

UNICAMP

UNIVERSIDADE ESTADUAL DE
CAMPINAS

Instituto de Matemática, Estatística e
Computação Científica

GABRIELLY DA SILVA ROMAN

**Um estudo sobre códigos perfeitos nas métricas
 l_p sob o reticulado ambiente A_n**

Campinas

2024

Gabrielly da Silva Roman

Um estudo sobre códigos perfeitos nas métricas l_p sob o reticulado ambiente A_n

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestra em Matemática Aplicada.

Orientador: João Eloir Strapasson

Este trabalho corresponde à versão final da Dissertação defendida pela aluna Gabrielly da Silva Roman e orientada pelo Prof. Dr. João Eloir Strapasson.

Campinas

2024

Ficha catalográfica
Universidade Estadual de Campinas (UNICAMP)
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

R661e Roman, Gabrielly da Silva, 1998-
Um estudo sobre códigos perfeitos nas métricas l_p sob o reticulado ambiente A_n / Gabrielly da Silva Roman. – Campinas, SP : [s.n.], 2024.

Orientador: João Eloir Strapasson.
Dissertação (mestrado) – Universidade Estadual de Campinas (UNICAMP), Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos reticulados. 2. Geometria discreta. 3. Ladrilhamento (Matemática). I. Strapasson, João Eloir, 1979-. II. Universidade Estadual de Campinas (UNICAMP). Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações Complementares

Título em outro idioma: A study of perfect codes in l_p metrics under the general ambient lattice A_n

Palavras-chave em inglês:

Lattice theory

Discrete geometry

Tiling (Mathematics)

Área de concentração: Matemática Aplicada

Titulação: Mestra em Matemática Aplicada

Banca examinadora:

João Eloir Strapasson [Orientador]

Leandro Bezerra de Lima

Eleonesio Strey

Data de defesa: 19-06-2024

Programa de Pós-Graduação: Matemática Aplicada

Identificação e informações acadêmicas do(a) aluno(a)

- ORCID do autor: <https://orcid.org/0009-0004-3303-2903>

- Currículo Lattes do autor: <https://lattes.cnpq.br/5915082972566935>

**Dissertação de Mestrado defendida em 19 de junho de 2024 e aprovada
pela banca examinadora composta pelos Profs. Drs.**

Prof(a). Dr(a). JOÃO ELOIR STRAPASSON

Prof(a). Dr(a). LEANDRO BEZERRA DE LIMA

Prof(a). Dr(a). ELEONESIO STREY

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Agradecimentos

Primeiramente, agradeço a Deus por ter me concedido saúde, força e perseverança para trilhar essa fase da minha vida.

À minha querida mãe, Marlene, deixo meus mais sinceros agradecimentos pela confiança, incentivo e amor. Essa etapa da minha vida em especial, eu encaro como a materialização de todos os seus esforços e sacrifícios. Obrigada, por me inspirar.

Em especial, agradeço ao meu namorado Maurílio Junior, pelo inabalável companheirismo durante os altos e baixos desse mestrado. Sua presença foi um verdadeiro porto seguro em Campinas, proporcionando conforto e segurança em diversos momentos. Sou imensamente grata por ter compartilhado comigo todo seu amor e cuidado, tornando minha jornada acadêmica mais leve e afetuosa.

Expresso minha sincera gratidão à minha família, em especial à minha mãe, avós e tios, dedicando um agradecimento especial à tia Anaete e aos tios Valdevino e Manoel, pelo apoio incondicional e carinho que sempre me fortaleceram.

Outro agradecimento especial é reservado para minha querida amiga e ex-colega de quarto Jessica, cuja amizade e apoio acadêmico foram imensuráveis durante esses anos. Sua amizade e parceria acadêmica fizeram e fazem toda diferença na minha vida.

Às minhas amigas Aurora, Carol, Luz e Roberta, meu muito obrigada. Compartilhar a casa e a vida cotidiana com vocês foi uma experiência única, permitindo-me apreciar a singularidade de cada uma. Sou grata por todas as risadas e bons momentos que carregarei comigo eternamente. Obrigada C6, por tudo.

Aos meus amigos de Aquidauana/MS estendo meus agradecimentos pelo apoio e confiança constantes. Todo meu carinho e gratidão por todos os amigos que tive o prazer de fazer desde minha chegada em Campinas. Vocês iluminaram meus dias com muita leveza e diversão. Sinto-me extremamente feliz e grata por ter conhecido cada pessoa que passou pela minha vida ao longo desses anos.

Expresso minha profunda gratidão ao meu orientador Prof. João Eloir Strapason, por toda paciência e conhecimentos compartilhados, que foram fundamentais para o desenvolvimento deste trabalho.

Agradeço aos professores da banca examinadora por aceitarem participar da minha banca de defesa e pelos comentários e sugestões que contribuíram para melhoria deste trabalho. Em especial, ao Prof. Leandro Bezerra por todo apoio e incentivo desde a graduação, agradeço por ter me motivado a alcançar novos patamares na minha carreira acadêmica.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001

Resumo

Códigos perfeitos apresentam o contexto mais adequado do ponto de vista de decodificação, uma vez que, sempre é possível decodificá-los garantindo a correção de algum erro. Nesse sentido, o propósito desta dissertação consiste num estudo de caso de códigos perfeitos sob o reticulado A_n . Para tal fim, foi realizada uma análise dos códigos perfeitos cujo reticulado ambiente é A_n , utilizando a métrica l_p . A título de ilustração, o foco principal foi em dimensão 2. Para entender a análise de códigos perfeitos, foram abordados os principais conceitos de reticulados que são necessários para o entendimento geral, além de uma breve introdução à teoria da informação, com ênfase na teoria dos códigos corretores de erros e foco no estabelecimento de uma conexão entre códigos e reticulados. Na sequência, foi introduzido os conceitos de ladrilhamento e de códigos perfeitos. Ao fim, o trabalho traz uma proposta de ladrilhamento do reticulado ambiente A_2 por meio de códigos perfeitos, apresentando um algoritmo que faz a busca por tais códigos perfeitos.

Palavras-chave: Código perfeito, métrica l_p , ladrilhamento.

Abstract

Perfect codes represent the most appropriate context from a decoding point of view, since it is always possible to decode them while guaranteeing the correction of any errors. In this sense, the purpose of this dissertation is a case study of perfect codes under the A_n lattice. To this end, we have analysed perfect codes whose general ambient lattice is A_n , using the l_p metric. To illustrate, the main focus was on dimension 2. In order to understand the analysis of perfect codes, the main concepts necessary for a general understanding were covered, as well as a brief introduction to information theory, with an emphasis on the theory of error-correcting codes and a focus on establishing a connection between codes and lattices. Next, the concepts of tiling and perfect codes were introduced. Finally, this dissertation proposes to tile the general A_2 lattice with perfect codes and presents an algorithm to search for such perfect codes.

Keywords: Perfect code, l_p metric, tiling.

Sumário

Introdução	11
1 Reticulados	13
1.1 Preliminares	13
1.2 Reticulados Equivalentes	19
1.3 Região Fundamental	20
1.4 Empacotamento e Cobertura	24
1.4.1 Empacotamento Esférico	24
1.4.2 Cobertura Esférica	28
1.5 Principais Reticulados Conhecidos na Literatura	30
1.5.1 Reticulado \mathbb{Z}^n	30
1.5.2 Reticulado A_n	30
1.5.3 Reticulado D_n	31
1.5.4 Reticulados E_6 , E_7 e E_8	32
1.5.5 Reticulado de Barnes-Wall Λ_{16}	33
1.5.6 Reticulado de Leech Λ_{24}	34
2 Códigos Lineares e Reticulados	37
2.1 Introdução	37
2.2 Códigos Corretores de Erros	38
2.3 Códigos q -ários	39
2.3.1 Métrica de Lee	40
2.4 Códigos e Reticulados: Construção A	41
2.5 Métrica p -Lee	42
3 Códigos Perfeitos na Métrica l_p	44
3.1 Introdução	44
3.2 Ladrilhamento	44
3.3 Códigos Perfeitos em Reticulados	47
3.4 Condição de Existência	49
4 Resultados Computacionais	52
4.1 Algoritmo	52
4.2 Resultados	56
4.2.1 Códigos Perfeitos em A_2	56
4.2.2 Códigos Perfeitos em A_3	76
4.3 Conclusões	77
4.4 Considerações Finais	79

REFERÊNCIAS	80
------------------------------	-----------

Introdução

O marco inicial da teoria da informação se deu em 1948 com o trabalho (SHANNON, 1948) publicado pelo matemático C. E. Shannon. Este estudo pioneiro introduziu a Teoria de Códigos Corretores de Erros e estabeleceu as bases teóricas que servem de suporte para o estudo de esquemas de transmissão de informação eficientes e seguros. Posteriormente, S. W. Golomb e L. R. Welch (GOLOMB; WELCH, 1970) apresentaram um dos primeiros trabalhos que investigou a existência de códigos perfeitos em \mathbb{Z}^n . Entretanto, a caracterização completa de códigos perfeitos só foi resolvida para o caso da métrica de Hamming em (LINT, 1975).

Códigos perfeitos e reticulados são campos de estudo que desempenham um papel importante na teoria da informação. Os códigos perfeitos são aqueles cujos raios das bolas centradas em palavras-código coincidem com o raio de empacotamento e preenchem todo o espaço ambiente. Já os reticulados são subgrupos aditivos discretos em \mathbb{R}^n , para determiná-los basta tomar todas as combinações lineares inteiras de vetores linearmente independentes.

Por meio da Construção A, se estabelece uma conexão entre códigos e reticulados, na qual construímos reticulados a partir de códigos corretores de erros. Nesse contexto, dado um reticulado que chamaremos de reticulado ambiente, um código é um sub-reticulado do ambiente.

Posto isso, a finalidade deste trabalho é aprofundar essa conexão entre códigos e reticulados, analisando casos de códigos perfeitos no reticulado ambiente A_n , munidos da métrica l_p . No decorrer da pesquisa, veremos a viabilidade de fazer conclusões a respeito de códigos perfeitos quando fixamos a dimensão n e variamos os valores de p .

Para alcançar tal objetivo, o trabalho segue organizado da seguinte maneira:

No [Capítulo 1](#), apresentamos alguns dos principais conceitos e propriedades para o entendimento da Teoria dos Reticulados. Exibimos, também, os principais reticulados apresentados na literatura.

No [Capítulo 2](#), abordamos de forma introdutória a Teoria dos Códigos Corretores de Erros, partindo de algumas noções iniciais. Na sequência apresentamos definições sobre códigos na métrica de Hamming, seguindo com a definição de códigos q -ários e a definição da métrica de Lee. Finalizamos o capítulo exibindo a conexão entre códigos e reticulados, por meio da Construção A e a definição da métrica p -Lee.

No [Capítulo 3](#), trabalhamos com os códigos perfeitos na métrica l_p . Apresentamos as definições básicas a respeito de ladrilhamento e de códigos perfeitos, além dos

teoremas que determinam sua existência.

O [Capítulo 4](#) é dedicado à compreensão do algoritmo e à análise dos casos de códigos perfeitos.

Finalizamos o presente trabalho apresentando as conclusões e perspectivas futuras.

As ilustrações apresentadas ao longo do texto foram geradas com o auxílio do software *Wolfram Mathematica*¹.

¹ www.wolfram.com/mathematica

1 Reticulados

1.1 Preliminares

Algébricamente, **reticulados** são subgrupos aditivos discretos em \mathbb{R}^n . Ou seja, um reticulado é qualquer subconjunto discreto $\Lambda \subset \mathbb{R}^n$ com a propriedade de que se $\mathbf{x}, \mathbf{y} \in \Lambda$ então $\mathbf{x} + \mathbf{y}$ e $-\mathbf{x}$ também pertencem a Λ .

Outra maneira de descrevermos um reticulado é como o conjunto de todas combinações lineares inteiras de vetores linearmente independentes.

Definição 1.1.1. *Seja $\{\mathbf{v}_1, \dots, \mathbf{v}_m\}$ um conjunto de vetores linearmente independentes em \mathbb{R}^n . O conjunto*

$$\Lambda = \left\{ \sum_{i=1}^m \lambda_i \mathbf{v}_i; \lambda_i \in \mathbb{Z} \right\},$$

*é chamado de **reticulado** e dizemos que $\{\mathbf{v}_1, \dots, \mathbf{v}_m\}$ é uma **base** do reticulado.*

Intuitivamente, um reticulado é um subconjunto do \mathbb{R}^n , infinito e discreto de pontos dispostos de forma regular.

Definição 1.1.2. *O número de vetores da base é chamado **posto** (ou **dimensão**) do reticulado Λ . Dizemos que um reticulado $\Lambda \subset \mathbb{R}^n$ possui **posto completo** quando o posto de Λ é igual a n .*

Exemplo 1.1.1. *Considere o reticulado gerado pela base $\{(0, 3), (1, 1)\}$, cujo posto é igual a 2 (pois, é a quantidade de vetores da base). A [Figura 1](#) ilustra alguns pontos desse reticulado.*

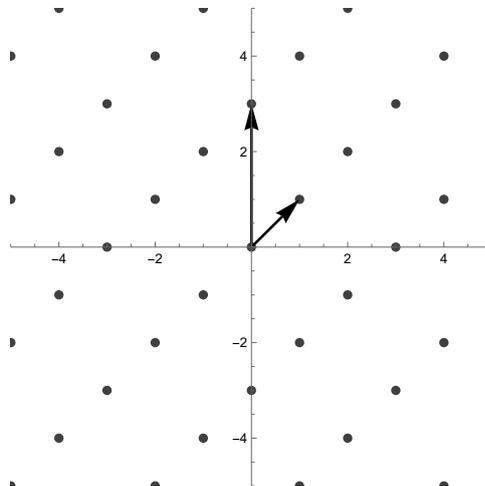


Figura 1 – Reticulado Λ gerado por $\{(0, 3), (1, 1)\}$

Definição 1.1.3. Seja $\Lambda \subset \mathbb{R}^n$ um reticulado e $\{\mathbf{v}_1, \dots, \mathbf{v}_m\}$ uma base de Λ tal que $\mathbf{v}_i = (v_{i1}, \dots, v_{in})$, para $i = 1, \dots, m$. Dizemos que a matriz

$$\mathbf{B} = \begin{pmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ v_{21} & v_{22} & \dots & v_{2n} \\ \vdots & \dots & \ddots & \vdots \\ v_{m1} & v_{m2} & \dots & v_{mn} \end{pmatrix}$$

é uma **matriz geradora** de Λ . Em outras palavras, uma matriz geradora de Λ é qualquer matriz cujas linhas formam uma base para o reticulado.

