UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Raphael Cascelli dos Santos Souza

A Conjectura de Golomb-Welch com raio 2 para infinitas dimensões

Juiz de Fora
2023

Raphael Cascelli dos Santos Souza

A Conjectura de Golomb-Welch com raio 2 para infinitas dimensões

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de Mestre em Matemática. Área de concentração: Álgebra

Orientadora: Profa. Dra. Beatriz Casulari da Motta Ribeiro

Juiz de Fora

2023

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

Cascelli dos Santos Souza, Raphael.
A Conjectura de Golomb-Welch com raio 2 para infinitas dimensões / Raphael Cascelli dos Santos Souza. – 2023.
99 f. : il.

Orientadora: Beatriz Casulari da Motta Ribeiro
Dissertação (Mestrado) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Programa de Pós-Graduação em Matemática, 2023.

1. Códigos corretores de erros. 2. Códigos perfeitos. 3.Reticulados. I. Casulari da Motta Ribeiro, Beatriz, orient. II. Título.

Raphael Cascelli dos Santos Souza

A conjectura de Golomb-Welch com raio 2 para infinitas dimensões

Dissertação apresentada ao Programa de Pós-graduação em Matemática da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de Mestre em Matemática. Área de concentração: Álgebra

Aprovada em 18 de agosto de 2023.

BANCA EXAMINADORA

Profª. Drª. Beatriz Casulari da Motta Ribeiro - Orientadora

Universidade Federal de Juiz de Fora

Prof. Dr. Frederico Sercio Feitosa

Universidade Federal de Juiz de Fora

Prof. Dr. Guilherme Chaud Tizziotti

Universidade Federal de Uberlândia

Juiz de Fora, 12/09/2023.

Documento assinado eletronicamente por **Beatriz Casulari da Motta Ribeiro**, **Professor(a)**, em 12/09/2023, às 11:36, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Frederico Sercio Feitosa**, **Professor(a)**, em 12/09/2023, às 11:48, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Guilherme Chaud Tizziotti**, **Usuário Externo**, em 12/09/2023, às 14:59, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no Portal do SEI-Ufjf (www2.ufjf.br/SEI) através do ícone Conferência de Documentos, informando o código verificador **1464124** e o código CRC **CDC52627**.

Dedico este trabalho à Mariana.

AGRADECIMENTOS

À minha noiva Mariana Barros de Souza por todo suporte e incentivo nos últimos meses que antecederam a conclusão do meu trabalho, pela paciência necessária para lidar comigo, além de todo amor e carinho constantes, sem os quais eu não teria conseguido ou sequer continuado.

À toda minha família pelo incentivo constante, confiança e amor. Hoje tenho a certeza de que sem seu apoio o caminho para alcançar aquilo que sonhei seria um pouco mais difícil.

À minha professora e orientadora Beatriz Casulari da Motta Ribeiro, por toda nossa trajetória juntos e principalmente, pela amizade, apoio, conselhos, direcionamentos e incentivo durante todo esse período. Espero, um dia, ser um matemático, professor e orientador tão bom quanto ela.

Aos professores Frederico Sercio Feitosa e Guilherme Chaud Tizziotti, por terem aceitado o convite para fazer parte da banca que avaliou este trabalho, colaborando para o resultado final aqui apresentado.

A cada um dos meus professores durante a graduação e mestrado na UFJF, por tudo que ensinaram e contribuíram para o meu crescimento acadêmico e pessoal.

A todos os meus amigos, os quais os nomes podem ser omitidos sem que haja desapreço por cada um, por todo suporte, companhia, incentivo e amor. Sou muito grato a cada um deles. Entretanto, não poderia deixar de agradecer especialmente ao meu amigo Vitor Monteiro Andrade Goulart por todos esses anos que moramos juntos, todo incentivo, estudos e troca de conhecimentos, pelas correções no texto e auxílio com a parte computacional e, à minha amiga Larissa Pereira Silva por todo carinho, incentivo e por ser minha família numa cidade e contexto que podem ser bastante desamparadores.

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

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo financiamento durante o mestrado.

"*Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet.*"
(Pierre de Fermat)

RESUMO

Um importante conceito da teoria de códigos é o do raio de empacotamento de um código, o qual definimos como sendo o raio máximo que nos permite cobrir o espaço em que o código está contido com bolas disjuntas centradas nas palavras do código. Neste sentido, os códigos perfeitos são códigos tais que não ocorre o caso de uma palavra errada estar fora de todas as bolas centradas nas palavras do código. O fato de um código ser perfeito ou não depende da métrica considerada. Nesse trabalho, vamos apresentar um estudo sobre os códigos perfeitos na métrica de Lee e os critérios para otimizar o raio em torno dos elementos do código. Por fim, apresentaremos a Conjectura de Golomb-Welch (1968) a qual afirma que não existem códigos lineares perfeitos de Lee para certos valores de dimensão e raio para alfabetos grandes. A demonstração geral ainda é um problema em aberto da Teoria dos Códigos, porém para raio 2, veremos uma demonstração de sua validade para infinitas dimensões relacionadas com um conjunto específico de números primos.

Palavras-chave: Códigos corretores de erros. Códigos perfeitos. Reticulados.

ABSTRACT

An important concept in coding theory is the packing radius of a code, which we define as the maximum radius that allows us to cover the space in which the code is contained with disjoint balls centered at the code words. In this sense, perfect codes are codes where the case of a wrong word being outside all the balls centered at the code words does not occur. Whether a code is perfect or not depends on the chosen metric. In this work, we will present a study on perfect linear codes in the Lee metric and the criteria to optimize the radius around the code elements. Finally, we will present the Golomb-Welch Conjecture (1968), which states that there are no perfect Lee codes for certain values of dimension and radius for large alphabets. The general proof of this conjecture still remains an open problem in Coding Theory, however, for radius 2, we will see a demonstration of its validity for infinite dimensions related to a specific set of prime numbers.

Keywords: Error correcting codes. Perfect codes. Lattices.

LISTA DE FIGURAS

Figura 1 – Mensagem codificada que será transmitida. 14
Figura 2 – Mensagem codificada que foi recebida. 14
Figura 3 – Esquema de Codificação e Decodificação. 15
Figura 4 – Exemplo de QR Code. 16
Figura 5 – Fotografia de Marte capturada pela espaçonave Mariner 4 (1965). 17
Figura 6 – Primeira foto colorida transmitida da superfície de Marte pela sonda Viking 1 (1976). 17
Figura 7 – Reticulado $\Lambda(\mathcal{C})$ 7-ário em $\mathbb{R}^2$. 21
Figura 8 – Exemplo da definição da métrica de Lee em um q-ágono regular. 31
Figura 9 – q^2-toro planificado. 42
Figura 10 – Visualização da superfície do q^2-toro. 43
Figura 11 – Exemplos de mono, do, tri, tetra e pentominó, respectivamente. 44
Figura 12 – Bolas de Lee $L_{2,1}, L_{3,1}, L_{2,2}$ e $L_{3,2}$, respectivamente. 44
Figura 13 – Bola $L(2, 1, (0, 0))$ em $\mathbb{R}^n$. O tracejado indica exatamente o X-pentominó de centro em $(0, 0)$. 45
Figura 14 – Polítopo cruzado inscrito em uma bola de Lee. 46
Figura 15 – Polítopos cruzados $P_{2,2}$ e $P_{3,1}$. 46
Figura 16 – Canal de Shannon com 5 fases. 47
Figura 17 – Representação geométrica do código. 48
Figura 18 – Empacotamento do toro 5×5 por P-pentominós. 49
Figura 19 – O X-pentominó que representa a esfera de Lee de raio 1. . . . 50
Figura 20 – Movimento do cavalo no xadrez. 54
Figura 21 – L-tetraminó gerado pelo salto do cavalo. 54
Figura 22 – Disposição final dos 16 cavalos no tabuleiro. 55
Figura 23 – Empacotamento do 8^2-toro por 16 L-tetraminós. 55
Figura 24 – Ladrilhamento de $\mathbb{Z}_5^2$ por pentominós. 60
Figura 25 – Ladrilhamento de $\mathbb{Z}_{13}^2$ por triskaidekominós. 60
Figura 26 – Bola de Lee $L_{3,2}$ composta por 25 cubos unitários. 63
Figura 27 – Porção da bola $L_{2,1}$ coberta pelo polítopo $P_{2,1}$. 71
Figura 28 – Estado da Conjectura de Golomb-Welch restrita a códigos lineares para $1 \leq n \leq 13$ e $1 \leq e \leq 13$. 75

SUMÁRIO

1 INTRODUÇÃO 10
2 TEORIA DE CÓDIGOS CORRETORES DE ERROS . . 12
2.1 O QUE É UM CÓDIGO? 12
2.2 CÓDIGOS LINEARES E RETICULADOS 18
2.3 MÉTRICAS, CORREÇÃO DE ERROS E CÓDIGOS PERFEITOS 24
2.3.1 Noções de espaços métricos 24
2.3.2 Correção de erros 27
2.3.3 Métricas em espaços de códigos 29
2.3.4 Códigos perfeitos na métrica de Hamming 38
3 CÓDIGOS PERFEITOS NA MÉTRICA DE LEE 42
3.1 GEOMETRIA DOS ESPAÇOS E BOLAS 42
3.2 O PROBLEMA DE EMPACOTAR ESPAÇOS 47
3.3 CONJECTURA DE GOLOMB-WELCH 56
4 O CASO DO RAIO 2 PARA INFINITAS DIMENSÕES 76
4.1 COBERTURAS HOMOGÊNEAS 76
4.2 CONJECTURA PARA PRIMOS AMIGÁVEIS 77
4.3 SOBRE A INFINITUDE DE $\mathcal{F}$ 88
5 CONCLUSÃO 96
REFERÊNCIAS 97

1 INTRODUÇÃO

Nos últimos anos, os avanços nas tecnologias de comunicação e armazenamento de dados têm desempenhado um papel fundamental em nossa sociedade cada vez mais digital. No entanto, à medida que nos tornamos mais dependentes desses sistemas, os erros de transmissão e armazenamento se tornaram uma preocupação crítica e é exatamente neste contexto que vemos a importância dos códigos corretores de erros.

Os códigos corretores de erros desempenham um papel vital em uma ampla gama de aplicações, desde comunicações sem fio e transmissão de dados via satélite até sistemas de armazenamento em nuvem e memória de computadores. Eles são projetados para detectar e corrigir erros introduzidos durante a transmissão ou o armazenamento de dados, garantindo a integridade e a confiabilidade das informações, mesmo em ambientes propensos a ruídos e interferências.

Na busca para aprimorar as técnicas de correção de erros e projetar sistemas mais eficientes surgem, dentre os códigos corretores de erros, os códigos perfeitos que, apresentando uma simetria e estrutura intrínseca, são capazes de atingir limites teóricos superiores em termos de capacidade de detecção e correção de erros. Um código linear é dito perfeito se bolas centradas em suas palavras cobrem todo o espaço. Utilizando a métrica de Hamming, que mede a distância entre palavras pela contagem das entradas distintas, são bem conhecidos exemplos de códigos perfeitos.

Nosso interesse, nesse trabalho, está nos códigos perfeitos na métrica de Lee, que leva em conta não só quantas são as entradas diferentes de duas palavras, mas também seus valores. Nesse sentido, o norteador do trabalho é a Conjectura de Golomb-Welch, proposta em 1970: não existem, na métrica de Lee, códigos lineares perfeitos $LP(n, e)$ para os parâmetros dimensão $n \geq 3$ e raio $e \geq 2$.

A conjectura já foi mostrada válida para infinitas classes de parâmetros, porém continua sendo uma questão em aberto na teoria dos códigos corretores de erros pois, até o momento, não foi completamente resolvida. No entanto, ao longo dos anos, foram feitos avanços significativos na compreensão da conjectura e na construção de códigos que se aproximam dos limites impostos por ela. As

técnicas e ferramentas matemáticas para estudar a conjectura e seus efeitos inclusive apresentam contribuições em outras áreas da Matemática e da Ciência da Computação.

Nesta direção, o Capítulo 2 é dedicado à apresentação dos conceitos básicos do que será abordado no trabalho. Começamos por apresentar a ideia do que é um código e uma das principais aplicações que motivou os avanços da teoria. Em seguida, definimos formalmente os códigos lineares e reticulados, bem como a noção de métrica em um espaço de códigos, correção de erros e códigos perfeitos.

O Capítulo 3 trata de relacionar os códigos perfeitos na métrica de Lee com o que já conhecemos sobre os códigos de Hamming, discutido no final do capítulo 2. Iniciamos introduzindo a geometria do espaço em que iremos trabalhar e em seguida abordamos o problema de empacotar tal espaço com bolas na métrica de Lee. Ao final do capítulo apresentamos as discussões introduzidas por Golomb e Welch que os levaram à formulação da Conjectura, além de alguns resultados notáveis de outros pesquisadores na direção de sua demonstração.

No Capítulo 4, apresentaremos a abordagem do problema feita por Claudio Qureshi, Antônio Campello e Sueli Costa quando o raio é igual a 2. Vamos introduzir um conjunto especial de números primos, chamados amigáveis, juntamente com uma função injetiva cujo domínio é este conjunto de primos. A seguir, mostraremos que nenhum código linear perfeito de Lee existe com raio 2 e dimensão n, onde $2n^2 + 2n + 1$ tem como maior divisor um primo amigável. Por fim, provaremos que existem infinitos primos amigáveis, finalizando a demonstração de que a Conjectura de Golomb-Welch é verdadeira se o raio é 2 para infinitas dimensões.

2 TEORIA DE CÓDIGOS CORRETORES DE ERROS

O principal objetivo deste capítulo é introduzir os códigos corretores de erros, bem como algumas aplicações que motivaram os avanços dos estudos nesta área e algumas das suas propriedades mais importantes. Estudaremos também os chamados códigos perfeitos e em particular, os Códigos de Hamming.

2.1 O QUE É UM CÓDIGO?

O exemplo mais familiar de um código corretor de erros é um idioma. Por exemplo, a língua portuguesa tem 23 letras, mas vamos considerar ainda o espaço em branco, o ç e as vogais acentuadas separadamente, fazendo com que o alfabeto A tenha mais letras e a língua portuguesa possa ser considerada como um elemento de A^{46}. Esse número 46 é o tamanho da mais longa palavra dessa língua, o termo médico "*PNEUMOULTRAMICROSCOPICOSSILICOVULCANOCONIÓTICO*".

Como conhecemos a língua, se recebemos uma mensagem, digamos *"DINOSSALRO"* (no caso, é DINOSSALRO com 36 espaços em branco em seguida), sabemos corrigir, pois a palavra que mais se assemelha é *"DINOSSAURO"*.

No entanto, esse código não é eficiente. De fato, a língua portuguesa tem palavras muito "próximas" das outras. Por exemplo, "FATO", "GATO", "JATO", "MATO", "PATO", "RATO" e "TATO" têm apenas uma letra de diferença. Assim, ao receber "AATO", sabemos que há erro, mas não sabemos corrigir; já ao recebermos "GATO" não temos nem como saber se a mensagem possui algum erro.

Para corrigir esse tipo de problema, os códigos corretores de erros têm como função acrescentar novas informações que serão transmitidas fazendo com que estas possam ser corrigidas quando ocorrem ruídos. Vejamos um exemplo de código binário na detecção e correção de erros:

Exemplo 2.1.1. [9] Os códigos binários de correção de erros operam no nível dos bits, e cada bit é considerado como um dígito podendo ser 0 ou 1. Neste caso, utilizaremos um código com 5 bits por letra codificada.

Neste exemplo, trabalharemos com mensagens apenas com letras de A a Z. Dada uma mensagem, devemos proceder da seguinte maneira:

- Retirar todos os espaços entre palavras, acentos e caracteres especiais;
- Verificar se a mensagem possui uma quantidade múltipla de 5 letras;
- Caso o item anterior seja falso, adicionar o caractere ∅ até que seja verdadeiro;
- Separar a mensagem em blocos de 5 elementos;
- Considerar cada bloco como uma matriz coluna;
- Associar cada letra do vetor coluna a sua respectiva codificação de 5 bits.

O último item faz menção à Tabela Emicode (Tabela 1), em que cada símbolo do código é representado por uma sequência de 5 bits.

Letra	**Código**	**Letra**	**Código**	**Letra**	**Código**
A	11100	J	10001	S	01000
B	11001	K	10000	T	00111
C	01110	L	01111	U	00110
D	10111	M	11000	V	00101
E	10110	N	01101	W	00100
F	10101	O	01100	X	00011
G	10100	P	01011	Y	00010
H	10011	Q	01010	Z	00001
I	10010	R	01001	∅	00000

Tabela 1 – Tabela Emicode.

Consideremos a mensagem, já encriptada, *"K nxm zh Jptd Xqtg"*. Após realizarmos as 4 primeiras etapas do processo de tratamento da mensagem, dado anteriormente, obtemos *KNXMZ HJPTD XQTG∅*. Faremos os próximos passos apenas com o primeiro bloco *KNXMZ*.

De acordo com a Tabela Emicode, obtemos:

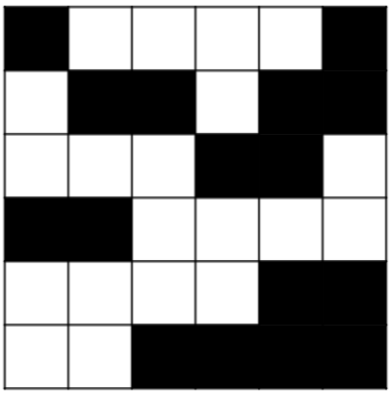
$$\begin{bmatrix} K \\ N \\ X \\ M \\ Z \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Agora, vamos inserir uma linha abaixo e uma coluna à direita da matriz de maneira que se a soma dos elementos da linha (ou da coluna) for ímpar adicionamos um dígito 1 e, se for par, 0. A matriz 5×5 original está associada à informação em si enquanto a coluna e a linha inseridas são utilizadas para detecção e correção de erros.

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

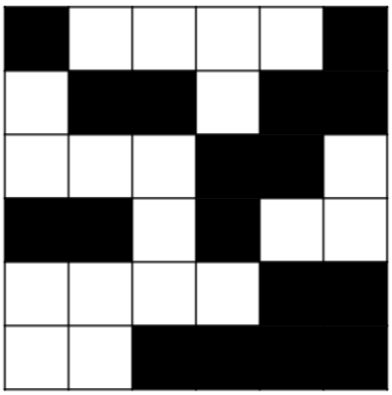
Dada esta nova matriz, podemos gerar uma grade quadriculada com células pretas e brancas fazendo correspondência com as entradas iguais a 1 e 0, respectivamente. Note que depois de inserirmos as redundâncias, todas as linhas e colunas possuem uma quantidade par de 0's e 1's. A Figura 1 a seguir é a mensagem codificada que iremos transmitir, uma espécie simplificada de QR Code.

Figura 1 – Mensagem codificada que será transmitida.



Fonte: Elaborada pelo autor (2023).

Figura 2 – Mensagem codificada que foi recebida.



Fonte: Elaborada pelo autor (2023).

Suponhamos agora que devido à interferências na transmissão de dados

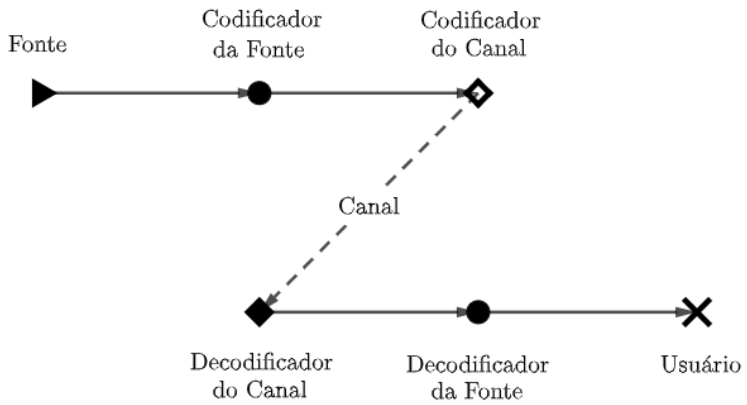
tenha ocorrido algum erro e a mensagem que recebemos foi a da Figura 2. Neste caso, como faríamos para perceber que há um erro na mensagem e possivelmente como vamos corrigí-lo?

Primeiramente, pela forma que a mensagem foi gerada, devemos ter uma quantidade par de quadrados pretos e brancos em cada linha e coluna. Desta maneira, como há um erro na mensagem, alguma linha e coluna deve possuir uma quantidade ímpar de quadrados de mesma cor. Então, devemos encontrar a linha e a coluna e, sua interseção é exatamente o quadrado em que há erro.

Por fim, como sabemos exatamente a célula em que há erro, basta invertermos sua cor na mensagem que foi recebida e teremos exatamente a mensagem que foi transmitida, livre de erros. Este código é capaz de detectar e corrigir 1 erro, como veremos mais à frente quando estivermos estudando os códigos de Hamming.

O procedimento do Exemplo 2.1.1 pode ser esquematizado como na Figura 3. O canal pode ser, por exemplo, de radiofrequência, de micro-ondas, cabo, circuito integrado digital, fita magnética, disco de armazenamento, etc, e é onde ocorre o ruído ou interferência na mensagem. Iremos considerar, durante todo o texto, canais simétricos, isto é, canais em que todos os símbolos transmitidos têm a mesma probabilidade (pequena) de serem recebidos errados e se um símbolo é recebido errado, a probabilidade de ser qualquer um dos outros é a mesma.

Figura 3 – Esquema de Codificação e Decodificação.



Fonte: Elaborada pelo autor (2023).

Como dissemos anteriormente, o Exemplo 2.1.1 apresenta uma versão simplificada de um QR Code. Entretanto, um QR Code é composto por um padrão de quadrados pretos e brancos organizados em uma matriz quadrada e composto por zonas de correção de erros. Cada padrão representa um conjunto de dados codificados de informação. As zonas possuem uma característica de correção de erros embutida. Isso significa que, mesmo que haja danos ou distorções na imagem do código, o conteúdo ainda pode ser decodificado com sucesso.

Figura 4 – Exemplo de QR Code.

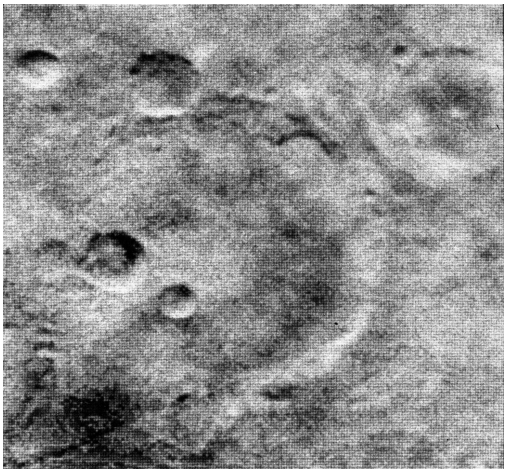
Fonte: Elaborada pelo autor (2023).

Na década de 1970, a indústria emergente de computadores e a indústria telefônica foram os primeiros usuários das tecnologias de correção de erros. Os sistemas de memória de computadores utilizam códigos de Hamming para evitar erros durante a transferência de dados dentro do computador. Com o início do programa espacial, a NASA (em inglês, *National Aeronautics and Space Administration*) se tornou uma grande usuária e desenvolvedora de tecnologias de códigos de correção de erros. A capacidade limitada de carga dos foguetes exigiu a miniaturização das cargas úteis e a otimização do peso, o que levou ao uso de códigos de correção de erros para melhorar a precisão da transmissão de sinais com baixa potência dos rádios e transmissores usados para enviar informações de volta à Terra.

Em 1965, a espaçonave Mariner 4, se tornou a primeira a fotografar de perto outro planeta e, obteve fotografias (sem cor) de Marte. As imagens tinham 200×200 pixels, sendo que cada pixel era atribuído a um dos 64 níveis de brilho (6

bits). A transmissão de uma única imagem levou cerca de 8 horas com velocidade de transmissão de aproximadamente 8 bits por segundo. Já a espaçonave Mariner 9, em 1972, obteve imagens muito melhores usando um código de Reed-Muller com 6 bits de informação e 26 bits adicionais para fornecer correção de erros. Embora a velocidade de transmissão agora fosse de cerca de $1,6 \times 10^4$ bits por segundo, as imagens individuais eram maiores, então cerca de 10^5 bits por segundo estavam sendo adquiridos pelas câmeras. Isso significava que as imagens eram armazenadas para transmissão. A Viking 1, que pousou em Marte em 1976, conseguiu capturar imagens coloridas. A NASA utilizou diversos códigos de correção de erros, como o Reed-Muller, o Golay e o Reed-Solomon, dependendo das características e necessidades de cada missão. No entanto, encontrar um sistema de correção de erros que se ajuste a todas as missões continua sendo um desafio devido à diversidade das situações enfrentadas em diferentes espaçonaves e distâncias da Terra.

Figura 5 – Fotografia de Marte capturada pela espaçonave Mariner 4 (1965).



Fonte: `https://www.nasa.gov/image-feature/mariner-4-image-of-mars`. Acesso em 20 jul. 2023.

Figura 6 – Primeira foto colorida transmitida da superfície de Marte pela sonda Viking 1 (1976).

Fonte: `https://www.jpl.nasa.gov/images/pia00563-first-color-image-from-viking-lander-1`. Acesso em 20 jul. 2023.

Embora o estudo dos códigos corretores de erros seja de grande interesse de engenheiros e cientistas de Telecomunicações e Computação, este texto tem por

objetivo apresentar uma análise dos aspectos mais essenciais e fundamentais da teoria, os de natureza algébrica.

No decorrer do texto utilizamos a seguinte convenção: dados $p \in \mathbb{Z}$ primo e $n \in \mathbb{N}$, o corpo finito com $q = p^n$ elementos será denotado por $\mathbb{F}_q$, enquanto $\mathbb{Z}_q$ representa o anel dos resíduos inteiros módulo q.

2.2 CÓDIGOS LINEARES E RETICULADOS

Nesta seção, exploraremos os códigos corretores de erros lineares e reticulados, que desempenham um papel fundamental na transmissão e armazenamento confiáveis de informações em sistemas de comunicação e armazenamento de dados.

Abordaremos ainda os conceitos fundamentais, propriedades e técnicas de codificação relacionadas a esses dois tipos de códigos. Exploraremos a estrutura dos códigos lineares, incluindo a matriz geradora e a matriz de verificação de paridade, bem como os algoritmos de codificação e decodificação. Além disso, investigaremos os códigos reticulados, destacando suas propriedades especiais e aplicações práticas.

É importante salientarmos que neste texto trataremos de códigos sobre anéis de resíduos, corpos finitos e corpos de característica 0. Em cada caso será dado o espaço em que estaremos trabalhando. Porém, a definição de um código linear pode ser feita de maneira mais geral, como faremos a seguir:

Definição 2.2.1. Sejam A um anel comutativo com unidade e M um A-módulo. Dizemos que $\mathcal{C}$ é um *código linear* se $\mathcal{C}$ for um A-submódulo de M.

A partir daí, cada caso e suas particularidades, serão tratados como em [11] para corpos finitos e como em [17], caso contrário.

Definição 2.2.2. Seja $q \in \mathbb{N}$. Um *código linear q-ário* $\mathcal{C}$ é um $\mathbb{Z}_q$-submódulo de $\mathbb{Z}_q^n$. Chamamos $\mathbb{Z}_q$ de *alfabeto* e seus elementos de *letras*. Por sua vez, chamamos $\mathcal{C}$ de *dicionário* e seus elementos de *palavras*.

