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

RELATÓRIO DE INICIAÇÃO CIENTÍFICA

Códigos e reticulados

Discente: *Matheus Lopes Tolezano*
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 E RETICULADOS

Apresentamos os códigos corretores de erros sob o ponto de vista algébrico, demonstrando os benefícios de se mesclar códigos e estruturas algébricas: melhores e mais sofisticados algoritmos de codificação e decodificação de erros. O principal objetivo é estudar elementos geométricos envolvidos na teoria de códigos e assim utilizar toda a base algébrica mesclada a uma visualização geométrica de alguns importantes conceitos. Com isso, a estrutura algébrica a qual estamos interessado é a de reticulados. A partir da associação da teoria de códigos com reticulados, apresentamos o que chamamos de "Construção A".

Palavras-chave: Códigos algébricos. Códigos geométricos. Reticulados. Teoria da informação.

INTRODUÇÃO

A teoria de códigos corretores de erros é uma parte de uma área conhecida como teoria da informação. Essa teoria fundada pelo matemático Claude E. Shannon ganhou força a partir da década de 70 com as pesquisas espaciais e a grande popularização dos computadores.

Os códigos participam do nosso cotidiano de inúmeras formas, estando presente sempre que fazemos o uso de informações digitalizadas, por exemplo, ao assistirmos um programa de televisão, falar ao telefone, mandar mensagem para alguém via pager e até mesmo ao navegarmos pela internet. Um código é um modo organizado de transmitir ou armazenar informações, que permita, ao recuperar a informação, detectar e corrigir erros. Um exemplo clássico de um código corretor de erro é um idioma. Para entendê-lo, vamos analisar a seguinte situação: se uma mensagem de texto é recebida com a palavra **LIÃO**, é possível detectar o erro rapidamente pois a palavra não existe no idioma. Com isso, a palavra é corrigida para **LEÃO**, que é a palavra "mais próxima" e, neste caso, foi possível corrigir o erro. Entretanto, se a mensagem recebida é **ZEIA**, é possível detectar o erro, mas não é possível corrigí-lo, pois existem muitas palavras no idioma que estão próximas dela. E ainda, existe o caso em que não é possível detectar o erro. Se recebermos a palavra **VISTA**, quando na verdade a mensagem original é **MISTA**, é impossível a correção, já que **VISTA** é uma palavra do idioma.

Para ilustrar os princípios dessa teoria, vamos analisar um exemplo. Suponha que exista um robô que se move sobre um tabuleiro quadriculado de modo que robô se desloque para as seguintes posições Leste, Oeste, Norte e Sul e que o mesmo se desloque sempre do centro de uma casa, para o centro de outra por meio de um comando. Os quatro comandos podem ser codificados como elementos de $\{0,1\}^2$:

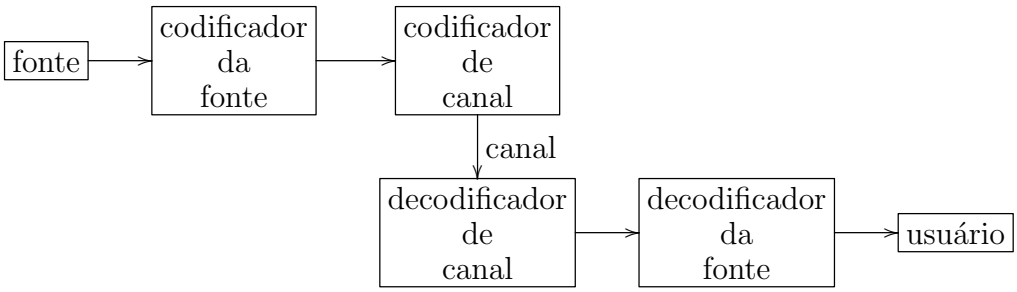
$$\text{Leste} \longmapsto 00 \qquad \text{Norte} \longmapsto 10$$
$$\text{Oeste} \longmapsto 01 \qquad \text{Sul} \longmapsto 11$$

O código ao lado direito das coordenadas acima é chamado de **código da fonte**. Vamos supor agora que esses pares serão transmitidos via rádio e que durante o processo de transmissão, ocorra algum tipo de interferência e ruídos. Suponha também que, ao enviarmos a mensagem 00, na chegada, recebemos como 01, fazendo com que o robô se desloque para Oeste ao invés de ir para Leste. O que é feito então, é a recodificação das palavras de modo a introduzir redundâncias que permitam a detecção do erro. A partir disso, podemos modificar o nosso código como se segue:

$$00 \longmapsto 00000$$
$$01 \longmapsto 01011$$
$$10 \longmapsto 10110$$
$$11 \longmapsto 11101$$

Nessa recodificação, as duas primeiras posições reproduzem o código da fonte, e as três posições restantes são redundâncias introduzidas. O novo código introduzido na recodificação é chamado de **código de canal**. Suponhamos que se tenha introduzido um erro ao transmitirmos a palavra 01011, de modo que a mensagem recebida seja 01111. Ao compararmos essa mensagem com as palavras do código, percebemos que não lhe pertence e, portanto, o erro é detectado. A palavra mais próxima do código (a que tem menor número de componentes diferentes) é 01011, que é justamente a palavra transmitida.

A figura abaixo ilustra o processo de detecção e correção de erros.



Um tipo de código bem conhecido é o registro ISBN (International Standard Book Number) de um livro. Um elemento desse código é uma sequência de nove dígitos seguidos de um dígito de controle, $n_1n_2n_3...n_9 - n_{10}$, onde n_i é inteiro entre 0 e 9, para $i = 1, ..., 9$ e o dígito de controle n_{10} é obtido da forma:

$$n_{10} = 11 - \left(\sum_{i=1}^{9} (11 - i)n_i) \right) \text{mod} 11 .$$

Assim, o controle n_{10} poderá ser $0, 1, 2, ..., 9$ ou 10, sendo que neste último caso representa-se por X. Uma pergunta natural é: por que definir uma expressão como esta para o controle? Note, por exemplo, que se definíssemos o dígito de controle para o registro de livros por uma expressão mais simples, como fazer a soma dos dígitos módulo 10, o controle não detectaria a troca de ordem na digitação, que é um erro muito comum. O código ISBN é um exemplo de código que detecta (embora não corrija) um erro.

Uma outra área que exploramos neste trabalho corresponde ao estudo dos reticulados. Os reticulados têm se revelado extremamente úteis em aplicações de telecomunicações e na criptografia "pós-quântica". Além disso, do ponto de vista teórico, eles despertam o interesse de muitos pesquisadores. Basicamente, quando estudamos reticulados, no geral, o que estamos buscando é, fixada uma dimensão, qual é o melhor reticulado nesta dimensão em relação a uma propriedade. A partir disso, podemos dizer que um reticulado pode ser "bom" em algum aspecto, mas não ser "bom" em outro.

Um empacotamento esférico em $\mathbb{R}^n$ é uma reunião de esferas de mesmo raio em $\mathbb{R}^n$ de modo que duas esferas quaisquer deste arranjo apenas se toquem no bordo, ou não possuam interseção alguma. Além disso, queremos que este arranjo ocupe o "maior espaço possível". Já um empacotamento reticulado em $\mathbb{R}^n$, é um empacotamento esférico cujo o conjunto dos centros das esferas forma um reticulado.

O problema de encontrar o empacotamento esférico que cobre a maior parte do espaço foi relacionado à teoria dos códigos corretores de erros em 1948 por Claude E. Shannon e, a partir disso, neste trabalho buscou-se uma relação entre a teoria de códigos e conceitos sobre reticulados. Essa relação entre conceitos de códigos e reticulados chamamos de "Construção A", assunto que será abordado na Seção 2.5.

O presente trabalho está dividido em dois capítulos. No primeiro capítulo veremos alguns conceitos básicos sobre códigos corretores de erros, e a classe de código a qual será trabalhado, os códigos lineares. Além disso, são abordados alguns conceitos a mais como as matrizes geradoras de um código, códigos duais, um algoritmo de decodificação e, por fim, um outro tipo de métrica bastante utilizada ao adaptarmos à classe de códigos q-ários: a métrica de Lee. No segundo capítulo, começamos a introduzir a teoria de reticulados, com foco em

reticulados no plano. Em seguida, são apresentadas as regiões fundamentais e densidade, alguns resultados importantes sobre a matriz de Gram, determinante de um reticulado além de uma breve apresentação sobre reticulados congruentes e reticulados equivalentes. Por fim, será definida a Construção A, uma aplicação que relaciona a classe de códigos lineares mencionada anteriormente à teoria de reticulados.

CAPÍTULO 1

CÓDIGOS CORRETORES DE ERROS

Nosso capítulo inicial tem por objetivo trazer os principais conceitos da teoria de códigos, assim como apresentados em [3]. Para entendimento dos conceitos básicos algébricos também sugerimos uma consulta a textos básicos de estruturas algébricas, como [2] e a algum texto de álgebra linear básica, como por exemplo [4]. Ao longo do capítulo, elementos de [5] também foram utilizados como parâmetro e consequentemente norteando o trabalho que tem por um de seus objetivos mesclar conceitos geométricos e algébricos da teoria de códigos. Para uma visão mais geral sobre os códigos algébricos, sugerimos como texto introdutório o trabalho [1].

1.1 Conceitos básicos

Seja A um conjunto finito com q elementos ($|A| = q$), um **código corretor de erros**, C, de comprimento n é um subconjunto próprio de A^n. Cada elemento de C é chamado de palavra do código (no alfabeto A). Seja $m = |C|$ o número de palavras no código. A **taxa de informação** de C é definida como:

$$R(C) = \frac{\log_q m}{n}$$

A taxa de informação permite, de certa forma, compararmos a eficiência de códigos de diferentes tamanhos.

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

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

Por exemplo, em $\{0,1\}^3$, temos

$$d(001,111) = 2$$
$$d(000,111) = 3$$
$$d(100,110) = 1$$

Geometricamente, para $A = \mathbb{Z}_2$, temos que $\mathbb{Z}_2^n$ são os vértices de um hipercubo em $\mathbb{R}^n$ e códigos binários são subconjuntos destes conjuntos de vértices. A distância de Hamming em $\mathbb{Z}_2^n$ entre dois destes vértices é dada pelo caminho com menor número de arestas conectando estes vértices.