Outra maneira de representar um reticulado é utilizando a forma matricial:

$$\Lambda = \Lambda(B) = \{\mathbf{x}B; \quad \mathbf{x} \in \mathbb{Z}^m\}.$$

Exemplo 1.1.2. Considerando o [Exemplo 1.1.1](#), uma matriz geradora do reticulado em questão é dada por: $B = \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix}$.

Observação 1.1.1. Se B é uma matriz geradora para o reticulado Λ , representamos por $\text{span}(B)$ o espaço vetorial gerado pelas linhas da matriz B . Este é o menor subespaço de \mathbb{R}^n (de menor dimensão) que contém o reticulado Λ .

Definição 1.1.4. Uma matriz quadrada U com entradas inteiras é chamada **matriz unimodular** se $\det(U) = \pm 1$.

A inversa de uma matriz unimodular também é uma matriz unimodular. O produto de duas matrizes unimodulares é uma matriz unimodular. O conjunto de todas as matrizes unimodulares de ordem n munido com a multiplicação usual de matrizes é um grupo. Este grupo é denotado por $Gl_n(\mathbb{Z})$.

Um reticulado não possui uma única base, conseqüentemente, não possui uma única matriz geradora. O próximo resultado nos fornece uma condição necessária e suficiente para que duas matrizes sejam geradoras de um mesmo reticulado.

Teorema 1.1.1. B_1 e B_2 são matrizes geradoras de um reticulado Λ se, e somente se, existe uma matriz unimodular U tal que $B_2 = UB_1$.

Demonstração. (\Rightarrow) Sejam $\{\mathbf{a}_1, \dots, \mathbf{a}_m\}$ e $\{\mathbf{b}_1, \dots, \mathbf{b}_m\}$ as linhas de B_1 e B_2 respectivamente. Por hipótese B_1 e B_2 geram o mesmo reticulado, logo para $i = \{1, \dots, m\}$ existem $\mathbf{u}_i, \mathbf{v}_j \in \mathbb{Z}^m$ tal que $\mathbf{a}_i = \mathbf{v}_i B_2$ e $\mathbf{b}_j = \mathbf{u}_j B_1$. Assim temos $B_1 = VB_2$ e $B_2 = UB_1$, onde $U, V : m \times m$ são matrizes com entradas inteiras, conforme definido. Combinando as duas equações tem-se

$$B_2 = UVB_2 \Rightarrow (UV - I)B_2 = 0.$$

Note que, cada linha da matriz $X = UV - I$ representa uma equação linear de $\mathbf{b}_1, \dots, \mathbf{b}_m$ ($x_{i1}\mathbf{b}_1 + \dots + x_{im}\mathbf{b}_m = \mathbf{0}$). E como $\mathbf{b}_1, \dots, \mathbf{b}_m$ são linearmente independentes, então os coeficientes correspondentes devem ser todos 0. Portanto

$$UV - I = 0 \quad \Rightarrow \quad UV = I \quad \Rightarrow \quad \det(U) \cdot \det(V) = 1,$$

isso mais o fato de que U e V são matrizes com entradas inteiras implica que $\det(U) = \det(V) = \pm 1$, logo U e V são matrizes unimodulares. Sendo assim, existe uma matriz quadrada U com entradas inteiras e $\det(U) = \pm 1$, tal que $B_2 = UB_1$.

(\Leftarrow) Existe uma matriz unimodular U tal que $B_2 = UB_1$, logo $\mathbf{b}_i = \mathbf{u}_i B_1 \quad \forall i \in \{1, \dots, m\}$. Por outro lado, tem-se $B_1 = VB_2$, com $V = U^{-1}$ (que é uma matriz unimodular). Então para cada $j \in \{1, \dots, m\}$ temos que $\mathbf{b}_j = \mathbf{v}_j B_1$. Logo B_1 e B_2 geram o mesmo reticulado. \square

Com isso, dada uma base de um reticulado basta multiplicar à esquerda da matriz geradora por uma matriz unimodular qualquer e obter outras bases para esse mesmo reticulado. E a partir disso, temos a ideia de que reticulados podem ter bases boas e bases ruins. Uma base é considerada boa quando os vetores que a compõem tem a menor norma e são o mais perpendicular possível. Falando de maneira mais informal, podemos pegar vetores completamente diferentes e gerar o mesmo reticulado, desde que sejam cumpridas as considerações do [Teorema 1.1.1](#).

Exemplo 1.1.3. Considere o reticulado gerado por $B_1 = \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix}$ e $B_2 = \begin{pmatrix} 1 & 4 \\ 0 & -3 \end{pmatrix}$ ambas são matrizes geradoras de Λ , pois

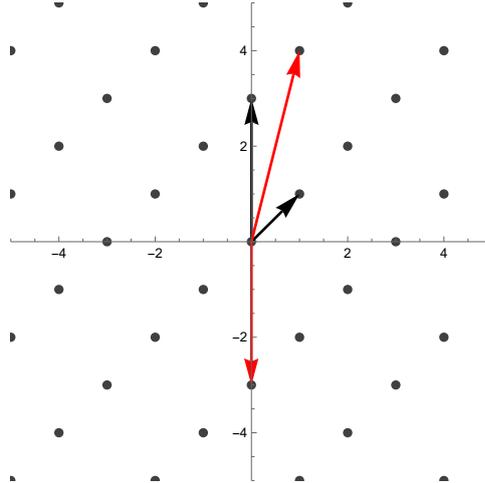
$$\begin{pmatrix} 1 & 4 \\ 0 & -3 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix},$$

isto é, $B_2 = UB_1$, onde $U = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$.

Na [Figura 2](#) podemos observar que as bases $\{(0, 3), (1, 1)\}$ e $\{(1, 4), (0, -3)\}$ geram o mesmo reticulado. Analisando a angulação entre os vetores das bases percebe-se que, a base $\{(0, 3), (1, 1)\}$ representada pelos vetores pretos é mais ortogonal quando comparada à base $\{(1, 4), (0, -3)\}$ representada pelos vetores em vermelho. Ou seja, comparando as bases apresentadas, a que mais se aproxima da ortogonalidade é a base $\{(0, 3), (1, 1)\}$.

Definição 1.1.5. A matriz $G = BB^t$ é chamada de **matriz de Gram** de Λ associada à base $\{\mathbf{v}_1, \dots, \mathbf{v}_m\}$.

Exemplo 1.1.4. Considere as matrizes $B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ e $B_2 = \begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix}$, ambas geram o mesmo reticulado. Então, de acordo com a [Definição 1.1.5](#) as matrizes de Gram associadas à B_1 e B_2 respectivamente são

Figura 2 – Bases distintas do reticulado Λ

$$G_1 = B_1 B_1^t = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

e

$$G_2 = B_2 B_2^t = \begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 10 & 13 \\ 13 & 17 \end{pmatrix}.$$

Note que, $\det(G_1) = \det(G_2) = 1$. O fato do determinante de matrizes de Gram diferentes de um mesmo reticulado serem iguais não é um caso particular do [Exemplo 1.1.4](#). Os determinantes das matrizes de Gram de um mesmo reticulado são sempre iguais, de acordo com o [Teorema 1.1.2](#). Outro fato interessante sobre a matriz de Gram é que, essa matriz é simétrica e suas entradas são produtos internos $\langle \mathbf{v}_i, \mathbf{v}_j \rangle$ (onde \mathbf{v}_k são vetores da base $k = 1, \dots, m$). Assim, as entradas da matriz de Gram guardam informações métricas importantes, pois referem-se às posições relativas dos vetores da base do reticulado.

Teorema 1.1.2. *O determinante de uma matriz de Gram de um reticulado é invariante por mudança de base.*

Demonstração. Sejam B_1 e B_2 matrizes geradoras de um mesmo reticulado Λ . Pelo [Teorema 1.1.1](#), existe uma matriz unimodular U tal que $B_2 = UB_1$. Assim, $G_2 = B_2 B_2^t = UB_1 B_1^t U^t = UG_1 U^t$.

Logo,

$$\det(G_2) = \det(UG_1 U^t) = \det(U) \cdot \det(G_1) \cdot \det(U^t) = \det(G_1).$$

A última igualdade segue pois, $\det(U) = \det(U^t) = \pm 1$. Portanto, o determinante de uma matriz de Gram independe da base escolhida. \square

Definição 1.1.6. Chamamos de **determinante de um reticulado** Λ e denotamos por $\det(\Lambda)$ o determinante de uma matriz de Gram de Λ , isto é,

$$\det(\Lambda) = \det(G).$$

A partir da matriz de Gram podemos falar também do **volume** de um reticulado, denotado por $\text{vol}(\Lambda)$ e que é dado por $\text{vol}(\Lambda) = \sqrt{\det(\Lambda)} = \sqrt{\det(BB^t)}$. Se o reticulado for de posto máximo então o volume euclidiano de Λ se reduz à $\text{vol}(\Lambda) = |\det(B)|$.

Definição 1.1.7. Dados Λ e Λ' reticulados tais que $\Lambda' \subseteq \Lambda$, Λ' é dito um **sub-reticulado** de Λ . Ou seja, um subconjunto de um reticulado é um sub-reticulado se, e somente se for um subgrupo aditivo discreto do \mathbb{R}^n .

Considere $\Lambda \subset \mathbb{R}^n$ um reticulado de posto completo com matriz geradora B . Uma maneira de obter um sub-reticulado é, considerando M uma matriz inteira $n \times n$ com $\det(M) \neq 0$, onde MB será uma matriz geradora de posto completo do sub-reticulado Λ' de Λ . Desde que $\Lambda \subset \mathbb{R}^n$ seja um reticulado de posto completo, o sub-reticulado $\Lambda' \subseteq \Lambda$ é um subgrupo de \mathbb{R}^n . Em virtude disso, Λ pode ser particionado de tal forma que $\frac{\Lambda}{\Lambda'}$ forma um grupo quociente finito (COSTA et al., 2017). Sendo assim, considere B uma matriz geradora para Λ e $B' = MB$, onde M é uma matriz inteira com determinante diferente de zero. O número de elementos de $\frac{\Lambda}{\Lambda'}$ é dado por (COSTA et al., 2017)

$$\left| \frac{\Lambda}{\Lambda'} \right| = \frac{\text{vol}(\Lambda')}{\text{vol}(\Lambda)} = | \det(M) |.$$

Exemplo 1.1.5. Sejam Λ o reticulado gerado por $B = \{(3, 1), (1, \sqrt{3}/2)\}$, $\Lambda' \subset \Lambda$ e M a matriz cujas linhas são compostas pelos vetores $\{(1, 2), (3, 0)\}$. Fazendo a multiplicação de M pela matriz geradora de Λ obtemos a matriz geradora MB do sub-reticulado $\Lambda' \subset \Lambda$. Na [Figura 3](#) os pontos pretos são os pontos de Λ , já os pontos vermelhos representam os pontos do sub-reticulado $\Lambda' \subset \Lambda$.

Definição 1.1.8. Um reticulado $\Lambda \subset \mathbb{R}^n$ é dito **ortogonal** se Λ possui uma base formada por vetores ortogonais.

Exemplo 1.1.6. O reticulado gerado pela base $B = \{(2, 1), (-1, 2)\}$ é ortogonal, pois os vetores da base são ortogonais. Veja na [Figura 4](#) a ilustração desse reticulado.

Note que, a base formada pelos vetores $\mathbf{v}_1 = (1, 3)$ e $\mathbf{v}_2 = (-1, 2)$ não é ortogonal, pois os vetores \mathbf{v}_1 e \mathbf{v}_2 não são vetores ortogonais. Então é importante salientar que, nem toda base de um reticulado ortogonal é ortogonal.

Definição 1.1.9. O **reticulado dual** do reticulado Λ é definido por:

$$\Lambda^* = \{\mathbf{x} \in \text{span}(B); \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}, \forall \mathbf{y} \in \Lambda\}.$$

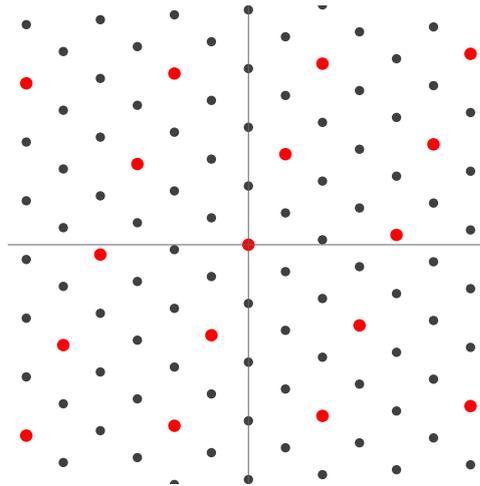


Figura 3 – Reticulado Λ e o sub-reticulado gerado por MB

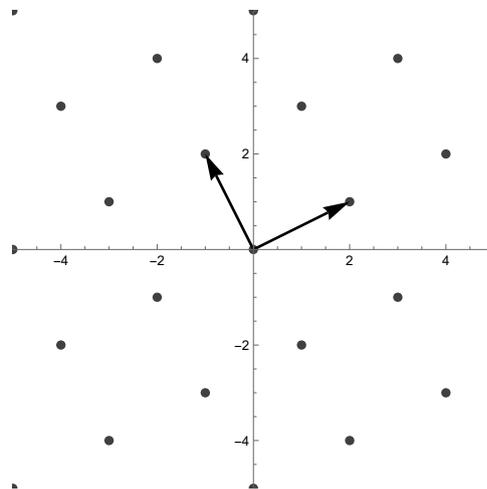


Figura 4 – Reticulado ortogonal gerado por $\{(2, 1), (-1, 2)\}$

Isto é, o dual de um reticulado $\Lambda \subset \mathbb{R}^n$ é o conjunto de todos os pontos de $\text{span}(B)$ cujo produto interno com qualquer um dos pontos de Λ é um número inteiro. Além disso, uma base do reticulado dual está associada à uma base escolhida do reticulado original.