Quando $q \in \mathbb{N}$ é primo, $\mathbb{Z}_q \cong \mathbb{F}_q$ e assim, podemos definir:

Definição 2.2.3. Um $(n; m)$ *código* $\mathcal{C}$ sobre $\mathbb{F}_q$ é um subconjunto próprio de $\mathbb{F}_q^n$ com m elementos de *comprimento* n. Dizemos que $\mathcal{C} \subset \mathbb{F}_q^n$ é um $[n; k]$ *código linear* sobre $\mathbb{F}_q$ se $\mathcal{C}$ for um subespaço vetorial de dimensão k de $\mathbb{F}_q^n$.

Podemos estender a definição de código para o espaço Euclidiano real n-dimensional como faremos a seguir:

Definição 2.2.4. Seja $\{v_1, v_2, \ldots, v_k\}$ um conjunto de vetores linearmente independentes em $\mathbb{R}^n$ tal que $k \leq n$. Dizemos que um *reticulado* é o conjunto

$$\Lambda = \left\{ \sum_{i=1}^{k} c_i v_i \, : \, c_i \in \mathbb{Z}, \, \forall i = 1, 2, \ldots, k \right\}$$

e $\{v_1, v_2, \ldots, v_k\}$ é uma *base* do reticulado.

Observação 2.2.5. Note que um reticulado é um código linear em $\mathbb{R}^n$, pois é um $\mathbb{Z}$-submódulo de $\mathbb{R}^n$.

A principal característica de um reticulado é a regularidade de sua estrutura. Os pontos do reticulado estão dispostos de forma uniforme, seguindo um padrão específico de espaçamento entre eles. Essa regularidade permite que os reticulados sejam utilizados para discretizar o espaço contínuo, transformando-o em uma grade matemática discreta. Além disso, os reticulados possuem propriedades adicionais, como a propriedade de fechamento sob soma e multiplicação por escalares, o que os torna ferramentas poderosas em várias áreas de estudo.

O teorema a seguir e sua demonstração podem ser encontrados em [25].

Teorema 2.2.6. *$\Lambda \subset \mathbb{R}^n$ é um reticulado se, e somente se, Λ é um subgrupo aditivo discreto.*

Uma pergunta natural que poderia surgir a partir da definição de códigos lineares e reticulados é se seria possível determinar uma relação entre estes dois tipos de objetos. Os resultados a seguir demonstram uma conexão entre esses dois conceitos fundamentais, revelando a importância de explorar a interação entre a álgebra linear e a geometria para o desenvolvimento de códigos de correção de erros eficientes e de alta qualidade.

Teorema 2.2.7. *Considere a aplicação sobrejetora*

$$\phi : \mathbb{Z}^n \longrightarrow \mathbb{Z}_q^n$$
$$(x_1, \ldots, x_n) \longmapsto (\overline{x_1}, \ldots, \overline{x_n}),$$

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

Demonstração. Seja $\mathcal{C}$ um código linear q-ário. Como $\phi^{-1}(\mathcal{C}) \subseteq \mathbb{Z}^n$ é um conjunto discreto, basta mostrarmos que $\phi^{-1}(\mathcal{C})$ é um grupo aditivo e assim, pelo Teorema 2.2.6 teremos que $\phi^{-1}(\mathcal{C})$ é um reticulado. Mostremos então que $\phi^{-1}(\mathcal{C})$ é um grupo aditivo. Note que:

- $0 \in \phi^{-1}(\mathcal{C})$, pois $\phi(0) = \overline{0} \in \mathcal{C}$, e;
- Se $a, b \in \phi^{-1}(\mathcal{C})$, então $\phi(a) = \overline{a} \in \mathcal{C}$ e $\phi(b) = \overline{b} \in \mathcal{C}$. Assim,

  $$\phi(a - b) = \overline{a - b} = \overline{a} - \overline{b} \in \mathcal{C}\,.$$

  Portanto, $a - b \in \phi^{-1}(\mathcal{C})$, donde $\phi^{-1}(\mathcal{C})$ é subgrupo aditivo de $\mathbb{R}^n$.

Agora, seja $\mathcal{C} \in \mathbb{Z}_q^n$ tal que $\phi^{-1}(\mathcal{C})$ é um reticulado. Temos que $\mathcal{C} = \phi(\phi^{-1}(\mathcal{C}))$ é subgrupo de $\mathbb{Z}_q^n$, pois é a imagem inversa de um subgrupo de $\mathbb{Z}^n$ via um homomorfismo de grupos. Portanto, $\mathcal{C}$ é um código linear q-ário. □

Definição 2.2.8. Chamamos de *Construção A* a aplicação ϕ do Teorema 2.2.7 que relaciona um código linear q-ário $\mathcal{C}$ a um reticulado $\phi^{-1}(\mathcal{C})$ e chamamos o reticulado $\Lambda_A(\mathcal{C}) = \phi^{-1}(\mathcal{C})$ de *reticulado q-ário.*

Proposição 2.2.9. *Se* $\mathcal{C} \subseteq \mathbb{Z}_q^n$ *é um código linear* q*-ário, então o posto de* $\Lambda_A(\mathcal{C})$ *é* n.

A Proposição 2.2.9 pode ser encontrada em [4] e sua demonstração utiliza o seguinte lema, cuja demonstração está em [17]:

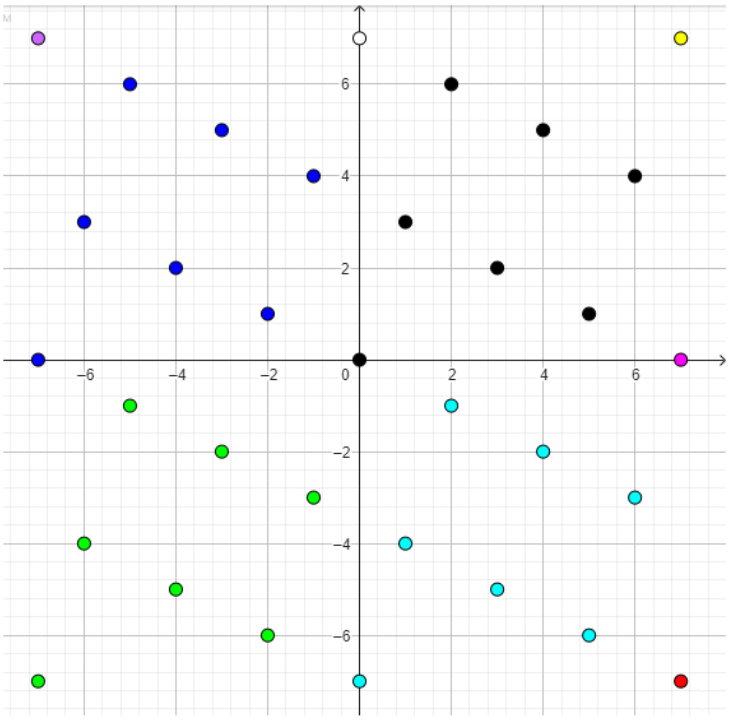
Lema 2.2.10. *Sejam* $v_i = (v_{i1}, \ldots, v_{in}) \in \mathbb{Z}^n$ *para* $i = 1, \ldots, m$, *com* $m \leq n$. *Se* $\{v_1, \ldots, v_m\}$ *é linearmente independente sobre* $\mathbb{Z}$, *então* $\{v_1, \ldots, v_m\}$ *é linearmente independente sobre* $\mathbb{R}$.

Exemplo 2.2.11. A Figura 7 mostra o reticulado gerado pelo código 7-ário

$$\mathcal{C} = \langle(\overline{1}, \overline{3})\rangle = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{3}), (\overline{2}, \overline{6}), (\overline{3}, \overline{2})(\overline{4}, \overline{5}), (\overline{5}, \overline{1}), (\overline{6}, \overline{4})\}.$$

Os pontos de mesma cor representam cópias da caixa $[0, 7)^2$ em $\mathbb{R}^2$.

Figura 7 – Reticulado $\Lambda(\mathcal{C})$ 7-ário em $\mathbb{R}^2$.



Fonte: Elaborada pelo autor (2023).

Deste ponto até o final da seção, vamos tratar apenas de códigos sobre $\mathbb{F}_q$, como na Definição 2.2.3.

A de um código linear $\mathcal{C}$ é definida como o número de elementos de uma base, ou seja, a quantidade mínima de elementos $v_1, v_2, ..., v_k \in \mathcal{C}$ tal que todo elemento $v \in \mathcal{C}$ pode ser descrito como combinação linear $v = \lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_k v_k$, com $\lambda_1, \lambda_2, ..., \lambda_k$ escalares em $\mathbb{F}_q$. Essa noção coincide, claramente, com a de dimensão de um espaço vetorial sobre $\mathbb{F}_q$.

Observe ainda que cada um dos k escalares pode assumir q valores distintos e, como estamos considerando uma base de $\mathcal{C}$, obtemos q^k combinações lineares distintas, ou seja, $\mathcal{C}$ tem q^k elementos e um $[n;k]$ código linear é um $(n;q^k)$ código sobre $\mathbb{F}_q$.

Apenas a estrutura de espaço vetorial já permite detectarmos erros. Se considerarmos um $[n;k]$ código linear $\mathcal{C}$, com $k<n$ e $v\in\mathcal{C}$ uma palavra, suponha que ao transmitirmos a palavra v recebamos a palavra w (podendo inclusive ocorrer $v=w$). Ao recebermos a mensagem w, procedemos antes de tudo com a verificação de que esta mensagem é uma palavra do nosso dicionário, ou seja, verificamos se $w\in\mathcal{C}$. Isto se dá de maneira simples, se lembrarmos que um subespaço vetorial é definido por um sistema de equações lineares homogêneas. Desta forma, definimos:

Definição 2.2.12. Se considerarmos a matriz $H\in M(n-k,n,\mathbb{F}_q)$ definida pelos coeficientes do sistema linear, podemos representar este sistema matricialmente pela equação

$$H\begin{bmatrix} x_1\\ x_2\\ \vdots\\ x_n\end{bmatrix}=\begin{bmatrix} 0\\ 0\\ \vdots\\ 0\end{bmatrix}$$

e temos que $\mathcal{C}$ é o conjunto solução deste sistema. Uma matriz H satisfazendo esta propriedade é chamada de *matriz de verificação de paridade*.

Pela Definição 2.2.12, se w for uma palavra recebida, e denotarmos por w^t a matriz transposta (ou vetor coluna), basta efetuar o produto Hw^t para sabermos se w pertence a $\mathcal{C}$. Se $w\notin\mathcal{C}$, sabemos que a mensagem recebida é equivocada, ou seja, conseguimos detectar a ocorrência de um erro.

Observação 2.2.13. Se $\mathcal{C}$ é um código linear de dimensão k, o posto da matriz H é igual $n-k$. Portanto, a matriz H deve ter $n-k$ linhas linearmente independentes.

Agora, notamos que se houve um erro, podemos ter $w\neq v$ mas com $w\in\mathcal{C}$. E, ainda, como $\mathcal{C}$ possui q^k elementos e $\mathbb{F}_q^n$ possui q^n elementos, então $q^n-q^k=q^k(q^{n-k}-1)$ elementos não pertencem a $\mathcal{C}$. Se assumirmos a hipótese de que o ruído perturba a palavra transmitida v de modo que possamos receber

qualquer elemento de $\mathbb{F}_q^n$, a probabilidade P de detectarmos o erro é dada por:

$$P = \frac{\#\{x \in \mathbb{F}_q^n \,|\, x \notin \mathcal{C}\}}{\#\mathbb{F}_q^n} = \frac{q^n - q^k}{q^n} = 1 - \frac{1}{q^{n-k}}\,.$$

Como $q \geq 2$ e $n - k \geq 1$, temos que $P < 1$ e esta cresce conforme q ou $n - k$ crescem. Assim, se quisermos detectar em média 999 erros a cada 1000 ocorrências, se tivermos $q = 2$, basta termos $n - k \geq 10$. Como

$$\lim_{q\to\infty} \frac{1}{q^{n-k}} = \lim_{n-k\to\infty} \frac{1}{q^{n-k}} = 0,$$

podemos detectar erros com a confiança tão grande quanto quisermos.

Além da matriz de verificação de paridade de um código, outro conceito importante que devemos considerar é o de matriz geradora de um código, a qual veremos a seguir:

Definição 2.2.14. Seja $\mathcal{B} = \{v_1, v_2, \ldots, v_k\}$ uma base ordenada de $\mathcal{C}$. A *matriz geradora* G de $\mathcal{C}$ associada à base $\mathcal{B}$ é a matriz cujas linhas são os vetores $v_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, $i = 1, 2, \ldots, k$, isto é

$$G = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix} = \begin{bmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & \ldots & v_{kn} \end{bmatrix}.$$

Observação 2.2.15. Note que a matriz geradora G para um código $\mathcal{C}$ não é única, pois ela depende da escolha da base $\mathcal{B}$.

A partir de matrizes geradoras G podemos construir códigos lineares, bastando para isso, consideramos a transformação linear:

$$\begin{aligned} T : \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ x &\longmapsto xG \end{aligned}$$

Assim, temos um código $\mathcal{C} = T(\mathbb{F}_q^k)$. Nesse caso, consideramos $\mathbb{F}_q^k$ como sendo o código da fonte, $\mathcal{C}$, o código do canal e a transformação T, uma codificação.

Este fato não será mostrado aqui, porém, é possível inclusive determinar uma relação direta entre matrizes de verificação de paridade e matrizes geradoras para um dado código $\mathcal{C}$, como feito em [11].

2.3 MÉTRICAS, CORREÇÃO DE ERROS E CÓDIGOS PERFEITOS

Nesta seção, veremos as métricas de Hamming, de Lee e de Manhattan em espaços de códigos mas antes vamos introduzir a noção geral de métrica em um conjunto. Utilizaremos estes conceitos para calcular um dos principais parâmetros de um dado código, além de necessitarmos dessas ferramentas para determinarmos um algoritmo útil na geração de um código linear. Em seguida, veremos a definição formal de um código perfeito e por fim, estudaremos o caso dos códigos perfeitos com erros medidos na métrica de Hamming.

Nosso principal objetivo é observar os principais paralelos entre as métricas que serão apresentadas e preparar o leitor para um estudo mais aprofundado dos chamados códigos perfeitos na métrica de Lee que serão discutidos no capítulo 3.

2.3.1 Noções de espaços métricos

Antes de avançarmos nosso estudo dos códigos corretores de erros, vejamos agora algumas definições e resultados importantes em relação a uma métrica em um espaço qualquer.

Definição 2.3.1. Uma métrica em um conjunto X é uma função $d : X \times X \to \mathbb{R}$ satisfazendo as seguintes propriedades:

1. $d(x, y) > 0$ se $x \neq y$ e $d(x, x) = 0$, para quaisquer $x, y \in X$;
2. $d(x, y) = d(y, x)$, para quaisquer $x, y \in X$;
3. $d(x, z) \leq d(x, y) + d(y, z)$, para quaisquer $x, y, z \in X$.

O par (X, d) é chamado *espaço métrico*.

Observação 2.3.2. Na definição anterior denominamos as propriedades 1, 2 e 3 de uma métrica como positiva definida, associativa e desigualdade triangular, respectivamente.

Definição 2.3.3. Sejam (X, d) um espaço métrico, um ponto $a \in X$ e $r > 0$. Definimos a bola $B(a; r)$ e a esfera $S(a; r)$, ambas de centro em a e raio r dadas

por:

$$B(a;r) = \{x \in X : d(x, x_0) \leq r\}$$

e

$$S(a;r) = \{x \in X : d(x, x_0) = r\}.$$

Definição 2.3.4. Sejam (X, d) um espaço métrico e $x \in X$. Definimos o *peso do vetor* $x \in X$ como

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

Quando estivermos trabalhando com métricas específicas, usaremos um subíndice $d_\star(\cdot;\cdot)$ para identificar a métrica. O mesmo subíndice será adotado para designar todos os conceitos derivados da métrica, tais como $B_\star(\cdot;\cdot)$, $S_\star(\cdot;\cdot)$ e $\omega_\star(\cdot)$.

Definição 2.3.5. Dado um código $\mathcal{C}$ sobre um espaço métrico (X, d), definimos a *distância mínima* entre seus pontos como

$$\delta_{\min} = \delta_{\min}(\mathcal{C}) = \min\{d(x, y) \ : \ x, y \in \mathcal{C}, \ x \neq y\}.$$

Quando o código $\mathcal{C}$ for linear, temos:

$$d(x, y) = d(x - x, y - x) = d(0, z)$$

para quaisquer $x, y \in X$, onde $z = x - y$. Ou ainda, como $x - y \in \mathcal{C}$ sempre que $x, y \in \mathcal{C}$, temos:

$$\delta_{\min} = \min\{\omega(x) \ : \ 0 \neq x \in \mathcal{C}\}.$$

Definição 2.3.6. Seja (X, d) um espaço métrico. Dizemos que uma função $f : X \longrightarrow X$ é uma *isometria* de X se preserva distâncias. Isto é, se

$$d(f(x), f(y)) = d(x, y) \ \ \forall x, y \in X.$$

Proposição 2.3.7. *Toda isometria de $\mathbb{F}_q^n$ é uma bijeção de $\mathbb{F}_q^n$.*

Demonstração. Seja $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ uma isometria. Suponha que para $x, y \in \mathbb{F}_q^n$ tenhamos $f(x) = f(y)$. Logo, $d(x, y) = d(f(x), f(y)) = 0$, o que implica que $x = y$. 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. □

A proposição a seguir pode ser encontrada em [11].

Proposição 2.3.8. *1. A função identidade de $\mathbb{F}_q^n$ é uma isometria.*

2. Se f é uma isometria de $\mathbb{F}_q^n$, então f^{-1} é uma isometria de $\mathbb{F}_q^n$.

3. Se f e g são isometrias de $\mathbb{F}_q^n$, então $f \circ g$ é uma isometria de $\mathbb{F}_q^n$.

Vejamos alguns exemplos de isometrias:

Exemplo 2.3.9. Se $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ é uma bijeção, e k é um número inteiro tal que $1 \leq k \leq n$, a aplicação

$$\begin{aligned} T_f^k : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q^n \\ (x_1, x_2, \ldots, x_n) &\longmapsto (x_1, x_2, \ldots, f(x_k), \ldots, x_n) \end{aligned}$$

é uma isometria.

Exemplo 2.3.10. Se π é uma bijeção do conjunto $\{1, 2, \ldots, n\}$ nele próprio, também chamada de permutação de $\{1, 2, \ldots, n\}$, a aplicação permutação de coordenadas

$$\begin{aligned} T_\pi : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q^n \\ (x_1, x_2, \ldots, x_n) &\longmapsto (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}) \end{aligned}$$

é uma isometria.

A definição a seguir será muito utilizada posteriormente para métricas de Hamming e de Lee na classe dos códigos lineares.

Definição 2.3.11. Um código $\mathcal{C} \subseteq \mathbb{A}^n$ (onde $\mathbb{A}$ é finito ou infinito) é dito *geometricamente uniforme* se, e somente se, dadas duas palavras x, y quaisquer do código existir uma isometria $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ tal que:

1. $\varphi(\mathcal{C}) = \mathcal{C}$;
2. $\varphi(x) = y$.

Observação 2.3.12. Note que pela Definição 2.3.11, se um código $\mathcal{C}$ for geometricamente uniforme, além de ser invariante por isometrias, as bolas e esferas centradas nas palavras do código possuem a mesma cardinalidade, desde que estejamos considerando o mesmo raio. De fato, basta notarmos que se φ é uma isometria tal que $\mathcal{C}$ é geometricamente uniforme e $x, y \in \mathcal{C}$ então

$$\varphi(B(x;r)) = B(\varphi(x);r) = B(y;r).$$

2.3.2 Correção de erros

Dada uma métrica d em $\mathbb{F}_q^n$, temos uma boa maneira de tentar corrigir erros. Vamos supor que a palavra transmitida foi $x \in \mathcal{C}$ e a palavra recebida foi $y \notin \mathcal{C}$. Se a métrica em si for razoável (considerando-se as características físicas do canal de transmissão de informação), é plausível supormos que a probabilidade de y estar "longe" de x é menor que a probabilidade de estar "perto" no sentido de que para quaisquer $\alpha, \beta \in \mathbb{R}$ e $m > 0$ com $0 \leq \beta \leq \alpha$, então a probabilidade de termos $\alpha \leq d(x,y) \leq \alpha + m$ é menor ou igual que a probabilidade de termos $\beta \leq d(x,y) \leq \beta + m$. Obviamente esta probabilidade é definida pelas características físicas do canal de transmissão mas como neste texto não estamos tratando de canais específicos, vamos sempre assumir que esta hipótese é verdadeira.

Desta maneira, temos um mecanismo sistemático e natural para corrigir erros: se a palavra recebida $y \notin \mathcal{C}$, escolhemos o ponto x de $\mathcal{C}$ mais próximo de y, ou seja, escolhemos $x \in \mathcal{C}$ tal que

$$d(y,x) = \min\{d(y,c) \ : \ c \in \mathcal{C}\}.$$

Neste sentido, primeiramente é útil obtermos um raio mínimo no sentido de que quaisquer bolas em torno das palavras do código nunca se interceptem, a menos do bordo em alguns casos. Este raio é obtido a partir da distância mínima e será definido como a seguir:

Definição 2.3.13. Seja $\delta_{\min}$ a distância mínima de um código $\mathcal{C}$. O *raio do código* é definido como o inteiro não-negativo

$$r = \left\lfloor \frac{\delta_{\min} - 1}{2} \right\rfloor.$$

Por vezes, dizemos que este código $\mathcal{C}$ é um código *r-corretor de erros*.

Observação 2.3.14. Note que, de fato quando $x, y \in \mathcal{C}$ distintos, as bolas $B_d(x;r)$ e $B_d(y;r)$ são sempre disjuntas. Suponhamos que $c_0 \in \mathcal{C}$ pertença a interseção destas, temos pela desigualdade triangular

$$\begin{aligned} d(x,y) &\leq d(x,c_0) + d(y,c_0) \\ &\leq \left\lfloor \frac{\delta_{\min}-1}{2} \right\rfloor + \left\lfloor \frac{\delta_{\min}-1}{2} \right\rfloor \\ &\leq \delta_{\min} - 1\,, \end{aligned}$$

uma contradição, pois, por definição, $\delta_{\min} \leq d(x,y)$.

De modo geral, dizemos que a capacidade de correção do código é R se podemos garantir que, caso a palavra transmitida x e a recebida y distem no máximo R, então temos certeza de estar corrigindo o código. Dessa forma, temos que se a distância entre a mensagem enviada x e a mensagem recebida y for menor ou igual a $\left\lfloor \frac{\delta_{\min}-1}{2} \right\rfloor$, temos que x é o ponto de $\mathcal{C}$ mais próximo de y e estamos de fato corrigindo o erro ocorrido durante a transmissão da mensagem.

Geometricamente, podemos pensar na capacidade de correção como sendo o maior natural R tal que

$$B(x;R) \cap B(y;R) = \emptyset$$

para quaisquer $x, y \in \mathcal{C}$ distintos. Daí, podemos definir o importante conceito de raio de empacotamento:

Definição 2.3.15. Seja $\mathcal{C}$ um código em $\mathbb{F}_q^n$. Dizemos que o código $\mathcal{C}$ é um *empacotamento* de $\mathbb{F}_q^n$ (ou o código $\mathcal{C}$ *empacota* o espaço $\mathbb{F}_q^n$) se existir um raio $r > 0$ tal que $B(x;r) \cap B(y;r) = \emptyset$, para quaisquer elementos x, y distintos de $\mathcal{C}$. Assim, dizemos que o *raio de empacotamento*, $\rho(\mathcal{C})$, de um código $\mathcal{C}$ é o raio máximo que nos permite empacotar bolas disjuntas centradas nas palavras do código. Isto é,

$$\rho(\mathcal{C}) = \max\{r \in \mathbb{N} \ : \ B(x;r) \cap B(y;r) = \emptyset,\ \forall x, y \in \mathcal{C},\ x \neq y\}\,.$$

Desta forma, a capacidade de correção de um código $\mathcal{C}$ é definida diretamente através do raio de empacotamento $\rho(\mathcal{C})$ que por sua vez é limitado inferiormente pelo raio do código definido a partir da distância mínima $\delta_{\min}$.

Além disso, o raio de empacotamento está relacionado com o problema de empacotamento de esferas, que consiste em dispor esferas de mesmo raio no espaço de tal modo que a interseção de duas delas contenha no máximo um ponto ou bordo, dependendo da métrica adotada. O objetivo do empacotamento é encontrar um arranjo de esferas idênticas de tal forma que a fração do espaço coberto por essas esferas seja o maior possível.

Posteriormente, estaremos interessados em códigos com raio de empacotamento suficientemente grande para empacotar todo o espaço $\mathbb{F}_q^n$.

2.3.3 Métricas em espaços de códigos

Agora, podemos introduzir os conceitos de códigos de Hamming e códigos de Lee e, em seguida, vamos calcular seus respectivos raios de empacotamento.

Definição 2.3.16. Dados $x, y \in \mathbb{F}_q^n$ com $x = (x_1, x_2, \ldots, x_n)$ e $y = (y_1, y_2, \ldots, y_n)$, a distância de Hamming d_H é definida como

$$d_H(x, y) = \#\{i \ : \ x_i - y_i \neq 0, \ i = 1, 2, \ldots, n\}. \tag{2.1}$$

Proposição 2.3.17. *d_H é uma métrica em $\mathbb{F}_q^n$.*

Demonstração. Consideremos em $\mathbb{F}_q^n$ os vetores $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$ e $z = (z_1, z_2, \ldots, z_n)$.

Para mostrarmos que d_H é de fato uma métrica positiva definida, basta notarmos que, como $d_H(x, y)$ é a quantidade de coordenadas diferentes entre x e y, $d_H(x, y)$ é sempre maior ou igual a zero, valendo a igualdade se, e somente se, as i-ésimas coordenadas x_i e y_i são iguais para todo i.

Do mesmo modo, a propriedade de d_H ser simétrica é satisfeita pois as i-ésimas coordenadas de x que o diferem de y também são as i-ésimas coordenadas de y que o diferem de x. Isto é, $d_H(x, y) = d_H(y, x)$.

Por fim, a desigualdade triangular é mostrada a partir do raciocínio que a contribuição das i-ésimas coordenadas de x e y para $d_H(x, y)$ é igual a zero se $x_i = y_i$, e igual a um se $x_i \neq y_i$. No caso em que a contribuição é igual a zero, certamente a contribuição das i-ésimas coordenadas a $d_H(x, y)$ é menor ou igual a

das i-ésimas coordenadas a $d_H(x,z) + d_H(z,y)$ podendo assumir os valores 0, 1 ou 2. No outro caso, temos que $x_i \neq y_i$ e, portanto, não podemos ter $x_i = z_i$ e $z_i = y_i$. Consequentemente, a contribuição das i-ésimas coordenadas a $d_H(x,z) + d_H(z,y)$ é maior ou igual a um, que é a contribuição das i-ésimas coordenadas a $d_H(x,y)$. □

A métrica de Hamming foi criada com base em uma ideia fundamental: medir a distância entre duas sequências de bits para avaliar sua similaridade ou diferença. Essa métrica, desenvolvida por Hamming, aparece pela primeira vez em seu artigo [10] de 1950.

Como vimos, a métrica de Hamming conta o número de bits que precisam ser alterados em uma sequência para se igualar à outra, de forma que quanto maior o número de posições diferentes, maior a distância de Hamming entre as sequências. Entretanto, se considerarmos um vetor $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$, o peso de Hamming $\omega_H(x)$ identifica o número de coordenadas não nulas de x, mas ignora totalmente o valor assumido por estas coordenadas quando estes não se anulam. A fim de obter um refinamento natural da métrica de Hamming, vamos definir as métricas que são parte fundamental do escopo deste texto.