Exemplo 1.1 *Vamos considerar os seguintes códigos:*

$$C_1 = \{(1,1,1),(0,0,0)\} \subset \mathbb{Z}_2^3$$

e

$$C_2 = \{(1,1,1,0),(0,0,0,0),(1,0,0,1),(1,1,1,1)\} \subset \mathbb{Z}_2^4.$$

Conseguimos identificar a distância mínima e distância máxima por meio da Figura 1.1 abaixo:

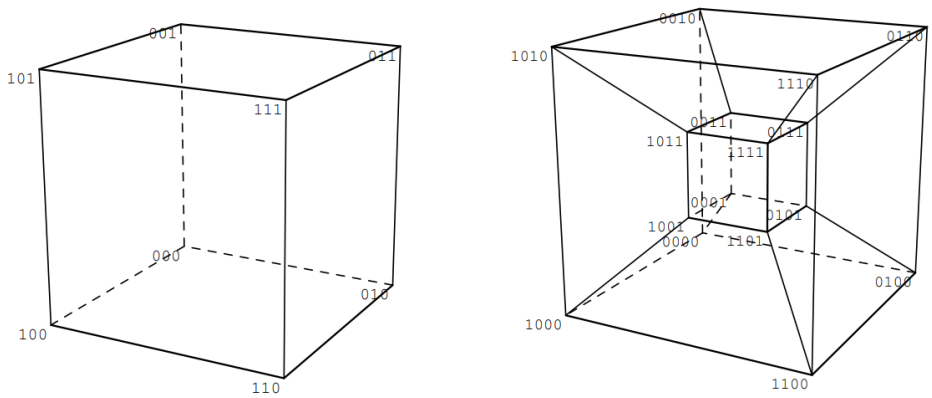


Figura 1.1

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

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

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

$$|D(a,r)| = \sum_{i=0}^{r} \left(\begin{array}{c} n \\ i \end{array} \right) (q-1)^i.$$

Definição 1.2 *Seja C um código. A distância mínima de C é o número*

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

Dado um código C com distância mínima d, define-se

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

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*

$$D(c,\kappa) \cap D(c',\kappa) = \emptyset.$$

Demonstração: Sejam c e c' $\in C$. Suponha por absurdo que existe $x \in D(c,\kappa) \cap D(c',\kappa)$, logo $x \in D(c,\kappa)$ e $x \in D(c',\kappa)$ então $d(c,x) \leq \kappa$ e $d(c',x) \leq \kappa$. Por desigualdade triangular, simetria e pela definição acima de κ, temos que,

$$d(c,c') \leq d(c,x) + d(x,c') = d(c,x) + d(c',x) \leq 2\kappa \leq d-1,$$

um absurdo, pois pela Definição 1.2, $d(c,c') \geq d$, ou seja, a distância mínima d não pode ser maior do que a distância entre c e c'. ■

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

Demonstração: Se ao transmitirmos uma palavra $\mathbf{c}$ do código cometemos t erros com $t < \kappa$, recebendo a palavra $\mathbf{r}$, então $d(\mathbf{r},\mathbf{c}) = t \leq \kappa$; enquanto que, pelo Lema 1.2, a distância de $\mathbf{r}$ a qualquer outra palavra do código é mais do que κ. Isso determina $\mathbf{c}$ univocamente a partir de $\mathbf{r}$.
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 1.3 *Seja $C \subset A^n$ um código com distância mínima d e seja $\kappa = \left[\frac{d-1}{2}\right]$. O código C será dito perfeito se*

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

Exemplo 1.2 *Vamos criar um código fonte e um código de canal para um robô que se desloca num tabuleiro tridimensional e que levanta e abaixa cada braço separadamente. Suponha que o nosso robô esteja na seguinte posição inicial*

Figura 1.2: Posição inicial.

Seja $\{0,1\}^3$. Daí, temos que

$$\begin{array}{lll} Leste \to 000 & Sul \to 011 & A.E \to 110 \\ Oeste \to 001 & L.E \to 100 & A.D \to 111 \\ Norte \to 010 & L.D \to 101 & \end{array}$$

é o nosso *código fonte*, onde L.E = Levantar braço esquerdo; L.D = Levantar braço direito; A.E = Abaixar braço esquerdo; A.D = Abaixar braço direito.
A partir disso, criamos nosso código de canal:

$$\begin{array}{lll} 000 \to 0000000 & 011 \to 0111010 & 110 \to 1101000 \\ 001 \to 0011100 & 100 \to 1001101 & 111 \to 1110100 \\ 010 \to 0100110 & 101 \to 1010110 & \end{array}$$

Note que a distância mínima é $d = 3$. Daí, temos que o código pode corrigir até $\kappa = 1$ erro e detectar até 2 erros.

Exemplo 1.3 *Vejamos se é perfeito o código criado no Exemplo 1.2.*

Seja M o código criado no exemplo anterior. Sabemos que $M \subset \{0,1\}^7$ um código com distância mínima d, $\kappa = \left[\frac{d-1}{2}\right]$. O código M será perfeito se

$$\bigcup_{m \in M} D(m, \kappa) = \{0,1\}^7.$$

Do código M sabemos que $d = 3$ e portanto $\kappa = 1$. Para determinar sua cardinalidade, usaremos o Lema 1.1. Temos que,

$$1)|D(m_1,1)| = \sum_{i=0}^{1} \left(\begin{array}{c} 7 \\ i \end{array} \right) (2-1)^i = \left(\begin{array}{c} 7 \\ 0 \end{array} \right) . \, 1^0 + \left(\begin{array}{c} 7 \\ 1 \end{array} \right) . \, 1^1 = 8$$

$$2)|D(m_2,1)| = \sum_{i=0}^{1} \left(\begin{array}{c} 7 \\ i \end{array} \right) (2-1)^i = 8, \qquad m_i \in M$$

Recursivamente para as oito palavras do código M, teremos

$$|D(m_1,1)| = |D(m_2,1)| = ... = |D(m_8,1)| = 8.$$

Logo, $|D(m_1,1)| + |D(m_2,1)| + ... + |D(m_8,1)| = 64$ *palavras.*

Sabemos ainda que o espaço $\mathbb{F}_2^7$ possui 128 palavras.

Portanto, como $\bigcup_{m \in M} D(m,\kappa) \neq \{0,1\}^7$, o código M não é perfeito.

Exemplo 1.4 *Usando a estratégia citada no texto do caso do código do robô decodifiquemos as seguintes mensagens: 01011, 01101, 11011, 10011 e 10001.*

Vamos denotar o código do robô da seguinte maneira:

$$Leste = 00 \to 00000 \ (c_1) \quad Norte = 10 \to 10110 \ (c_3)$$
$$Oeste = 01 \to 01011 \ (c_2) \quad Sul = 11 \to 11101 \ (c_4)$$

Note que, a distância mínima do código acima é $d = 3$ e daí, $\kappa = 1$. Logo, pelo Teorema 1.1, o código pode corrigir até $\kappa = 1$ erro e detectar até 2 erros.

É fácil notar que, 01011 $\to$ Oeste, 01101 $\to$ sul e 11011 $\to$ Oeste.

Observe que nos casos acima, ao calcularmos $d(c_4, 01101)$ encontramos 1. Ou seja, o código detectou um erro e daí conseguimos concluir que a palavra está no disco de centro c_4 e portanto decodificamos a mensagem.

Note que no caso das mensagens 10011 e 10001, ao analisarmos, encontramos dois erros. Pelo teorema, o código M corrige até 1 erro. Logo, o código não é capaz de corrigir os erros e consequentemente não é possível decodificar as mensagens.

1.2 Códigos lineares

Denotaremos por $\mathbb{K}$ um corpo finito com q elementos tomado como alfabeto. Temos, portanto, para cada número natural n, um $\mathbb{K}$-espaço vetorial $\mathbb{K}^n$ de dimensão n.

Definição 1.4 *Um código $C \subset \mathbb{K}^n$ será chamado de código linear se for um subespaço vetorial de $\mathbb{K}^n$.*

O código do robô da Introdução deste trabalho é um código linear, pois o alfabeto nesse caso é $A = \mathbb{F}_2$, o corpo de Galois, e o código é o subespaço vetorial de $\mathbb{F}_2^5$, imagem da transformação linear

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

Todo código linear é por definição um espaço vetorial de dimensão finita. Seja k a dimensão do código C e seja $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ uma de suas bases. Daí, todo elemento de C se escreve de modo único na forma

$$\lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2 + ... + \lambda_k \mathbf{v}_k,$$

onde os λ_i, $i = 1, ..., k$, são elementos de $\mathbb{K}$. Segue daí que

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

e, consequentemente,

$$dim_K C = \log_q q^k = \log_q M.$$

Se C for um código linear de dimensão k de $\mathbb{F}^n$, a taxa de informação de C será

$$R(C) = \frac{k}{n}.$$

A taxa de informação do código do Exemplo 1.2 é $\frac{\log_2 2^7}{8} = 0,875$.

Definição 1.5 *Dado $\mathbf{x} \in \mathbb{K}^n$, define-se o peso de x como sendo o número inteiro*

$$\omega(\mathbf{x}) \equiv |\{i : x_i \neq 0\}|.$$

Em outras palavras, temos que

$$\omega(\mathbf{x}) = d(\mathbf{x}, 0),$$

onde d representa a métrica de Hamming.

Definição 1.6 *O peso de um código linear C é o inteiro*

$$\omega(C) \equiv min\{\omega(\mathbf{x}) : \mathbf{x} \in C \backslash \{0\}\}.$$

Proposição 1.1 *Seja $C \subset \mathbb{K}^n$ um código linear com distância mínima d. Temos que*

i) $\forall \mathbf{x}, \mathbf{y} \in \mathbb{K}^n$, $d(\mathbf{x}, \mathbf{y}) = \omega(\mathbf{x} - \mathbf{y})$.
ii) $d = \omega(C)$.

Note que a proposição acima nos mostra que, em códigos lineares com M elementos, podemos calcular a distância mínima d a partir de $M - 1$ cálculos de distâncias, em vez dos $\begin{pmatrix} M \\ 2 \end{pmatrix}$ cálculos anteriormente requeridos. Na prática, em códigos grandes, esse método para o cálculo de d é inviável pois representa um custo computacional muito elevado.

Em virtude da Proposição 1.1 (ii), a distância mínima de um código linear C será também chamada de *peso do código C*.

Na álgebra linear, temos duas maneiras práticas de se escrever subespaços vetoriais C de um espaço vetorial $\mathbb{K}^n$, uma como imagem e outra como núcleo de transformações lineares.

Vejamos como se obtém a representação de C como imagem de uma transformação linear. Escolha uma base $\{v_1, v_2, ..., v_k\}$ de C e considere a aplicação linear

$$\begin{array}{rccc} T: & \mathbb{K}^k & \longrightarrow & \mathbb{K}^n \\ & \mathbf{x} = (x_1, ..., x_k) & \longmapsto & x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + ... + x_k\mathbf{v}_k \end{array}$$

Temos que T é uma transformação linear injetora, tal que $Im(T) = C$.