Observação 1.1.2. *Se $\Lambda \subset \mathbb{R}^n$ for um reticulado de posto completo, o dual de Λ pode ser escrito como:*

$$\Lambda^* = \{\mathbf{x} \in \mathbb{R}^n; \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}, \forall \mathbf{y} \in \Lambda\}.$$

Proposição 1.1.1. *(CONWAY; SLOANE, 2013) Se B é uma matriz geradora para um reticulado $\Lambda \subset \mathbb{R}^n$ de posto completo, então $(B^{-1})^t$ é uma matriz geradora para o reticulado dual Λ^* .*

Definição 1.1.10. *Se $\Lambda = \Lambda^*$, dizemos que Λ é **unimodular**, e isso significa que qualquer de suas matrizes de Gram são unimodulares.*

Exemplo 1.1.7. O reticulado gerado por $\{(1, 0), (0, 1)\}$ é unimodular, pois, a matriz geradora formada por esses vetores é a matriz identidade (I) e $(I^{-1})^t = I$.

1.2 Reticulados Equivalentes

Antes de apresentar a definição de reticulado equivalente, vamos elucidar a métrica que passaremos a utilizar daqui por diante. Neste trabalho vamos considerar métricas em \mathbb{R}^n induzidas por uma norma, isto é $d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|$. A norma em questão é a **norma l_p** , $1 \leq p < \infty$, descrita da seguinte maneira:

Dados os vetores $\mathbf{x} = (x_1, \dots, x_n)$ e $\mathbf{y} = (y_1, \dots, y_n)$, $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, para cada $1 \leq p < \infty$, a **norma l_p** de um vetor $\mathbf{x} \in \mathbb{R}^n$ é definida como

$$\|\mathbf{x}\|_p = \left(\sum_{i=1}^n |x_i|^p \right)^{\frac{1}{p}},$$

e a métrica induzida pela norma é descrita como

$$d^p(\mathbf{x}, \mathbf{y}) = \left(\sum_{i=1}^n |x_i - y_i|^p \right)^{\frac{1}{p}}.$$

Quando $p = 1$, a métrica induzida pela norma l_1 é chamada de métrica da soma. E a métrica induzida pela norma l_2 é chamada de métrica euclidiana.

A **norma l_∞** de um vetor $\mathbf{x} \in \mathbb{R}^n$ é definida por

$$\|\mathbf{x}\|_\infty = \max\{|x_1|, \dots, |x_n|\}$$

e a métrica induzida pela norma é dada por

$$d^\infty(\mathbf{x}, \mathbf{y}) = \max\{|x_1 - y_1|, \dots, |x_n - y_n|\},$$

tal que $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$.

Essa métrica induzida pela norma l_∞ é conhecida como norma do máximo. Essas métricas nomeadas acima, em geral, são bastante utilizadas e ao longo do trabalho deixaremos claro qual valor de p que está sendo considerado.

Definida a métrica do nosso interesse (l_p), daremos continuidade apresentando conceitos e resultados sobre reticulados.

Dados Λ_1 e Λ_2 reticulados equivalente na métrica euclidiana, considere a definição a seguir.

Definição 1.2.1. Dois reticulados Λ_1 e Λ_2 em \mathbb{R}^n são ditos **equivalentes** se podemos obter Λ_1 por meio de Λ_2 por uma composição de rotações, reflexões e mudança de escala,

isto é, se existirem uma matriz unimodular U , uma matriz ortogonal Q e um número real positivo c tais que $B_1 = cUB_2Q$, em que B_1 e B_2 são matrizes geradoras de Λ_1 e Λ_2 , respectivamente. Dizemos que c é a **razão de semelhança** de Λ_1 para Λ_2 .

Proposição 1.2.1. (*LAVOR et al., 2006*) Dois reticulados Λ_1 e Λ_2 são equivalentes em \mathbb{R}^n com razão de semelhança $c \in \mathbb{R}_+$ se, e somente se, existem matrizes de Gram G_1 e G_2 de Λ_1 e Λ_2 , respectivamente, tais que $G_2 = c^2G_1$.

Reticulados equivalentes são idênticos quando nos referimos às propriedades relativas à métrica euclidiana. Em outras métricas, é necessário utilizar outras noções de equivalência.

Exemplo 1.2.1. Considere o reticulado gerado pela base $\{(1, 0, 0), (-1/2, \sqrt{3}/2, 0)\}$ (chamado reticulado hexagonal imerso no \mathbb{R}^3), e o reticulado com base $\{(-1, 1, 0), (0, -1, 1)\}$ (conhecido como reticulado A_2). Sejam G_1 e G_2 matrizes de Gram do reticulado hexagonal e do reticulado A_2 , respectivamente. Observe que

$$G_1 = \begin{pmatrix} 1 & 0 & 0 \\ -1/2 & \sqrt{3}/2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1/2 \\ 0 & \sqrt{3}/2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1/2 \\ -1/2 & 1 \end{pmatrix}.$$

$$G_2 = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}.$$

Como $G_1 = (\sqrt{2})^2 G_2$, pela [Proposição 1.2.1](#), o reticulado hexagonal e o reticulado A_2 são equivalentes, com razão de semelhança $\sqrt{2}$.

1.3 Região Fundamental

Regiões fundamentais associadas a um reticulado são regiões que ladrilham o $\text{span}(B)$ por meio de translações de pontos do reticulado.

Definição 1.3.1. Qualquer região $\mathcal{F} \subset \mathbb{R}^n$ é chamado **região fundamental** de um reticulado Λ de posto m se

$$\text{span}(B) = \bigcup_{\mathbf{x} \in \Lambda} (\mathbf{x} + \mathcal{F})$$

e dois ladrilhos $\mathbf{x}_1 + \mathcal{F}$ e $\mathbf{x}_2 + \mathcal{F}$, com $\mathbf{x}_1, \mathbf{x}_2 \in \Lambda$ e $\mathbf{x}_1 \neq \mathbf{x}_2$, ou não se interseptam ou se interseptam apenas nos bordos.

Caso o reticulado tenha posto completo ($m = n$) então $\text{span}(B) = \mathbb{R}^n$.

Duas importantes regiões fundamentais são o paralelotopo fundamental e a região de Voronoi.

Definição 1.3.2. *O paralelotopo fundamental é uma interpretação geométrica para o número $\text{vol}(\Lambda)$, que é definido por*

$$\mathcal{P}(B) = \{\theta_1 \mathbf{v}_1 + \dots + \theta_m \mathbf{v}_m; 0 \leq \theta_i < 1, i = 1, \dots, m\}. \quad (1.1)$$

Um paralelotopo fundamental depende da escolha da base, pois $\mathcal{P}(B)$ está contido no subespaço m -dimensional de \mathbb{R}^n gerado pelo conjunto de vetores $\mathbf{v}_1, \dots, \mathbf{v}_m$. Logo, bases diferentes determinam regiões diferentes.

Proposição 1.3.1. (*LAVOR et al., 2006*) *O paralelotopo fundamental é uma região fundamental.*

É importante saber que $\mathcal{P}(B)$ é uma região fundamental, pois

Proposição 1.3.2. (*ROGERS, 1964*) *O volume de qualquer região fundamental de um reticulado $\Lambda \subset \mathbb{R}^n$ é o mesmo.*

Definição 1.3.3. *O volume de um reticulado denotado por $\text{vol}(\Lambda)$ é dado por $\text{vol}(\Lambda) = \sqrt{\det(\Lambda)}$.*

Se o reticulado for de posto máximo então o volume euclidiano de Λ se reduz à $\text{vol}(\Lambda) = \sqrt{\det(BB^t)} = |\det(B)|$. Qualquer região fundamental de Λ tem volume $\text{vol}(\Lambda)$ como definido acima.

Exemplo 1.3.1. *Considere o reticulado Λ cuja base é $B = \{(0, 3), (1, 1)\}$. Na Figura 5 temos dois ladrilhamentos em \mathbb{R}^2 por vetores do mesmo reticulado. O primeiro com relação à base $B = \{(0, 3), (1, 1)\}$ e o segundo com relação à base $B_1 = \{(1, 4), (0, -3)\}$. Além disso,*

$$\det(B) = \begin{vmatrix} 0 & 3 \\ 1 & 1 \end{vmatrix} = -3 \quad e \quad \det(B_1) = \begin{vmatrix} 1 & 4 \\ 0 & -3 \end{vmatrix} = -3.$$

Então, $\text{vol}(\Lambda) = 3$, de acordo com a definição de volume. E com esse exemplo geométrico da Figura 5 podemos ver com clareza que bases distintas vão determinar regiões fundamentais distintas.

Podemos observar também pela imagem acima que, geometricamente, as regiões fundamentais são diferentes. Nesse caso, a primeira base é “melhor” que a segunda, pois seus vetores são mais ortogonais.

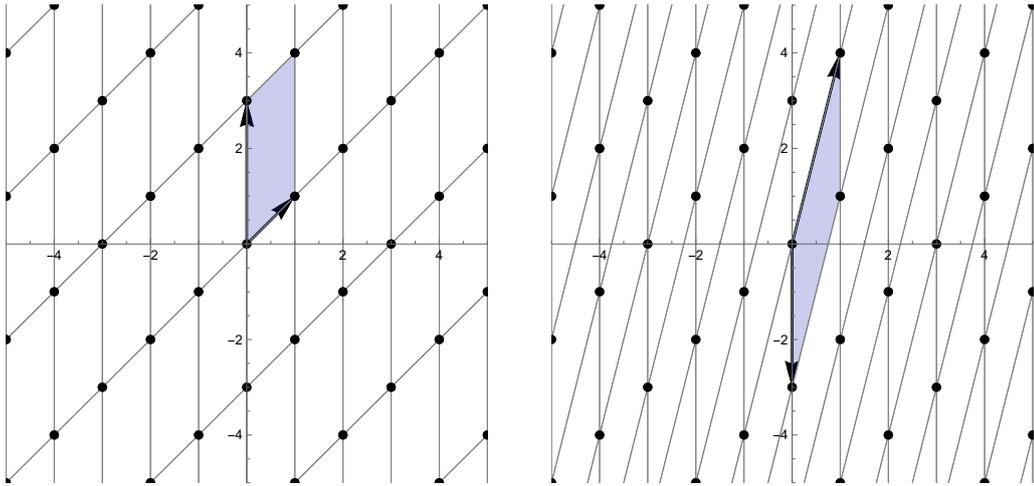


Figura 5 – Regiões fundamentais do reticulado Λ associadas às bases B e B_1 , respectivamente

A escolha por bases “melhores” levam em consideração os aspectos de ortogonalidade e de bases reduzidas. A ortogonalidade de vetores facilita nos cálculos, o que num contexto computacional é preferível. E bases reduzidas são vantajosas pelos vetores da base serem curtos e o mais próximos da ortogonalidade.

Conforme mencionado anteriormente, outra região fundamental importante é a região de Voronoi.

Definição 1.3.4. A *região de Voronoi* de um ponto $\mathbf{v} \in \Lambda$ (em relação à métrica d) é o conjunto

$$\mathcal{V}_d(\mathbf{v}) = \{\mathbf{x} \in \text{span}(B); d(\mathbf{x}, \mathbf{v}) \leq d(\mathbf{x}, \mathbf{u}), \forall \mathbf{u} \in \Lambda\}.$$

Se d é uma métrica induzida por uma norma $\|\cdot\|$ em \mathbb{R}^n , podemos reescrever a definição acima da seguinte maneira:

$$\mathcal{V}_d(\mathbf{v}) = \{\mathbf{x} \in \text{span}(B); \|\mathbf{x} - \mathbf{v}\| \leq \|\mathbf{x} - \mathbf{u}\|, \forall \mathbf{u} \in \Lambda\}.$$

Em outras palavras, podemos dizer que $\mathcal{V}_d(\mathbf{v})$ é o conjunto dos pontos do $\text{span}(B)$ que estão mais próximos de \mathbf{v} do qualquer outro ponto do reticulado (considerando a métrica d). Neste trabalho iremos considerar apenas métricas induzidas pela norma em \mathbb{R}^n .

Tendo em vista que estamos levando em consideração a métrica, vamos denotar a região de Voronoi indexando a métrica escolhida. Por exemplo, $\mathcal{V}_1(\mathbf{v})$, $\mathcal{V}_2(\mathbf{v})$ e $\mathcal{V}_\infty(\mathbf{v})$ representam respectivamente a região de Voronoi nas métricas da soma, euclidiana e do máximo. Vale salientar que nas métricas da soma e do máximo, a região de Voronoi nem sempre é uma região fundamental (veja [(STREY, 2017), p.29]).