Em seu artigo de 1958, [19], Lee definiu a métrica circular em $\mathbb{F}_q^n$: a distância entre duas palavras é a soma das distâncias entre suas i-ésimas letras. Lee percebeu que as características da métrica circular podem ser observadas em certos dispositivos físicos e eletrônicos, como rodas de impressão ou anéis contadores.

Se considerarmos que $0 \leq x_i \leq q-1$ para cada $i = 1, 2, \ldots, n$ e que estamos trabalhando módulo q, podemos identificar $\mathbb{F}_q \cong \mathbb{Z}_q$ com as i-ésimas raízes da unidade $\{e^0, e^{2\pi i/q}, e^{4\pi i/q}, \ldots, e^{2(q-1)\pi i/q}\}$, que são vértices de um polígono regular de q lados no plano. Assim, dadas a e b as i-ésimas letras de duas palavras quaisquer, a distância circular entre a e b é o menor número de arestas de um polígono regular de q lados que precisamos percorrer para ligar $e^{2a\pi i/q}$ e $e^{2b\pi i/q}$.

De forma mais rigorosa, definimos a métrica circular como a seguir:

Definição 2.3.18. Definimos a *métrica de Lee (ou métrica circular)* $d_L(x,y)$ entre dois pontos $x, y \in \mathbb{Z}_q^n$ como sendo

$$d_L(x,y) = d_L((x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n)) = \sum_{i=1}^{n} |x_i - y_i|_L, \tag{2.2}$$

onde

$$\begin{aligned} |x_i - y_i|_L &= \min\{x_i - y_i, y_i - x_i\} \pmod q \\ &= \min\{|x_i - y_i|, q - |x_i - y_i|\} \end{aligned}$$

e $|\cdot|$ é o valor absoluto usual em $\mathbb{R}$.

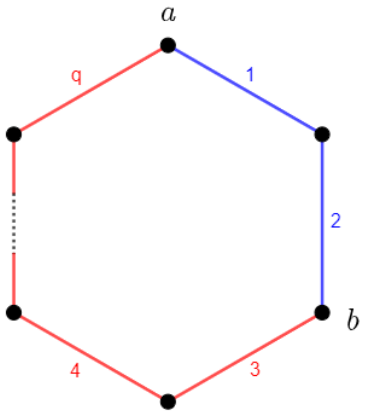
Observação 2.3.19. Na Definição 2.3.18, não exigimos que $\mathbb{Z}_q$ seja corpo, como proposto (mas não provado) por Ulrich em [27]. Apresentamos uma demonstração de que $(\mathbb{Z}_q^n, d_L)$ é, de fato, um espaço métrico na Proposição 2.3.21.

Exemplo 2.3.20. Sejam $a, b \in \mathbb{Z}_q$. Queremos calcular $d_L(a, b)$. Temos

$$d_L(a,b) = |a-b|_L = \min\{|a-b|, q-|a-b|\} = \begin{cases} |a-b|, & \text{se } |a-b| \leq \dfrac{q}{2}; \\ q-|a-b|, & \text{caso contrário.} \end{cases}$$

Agora, utilizando o raciocínio geométrico, suponha que a e b sejam vértices de um q-ágono regular no plano. Podemos supor que a esteja posicionado entre as faces ordenadas 1 e q. Consideremos b posicionado como na Figura 8.

Figura 8 – Exemplo da definição da métrica de Lee em um q-ágono regular.



Fonte: Elaborada pelo autor (2023).

As trajetórias em azul e vermelho representam o caminho para ligarmos os vértices a e b e assim, o mínimo módulo q é exatamente a menor trajetória a

ser percorrida. Note que se $|a-b| \leq \frac{q}{2}$, a menor trajetória será a azul em sentido horário e caso $|a-b| > \frac{q}{2}$, a vermelha em sentido anti-horário.

Proposição 2.3.21. *A métrica de Lee d_L é, de fato, uma métrica em $\mathbb{Z}_q^n$.*

Demonstração. Vamos utilizar a definição de d_L para mostrar que a métrica de Lee é positiva definida, simétrica e obedece à desigualdade triangular.

Como $\mathbb{Z}_q^n$ é descrito a partir de n cópias de $\mathbb{Z}_q$, basta mostrarmos que d_L é uma métrica em $n = 1$, pois um argumento indutivo implicaria em realizarmos a operação de distância entre as i-ésimas componentes do espaço $\mathbb{Z}_q^n$ separadamente.

Desta maneira, consideremos $x, y \in \mathbb{Z}_q$.

Como $d_L(x,y) = \min\{x-y, y-x\} \pmod q$ (pela Definição 2.3.18), segue imediatamente que $0 \leq d_L(x,y) < q$, em particular, $d_L(x,y) \geq 0$. Portanto, d_L é positiva definida e, $d_L(x,y) = 0$ se, e só, se $x = y$.

Novamente, utilizando a Definição 2.3.18, temos

$$\begin{aligned} d_L(x,y) &= \min\{x-y, y-x\} \pmod q \\ &= \min\{y-x, x-y\} \pmod q \\ &= d_L(y,x). \end{aligned}$$

Portanto, d_L é simétrica.

Por fim, note que como $d_L(x,y) = \min\{|x-y|, q-|x-y|\}$ segue que $d_L(x,y) \leq |x-y|$ e também, $d_L(x,y) \leq q-|x-y|$.

Daí, dado $z \in \mathbb{Z}_q$, temos as seguintes possibilidades para $|x-z|_L$ e $|z-y|_L$:

1. $d_L(x,z) = |x-z|$ e $d_L(z,y) = |z-y|$;

$$\begin{aligned} d_L(x,y) &\leq |x-y| \\ &= |x+z-z-y| \\ &= |(x-z)+(z-y)| \\ &\leq |x-z| + |z-y| \\ &= d_L(x,z) + d_L(z,y). \end{aligned}$$

2. $d_L(x,z) = |x-z|$ e $d_L(z,y) = q - |z-y|$, ou o contrário;

$$\begin{aligned} d_L(x,y) &\leq q - |x-y| \\ &= q - |x+z-z-y| \\ &= q - |(x-z)+(z-y)| \\ &\leq q - (|x-z| + |z-y|) \\ &= q - |x-z| - |z-y| \\ &\leq q - |x-z| - |z-y| + 2|x-z| \\ &= |x-z| + q - |z-y| \\ &= d_L(x,z) + d_L(z,y). \end{aligned}$$

3. $d_L(x,z) = q - |x-z|$ e $d_L(z,y) = q - |z-y|$;

$$\begin{aligned} d_L(x,y) &\leq q - |x-y| \\ &\leq 2q - |x-y| \\ &= 2q - |x+z-z-y| \\ &= 2q - |(x-z)+(z-y)| \\ &\leq 2q - (|x-z| + |z-y|) \\ &= 2q - |x-z| - |z-y| \\ &= q - |x-z| + q - |z-y| \\ &= d_L(x,z) + d_L(z,y). \end{aligned}$$

Portanto, em todos os casos, $d_L(x,y) \leq d_L(x,z) + d_L(z,y)$, isto é, vale a desigualdade triangular para d_L.

Logo, como mostramos, d_L é de fato uma métrica em $\mathbb{Z}_q$, assim pela discussão inicial, segue que d_L é métrica em $\mathbb{Z}_q^n$. □

Analogamente à métrica de Lee, em $\mathbb{R}^n$ definimos:

Definição 2.3.22. Sejam $x, y \in \mathbb{R}^n$. Definimos a *métrica de Manhattan* (também conhecida como métrica L^1, do táxi ou da soma) como

$$d_l(x,y) = d_l((x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n)) = \sum_{i=1}^{n} |x_i - y_i|, \tag{2.3}$$

onde $|\cdot|$ é o valor absoluto usual em $\mathbb{R}^n$.

Proposição 2.3.23. *A métrica de Manhattan é, de fato, uma métrica em* $\mathbb{R}^n$.

Definição 2.3.24. Seja $\mathcal{C}$ um código de Lee. Para $q \geq 2$, $n \in \mathbb{N}$ e um inteiro $e > 0$, definimos a bola de Lee em $\mathbb{Z}_q^n$ (e $\mathbb{Z}^n$) de raio e e centro em um ponto $x \in \mathcal{C}$ como

$$qL(n, e, x) = qL_{n,e}(x) = \{y \in \mathbb{Z}_q^n \,:\, d_L(y, x) \leq e\},$$
$$L(n, e, x) = L_{n,e}(x) = \{y \in \mathbb{Z}^n \,:\, d_l(y, x) \leq e\}.$$

Observação 2.3.25. No decorrer do texto, nos referimos como *Códigos de Lee* tanto os códigos q-ários sobre $\mathbb{Z}_q^n$ quanto os reticulados sobre $\mathbb{Z}^n$ munidos das métricas de Lee e de Manhattan, respectivamente. Além disso, quando não houverem duplas interpretações, podemos omitir a coordenada x e denotarmos as bolas de Lee simplesmente por $qL_{n,e}$ e $L_{n,e}$, assim como nos referirmos apenas como $L_{n,e}$ mesmo que estejam sobre $\mathbb{Z}_q^n$.

As proposições a seguir mostram os respectivos raios de empacotamento para códigos na métrica de Hamming e na métrica de Lee:

Proposição 2.3.26. *Considerando em* $\mathbb{F}_q^n$ *a métrica de Hamming, temos que para todo código linear* $\mathcal{C} \subset \mathbb{F}_q^n$, $\left\lfloor \dfrac{\delta_{\min} - 1}{2} \right\rfloor = \rho(\mathcal{C})$, *onde* $\delta_{\min}$ *é a distância mínima de* $\mathcal{C}$ *na métrica de Hamming.*

Demonstração. Vamos mostrar que se $r > \left\lfloor \dfrac{\delta_{\min} - 1}{2} \right\rfloor$ então existem $x, y \in \mathcal{C}$ tais que $B_H(x; r) \cap B_H(y; r) \neq \emptyset$.

Se $\delta_{\min} = 2k + \varepsilon$, com $\varepsilon \in \{0, 1\}$, então

$$k + \varepsilon = \left\lfloor \frac{\delta_{\min} - 1}{2} \right\rfloor + 1\,.$$

Como existe $x = (x_1, x_2, \ldots, x_n) \in \mathcal{C}$, tal que $\omega_H(x) = \delta_{\min}$. Então, x possui exatamente $2k + \varepsilon$ coordenadas não nulas. Suponhamos que estas sejam as coordenadas no conjunto $I \cup J \cup \{l_\varepsilon\}$ onde

$$I = \{i_1, i_2, \ldots, i_k\},$$
$$J = \{j_1, j_2, \ldots, j_k\}$$

e $\{l_\varepsilon\} = \emptyset$ se $\varepsilon = 0$.

Seja $z = (z_1, z_2, \ldots, z_n)$ o vetor definido por

$$z_m = \begin{cases} x_m, & \text{se} \quad m \notin I \cup \{l_\varepsilon\}, \\ 0, & \text{se} \quad m \in I \cup \{l_\varepsilon\}. \end{cases}$$

Temos então

$$d_H(z, x) = \#(I \cup \{l_\varepsilon\}) = k + \varepsilon$$

e

$$d_H(z, 0) = \#J = k\,.$$

Assim, $z \in B_H(0; k+\varepsilon) \cap B_H(x; k+\varepsilon)$, de modo que $\rho(\mathcal{C}) < k+\varepsilon = \left\lfloor \frac{\delta_{\min} - 1}{2} \right\rfloor + 1$ e concluímos que $\rho(\mathcal{C}) = \left\lfloor \frac{\delta_{\min} - 1}{2} \right\rfloor$. □

Proposição 2.3.27. *Considerando em $\mathbb{Z}_q^n$ a métrica de Lee, temos que para todo código linear q-ário $\mathcal{C} \subseteq \mathbb{Z}_q^n$, $\left\lfloor \frac{\delta_{\min} - 1}{2} \right\rfloor = \rho(\mathcal{C})$, onde $\delta_{\min}$ é a distância mínima de $\mathcal{C}$ na métrica de Lee.*

Demonstração. Vamos mostrar que as bolas de Lee centradas nas palavras do código $\mathcal{C}$ e com raio $\rho = \rho(\mathcal{C})$, não se interceptam.

Suponha que exista $x \in qL(n, \rho, c_1) \cap qL(n, \rho, c_2)$, com $c_1, c_2 \in \mathcal{C}$.

Então, temos:

$$d_L(c_1, c_2) \leq d_L(c_1, x) + d_L(x, c_2) \leq 2\rho \leq 2\left(\frac{\delta_{\min} - 1}{2}\right) < \delta_{\min},$$

o que é uma contradição.

Agora, mostremos que ρ é, de fato, o maior raio inteiro tal que as bolas de Lee em torno de cada palavra do código $\mathcal{C}$ não se tocam.

Seja $\rho_0 = \rho + 1$.

Suponhamos que as bolas de Lee em torno de cada palavra do código $\mathcal{C}$ com raio ρ_0 não se interceptem.

Desta maneira, para todo $a, b \in \mathcal{C}$, temos que

$$d_L(a,b) > 2(\rho+1) = 2\rho+2 = \begin{cases} \delta_{\min}+1, & \text{se} \quad \delta_{\min} \text{ for par;} \\ \delta_{\min}+2, & \text{se} \quad \delta_{\min} \text{ for ímpar,} \end{cases}$$

o que contradiz o fato de $\delta_{\min}(\mathcal{C}) = \min\{d_L(x,0)\,;\, 0 \neq x \in \mathcal{C}\}$. □

Proposição 2.3.28. *Seja $\mathcal{C} \subseteq \mathbb{Z}_q^n$ um código linear com raio de empacotamento $\rho = \rho(\mathcal{C})$ na métrica de Lee. Se $2\rho < q$, então o reticulado q-ário $\Lambda(\mathcal{C}) \subseteq \mathbb{Z}^n$ associado a $\mathcal{C}$ por meio da Construção A é um código com raio de empacotamento $\rho(\mathcal{C})$ na métrica de Manhattan.*

Demonstração. Seja $\rho(\Lambda_A(\mathcal{C}))$ o raio de empacotamento do reticulado $\Lambda_A(\mathcal{C})$.

Pela construção de $\Lambda_A(\mathcal{C})$, temos que $\rho(\Lambda_A(\mathcal{C})) \leq \rho(\mathcal{C})$. Vamos mostrar então que, $\rho(\Lambda_A(\mathcal{C})) = \rho(\mathcal{C})$.

Suponhamos que existam $x \in \mathbb{Z}^n$ e $y_1, y_2 \in \Lambda_A(\mathcal{C})$ tais que $d_l(x, y_1) \leq \rho$ e $d_l(x, y_2) \leq \rho$.

Considerando os resíduos módulo q, temos $d_L(\overline{x}, \overline{y_1}) \leq \rho$ e $d_L(\overline{x}, \overline{y_2}) \leq \rho$, com $\overline{y_1}, \overline{y_2} \in \mathcal{C}$.

Daí, temos que $\overline{y_1} = \overline{y_2}$ pois, caso contrário, $\overline{x} \in qL(n, \rho, \overline{y_1}) \cap qL(n, \rho, \overline{y_2})$, que é um absurdo, dado que $\rho(\mathcal{C})$ é o raio de empacotamento de $\mathcal{C}$.

Portanto, segue que $y_1 = y_2 + qy$, para algum $y \in \mathbb{Z}^n$, e assim

$$\begin{aligned} d_l(y_1, y_2) &= d_l(y_2 + qy, y_2) \\ &= d_l(qy, 0) \\ &= q \cdot d_l(y, 0), \end{aligned}$$

pois $\Lambda_A(\mathcal{C})$ é linear.

Entretanto, temos também que

$$d_l(y_1, y_2) \leq d_l(y_1, x) + d_l(x, y_2) \leq \rho + \rho = 2\rho < q,$$

por hipótese.

Assim, $q \cdot d_l(y, 0) < q$ o que implica em $y = 0$ e portanto, $y_1 = y_2$.

Logo, as bolas de raio $\rho = \rho(\mathcal{C})$ centradas na palavras de $\Lambda_A(\mathcal{C})$ são disjuntas, de modo que $\rho(\Lambda_A(\mathcal{C})) \geq \rho(\mathcal{C})$ o qual concluímos que $\rho(\Lambda_A(\mathcal{C})) = \rho(\mathcal{C})$, como queríamos provar. □

A definição a seguir decorre imediatamente da definição de distância mínima em um código de Lee:

Definição 2.3.29. Dizemos que um código de Lee $\mathcal{C}$ é um *código e-corretor de erros* se quaisquer dois elementos distintos de $\mathcal{C}$ têm distância pelo menos igual a $2e + 1$.

Por fim, vejamos uma proposição que mostra a equivalência das métricas de Hamming e Lee para certos espaços.

Proposição 2.3.30. *Se $p = 2$ ou $p = 3$, a métrica de Lee coincide com a métrica de Hamming em $\mathbb{Z}_p$.*

Demonstração. Com efeito, se $a, b \in \mathbb{Z}_2$ então

$$d_L(a,b) = \begin{cases} \min\{0,2\} = 0, & \text{se } a = b \\ \min\{1,1\} = 1, & \text{se } a \neq b\,. \end{cases}$$

Agora, se $a, b \in \mathbb{Z}_3$, então

$$d_L(a,b) = \begin{cases} \min\{0,3\} = 0, & \text{se } a = b \\ \min\{1,2\} = 1, & \text{se } a \neq b\,. \end{cases}$$

Logo, para $a, b \in \mathbb{Z}_p$, com $p = 2$ ou $p = 3$ temos

$$\begin{aligned} d_L(a,b) &= \begin{cases} 0, & \text{se } a = b \\ 1, & \text{se } a \neq b \end{cases} \\ &= d_H(a,b). \end{aligned}$$

□

2.3.4 Códigos perfeitos na métrica de Hamming

A partir deste ponto, vamos apresentar os critérios para que um código seja perfeito utilizando a métrica de Hamming, lembrando que investigaremos esta classe de códigos apenas sobre corpos finitos $\mathbb{F}_q$. Nosso intuito é iniciar uma discussão sobre os códigos perfeitos e deixaremos o estudo dos códigos perfeitos com erros medidos na métrica de Lee para os próximos capítulos.

Definição 2.3.31. Dizemos que um código linear $\mathcal{C} \subset \mathbb{F}_p^n$ é um *código perfeito* se

$$\bigcup_{u \in \mathcal{C}} B(u; r) = \mathbb{F}_p^n$$

e

$$B(u; r) \cap B(v; r) = \emptyset$$

qualquer que seja $u, v \in \mathcal{C}$ com $u \neq v$. Neste caso, $r = \rho(\mathcal{C})$.

O Lema 2.3.32 e o Corolário 2.3.33 serão importantes para o estudo de códigos perfeitos na métrica de Hamming.

Lema 2.3.32. *Seja H a matriz teste de paridade de um código linear $\mathcal{C}$. Temos que o peso de $\mathcal{C}$ é maior do que ou igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes.*

Demonstração. Primeiramente, suponhamos que cada conjunto de $s-1$ colunas de H é linearmente independente. Seja $c = (c_1, c_2, \ldots, c_n)$ uma palavra não nula de $\mathcal{C}$, e sejam $h^1, h^2, \ldots, h^n$ as colunas de H. Como $Hc^t = 0$, temos que

$$0 = H \cdot c^t = \sum_{i=1}^{n} c_i h^i. \tag{2.4}$$

Uma vez que $\omega(c)$ é o número de componentes não nulas de c, segue que se $\omega(c) \leq s-1$, teríamos por (2.4) uma combinação resultando no vetor nulo de um número l de colunas de H, com $1 \leq l \leq s-1$, o que é um contradição. Logo, $\omega(c) \geq s$ e, portanto, $\omega(\mathcal{C}) \geq s$.

Reciprocamente, suponhamos que $\omega(\mathcal{C}) \geq s$. Suponhamos também, por absurdo, que H tenha $s-1$ colunas linearmente dependentes, digamos $h^{i_1}, h^{i_2}, \ldots, h^{i_{s-1}}$.

Daí, existiriam $c_{i_1}, c_{i_2}, \ldots, c_{i_{s-1}}$, não todos nulos, no corpo tais que

$$c_{i_1}h^{i_1} + c_{i_2}h^{i_2} + \ldots + c_{i_{s-1}}h^{i_{s-1}}.$$

Portanto, $c = (0, \ldots, c_{i_1}, 0, \ldots, c_{i_2}, 0, \ldots, c_{i_{s-1}}, 0, \ldots, 0) \in \mathcal{C}$ e, assim,

$$\omega(c) \leq s - 1 < s,$$

o que é uma contradição. □

Corolário 2.3.33. *Seja H a matriz teste de paridade de um código linear $\mathcal{C}$. Temos que o peso de $\mathcal{C}$ é igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H são linearmente dependentes.*

Demonstração. Com efeito, suponhamos que $\omega(\mathcal{C}) = s$, logo, todo conjunto de $s-1$ colunas de H é linearmente independente. Por outro lado, existem s colunas de H linearmente dependentes pois, caso contrário, pelo Lema 2.3.32, teríamos $\omega(\mathcal{C}) \geq s + 1$.

Reciprocamente, suponhamos que todo conjunto de $s-1$ vetores colunas de H é linearmente independente e existem s colunas linearmente dependentes. Pelo Lema 2.3.32, temos que $\omega(\mathcal{C}) \geq s$. Mas $\omega(\mathcal{C})$ não pode ser maior que s pois, neste caso, novamente o Lema 2.3.32 nos diria que todo conjunto com s colunas de H é linearmente independente, o que é uma contradição. □

Definição 2.3.34. Sejam $n = 2^r - 1$, com $r \geq 2$, e H_r a matriz de ordem $r \times (2^r - 1)$ cujas colunas são todos os vetores não nulos de $\mathbb{F}_2^r$. O código linear

$$\mathcal{H}_r = \{x \in \mathbb{F}_2^{2^r-1} \ : \ H_r \cdot x^t = 0\}$$

que tem H_r como matriz de verificação de paridade é chamado de *Código de Hamming*. Temos que $\mathcal{H}_r$ é um $[2^r - 1; 2^r - r - 1]$ código linear.

Teorema 2.3.35. *Um código de Hamming $\mathcal{H}_r$ tem distância mínima* 3.

Demonstração. Seja H_r a matriz de verificação de paridade de $\mathcal{H}_r$. Pelo Corolário 2.3.33 para mostrarmos que a distância mínima $\delta_{\min}$ do código é igual a 3 basta mostrarmos que quaisquer pares de colunas de H_r são linearmente independentes e existem 3 colunas de H_r que são linearmente dependentes.

De fato, quaisquer 2 colunas são sempre linearmente independentes pois as colunas de H_r são os $2^r - 1$ vetores não nulos de $\mathbb{F}_2^r$ e, desta maneira suas colunas são duas a duas linearmente independentes. Agora, podemos afirmar que existem 3 colunas de H_r que são linearmente dependentes pois o conjunto $\{h_1, h_2, h_3\}$, onde $h_1, h_2 \in \mathbb{F}_2^r$ e $h_3 = h_1 + h_2 \in \mathbb{F}_2^r$, é linearmente dependente e, assim, segue o resultado. □

Lema 2.3.36. *Sejam $x \in \mathbb{F}_p^n$ e $n \in \mathbb{N}$. Então,*

$$\#(B_H(x;r)) = \sum_{i=0}^{r} \binom{n}{i} (p-1)^i$$

Demonstração. Inicialmente, note que $\#(B_H(x;r)) = \#(B_H(0;r))$, pois a translação do centro de uma bola da origem para um ponto qualquer estabelece uma bijeção entre $\#(B_H(x;r))$ e $\#(B_H(0;r))$.

Se $y \in B_H(0;r)$ então y possui exatamente i coordenadas não nulas para algum $i \leq r$. Desta maneira, temos $\binom{n}{i}$ possíveis escolhas para as coordenadas de y. E ainda, como cada coordenada não nula de y pode assumir os valores $1, 2, \ldots, p-1$, temos um total de $\binom{n}{i}(p-1)^i$ vetores que distam i de um ponto.

Portanto,

$$\#(B_H(x;r)) = \sum_{i=0}^{r} \binom{n}{i} (p-1)^i$$

como queríamos demonstrar. □

Teorema 2.3.37. *O código de Hamming $\mathcal{H}_r$ é um código perfeito na métrica de Hamming.*

Demonstração. Primeiramente, pelo Teorema 2.3.35, sabemos que a distância mínima de $\mathcal{H}_r$ é 3. Portanto, o raio de empacotamento de $\mathcal{H}_r$ é igual a $\left\lfloor \frac{3-1}{2} \right\rfloor = 1$. Afirmamos que as bolas de raio 1 centradas nos elementos de $\mathcal{H}_r$ cobrem $\mathbb{F}_2^{2^r-1}$.

De fato, pelo Lema 2.3.36 temos

$$\begin{aligned} \#(B_H(u;1)) &= \binom{2^r-1}{0} + \binom{2^r-1}{1} \\ &= 1 + (2^r - 1) \\ &= 2^r, \end{aligned}$$

para todo $u \in \mathcal{H}_r$ e

$$\begin{aligned} 2^r \cdot \#\mathcal{C} &= 2^r \cdot (2^{2^r - r - 1}) \\ &= 2^{2^r - 1} \\ &= \#(\mathbb{F}_2^{2^r - 1}). \end{aligned}$$

Portanto, concluímos que as bolas $B_H(u; 1)$ cobrem $\mathbb{F}_2^{2^r-1}$ e assim, $\mathcal{H}_r$ é um código perfeito. □

Nesta seção, vimos uma classe de códigos lineares com erros medidos na métrica de Hamming, conhecidos como *Códigos Binários de Correção de Erros*, os quais somos capazes de determinar os parâmetros a fim de que tais códigos sejam perfeitos. Isto é, dado $r > 0$, para que um código de Hamming seja perfeito basta tomarmos $q = 2$ e $n = 2^r - 1$, o que implica em um código linear que possui $2^r - r - 1$ elementos em sua base e distância mínima $\delta_{\min} = 3$. Portanto, a capacidade de correção de um código de Hamming é de 1 erro e assim, sempre é possível detectar e corrigir os erros nas mensagens.

Entretanto, como já discutimos anteriormente, a métrica de Hamming considera apenas coordenadas distintas em seu cálculo, e vimos inclusive, que a métrica de Lee nos parece mais eficaz, no sentido de ponderar sobre outras informações intrínsecas ao espaço em que estivermos trabalhando.

Nesta direção, uma pergunta importante que devemos nos fazer é: é possível determinar, para os códigos de Lee, uma quantidade q de letras para as quais as bolas n-dimensionais de raio e em torno das palavras do código nos forneçam empacotamentos perfeitos dos espaços?

3 CÓDIGOS PERFEITOS NA MÉTRICA DE LEE

Neste capítulo, estamos interessados em tentar responder a pergunta feita no final do capítulo anterior. Estudaremos casos especiais em que um código possa ser perfeito na métrica de Lee para certos parâmetros e veremos a Conjectura de Golomb-Welch, cuja demonstração geral ainda está em aberto.

3.1 GEOMETRIA DOS ESPAÇOS E BOLAS

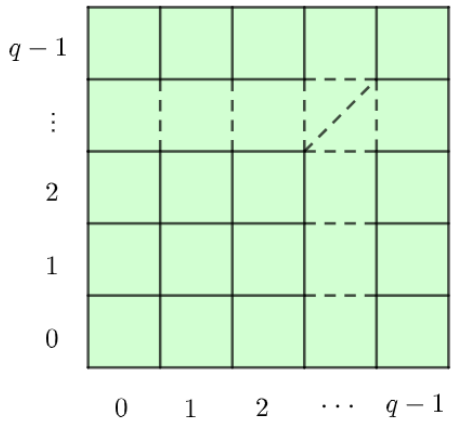
Antes de prosseguirmos no estudo dos códigos perfeitos na métrica de Lee, precisamos definir os entes geométricos com os quais iremos trabalhar, sejam eles a estrutura das bolas ou até mesmo os espaços em questão.