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

$$T : \mathbb{K}^k \longrightarrow \mathbb{K}^n$$

e definir $C = Im(T)$. Essa é a forma paramétrica do subespaço C, pois os elementos de C são parametrizados pelos elementos $\mathbf{x}$ de $\mathbb{K}^k$ através de T, tornando fácil gerar todos os elementos de C. Note que nessa representação, é, porém, difícil decidir se um dado elemento $\mathbf{v}$ de $\mathbb{K}^n$ pertence ou não a C pois, para isso, é necessário resolver o sistema de n equações nas k incógnitas $x_1, ..., x_k$ abaixo

$$x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + ... + x_k\mathbf{v}_k = \mathbf{v}.$$

Essa resolução, em geral, representa um alto custo computacional. A outra maneira de descrevermos um código C é através do núcleo de uma transformação linear. Sendo assim, tome um subespaço C' de $\mathbb{K}^n$ complementar de C, isto é,

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

e considere a aplicação linear

$$\begin{array}{rccc} H: & C \oplus C' & \longrightarrow & \mathbb{K}^{n-k} \\ & \mathbf{u} \oplus \mathbf{v} & \longmapsto & \mathbf{v} \end{array}$$

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

Exemplo 1.5 *A representação dada do código do robô é a representação paramétrica. Vamos representar esse mesmo código como núcleo de uma transformação linear.*

Seja C o código do robô e defina

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

Daí,

$$\begin{aligned} Ker(T) &= \{(x_1, x_2) \in \mathbb{F}_2^2 : T(x_1, x_2) = (0, 0, 0, 0, 0)\} \\ Ker(T) &= \{(x_1, x_2) \in \mathbb{F}_2^2 : (x_1, x_2, x_1, x_1 + x_2, x_2) = (0, 0, 0, 0, 0)\} \end{aligned}$$

Portanto, resolvendo o sistema encontramos $x_1 = 0$ e $x_2 = 0$.

Temos que,

$$\begin{aligned} Ker(T) &= \{(x_1, x_2, x_1, x_1 + x_2, x_2) : x_1, x_2 \in \mathbb{F}_2\} \\ Ker(T) &= \{(x_1, 0, x_1, x_1, 0) + (0, x_2, 0, x_2, x_2) : x_1, x_2 \in \mathbb{F}_2\} \\ Ker(T) &= \{x_1(1, 0, 1, 1, 0) + x_2(0, 1, 0, 1, 1) : x_1, x_2 \in \mathbb{F}_2\} \\ Ker(T) &= \langle (1, 0, 1, 1, 0), (0, 1, 0, 1, 1) \rangle. \end{aligned}$$

Exemplo 1.6 *Dada a transformação linear*

$$\begin{array}{rccc} T: & \mathbb{F}_2^6 & \longrightarrow & \mathbb{F}_2^3 \\ & (x_1, ..., x_6) & \longmapsto & (x_1 + x_4, x_1 + x_2 + x_3 + x_5, x_1 + x_2 + x_6) \end{array}$$

defina o código C como sendo o núcleo de T. Vamos determinar se os vetores 100111 e 010101 pertencem ou não a C.

Note que, $C = Ker(T)$. Ou seja, para que os vetores pertençam a C, basta aplicarmos a transformação linear em cada um deles e verificarmos se estão ou não no núcleo.

$$\begin{aligned} T(100111) &= (1+1, 1+0+0+1, 1+0+1) \\ &= (0,0,0). \end{aligned}$$

Portanto, $100111 \in Ker(T) = C$.

$$\begin{aligned} T(010101) &= (0+1, 0+1+0+0, 0+1+1) \\ &= (1,1,0). \end{aligned}$$

Observe que neste caso, $010101 \notin Ker(T)$.

Sempre que se define uma classe de objetos matemáticos, como por exemplo a classe dos códigos lineares de comprimento n sobre um corpo $\mathbb{K}$, define-se também a noção de equivalência entre esses objetos. A noção de equivalência de códigos repousa sobre o conceito de isometria que definiremos abaixo.

Definição 1.7 *Sejam $\mathbb{K}$ um corpo finito e n um número natural. Diremos que uma função $F : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ é uma **isometria** de $\mathbb{K}^n$ se ela preserva distâncias de Hamming. Em símbolos,*

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

Proposição 1.2 *Toda isometria de $\mathbb{K}^n$ é uma bijeção de $\mathbb{K}^n$.*

Demonstração: Seja $F : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ uma isometria. Suponha que para $\mathbf{x}, \mathbf{y} \in \mathbb{K}^n$ tenhamos $F(\mathbf{x}) = F(\mathbf{y})$. Logo, $d(\mathbf{x}, \mathbf{y}) = d(F(\mathbf{x}), F(\mathbf{y})) = 0$, o que implica que $\mathbf{x} = \mathbf{y}$. Assim, provamos que F é injetora, e como toda aplicação injetora de um conjunto finito nele próprio é sobrejetora, temos que F é uma bijeção. ■

Definição 1.8 *Seja $\mathbb{K}$ um corpo finito. Dois códigos lineares C e C' são equivalentes se existir uma isometria $T : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ tal que $T(C) = C'$.*

Definição 1.9 *Um código $C \subset A^n$ é chamado de **geometricamente uniforme** se, e somente se, dadas duas palavras quaisquer $\mathbf{x}$ e $\mathbf{y}$ do código existe uma isometria $\phi : A^n \to A^n$ tal que:*

i. $\phi(C) = C$ *(a isometria leva o código no código)*

ii. $\phi(\mathbf{x}) = \mathbf{y}$.

1.2.1 Matriz Geradora de um Código

Sejam $\mathbb{K}$ o corpo finito com q elementos e $C \subset \mathbb{K}^n$ um código linear. Chamaremos de *parâmetros do código linear* C à terna (n, k, d), onde k é a dimensão de C sobre $\mathbb{K}$, e d representa a distância mínima de C, que é também igual ao peso $\omega(C)$ do código C. Note que o número de elementos M de C é igual a q^k. Seja $\mathcal{B} = \{\mathbf{v}_1, ..., \mathbf{v}_k\}$ uma base ordenada de C e considere a matriz G, cujas linhas são os vetores $\mathbf{v}_i = (v_{i1}, ..., v_{in})$, $i = 1, ..., k$, isto é,

$$G = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}$$

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

$$\begin{aligned} T : \mathbb{K}^k &\longrightarrow \mathbb{K}^n \\ \mathbf{x} &\longmapsto \mathbf{x}G \end{aligned}$$

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

$$T(\mathbf{x}) = \mathbf{x}G = x_1\mathbf{v}_1 + ... + x_k\mathbf{v}_k,$$

logo $T(K^k) = C$. Podemos considerar $\mathbb{K}^k$ como sendo o código da fonte, C, o código de canal e a transformação T, uma codificação. Note que a matriz G não é univocamente determinada por C, pois ela depende da escolha da base $\mathcal{B}$. Segue então, que duas matrizes geradoras de um mesmo código C podem ser obtidas uma da outra por uma sequência de operações do tipo:

(L1) Permutação de duas linhas.

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

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

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

$$\begin{aligned} T : \mathbb{K}^k &\longrightarrow \mathbb{K}^n \\ \mathbf{x} &\longmapsto \mathbf{x}G \end{aligned}$$

Definição 1.10 *Diremos 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 $k \times (n-k)$.

Dado um código C, nem sempre é possível achar uma matriz geradora de C na forma padrão. Por exemplo, o código $\mathbb{F}_2^5$ 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.

No entanto, efetuando também permutações das colunas de G, podemos obter a matriz

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

que é a matriz geradora na forma 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' equivalente a C.

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

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

1.2.2 Códigos Duais

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

$$\langle \mathbf{u}, \mathbf{v} \rangle = u_1 v_1 + ... + u_n v_n.$$

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

$$\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle$$

e bilinear

$$\langle \mathbf{u} + \lambda \mathbf{w}, \mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle + \lambda \langle \mathbf{w}, \mathbf{v} \rangle$$

para todo $\lambda \in \mathbb{K}$.

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

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

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

i) $C^{\perp}$ é um subespaço vetorial de $\mathbb{K}^n$;
ii) $\mathbf{x} \in C^{\perp} \Longleftrightarrow G\mathbf{x}^t = 0$.

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

Proposição 1.3 *Seja $C \subset \mathbb{K}^n$ 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 $C^{\perp}$.

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

Lema 1.4 *Suponha que C seja um código de dimensão k em $\mathbb{K}^n$ com matriz geradora G. Uma matriz H de ordem $(n-k) \times n$, com coeficientes em $\mathbb{K}$ e com linhas linearmente independentes, é uma matriz geradora de $C^{\perp}$ se, e somente se,*

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

Corolário 1.1 $(C^{\perp})^{\perp} = C$.

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

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

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.
Note que, para verificar se um determinado vetor v em $\mathbb{K}^n$ pertence ou não a um código

C com matriz geradora G, é preciso verificar se o sistema de n equações com k incógnitas $\mathbf{x} = (x_1, ..., x_k)$, dado por

$$\mathbf{x}G = \mathbf{v},$$

admite solução. Em geral, essa questão requer um custo computacional elevado para ser respondida. No entanto, trabalhando com uma matriz teste de paridade H, a solução pode ser encontrada mais rapidamente. Basta verificar se é nulo o vetor $H\mathbf{v}^t$.

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

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 somente se, quaisquer $s-1$ colunas de H são linearmente independentes.*

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 somente se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

Exemplo 1.7 *Vamos determinar, por uma matriz geradora, o código dual do código C do Exemplo 1.5.*

Vamos encontrar a matriz G. Observe que,

$C = Ker(T) = \langle (1,0,0,1,1,1), (0,1,0,0,1,1), (0,0,1,0,1,0) \rangle = \mathcal{B}$. Logo,

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

onde G é a matriz geradora de C associada a base $\mathcal{B}$. A partir da matriz G em sua forma padrão, encontramos com facilidade, utilizando a Proposição 1.3, a matriz teste de paridade H dada por

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

que é a matriz geradora de $C^{\perp}$.

Exemplo 1.8 *Seja C o código binário gerado pela matriz*

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

a) Vamos determinar o seu comprimento, sua dimensão e o seu número de elementos.
b) Vamos determinar uma matriz teste de paridade para C e a sua distância mínima.

a) Note que ao reduzirmos G a sua forma padrão, teremos quatro linhas linearmente independentes, formadas por vetores da base canônica de $\mathbb{F}_2^4$. Logo, C possui dimensão 4, e comprimento 6. O número de elementos é dado por q^k, daí, C possui $2^4 = 16$ elementos.

b) Queremos encontrar H, matriz teste de paridade para C. Logo, como G está em sua forma padrão, efetuando uma sequência de operações temos

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

Pelo Teorema 1.3, como temos que quaisquer 2 colunas de H que são linearmente independentes e existem 3 colunas linearmente dependentes, e portanto, pela Proposição 1.1(ii), a distância mínima é 3.