Observação 1.3.1. Se $\Lambda \subset \mathbb{R}^n$ for um reticulado de posto completo, a região de Voronoi de $\mathbf{v} \in \Lambda$, pode ser reescrita como:

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

Após criar uma dessas regiões, é possível gerar todas as demais através de translações (LAVOR et al., 2006):

Proposição 1.3.3. Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e $\mathbf{v} \in \Lambda$. Temos que

$$\mathcal{V}_d(\mathbf{v}) = \mathbf{v} + \mathcal{V}_d(\mathbf{0})$$

Demonstração. Como a métrica d é proveniente de uma norma então $d(\mathbf{x} + \mathbf{a}, \mathbf{y} + \mathbf{a}) = d(\mathbf{x}, \mathbf{y}) \forall \mathbf{x}, \mathbf{y}, \mathbf{a} \in \mathbb{R}^n$. Para todo $\mathbf{v} \in \Lambda$, temos que

$$\begin{aligned} \mathbf{x} \in \mathcal{V}_d(\mathbf{v}) &\iff \mathbf{x} \in \text{span}(B) \text{ e } d(\mathbf{x}, \mathbf{v}) \leq d(\mathbf{x}, \mathbf{u}) \forall \mathbf{u} \in \Lambda \\ &\iff \mathbf{x} - \mathbf{v} \in \text{span}(B) \text{ e } d(\mathbf{x} + (-\mathbf{v}), \mathbf{v} + (-\mathbf{v})) \leq d(\mathbf{x} + (-\mathbf{v}), \mathbf{u} + (-\mathbf{v})) \\ &\quad \forall \mathbf{u} - \mathbf{v} \in \Lambda \\ &\iff \mathbf{x} - \mathbf{v} \in \text{span}(B) \text{ e } d(\mathbf{x} - \mathbf{v}, \mathbf{0}) \leq d(\mathbf{x} - \mathbf{v}, \mathbf{w}) \forall \mathbf{w} \in \Lambda, \text{ onde } \mathbf{w} = \mathbf{u} - \mathbf{v} \\ &\iff \mathbf{x} - \mathbf{v} \in \mathcal{V}_d(\mathbf{0}) \\ &\iff \mathbf{x} \in \mathbf{v} + \mathcal{V}_d(\mathbf{0}) \end{aligned}$$

Portanto, $\mathcal{V}_d(\mathbf{v}) = \mathbf{v} + \mathcal{V}_d(\mathbf{0})$. □

Exemplo 1.3.2. Iremos considerar novamente o reticulado $\Lambda \subset \mathbb{R}^2$, cuja base é $B = \{(0, 3), (1, 1)\}$. A Figura 6 mostra o ladrilhamento de \mathbb{R}^2 por translações de $\mathcal{V}_2(\mathbf{0})$ pelos pontos do reticulado.

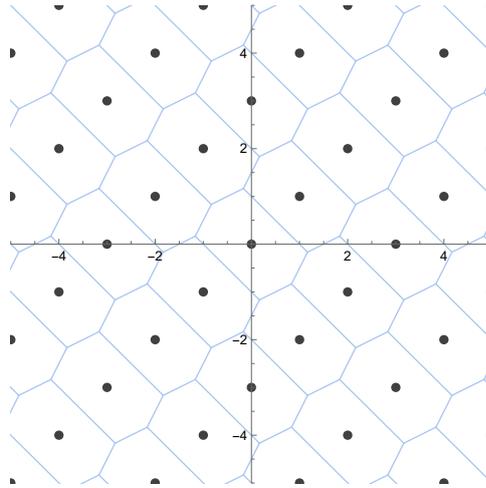


Figura 6 – Região de Voronoi de Λ utilizando a métrica euclidiana

Observe que, $\text{vol}(\mathcal{V}_2(\mathbf{0})) = \text{vol}(\Lambda) = 3$, pois $\mathcal{V}_2(\mathbf{0})$ é uma região fundamental de Λ .

Uma observação interessante a se fazer é que, o paralelotopo fundamental muda conforme a base escolhida como vimos anteriormente. Já a região de Voronoi independe da escolha da base, a região é sempre a mesma. Isso porque a própria definição do paralelotopo fundamental usa a base do reticulado como parâmetro, o que não acontece com a definição da região de Voronoi. Além disso, regiões de Voronoi de um mesmo reticulado diferindo apenas na métrica possuem o mesmo volume, desde que sejam regiões fundamentais.

1.4 Empacotamento e Cobertura

Intuitivamente, a **densidade de empacotamento** mede a proporção do espaço que foi preenchido por discos de mesmo tamanho, cujos interiores não se interceptam ou se interceptam apenas nos bordos. Para isso, sempre iremos ressaltar qual a métrica a ser utilizada.

O problema de densidade de empacotamento está intimamente ligada ao problema de empacotamento esférico, que é justamente descobrir qual a melhor maneira de distribuir os discos conforme descrito acima. Para cada dimensão procuramos o reticulado com maior densidade de empacotamento, isto é, fixada uma dimensão, queremos o reticulado cujas bolas centradas nos pontos do reticulado cubram o espaço da melhor maneira possível. No melhor dos casos, o empacotamento perfeito é aquele em que o espaço é totalmente ocupado.

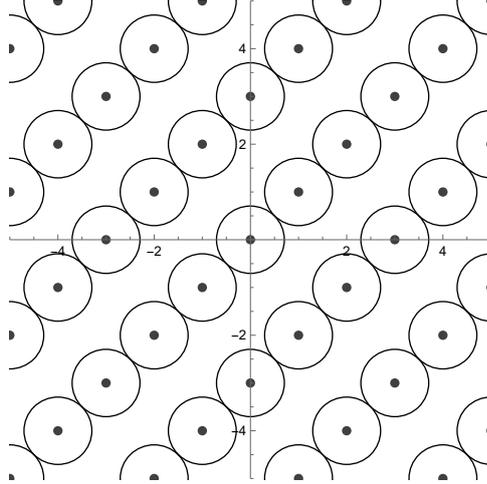
Um conceito “dual” ao do empacotamento esférico é o de cobertura esférica. O problema de cobertura esférica consiste em, dado um reticulado, obter o menor raio possível de tal forma que todo o \mathbb{R}^n seja coberto pelas esferas de mesmo raio centradas nos pontos do reticulado. Assim, queremos obter reticulados com a menor densidade de cobertura em cada dimensão.

1.4.1 Empacotamento Esférico

Definição 1.4.1. *Sejam d uma métrica em \mathbb{R}^n e V um subespaço vetorial de \mathbb{R}^n . Um **empacotamento esférico** em V é uma coleção de bolas, todas de mesmo raio, de modo que quaisquer duas bolas ou não se interceptem ou se interceptem apenas no bordo. Um **empacotamento reticulado** é um empacotamento esférico tal que o conjunto dos centros das bolas forma um reticulado $\Lambda \subset \mathbb{R}^n$ em $V = \text{span}(B)$.*

Exemplo 1.4.1. *A Figura 7 ilustra o empacotamento, em relação à métrica euclidiana, do reticulado Λ gerado pela base $B = \{(0, 3), (1, 1)\}$.*

A seguir, apresentaremos um resultado que assegura a existência do empacotamento reticulado.

Figura 7 – Empacotamento do reticulado Λ

Teorema 1.4.1. *Se Λ é um reticulado em \mathbb{R}^n , então existe $r > 0$ tal que $B(\mathbf{x}, r) \cap \Lambda = \{\mathbf{x}\}$ para todo $\mathbf{x} \in \Lambda$.*

Demonstração. Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. Como Λ é um subgrupo aditivo e discreto de \mathbb{R}^n , temos que $\mathbf{0} \in \Lambda$ e existe $r > 0$ tal que $B(\mathbf{0}, r) \cap \Lambda = \{\mathbf{0}\}$. Deste modo, para cada $\mathbf{x} \in \Lambda$ tem-se:

$$\begin{aligned} \mathbf{y} \in B(\mathbf{x}, r) \cap \Lambda &\iff (\mathbf{x} - \mathbf{y}) \in B(\mathbf{0}, r) \cap \Lambda \\ &\iff \mathbf{x} - \mathbf{y} = \mathbf{0} \\ &\iff \mathbf{x} = \mathbf{y} \end{aligned}$$

Ou seja, $B(\mathbf{x}, r) \cap \Lambda = \{\mathbf{x}\}$ para todo $\mathbf{x} \in \Lambda$. □

Se $\mathcal{V}_d(\mathbf{v})$ for uma região fundamental, uma abordagem simplificada para interpretar a densidade de empacotamento de um reticulado consiste em comparar o volume da região de Voronoi $\mathcal{V}_d(\mathbf{v})$ de um ponto $\mathbf{v} \in \Lambda$ com o volume da maior bola centrada em \mathbf{v} inscrita em $\mathcal{V}_d(\mathbf{v})$.

Definição 1.4.2. *Chamamos de **raio de empacotamento** de um reticulado Λ o valor:*

$$\rho = \max\{r; B_d[\mathbf{0}, r] \subset \mathcal{V}_d(\mathbf{0})\},$$

onde $B_d[\mathbf{0}, r]$ denota a bola fechada na métrica d de centro $\mathbf{0}$ e raio r .

Exemplo 1.4.2. *Seguindo com o mesmo reticulado do exemplo anterior (Exemplo 1.4.1), veja na Figura 8 a representação gráfica da maior bola euclidiana possível inscrita na região de Voronoi $\mathcal{V}_2(\mathbf{0})$.*

Do fato de que um reticulado é um subgrupo aditivo discreto de \mathbb{R}^n , podemos garantir a existência de um vetor de norma mínima (COSTA et al., 2017). E com isso, relacionamos o conceito de norma mínima com o raio de empacotamento de um reticulado.

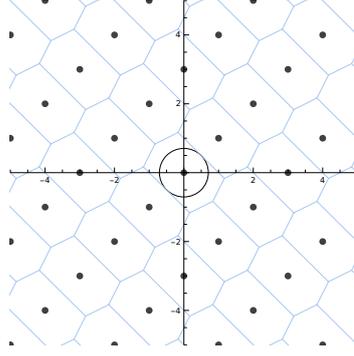


Figura 8 – Região de Voronoi de Λ e seu empacotamento associado

Definição 1.4.3. *Seja d uma métrica em \mathbb{R}^n . A **norma mínima** λ de um reticulado $\Lambda \subset \mathbb{R}^n$ é definida por*

$$\lambda = \min\{d(\mathbf{x}, 0); \mathbf{x} \in \Lambda, \mathbf{x} \neq 0\}.$$

Os vetores de Λ que satisfazem a norma mínima são chamados **vetores de norma mínima**.

Proposição 1.4.1. *(NAVES, 2009) Sejam d uma métrica em \mathbb{R}^n e $\Lambda \subset \mathbb{R}^n$. O **raio de empacotamento** de Λ é dado por*

$$\rho = \frac{\lambda}{2},$$

onde λ é a norma mínima do reticulado Λ .

Demonstração. Tome $\mathbf{u}, \mathbf{v} \in \Lambda$ e $r = \frac{\lambda}{2}$. Suponha que $\mathbf{x} \in B_d(\mathbf{u}, r) \cap B_d(\mathbf{v}, r)$, com \mathbf{x} qualquer em \mathbb{R}^n . Sabemos que $d(\mathbf{u}, \mathbf{x}) + d(\mathbf{x}, \mathbf{v}) \geq d(\mathbf{u}, \mathbf{v}) = d(\mathbf{u} - \mathbf{v}, 0) \geq \lambda$ e que $d(\mathbf{u}, \mathbf{x}) + d(\mathbf{x}, \mathbf{v}) < \frac{\lambda}{2} + \frac{\lambda}{2} = \lambda$, o que é contradição. Logo, $B_d(\mathbf{u}, r) \cap B_d(\mathbf{v}, r) = \emptyset$. Agora basta provar que $r = \frac{\lambda}{2}$ é o maior raio possível para o empacotamento reticulado. Se $r > \frac{\lambda}{2}$, considere $\mathbf{u} \in \Lambda$ tal que $d(\mathbf{u}, 0) = \lambda$, então $\mathbf{w} = \frac{\mathbf{u}}{2} \in \mathbb{R}^n$ temos $d(\mathbf{w}, \mathbf{u}) = d(\mathbf{w}, \mathbf{0}) = \frac{\lambda}{2} < r$, o que nos leva a outra contradição, pois teríamos que $\mathbf{w} \in B_d(\mathbf{u}, r) \cap B_d(\mathbf{0}, r) = \emptyset$. Portanto $r = \frac{\lambda}{2} = \rho$. \square

Entretanto, a determinação do vetor de norma mínima em um reticulado nem sempre é trivial. O problema de encontrar λ é conhecido como o problema do vetor mais curto (SVP - Shortest Vector Problem). Trata-se de um desafio computacional complexo, classificado como NP-difícil (MICCIANCIO; GOLDWASSER, 2002). Na métrica euclidiana, conjectura-se que não existe um algoritmo de tempo polinomial capaz de resolver esse problema (MICCIANCIO; GOLDWASSER, 2002).

Dado um empacotamento em \mathbb{R}^n associado a um reticulado Λ , dizemos que um empacotamento é considerado bom quando a proporção do espaço ocupado pelas

bolas de empacotamento se aproxima ao máximo do $\text{span}(B)$ (onde B é uma base de Λ). Formalmente, essa proporção é expressa pela densidade de empacotamento.