Definição 3.1.1. Sejam $n \in \mathbb{N}$ e um inteiro $q \geq 2$. Um q^n*-toro* é uma hipermatriz n-dimensional que consiste de $q \times q \times \cdots \times q = q^n$ células unitárias.

Se $n \geq 3$, nossa percepção limitada de espaço torna a visualização geométrica dos q^n-toros irrealizável. Faremos o caso particular 2-dimensional a seguir.

Exemplo 3.1.2. Sejam $q \geq 2$ e $n = 2$. O q^2-toro planificado é uma matriz com $q \times q$ células unitárias (Figura 9). Esta é a representação que associamos a $\mathbb{Z}_q^2$.

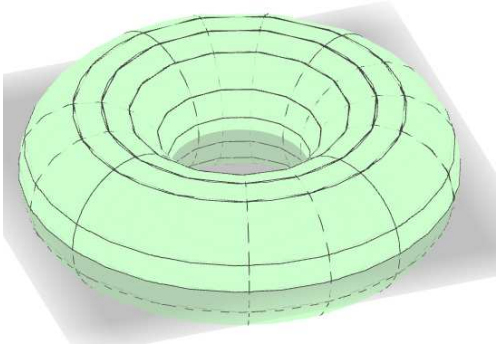
Figura 9 – q^2-toro planificado.



Fonte: Elaborada pelo autor (2023).

Porém, como em $\mathbb{Z}_q^2$, estamos trabalhando com as operações de soma e multiplicação módulo q, é natural que exista um tipo de periodicidade com esta matriz, no sentido de que os pontos $(q-1, y)$ e $(0, y)$ são adjacentes, assim como $(x, q-1)$ e $(x, 0)$, quaisquer que sejam $0 \leq x, y \leq q-1$. Não entraremos nas questões topológicas, mas, a grosso modo, podemos considerar que as laterais da matriz estão "coladas" obedecendo a orientação formando um cilindro, que também possui suas bordas "coladas" formando um toro (Figura 10).

Figura 10 – Visualização da superfície do q^2-toro.



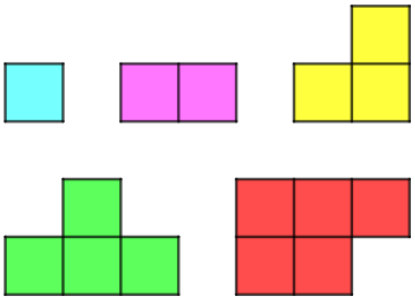
Fonte: Elaborada pelo autor (2023).

De forma geral, um q^n-toro é uma estrutura que envolve o espaço $\mathbb{Z}_q^n$ de forma toroidal, permitindo a continuidade nas bordas, refletindo as propriedades cíclicas e periódicas do espaço $\mathbb{Z}_q^n$. Cada coordenada em uma dimensão pode ser considerada como "anel" que envolve o espaço toroidal, e as coordenadas em diferentes dimensões se interconectam se assemelhando a uma série de anéis entrelaçados e torcidos, com furos centrais e túneis conectando os toroides.

O Exemplo 3.1.2 serve como um exercício de visualização dos espaços. No texto, utilizaremos apenas as representações geométricas planificadas dos q^n-toros.

Definição 3.1.3. Definimos como *poliominó* uma figura geométrica plana formada por quadrados iguais, unidos de modo que pelo menos um lado de cada quadrado coincida com um lado de outro quadrado. Identificamos cada poliominó com o prefixo grego apropriado de acordo com a quantidade de quadrados (Figura 11).

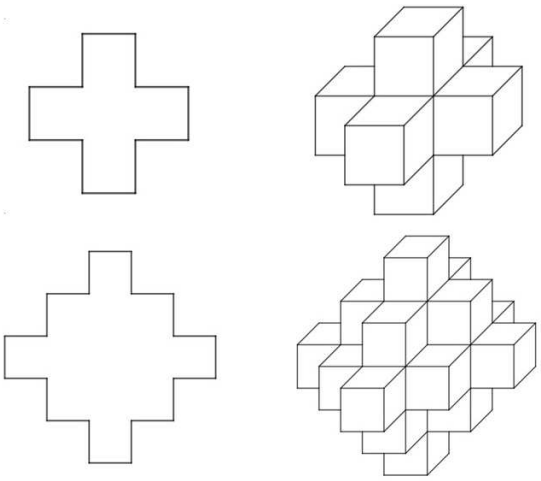
Figura 11 – Exemplos de mono, do, tri, tetra e pentominó, respectivamente.



Fonte: Elaborada pelo autor (2023).

Exemplo 3.1.4. Por conta da definição das métricas de Lee e de Manhattan, as bolas de Lee sobre $\mathbb{Z}_q^2$ e $\mathbb{Z}^2$, respectivamente, podem ser vistas como poliominós no espaço em que estão inseridas. A seguir mostramos a representação geométrica (ou poliominós) para os casos de bolas de Lee com parâmetros $(n, e) \in \{2, 3\} \times \{1, 2\}$:

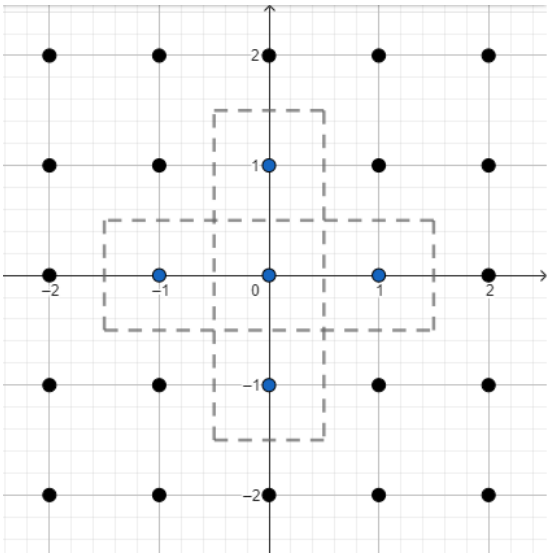
Figura 12 – Bolas de Lee $L_{2,1}, L_{3,1}, L_{2,2}$ e $L_{3,2}$, respectivamente.



Fonte: Elaborada pelo autor (2023).

No Exemplo 3.1.4, as bolas em $\mathbb{R}^n$ na métrica de Manhattan não são exatamente poliominós, embora sejam utilizadas por quase todos os autores sem perda de significado. Como $\mathbb{Z}^n$ é um espaço discreto, se considerarmos a métrica de Manhattan, a bola $L_{n,e}$ seria a princípio um conjunto de pontos isolados que estejam a uma distância no máximo igual a e do centro da bola. Entretanto, é usual que mesmo que estejamos trabalhando com métricas distintas, d_L e d_l, para dimensão n e raio e, as bolas sejam representadas pelo mesmo poliominó. O que varia em cada caso, de fato, é o espaço que elas estão inseridas.

Figura 13 – Bola $L(2, 1, (0, 0))$ em $\mathbb{R}^n$. O tracejado indica exatamente o X-pentominó de centro em $(0, 0)$.



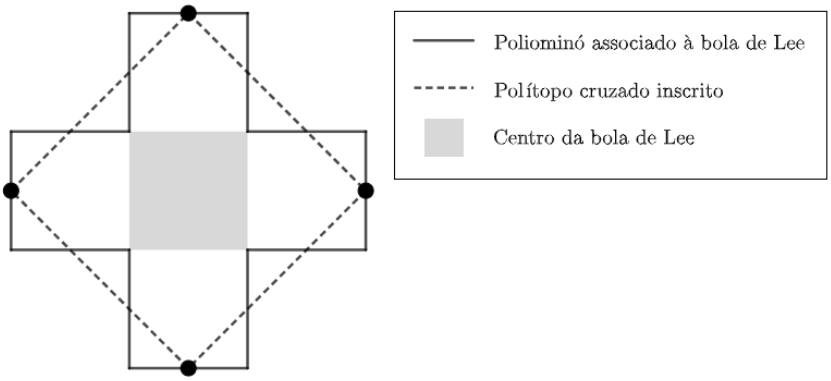
Fonte: Elaborada pelo autor (2023).

Definição 3.1.5. Sejam $n \in \mathbb{N}$ e um inteiro $e > 0$. Para toda esfera de Lee n-dimensional de raio e, $L_{n,e}$, definimos o *polítopo cruzado inscrito* $P_{n,e}$ como a menor figura convexa contendo os $2n$ pontos centrais de suas hiperfaces extremas $(n-1)$-dimensionais.

Na Figura 14, temos uma bola de Lee $L_{2,1}$ e o polítopo cruzado associado $P_{2,1}$. A bola de Lee possui 5 células, sendo que a célula em cinza é a palavra do

código na qual a bola está centrada. Note que, como $L_{2,1}$ é bidimensional, pela definição, as hiperfaces extremas consideradas devem ser unidimensionais. Assim, os pontos pretos na figura indicam as regiões centrais das hiperfaces (que neste caso são linhas) extremas ao centro da bola de Lee. Assim, a bola de Lee $L_{2,1}$ é representada pelo pentominó em formato de cruz e o polítopo cruzado associado à esfera, $P_{2,1}$, é a figura delimitada pelo tracejado, que, neste caso, é um quadrado.

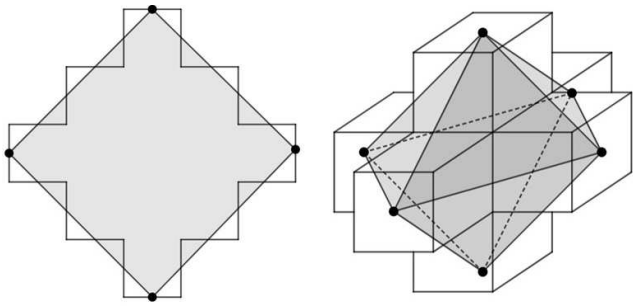
Figura 14 – Polítopo cruzado inscrito em uma bola de Lee.



Fonte: Elaborada pelo autor (2023).

Exemplo 3.1.6. Na Figura 15 vemos os polítopos cruzados inscritos nas bolas de Lee com parâmetros $(2, 2)$ e $(3, 1)$, respectivamente. Em dimensão 2, o polítopo é um quadrado, enquanto em dimensão 3, um octaedro regular.

Figura 15 – Polítopos cruzados $P_{2,2}$ e $P_{3,1}$.

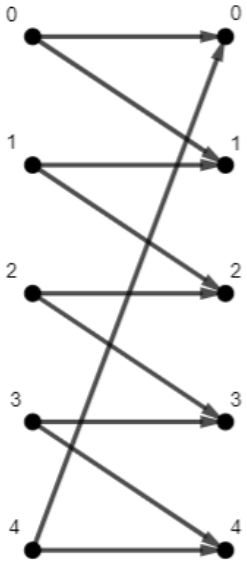


Fonte: Elaborada pelo autor (2023).

3.2 O PROBLEMA DE EMPACOTAR ESPAÇOS

Em seu artigo [26], Shannon considerou o problema de um código em que fosse possível eliminar completamente os erros em um canal usando um código 5-ário, utilizando um alfabeto de inteiros módulo 5, no qual o padrão dos erros é dado da seguinte forma, como na Figura 16.

Figura 16 – Canal de Shannon com 5 fases.



Fonte: Elaborada pelo autor (2023).

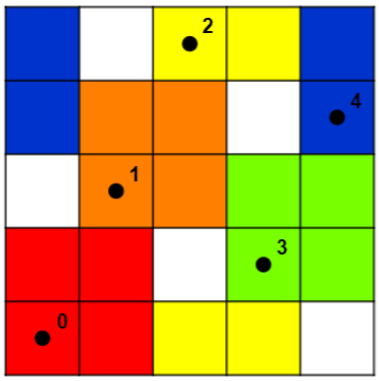
Quando um inteiro m é enviado, podemos receber os inteiros m ou $m+1$, com probabilidades p e q, respectivamente. Desta maneira, se este for um código, ao enviarmos um mesmo símbolo k vezes, ainda existe uma probabilidade q^k de um erro ocorrer em nossa mensagem. No entanto, existe um código, utilizando apenas duas letras do alfabeto por palavra que elimina os erros completamente.

Para eliminarmos os erros, basta definirmos

$$\begin{aligned} 0 &= (0,0) \\ 1 &= (1,2) \\ 2 &= (2,4) \\ 3 &= (3,1) \\ 4 &= (4,3) \end{aligned} \tag{3.1}$$

Neste código, se (a,b) é uma palavra do código, toda vez que as palavras (a,b), $(a+1,b)$, $(a,b+1)$ ou $(a+1,b+1)$ forem recebidas, podemos assegurar que ouve algum erro nos três últimos casos e a palavra enviada certamente foi (a,b). A representação geométrica deste fato é dada na Figura 17 a seguir.

Figura 17 – Representação geométrica do código.



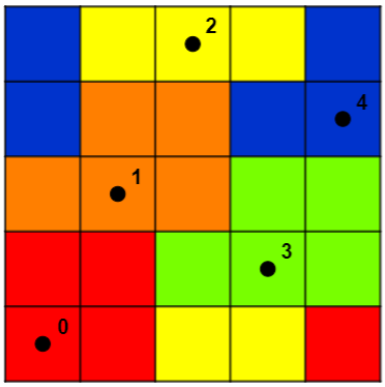
Fonte: Elaborada pelo autor (2023).

As 25 possíveis palavras (a,b) são representadas por 25 células do 5×5 toro, com coordenadas (a,b). As palavras do código (3.1) correspondem às células com pontos. À esquerda de cada ponto há uma célula "ambígua", porém, para que alguma dessas células seja acessada, deve ter ocorrido um erro no envio da mensagem e não na transmissão, pois é fácil ver que as células $(4,0)$, $(2,1)$, $(0,2)$, $(3,3)$ e $(1,4)$ não correspondem às palavras do código ou ainda, palavras do código

com erros provenientes do canal. Portanto, como nenhuma dessas ambiguidades são acessadas, qualquer mensagem recebida pode ser unicamente interpretada.

O empacotamento dos 5 quadrados 2×2 no 5×5 toro mostrado na Figura 17 é razoavelmente eficiente, mas o código não é perfeito. Em particular, há 5 pontos que não são relacionados a nenhuma das bolas em torno das palavras do código. Para o canal descrito pelos possíveis erros estatísticos na Figura 16, nenhuma melhoria adicional é possível. No entanto, se outros erros são remotamente possíveis, então é vantajoso atribuir os 5 pontos que não são usados às regiões de ambiguidade das 5 palavras do código. Façamos do seguinte modo: onde o erro que ocorre quando (a, b) é recebido como $(a - 1, b)$ também será corrigido. Como não há mais pontos do toro que não sejam relacionados a alguma palavra do código, este código fornece um empacotamento do espaço e corresponde geometricamente ao ladrilhamento do 5×5 toro utilizando P-pentominós, como na Figura 18:

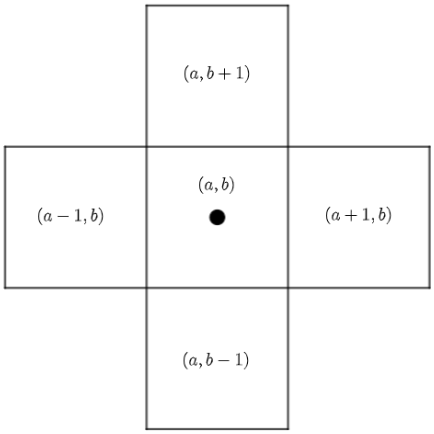
Figura 18 – Empacotamento do toro 5×5 por P-pentominós.



Fonte: Elaborada pelo autor (2023).

Observação 3.2.1. A bola com centro em um ponto (a, b) em $\mathbb{Z}_q^2$ de raio $e = 1$ na métrica de Lee é um X-pentominó cuja figura resultante é exatamente gerada a partir da palavra do código (a, b) deslocando suas componentes em 1 unidade, para cima e para baixo.

Figura 19 – O X-pentominó que representa a esfera de Lee de raio 1.



Fonte: Elaborada pelo autor (2023).

Este resultado mostraremos posteriormente mas, em geral, uma bola de Lee de raio e em duas dimensões, consiste em um poliominó que possui $e^2 + (e+1)^2 = 2e^2 + 2e + 1$ quadrados.

Desta forma, para um código em que estamos considerando a métrica de Lee podemos definir o seguinte:

Definição 3.2.2. Sejam $\mathcal{C}$ um código linear, $n \in \mathbb{N}$, inteiros $e, q > 0$ e d_L a métrica de Lee. Dizemos que $\mathcal{C}$ é um *código de Lee perfeito e-corretor de erros* se para cada $x \in \mathbb{Z}_q^n$, existe um único elemento $c \in \mathcal{C}$ tal que $d_L(x, c) \leq e$. O conjunto de tais códigos com estes parâmetros será denotado por $LP(n, e, q)$. Se $q \geq 2e + 1$, dizemos que $LP(n, e, q)$ está sobre um alfabeto grande e, caso contrário, sobre um alfabeto pequeno. Definimos o mesmo para os códigos de Lee sobre $\mathbb{Z}^n$ com a métrica de Manhattan d_l, denotando o conjunto neste caso por $LP(n, e)$.

Definição 3.2.3. Dizemos que um código de Lee e-corretor de erros sobre $\mathbb{Z}_q^n$ (ou $\mathbb{Z}^n$) é um *ladrilhamento* do espaço em que está contido, se este for um código perfeito e, assim as bolas de Lee, $qL(n, e)$ (ou $L(n, e)$) centradas nos pontos do código são ditas *ladrilhos* do espaço.

Observação 3.2.4. Visto que conseguimos caracterizar as esferas na métrica de Lee como poliominós, é natural pensarmos que exista uma equivalência ao cobrir o espaço em que estivermos trabalhando com tais peças. Neste sentido podemos dizer que se $P, X \subset \mathbb{Z}_q^n$, onde P é um poliominó e X um conjunto de pontos de $\mathbb{Z}_q^n$, uma coleção $\mathcal{P}$ de cópias de P obtidas por meio de translações, é um empacotamento de $\mathbb{Z}_q^n$ se:

$$(P + x) \cap (P + x') = \emptyset,$$

para todo $x, x' \in X$, tais que $x \neq x'$. Da mesma forma, dizemos que $\mathcal{P}$ é um ladrilhamento de $\mathbb{Z}_q^n$, se for um empacotamento tal que

$$\bigcup_{x \in X} P + x = \mathbb{Z}_q^n.$$

Como estamos nos tratando de códigos geometricamente uniformes, assim como fizemos para as bolas na métrica de Hamming, podemos determinar a quantidade de palavras em uma bola de Lee para um dado raio e, qualquer que seja a palavra do código em que a bola esteja centrada. Os lemas a seguir determinam a quantidade de palavras em uma bola de Lee e o diâmetro que tais bolas possuem.

Lema 3.2.5. *Sejam $n \in \mathbb{N}$, $e > 0$ e $q \geq 2$. Se $\mathcal{C} \subseteq \mathbb{Z}_q^n$ for um código geometricamente uniforme e-corretor de erros medidos na métrica de Lee, então:*

$$\#(qL_{n,e}(x)) = \sum_{k \geq 0} 2^k \binom{n}{k} \binom{e}{k},$$

qualquer que seja $x \in \mathcal{C}$.

Demonstração. Para calcularmos a quantidade de elementos em uma bola em torno de um ponto qualquer, podemos considerar as n componentes de uma palavra do código como "caixas" e assim, teremos e "redundâncias" para distribuir entre estas caixas.

Para qualquer $k \leq e$, vamos estudar o problema de distribuir as e redundâncias em exatamente k caixas. Existem $\binom{n}{k}$ maneiras de escolher k das n caixas para conter todos os incrementos. Cada k caixas escolhidas podem receber um desvio tanto positivo quanto negativo, bastando para isso notar que toda vez que

uma palavra com k-ésima coordenada x_k for enviada podemos receber tanto $x_k - 1$ quanto $x_k + 1$, de forma que há 2^k maneiras em que isto seja feito.

Por fim, existem $\binom{e}{k}$ maneiras de distribuir e redundâncias dentre as k caixas selecionadas de modo que nenhuma caixa fique vazia. Logo, temos

$$\#(qL_{n,e}(x_1, x_2, \ldots, x_n)) = \sum_{k\geq 0} 2^k \binom{n}{k}\binom{e}{k}.$$

Como consideramos apenas propriedades relacionadas à dimensão n e raio e, a palavra $x \in \mathcal{C}$, que é o centro da bola, pode ser tomada de forma arbitrária e assim, o resultado segue. □

Observação 3.2.6. Note que pelo Lema 3.2.5 temos

$$\#(qL_{n,e}) = \sum_{k\geq 0} 2^k \binom{n}{k}\binom{e}{k} = \sum_{k\geq 0} 2^k \binom{e}{k}\binom{n}{k} = \#(qL_{e,n}),$$

de modo que as bolas na métrica de Lee são simétricas em relação à n e e. Além disso, como $\binom{i}{j}$ não é definido quando $i < j$, podemos reescrever

$$\#(qL_{n,e}) = \sum_{k=0}^{\min\{n,e\}} 2^k \binom{n}{k}\binom{e}{k}.$$

Proposição 3.2.7. *O diâmetro de uma bola de Lee n-dimensional, $L_{n,e} \subset \mathbb{Z}^n$, é exatamente* $\operatorname{diam}(L_{n,e}) = 2e + 1$*, onde e é o raio da bola.*

Demonstração. Sejam $a = (a_1, a_2, \ldots, a_n)$ o centro de uma bola de Lee n-dimensional de raio e, $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ e $d = \operatorname{diam}(L_{n,e}(a))$ o diâmetro desta bola.

Se o ponto $(x_1, x_2, \ldots, x_n)$ pertence à bola $L_{n,e}(a)$, então:

$$d_l((a_1, a_2, \ldots, a_n), (x_1, x_2, \ldots, x_n)) \leq e.$$

Portanto, os pontos

$$(a_1 + e,\, a_2,\, \ldots,\, a_n),\ (a_1,\, a_2 + e,\, \ldots,\, a_n),\ \ldots,\ (a_1,\, a_2,\, \ldots,\, a_n + e),$$

assim como os pontos

$$(a_1 - e,\, a_2,\, \ldots,\, a_n),\ (a_1,\, a_2 - e,\, \ldots,\, a_n),\ \ldots,\ (a_1,\, a_2,\, \ldots,\, a_n - e)$$

pertencem à esfera com centro em a e raio e.

Por definição, o diâmetro é o supremo das distâncias entre dois pontos de um subconjunto de um espaço métrico.

Desta maneira, olhando para um i-ésimo eixo coordenado ($i = 1, 2, \ldots, n$), temos que os pontos

$$(a_1, \ldots, a_i - e, \ldots, a_n), (a_1, \ldots, a_i - e + 1, \ldots, a_n), (a_1, \ldots, a_i - e + 2, \ldots, a_n),$$
$$\ldots, (a_1, \ldots, a_i, \ldots, a_n), (a_1, \ldots, a_i + 1, \ldots, a_n), \ldots,$$
$$(a_1, \ldots, a_i + e - 1, \ldots, a_n), \ldots, (a_1, \ldots, a_i + e, \ldots, a_n)$$

pertencem à bola.

Logo, o ponto $(a_1, \ldots, a_i - e, \ldots, a_n)$ está a $2e$ pontos de distância do ponto $(a_1, \ldots, a_i + e, \ldots, a_n)$ e, desta forma o diâmetro d da bola é no mínimo $2e + 1$.

Suponhamos agora que o diâmetro da bola é maior que $2e + 1$.

Se $d > 2e + 1$, existe algum ponto $(a_1, \ldots, a_i + e + t, \ldots, a_n)$, onde $t \geq 1$, que pertence à bola.

Porém,

$$d_l((a_1, \ldots, a_i, \ldots, a_n), (a_1, \ldots, a_i + e + t, \ldots, a_n)) = |a_i + e + t - a_i| = e + t > e,$$

pois $e > 0$ e $t \geq 1$, o que é uma contradição.

Logo, o diâmetro d da bola é exatamente $2e + 1$. □

A proposição anterior pode ser repetida utilizando subconjuntos arbitrários de pontos da bola desde que estejam em uma mesma reta, porém, como o espaço Euclidiano $\mathbb{Z}^n$ é simétrico, basta calcularmos sobre um eixo dado e utilizarmos isometrias.

Proposição 3.2.8. ***(Cota de Hamming)*** *Seja $\mathcal{C} \subset \mathbb{Z}_q^n$ um código de Lee geometricamente uniforme e-corretor de erros. O número de palavras no dicionário de $\mathcal{C}$ não excede*

$$\frac{q^n}{\sum_{k \geq 0} 2^k \binom{n}{k} \binom{e}{k}}.$$

Demonstração. Sabemos que as palavras do código devem ser cercadas por bolas disjuntas de raio e. Além disso, há q^n palavras neste espaço, e cada palavra do código, que é centro de alguma bola, possui $\#(qL_{n,e})$ delas. Então, o código deve ter no máximo

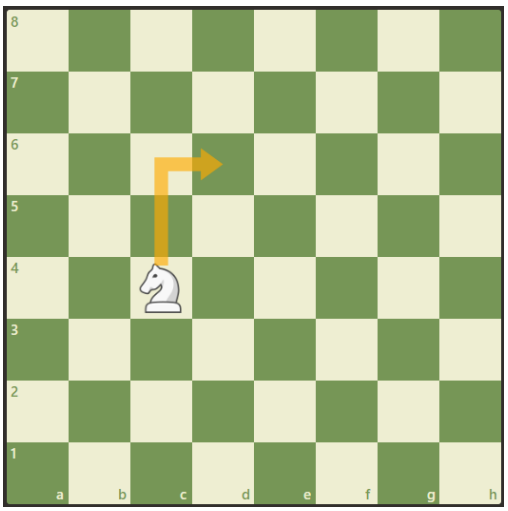
$$\#\mathcal{C} \leq \frac{q^n}{|qL_{n,e}|}$$

palavras.
Logo, pelo Lema 3.2.5, o resultado segue imediatamente. □

Uma condição necessária para que exista um empacotamento é que, dados n, e e q, $\#L(n,e)$ seja um divisor de q^n.

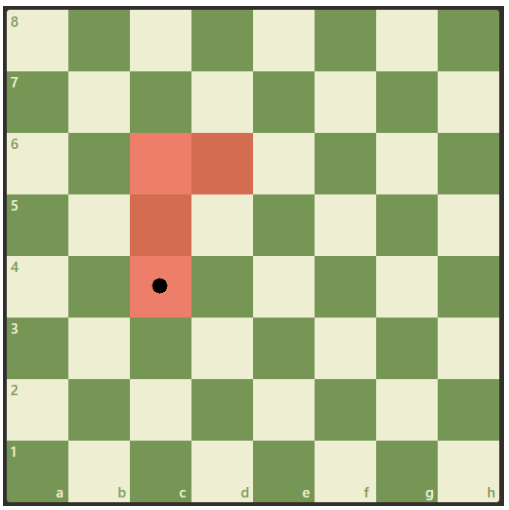
Exemplo 3.2.9. Consideremos um tabuleiro de xadrez no formato de um 8^2-toro em que a regra padrão é mantida. Como neste caso o tabuleiro possui as bordas opostas conectadas, a fileira 8 é adjacente à fileira 1, assim como a coluna h é adjacente à coluna a. Um cavalo pode se mover duas casas horizontalmente e, em seguida, uma casa verticalmente, entretanto fixemos o movimento do cavalo a duas casas pra cima e uma pra direita, como na Figura 20.

Figura 20 – Movimento do cavalo no xadrez.



Fonte: Elaborada pelo autor (2023).

Figura 21 – L-tetraminó gerado pelo salto do cavalo.