1.2.3 Decodificação

Chama-se **decodificação** ao procedimento de detecção e correção de erros num determinado código. O método geral de decodificação para códigos lineares é um aperfeiçoamento de um método inventado por D. Slepian do Laboratório Bell na década de 60. O método original de Slepian tinha um custo muito alto e os aperfeiçoamentos visaram reduzir este custo.

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

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

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

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

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

Seja H a matriz teste de paridade do código. Como $H\mathbf{c}^t = 0$, temos que

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

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

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

Lema 1.5 *Seja C um código linear em $\mathbb{K}^n$ com capacidade de correção κ. Se $\mathbf{r} \in \mathbb{K}^n$ e $\mathbf{c} \in C$ são tais que $d(\mathbf{c}, \mathbf{r}) \leq \kappa$, então existe um único vetor $\mathbf{e}$ com $\omega(\mathbf{e}) \leq \kappa$, cuja síndrome é igual à síndrome de $\mathbf{r}$ e tal que $\mathbf{c} = \mathbf{r} - \mathbf{e}$.*

Exemplo 1.9 *Determinação de $\mathbf{e}$ quando $\omega(\mathbf{e}) \leq 1$.*

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

Se $H\mathbf{e}^t = 0$, então $\mathbf{r} \in C$ e se toma $\mathbf{c} = \mathbf{r}$.
Suponhamos $H\mathbf{e}^t \neq 0$, então $\omega(\mathbf{e}) = 1$ e, portanto, $\mathbf{e}$ tem apenas uma coordenada não nula. Nesse caso, consideremos que $\mathbf{e} = (0, ..., \alpha, ..., 0)$ com $\alpha \neq 0$ na i-ésima posição. Logo,

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

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

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

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

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

Seja H a matriz teste de paridade do código C e seja $\mathbf{r}$ um vetor recebido. (Suponha $d \leq 3$).

i) Calcule $H\mathbf{r}^t$.

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

iii) Se $H\mathbf{r}^t = \mathbf{s}^t \neq 0$, compare $\mathbf{s}^t$ com as colunas de H.

iv) Se existirem i e α tais que $\mathbf{s}^t = \alpha h^i$, para $\alpha \in \mathbb{K}$, 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.

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

Seja $\mathbf{v} \in \mathbb{K}^n$. Defina

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

Lema 1.6 *Os vetores* $\mathbf{u}$ *e* $\mathbf{v}$ *de* $\mathbb{K}^n$ *têm a mesma síndrome se, e somente se,* $\mathbf{u} \in \mathbf{v} + C$.

Proposição 1.7 *Seja C um (n, k)-código linear. Temos que*
i) $\mathbf{v} + C = \mathbf{v}' + C \Leftrightarrow \mathbf{v} - \mathbf{v}' \in C$;
ii) $(\mathbf{v} + C) \cap (\mathbf{v}' + C) \neq \emptyset \Longrightarrow \mathbf{v} + C = \mathbf{v}' + C$;
iii) $\bigcup_{\mathbf{v} \in K^n} (\mathbf{v} + C) = \mathbb{K}^n$;
iv) $|(\mathbf{v} + C)| = |C| = q^k$.

Note que, a relação definida em $\mathbb{K}^n$ na Proposição 1.7 (i), dada por

$$v, v' \in \mathbb{K}^n \Longleftrightarrow v - v' \in C$$

é uma relação de equivalência. Logo, os itens (ii), (iii) e (iv) saem como consequência deste fato. Cada conjunto da forma $\mathbf{v} + C$ é chamado de *classe lateral* de $\mathbf{v}$ segundo C. Note que

$$\mathbf{v} + C = C \Longleftrightarrow \mathbf{v} \in C.$$

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

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

Exemplo 1.10 *Seja C o (4,2)-código gerado sobre* $\mathbb{F}_2$ *pela matriz*

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

Logo,

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

e as classes laterais segundo C são

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

Note que o Lema 1.6 nos estabelece uma correspondência 1 a 1 entre classes laterais e síndromes. Todos os elementos de uma classe lateral têm mesma síndrome, e elementos de classes laterais distintas possuem síndromes distintas.

Definição 1.11 *Um vetor de peso mínimo numa classe lateral é chamado de elemento líder dessa classe.*

No código do exemplo acima, temos que: 0000 é líder de C, 1000 é líder de 1000+C, 0100 e 0001 são líderes de 0100+C, e 0010 é líder de 0010+C.

Vamos agora discutir um algoritmo de correção de mensagens que tenham sofrido um número de erros menor ou igual à capacidade de correção do código, que é $\kappa = [\frac{d-1}{2}]$.

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

Algoritmo de Decodificação

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

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

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

Justificativa: Dado $\mathbf{r}$, e sejam $\mathbf{c}$ e $\mathbf{e}$, respectivamente, a mensagem transmitida e o vetor erro. Como $H\mathbf{e}^t = H\mathbf{r}^t$, temos que a classe lateral onde $\mathbf{e}$ se encontra está determinada pela síndrome de $\mathbf{r}$. Se $\omega(\mathbf{e}) \leq \kappa$, temos que $\mathbf{e}$ é o único elemento líder l de sua classe e, portanto, é conhecido e se encontra na tabela. Consequentemente, pelo Lema 1.5, $\mathbf{c} = \mathbf{r} - \mathbf{e} = \mathbf{r} - l$ é determinado.

Exemplo 1.11 *Sejam G_1 e G_2, respectivamente, matrizes geradoras de códigos com parâmetros (n_1, k_1, d_1) e (n_2, k_2, d_2) definidos sobre um mesmo corpo finito.*

(i) Mostremos que o código com matriz geradora

$$\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$$

tem parâmetros (n, k, d), em que $n = n_1 + n_2$, $k = k_1 = k_2$ e $d = min\{d_1, d_2\}$.

(ii) Suponha $k_1 = k_2$. Mostremos que o código com matriz geradora

$$\begin{pmatrix} G_1 & G_2 \end{pmatrix}$$

tem parâmetros (n, k, d), em que $n = n_1 + n_2$, $k = k_1 = k_2$ e $d \geq d_1 + d_2$.

i) Observe que G_1 possui comprimento n_1, ou seja, possui n_1 colunas. Note também que G_1 possui dimensão k_1, ou seja, possui k_1 linhas. Logo,

$$G_1 = \begin{pmatrix} v_1 \\ \vdots \\ \vdots \\ v_{k_1} \end{pmatrix}_{k_1 \times n_1}$$

E ainda, o mesmo vale para a matriz G_2,

$$G_2 = \begin{pmatrix} u_1 \\ \vdots \\ \vdots \\ u_{k_2} \end{pmatrix}_{k_2 \times n_2}$$

Daí, ao representarmos G, temos que:

$$G = \begin{pmatrix} v_1 & \\ v_2 & 0 \\ v_3 & \\ \vdots & \\ v_{k_1} & u_1 \\ 0 & u_2 \\ & u_3 \\ & \vdots \\ & u_{k_2} \end{pmatrix}_{(k_1+k_2)\times(n_1+n_2)} ,$$

onde a matriz G é composta por $k_1 + k_2$ linhas e $n_1 + n_2$ colunas. Portanto, $k = k_1 + k_2$ e $n = n_1 + n_2$. Para encontrarmos a distância mínima d, vamos considerar a matriz G acima e o peso do código, já que $d = w(C)$. Como o peso é o número de entradas não-nulas das $k_1 + k_2$ linhas, observe que nas k_1 linhas, d é no mínimo d_1, pois as demais entradas são nulas. O mesmo vale nas k_2 linhas. Logo, $d = min\{d_1, d_2\}$.

ii) Assim como o item i), estamos olhando para as matrizes G_1 e G_2, logo,

$$G = \begin{pmatrix} v_1 & u_1 \\ \vdots & \vdots \\ v_{k_1} & u_{k_2} \end{pmatrix},$$

Assim, como G_1 tem comprimento n_1 e G_2 tem comprimento n_2 temos que $n = n_1 + n_2$.

Faremos a mesma análise para k, como G_1 tem dimensão k_1 e G_2 tem dimensão k_2 e, por hipótese, $k_1 = k_2$, segue que $k = k_1 = k_2$.

Exemplo 1.12 *Seja C um código binário com matriz geradora*

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

a) Vamos determinar o comprimento, a dimensão e o número de elementos de C.
b) Vamos construir uma matriz teste de paridade de C, calcule a dimensão de $C^{\perp}$ e a distância mínima de C. É perfeito o código C?
c) Ache o vetor erro da mensagem r = 11110010, admitindo que apenas um erro foi cometido.

d) Determine o número das classes laterais com líderes de peso $\geq$ 2.

a) Como G possui quatro linhas linearmente independentes, logo, C = 4. Daí, como G é formado por 4 vetores, sua dimensão é 4. O número de elementos é dado por q^k, onde $k = 4$ e $q = 2$. Portanto, $2^4 = 16$ elementos.

b) Ao colocarmos G na forma padrão, teremos:

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

Daí, utilizando a Proposição 1.3,

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

Pela Proposição 1.3, H é uma matriz geradora de $C^{\perp}$ e, portanto, a dimensão de $C^{\perp}$ é $n-k = 4$. Note que pelo Teorema 1.3 como quaisquer 2 colunas da matriz H são linearmente independentes e existem 3 colunas linearmente dependentes, segue que a distância mínima é 3.
Vamos verificar se o código é perfeito. Para que um código seja perfeito, pela Definição 1.3, devemos ter:

$$\bigcup_{c \in C} D(c, \kappa) = \mathbb{F}_2^8.$$

Do código C sabemos que $d = 3$ e portanto $\kappa = 1$. Do Lema 1.1, temos que,

$$1)|D(c_1, 1)| = \sum_{i=0}^{1} \begin{pmatrix} 8 \\ i \end{pmatrix} (2-1)^i = \begin{pmatrix} 8 \\ 0 \end{pmatrix} . 1^0 + \begin{pmatrix} 8 \\ 1 \end{pmatrix} . 1^1 = 9$$

$$2)|D(c_2, 1)| = \sum_{i=0}^{1} \begin{pmatrix} 8 \\ i \end{pmatrix} (2-1)^i = 9, \qquad c_i \in C$$

Recursivamente para as dezesseis palavras do código C, teremos

$$|D(c_1, 1)| = |D(c_2, 1)| = ... = |D(c_{16}, 1)| = 9.$$

Logo, $|D(c_1, 1)| + |D(c_2, 1)| + ... + |D(c_{16}, 1)| = 144$ palavras

Sabemos ainda que o espaço $\mathbb{F}_2^8$ possui 256 palavras.

