltada para apresentação dos principais elementos que alicerçam tal teoria matemática e cumpre também o papel de ser uma "base" para avanços em pesquisas, de modo que contribua para construção de novos teoremas, proposições e também seja uma base sólida para desenvolvimento de áreas que possuam aplicação matemática fundamentadas nos tópicos abordados.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] CRUZ, G. S. *O uso do GAP no estudo da teoria de grupos*. Trabalho de Conclusão de Curso (Graduação em Licenciatura em Matemática) – Departamento de Matemática Pura e Aplicada - CCENS, Universidade Federal do Espírito Santo, (2024).

[2] COSTA, R. B. *Código de grupo cíclico*. Trabalho de Conclusão de Curso (Graduação em Licenciatura em Matemática) – Departamento de Matemática Pura e Aplicada - CCENS, Universidade Federal do Espírito Santo, (2022).

[3] GONÇALVES, A. *Introdução à Álgebra*. Projeto Euclides, IMPA, Rio de Janeiro, (2006).

[4] HEFEZ, A. e VILELA, M. L. T. *Códigos Corretores de Erros*, Rio de Janeiro, IMPA, (2002).

[5] MILIES, C. P.; SEHGAL, S. K. *An introduction to group rings*. Dordrecht: Kluwer Academic Publishers, (2002).