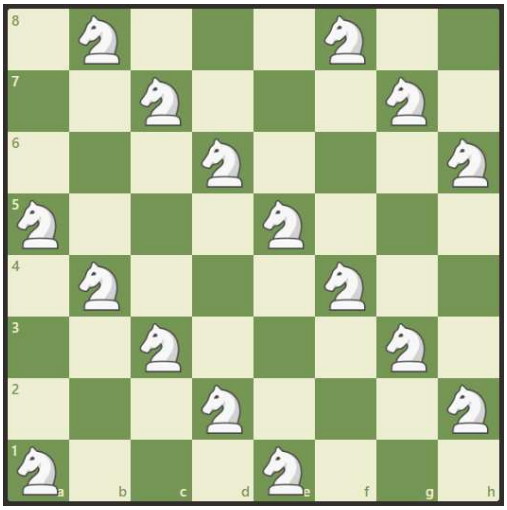


Fonte: Elaborada pelo autor (2023).

Considerando a casa inicial onde o cavalo está antes do movimento, sua trajetória pelo tabuleiro possui a forma de um L-tetraminó (Figura 21). Neste caso, temos uma peça com 4 células. Pela Proposição 3.2.8, como 4 divide 64, deve existir uma forma de cobrir este tabuleiro utilizando os tetraminós gerados pelo salto do cavalo. Nosso trabalho agora é determinar as posições iniciais dos cavalos.

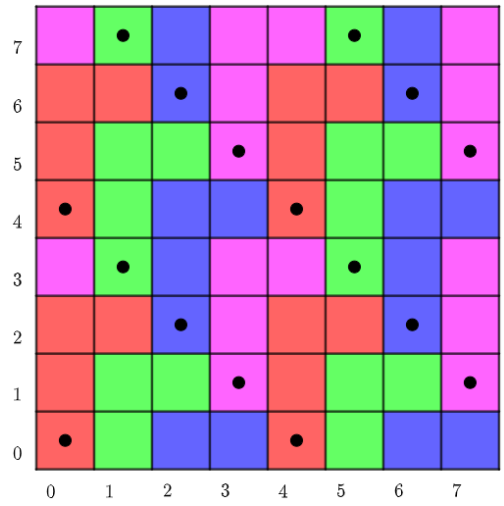
Coloquemos um cavalo em $a1$ e outro exatamente acima da casa que o cavalo anterior termina o salto. Por exemplo, dado o primeiro cavalo em $a1$, o segundo estará em $b4$, o terceiro em $c7$, o quarto em $d2$, e assim sucessivamente. Acontece que ao colocarmos o oitavo cavalo em $h6$, o nono retornaria para a casa $a1$. Assim, colocamos o nono cavalo na casa $a5$ e repetimos todo o processo. Note que esses 8 cavalos são exatamente translações dos 8 primeiros. A disposição final dos cavalos é dada na Figura 22.

Figura 22 – Disposição final dos 16 cavalos no tabuleiro.



Fonte: Elaborada pelo autor (2023).

Figura 23 – Empacotamento do 8^2-toro por 16 L-tetraminós.



Fonte: Elaborada pelo autor (2023).

Como cada cavalo gera uma peça que possui 4 células, podemos cobrir todo o tabuleiro toroidal, o que pode ser visto na Figura 23. Assim, o conjunto dos 16 L-tetraminós é um código perfeito em $\mathbb{Z}_8^2$. Este exemplo reforça a ideia de que não é necessário que as bolas de Lee possuam cardinalidade prima para que haja um ladrilhamento do espaço.

3.3 CONJECTURA DE GOLOMB-WELCH

Em seu artigo [7], Golomb e Welch discutem a existência de códigos $\mathcal{C} \in LP(n, e, q)$. Veremos nesta seção suas construções para determinados parâmetros. Os estudos que realizaram juntamente com as demonstrações apresentadas abrem caminho para a formulação da chamada Conjectura de Golomb-Welch.. É importante citarmos que neste texto, não cobriremos códigos lineares q-ários sobre alfabetos pequenos.

Por agora, vejamos os casos para os quais Golomb e Welch construíram códigos perfeitos com erros medidos na métrica de Lee:

Teorema 3.3.1. *Sejam um inteiro $e > 0$ e $q = 2e + 1$. Existe um código perfeito na métrica de Lee, e-corretor de erros e com palavras de comprimento 1 sobre um alfabeto com q letras.*

Demonstração. Seja $e > 0$. Consideremos o código $\mathcal{C} = \{a\}$, onde $a \in \mathbb{Z}_{2e+1}$. Sabemos que, independentemente da escolha da palavra a, a bola $qL_{1,e}(a)$ possui

$$\begin{aligned}
\#(qL_{1,e}(a)) &= \sum_{k=0}^{1} 2^k \binom{1}{k}\binom{e}{k} \\
&= 2^0\binom{1}{0}\binom{e}{0} + 2^1\binom{1}{1}\binom{e}{1} \\
&= 1 \cdot 1 \cdot 1 + 2 \cdot 1 \cdot e \\
&= 2e + 1
\end{aligned}$$

elementos. Como $\#\mathbb{Z}_{2e+1} = 2e + 1$ e $\mathcal{C}$ é composto por apenas uma palavra, segue que $qL_{1,e}(a) = \mathbb{Z}_{2e+1}$, qualquer que seja $a \in \mathbb{Z}_{2e+1}$. Logo, o código $\mathcal{C}$ é perfeito. □

Teorema 3.3.2. *Sejam um inteiro $e > 0$ e $q = 2e^2 + 2e + 1$. Existe um código perfeito na métrica de Lee, e-corretor de erros e com palavras de comprimento 2 sobre um alfabeto com q letras.*

Demonstração. Seja $\mathcal{C} = \{(a, (2e + 1)a) : a \in \mathbb{Z}_q\}$ um código em $\mathbb{Z}_q^2$. Vamos mostrar que $\mathcal{C}$ é perfeito na métrica de Lee.

Como $\mathcal{C}$ é um submódulo do $\mathbb{Z}_q$-módulo $\mathbb{Z}_q^2$ em relação à adição, coordenada a coordenada, $\mathcal{C}$ é um código linear e portanto a distância mínima $\delta_{\min}(\mathcal{C})$ é igual

ao seu peso mínimo. Daí, sabemos que o código $\mathcal{C}$ é e-corretor de erros se seu peso mínimo for pelo menos $2e+1$. Seja $a \not\equiv 0 \pmod{q}$ com $0 < a \leq q-1$. Temos:

$$\begin{aligned}\omega((a,(2e+1)a)) &= d_L((a,(2e+1)a),(0,0)) \\ &= |a-0|_L + |(2e+1)a-0|_L \\ &= \min\{|a|,\, q-|a|\} + \min\{|(2e+1)a|,\, q-|(2e+1)a|\}.\end{aligned}$$

Suponhamos que $d_L((a,(2e+1)a),(0,0)) \leq 2e+1$. Neste caso, como $|a|_L + |(2e+1)a|_L \leq 2e+1$, pelo menos uma das parcelas da soma anterior é menor ou igual a e.

Se $1 \leq |a|_L \leq e$, temos:

1. Se $|a|_L = a$, então:

$$\begin{aligned}d_L((a,(2e+1)a),(0,0)) &= a + \min\{|(2e+1)a|,\, q-|(2e+1)a|\} \\ &= a + \min\{|(2e+1)a|,\, 2e^2+2e+1-|(2e+1)a|\}\end{aligned}$$

Como $1 \leq a \leq e$, temos $(2e+1)a \leq (2e+1)e = 2e^2+e < q$ e assim $|(2e+1)a| = (2e+1)a$. Logo:

$$\begin{aligned}d_L((a,(2e+1)a),(0,0)) &= a + \min\{(2e+1)a,\, 2e^2+2e+1-2ea-a\} \\ &= \min\{(2e+1)a+a,\, 2e^2+2e+1-2ea-a+a\} \\ &= \min\{(2e+2)a,\, 2e^2+2e+1-2ea\} \\ &= \min\{(2e+2)a,\, 2e(e+1-a)+1\} \\ &\geq 2e+1.\end{aligned}$$

2. Se $|a|_L = q-a$, então:

$$d_L((a,(2e+1)a),(0,0)) = q-a+\min\{|(2e+1)a|,\, q-|(2e+1)a|\}$$

Se $e=1$, então $q=5$ e assim

$$d_L((a,3a),(0,0)) = 5-a+\min\{3a,\, 5-3a\},$$

com $a=3$ ou $a=4$, pois $0<a\leq 4$ e por hipótese, $5-a<a$. Daí, temos:

$$\begin{aligned}d_L((3,9),(0,0)) &= d_L((3,4),(0,0)) \\ &= 5-3+\min\{9,\, 5-9\} \\ &= 2+\min\{4,\, 1\} \\ &= 2+1=3=2e+1,\end{aligned}$$

e

$$\begin{aligned} d_L((4,12),(0,0)) &= d_L((4,2),(0,0)) \\ &= 5-4+\min\{12,\, 5-12\} \\ &= 1+\min\{2,\, 3\} \\ &= 1+2=3=2e+1. \end{aligned}$$

Portanto, se $e=1$, $d_L((a,(2e+1)a),(0,0))=2e+1$, para qualquer a.

Agora, seja $e>1$. Se $1\leq q-a\leq e-1$, então $q-e+1\leq a\leq q-1$. Desta maneira, $|(2e+1)(q-e+1)|\leq|(2e+1)a|\leq|(2e+1)(q-1)|$, em $\mathbb{Z}_q$. Daí, como $q=2e^2+2e+1$, temos:

$$\begin{aligned} (2e+1)(1-e) &= 2e+1-2e^2-e \\ &= -2e^2+e+1 \\ &= 2e+1+e+1 \\ &= 3e+2 \end{aligned}$$

e

$$(2e+1)(-1)=2e^2.$$

Portanto, em $\mathbb{Z}_q$, $(2e+1)(q-e+1)=3e+2$ e $(2e+1)(q-1)=2e^2$, e assim, temos:

$$3e+2\leq|(2e+1)a|\leq 2e^2. \tag{3.2}$$

Da primeira desigualdade em (3.2), segue imediatamente que

$$|(2e+1)a|\geq 2e+1$$

e, por outro lado, se multiplicarmos por (-1) e somarmos q em todas as parcelas da desigualdade, temos:

$$q-2e^2\leq q-|(2e+1)a|\leq q-(3e+2)$$

donde

$$q-|(2e+1)a|\geq q-2e^2=2e+1,$$

isto é,

$$d_L((a,(2e+1)a),(0,0)) = q - a + \min\{|(2e+1)a|,\, q - |(2e+1)a|\} \geq 2e+1.$$

Por fim, se $q - a = e$, temos:

$$\begin{aligned}
|(2e+1)a| &= |(2e+1)(q-e)| \\
&= |(2e+1)(2e^2+2e+1-e)| \\
&= |(2e+1)(2e^2+e+1)| \\
&= |4e^3+4e^2+3e+1| \\
&= |(2e^2+2e+1)2e+e+1| \\
&= |e+1| = e+1,
\end{aligned}$$

e portanto,

$$\begin{aligned}
d_L((a,(2e+1)a),(0,0)) &= q - a + \min\{|(2e+1)a|,\, q - |(2e+1)a|\} \\
&= e + \min\{e+1,\, 2e^2+2e+1-(e+1)\} \\
&= e + \min\{e+1,\, 2e^2+e\} \\
&= e+e+1 = 2e+1.
\end{aligned}$$

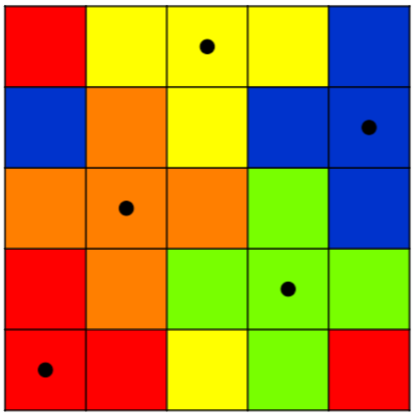
Logo, em todos os casos, segue que $d_L((a,(2e+1)a),(0,0)) \geq 2e+1$, como queríamos mostrar.

Note que não é necessário considerar separadamente o caso em que a segunda componente é $\leq e$, pois a palavra $(a,(2e+1)a)$ pode ser reescrita tomando $a = -(2e+1)b$, daí

$$\begin{aligned}
(a,(2e+1)a) &= (-(2e+1)b, -(2e+1)^2 b) \\
&= (-(2e+1)b, -(4e^2+4e+1)b) \\
&= (-(2e+1)b, -(2(2e^2+2e+1)-1)b) \\
&= (-(2e+1)b, b).
\end{aligned}$$

Desta maneira, $\omega((-(2e+1)b,b)) = \omega((b,(2e+1)b))$ e retornamos ao caso em que a primeira componente é $\leq e$, o qual já mostramos. □

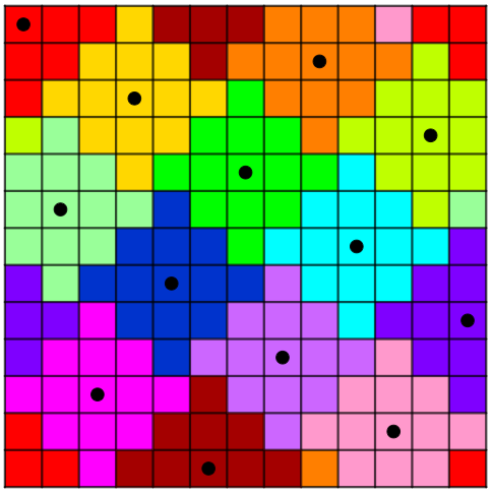
Figura 24 – Ladrilhamento de $\mathbb{Z}_5^2$
por pentominós.



Fonte: Elaborada pelo autor (2023).

Se $e = 1$, o empacotamento perfeito do 5^2-toro com 5 X-pentominós está na Figura 24. Veja que os centros estão nas mesmas posições que as da Figura 18. Se $e = 2$, o empacotamento perfeito do 13^2-toro com 13 triskaidekominós está na Figura 25.

Figura 25 – Ladrilhamento de $\mathbb{Z}_{13}^2$
por triskaidekominós.



Fonte: Elaborada pelo autor (2023).

Teorema 3.3.3. *Sejam um natural $n \geq 2$ e $q = 2n + 1$. Existe um código perfeito na métrica de Lee, 1-corretor de erros e com palavras de comprimento n sobre um alfabeto com q letras.*

Demonstração. Seja A o conjunto de todos os pontos $a = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}_q^n$ que satisfazem a congruência:

$$\sum_{i=1}^{n} i a_i \equiv 0 \pmod{2n+1}. \tag{3.3}$$

Para cada $a \in A$, consideremos $qL_{n,1}(a)$. Para uma escolha arbitrária de $a_2, a_3, \ldots, a_n$, suponhamos que

$$\sum_{i=2}^{n} i a_i \equiv r \pmod{2n+1}. \tag{3.4}$$

Como $\mathbb{Z}_q$ é q-periódico, existe $a_1 \in \mathbb{Z}_q$ tal que $a_1 + r \equiv 0 \pmod{2n+1}$. Portanto, existem q^{n-1} soluções para a equação (3.3) pois para cada r, como em (3.4), deve existir um único valor entre 0 e $2n$ que satisfaça a equação. Note que cada ponto de $\mathbb{Z}_q^n$ dista 1 de algum ponto em A.

Agora, seja $b = (b_1, b_2, \ldots, b_n) \in \mathbb{Z}_q^n$. Temos:

$$\sum_{i=1}^{n} i b_i \equiv k \pmod{2n+1}, \tag{3.5}$$

onde $0 \leq k \leq 2n$. Temos as seguintes possibilidades:

1. Se $k = 0$, então $b \in A$.

2. Se $1 \leq k \leq n$, consideremos o ponto $b' \in \mathbb{Z}_q^n$, trocando a k-ésima coordenada de b por $b_k - 1$, de modo que b' seja um elemento de A.
   De fato,

$$\sum_{\substack{i=1 \\ i \neq k}}^{n} i b_i + k(b_k - 1) \equiv \sum_{i=1}^{n} i b_i - k \equiv 0 \pmod{2n+1},$$

   e assim, $d_L(b, b') = 1$.

3. Se $n+1 \leq k \leq 2n$, consideremos um ponto $b'' \in \mathbb{Z}_q^n$, trocando a $2n+1-k$-ésima coordenada de b por $b_{2n+1-k}+1$. Da mesma forma,

$$\begin{aligned}\sum_{\substack{i=1 \\ i \neq 2n+1-k}}^{n} ib_i + (2n+1-k)(b_{2n+1-k}+1) &\equiv \sum_{i=1}^{n} ib_i + 2n + 1 - k \\ &\equiv \sum_{i=1}^{n} ib_i - k \\ &\equiv 0 \pmod{2n+1},\end{aligned}$$

de modo que $d_L(b, b'') = 1$ e portanto, b'' é um elemento de A.

Desta maneira, todos os pontos de $\mathbb{Z}_q^n$ distam no máximo 1 de algum ponto de A, isto é, as bolas de Lee $qL_{n,1}(a)$, $a \in A$, possuem $2n+1$ elementos. Portanto, a união das bolas em torno dos pontos de A compreendem

$$q^{n-1} + q^{n-1} \cdot 2n = q^{n-1}(2n+1) = q^n$$

pontos, se as bolas forem todas disjuntas entre si.

Entretanto, como cada ponto de $\mathbb{Z}_q^n$ está a uma distância 1 de um, e somente um, ponto de A, as bolas devem necessariamente ser disjuntas e cobrir todo o espaço. Logo, as bolas $qL_{n,1}(a)$, com $a \in A$, ladrilham o espaço $\mathbb{Z}_q^n$ e portanto, o código é perfeito. □

Os Teoremas 3.3.1, 3.3.2 e 3.3.3 fornecem empacotamentos ótimos do espaço $\mathbb{Z}_q^n$ por bolas na métrica de Lee para os seguintes parâmetros:

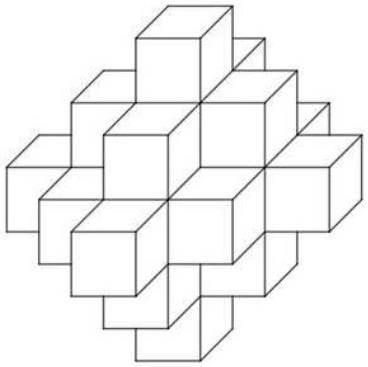
- $n = 1$, $e > 0$ e $q = 2e + 1$;
- $n = 2$, $e > 0$ e $q = e^2 + (e+1)^2$, e;
- $n \in \mathbb{N}$, $e = 1$ e $q = 2n + 1$.

Portanto, vimos que é possível em alguns casos, para alfabetos grandes, construir bolas que sejam bem sucedidas em cobrir seus espaços. Inclusive, no caso em que q é um alfabeto pequeno (especificamente, um fator de $2n+1$ contendo todos os fatores primos distintos de $2n+1$) às vezes pode ser possível como ilustrado para $n = 4$ e $q = 3$ em [7].

Entretanto, nem todas as bolas $L_{n,e}$ são capazes de ladrilhar o espaço n-dimensional. O primeiro contra-exemplo é o seguinte:

Teorema 3.3.4. *Sejam $n = 3$, $e = 2$ e $q \geq 2e + 1$. Não existe $LP(3, 2)$-código sobre alfabetos grandes.*

Figura 26 – Bola de Lee $L_{3,2}$ composta por 25 cubos unitários.



Fonte: Elaborada pelo autor (2023).

Demonstração. Suponhamos que $\mathbb{R}^3$ possa ser ladrilhado e seja

$$\mathcal{L} = \{L_i := L_{3,2}(a_i, b_i, c_i)\,;\, i = 0, 1, 2, \dots\}$$

um ladrilhamento por bolas de Lee de dimensão 3, raio 2 e centro em $(a_i, b_i, c_i) \in \mathbb{R}^3$. Podemos supor, sem perda de generalidade, que $L_0 \in \mathcal{L}$, onde $(a_0, b_0, c_0) = (0, 0, 0)$. Agora, seja $L_1 \in \mathcal{L}$ a bola contendo a palavra $(2, 1, 0)$. Então,

$$d_l((a_1, b_1, c_1), (2, 1, 0)) = |a_1 - 2| + |b_1 - 1| + |c_1 - 0| \leq 2.$$

Note que como $d_l((2, 1, 0), (0, 0, 0)) = |2| + |1| > 2$, segue que $L_1 \neq L_0$. Como $\mathcal{L}$ é um ladrilhamento, as bolas L_0 e L_1 são disjuntas, e assim

$$d_l((a_1, b_1, c_1), (0, 0, 0)) = |a_1 - 0| + |b_1 - 0| + |c_1 - 0| \geq 5 = 2 \cdot 2 + 1.$$

Porém, temos:

$$\begin{aligned}|a_1| + |b_1| + |c_1| &= |a_1 - 2 + 2| + |b_1 - 1 + 1| + |c_1| \\ &\leq |a_1 - 2| + 2 + |b_1 - 1| + 1 + |c_1| \\ &= |a_1 - 2| + |b_1 - 1| + |c_1| + 3 \\ &\leq 2 + 3 = 5,\end{aligned}$$

onde vale a igualdade se, e somente se, $a_1 - 2 \geq 0$ e $b_1 - 1 \geq 0$. Então, temos que $a_1 \geq 2$, $b_1 \geq 1$ e $a_1 + b_1 + |c_1| = 5$.

Suponhamos que $a_1 \geq 3$. Desta maneira, temos

$$|a_1 - 3| + |b_1| + |c_1| = a_1 - 3 + b_1 + |c_1| = 5 - 3 = 2,$$

e portanto, $(3, 0, 0) \in L_1$.

Agora, afirmamos que a palavra $(2, -1, 0)$ está fora de L_0 e L_1. De fato,

$$d_l((2, -1, 0), (0, 0, 0) = |2 - 0| + | - 1 - 0| + |0 - 0| = 2 + 1 + 0 = 3$$

e

$$\begin{aligned}d_l((2, -1, 0), (a_1, b_1, c_1)) &= |a_1 - 2| + |b_1 - (-1)| + |c_1 - 0| \\ &= |a_1 - 2| + |b_1 + 1| + |c_1| \\ &= a_1 - 2 + b_1 + 1 + |c_1| \\ &= a_1 + b_1 + |c_1| - 1 = 5 - 1 = 4.\end{aligned}$$

Portanto, $(2, -1, 0)$ pertence a uma terceira bola, digamos $L_2 \in \mathcal{L}$. Para esta nova bola temos:

$$d_l((a_2, b_2, c_2), (0, 0, 0)) = |a_2 - 0| + |b_2 - 0| + |c_2 - 0| \geq 5 = 2 \cdot 2 + 1,$$

e

$$d_l((a_2, b_2, c_2), (2, -1, 0)) = |a_2 - 2| + |b_2 + 1| + |c_2 - 0| \leq 2.$$

Utilizando um argumento análogo ao anterior, podemos mostrar que $a_2 \geq 2$ e $a_2 + b_2 + |c_2| = 5$.

Suponhamos que $a_2 \geq 3$. Desta maneira, temos

$$d_l((3,0,0),(a_2,b_2,c_2)) = |a_2-3|+|b_2-0|+|c_2-0| = a_2-3+b_2+|c_2| = 5-3 = 2,$$

e portanto, $(3,0,0) \in L_2$.

Entretanto, como $\mathcal{L}$ é um ladrilhamento e $L_1, L_2 \in \mathcal{L}$ então $a_1 = 2$ ou $a_2 = 2$, estritamente, pois L_1 e L_2 são disjuntas. Como $\mathbb{R}^3$ é simétrico, suponhamos, sem perda de generalidade, que $a_1 = 2$ e $c_1 \geq 0$. De fato, se $a_2 = 2$, basta aplicarmos a simetria $f(a,b,c) = (b,a,c)$ e, se $c < 0$, aplicamos $f(a,b,c) = (a,b,-c)$. Temos então, 3 casos a considerar:

1. $(a_1, b_1, c_1) = (2,3,0)$;

   Sejam L_0 e $L_1 = L_{3,2}(2,3,0)$ elementos do ladrilhamento $\mathcal{L}$.
   Note que o ponto $(1,1,1)$ não está em L_0 ou L_1, pois

   $$d_l((0,0,0),(1,1,1)) = |1-0|+|1-0|+|1-0| = 1+1+1 = 3$$

   e

   $$d_l((2,3,0),(1,1,1)) = |2-1|+|3-1|+|0-1| = 1+2+1 = 4.$$

   Portanto, para algum ponto $(a_3,b_3,c_3) \in \mathbb{R}^3$, existe $L_3 \in \mathcal{L}$ tal que $(1,1,1) \in L_3$. Então, temos:

   $$\begin{aligned} d_l((0,0,0),(a_3,b_3,c_3)) &= |a_3-0|+|b_3-0|+|c_3-0| \geq 5; \\ d_l((2,3,0),(a_3,b_3,c_3)) &= |a_3-2|+|b_3-3|+|c_3-0| \geq 5; \\ d_l((a_3,b_3,c_3),(1,1,1)) &= |a_3-1|+|b_3-1|+|c_3-1| \leq 2. \end{aligned}$$

   Note que

   $$\begin{aligned} 5 \leq |a_3|+|b_3|+|c_3| &= |a_3-1+1|+|b_3-1+1|+|c_3-1+1| \\ &\leq |a_3-1|+1+|b_3-1|+1+|c_3-1|+1 \\ &= |a_3-1|+|b_3-1|+|c_3-1|+3 \\ &\leq 2+3 = 5. \end{aligned}$$

   Daí, segue que $a_3 \geq 1$, $b_3 \geq 1$, $c_3 \geq 0$ e $a_3+b_3+c_3 = 5$.

Vamos mostrar que $|a_3 - 2| + |b_3 - 3| + |c_3| > 5$. Suponhamos que

$$|a_3 - 2| + |b_3 - 3| + |c_3| = 5\,.$$

Como $a_3 + b_3 + c_3 = 5$, temos:

$$\begin{aligned} |a_3 - 2| + |b_3 - 3| + |c_3| &= a_3 + b_3 + c_3 \\ &= a_3 - 2 + 2 + b_3 - 3 + 3 + c_3 \\ &= (a_3 - 2) + (b_3 - 3) + c_3 + 5. \end{aligned}$$

Como $c_3 \geq 0$, $|c_3| = c_3$ e, portanto $|a_3 - 2| + |b_3 - 3| = (a_3 - 2) + (b_3 - 3) + 5$. Fazendo $x = a_3 - 2$ e $y = b_3 - 3$, temos:

$$|x| + |y| = x + y + 5,$$

que não possui solução para $x, y \in \mathbb{Z}$. Portanto, $|a_3 - 2| + |b_3 - 3| + |c_3| > 5$. Desta maneira, $|a_3 - 2| > a_3$ apenas quando $a_3 \leq 2$ e, um raciocínio análogo nos diz que $b_3 \leq 3$.

O caso em que $a_3 = 2$ e $b_3 = 3$, implica em $c_3 = 0$, e assim, $(a_3, b_3, c_3) = (a_1, b_1, c_1)$, o que é uma contradição pois $(1, 1, 1) \in L_3$ e $(1, 1, 1) \notin L_1$.

Note que mesmo quando estritamente $a_3 = 2$ ou $b_3 = 3$, a inequação

$$|a_3 - 2| + |b_3 - 3| + |c_3| > 5$$

não é satisfeita. De fato, se $a_3 = 2$ e $b_3 < 3$, como $b_3 \geq 1$, segue que $b_3 = 1$ ou $b_3 = 2$. Substituindo, temos

$$5 < |2 - 2| + |1 - 3| + |2| = 4$$

e

$$5 < |2 - 2| + |2 - 3| + |1| = 2.$$

Da mesma maneira, se $a_3 < 2$ e $b_3 = 3$, como $a_3 \geq 1$, segue que $a_3 = 1$. Substituindo, temos

$$5 < |1 - 2| + |3 - 3| + |1| = 2.$$

Portanto, $a_3 \leq 1$ e $b_3 \leq 2$.