Portanto, como $\bigcup_{c \in C} D(c, \kappa) \neq \{0, 1\}^8$, o código C não é perfeito.

c) Vamos considerar a matriz H do item anterior. Como a palavra recebida e o vetor erro tem a mesma síndrome, segue que

$$He^t = Hr^t = H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = 1 \cdot h^4$$

Portanto, $e = (00010000)$.

d) Ao efetuarmos as combinações lineares com os vetores da base, encontramos as palavras do código C = {10111000, 11001100, 01011010, 00110011, 00011101, 00000000, 10100101, 11010001, 01000111, 00101110, 01101001, 01110100, 10010110, 11111111, 11100010, 10001011}.

Observe que pela Proposição 1.7 sabemos que existem 16 classes laterais para cada elemento. Sabemos também que $\mathbb{F}_2^8 = 256$ palavras. Daí, o número de classes laterais é dado por $\frac{256}{16} = 16$. Note que, ao analisarmos as classes laterais com líderes de peso menor ou igual a dois, encontramos 9 classes. Basta observar que ao operarmos $\mathbf{v} + C$, onde C são as palavras do nosso código, os vetores $\mathbf{v}$ (alternando a posição do 1 em cada entrada) serão

líderes, já que quando operamos $\mathbf{v} + C$, resultarão em elementos com peso maior ou igual a dois. Daí, como temos 16 classes laterais e 9 delas possuem líderes de peso menor ou igual a dois, logo, existem $16 - 9 = 7$ classes laterais com líderes de peso maior ou igual a 2.

Exemplo 1.13 *Seja C um código binário de comprimento 7 cuja matriz teste de paridade é*

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

a) Vamos construir uma matriz geradora G para C.
b) Mostremos que a dimensão de C é 4 e sua distância mínima é $d = 3$.
c) Supondo que no máximo um erro é introduzido na transmissão, decodifique 0010101 e 1000010.

a) Usando a Proposição 1.3 e o Corolário 1.1 temos,

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

b) Encontrada a matriz G, ao colocarmos G em sua forma padrão, teremos:

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

ou seja, temos quatro vetores que geram nosso código C. Logo, a dimensão de C é quatro. Por outro lado, observe que as colunas 4, 5 e 6 da matriz teste de paridade são linearmente dependentes, e que quaisquer duas colunas de H são linearmente independentes. Portanto, pelo Teorema 1.3 $w(C) = 3$. Segue pela Proposição 1.1 que $d = 3$.

c) Como $d = 3$, logo $\kappa = 1$. Vamos determinar os elementos de $u \in \mathbb{F}_2^7$ tal que $w(u) \leq 1$.

líder	síndrome
0000000	000
0000001	111
0000010	011
0000100	101
0001000	110
0010000	001
0100000	010
1000000	100

Calculando as síndromes, onde $s^t = Hr^t$, temos:

$$H \cdot r^t = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = 011$$

e, portanto, o correspondente na tabela acima é $e = (0000010)$. Consequentemente,

$$\mathbf{c} = \mathbf{r} - \mathbf{e} \Rightarrow \mathbf{c} = (0010101) - (0000010) = (0010111).$$

Para $\mathbf{r} = (1000010)$,

$$H \cdot r^t = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = 111$$

e, portanto, o correspondente na tabela acima é $\mathbf{e} = (0000001)$. Consequentemente,

$$\mathbf{c} = \mathbf{r} - \mathbf{e} \Rightarrow \mathbf{c} = (1000010) - (0000001) = (1000011).$$

1.3 Códigos q-ários: A distância de Lee

Chamamos códigos q-ários os que têm por alfabeto o anel $\mathbb{Z}_q$ dos inteiros módulo q. Em função da tecnologia computacional disponível atualmente, os códigos mais utilizados são essencialmente os binários. Outros códigos são também usados em outras etapas e posteriormente convertidos em binários. Este é o caso dos códigos de bloco q-ários que serão introduzidos com exemplos e a noção de distância de Lee, métrica comumente utilizada e adaptada a esta classe de códigos.

A métrica de Lee pode ser definida da seguinte maneira:

Definição 1.12 *Dados $\overline{a}, \overline{b} \in [\overline{0}, \overline{q})$ com $0 \leq a, b < q$, definimos a* ***métrica de Lee*** *por*

$$d_{Lee}(\overline{a}, \overline{b}) = min\{|a - b|, q - |a - b|\}.$$

Com isso, por exemplo, em $\mathbb{Z}_{13}$, $d_{Lee}(\overline{1}, \overline{4}) = 3$ e $d_{Lee}(\overline{1}, \overline{12}) = 2$. Colocando as classes de $\mathbb{Z}_q$ como os vértices de um polígono regular de q lados, a distância de Lee entre duas classes será o menor número de arestas que conectam esses vértices.

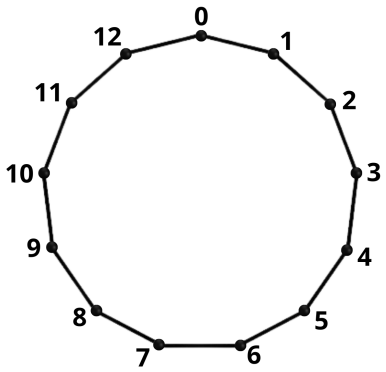


Figura 1.3: Representação geométrica de $\mathbb{Z}_{13}$ com a distância de Lee.

A distância de Lee em $\mathbb{Z}_q^n$ é definida como a soma das distâncias nas coordendas:

$$d_{Lee}((\overline{a_1}, \overline{a_2}, ..., \overline{a_n}), (\overline{b_1}, \overline{b_2}, ..., \overline{b_n})) = \sum_{i=1}^{n} d_{Lee}(\overline{a_i}, \overline{b_i}).$$

Podemos definir os conceitos de esfera e bola da mesma maneira que fizemos com a distância de Hamming. Para $n = 2$, os pontos de $\mathbb{Z}_q^2$ correspondem aos vértices de uma malha quadriculada desenhada em um quadrado de lado q. Os bordos deste quadrado devem ser identificados e portanto esta malha irá estar sobre um toro. A distância de Lee entre dois vértices é a distância do grafo, ou seja, o número mínimo de arestas na malha para ir de um vértice a outro. A Figura 1.4 representa $\mathbb{Z}_5^2$. Note que, $d_{Lee}((\overline{2}, \overline{3}), (\overline{4}, \overline{4})) = 3$.

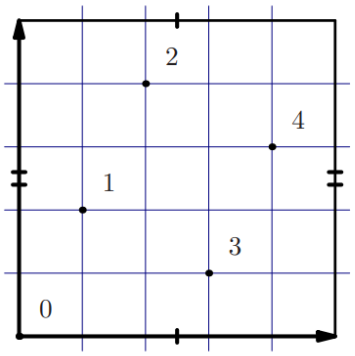


Figura 1.4: Representação geométrica de $\mathbb{Z}_5^2$.

CAPÍTULO 2

RETICULADOS

Nosso objetivo inicial na proposição deste trabalho foi estudar elementos geométricos envolvidos na teoria de códigos. Tentar compreender as relações e, a partir da nossa base algébrica (resumidamente apresentada no Capítulo 1), identificar relações com os entes geométricos estudados. Neste capítulo trataremos da estrutura dos reticulados. Uma estrutura geométrica, que como veremos tem sua utilidade no estudo de códigos. Nosso estudo introdutório se baseia em [5], um texto mais geral sobre o estudo de códigos geométricos e em [6], um trabalho mais direcionado para o estudo dos reticulados. Para as demonstrações omitidas neste capítulo sugerimos uma consulta aos dois textos citados, pois estes apresentam a maioria das demonstrações.

Reticulados têm mostrado uma grande utilidade em aplicações em telecomunicações e criptografia. Quando estudamos reticulados, o que estamos buscando é, encontrar o melhor reticulado possível em $\mathbb{Z}^n$, onde n é a dimensão, em relação à uma certa propriedade. O problema de encontrar o melhor código possível em $\mathbb{Z}^n$ corresponde, em $\mathbb{R}^n$, ao problema do *empacotamento esférico*. Ou seja, queremos distribuir esferas de raio r em $\mathbb{R}^n$, de modo que:

i. Duas esferas quaisquer deste arranjo apenas se toquem em um ponto da "casca", ou não possuam intersecção nenhuma;

ii. Este arranjo de esferas ocupe o "maior espaço possível".

Este problema torna-se um pouco menos complicado quando se tem alguma estrutura algébrica no código, ou seja, nos centros das esferas. O mesmo vale para o empacotamento esférico em $\mathbb{R}^n$ e, neste caso, a estrutura algébrica é a de *reticulado*. Para entendermos melhor sobre reticulados e empacotamento de esferas, veremos a seguir algumas definições e resultados.

Observe que o empacotamento de esferas vai de encontro na teoria de códigos ao que tratamos na Seção 1.1. Naquela oportunidade o Lema 1.2 nos diz que os discos com centro nas palavras dos códigos não se interceptam, enquanto a Definição 1.3 de códigos perfeitos nos coloca no caminho do objetivo do item (ii) acima.

Definição 2.1 *Dado $\{v_1, v_2, ..., v_m\}$ um conjunto de vetores linearmente independentes em $\mathbb{R}^n$, definimos por **reticulado** o conjunto*

$$\Lambda = \left\{ \sum_{i=1}^{m} \lambda_i v_i, \lambda_i \in \mathbb{Z} \text{ para todo } i = 1, 2, ..., m \right\}.$$

Além disso, damos o nome de **base** do reticulado para o conjunto $\{v_1, v_2, ..., v_m\}$.