Definição 1.4.4. Definimos a **densidade de empacotamento** de um reticulado Λ de posto m com relação a métrica d como:

$$\Delta_d(\Lambda) = \frac{\text{volume euclidiano } m\text{-dimensional de uma esfera de raio } \rho}{\text{volume euclidiano } m\text{-dimensional de uma região fundamental de } \Lambda},$$

ou seja,

$$\Delta_d(\Lambda) = \frac{\text{vol}_m(B_d[\mathbf{0}, \rho])}{\text{vol}(\Lambda)} = \frac{\text{vol}_m(B_d[\mathbf{0}, 1])\rho^m}{\sqrt{\det(\Lambda)}} = \frac{V_{m_d}\rho^m}{\sqrt{\det(\Lambda)}}.$$

Onde V_{m_d} é o volume da bola unitária. Na métrica euclidiana, o volume da bola unitária m -dimensional é dado em (CONWAY; SLOANE, 2013) por:

$$V_{m_2} = \begin{cases} \frac{\pi^{m/2}}{\left(\frac{m}{2}\right)!}, & \text{se } m \text{ é par} \\ \frac{2^m \pi^{(m-1)/2} ((m-1)/2)!}{m!}, & \text{se } m \text{ é ímpar.} \end{cases} \quad (1.2)$$

Considerando a métrica da soma, temos que o volume da bola unitária em \mathbb{R}^m é dada em (RUSH; SLOANE, 1987) por:

$$V_{m_1} = \frac{2^m}{m!}. \quad (1.3)$$

Perceba que fixando uma dimensão, o volume da bola unitária m -dimensional é conhecido. Portanto, o problema de empacotamento se reduz ao estudo de um outro parâmetro, conhecido como densidade de centro.

Definição 1.4.5. A **densidade de centro** de um reticulado Λ em relação a métrica d é o número

$$\delta_d = \frac{\rho^n}{\sqrt{\det(\Lambda)}}.$$

A densidade de centro fornece uma maneira de comparar reticulados de mesma dimensão.

Exemplo 1.4.3. Já sabemos que um dos problemas de empacotamento esférico de um reticulado, ao fixarmos uma dimensão e uma métrica, consiste em encontrar o reticulado com a maior densidade possível. Em dimensão um utilizando a métrica euclidiana, os pontos de coordenadas inteiras da reta formam o reticulado \mathbb{Z} , cuja densidade de empacotamento é $\Delta_2 = 1$. Os intervalos são as “bolas” de empacotamento, como mostra a [Figura 9](#) (o intervalo é representado pelo segmento de reta destacado em preto).

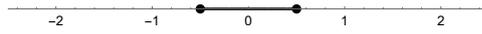
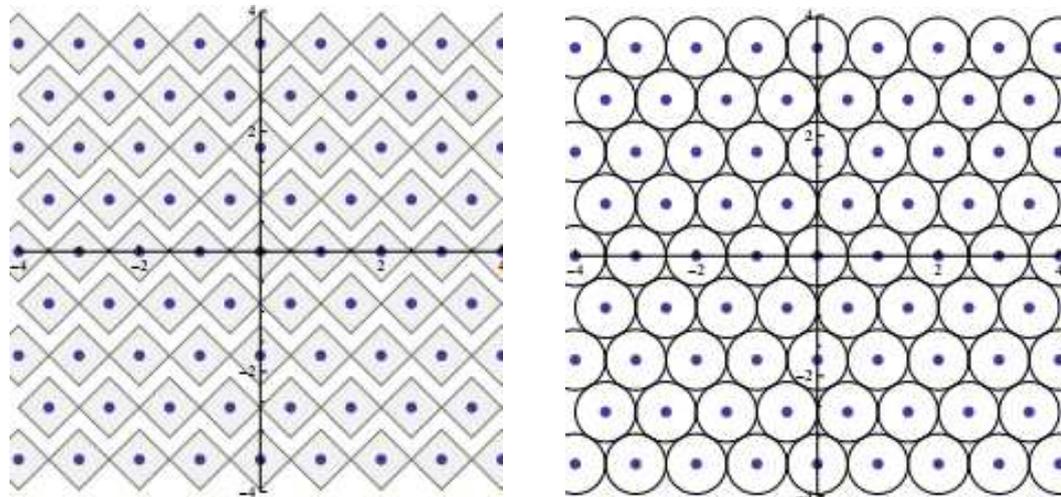


Figura 9 – Empacotamento do reticulado \mathbb{Z}

Exemplo 1.4.4. Em dimensão dois o reticulado hexagonal gerado por $\{(1, 0), (1/2, \sqrt{3}/2)\}$, tem as seguintes densidades considerando a métrica da soma e a métrica euclidiana ($\rho = \frac{1}{2}$):

$$\Delta_1(\Lambda) = \frac{1/4}{\sqrt{3}/2} \simeq 0,5773 \text{ e } \Delta_2(\Lambda) = \frac{\pi/4}{\sqrt{3}/2} \simeq 0,9069.$$

Este é o reticulado mais denso em \mathbb{R}^2 com a métrica euclidiana (CONWAY; SLOANE, 2013). Na Figura 10 temos o empacotamento do reticulado hexagonal com duas métricas diferentes.



(a) Métrica da soma

(b) Métrica euclidiana

Figura 10 – Fonte: [(JORGE,), p. 20]

Exemplo 1.4.5. Já em dimensão três, Gauss mostrou em 1831 que o reticulado FCC (Face-Centered Cubic) é o reticulado com maior densidade nessa dimensão (CONWAY; SLOANE, 2013). Uma base para o reticulado FCC é $\{(2, 0, 0), (1, 1, 0), (1, 0, 1)\}$, e temos que $\det(B) = 2$, $\lambda = \sqrt{2}$ e $\rho = \frac{\sqrt{2}}{2}$. Logo $\Delta_2 = \frac{\sqrt{2}\pi}{6} \simeq 0,7405$. Veja a Figura 11:

1.4.2 Cobertura Esférica

Como dito no início dessa sessão, a densidade de cobertura esférica é um conceito “dual” à da densidade de empacotamento e nele procuramos o menor raio possível de esferas de mesmo raio que cubram todo o $\text{span}(\Lambda)$. Ou seja, agora o objetivo é minimizar a área das regiões sobrepostas dada uma dimensão.

Definição 1.4.6. Dados um reticulado Λ , uma métrica d em \mathbb{R}^n e $V = \text{span}(\Lambda)$, o conjunto $\Lambda + B_d[\mathbf{0}, r]$ é dito uma **cobertura** de V se $V \subseteq (\Lambda + B_d[\mathbf{0}, r])$.

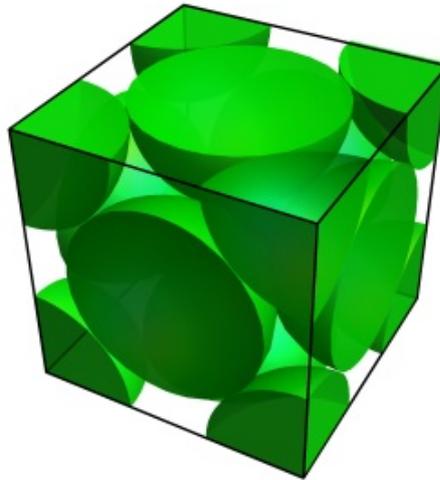


Figura 11 – Fonte: [(COSTA et al., 2017), p. 14]

Definição 1.4.7. *Sejam $\Lambda \subset \mathbb{R}^n$, $V = \text{span}(\Lambda)$ e d uma métrica. Definimos o **raio de cobertura** como*

$$\mu = \min\{r; V \subseteq \Lambda + B_d[\mathbf{0}, r]\}.$$

Exemplo 1.4.6. *Considere o reticulado Λ gerado por $B = \{(0, 3), (1, 1)\}$. A Figura 12 mostra a cobertura de \mathbb{R}^2 desse reticulado com respeito a métrica euclidiana.*

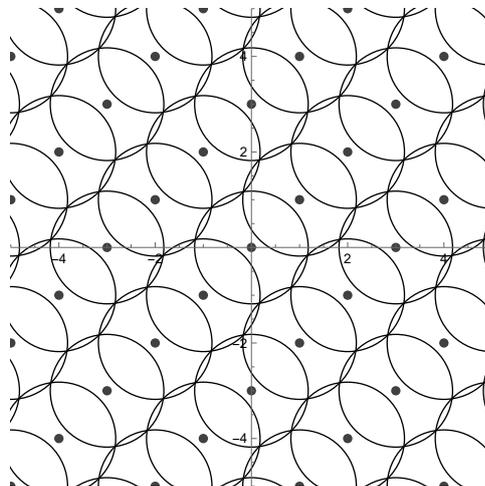


Figura 12 – Cobertura do reticulado Λ

Definição 1.4.8. *A **densidade de cobertura** é dada por*

$$\Theta_d(\Lambda) = \frac{\text{vol}(B_d[\mathbf{0}, \mu])}{\text{vol}(\Lambda)} = \frac{V_{m_d} \mu^m}{\sqrt{\det(\Lambda)}}.$$

Perceba que, dado um reticulado em \mathbb{R}^n , a densidade de empacotamento $\Delta_d(\Lambda)$ é um número menor ou igual a 1, já a densidade de cobertura $\Theta_d(\Lambda)$ é sempre maior ou igual a 1. Isto é,

$$0 < \Delta_d(\Lambda) \leq 1 \leq \Theta_d(\Lambda).$$

1.5 Principais Reticulados Conhecidos na Literatura

Reticulados importantes são reticulados que possuem estruturas especiais. E geralmente são facilmente encontrados na literatura. Serão expostos alguns dos parâmetros de reticulados que vimos até o momento, como: paralelotopo fundamental, volume, região de Voronoi, bola de raio 1 centrada na origem, norma mínima, raio de empacotamento, densidade de empacotamento, centro de densidade, raio de cobertura e densidade de cobertura. As referências utilizadas nessa sessão foram (CONWAY; SLOANE, 2013) e (COSTA et al., 2017).

1.5.1 Reticulado \mathbb{Z}^n

O reticulado cúbico \mathbb{Z}^n é definido como

$$\mathbb{Z}^n = \{(x_1, \dots, x_n); x_i \in \mathbb{Z}, i = 1, \dots, n\}.$$

No Exemplo 1.4.3 temos o reticulado \mathbb{Z} , conforme a definição acima. Esse tipo de reticulado é unimodular de ordem n , e uma matriz geradora simples é a matriz identidade de ordem n . A Tabela 1 apresenta algumas características importantes sobre esse reticulado na métrica euclidiana, que facilitam trabalhar com o mesmo.

Tabela 1 – Características do reticulado \mathbb{Z}^n

Determinante de \mathbb{Z}^n	$\det = 1$
Norma mínima	$\lambda = 1$
Raio de empacotamento	$\rho = 1/2$
Densidade de empacotamento	$\Delta(\mathbb{Z}^n) = V_n 2^{-n}$
Densidade de centro	$\delta(\mathbb{Z}^n) = 2^{-n}$
Raio de cobertura	$\mu = \sqrt{n}/2$
Densidade de cobertura	$\Theta(\mathbb{Z}^n) = n^{n/2} V_n 2^{-n}$

Fontes: [(COSTA et al., 2017), p. 21] e [(CONWAY; SLOANE, 2013), p. 106]

1.5.2 Reticulado A_n

Para $n \geq 1$, o reticulado A_n é definido como

$$A_n = \left\{ (x_0, x_1, \dots, x_n) \in \mathbb{Z}^{n+1}; \sum_{i=0}^n x_i = 0 \right\}.$$

A fim de ilustrar, no Exemplo 1.2.1 temos o reticulado hexagonal que é equivalente ao reticulado A_2 , considerando as respectivas métricas. No entanto, uma base possível que gera o reticulado A_2 é $B = \{(-1, 1, 0), (-1, 0, 1)\}$.

De modo geral, A_n é um reticulado localizado no hiperplano de \mathbb{R}^{n+1} , onde a soma das coordenadas é igual a zero. E sua matriz geradora tem mais colunas que linhas ($n \times (n + 1)$). Nesse sentido, uma possível matriz para esse reticulado é:

$$B = \begin{pmatrix} -1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & -1 & 1 \end{pmatrix}.$$

A [Tabela 2](#) mostra algumas características do reticulado A_n considerando a métrica euclidiana.

Tabela 2 – Características do reticulado A_n

Volume de A_n	$vol(A_n) = n + 1$
Norma mínima	$\lambda = \sqrt{2}$
Raio de empacotamento	$\rho = 1/\sqrt{2}$
Densidade de centro	$\delta(A^n) = 2^{-n/2}(n + 1)^{-1/2}$
Raio de cobertura	$\mu = \rho(2a(n + 1 - a)/(n + 1))^{1/2}$, $a = \lfloor (n + 1)/2 \rfloor$

Fontes: [([COSTA et al., 2017](#)), p. 22] e [([CONWAY; SLOANE, 2013](#)), p. 109]

1.5.3 Reticulado D_n

Com $n \geq 3$, definimos o reticulado D_n como

$$D_n = \left\{ (x_1, \dots, x_n) \in \mathbb{Z}^n; \sum_{i=1}^n x_i \text{ é par} \right\}.$$

Ou seja, esse é um reticulado em \mathbb{R}^n cujos vetores da base possuem entradas inteiras e a soma das coordenadas de cada vetor da base é par. Uma base possível para esse reticulado é representada pela matriz B :

$$B = \begin{pmatrix} -1 & -1 & 0 & \dots & 0 & 0 & 0 \\ 1 & -1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & -1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & -1 \end{pmatrix}.$$

Na [Tabela 3](#) temos algumas das características do reticulado D_n considerando a métrica euclidiana.