Por fim, temos duas possibilidades: $(a_3, b_3, c_3) = (1, 1, 3)$ ou $(a_3, b_3, c_3) = (1, 2, 2)$. Porém, se $(a_3, b_3, c_3) = (1, 2, 2)$, temos

$$d_l((1, 2, 2), (2, 3, 0)) = |1 - 2| + |2 - 3| + |2 - 0| = 4,$$

que é uma contradição, pois, por hipótese, $(2, 3, 0)$ é o centro da bola L_1 e assim qualquer de seus pontos devem estar a uma distância pelo menos igual a 5 de algum ponto de L_3. Logo, $(a_3, b_3, c_3) = (1, 1, 3)$.

Agora, seja $\varphi : E^3 \to E^3$ dada por $\varphi(x, y, z) = (2 - x, 3 - y, z)$, uma isometria. Seja dado o ponto $(1, 2, 1)$. Note que $(1, 2, 1) \notin L_0 \cup L_1 \cup L_3$, $\varphi(1, 2, 1) = (1, 1, 1)$ e além disso, φ permuta L_0 e L_1. De fato, se $(a, b, c) \in L_0$ temos

$$d_l(\varphi(a, b, c), (2, 3, 0)) = d_l(\varphi(a, b, c), \varphi(0, 0, 0)) = d_l((a, b, c), (0, 0, 0)) \leq 2,$$

portanto, $\varphi(L_0) \subset L_1$.

Agora, dado $(a', b', c') \in L_1$ temos

$$d_l((a', b', c'), \varphi(0, 0, 0)) = d_l((a', b', c'), (2, 3, 0)) \leq 2,$$

portanto, $L_1 \subset \varphi(L_0)$, donde segue que $\varphi(L_0) = L_1$.
De forma análoga, mostramos que $\varphi(L_1) = L_0$.

Por fim, seja dada a bola $L_4 \in \mathcal{L}$ tal que φ permute L_3 e L_4. Note que o centro da bola L_4 é o ponto $(1, 2, 3) = \varphi^{-1}(1, 1, 3)$ e $(1, 2, 1) \in L_4$ pois

$$d_l((1, 2, 3), (1, 2, 1)) = |1 - 1| + |2 - 2| + |3 - 1| = 2.$$

Logo, como $(1, 2, 1) \notin L_3$ e

$$0 < d_l((1, 2, 3), (1, 1, 3)) = |1 - 1| + |2 - 1| + |3 - 3| = 1 \leq 2$$

as bolas L_3 e L_4 não coincidem e não são disjuntas, o que contradiz a hipótese de que $\mathcal{L}$ é um ladrilhamento.

2. $(a_1, b_1, c_1) = (2, 2, 1)$;

Sejam L_0 e $L_1 = L_{3,2}(2,2,1)$ elementos do ladrilhamento $\mathcal{L}$.
Note que o ponto $(1,1,-1)$ não está em L_0 ou L_1, pois

$$d_l((0,0,0),(1,1,-1)) = |0-1| + |0-1| + |0-(-1)| = 1+1+1 = 3$$

e

$$d_l((2,2,1),(1,1,-1)) = |2-1| + |2-1| + |1-(-1)| = 1+1+2 = 4.$$

Portanto, para algum ponto $(a_3,b_3,c_3) \in \mathbb{R}^3$, existe $L_3 \in \mathcal{L}$ tal que $(1,1,-1) \in L_3$. Então, temos:

$$\begin{aligned} d_l((0,0,0),(a_3,b_3,c_3)) &= |a_3-0| + |b_3-0| + |c_3-0| \geq 5; \\ d_l((2,2,1),(a_3,b_3,c_3)) &= |a_3-2| + |b_3-2| + |c_3-1| \geq 5; \\ d_l((a_3,b_3,c_3),(1,1,-1)) &= |a_3-1| + |b_3-1| + |c_3+1| \leq 2. \end{aligned}$$

Como no caso (1), note que

$$\begin{aligned} 5 \leq |a_3| + |b_3| + |c_3| &= |a_3-1+1| + |b_3-1+1| + |c_3+1-1| \\ &\leq |a_3-1| + 1 + |b_3-1| + 1 + |c_3+1| + 1 \\ &= |a_3-1| + |b_3-1| + |c_3+1| + 3 \\ &\leq 2+3 = 5. \end{aligned}$$

Daí, segue que $a_3 \geq 1$, $b_3 \geq 1$, $c_3 \leq 1$ e $a_3 + b_3 + |c_3| = 5$.

Agora, temos $|a_3-2| + |b_3-2| + |c_3-1| > 5$. Desta maneira, $a_3 \leq 2$ e $b_3 \leq 2$. Afirmamos que $a_3 = 1$ e $b_3 = 1$. Com efeito, suponhamos que $a_3 = 2$, e neste caso, como $1 \leq b_3 \leq 2$, temos:

Se $b_3 = 1$, então $c_3 = -2$, e assim

$$d_l((2,1,-2),(2,2,1)) = |2-2| + |1-2| + |-2-1| = 0+1+3 = 4 < 5.$$

Se $b_3 = 2$, então $c_3 = 1$ ou $c_3 = -1$. Em ambos os casos temos

$$d_l((2,2,c_3),(2,2,1)) = |2-2| + |2-2| + |c_3-1| = |c_3-1| < 5.$$

Portanto, $a_3 = 1$. Daí, se $b_3 = 2$, então $c_3 = -2$, e assim

$$d_l((1,2,-2),(2,2,1)) = |1-2| + |2-2| + |-2-1| = 1+0+3 = 4 < 5.$$

Logo, $a_3 = 1$ e $b_3 = 1$, o que implica que o ponto $(a_3, b_3, c_3) = (1, 1, -3)$ é a única solução das desigualdades.

Agora, seja dado o ponto $(1, 2, -1)$. Note que $(1, 2, -1) \notin L_0 \cup L_1 \cup L_3$ e assim, para algum ponto $(a_4, b_4, c_4) \in \mathbb{R}^3$, existe $L_4 \in \mathcal{L}$ tal que $(1, 2, -1) \in L_4$. Portanto, temos

$$\begin{aligned} d_l((a_4, b_4, c_4), (0, 0, 0)) &= |a_4 - 0| + |b_4 - 0| + |c_4 - 0| \geq 5 \\ d_l((a_4, b_4, c_4), (2, 2, 1)) &= |a_4 - 2| + |b_4 - 2| + |c_4 - 1| \geq 5 \\ d_l((a_4, b_4, c_4), (1, 1, -3)) &= |a_4 - 1| + |b_4 - 1| + |c_4 + 3| \geq 5 \\ d_l((a_4, b_4, c_4), (1, 2, -1)) &= |a_4 - 1| + |b_4 - 2| + |c_4 + 1| \leq 2 \end{aligned}$$

A segunda e a quarta inequações implicam em $a_4 \leq 3$, $c_4 \leq -1$, enquanto a terceira e a quarta implicam em $a_4 \geq 1$, $b_4 \geq 2$, $c_4 \geq -1$ e

$$a_4 + b_4 - 2 + |c_4 + 3| = 5\,.$$

Desta forma, $c_4 = -1$ e $a_4 + b_4 = 5$. Como $1 \leq a_4 \leq 3$, segue que:

$$(a_4, b_4, c_4) \in \{(1, 4, -1),\ (2, 3, -1),\ (3, 2, -1)\}.$$

Afirmamos que $(1, 4, -1)$ é a única solução das desigualdades. De fato, se $a_4 = 2$, segue que $(a_4, b_4, c_4) = (2, 3, -1)$ e temos

$$d_l((2, 3, -1), (2, 2, 1)) = |2 - 2| + |3 - 2| + |-1 - 1| = 0 + 1 + 2 = 3 < 5.$$

Da mesma forma, se $a_4 = 3$, $(a_4, b_4, c_4) = (3, 2, -1)$ e

$$d_l((3, 2, -1), (2, 2, 1)) = |3 - 2| + |2 - 2| + |-1 - 1| = 1 + 0 + 2 = 3 < 5.$$

Logo, $a_4 = 1$ e $(a_4, b_4, c_4) = (1, 4, -1)$ é a única solução das desigualdades. Por fim, seja $\varphi : E^3 \to E^3$ dada por $\varphi(x, y, z) = (z + 3,\ y - 1,\ x - 1)$, uma isometria. Desta maneira, temos

$$\begin{aligned} \varphi(L_3) &= \varphi(L_{3,2}(1, 1, -3)) \\ &= L_{3,2}(\varphi(1, 1, -3)) \\ &= L_{3,2}(-3 + 3, 1 - 1, 1 - 1) \\ &= L_{3,2}(0, 0, 0) \\ &= L_0 \end{aligned}$$

e

$$\begin{aligned}\varphi(L_4) &= \varphi(L_{3,2}(1,4,-1)) \\ &= L_{3,2}(\varphi(1,4,-1)) \\ &= L_{3,2}(-1+3, 4-1, 1-1) \\ &= L_{3,2}(2,3,0) \\ &= L_1,\end{aligned}$$

e portanto, voltamos ao caso (1).

3. $(a_1, b_1, c_1) = (2, 1, 2)$.

   O caso (3) pode ser reduzido ao caso (2), se considerarmos a simetria $f(a, b, c) = (a, c, b)$.

Logo, não é possível cobrir o espaço tridimensional com bolas de Lee de raio 2. □

Além de apresentarem um exemplo de que não é possível cobrir o espaço $\mathbb{Z}^3$ com bolas $L_{3,2}$, Golomb e Welch, acreditavam que uma prova geral da incapacidade de $L_{n,e}$ em ladrilhar o espaço n-dimensional, para n e e grandes, residia no estudo da aproximação das bolas $L_{n,e}$ pelos polítopos cruzados n-dimensionais $P_{n,e}$ associados. Mostraremos a seguir seus avanços neste sentido. A demonstração da Proposição 3.3.5 pode ser encontrada em [5].

Proposição 3.3.5. *Sejam $n \in \mathbb{N}$ e $e > 0$. O polítopo cruzado regular n-dimensional $P_{n,e}$ possui volume dado por*

$$\mathrm{vol}(P_{n,e}) = \frac{D^n}{n!} = \frac{(2e+1)^n}{n!},$$

onde $D = \mathrm{diam}(L_{n,e})$ é o diâmetro Euclidiano da bola $L_{n,e}$.

Exemplo 3.3.6. Para um X-pentominó, $L_{2,1}$, podemos calcular a porção da bola de Lee que é coberta pelo polítopo cruzado inscrito, $P_{2,1}$ (Figura 27).

O volume do X-pentominó é exatamente a quantidade de quadrados unitários que compõe a bola, isto é, $\#L_{2,1} = 5$, enquanto o volume do polítopo, como na definição (Proposição 3.3.5) é igual a

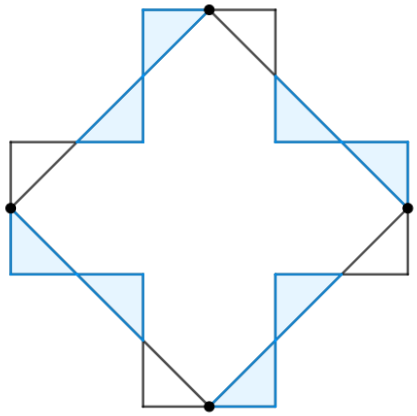
$$\mathrm{vol}(P_{2,1}) = \frac{(2 \cdot 1 + 1)^2}{2!} = \frac{3^2}{2} = \frac{9}{2}.$$

Logo, o polítopo cobre

$$\frac{\text{vol}(P_{2,1})}{\#L_{2,1}} = \frac{\frac{9}{2}}{5} = \frac{9}{10}$$

da bola de Lee de dimensão 2 e raio 1, isto é, o *mosaico* de quadrados inscritos induzido no empacotamento por X-pentominós, recobre apenas 90% da área total.

Figura 27 – Porção da bola $L_{2,1}$ coberta pelo polítopo $P_{2,1}$.



Fonte: Elaborada pelo autor (2023).

Qualquer empacotamento de um espaço n-dimensional com bolas $L_{n,e}$ induz um empacotamento com o polítopos cruzados. Em geral, o fator de eficiência relativa é:

Definição 3.3.7. Seja $n \in \mathbb{N}$ e $e > 0$. Dado um empacotamento de um conjunto n-dimensional por bolas de Lee, $L_{n,e}$, definimos a *eficiência* de um empacotamento por polítopos cruzados $P_{n,e}$, como sendo $0 < E_n(e) \leq 1$ dada por

$$E_n(e) = \frac{\text{vol}(P_{n,e})}{\#L_{n,e}}.$$

Em [7], Golomb e Welch utilizaram o mesmo tipo de argumento do Exemplo 3.3.6 para provar os dois teoremas a seguir. Apresentaremos a ideia da prova proposta por eles, sem discorrer muito em detalhes.

Teorema 3.3.8. *As bolas $L_{3,e}$ não ladrilham $\mathbb{R}^3$, para qualquer $e > e_0$.*

Demonstração. Se $L_{3,e}$ fosse capaz de ladrilhar o espaço tridimensional, isto induziria um empacotamento do espaço por octaedros regulares inscritos, com uma eficiência de empacotamento de

$$\begin{aligned} E_3(e) &= \frac{\mathrm{vol}(P_{n,e})}{\#L_{n,e}} \\ &= \frac{(2e+1)^3/6}{(8e^3+12e^2+16e+6)/6} \\ &= \frac{(2e+1)^3}{(2e+1)^3+5(2e+1)} \\ &= \frac{1}{1+5/(2e+1)^2}. \end{aligned}$$

É provado em [5] que octaedros regulares não são capazes de preencher completamente o espaço tridimensional.

Ainda, é possível mostrar que, se uma figura não cobre o espaço com uma eficiência de empacotamento igual a 1, então existe um limite superior $\alpha > 0$ para a densidade de empacotamento com $\alpha < 1$.

Assim que $E_3(e)$ excede α, o empacotamento por bolas de Lee induz um empacotamento octaédrico que excede o limite na densidade do empacotamento octaédrico.

Como $E_3(e) \longrightarrow 1$ quando $e \longrightarrow +\infty$, $E_3(e) > \alpha$ para $e > e_0$, e_0 dado. □

Teorema 3.3.9. *Para $n > 4$ e $e > e_n$, as bolas $L_{n,e}$ não conseguem ladrilhar o espaço Euclidiano n-dimensional $\mathbb{Z}^n$.*

Demonstração. Em um espaço Euclidiano n-dimensional, para $n > 4$, é sabido que polítopos cruzados regulares não cobrem o espaço (veja [5]).

Novamente, existe uma densidade de empacotamento máxima α_n, que deveria ser excedida pelas esferas inscritas, para $e > e_n$, se o empacotamento por bolas de Lee existisse.

Isto depende apenas do fato que

$$E_3(e) = \frac{\mathrm{vol}(P_{n,e})}{\#L_{n,e}} \longrightarrow 1,$$

quando $e \longrightarrow +\infty$. □

De fato, se o raio for suficientemente grande, os poliominós associados às bolas de Lee discretas em $\mathbb{Z}^n$ passam a se comportar como bolas de Manhattan em $\mathbb{R}^n$, isto é, polítopos cruzados os quais são conhecidos por não ladrilhar o espaço para $n > 4$.

Observação 3.3.10. Para $n = 3$, Minkowski em [21] considerou o reticulado $\Lambda \subseteq \mathbb{R}^3$ com base $\{(1, -2, 3), (-2, 3, 1), (3, 1, -2)\}$ e provou que sua densidade de empacotamento na métrica de Manhattan é igual a $\alpha = \frac{18}{19}$. Essa é a densidade máxima na métrica de Manhattan em $\mathbb{R}^3$. Para $n > 3$, apenas alguns limitantes inferiores são conhecidos da densidade de empacotamento do polítopo cruzado n-dimensional (veja [6]).

O Teorema 3.3.9 não é explícito nem eficaz em termos de mostrar apenas a existência de uma constante $e_n > 0$. No entanto, Post [23] forneceu um primeiro limite explícito para e_n no caso de códigos periódicos. Esse resultado foi posteriormente melhorado de forma assintótica por Astola [2], e por Lepistö [20].

Desta maneira, os teoremas anteriores nos afirmam que não existem ladrilhamentos do espaço $\mathbb{Z}^n$ por bolas na métrica de Lee para os seguintes parâmetros:

- $n = 3$, $e = 2$, e;
- $n \geq 5$, $e > e_n$, onde e_n depende do limite de eficiência de empacotamento, α, do polítopo cruzado no espaço $\mathbb{Z}^n$.

Os resultados alcançados por Golomb e Welch foram fundamentais para o desenvolvimento da teoria dos códigos corretores de erros, destacando-se pelo rigor matemático e pela elegância das construções apresentadas. Esses casos específicos abrem caminho para a formulação da conjectura geral, que será postulada a seguir:

Conjectura 3.3.11. ***(Golomb-Welch, Versão Fraca)*** *Sejam $n \in \mathbb{N}$, $e > 0$ e $q \geq 2e + 1$. Não existem $LP(n, e, q)$-códigos sobre alfabetos grandes para $n \geq 3$ e $e \geq 2$.*

Na última seção de seu artigo [7], Golomb e Welch formulam sua Conjectura em termos de ladrilhamentos do espaço euclidiano n-dimensional $\mathbb{Z}^n$. Assim, em relação ao Teorema 2.2.7, a seguinte conjectura é natural:

Conjectura 3.3.12. ***(Golomb-Welch, Versão Forte)*** *Sejam $n \in \mathbb{N}$ e $e > 0$. Não existem $LP(n, e)$-códigos para $n \geq 3$ e $e \geq 2$.*

Embora a Conjectura ainda permaneça aberta em sua totalidade, pesquisadores têm se dedicado a investigar casos específicos que oferecem perspectivas promissoras. Neste sentido, destacamos os seguintes resultados:

Teorema 3.3.13. *[15] Não existe $LP(n, e)$-código para*

$$\begin{aligned}
3 \leq n \leq 74 \quad & e \quad \max\left\{\frac{\sqrt{2}}{2}n - \frac{3}{4}\sqrt{2} - \frac{1}{2},\, 2\right\} \leq e, \\
75 \leq n \leq 405 \quad & e \quad \max\left\{18,\, \sqrt{2n+40}\right\} \leq e \leq \frac{n-21}{3} \\
& \textit{ou} \quad \frac{\sqrt{2}}{2}n - \frac{3}{4}\sqrt{2} - \frac{1}{2} \leq e, \\
406 \leq n \leq 876 \quad & e \quad \sqrt{2n+40} \leq e \leq \frac{n-21}{3} \\
& \textit{ou} \quad e \geq 285, \\
n \geq 876 \quad & e \quad \sqrt{2n+40} \leq e.
\end{aligned}$$

O caso mais difícil da Conjectura de Golomb-Welch parece ser quando $e = 2$. Nos dedicaremos a ele, considerando infinitas dimensões $n \in \mathbb{N}$ sobre certas condições no próximo capítulo. Entretanto, algumas abordagens já foram feitas anteriormente.

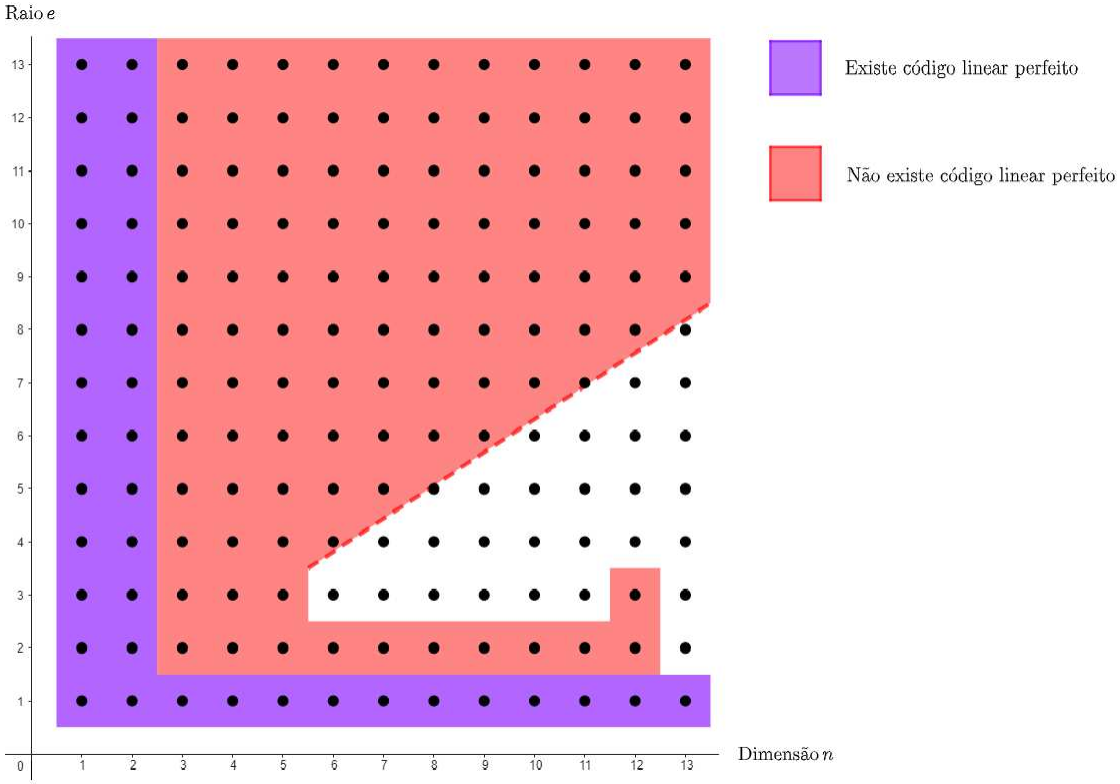
Em [18], o autor prova, utilizando uma técnica completamente nova, que se o volume da esfera $\#L_{n,2} = 2n^2 + 2n + 1$ é primo e uma certa condição é satisfeita, então os códigos $LP(n, 2)$ não existem. Mas, como apontado por Horak em [15], esta condição não é restritiva. Por exemplo, de 12706 números $n \leq 10^5$ com $p = 2n^2 + 2n + 1$ primo, apenas 4 números n não satisfazem a condição. Já a não-existência de um $LP(6, 2)$-código é mostrada em [12]. Mais geralmente, a não-existência de $LP(n, 2)$-códigos para $n \leq 2$ é provada em [14] usando um método computacional. A prova é baseada no fato de não existir um homomorfismo

$\phi : \mathbb{Z}^n \to G$, onde G é um grupo abeliano de ordem $|L(n,2)|$, cuja restrição de ϕ a $L(n,2)$ é uma bijeção em G. O método torna-se computacionalmente inviável, no entanto, à medida que n aumenta. Uma abordagem similar é usada em [29] para mostrar a não-existência de:

- $LP(n,3)$-códigos para alguns valores de $n \equiv 12,\ 21 \pmod{27}$, e;
- $LP(n,4)$-códigos para alguns valores de $n \equiv 3,\ 5,\ 21,\ 23 \pmod{27}$.

Uma representação gráfica do estado em que se encontra a Conjectura para dimensões n e raios e, ambos menores que 14, está na Figura 28.

Figura 28 – Estado da Conjectura de Golomb-Welch restrita a códigos lineares para $1 \leq n \leq 13$ e $1 \leq e \leq 13$.



Fonte: Elaborada pelo autor (2023).

4 O CASO DO RAIO 2 PARA INFINITAS DIMENSÕES

Neste capítulo, apresentaremos a abordagem da Conjectura de Golomb-Welch para raio $e = 2$ feita por Qureshi, Campello e Costa em [24]. A técnica se assemelha ao que foi proposto em [18], porém, em vez de impor a condição de que $2n^2 + 2n + 1$ seja um número primo, é exigido apenas que tal número seja divisível por um número primo do tipo *amigável*, que definiremos em breve.

No decorrer de todo o capítulo consideramos apenas códigos lineares em $\mathbb{Z}^n$ (ou seja, reticulados), que são subgrupos aditivos de $\mathbb{Z}^n$.

4.1 COBERTURAS HOMOGÊNEAS

Consideremos $L_{n,e}$ a bola em $\mathbb{Z}^n$ de raio $e > 0$, centrada em 0, em relação à métrica de Manhattan. O resultado a seguir, de Horak e AlBdaiwi [13], nos fornece um critério para determinar se $LP(n, e)$ é vazio ou não.

Teorema 4.1.1. *$LP(n, e) = \emptyset$ se, e somente se, existe um grupo abeliano G e um homomorfismo $\phi : \mathbb{Z}^n \to G$ tal que $\phi\Big|_{L_{n,e}} : L_{n,e} \to G$ é uma bijeção.*

Mais geralmente, podemos definir:

Definição 4.1.2. Dizemos que um reticulado $\mathcal{C} \subseteq \mathbb{Z}^n$ é uma *λ-cobertura homogênea* com raio $e > 1$ se, cada ponto $x \in \mathbb{Z}^n$ pertence a exatamente λ esferas de Lee de raio e e centro em alguma palavra do código. Isto é, existem $c_1, c_2, \ldots, c_\lambda \in \mathcal{C}$ tais que

$$x \in \bigcap_{1 \leq i \leq \lambda} L(n, e, c_i),$$

e

$$x \notin L(n, e, c)\, \forall c \in \mathcal{C} \setminus \{c_1, \ldots, c_\lambda\},$$

qualquer que seja $x \in \mathbb{Z}^n$. Denotamos por $Cov^\lambda(n, e)$ o conjunto de todas as λ-coberturas homogêneas $\mathcal{C} \subseteq \mathbb{Z}^n$ com raio e. Em particular, se $\lambda = 1$, então $Cov^1(n, e) = LP(n, e)$.

O teorema a seguir é uma reformulação do Teorema 4.1.1 em relação às λ-coberturas homogêneas.

Teorema 4.1.3. *O conjunto $Cov^{\lambda}(n,e)$ é não-vazio se, e somente se, existe um grupo abeliano G e um homomorfismo $\phi : \mathbb{Z}^n \to G$ tal que $\phi\Big|_{L_{n,e}} : L_{n,e} \to G$ é uma aplicação λ-para-1.*

Demonstração. Temos as seguintes equivalências:

i. $\mathcal{C} \in Cov^{\lambda}(n,e)$;

ii. Para cada $x \in \mathbb{Z}^n$ existem exatamente λ palavras do código, $c_1, c_2, \ldots, c_\lambda \in \mathcal{C}$, tais que $x \in c_i + L_{n,e}$, com $i = 1, 2, \ldots, \lambda$;

iii. Para cada $x \in \mathbb{Z}^n$ a equação $x = y + c$ possui exatamente λ soluções, com $y \in L_{n,e}$ e $c \in \mathcal{C}$;

iv. Para cada $x \in \mathbb{Z}^n$, existem exatamente λ valores de $y \in L_{n,e}$ tais que $y + \mathcal{C} = x + \mathcal{C}$;

v. A aplicação $\pi_{\mathcal{C}} : \mathbb{Z}^n \to \frac{\mathbb{Z}^n}{\mathcal{C}}$ dada por $\pi_{\mathcal{C}}(x) = x + \mathcal{C}$ é uma aplicação λ-para-1 quando restrita à esfera $L_{n,e}$.

($\Rightarrow$) Seja $\mathcal{C} \in Cov^{\lambda}(n,e)$. Basta tomarmos $G = \frac{\mathbb{Z}^n}{\mathcal{C}}$ e $\phi : \mathbb{Z}^n \to G$ dada por $\phi(x) = x + \mathcal{C}$ e o resultado segue pelas equivalências anteriores.