A Figura 2.1 ilustra dois reticulados em $\mathbb{R}^2$: o reticulado $\mathbb{Z}^2$, dos pontos de coordenadas inteiras no plano, que tem por base $\beta = \{(0,1),(1,0)\}$, e o reticulado gerado pela base $\alpha = \{(2,1),(-1,3)\}$. A base de um reticulado não é única: $\beta' = \{(1,3),(0,1)\}$ também é base de $\mathbb{Z}^2$, pois o reticulado gerado por β' está contido em $\mathbb{Z}^2$ e $\mathbb{Z}^2$ está contido no reticulado gerado por β', já que, dado $(m,n) \in \mathbb{Z}^2$, temos

$$(m,n) = m(1,3) + (n = 3m)(0,1).$$

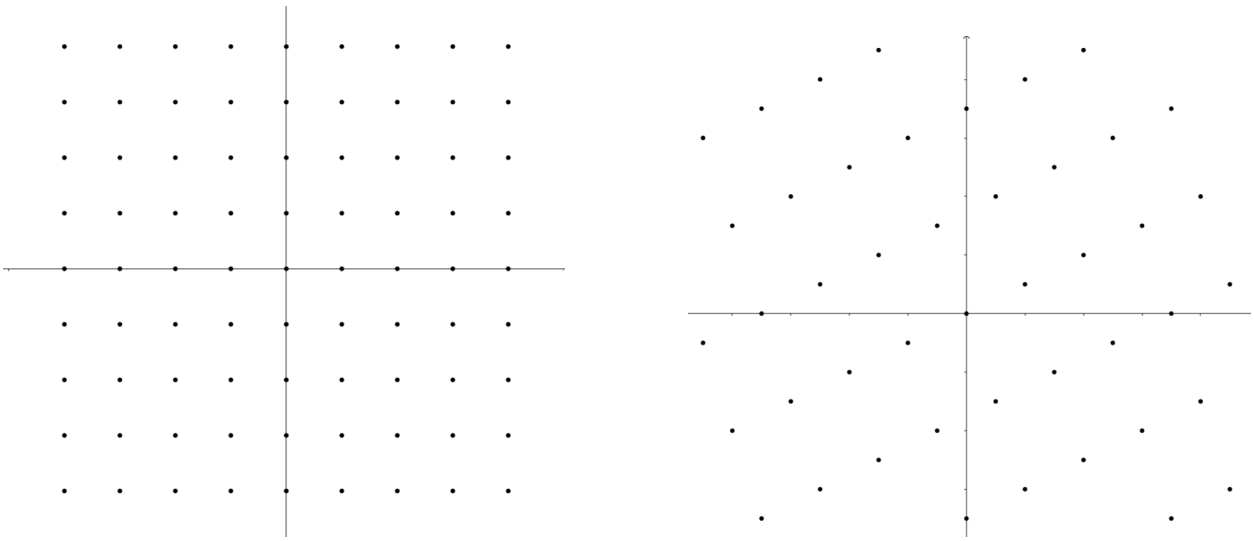


Figura 2.1: Reticulados no plano.

Observação 2.1 *Todo reticulado é geometricamente uniforme.*

2.1 Reticulados no Plano

Como primeiro exemplo de empacotamento determinado por um reticulado, vamos considerar o reticulado $\mathbb{Z}^2$. Um empacotamento esférico (neste caso, por discos) é feito colocando-se um disco D, de raio $\frac{1}{2}$, centrado em cada ponto $\mathbf{v}$ do reticulado. Note que, se tomarmos discos de raio maior do que $\frac{1}{2}$, haverá sobreposição; portanto, $\frac{1}{2}$ é o maior raio possível para um empacotamento de discos com centro em pontos de $\mathbb{Z}^2$. Este maior raio é chamado de *raio de empacotamento* ρ do reticulado.

Para medir a proporção da área do plano que foi ocupada pelo empacotamento, utilizamos um arranjo "complementar" dado pelas regiões de Voronoi dos pontos do reticulado. A **região de Voronoi** de um ponto $\mathbf{v} \in \mathbb{Z}^2$ é o conjunto $R(\mathbf{v})$ dos pontos de $\mathbb{R}^2$ que estão mais próximos de $\mathbf{v}$ do que de qualquer outro ponto de $\mathbb{Z}^2$.

Para identificarmos um reticulado mais geral do plano, uma região de Voronoi é determinada da seguinte forma: dados $\mathbf{u}$ e $\mathbf{v}$ dois pontos do plano, o conjunto de pontos que estão mais próximos de $\mathbf{v}$ do que de $\mathbf{u}$ corresponde ao semiplano que é determinado pela bissetriz do segmento $[\mathbf{u}, \mathbf{v}]$, que contém o ponto $\mathbf{v}$. Ao tomarmos a intersecção dos semiplanos relativamente próximos a $\mathbf{v}$, obteremos a região $R(\mathbf{v})$. A Figura 2.2 ilustra as regiões de Voronoi de $\mathbb{Z}^2$ e do reticulado Λ gerado por (2,1) e (-1,3).

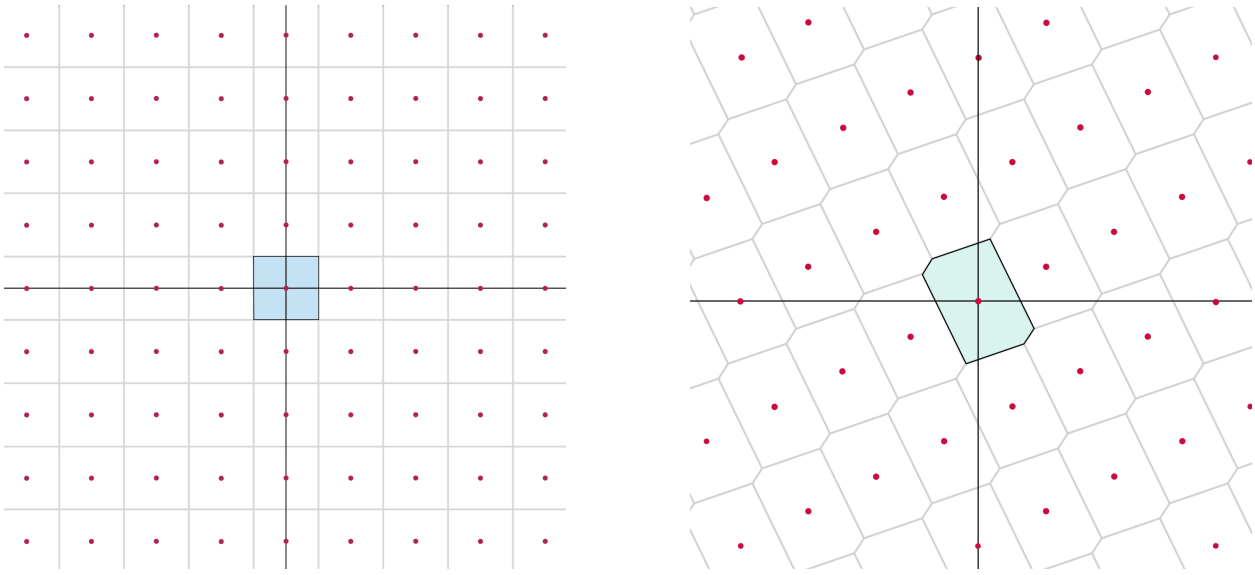


Figura 2.2: Regiões de Voronoi.

A definição formal da região de Voronoi para dimensão n é a mesma de dimensão 2:

Definição 2.2 *Se* $\mathbf{v} \in \Lambda$*, a* ***região de Voronoi*** *de* $\mathbf{v}$ *é o conjunto*

$$R(\mathbf{v}) = \{\mathbf{x} \in \mathbb{R}^n; ||\mathbf{v} - \mathbf{x}|| \leq ||\mathbf{v} - \mathbf{u}||, \forall \mathbf{u} \in \Lambda\}.$$

Observação 2.2 *Como a translação por um vetor do reticulado é uma isometria, toda região de Voronoi ao redor de um ponto* $\mathbf{v} \in \Lambda$ *pode ser obtida por uma translação da região de Voronoi do ponto zero, ou seja,*

$$R(\mathbf{v}) = R(\mathbf{0}) + \mathbf{v} = \{\mathbf{v} + \mathbf{x} \in \mathbb{R}^2; \mathbf{x} \in R(\mathbf{0})\}.$$

O importante sobre essas regiões é que elas constituem um ladrilhamento perfeito no plano: as regiões $R(\mathbf{v})$ cobrem o plano inteiro e se sobrepõem apenas nos pontos de fronteira (vértices ou arestas). Assim, a densidade do empacotamento de discos determinado pelo reticulado, é definida como a razão Δ entre a área do disco de empacotamento D e a área da região de Voronoi, fornecendo o quanto do plano foi coberto pelos discos. Temos então,

$$\Delta = \frac{\text{área}(D)}{\text{área}(R(\mathbf{0}))},$$

onde D é o disco de raio ρ, com ρ o raio de empacotamento, e $R(\mathbf{0})$ é a região de Voronoi de $\mathbf{0}$.

Exemplo 2.1 *Mostremos que, para* $\mathbb{Z}^2$*, temos* $\Delta = \frac{\pi}{4} \cong 0,7804$.

Note que, como estamos em $\mathbb{Z}^2$, a área do disco de empacotamento é dada por $D = \pi r^2$. E ainda, sabemos que a região de Voronoi de $\mathbb{Z}^2$ gera um quadrado. Como vimos anteriormente que o maior raio possível de empacotamento é $\frac{1}{2}$, temos:

$$\begin{aligned}
\Delta &= \frac{\text{área}(D)}{\text{área}(R(\mathbf{0}))} \\
\Delta &= \frac{\pi r^2}{l^2} \\
\Delta &= \frac{\pi(\frac{1}{4})}{1} \\
\Delta &= \frac{\pi}{4}
\end{aligned}$$

2.2 Regiões Fundamentais e Densidade

Seja Λ um reticulado em $\mathbb{R}^n$. Uma *região fundamental* F de Λ é um subconjunto fechado de $\mathbb{R}^n$ que ladrilha $\mathbb{R}^n$, ou seja, tomando os transladados $F + \mathbf{v}$, com $\mathbf{v} \in \Lambda$, conseguimos cobrir todo o $\mathbb{R}^n$ de modo que dois ladrilhos ou não têm interseção ou se interceptam apenas

nos bordos.

A região de Voronoi $R(\mathbf{0})$ é um exemplo de região fundamental de Λ. Uma segunda região fundamental bastante útil é o *politopo fundamental* gerado por uma base de Λ.

Definição 2.3 *Dado um reticulado Λ com base $\beta = \{\mathbf{u_1}, \mathbf{u_2}, ..., \mathbf{u_n}\}$, chamamos de* ***politopo fundamental*** *a região do $\mathbb{R}^n$ definida por*

$$P = \left\{ \sum_{i=1}^{n} a_i \mathbf{u}_i : 0 \leq a_i \leq 1 \right\}.$$

Para $n = 2$, este é o paralelogramo gerado por β. Da mesma forma que nos reticulados planos, o volume deste sólido n-dimensional é dado por $vol(P) = |det(A)|$, onde A é a matriz cujas colunas são os vetores da base β.

Uma primeira propriedade destas regiões já foi citada anteriormente na Observação 2.2. Uma segunda propriedade importante é que podemos ladrilhar $\mathbb{R}^n$ com estas regiões.