Tabela 3 – Características do reticulado D_n

Volume de D_n	$vol(D_n) = 4$
Norma mínima	$\lambda = \sqrt{2}$
Raio de empacotamento	$\rho = 1/\sqrt{2}$
Densidade de centro	$\delta(D_n) = 2^{-(n+2)/2}$
Raio de cobertura	$\mu = 1$ ($n = 3$) ou $\mu = \sqrt{n/4}$ ($n \geq 4$)

Fontes: [([COSTA et al., 2017](#)), p. 22] e [([CONWAY; SLOANE, 2013](#)), p. 117]

1.5.4 Reticulados E_6 , E_7 e E_8

O reticulado E_8 também é conhecido como reticulado de Gosset em homenagem a T. Gosser, que foi um dos primeiros a estudar sua geometria. Esse reticulado é definido em ([COSTA et al., 2017](#)) como

$$E_8 = \left\{ \mathbf{x} = (x_1, \dots, x_8) \in \mathbb{Z}^8; \mathbf{x} \in D_8 \text{ ou } \mathbf{x} + \left(\frac{1}{2}, \dots, \frac{1}{2} \right) \in D_8 \right\}.$$

Uma matriz geradora é

$$B = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 \end{pmatrix}.$$

E_8 tem a maior densidade de empacotamento na dimensão 8, não apenas entre reticulados, mas para qualquer empacotamento. Possui também a menor densidade de cobertura conhecida nesta dimensão ([COSTA et al., 2017](#)). Na [Tabela 4](#) podemos ver algumas características desse reticulado.

Os reticulados E_7 e E_6 são definidos por meio do reticulado E_8 da seguinte maneira:

$$E_7 = \{ \mathbf{x} = (x_1, \dots, x_8) \in E_8; x_1 = x_2 \} \text{ e}$$

$$E_6 = \{\mathbf{x} = (x_1, \dots, x_8) \in E_8; x_1 = x_2 = x_3\}.$$

Ambos são reticulados de posto 7 e 6 respectivamente definidos em \mathbb{R}^8 , e uma possível maneira de apresentar suas matrizes geradoras são

$$B_{E_7} = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & -1/2 & -1/2 & -1/2 & -1/2 \end{pmatrix} e$$

$$B_{E_6} = \begin{pmatrix} 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & -1/2 & -1/2 & -1/2 & -1/2 \end{pmatrix}.$$

E_7 é o reticulado mais denso em dimensão 7, assim como E_6 é o mais denso em dimensão 6 (COSTA et al., 2017). Na Tabela 4 temos mais algumas características importantes sobre os reticulados obordados nessa subseção com relação à métrica euclidiana.

Tabela 4 – Características dos reticulados: E_6 , E_7 e E_8

	E_6	E_7	E_8
Norma mínima (λ)	$\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$
Raio de empacotamento (ρ)	$1/\sqrt{2}$	$1/\sqrt{2}$	$1/\sqrt{2}$
Densidade de empacotamento (Δ)	0,3729	0,2953	0,2537
Densidade de centro (δ)	$1/8\sqrt{3}$	1/16	1/16
Raio de cobertura (μ)	$2/\sqrt{3}$	$\sqrt{3}/2$	1

Fontes: [(COSTA et al., 2017), p. 23] e [(CONWAY; SLOANE, 2013), p. 128]

1.5.5 Reticulado de Barnes-Wall Λ_{16}

Os chamados reticulados Barnes-Wall BW_n são definidos nas dimensões $n = 2^k$, k um número inteiro maior que dois. Λ_{16} tem a melhor densidade de empacotamento na dimensão 16. Uma matriz geradora possível é dada por $B_{\Lambda_{16}}$.

$$B_{\Lambda_{16}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Apresentamos na [Tabela 5](#) algumas características desse reticulado considerando a métrica euclidiana.

Tabela 5 – Características do reticulado Λ_{16}

Norma mínima	$\lambda = 4$
Raio de empacotamento	$\rho = 1$
Densidade de empacotamento	$\delta(\Lambda_{16}) = \pi^8/16 \cdot 8! = 0.01471\dots$
Densidade de centro	$\delta(\Lambda_{16}) = 1/16$
Raio de cobertura	$\mu = \rho\sqrt{3}$

Fontes: [([COSTA et al., 2017](#)), p. 23] e [([CONWAY; SLOANE, 2013](#)), p. 129]

1.5.6 Reticulado de Leech Λ_{24}

O reticulado Λ_{24} , foi introduzido por J. Leech em 1964. Em dimensão 24 ele possui a melhor densidade de empacotamento em relação aos demais reticulados. Uma possível matriz geradora para esse reticulado é dada por

Tabela 7 – Empacotamentos reticulados mais densos

Dimensão	1	2	3	4	5	6	7	8	16	24
Reticulado	\mathbb{Z}	A_2	$A_3 \sim D_3$	D_4	D_5	E_6	E_7	E_8	Λ_{16}	Λ_{24}

Tabela 8 – Reticulados com menor densidade de cobertura

Dimensão	1	2	3	4	5	16	24
Reticulado	\mathbb{Z}	A_2	$A_3^* \sim D_3^*$	A_4^*	A_5^*	A_{16}^*	Λ_{24}

2 Códigos Lineares e Reticulados

Neste capítulo, apresentamos uma breve introdução a teoria da informação, com ênfase na teoria dos códigos corretores de erros. O objetivo central do capítulo é estabelecer uma conexão entre códigos e reticulados. Para alcançar tal objetivo, iremos explicar o processo de construção de reticulados a partir de códigos lineares utilizando a Construção A.

Todos os resultados aqui apresentados foram baseados, em sua maioria, nas leituras de (COSTA et al., 2014), (LAVOR et al., 2006), (HEFEZ; VILLELA, 2008), (COSTA et al., 2017) e (MACWILLIAMS; SLOANE, 1977).

2.1 Introdução

Os códigos corretores de erros são muito utilizados quando se deseja transmitir ou armazenar dados permitindo detectar e corrigir certos tipos de erros, garantindo a confiabilidade. Tais códigos têm grande uso em comunicações via satélites, transmissão de dados entre computadores, em armazenamento de dados, transmissão de vídeo e áudio, entre outros.

Em suma, um código corretor de erro é uma maneira organizada de acrescentar algum dado adicional à cada informação que precisa ser transmitida ou armazenada, de modo que permita, ao recuperar a informação, detectar e corrigir os erros cometidos no processo de transmissão da informação (TSUCHIYA, 2012).

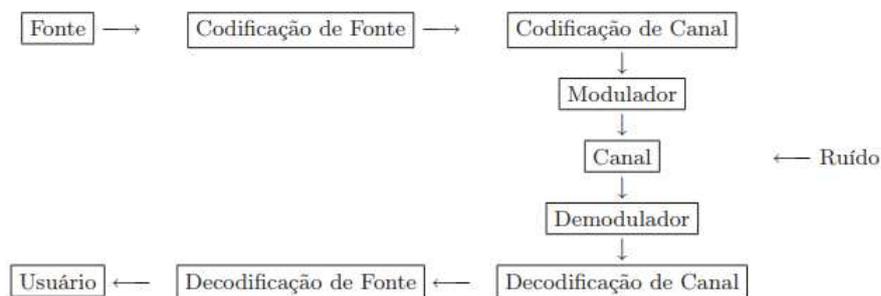


Figura 13 – Fonte: [(LAVOR et al., 2006), p. 10]

A teoria de códigos corretores de erros teve o marco inicial em 1948 no trabalho “A Mathematical Theory of Communications” (SHANNON, 1948) publicado pelo matemático C. E. Shannon, do Laboratório Bell, E.U.A.. De acordo com (HEFEZ; VILLELA, 2008), apenas na década de 70, com as pesquisas espaciais e a popularização dos

computadores que essa teoria começou chamar atenção de outros pesquisadores além dos matemáticos.

2.2 Códigos Corretores de Erros

Seja A um conjunto finito chamado **alfabeto**. O número de elementos de A , denotado por $|A|$, é q . Cada elemento do código é chamado de palavra-código.

Definição 2.2.1. *Um código corretor de erros é um subconjunto próprio qualquer de A^n , para algum número natural n .*

Definição 2.2.2. *Dados dois elementos $\mathbf{x}, \mathbf{y} \in A^n$, a distância de Hamming entre \mathbf{x} e \mathbf{y} é definida como*

$$d_H = |\{i; x_i \neq y_i, 1 \leq i \leq n\}|.$$

Se todas as palavras-código são equiprováveis, podemos decodificá-las com o **princípio da máxima verossimilhança**. Ou seja, se no receptor chegar uma palavra com erro, vamos decodificá-la pela palavra mais “próxima” desta e para isso utilizamos a função distância d_H definida em A^n .

É fácil ver que essa função distância satisfaz todas as propriedades de métrica, por isso ela também é conhecida como **métrica de Hamming**.

Exemplo 2.2.1. *Em \mathbb{Z}_2^4 temos*

$$d_H(1110, 1001) = 3 \quad e$$

$$d_H(1111, 0110) = 2.$$

Definição 2.2.3. *Dados um elemento $\mathbf{a} \in A^n$ e um número real $r > 0$, definimos a **esfera** e a **bola** de centro em \mathbf{a} e raio r como sendo, respectivamente os conjuntos*

$$S(\mathbf{a}, r) = \{\mathbf{x} \in A^n; d_H(\mathbf{x}, \mathbf{a}) = r\},$$

$$B(\mathbf{a}, r) = \{\mathbf{x} \in A^n; d_H(\mathbf{x}, \mathbf{a}) \leq r\}.$$

Definição 2.2.4. *Sejam $C \subset A^n$ um código e d uma métrica. A **distância mínima** de C na métrica d é o número*

$$d(C) = \min \{d(\mathbf{x}, \mathbf{y}); \mathbf{x}, \mathbf{y} \in C \text{ e } \mathbf{x} \neq \mathbf{y}\}.$$

Exemplo 2.2.2. *Considerando o código $C = \{(0000), (1001), (1110), (1111)\}$ em \mathbb{Z}_2^4 e a métrica de Hamming, temos que $d(C) = 1$, e essa distância mínima acontece entre as palavras (1110) e (1111) de C .*

Lema 2.2.1. (TSUCHIYA, 2012) *Seja C um código com distância mínima λ em uma métrica d e $k = \left\lfloor \frac{\lambda - 1}{2} \right\rfloor$. Se \mathbf{c} e \mathbf{c}' são palavras distintas de C , então*

$$B(\mathbf{c}, k) \cap B(\mathbf{c}', k) = \emptyset,$$

onde $B(\mathbf{a}, r) = \{\mathbf{x} \in A^n; d(\mathbf{x}, \mathbf{a}) \leq r\}$.

Teorema 2.2.1. (HEFEZ; VILLELA, 2008) *Seja C um código com distância mínima λ . Então C pode corrigir até $k = \left\lfloor \frac{\lambda - 1}{2} \right\rfloor$ erros e detectar até $\lambda - 1$ erros.*

O teorema acima mostra a importância da distância mínima de um código para detecção e correção de erros. Quanto maior for a distância mínima de um código, mais robusto ele é contra erros. Então quanto maior for a capacidade de detecção e correção de erros mais o código pode lidar com falhas de transmissão e/ou armazenamento de dados.

Observação 2.2.1. *Outra maneira de interpretar o Teorema 2.2.1 é geometricamente, visualizando a capacidade de correção como o maior raio $r \in \mathbb{N}$ em que as bolas centradas nas palavras do código não se sobrepõem, isto é, o maior $r \in \mathbb{N}$ tal que $B(\mathbf{c}, r) \cap B(\mathbf{c}', r) = \emptyset$ para quaisquer $\mathbf{c}, \mathbf{c}' \in C$ distintos. Em outras palavras, r é raio de empacotamento do código C (FIRER et al., 2018) e denotamos por $r(C)$. Logo:*

$$r(C) = \max\{r \in \mathbb{N}; B(\mathbf{c}, r) \cap B(\mathbf{c}', r) = \emptyset, \forall \mathbf{c}, \mathbf{c}' \in C, \mathbf{c} \neq \mathbf{c}'\}.$$

Proposição 2.2.1. (FIRER et al., 2018) *Seja d uma métrica em \mathbb{Z}_q^n . Dado um código C , o raio de empacotamento $r(C)$ satisfaz as desigualdades*

$$\left\lfloor \frac{d - 1}{2} \right\rfloor \leq r(C) < d.$$

Definição 2.2.5. *Seja $C \subset A^n$ um código com distância mínima d e seja $k = \left\lfloor \frac{d - 1}{2} \right\rfloor$. O código C será dito **perfeito** se*

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

2.3 Códigos q -ários

Sejam q um inteiro positivo, \mathbb{Z}_q o anel de inteiros módulo q e \mathbb{Z}_q^n o conjunto formado por todas n -uplas sobre \mathbb{Z}_q , ou seja,

$$\mathbb{Z}_q^n = \{(x_1, \dots, x_n); x_i \in \mathbb{Z}_q, \forall i \in \{1, \dots, n\}\}.$$

Definição 2.3.1. *Um código linear q -ário C é um subgrupo aditivo de \mathbb{Z}_q^n .*

Se q for um número primo, então um código linear C é um subespaço vetorial de \mathbb{Z}_q^n . E podemos encontrar uma base composta por $k \leq n$ vetores. Caso contrário podemos apenas garantir a existência de um conjunto minimal de geradores, não necessariamente linearmente independentes.

Exemplo 2.3.1. *Seja $C \subset \mathbb{Z}_5^2$, temos que*

$$C = \langle (\bar{2}, \bar{1}) \rangle = \{(\bar{0}, \bar{0}), (\bar{2}, \bar{1}), (\bar{4}, \bar{2}), (\bar{1}, \bar{3}), (\bar{3}, \bar{4})\}$$

é um código linear 5-ário.

Definição 2.3.2. *Uma **matriz geradora** para um código q -ário C é uma matriz cujas linhas formam um conjunto gerador de C .*

Todo código linear (q primo), a menos de uma permutação de colunas, tem uma matriz geradora na forma sistemática

$$B = (I_k \ M_{k \times n-k}).$$

Normalmente os códigos são estudados com a métrica de Hamming (conforme apresentamos na [Definição 2.2.2](#)). Na literatura existem muitos estudos a respeito da métrica de Hamming, por exemplo ([HUFFMAN; PLESS, 2010](#)) e ([MACWILLIAMS; SLOANE, 1977](#)). Como o foco desse trabalho é baseado em reticulados munidos da métrica l_p , iremos nos ater à métrica de Lee, pois mais a frente vamos apresentar a definição de outra métrica que é uma extensão da métrica de Lee em \mathbb{Z}_q^n , induzida pela métrica l_p em \mathbb{Z}^n . Tais códigos tiveram início no trabalho ([LEE, 1958](#)), proposto por Lee em 1958.