($\Leftarrow$) Seja $\phi :\ \mathbb{Z}^n \to G$ um homomorfismo tal que $\phi|_{L_{n,e}} : L_{n,e} \to G$ é uma aplicação λ-para-1. Definamos $\mathcal{C} = \ker(\phi)$. Então, pelo Primeiro Teorema do Isomorfismo de grupos, a aplicação $\psi : \frac{\mathbb{Z}^n}{\mathcal{C}} \to G$ dada por $\psi(x + \mathcal{C}) = \phi(x)$ é um isomorfismo. Logo, $\pi_{\mathcal{C}} = \psi \circ \phi : \mathbb{Z}^n \to \frac{\mathbb{Z}^n}{\mathcal{C}}$ dada por $\pi_{\mathcal{C}}(x) = x + \mathcal{C}$ é uma aplicação λ-para-1 quando restrita à esfera $L_{n,e}$. Portanto, pelas equivalências anteriores, segue que $Cov^{\lambda}(n,e)$ é não-vazio. □

4.2 CONJECTURA PARA PRIMOS AMIGÁVEIS

Em [24], os autores provam que a Conjectura de Golomb-Welch é verdadeira para raio 2 e dimensões $n \geq 3$ tais que o maior divisor primo de $2n^2 + 2n + 1$ seja amigável. Nesse sentido, nesta seção, vamos apresentar os primos amigáveis, que é um subconjunto infinito dos primos, fato que também vamos mostrar na seção seguinte.

Definição 4.2.1. Uma *raiz primitiva* r é um gerador do grupo $\mathbb{Z}_p^*$. E ainda, equivalentemente, a ordem multiplicativa de r módulo p é $\mathrm{ord}_p(r) = p-1$.

Pelo Pequeno Teorema de Fermat:

$$p \mid r^{p-1} - 1 = \left(r^{\frac{p-1}{2}} + 1\right)\left(r^{\frac{p-1}{2}} - 1\right).$$

Note que $r^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$, pois $p-1$ é o menor inteiro positivo tal que $r^p \equiv 1 \pmod{p}$. Desta forma, temos $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Portanto, quando $p \equiv 1 \pmod{4}$ o número $i = r^{\frac{p-1}{4}}$ é uma raiz de -1 módulo p, isto é, $i^2 \equiv -1 \pmod{p}$.

Agora, consideremos uma função

$$\eta : \{p \in \mathbb{N} \,:\, p \text{ é primo}\} \to \mathbb{Z}^+$$

que possui a propriedade como no Lema 4.2.2 a seguir:

Lema 4.2.2. *Seja p um número primo onde $p \equiv 1 \pmod{4}$. Existe um único inteiro $\eta(p) = \eta_p$ tal que $2\eta_p^2 + 2\eta_p + 1 \equiv 0 \pmod{p}$ e $0 < \eta_p \leq \frac{p-3}{2}$.*

Demonstração. Como $p \equiv 1 \pmod{4}$, pelo Pequeno Teorema de Fermat, -1 é um quadrado módulo p.

Note que o discriminante do polinômio $f(x) = 2x^2 + 2x + 1$,

$$\Delta = 2^2 - 4 \cdot 2 \cdot 1 = -4 = (2i)^2,$$

também é um quadrado módulo p.

Portanto, existem duas raízes diferentes módulo p.

Sejam η_0 e η_1 os únicos inteiros satisfazendo $0 \leq \eta_0 < \eta_1 \leq p-1$ tais que $f(\eta_0) \equiv f(\eta_1) \equiv 0 \pmod{p}$.

Pela relação entre raízes e coeficientes temos $\eta_0 + \eta_1 \equiv -1 \pmod{p}$.

Daí, segue que $\eta_0 + \eta_1 = p-1$, pois $0 \leq \eta_0 + \eta_1 < 2p-1$ e então

$$0 \leq \eta_0 \leq \frac{p-1}{2} \leq \eta_1.$$

Como $f(0) = 1$ e

$$\begin{aligned} f\left(\frac{p-1}{2}\right) &= 2\left(\frac{p-1}{2}\right)^2 + 2\left(\frac{p-1}{2}\right) + 1 \\ &= \frac{(p-1)^2}{2} + p - 1 + 1 \\ &= \frac{p^2 - 2p + 1}{2} + p \\ &= \frac{p^2 - 2p + 1 + 2p}{2} = \frac{p^2 + 1}{2} \end{aligned}$$

não são múltiplos de p, temos que $0 < \eta_0 \leq \dfrac{p-1}{2} - 1 = \dfrac{p-3}{2}$.

Por fim, definamos $\eta_p = \eta_0$ e, o resultado segue. □

Como sabemos, dado $n \in \mathbb{N}$, uma bola de Lee n-dimensional de raio $e = 2$, $L_{n,2}$, em torno de um ponto qualquer de $\mathbb{Z}^n$, possui

$$\begin{aligned} \#L_{n,2} &= \sum_{k=0}^{2} 2^k \binom{n}{k}\binom{2}{k} \\ &= 2^0\binom{n}{0}\binom{2}{0} + 2^1\binom{n}{1}\binom{2}{1} + 2^2\binom{n}{2}\binom{2}{2} \\ &= 1 \cdot 1 \cdot 1 + 2 \cdot n \cdot 2 + 4 \cdot \frac{n!}{2!(n-2)!} \cdot 1 \\ &= 1 + 4n + 2n(n-1) \\ &= 1 + 4n + 2n^2 - 2n \\ &= 2n^2 + 2n + 1 \end{aligned}$$

pontos.

Estamos interessados nos casos em que a dimensão n esteja relacionada de alguma forma com a cardinalidade das bolas de Lee em $\mathbb{Z}^n$ de raio 2. O próximo lema trata destes casos, em que $2n^2 + 2n + 1$ seja múltiplo de um primo p, além de garantir a injetividade da função η.

Lema 4.2.3. *Seja P o conjunto dos primos $p \equiv 1 \pmod 4$. A função $\eta : P \to \mathbb{Z}^+$ definida a partir do Lema 4.2.2 é injetiva. Além disso, se $\eta(p) = n$, com $p \in P$, então $2n^2 + 2n + 1 = mp$, para algum inteiro positivo $m < p$. Em particular, p é o maior primo divisor de $2n^2 + 2n + 1$.*

Demonstração. Comecemos por mostrar a segunda afirmação, isto é, que

$$2\eta(p)^2 + 2\eta(p) + 1 = mp$$

para algum $m < p$.

Por definição, temos $2\eta(p)^2 + 2\eta(p) + 1 = mp$ para algum inteiro positivo m. Logo,

$$\begin{aligned} 2mp &= 2\left(2\eta(p)^2 + 2\eta(p) + 1\right) \\ &= 4\eta(p)^2 + 4\eta(p) + 2 \\ &= (2\eta(p) + 1)^2 + 1 \\ &\leq \left(2 \cdot \frac{p-3}{2} + 1\right)^2 + 1 \\ &= (p-2)^2 + 1 < p^2 + p^2 = 2p^2, \end{aligned}$$

de onde obtemos $m < p$.

Agora, vamos mostrar que de fato η é injetiva. Sejam $p, q \in P$. Suponhamos que $\eta(p) = \eta(q)$. Como p é o maior primo divisor de $2\eta(p)^2 + 2\eta(p) + 1$ e como, por hipótese, $\eta(p) = \eta(q)$, p é também o maior primo divisor de $2\eta(q)^2 + 2\eta(q) + 1$. Entretanto, para $q \in P$, o resultado que mostramos anteriormente também garante que q é o maior primo divisor de $2\eta(q)^2 + 2\eta(q) + 1$.

Logo, p e q devem ser iguais donde segue que η é um função injetiva. □

Vamos definir a seguir o conjunto de números primos que é o objeto principal do estudo apresentado no decorrer deste capítulo.

Definição 4.2.4. Sejam p um primo tal que $p \equiv 1 \pmod 4$, i a raiz quadrada de -1 módulo p e $\langle 4 \rangle_p$ o subgrupo multiplicativo de $\mathbb{Z}_p^*$ gerado por 4. Dizemos que p é *amigável* se, $2i \notin \langle 4 \rangle_p$ ou $-2i \notin \langle 4 \rangle_p$. Denotaremos por $\mathcal{F}$ o conjunto de todos os primos amigáveis.

Lema 4.2.5. ***(Condição de Amigabilidade)*** *Sejam p um número primo com $p \equiv 1 \pmod 4$ e i tal que $i^2 \equiv -1 \pmod p$. Então, $2i \in \langle 4 \rangle_p$ se, e somente se, $-2i \in \langle 4 \rangle_p$.*

Demonstração. Seja $2i \in \langle 4 \rangle_p$. Então, existe um inteiro x, tal que $2i \equiv 4^x \pmod{p}$. Daí,

$$(2i)^3 = 2^3 i^3 = -8i = -2i \cdot 4 \equiv 4^{3x} \pmod{p}.$$

Logo, $-2i \equiv 4^{3x-1} \pmod{p}$, donde, $-2i \in \langle 4 \rangle_p$. A recíproca é válida utilizando o mesmo raciocínio e, assim, o resultado segue. □

Exemplo 4.2.6. Vamos verificar se 5, 13 e 17 são amigáveis.

Primeiramente, notemos que todos são da forma $4k + 1$, para algum $k \in \mathbb{N}$. Agora, precisamos determinar $i \in \mathbb{Z}_p^*$ tal que $i^2 \equiv -1 \pmod{p}$ e calcular o subgrupo multiplicativo gerado por 4 em cada caso.

Para $p = 5$, é fácil ver que $2^2 \equiv 4 \equiv -1 \pmod{5}$ e portanto $i = 2$, $-i = 3$. Além disso,

$$\begin{aligned}
\langle 4 \rangle_5 &= \{4^0, 4^1, 4^2, 4^3, 4^4\} \\
&= \{1, 4, 16, 64, 256\} \\
&= \{1, 4, 1, 4, 1\} \\
&= \{1, 4\}.
\end{aligned}$$

Portanto, $4 = 2i \in \langle 4 \rangle_5$ e desta maneira, $5 \notin \mathcal{F}$.

Para $p = 13$, temos $5^2 \equiv 25 \equiv 12 \equiv -1 \pmod{13}$ e, então, $i = 5$, $-i = 8$. Além disso,

$$\begin{aligned}
\langle 4 \rangle_{13} &= \{4^0, 4^1, 4^2, \ldots, 4^{12}\} \\
&= \{1, 4, 16, 64, 256, 1.024, 4.096, 16384, 65536, \\
&\quad 262144, 1048576, 4194304, 16777216\} \\
&= \{1, 4, 3, 12, 9, 10, 1, 4, 3, 12, 9, 10, 1\} \\
&= \{1, 3, 4, 9, 10, 12\}.
\end{aligned}$$

Portanto, $10 = 2i \in \langle 4 \rangle_{13}$ e desta maneira, $13 \notin \mathcal{F}$.

Vimos que 5 e 13 não são primos amigáveis. Vejamos agora o caso $p = 17$.

Note que $4^2 \equiv 16 \equiv -1 \pmod{17}$ e, então, $i = 4$, $-i = 13$. Além disso,

$$\begin{aligned}\langle 4\rangle_{17} &= \{4^0, 4^1, 4^2, \ldots, 4^{16}\} \\ &= \{1, 4, 16, 64, 256, 1024, 4096, 16384, 65536, 262144, 1048576, 4194304, \\ &\quad 16777216, 67108864, 268435456, 1073741824, 4294967296\} \\ &= \{1, 4, 16, 13, 1, 4, 16, 13, 1, 4, 16, 13, 1, 4, 16, 13, 1\} \\ &= \{1, 4, 13, 16\}.\end{aligned}$$

Portanto, $8 = 2i \notin \langle 4\rangle_{17}$ e desta maneira, $17 \in \mathcal{F}$, isto é, 17 é o primeiro primo com a propriedade de ser amigável.

Quando os primos crescem, o custo para determinar $\langle 4\rangle_p$ e $\pm i$ aumenta e, neste sentido, facilita utilizar recursos computacionais para os cálculos. Para fins de comparação, vejamos agora esse processo para um primo de 4 dígitos que, de certa forma, é um primo razoavelmente pequeno porém nos renderia uma quantidade massiva de cálculos se fosse feito à mão.

Para $p = 1997$, temos $i = 412$ e $-i = 1585$, de forma que

$$412^2 \equiv 169744 \equiv 84 \times 1997 + 1996 \equiv -1 \pmod{1997}$$

e

$\langle 4\rangle_{1997} = \{1, 4, 6, 7, 9, 10, 15, 16, 17, 22, 24, 25, 26, 28, 29, 33, 36, 37, 38, 39, 40, 42, 46, 49, 53, 54, 55, 57, 60, 61, 62, 63, 64, 65, 67, 68, 69, 70, 71, 79, 81, 82, 86, 88, 89, 90, 93, 94, 95, 96, 100, 101, 102, 104, 105, 109, 112, 115, 116, 118, 119, 121, 123, 129, 132, 135, 139, 141, 143, 144, 146, 148, 150, 151, 152, 153, 154, 155, 156, 157, 160, 163, 166, 168, 169, 170, 174, 175, 177, 182, 184, 193, 194, 196, 198, 199, 203, 205, 206, 209, 212, 214, 215, 216, 219, 220, 222, 223, 225, 226, 227, 228, 229, 231, 233, 234, 235, 239, 240, 244, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 259, 260, 261, 262, 263, 266, 268, 271, 272, 273, 274, 276, 280, 283, 284, 289, 290, 291, 293, 294, 295, 297, 298, 299, 307, 309, 313, 316, 317, 318, 321, 322, 324, 328, 330, 333, 334, 337, 339, 341, 342, 343, 344, 346, 351, 352, 353, 356, 358, 359, 360, 361, 362, 365, 366, 367, 370, 371, 372, 374, 375, 376, 378, 380, 381, 382, 384, 385, 389, 390, 393, 394, 397, 399, 400, 401, 402, 403, 404, 408, 409, 411, 414, 415, 416, 419, 420, 421, 422, 425, 426, 427, 431, 434, 435, 436, 437, 441, 442, 443,

447, 448, 451, 455, 457, 460, 461, 464, 467, 469, 472, 473, 474, 476, 477, 479, 482, 483, 484, 485, 486, 487, 490, 491, 492, 493, 495, 497, 499, 501, 503, 509, 513, 515, 516, 517, 519, 523, 528, 529, 530, 533, 534, 535, 537, 538, 540, 543, 549, 550, 553, 554, 555, 556, 557, 558, 559, 561, 562, 563, 564, 565, 567, 570, 572, 573, 574, 576, 584, 585, 587, 589, 591, 592, 593, 599, 600, 602, 603, 604, 606, 607, 608, 610, 611, 612, 613, 616, 619, 620, 621, 622, 623, 624, 625, 628, 629, 630, 633, 635, 638, 639, 640, 641, 646, 647, 649, 650, 651, 652, 654, 655, 658, 659, 661, 662, 663, 664, 665, 670, 672, 676, 677, 680, 683, 685, 690, 691, 694, 696, 698, 700, 701, 707, 708, 709, 710, 711, 713, 714, 723, 725, 726, 728, 729, 733, 735, 736, 738, 743, 745, 746, 754, 758, 761, 763, 766, 767, 769, 772, 774, 776, 779, 782, 784, 787, 790, 792, 795, 796, 801, 803, 805, 807, 809, 810, 812, 814, 817, 820, 821, **824**, 825, 826, 831, 833, 834, 835, 836, 837, 839, 841, 843, 846, 847, 848, 855, 856, 858, 859, 860, 861, 864, 865, 866, 876, 877, 878, 880, 888, 890, 892, 893, 895, 898, 900, 901, 903, 904, 905, 906, 907, 908, 909, 912, 913, 915, 916, 918, 919, 924, 925, 926, 930, 932, 933, 935, 936, 940, 942, 943, 945, 947, 949, 950, 953, 955, 956, 957, 960, 961, 962, 969, 973, 975, 976, 977, 978, 981, 983, 985, 987, 988, 989, 992, 993, 996, 997, 1000, 1001, 1004, 1005, 1008, 1009, 1010, 1012, 1014, 1016, 1019, 1020, 1021, 1022, 1024, 1028, 1035, 1036, 1037, 1040, 1041, 1042, 1044, 1047, 1048, 1050, 1052, 1054, 1055, 1057, 1061, 1062, 1064, 1065, 1067, 1071, 1072, 1073, 1078, 1079, 1081, 1082, 1084, 1085, 1088, 1089, 1090, 1091, 1092, 1093, 1094, 1096, 1097, 1099, 1102, 1104, 1105, 1107, 1109, 1117, 1119, 1120, 1121, 1131, 1132, 1133, 1136, 1137, 1138, 1139, 1141, 1142, 1149, 1150, 1151, 1154, 1156, 1158, 1160, 1161, 1162, 1163, 1164, 1166, 1171, 1172, 1173, 1176, 1177, 1180, 1183, 1185, 1187, 1188, 1190, 1192, 1194, 1196, 1201, 1202, 1205, 1207, 1210, 1213, 1215, 1218, 1221, 1223, 1225, 1228, 1230, 1231, 1234, 1236, 1239, 1243, 1251, 1252, 1254, 1259, 1261, 1262, 1264, 1268, 1269, 1271, 1272, 1274, 1283, 1284, 1286, 1287, 1288, 1289, 1290, 1296, 1297, 1299, 1301, 1303, 1306, 1307, 1312, 1314, 1317, 1320, 1321, 1325, 1327, 1332, 1333, 1334, 1335, 1336, 1338, 1339, 1342, 1343, 1345, 1346, 1347, 1348, 1350, 1351, 1356, 1357, 1358, 1359, 1362, 1364, 1367, 1368, 1369, 1372, 1373, 1374, 1375, 1376, 1377, 1378, 1381, 1384, 1385, 1386, 1387, 1389, 1390, 1391, 1393, 1394, 1395, 1397, 1398, 1404, 1405, 1406, 1408, 1410, 1412, 1413, 1421, 1423, 1424, 1425, 1427, 1430, 1432, 1433, 1434, 1435, 1436, 1438, 1439, 1440, 1441, 1442, 1443, 1444, 1447, 1448, 1454, 1457, 1459, 1460, 1462, 1463, 1464, 1467, 1468, 1469, 1474, 1478, 1480, 1481, 1482, 1484, 1488, 1494, 1496, 1498, 1500,

1502, 1504, 1505, 1506, 1507, 1510, 1511, 1512, 1513, 1514, 1515, 1518, 1520, 1521, 1523, 1524, 1525, 1528, 1530, 1533, 1536, 1537, 1540, 1542, 1546, 1549, 1550, 1554, 1555, 1556, 1560, 1561, 1562, 1563, 1566, 1570, 1571, 1572, 1575, 1576, 1577, 1578, 1581, 1582, 1583, 1586, 1588, 1589, 1593, 1594, 1595, 1596, 1597, 1598, 1600, 1603, 1604, 1607, 1608, 1612, 1613, 1615, 1616, 1617, 1619, 1621, 1622, 1623, 1625, 1626, 1627, 1630, 1631, 1632, 1635, 1636, 1637, 1638, 1639, 1641, 1644, 1645, 1646, 1651, 1653, 1654, 1655, 1656, 1658, 1660, 1663, 1664, 1667, 1669, 1673, 1675, 1676, 1679, 1680, 1681, 1684, 1688, 1690, 1698, 1699, 1700, 1702, 1703, 1704, 1706, 1707, 1708, 1713, 1714, 1717, 1721, 1723, 1724, 1725, 1726, 1729, 1731, 1734, 1735, 1736, 1737, 1738, 1740, 1741, 1742, 1743, 1744, 1745, 1746, 1747, 1748, 1749, 1750, 1753, 1757, 1758, 1762, 1763, 1764, 1766, 1768, 1769, 1770, 1771, 1772, 1774, 1775, 1777, 1778, 1781, 1782, 1783, 1785, 1788, 1791, 1792, 1794, 1798, 1799, 1801, 1803, 1804, 1813, 1815, 1820, 1822, 1823, 1827, 1828, 1829, 1831, 1834, 1837, 1840, 1841, 1842, 1843, 1844, 1845, 1846, 1847, 1849, 1851, 1853, 1854, 1856, 1858, 1862, 1865, 1868, 1874, 1876, 1878, 1879, 1881, 1882, 1885, 1888, 1892, 1893, 1895, 1896, 1897, 1901, 1902, 1903, 1904, 1907, 1908, 1909, 1911, 1915, 1916, 1918, 1926, 1927, 1928, 1929, 1930, 1932, 1933, 1934, 1935, 1936, 1937, 1940, 1942, 1943, 1944, 1948, 1951, 1955, 1957, 1958, 1959, 1960, 1961, 1964, 1968, 1969, 1971, 1972, 1973, 1975, 1980, 1981, 1982, 1987, 1988, 1990, 1991, 1993, 1996}.

Portanto, como $2i = 824$ é um elemento de $\langle 4 \rangle_{1997}$, 1997 não é um primo amigável.

Observação 4.2.7. Os primos amigáveis menores que 1000 são: 17, 73, 89, 97, 193, 233, 241, 257, 281, 337, 353, 401, 433, 449, 557, 601, 617, 641, 673, 769, 881, 929, 937 e 977. O conjunto de todos os números primos possui 168 elementos menores que 1000, ao passo que $\mathcal{F}$ possui 24 elementos menores que 1000. Assim,

$$\lim_{x \mapsto 1000} \frac{\#\{p \in \mathcal{F} \,:\, p \leq x\}}{\#\{p \text{ primo} \,:\, p \leq x\}} = \frac{24}{168} = \frac{1}{7}.$$

Neste ponto, vamos mostrar que para primos amigáveis e certos $\lambda > 0$, o conjunto das λ-coberturas homogêneas em dimensão n e raio igual a 2 é vazio, mas antes, definamos um conjunto particular de inteiros que será utilizado como suporte na demonstração deste teorema principal.

Definição 4.2.8. Sejam dados p primo e $n \in \mathbb{N}$. Tomemos a, b os menores inteiros positivos tais que:

$$p \mid 4^a + 4n + 2$$

e,

$$p \mid 4^b - 1.$$

Definamos $\mathbb{X}_p$ como o conjunto dos inteiros da forma $ax + by$, com $x \geq 1, y \geq 0$.

Observação 4.2.9. Notemos que o conjunto $\mathbb{X}_p$ da Definição 4.2.8 é fechado para a adição. De fato, dados $k_1, k_2 \in \mathbb{X}_p$, existem $x_1, x_2 \geq 1$ e $y_1, y_2 \geq 0$, tais que

$$k_1 + k_2 = (ax_1 + by_1) + (ax_2 + by_2) = a(x_1 + x_2) + b(y_1 + y_2) \in \mathbb{X}_p.$$

Agora, vejamos o teorema de maior importância, até o momento, e sua demonstração feita em [24], como a seguir:

Teorema 4.2.10. *Seja $\eta : \mathcal{F} \to \mathbb{Z}^+$ como no Lema 4.2.3. Se p é um primo amigável e $n = \eta(p)$, então $Cov^{\lambda}(n, 2) = \emptyset$, para todo λ tal que p não divide λ. Em particular, $Cov^1(n, 2) = LP(n, 2) = \emptyset$.*

Demonstração. Sejam p é um primo amigável e $n = \eta(p)$.

Pelo Lema 4.2.3, temos que $2n^2 + 2n + 1 = mp$, onde $m < p$ é um inteiro positivo. Além disso, $0 < n < \dfrac{p-1}{2}$, pois, por hipótese, $n = \eta(p)$.

Suponhamos, por contradição, que exista uma λ-cobertura homogênea $\mathcal{C} \subseteq \mathbb{Z}^n$ com raio $e = 2$ e $p \nmid \lambda$.

Pelo Teorema 4.1.3, existe um homomorfismo $\phi : \mathbb{Z}^n \to G$ tal que a restrição $\phi|_{L_{n,2}} : L_{n,2} \to G$ é uma aplicação λ-para-1. Em particular,

$$\#L_{n,2} = 2n^2 + 2n + 1 = \lambda|G|\,.$$

Desta maneira, $p \mid |G|$ pois, por hipótese, $p \nmid \lambda$. Portanto, existe um homomorfismo sobrejetor $\phi' : G \to \mathbb{Z}_p$. Deste modo, esta aplicação é $\frac{|G|}{p}$-para-1.

Agora, consideremos o homomorfismo $\psi = \phi' \circ \phi : \mathbb{Z}^n \to \mathbb{Z}_p$. Note que, a aplicação ψ restrita à $L_{n,2}$, $\psi|_{L_{n,2}} : L_{n,2} \to \mathbb{Z}_p$ é uma aplicação m-para-1.

Seja r uma raiz primitiva módulo p. Como $2n < p-1$, pela fórmula da série geométrica e Pequeno Teorema de Fermat, temos

$$\sum_{x\in L_{n,2}} \psi(x)^{2k} \equiv m\sum_{y=1}^{p-1} y^{2k} \equiv m\sum_{j=0}^{p-2} r^{2kj} \equiv \frac{m\left(r^{2k(p-1)}-1\right)}{r-1} \equiv 0 \pmod{p}, \quad (4.1)$$

para todo $1 \leq k \leq n$.

Seja $\{e_1, e_2, \ldots, e_n\}$ a base canônica de $\mathbb{R}^n$. Consideremos, $x_i = \psi(e_i)$, para todo $1 \leq i \leq n$, e $S_k = \sum_{i=1}^{n} x_i^{2k}$.

Em [18], o autor obtém a seguinte igualdade:

$$\sum_{x\in L_{n,2}} \psi(x)^{2k} = (4^k + 4n + 2)S_{2k} + 2\sum_{t=1}^{k-1} \binom{2k}{2t} S_{2t}S_{2(k-t)}. \quad (4.2)$$

Como p é um primo amigável, temos que p não divide $4^k + 4n + 2$. De fato, como $2n^2 + 2n + 1 \equiv 0 \pmod{p}$, então

$$(2n+1)^2 \equiv -1 \pmod{p}$$

e

$$2n + 1 \equiv \pm i \pmod{p},$$

onde i é uma raiz quadrada de -1 módulo p, que existe pois $p \equiv 1 \pmod{4}$.

Portanto, como p é amigável, pelo Lema 4.2.5, temos

$$4^k + 4n + 2 \equiv 4^k \pm 2i \not\equiv 0 \pmod{p},$$

já que, caso contrário, teríamos $\pm 2i \equiv 1 \pmod{4}$, o que é uma contradição, pois o quadrado do primeiro termo é congruente a 0 módulo 4.

Então, existe um inteiro $a_k \in \mathbb{Z}_p$ tal que $(4^k + 4n + 2) \cdot a_k \equiv 1 \pmod{p}$. Multiplicando por a_k ambos os lados da equação (4.2) e, utilizando a equação (4.1), temos

$$S_{2k} \equiv -2a_k \sum_{t=1}^{k-1} \binom{2k}{2t} S_{2t}S_{2(k-t)} \pmod{p}, \quad (4.3)$$

para todo $1 \leq k \leq n$.

Utilizando a equação obtida em (4.3), vamos provar por indução em k que, se $1 \leq k < \frac{p-1}{2}$ não é um elemento do conjunto $\mathbb{X}_p$, então $S_{2k} = 0$.

De fato, suponhamos que $S_{2k} = 0$, para todo $k \leq k_0 - 1$ que não está em $\mathbb{X}_p$. Vamos mostrar que $S_{2k_0} = 0$ se $k_0 \notin \mathbb{X}_p$. Suponhamos que $k_0 \notin \mathbb{X}_p$.