Assim como no caso planar, vamos avaliar o quão denso é um reticulado comparando o volume de uma região de Voronoi $R(\mathbf{v})$ com o volume da maior bola $B_r(\mathbf{v})$ que ela contém. Para isso, seja $r = \rho$ o raio de empacotamento de Λ, isto é, o maior número positivo tal que $B_r(\mathbf{0}) \subset R(\mathbf{0})$. Definimos a densidade de Λ por

$$\Delta = \frac{\text{vol}(B_\rho(\mathbf{0}))}{\text{vol}(R(\mathbf{0}))}.$$

Proposição 2.1 *P é uma região fundamental de Λ.*

Demonstração: De fato, P é fechado, e se

$$\mathbf{v} + P = \{\mathbf{x} + \mathbf{v} : \mathbf{x} \in P\},$$

então

(i) cada vetor de $\mathbb{R}^n$ está em um destes sólidos. De fato, se $\lfloor a \rfloor$ é a parte inteira do número real a (ou seja, $\lfloor a \rfloor \in \mathbb{Z}$ e $0 \leq a - \lfloor a \rfloor < 1$), então para cada vetor $\mathbf{v} = \sum_{i=1}^{n} a_i \mathbf{u_i}$ de $\mathbb{R}^n$, temos

$$\sum_{i=1}^{n} a_i \mathbf{u_i} = \underbrace{\sum_{i=1}^{n} \lfloor a_i \rfloor \, \mathbf{u_i}}_{\in \Lambda} + \underbrace{\sum_{i=1}^{n} (a_i - \lfloor a_i \rfloor) \, \mathbf{u_i}}_{\in P}.$$

Portanto, $\mathbb{R}^n = \bigcup_{\mathbf{v} \in \Lambda} \mathbf{v} + P$.

(ii) o interior de $\mathbf{v}+P$, isto é, o conjunto de pontos de $\mathbf{v}+P$ que não estão na fronteira, é o conjunto

$$int(\mathbf{v}+P)=\left\{\mathbf{v}+\sum_{i=1}^{n}a_i\mathbf{u_i}:0<a_i<1\right\},$$

e disso se conclui que nenhum ponto de $\mathbf{v}+P$ pode estar em outro transladado $\mathbf{u}+P$.

■

O fato de P ser uma região fundamental de Λ é crucial no estudo dos reticulados, pois

Proposição 2.2 *O volume de qualquer região fundamental de Λ é o mesmo.*

2.3 Matriz de Gram e o Determinante de um Reticulado

Seja $\beta=\{\mathbf{u_1},\mathbf{u_2},...,\mathbf{u_n}\}$, uma base do reticulado Λ, e seja $x=k_1\mathbf{u_1}+...+k_n\mathbf{u_n}$ um elemento de Λ. Escrevendo os vetores na forma de colunas, com as coordenadas na base canônica, temos

$$\mathbf{x}=\underbrace{\begin{bmatrix}u_{11}&\cdots&u_{1n}\\ \vdots&&\vdots\\ u_{n1}&\cdots&u_{nn}\end{bmatrix}}_{A}\cdot\begin{bmatrix}k_1\\ \vdots\\ k_n\end{bmatrix}=\begin{bmatrix}u_{11}k_1+&\cdots&+u_{1n}k_n\\ \vdots&&\vdots\\ u_{n1}k_1+&\cdots&+u_{nn}k_n\end{bmatrix}$$

Isso nos mostra que Λ é a imagem de $\mathbb{Z}^n$ pela matriz $A=(u_{ij})$, ou seja, todo $\mathbf{x}\in\Lambda$ é da forma $A\mathbf{v}^t$, para algum $\mathbf{v}=\{k_1,...,k_n\}$ em $\mathbb{Z}^n$. A matriz A é chamada de **matriz geradora** de Λ. E ainda, se A é uma matriz geradora de Λ, a matriz de **Gram** associada é $G=A^tA$.

Observação 2.3 *A matriz G guarda informações métricas importantes sobre a base escolhida. É claro que um reticulado tem várias bases diferentes e infelizmente a matriz de Gram podem mudar com a base. Assim, um reticulado possui várias matrizes de Gram diferentes. No entanto, o determinante de cada uma delas é o mesmo e só depende do reticulado.*

Considere, por exemplo, o reticulado Λ gerado por $\beta=\{\mathbf{u},\mathbf{v}\}$, com $\mathbf{u}=(n,n+1)$ e $\mathbf{v}=(-n-1,n)$, sendo n um número inteiro não-nulo. Os vetores $\mathbf{u'}=(n,n+1)$ e $\mathbf{v'}=(-1,2n+1)$ também formam uma base β' de Λ.

Exemplo 2.2 *Vamos verificar que β' também é base do reticulado Λ. Além disso, verificaremos também que as matrizes de Gram correspondentes a β e β' são:*

$$G = \begin{bmatrix} 2n^2+2n+1 & 0 \\ 0 & 2n^2+2n+1 \end{bmatrix} \quad e \quad G' = \begin{bmatrix} 2n^2+2n+1 & 2n^2 \\ 2n^2 & 4n^2+4n+2 \end{bmatrix}$$

Precisamos mostrar que existe uma transformação linear invertível entre β e β'.
Escrevendo $\mathbf{u}'$ e $\mathbf{v}'$ como combinação linear de $\mathbf{u}$ e $\mathbf{v}$, temos:

$$\begin{aligned} (i) \quad & \mathbf{u}' = a\mathbf{u} + b\mathbf{v} \\ (ii) \quad & \mathbf{v}' = c\mathbf{u} + d\mathbf{v}, \end{aligned}$$

onde a, b, c e d $\in \mathbb{Z}$.

Em (i), temos:

$$\begin{aligned} (n, n+1) &= a(n, n+1) + b(-n-1, n) \\ (n, n+1) &= (an, an+a) + (-bn-b, bn), \end{aligned}$$

Daí, temos o seguinte sistema:

$$\begin{cases} n = an + b(-n-1) \\ n+1 = a(n+1) + bn \end{cases}$$

Resolvendo o sistema, encontramos $a = 1$ e $b = 0$. Para (ii), analogamente, encontramos o sistema

$$\begin{cases} -1 = cn + d(-n-1) \\ 2n+1 = c(n+1) + dn \end{cases}$$

Resolvendo o sistema, encontramos $c = 1$ e $d = 0$. Logo, a matriz de transformação é dada por

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},$$

onde $det(M) = 1$. Logo, M é invertível e β' é base do reticulado Λ. Note que, para verificar que as matrizes de Gram G e G' correspondem a β e β', respectivamente, basta resolver $G = A^T A$ e $G' = A'^T A$, onde as matrizes A e A' são conhecidas.

Assim, um reticulado possui várias matrizes de Gram diferentes. No entanto, o determinante de cada uma delas é o mesmo e só depende do reticulado. Para verificar, considere as bases $\beta = \{\mathbf{u}_1, \mathbf{u}_2, ..., \mathbf{u}_n\}$ e $\beta' = \{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n\}$ de Λ e sejam A e B as matrizes geradoras associadas. Como β é a base de Λ, podemos escrever

$$\mathbf{v}_j = a_{1j}\mathbf{u}_1 + a_{2j}\mathbf{u}_2 + ... + a_{nj}\mathbf{u}_n \text{para} j = 1, 2, ..., n,$$

onde cada a_{ij} está em $\mathbb{Z}$. A transformação linear $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$, que leva $\mathbf{u}_j$ em $\mathbf{v}_j$, faz a mudança de base e tem matriz M com determinante ± 1. Daí,

$$B = MA$$

e $\det(B^T B) = \det(A^T M^T M A) = \det(A^T)\det(M^T)\det(M)\det(A) = \det(A^T A)$.

É fácil verificar que as duas matrizes do exemplo anterior têm determinante igual a $(2n^2 + 2n + 1)$. Por isso, definimos o **determinante de** Λ, $\det(\Lambda)$, como o determinante de uma matriz de Gram qualquer de Λ.

2.4 Reticulados Congruentes e Reticulados Equivalentes

Em códigos lineares, trabalhamos com códigos binários utilizando o conceito de **códigos equivalentes**: dois códigos lineares C_1 e C_2 são equivalentes se existir uma isometria φ tal que $\varphi(C_1) = C_2$. Além disso, códigos equivalentes possuem os mesmos parâmetros n, k, d.

Para reticulados, temos uma definição análoga de reticulados congruentes. Diremos que se dois reticulados são congruentes, então possuem o mesmo raio de empacotamento, mesma densidade e uma mesma matriz de Gram.

Diremos que Λ_1 e Λ_2 são **equivalentes** se existirem uma aplicação ortogonal $U : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ e um número real positivo λ tais que $(\lambda U)(\Lambda_1) = \Lambda_2$. Note que $\langle \lambda U\mathbf{u}, \lambda U\mathbf{v}\rangle = \lambda^2\langle \mathbf{u}, \mathbf{v}\rangle$ e que, por tabela, $\|\lambda U\mathbf{v}\| = \lambda\|\mathbf{v}\|$. Diremos que λ é a **razão de semelhança** de Λ_1 para Λ_2.

Se ρ_i e Δ_i são o raio de empacotamento e a densidade de Λ_i, para $i = 1, 2$, respectivamente, temos

$$\begin{aligned} min\{||\mathbf{x}|| : \mathbf{x} \in \Lambda_2\} &= min\{\lambda||\mathbf{y}|| : \mathbf{y} \in \Lambda_1\} \\ &= \lambda min\{||\mathbf{y}|| : \mathbf{y} \in \Lambda_1\} \end{aligned}$$

e segue que o raio de empacotamento de Λ_2 é $\rho_2 = \lambda\rho_1$. E também: se A é a matriz geradora de Λ_1, então λUA é a **matriz geradora** de Λ_2 e

$$\det(\lambda UA) = \det(\lambda I)\det(U)\det(A) = \lambda^n \det(A),$$

o que mostra que $\det(\Lambda_2) = \lambda^{2n}\det(\lambda_1)$. Portanto,

$$\begin{aligned}\Delta_2 &= \frac{\mathrm{vol}(B_{\rho_2(0)})}{\sqrt{\det(\Lambda_2)}} \\ &= \frac{\lambda^n \,\mathrm{vol}(B_{\rho_1(0)})}{\lambda^n\sqrt{\det(\Lambda_1)}} \\ &= \frac{\mathrm{vol}(B_{\rho_1(0)})}{\sqrt{\det(\Lambda_1)}} \\ &= \Delta_1\end{aligned}$$

Assim, reticulados equivalentes possuem a mesma densidade. Temos o seguinte resultado:

Proposição 2.3 *Se Λ_1 é semelhante a Λ_2 com razão de semelhança λ, então existem matrizes de Gram G_1 e G_2 para Λ_1 e Λ_2 tais que*

1. $G_2 = \lambda^2 G_1$,

2. $\rho_2 = \lambda\rho_1$,

3. $\Delta_2 = \Delta_1$.

Observe que, como tanto o raio quanto o volume podem ser calculados a partir de uma matriz de Gram do reticulado, a propriedade (1) implica nas condições (2) e (3). Além disso, outro fato importante é que, se vale a condição (1), então os reticulados são semelhantes.

Quando $\lambda = 1$, dizemos que os reticulados são **congruentes**. Neste caso, as matrizes de Gram e os raios de empacotamento são iguais.