2.3.1 Métrica de Lee

Definição 2.3.3. *Dados $\bar{\mathbf{x}}, \bar{\mathbf{y}} \in \mathbb{Z}_q$ a **distância de Lee** ou **métrica de Lee** em \mathbb{Z}_q é definida como*

$$d_{Lee}(\bar{\mathbf{x}}, \bar{\mathbf{y}}) = \min\{|\mathbf{x} - \mathbf{y}|, q - |\mathbf{x} - \mathbf{y}|\}.$$

Exemplo 2.3.2. *Em \mathbb{Z}_5^2 temos que $d_{Lee}(\bar{4}, \bar{2}) = 2$, $d_{Lee}(\bar{4}, \bar{0}) = 1$ e $d_{Lee}(\bar{0}, \bar{3}) = 2$. Na [Figura 14](#) temos uma representação geométrica de \mathbb{Z}_5 com a distância de Lee.*

Definição 2.3.4. *Dados $\bar{\mathbf{x}}, \bar{\mathbf{y}} \in \mathbb{Z}_q^n$, com $\bar{\mathbf{x}} = (\bar{x}_1, \dots, \bar{x}_n)$ e $\bar{\mathbf{y}} = (\bar{y}_1, \dots, \bar{y}_n)$, a **distância de Lee** em \mathbb{Z}_q^n é definida como*

$$d_{Lee}(\bar{\mathbf{x}}, \bar{\mathbf{y}}) = \sum_{i=1}^n \min\{|x_i - y_i|, q - |x_i - y_i|\} = \sum_{i=1}^n d_{Lee}(\bar{x}_i, \bar{y}_i).$$

Exemplo 2.3.3. *Em \mathbb{Z}_5^2 , temos $d_{Lee}((\bar{3}, \bar{4}), (\bar{3}, \bar{2})) = 3$, $d_{Lee}((\bar{2}, \bar{1}), (\bar{4}, \bar{2})) = 3$ e $d_{Lee}((\bar{0}, \bar{0}), (\bar{4}, \bar{1})) = 2$.*

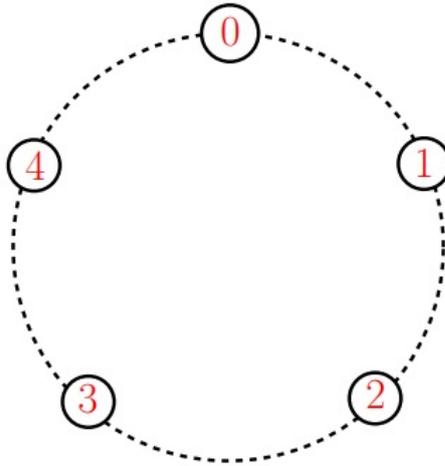


Figura 14 – Fonte: [(JÚNIOR, 2014), p. 32]

2.4 Códigos e Reticulados: Construção A

Uma maneira natural de construir reticulados é a partir de códigos, usando a chamada **Construção A**. A Construção A estendida para códigos q -ários (CONWAY; SLOANE, 2013) associa um código $C \subseteq \mathbb{Z}_q^n$ a um reticulado inteiro. Considere a aplicação sobrejetora ϕ

$$\begin{aligned} \phi : \mathbb{Z}^n &\longrightarrow \mathbb{Z}_q^n \\ (x_1, \dots, x_n) &\longmapsto (\bar{x}_1, \dots, \bar{x}_n) \end{aligned}$$

onde $\bar{x}_i = x_i \pmod{q}$ para $i = 1, \dots, n$. Dado $C \subset \mathbb{Z}_q^n$, definimos $\Lambda_A(C)$ como a imagem inversa de C por ϕ , ou seja, $\Lambda_A(C) = \phi^{-1}(C)$. É fácil ver que $\Lambda_A(C)$ é um reticulado se, e somente se, C é um código linear.

Definição 2.4.1. *Um reticulado que pode ser obtido via Construção A a partir de um código linear $C \subset \mathbb{Z}_q^n$ é chamado de **reticulado q -ário**.*

Exemplo 2.4.1. *Sejam $C \subset \mathbb{Z}_5^2$ o código linear*

$$C = \langle (\bar{1}, \bar{2}) \rangle = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{2}), (\bar{2}, \bar{4}), (\bar{3}, \bar{1}), (\bar{4}, \bar{3})\},$$

em que $\phi : \mathbb{Z}^2 \longrightarrow \mathbb{Z}_5^2$ e $\phi^{-1}(C) = \Lambda_A(C)$. Na Figura 15 temos o reticulado $\Lambda_A(C)$ em que cada caixa em vermelho representa uma cópia da caixa $[0, 5)^2$ em preto.

Observação 2.4.1. *Geometricamente, a imagem inversa dessa aplicação (Λ_A) pode ser vista como uma cópia dos pontos de C presentes no hiperplano $[0, q)^n$.*

Proposição 2.4.1. (CAMPELLO; JORGE; COSTA, 2012) *Seja $\Lambda_A(C)$ o reticulado q -ário associado a um código $C \subset \mathbb{Z}_q^n$. Valem as seguintes propriedades:*

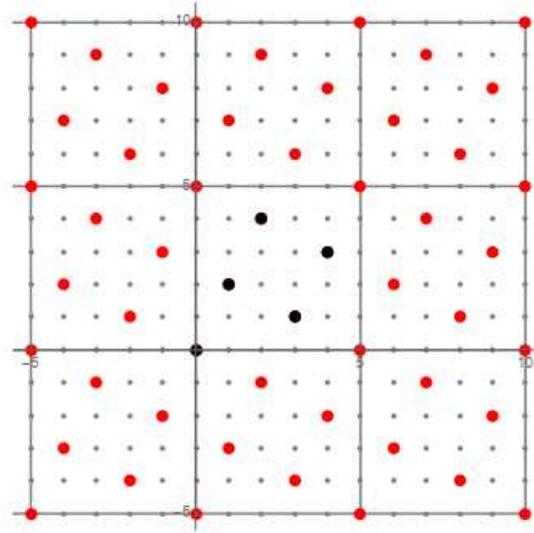


Figura 15 – Fonte: [(COSTA et al., 2017), p. 45]

1. O número de palavras de C é dado por

$$|C| = \left| \frac{\Lambda_A(C)}{q\mathbb{Z}^n} \right| = \frac{q^n}{\sqrt{\det(\Lambda_A(C))}}$$

2. Se C é gerado pela matriz $(I_{k \times k} \ M_{k \times (n-k)})$, então

$$B = \begin{pmatrix} I_{k \times k} & M_{k \times (n-k)} \\ 0_{(n-k) \times k} & qI_{(n-k) \times (n-k)} \end{pmatrix}$$

é uma matriz geradora para $\Lambda_A(C)$.

3. Todo reticulado $\Lambda \subset \mathbb{Z}^n$ é q -ário, para algum q , $1 \leq q \leq \sqrt{\det(\Lambda)}$.

A última propriedade da [Proposição 2.4.1](#) mostra que qualquer reticulado inteiro pode ser obtido via Construção A.

2.5 Métrica p -Lee

Levando em conta que o presente trabalho tem como objetivo central analisar códigos perfeitos utilizando a métrica l_p , apresentamos um breve resumo que introduz a noção da métrica p -Lee que é uma extensão da métrica de Lee em \mathbb{Z}_q^n , induzida pela métrica l_p em \mathbb{Z}^n , $1 \leq q < \infty$.

Sendo assim, considere nesse tópico a métrica l_p em $\Lambda_A(C) \subset \mathbb{Z}^n$ um reticulado obtido via Construção A e a métrica induzida p -Lee.

Sejam $\mathbf{x} = (x_1, \dots, x_n)$ e $\mathbf{y} = (y_1, \dots, y_n)$, $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^n$, para cada $1 \leq p < \infty$, a métrica l_p , denotada por d_p entre esses vetores, é definida como

$$d_p(\mathbf{x}, \mathbf{y}) = \left(\sum_{i=1}^n |x_i - y_i|^p \right)^{\frac{1}{p}}.$$

Quando $p = \infty$, a distância l_∞ é definida como

$$d_\infty(\mathbf{x}, \mathbf{y}) = \max\{|x_i - y_i|; i = 1, \dots, n\}.$$

Proposição 2.5.1. (CAMPELLO; JORGE; COSTA, 2012) *Sejam $1 \leq p < \infty$ e $\bar{\mathbf{x}}, \bar{\mathbf{y}} \in \mathbb{Z}_q^n$. A aplicação $d_{p, Lee} : \mathbb{Z}_q^n \times \mathbb{Z}_q^n \rightarrow \mathbb{R}$ dada por*

$$d_{p, Lee}(\bar{\mathbf{x}}, \bar{\mathbf{y}}) = \left(\sum_{i=1}^n (d_{Lee}(\bar{x}_i, \bar{y}_i))^p \right)^{\frac{1}{p}},$$

onde $d_{Lee}(\bar{\mathbf{x}}, \bar{\mathbf{y}}) = \min\{(\bar{\mathbf{x}} - \bar{\mathbf{y}})(\text{mod } q), (\bar{\mathbf{y}} - \bar{\mathbf{x}})(\text{mod } q)\}$, define uma métrica em \mathbb{Z}_q^n , a qual denotamos por **métrica p-Lee**.

No caso em que $p = \infty$, definimos analogamente

$$d_\infty(\bar{\mathbf{x}}, \bar{\mathbf{y}}) := \max\{d_{Lee}(\bar{x}_i, \bar{y}_i); i = 1, \dots, n\}.$$

A fim de estudar reticulados que estão munidos dessa métrica, temos alguns parâmetros importantes como a distância mínima por exemplo.

Definição 2.5.1. A **distância mínima** de um código $C \subset \mathbb{Z}_q^n$, na métrica p-Lee é definida como

$$d_{p, Lee}(C) = \min\{d_{p, Lee}(\bar{\mathbf{x}}, \bar{\mathbf{y}}); \bar{\mathbf{x}}, \bar{\mathbf{y}} \in C \text{ e } \bar{\mathbf{x}} \neq \bar{\mathbf{y}}\}.$$

Observação 2.5.1. Uma bola na métrica p-Lee é definida de modo análogo da maneira usual

$$B_{p, Lee}(\bar{\mathbf{x}}, R) = \{\bar{\mathbf{y}} \in \mathbb{Z}_q^n; d_{p, Lee}(\bar{\mathbf{x}}, \bar{\mathbf{y}}) \leq R\}.$$

Observação 2.5.2. Outro parecer importante é sobre o raio de empacotamento. Para $1 < p < \infty$ não valem os mesmos resultados que utilizamos na métrica de Lee no Teorema 2.2.1 e na Observação 2.2.1.

As métricas l_p e p-Lee até aqui abordadas serão utilizadas nos capítulos seguintes para encontrar códigos perfeitos C em \mathbb{Z}^n e \mathbb{Z}_q^n .

3 Códigos Perfeitos na Métrica l_p

Nesse capítulo vamos apresentar as definições básicas a respeito de ladrilhamento e de códigos perfeitos na métrica l_p em reticulados ambientes mais gerais. As principais referências utilizadas foram: (CAMPELLO; JORGE; COSTA, 2012), (ALVES; ANDRADE, 2014), (MATOS, 2018) e (STREY, 2020).

3.1 Introdução

Códigos perfeitos são aqueles cujos raios das bolas centradas em palavras-código coincidem com o raio de empacotamento e preenchem todo o espaço ambiente.

A caracterização completa de códigos perfeitos só foi resolvida para o caso da métrica de Hamming em (LINT, 1975). Já na métrica de Lee o problema se encontra em aberto e em (GOLOMB; WELCH, 1970) propõe-se uma solução com a Conjectura de Golomb-Welch.

Nesse capítulo, iremos abordar definições iniciais e teoremas que determinam a existência de códigos perfeitos na métrica l_p . Mas, antes de caracterizar os códigos perfeitos, vamos apresentar definições importantes para melhor abordagem do assunto.

3.2 Ladrilhamento

Definição 3.2.1. *Consideremos Λ_a um reticulado em \mathbb{R}^n , de agora em diante denominado como **reticulado ambiente**. Diremos que qualquer sub-reticulado $\Lambda \subset \Lambda_a$ é um **código** no ambiente Λ_a .*

Em razão do presente trabalho ter por objetivo fazer um estudo de códigos perfeitos sob o reticulado ambiente A_n , daqui em diante vamos passar a considerar o reticulado A_n como nosso reticulado ambiente. Vale lembrar que A_n para $n \geq 1$, é o reticulado definido como $A_n = \{(x_0, x_1, \dots, x_n) \in \mathbb{Z}^{n+1} : \sum_{i=0}^n x_i = 0\}$.

Para fins ilustrativos, vamos trabalhar em dimensão 2. Quando $n = 2$, sabemos que A_2 é equivalente ao reticulado hexagonal, cuja matriz geradora pode ser

$$B = \begin{pmatrix} 1 & 0 \\ -1/2 & \sqrt{3}/2 \end{pmatrix}.$$

Exemplo 3.2.1. Considere $\Lambda_a = A_2$ o reticulado ambiente. Seguindo a definição, um código é qualquer sub-reticulado de A_2 . A Figura 16 ilustra dois exemplos de códigos em A_2 , onde os pontos em azul representam os pontos dos respectivos códigos.