Como para qualquer k tal que $p \mid 4^k + 4n + 2$ é da forma $a + by$ e, assim sendo é um elemento de $\mathbb{X}_p$, seque que $p \nmid 4^{k_0} + 4n + 2$. Além disso, como $\mathbb{X}_p$ é fechado para a adição e $k_0 \notin \mathbb{X}_p$, segue que ao menos t ou $k_0 - t$ não pertence ao conjunto $\mathbb{X}_p$, onde $1 \leq t \leq k_0 - 1$. Daí, temos

$$\begin{aligned} 0 &= (4^{k_0} + 4n + 2)S_{2k_0} + 2\sum_{t=1}^{k_0-1} \binom{2k_0}{2t} S_{2t}S_{2(k_0-t)} \\ &= (4^{k_0} + 4n + 2)S_{2k_0}, \end{aligned}$$

em $\mathbb{Z}_p$. Logo, como $4^{k_0} + 4n + 2 \neq 0$, temos que $S_{2k_0} = 0$.

Agora, denotemos por

$$e_k = \sum_{1 \leq i_1 \leq \cdots \leq i_k \leq n} x_{i_1}^2 \ldots x_{i_k}^2,$$

o k-ésimo polinômio simétrico elementar em $x_1^2, x_2^2, \ldots, x_n^2$. Daí, pela identidade de Newton, para todo $1 \leq k \leq n$ temos

$$ke_k \equiv \sum_{i=1}^{k} (-1)^{i-1} e_{k-i} S_{2i} \equiv 0 \pmod{p}.$$

Como $0 < k \leq n < p$, segue que $e_k \equiv 0 \pmod{p}$ para todo $1 \leq k \leq n$. Pelas relações entre coeficientes e raízes, obtemos:

$$\prod_{i=1}^{n} (x - x_i^2) \equiv \sum_{i=0}^{n} (-1)^i e_i x^{n-i} \equiv x^n \pmod{p}.$$

Isto implica que, $x_i^{2n} = 0$ em $\mathbb{Z}_p$ e, então, $x_i = 0$ para $1 \leq i \leq n$, o que é uma contradição, pois ψ é sobrejetora. Portanto, $Cov^{\lambda}(n, 2) = \emptyset$. □

Como, para $q \geq 2e + 1$, códigos perfeitos de Lee em $\mathbb{Z}^n$ correspondem à códigos perfeitos de Lee em $\mathbb{Z}_q^n$, segue imediatamente do Teorema 4.2.10 que:

Corolário 4.2.11. *Se p é um primo amigável e $n = \eta(p)$, então não existe código linear perfeito de Lee de raio 2 em $\mathbb{Z}_q^n$ para $q \geq 5$.*

Observação 4.2.12. A função injetiva $\eta : \mathcal{F} \to \mathbb{Z}^+$ definida como no Lema 4.2.2 não possui uma lei geral de formação, entretanto por suas propriedades apresentadas podemos utilizar uma forma computacional simples para calcular a imagem dos primos amigáveis em seu domínio. A seguir apresentamos um algoritmo em Python que retorna o inteiro positivo $\eta(p)$ a partir de um primo $p \equiv 1 \pmod 4$ dado:

```
def find_eta_p_cong_1(p):
    eta_p = None
    limit = (p - 3) // 2
    for eta in range(1, limit + 1):
        if (2 * eta**2 + 2 * eta + 1) % p == 0:
            eta_p = eta
            break

    return eta_p
```

Algoritmo 4.1 – Função η em linguagem Python.

Utilizando tal algoritmo podemos calcular as imagens de η para os primos amigáveis menores que 1000 (da Observação 4.2.7):

$\eta(17) = 6$	$\eta(281) = 26$	$\eta(617) = 211$
$\eta(73) = 13$	$\eta(337) = 94$	$\eta(641) = 243$
$\eta(89) = 27$	$\eta(353) = 155$	$\eta(673) = 307$
$\eta(97) = 37$	$\eta(401) = 190$	$\eta(769) = 353$
$\eta(193) = 40$	$\eta(433) = 89$	$\eta(881) = 193$
$\eta(233) = 44$	$\eta(449) = 33$	$\eta(929) = 302$
$\eta(241) = 88$	$\eta(557) = 219$	$\eta(937) = 370$
$\eta(257) = 120$	$\eta(601) = 62$	$\eta(977) = 362$

4.3 SOBRE A INFINITUDE DE $\mathcal{F}$

Sabemos que primos amigáveis estão relacionados com alguns casos particulares da Conjectura de Golomb-Welch. Como vimos, se p for um primo amigável, podemos mostrar que não existem ladrilhamentos do espaço para certos parâmetros. É natural nos perguntarmos se essa abordagem nos permite ter uma quantidade considerável de casos particulares, visto que estamos trabalhando apenas com

alguns tipos de primos específicos. Neste sentido, agora, vamos nos concentrar em provar que existem infinitos primos amigáveis, o que nos daria uma quantidade também infinita de casos provados da Conjectura.

Como na Observação 4.2.7, é útil possuirmos uma maneira sistemática de determinarmos o quão "denso" é um subconjunto em relação ao conjunto dos números primos, no sentido de que quando estivermos interessados em estudar a infinitude (ou não) de certos subconjuntos de primos, bastaria investigar como tal subconjunto se distribui em relação ao conjunto maior em que ele está contido.

Para tanto, consideremos a definição a seguir:

Definição 4.3.1. A *densidade de um conjunto* X em relação aos números primos é dada por

$$\mathcal{D}(X) = \lim_{x \mapsto \infty} \frac{\#\{p \in X \,:\, p \leq x\}}{\#\{p \text{ primo} \,:\, p \leq x\}},$$

quando o limite existir.

Observação 4.3.2. Pelo Teorema dos Números Primos, podemos notar que a densidade do conjunto X, na definição anterior, é equivalente a

$$\mathcal{D}(X) = \lim_{x \mapsto \infty} \frac{\#\{p \in X \,:\, p \leq x\} \cdot \ln x}{x},$$

Se considerarmos que X possua n elementos, onde n é um inteiro não-negativo, pela equação anterior temos:

$$\mathcal{D}(X) = \lim_{x \mapsto \infty} \frac{n \cdot \ln x}{x} = n \lim_{x \mapsto \infty} \frac{\ln x}{x} = n \cdot 0 = 0.$$

Portanto, todo conjunto finito de números primos possui densidade nula, isto é, mostrar que um subconjunto de números primos possui densidade positiva é suficiente para concluirmos que este conjunto contém infinitos elementos.

Mostraremos então que $\mathcal{F}$ possui densidade positiva.

Definição 4.3.3. Sejam $a \geq 1$, $r \geq 0$ inteiros quaisquer e q primo. Definimos o subconjunto de primos $B(a, q, r)$, dado por

$$B(a, q, r) = \{p \,:\, \text{ord}_p(a) = mq^r, \text{para algum } m \in \mathbb{Z} \text{ tal que } q \not| m\}$$

onde $\text{ord}_p(a)$ é a ordem multiplicativa de a módulo p, isto é, dado $p \in B(a,q,r)$, existe $m \in \mathbb{Z}$, $q \nmid m$, tais que

$$a^{mq^r} \equiv 1 \pmod{p}.$$

Definição 4.3.4. Dados $x \in \mathbb{R}$ e $Y \subseteq \mathbb{Z}$, definimos a função $N_x(\cdot)$ dada por

$$N_x(Y) = \#\{y \in Y \,:\, y \leq x\},$$

que conta a quantidade de elementos menores ou iguais a x de Y.

Quando, em particular, $a = q = r = 2$, temos o seguinte resultado, que pode ser encontrado em [28]:

Teorema 4.3.5. *Seja $N_x(B(2,2,2))$. Existe um número real x_0 tal que para $x \geq x_0$, temos:*

$$N_x(B(2,2,2)) = \frac{x}{3\ln x} + O\left(\frac{x\sqrt{\ln(\ln x))}}{\ln x\sqrt{\ln(\ln x)}}\right). \tag{4.4}$$

Uma consequência direta deste teorema é que a densidade do conjunto $B(2,2,2)$ em relação ao conjunto dos números primos é dada por:

$$\begin{aligned}
\mathcal{D}(B(2,2,2)) &= \lim_{x\mapsto\infty} \frac{\#\{p \in B(2,2,2) \,:\, p \leq x\}}{\#\{p\,primo \,:\, p \leq x\}} \\
&= \lim_{x\mapsto\infty} \frac{N_x(B(2,2,2)) \cdot \ln x}{x} \\
&= \lim_{x\mapsto\infty} \frac{\left(\dfrac{x}{3\ln x} + O\left(\dfrac{x\sqrt{\ln(\ln x))}}{\ln x\sqrt{\ln(\ln x)}}\right)\right) \cdot \ln x}{x} \\
&= \lim_{x\mapsto\infty} \frac{x}{3\ln x} \cdot \frac{\ln x}{x} + \lim_{x\mapsto\infty} O\left(\frac{x\sqrt{\ln(\ln x))}}{\ln x\sqrt{\ln(\ln x)}}\right) \cdot \frac{\ln x}{x} \\
&= \frac{1}{3} + 0 = \frac{1}{3}.
\end{aligned}$$

Vamos estabelecer uma relação entre o conjunto $B(2,2,2)$ e o conjunto $\mathcal{F}$ dos números primos amigáveis, mas antes vejamos o seguinte lema:

Lema 4.3.6. *Seja $p > 2$ um número primo. Existe uma raiz primitiva r módulo p tal que $2 \equiv r^\alpha \pmod{p}$ para algum α divisor de $p-1$.*

Demonstração. Consideremos uma raiz primitiva r_0 módulo p.

Assim, podemos escrever

$$2 \equiv r_0^{\beta} \pmod{p},$$

onde $0 \leq \beta < p-1$.

Sejam $\alpha = \text{mdc}(\beta, p-1)$ e α_0 o produto dos primos divisores de $p-1$ que não dividem $\frac{p-1}{\alpha}$. Convencionamos $\alpha_0 = 1$ se este conjuntos de primos for vazio.

Daí, se $p-1 = q_1^{m_1} \dots q_k^{m_k}$ é a decomposição em primos de $p-1$, como

$$\alpha = \text{mdc}(\beta, p-1),$$

existem inteiros não-negativos $n_1, \dots, n_k$, com $0 \leq n_i \leq m_i$, $1 \leq i \leq k$, tais que

$$\alpha = q_1^{n_1} \dots q_k^{n_k}.$$

Desta maneira segue que

$$\frac{p-1}{\alpha} = q_1^{m_1-n_1} \dots q_k^{m_k-n_k}.$$

Agora, seja $\mathcal{I} = \{i_1, \dots, i_r\}$ o conjunto de índices tais que $m_{i_j} - n_{i_j} = 0$, para $1 \leq j \leq r$.

Note que $\alpha_0 = \prod_{i_j \in \mathcal{I}} q_{i_j} = q_{i_1} \dots q_{i_r}$.

Como $\text{mdc}\left(\frac{p-1}{\alpha}, \alpha_0\right) = 1$, pelo Teorema Chinês do Resto, existe $u \in \mathbb{Z}^+$ satisfazendo as congruências

$$u \equiv \frac{\beta}{\alpha} \pmod{\frac{p-1}{\alpha}} \quad \text{e} \quad u \equiv 1 \pmod{\alpha_0}. \tag{4.5}$$

Portanto,

$$\begin{aligned} \text{mdc}\left(u, \frac{p-1}{\alpha}\right) &= \text{mdc}\left(\frac{\beta}{\alpha}, \frac{p-1}{\alpha}\right) \\ &= \frac{1}{\alpha} \cdot \text{mdc}(\beta, p-1) \\ &= \frac{1}{\alpha} \cdot \alpha = 1. \end{aligned}$$

e

$$\mathrm{mdc}(u, \alpha_0) = \mathrm{mdc}(1, \alpha_0) = 1.$$

Desta maneira, como $\mathrm{mdc}\Big(u, \frac{p-1}{\alpha}\Big) = 1 = \mathrm{mdc}(u, \alpha_0)$, temos:

$$\begin{aligned} 1 = \mathrm{mdc}\Big(u, \frac{p-1}{\alpha}\Big) &= \mathrm{mdc}\Big(u, q_1^{m_1-n_1} \dots\ q_k^{m_k-n_k}\Big) \\ &= \mathrm{mdc}\Big(u, q_1^{m_1-n_1}\Big) \dots \mathrm{mdc}\Big(u, q_k^{m_k-n_k}\Big), \end{aligned}$$

e da mesma forma

$$1 = \mathrm{mdc}(u, \alpha_0) = \mathrm{mdc}(u, q_{i_1} \dots\ q_{i_r}) = \mathrm{mdc}(u, q_{i_1}) \dots \mathrm{mdc}(u, q_{i_r}),$$

pois q_i, $q_{i'}$ são primos entre si, para todo $i \neq i'$.

Isto é, $\mathrm{mdc}(u, q_i) = 1$, $1 \leq i \leq k$.

Daí, segue que

$$\begin{aligned} \mathrm{mdc}(u, p-1) &= \mathrm{mdc}(u, q_1^{m_1} \dots q_k^{m_k}) \\ &= \mathrm{mdc}(u, q_1^{m_1}) \dots \mathrm{mdc}(u, q_k^{m_k}) \\ &= 1 \dots 1 = 1. \end{aligned}$$

Como $u \equiv \dfrac{\beta}{\alpha}\ \Big(\mathrm{mod}\ \dfrac{p-1}{\alpha}\Big)$, temos que $\beta \equiv \alpha u\ \pmod{p-1}$ e podemos escrever

$$\beta = \alpha u + (p-1)h,$$

para algum $h \in \mathbb{Z}$.

Assim,

$$2 \equiv r_0^{\beta} = r_0^{\alpha u + (p-1)h} = (r_0^u)^{\alpha} \cdot (r_0^{p-1})^h \pmod{p}.$$

Pelo Pequeno Teorema de Fermat, $r_0^{p-1} \equiv 1\ \pmod{p}$, e então

$$2 \equiv (r_0^u)^{\alpha} \pmod{p}.$$

Definamos $r := r_0^u$.

Como

$$\mathrm{ord}_p(r) = \frac{p-1}{\mathrm{mdc}(p-1, u)} = \frac{p-1}{1} = p-1,$$

concluímos que r também é uma raiz primitiva e $2 \equiv r^{\alpha}\ \pmod{p}$ onde $\alpha \mid p-1$. $\square$

Teorema 4.3.7. *Seja* $P = \{p \text{ primo} : p \equiv 1 \pmod 4\}$, $\mathcal{F}$ *o conjunto dos primos amigáveis e* $B(2,2,2)$ *o conjunto dos primos* p *tais que a ordem multiplicativa de* 2 *módulo* p *é* $ord_p(2) = 4m$ *para algum* m *inteiro ímpar. Então,* $B(2,2,2) \subseteq P$ *e o conjunto dos primos amigáveis é dado por*

$$\mathcal{F} = P \backslash B(2,2,2) = \{p \in P : p \notin B(2,2,2)\}.$$

Demonstração. Seja $p \in B(2,2,2)$.

Então, $\text{ord}_p(2) = 4m$.

Pelo Teorema de Lagrange, $4m$ divide $\#\mathbb{Z}_p^* = p - 1$.

Portanto, $p \equiv 1 \pmod 4$ e assim $p \in P$.

Logo, $B(2,2,2) \subseteq P$.

Agora, sejam $p \in P$ e r uma raiz primitiva módulo p.

Tomemos $\text{ord}_p(2) = 2^\gamma m$, onde m é um inteiro ímpar, $\gamma \geq 0$ e $2 \equiv r^\alpha \pmod p$ com $0 \leq \alpha < p - 1$.

Pelo Lema 4.3.6, sem perda de generalidade, podemos supor que $\alpha \mid p - 1$ e assim, temos:

$$2^\gamma m = \text{ord}_p(2) = \frac{\text{ord}_p(r)}{\text{mdc}(\text{ord}_p(r), \alpha)} = \frac{p-1}{\alpha}. \tag{4.6}$$

Tomemos $i = r^{\frac{p-1}{4}}$.

Daí, como $p \in P$, temos as seguintes equivalências:

$$\begin{array}{lll}
& p \notin \mathcal{F} & \\
\Leftrightarrow & 2i \equiv 4^x \pmod p & \text{para algum } x \in \mathbb{Z} \\
\Leftrightarrow & r^{\alpha + \frac{p-1}{4}} \equiv r^{2\alpha x} \pmod p & \text{para algum } x \in \mathbb{Z} \\
\Leftrightarrow & \alpha + \dfrac{p-1}{4} \equiv 2\alpha x \pmod{p-1} & \text{para algum } x \in \mathbb{Z} \\
\Leftrightarrow & \dfrac{p-1}{4} \equiv (2x-1)\alpha \pmod{p-1} & \text{para algum } x \in \mathbb{Z} \\
\Leftrightarrow & \dfrac{p-1}{\alpha} \equiv 4(2x-1) \pmod{\dfrac{4(p-1)}{\alpha}} & \text{para algum } x \in \mathbb{Z} \\
\Leftrightarrow & 2^\gamma m \equiv 4(2x-1) \pmod{2^{\gamma+2}m} & \text{para algum } x \in \mathbb{Z} \\
\Leftrightarrow & 4(2x-1) + 2^{\gamma+2}my = 2^\gamma m & \text{para alguns } x, y \in \mathbb{Z}
\end{array}$$

Afirmamos que a equação $4(2x-1)+2^{\gamma+2}my = 2^{\gamma}m$ para alguns $x, y \in \mathbb{Z}$, possui solução se, e somente se, $\gamma = 2$.

De fato, se $\gamma \leq 1$, então

$$4(2x-1)+2^{\gamma+2}my = 4(2^{\gamma}my+2x-1)$$

é múltiplo de 4, enquanto $2^{\gamma}m$ não o é.

Da mesma forma, se $\gamma \geq 3$, então

$$2^{\gamma}m = 8 \cdot 2^{\gamma-3}m$$

é múltiplo de 8, enquanto

$$4(2x-1)+2^{\gamma+2}my = 8(2^{\gamma-1}my+x)-4$$

não o é.

Agora, se $\gamma = 2$, a equação pode ser reescrita da seguinte forma, visto que m é um inteiro ímpar:

$$\begin{aligned}
& 4(2x-1)+2^{2+2}my &&= 2^2m \\
\Leftrightarrow\ & 4(2x-1)+4(4my) &&= 4m \\
\Leftrightarrow\ & 4(2x-1+4my) &&= 4m \\
\Leftrightarrow\ & 2x-1+4my &&= m \\
\Leftrightarrow\ & 2x+4my &&= m+1 \\
\Leftrightarrow\ & x+2my &&= \frac{m+1}{2}
\end{aligned}$$

e possui a solução inteira $(x, y) = \left(\frac{m+1}{2}, 0\right)$.

Portanto, $p \in P\backslash\mathcal{F}$ se, e somente se, $\gamma = 2$. Isto é, se, e somente se, $p \in B(2,2,2)$.

Logo, $\mathcal{F} = P\backslash B(2,2,2)$. □

Corolário 4.3.8. *O conjunto dos primos amigáveis possui densidade* $\mathcal{D}(\mathcal{F}) = \frac{1}{6}$. *Em particular, existem infinitos primos amigáveis.*

Demonstração. Pelo Teorema dos Números Primos, o conjunto

$$P = \{\text{p primo} : p \equiv 1 \pmod 4\}$$

tem densidade $\mathcal{D}(P) = \frac{1}{2}$.

Agora, pelo Teorema 4.3.5, a densidade do conjunto $B(2,2,2)$ relativa aos números primos é igual a

$$\mathcal{D}(B(2,2,2)) = \frac{1}{3}.$$

Por fim, pelo Teorema 4.3.7, a densidade de $\mathcal{F}$ é dada por

$$\mathcal{D}(\mathcal{F}) = \mathcal{D}(P \backslash B(2,2,2)) = \mathcal{D}(P) - \mathcal{D}(B(2,2,2)) = \frac{1}{2} - \frac{1}{3} = \frac{1}{6}.$$

Como um conjunto finito possui densidade nula, concluímos então que o conjunto $\mathcal{F}$ deve possuir infinitos elementos pois sua densidade é positiva. □

Corolário 4.3.9. *Existem infinitas dimensões $n \geq 3$ para as quais $LP(n,2) = \emptyset$.*

Demonstração. Pelo Corolário 4.3.8, o conjunto $\mathcal{F}$ dos primos amigáveis possui infinitos elementos e como a função η é injetora, temos que sua imagem $\eta(\mathcal{F})$ também possui infinitos elementos. Por fim, pelo Teorema 4.2.10, $LP(n,2) = \emptyset$, para todo $n \in \eta(\mathcal{F})$. □

Dessa forma, existem infinitas dimensões n para as quais não existe código de Lee perfeito de raio 2 e dimensão n.

Encerramos destacando que essa demonstrção levanta uma aparente conexão entre os primos amigáveis e os primos representados pela forma quadrática $f(x,y) = 4x^2 + 4xy + 9y^2$. Os primeiros valores desta sequência de primos são 17, 73, 89, 97, 193, 233, 241, 281, 401, 433, 449, 601, 617, 641, 673, 769, 929, 937, 977, que são todos primos amigáveis. Primos representados por formas quadráticas compõem uma área muito importante da teoria dos números e têm conexão com curvas elípticas e teoria dos corpos de classes. Esse resultado pode levar a uma prova alternativa da existência de infinitos primos amigáveis e, consequentemente, uma nova prova da não existência de códigos perfeitos lineares com parâmetros $(n,2)$ para infinitos valores de $n > 2$. Essa consideração nos leva a questionar se a utilização de formas quadráticas mais abrangentes poderia auxiliar na prova de outros resultados de não existência em relação à métrica de Lee e fornecer novas perspectivas em relação à Conjectura de Golomb-Welch como um todo em seu caso geral.

5 CONCLUSÃO

Há mais de 50 anos, Golomb e Welch propuseram a conjectura que afirma que não há códigos lineares perfeitos para os parâmetros dimensão $n \geq 3$ e raio $e \geq 2$, com erros medidos na métrica de Lee. Nesse trabalho, vimos alguns dos casos elementares e, finalmente, o caso com $e = 2$ para infinitas dimensões, que têm relação com um conjunto especial de primos. No entanto, a conjectura permanece aberta para infinitos casos, apesar de muitos esforços de diferentes pesquisadores, o que significa que há espaço para estudo no tema. Notamos ainda que cada passo dado na direção de algum caso particular muitas vezes é apoiado numa nova ideia disruptiva que pouco se relaciona com os outros casos já provados. Isto parece dificultar, de alguma forma, uma demonstração geral da conjectura. De qualquer modo, depois do estudo para essa dissertação, nossa expectativa é que, em geral, a Conjectura de Golomb-Welch seja verdadeira e esperamos, futuramente, contribuir para essa conclusão.

REFERÊNCIAS

1 AMERICAN MATHEMATICAL SOCIETY. Feature Column. **Digital Revolution (Part III) - Error Correction Codes**. American Mathematical Society, 2003. Disponível em https://www.ams.org/publicoutreach/feature-column/fcarc-errors6. Acesso em 30 mar. 2023.

2 ASTOLA, J. An Elias-type bound for Lee codes over large alphabets and its application to perfect codes. **IEEE Trans. Inf. Theory**, v. 28, n. 1, p. 111-113, 1982.

3 CASCELLI, R. **Códigos Perfeitos e Raio de Empacotamento**. Monografia (Graduação em Matemática) - Instituto de Ciências Exatas, UFJF, Juiz de Fora, 2019. Disponível em https://https://www2.ufjf.br/matematica/wp-content/uploads/sites/393/2014/02/C%C3%B3digos-Perfeitos-e-Raio-de-Empacotamento.pdf. Acesso em 8 jul. 2023.

4 CONWAY, J.H.; SLOANE, N.J.A. **Sphere Packings, Lattices and Groups**. New York: Springer, 1999.

5 COXETER, H. S. M. **Regular Polytopes**.New York: Macmillan, 1963.

6 ETZION, T., VARDY, A., YAAKOBI, E. Dense Error-Correcting Codes in the Lee Metric. **IEEE Inf. Theory Workshop**, ITW 2010 Dublin, 2010.

7 GOLOMB, S. W.; WELCH, L. R. Perfect codes in the Lee metric and the packing of polyominoes. **SIAM Journal on Applied Mathematics** v. 18, n. 2, p. 302-317, 1970.

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

9 GUIMARÃES, I. (MathGurl) **COMO CORRIGIR ERROS?!**. YouTube, publicado em 14 jul. 2022. Disponível em: https://www.youtube.com/watch?v=ASxioReFKlI. Acesso em 8 jul. 2023.

10 HAMMING, R. W. Error detecting and error correcting codes. **The Bell System Technical Journal**. v. 29, n. 2, p. 147 - 160, 1950.

11 HEFEZ, Abramo; VILLELA, Maria Lúcia T. **Códigos Corretores de Erros**. 2.ed. Rio de Janeiro: IMPA, 2008.

12 HORAK, P. On perfect Lee codes. **Discrete Math**, v. 309, n. 18, p. 5551–5561, 2009.

13 HORAK, P.; ALBDAIWI, B. F.Diameter perfect Lee codes. **IEEE Trans. Inf. Theory**. v. 58, n. 8, p. 5490–5499, 2012.

14 HORAK, P.; GROSEK, O. A new approach towards the Golomb-Welch conjecture. **European Journal of Combinatorics**. v. 38, p. 12–22, 2014.

15 HORAK, P.; KIM, D. 50 years of the Golomb–Welch conjecture. **IEEE Trans. Inf. Theory**, v. 64, n. 4, p. 3048-3061, 2017.

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

17 JORGE, G. C. **Reticulados q-ários e algébricos**. Tese (Doutorado em Matemática) - Instituto de Matemática, Estatística e Computação Científica, UNICAMP, Campinas, 2012. Disponível em `https://hdl.handle.net/20.500.12733/1617000`. Acesso em 20 jul. 2023.

18 KIM, D. Nonexistence of perfect 2-error-correcting Lee codes in certain dimensions. **European Journal of Combinatorics**, v. 63, p. 1–5, 2017.

19 LEE, C. Some properties of nonbinary error-correcting codes. **IRE Transactions on Information Theory**. v. 4, n. 2, p. 77-82, 1958.

20 LEPISTÖ, T. A modification of the Elias-bound and nonexistence theorems for perfect codes in the Lee-metric. **Information and Control**, v. 49, n. 2, p. 109-124, 1981.

21 MINKOWSKI, H. Dichteste gitterförmige Lagerung kongruenter Körper. **Nachrichten von der Gesellschaft der Wissenschaften**. p.311–355, 1904.

22 MORAIS, G. **Códigos perfeitos na métrica de Lee e a Conjectura de Golomb-Welch**. Dissertação (Mestrado em Matemática Aplicada) - Instituto de Ciência e Tecnologia, UNIFESP, São José dos Campos, 2017. Disponível em `https://repositorio.unifesp.br/handle/11600/50647`. Acesso em 8 jul. 2023.

23 POST, K. A. Nonexistence theorems on perfect Lee codes over large alphabets. **Information and Control**. v. 29, n. 4, p. 369–380, 1975.

24 QURESHI, C.; CAMPELLO, A.; COSTA, S. Non-Existence of Linear Perfect Lee Codes With Radius 2 for Infinitely Many Dimensions. **IEEE Trans. Inf. Theory**. v. 64, n. 4, p. 3042-3047, 2018.

25 SAMUEL, P. **Algebraic Theory of Numbers**. Michigan: Hermann, 1970.

26 SHANNON, Claude E. A Mathematical Theory of Communication. **Bell System Technical Journal**. v. 27, p. 379–423, 623–656, 1948.

27 ULRICH, W. Non-binary error correction codes. **Bell System Technical Journal**. v. 36, n. 6, p. 1341–1388, 1957.

28 WIERTELAK, K. On the density of some sets of primes I. **Acta Arithmetica**. v. 34, n. 3, p. 183–196, 1978.

29 ZHANG, T.; GE, G. Perfect and quasi-perfect codes under the lp metric. **IEEE Trans. Inf. Theory**. v. 63, n. 7, p. 4325–4331, 2017.