Assim como nos códigos, não costuma-se fazer distinção entre reticulados congruentes e vários reticulados são identificados na literatura pela matriz de Gram. Um exemplo importante é o dos reticulados $D_n, n \geq 3$. Os reticulados D_3, D_4 e D_5 são definidos pelas matrizes de Gram

$$\begin{bmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & e \end{bmatrix}, \quad \begin{bmatrix} 2 & 0 & -1 & 0 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{bmatrix} \text{ e } \quad \begin{bmatrix} 2 & 0 & -1 & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 \\ -1 & -1 & 2 & -1 & 0 \\ 0 & 0 & -1 & 2 & 1 \\ 0 & 0 & 0 & -1 & 2 \end{bmatrix}$$

A matriz de Gram do reticulado D_n, para $n \geq 6$, tem as mesmas 4 primeiras linhas de D_5 (completadas com zeros à direita) e as linhas 5, 6, 7, ..., n são obtidas da quarta linha, que é o vetor (0,0,-1,2,-1,0,...,0), por deslocamentos à direita:

$$\begin{bmatrix}
2 & 0 & -1 & 0 & & & \cdots & & 0 & 0 \\
0 & 2 & -1 & 0 & 0 & & & & & 0 \\
-1 & -1 & 2 & -1 & 0 & 0 & \cdots & & & \\
0 & 0 & -1 & 2 & -1 & 0 & & & & \\
0 & 0 & 0 & -1 & 2 & -1 & & & \vdots & \\
\vdots & & & & \ddots & & & & & \\
 & & & & & 0 & -1 & 2 & -1 & 0 \\
0 & & & & \cdots & & 0 & -1 & 2 & -1 \\
0 & 0 & & & & & & 0 & -1 & 2
\end{bmatrix}$$

2.5 Construção A

Códigos lineares em $\mathbb{Z}_q^n$ podem ser "levantados" para reticulados em $\mathbb{Z}^n$ via Construção A, onde a Construção A é definida como segue:

Proposição 2.4 *Considere a aplicação sobrejetora*

$$\begin{aligned} \phi : \mathbb{Z}^n &\longrightarrow \mathbb{Z}_q^n \\ (x_1, ..., x_n) &\longmapsto (\overline{x_1}, ..., \overline{x_n}), \end{aligned}$$

onde $\overline{x_i}$ é obtido por meio de redução de módulo q para todo $i = 1, ..., n$. Temos que $C \subset \mathbb{Z}_q^n$ é um código linear q-ário se, e somente se, $\phi^{-1}(C) \subset \mathbb{Z}^n$ é um reticulado em $\mathbb{R}^n$. Além disso, $q\mathbb{Z}^n \subset \phi^{-1}(C)$.

Definição 2.4 *Chamamos de **Construção A** a aplicação que relaciona um código linear q-ário a um reticulado $\phi^{-1}(C)$ e chamamos o reticulado $\Lambda(C) = \phi^{-1}(C)$ de reticulado q-ário.*

Exemplo 2.3 *A Figura mostra o reticulado gerado pelo código 7-ário $C = \langle(\overline{1}, \overline{3})\rangle = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{3}), (\overline{2}, \overline{6}), (\overline{3}, \overline{2}), \overline{4}, \overline{5}), (\overline{5}, \overline{1}), (\overline{6}, \overline{4})\}$. Os pontos de mesma cor representam cópias da caixa $\mathbb{Z}_7^2$*

Definição 2.5 *Um reticulado que pode ser obtido via Construção A a partir de um código linear $C \subset \mathbb{Z}_q^n$ é chamado de reticulado q-ário.*

Proposição 2.5 *Um reticulado $\Lambda \subset \mathbb{Z}^n$ contém $q\mathbb{Z}^n$ se, e somente se, pode ser obtido via Construção A a partir de algum código q-ário de comprimento n.*

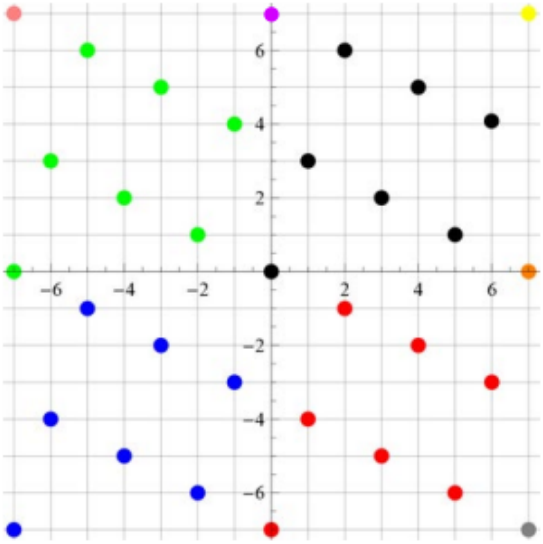


Figura 2.3: $\Lambda(C)$. Fonte [6]

Demonstração: Ver [6], p. 60. ■

Lema 2.1 *Se* $\{\mathbf{v}_1, ..., \mathbf{v}_m\}$ *é um conjunto de vetores linearmente independente sobre* $\mathbb{Z}$*, então* $\{\mathbf{v}_1, ..., \mathbf{v}_m\}$ *é linearmente independente sobre* $\mathbb{R}$*.*

Corolário 2.1 *Se* $C \subset \mathbb{Z}_q$ *é um código linear q-ário, então o posto de* $\Lambda(C)$ *é igual a n.*

Proposição 2.6 *Dado um código linear q-ário* $C \subset \mathbb{Z}_q^n$ *com conjunto de geradores* $\beta = \{\overline{\mathbf{v}_1}, ..., \overline{\mathbf{v}_m}\} \subset \mathbb{Z}_q^n$*, temos que o conjunto* $\{\mathbf{v}_1, ..., \mathbf{v}_m, qe_1, ..., e_n\} \subset \mathbb{R}^n$*, onde* $\{e_1, ..., e_n\}$ *é a base canônica de* $\mathbb{R}$*, gera o reticulado* $\Lambda(C)$*.*

Teorema 2.1 *Sejam* $q \in \mathbb{N}$ *um número primo e* $B = (\overline{I_{m\times n} M_{m\times(n-m)}})$ *uma matriz geradora do código* $C \subset \mathbb{Z}_q^n$*. Uma atriz geradora do reticulado q-ário* $\Lambda(C)$ *é dada por*

$$B_{\Lambda(C)} = \begin{pmatrix} I_{m\times n} & M_{m\times(n-m)} \\ 0_{(n-m)\times m} & qI_{(n-m)\times(n-m)} \end{pmatrix}_{m\times n}.$$

Exemplo 2.4 *Consideremos o código* $C \subset \mathbb{Z}_5^4$*, 5-ário com matriz geradora*

$$B = \begin{pmatrix} \overline{1} & \overline{0} & \overline{1} & \overline{4} \\ \overline{0} & \overline{1} & \overline{1} & \overline{1} \end{pmatrix}.$$

Pelo Teorema 2.1, temos que

$$B_{\Lambda(C)} = \begin{pmatrix} 1 & 0 & 1 & 4 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix}$$

é uma matriz geradora de $\lambda(C)$.

Exemplo 2.5 *Vamos considerar agora o código binário $C \subset \mathbb{Z}_2^8$ com matriz geradora*

$$B = \begin{pmatrix} \overline{1} & \overline{0} & \overline{0} & \overline{0} & \overline{1} & \overline{1} & \overline{1} & \overline{0} \\ \overline{0} & \overline{1} & \overline{0} & \overline{0} & \overline{1} & \overline{1} & \overline{0} & \overline{1} \\ \overline{0} & \overline{0} & \overline{1} & \overline{0} & \overline{1} & \overline{0} & \overline{1} & \overline{1} \\ \overline{0} & \overline{0} & \overline{0} & \overline{1} & \overline{0} & \overline{1} & \overline{1} & \overline{1} \end{pmatrix}$$

Esse código é conhecido como Código de Hamming estendido, denotado por H_8.
Pelo Teorema 2.1, temos

$$B_{\Lambda(H_8)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

é uma matriz geradora para $\Lambda(H_8)$.

Note que a matriz de Gram de $\Lambda(H_8)$ é dada por

$$B_{\Lambda(H_8)} \left(B_{\Lambda(H_8)}\right)^T = \begin{pmatrix} 4 & 2 & 2 & 2 & 2 & 2 & 2 & 0 \\ 2 & 4 & 2 & 2 & 2 & 2 & 0 & 2 \\ 2 & 2 & 4 & 2 & 2 & 0 & 2 & 2 \\ 2 & 2 & 2 & 4 & 0 & 2 & 2 & 2 \\ 2 & 2 & 2 & 0 & 4 & 0 & 0 & 0 \\ 2 & 2 & 0 & 2 & 0 & 4 & 0 & 0 \\ 2 & 0 & 2 & 2 & 0 & 0 & 4 & 0 \\ 0 & 2 & 2 & 2 & 0 & 0 & 0 & 4 \end{pmatrix}.$$

CONSIDERAÇÕES FINAIS

O estudo proposto sobre códigos e reticulados rendeu boas discussões e resultados importantes. Antes de falar sobre os resultados, é importante mencionar a importância de termos uma estrutura algébrica que nos permite nos aprofundar na teoria de códigos. Com isso, podemos destacar o Teorema 1.1, onde por meio dele podemos verificar o quão eficiente pode ser um código, pois aqui levamos em consideração o custo computacional. Outro resultado importante, foi o Teorema 1.3, resultado importante para descobrirmos um dos principais parâmetros de um código: a distância mínima.

Na teoria de reticulados temos vários resultados que nos ajudaram a compreender a relação destes com códigos lineares. Desde a definição de reticulados, regiões fundamentais, densidade e matriz de Gram, esta última associada a uma matriz geradora de um reticulado. O trabalho seguiu com o cronograma previsto, trazendo resultados satisfatórios, possibilitando a ampliação da área de pesquisa para um futuro tema de TCC.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] 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.

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

[3] HEFEZ, A. VILELA, M. L. T. *Códigos Corretores de Erros*, Rio de Janeiro, IMPA, 2002.

[4] HEFEZ, A.; FERNANDEZ, C. d. S. *Introdução à Álgebra Linear*. 2. ed. Rio de Janeiro: Coleção PROFMAT, SBM, 2016.

[5] LAVOR, C. C.; ALVEZ, M. M. et al. *Uma introdução à teoria de códigos*. Notas em Matemática Aplicada. Vol. 21. SBMAC, 2012.

[6] EDUARDO, L.N.G. *Introdução à teoria dos reticulados e suas propriedades*. Trabalho de Conclusão de Curso (Graduação em Matemática Computacional) - Universidade Federal de São Paulo, São Paulo, 2021.