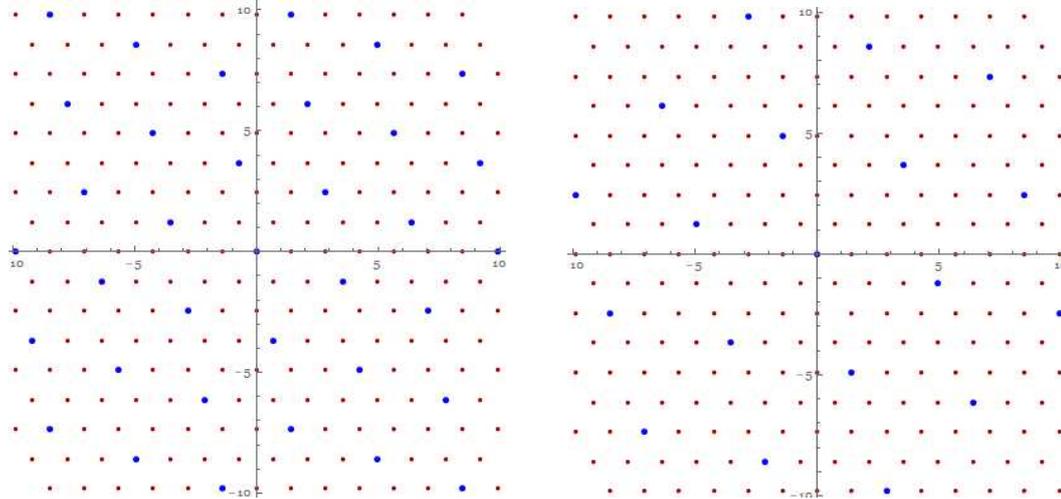


Figura 16 – Exemplos de códigos em A_2

Podemos caracterizar ladrilhamentos de maneiras distintas. Em (STREY, 2020) foi apresentada duas versões de ladrilhamento que são relacionadas, os ladrilhamentos discreto e contínuo. Um ladrilhamento discreto é uma maneira de cobrir o reticulado ambiente somente em seus pontos, por meio de translação de um conjunto finito pelos pontos do código. Já o ladrilhamento contínuo cobre o espaço $V = \text{span}(\Lambda_a)$, por meio da translação de uma região $\mathcal{R} \subset V$ pelos pontos do código.

Então, vamos apresentar aqui a definição de ladrilhamento, que é crucial para introduzir o conceito de código perfeito.

Definição 3.2.2. Um **ladrilhamento** do \mathbb{R}^n por um reticulado Λ é uma cobertura do \mathbb{R}^n por uma região \mathcal{R} fixada, de modo que quaisquer duas regiões ou se interceptam apenas no bordo ou não se interceptam, isto é, $\mathbb{R}^n = \bigcup_{\lambda \in \Lambda} (\lambda + \mathcal{R})$, em que \mathcal{R} é uma região fundamental qualquer.

A região \mathcal{R} pode ser:

- $\mathcal{P} = \left\{ \mathbf{y} = \sum_{i=1}^n \theta_i \mathbf{v}_i : \theta_i \in [0, 1), \mathbf{v}_i \in B \text{ (base de } \Lambda) \right\}$, um paralelepípedo fundamental;
- $\mathcal{V}(0) = \{ \mathbf{y} \in \mathbb{R}^n : \|\mathbf{y}\| \leq \|\mathbf{y} - \mathbf{u}\|, \forall \mathbf{u} \in \Lambda \}$, a região de Voronoi na origem;
- etc.

Outro conceito importante e que utilizaremos bastante daqui pra frente é o de bola discreta. Na métrica l_p , a bola em Λ_a centrada em $\mathbf{x} \in \Lambda_a$, onde $\mathbf{x} = (x_1, \dots, x_n)$, e raio $r > 0$ é descrita da seguinte maneira:

Definição 3.2.3. Dado um reticulado Λ_a , a **bola discreta** denotada por $\tilde{B}_p(\mathbf{x}, r)$ (bola na métrica l_p), centrada em $\mathbf{x} = (x_1, \dots, x_n) \in \Lambda_a$ e com raio $r > 0$, é definida como:

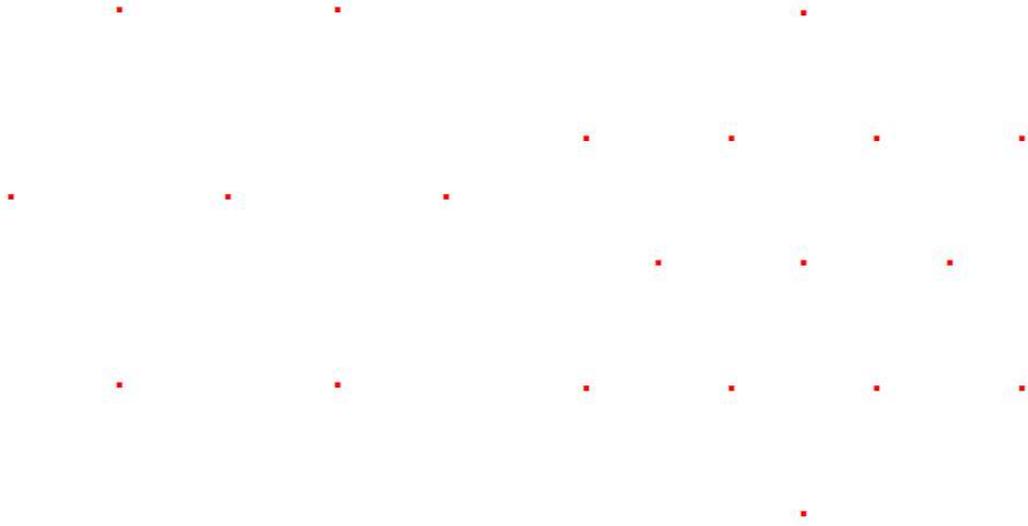
$$\tilde{B}_p(\mathbf{x}, r) = \{\mathbf{y} \in \Lambda_a : |x_1 - y_1|^p + \dots + |x_n - y_n|^p \leq r^p\}, \quad 1 \leq p < \infty$$

e

$$\tilde{B}_\infty(\mathbf{x}, r) = \{\mathbf{y} \in \Lambda_a : \max\{|x_1 - y_1|, \dots, |x_n - y_n|\} \leq r\}, \quad p = \infty.$$

Quando $\mathbf{x} = \mathbf{0}$, denotaremos a bola simplesmente por $\tilde{B}_p(r)$ ou $\tilde{B}_\infty(r)$.

Exemplo 3.2.2. Em A_2 , considerando $r^2 = 2$, $r^2 = 6$ e a métrica l_2 , temos respectivamente na [Figura 17](#) as seguintes bolas em A_2 :



(a) Bola discreta em A_2 ($r^2 = 2$)

(b) Bola discreta em A_2 ($r^2 = 6$)

Figura 17 – Exemplos de bolas discretas em A_2

Ainda falando sobre tipos de ladrilhamento, vamos apresentar a seguir a definição de poli-Voronoi, que é um tipo de ladrilho associado a $\tilde{B}_p(r)$.

Definição 3.2.4. Um **poli-Voronoi** é uma região formada pela união finita de regiões de Voronoi. Um poli-Voronoi, centrado em $\mathbf{x} \in \Lambda$, é a união das regiões de Voronoi dos pontos $\mathbf{y} \in \tilde{B}_p(\mathbf{x}, r) \subset \Lambda_a$, ou seja,

$$\mathcal{P}_V = \mathcal{V}(\mathbf{x}) + \tilde{B}_p(\mathbf{x}, r) = \bigcup_{\mathbf{y} \in \tilde{B}_p(\mathbf{x}, r)} \mathcal{V}(\mathbf{x} + \mathbf{y}).$$

Exemplo 3.2.3. *Seja A_2 o reticulado ambiente. Como o objetivo é ladrilhar A_2 pelo sub-reticulado, e o sub-reticulado está atrelado ao reticulado ambiente, vamos tomar em A_2 cada ponto que está na bola discreta $\tilde{B}_p(\mathbf{x}, r)$, centralizar uma região de voronoi para cada ponto \mathbf{x} e realizar a união dessas regiões. Essa união resulta em um poli-Voronoi. Para $p = 2$, vamos considerar as bolas discretas do Exemplo 3.2.2 ($\tilde{B}_2(\mathbf{x}, \sqrt{2})$ e $\tilde{B}_2(\mathbf{x}, \sqrt{6})$). Essas regiões podem ser observadas na Figura 18.*

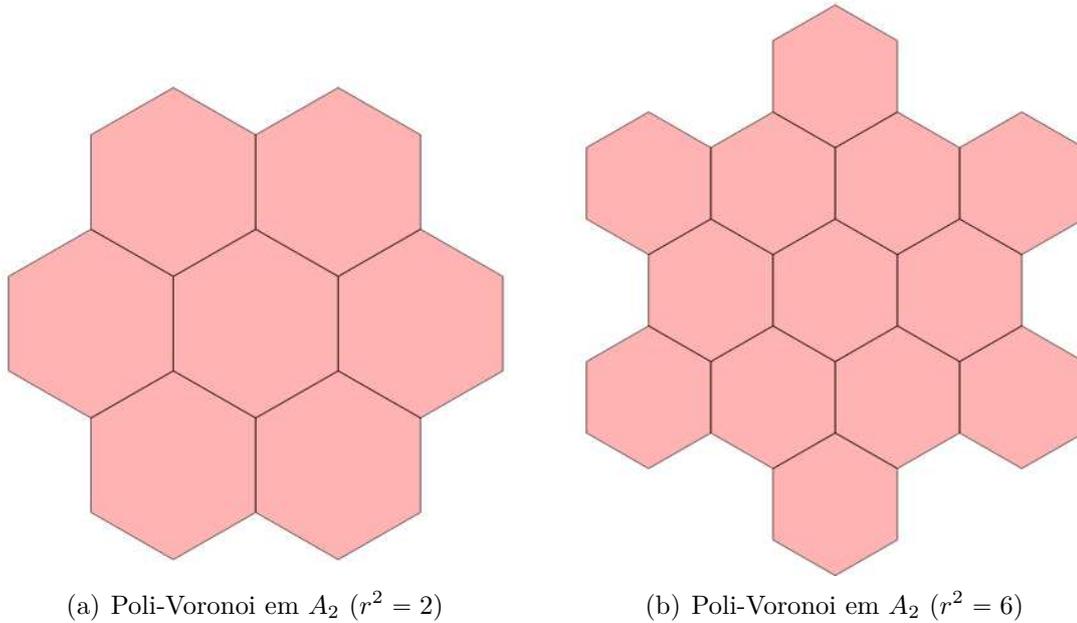


Figura 18 – Exemplos de poli-Voronoi em A_2

Exemplo 3.2.4. *Dando prosseguimento com as mesmas bolas $\tilde{B}_2(\mathbf{x}, \sqrt{2})$ e $\tilde{B}_2(\mathbf{x}, \sqrt{6})$ do exemplo anterior, vamos mostrar como fica o ladrilhamento associado às respectivas bolas em A_2 . Na Figura 19 podemos ver os dois ladrilhos. Note que, cada poli-voronoi está centrado em pontos de Λ e, se espalharmos os poli-voronoi por todos os pontos desse sub-reticulado, temos dois ladrilhamentos distintos em A_2 .*

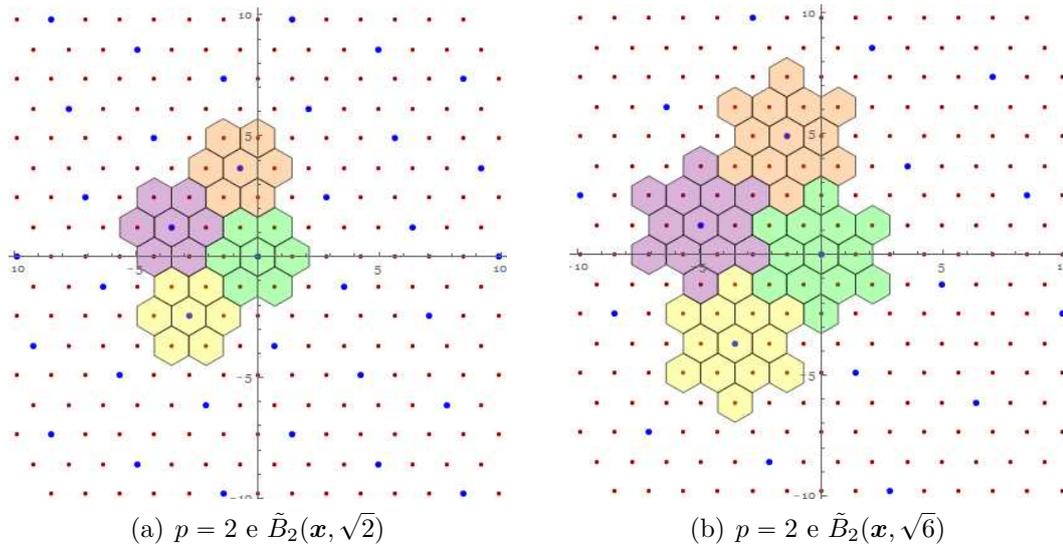
3.3 Códigos Perfeitos em Reticulados

Nosso interesse é caracterizar a tripla (n, r, p) que admitem códigos perfeitos na métrica l_p , $1 \leq p < \infty$. Trabalharemos inicialmente com os códigos perfeitos em A_2 (para fins ilustrativos) variando os valores de p . Com esse intuito, vamos apresentar a seguir conceitos que utilizaremos como base.

Definição 3.3.1. *O conjunto de todas as **distâncias realizáveis** em Λ_a contido em \mathbb{R}^n é*

$$\mathcal{D}_n = \mathcal{D}_n(\Lambda_a) = \{\|\mathbf{x}\|_2 : \mathbf{x} \in \Lambda_a\}.$$

Observação 3.3.1. *Na Definição 3.3.1 em \mathcal{D}_n , o índice n diz respeito à dimensão do reticulado.*


 Figura 19 – Ladrilhamentos associados às bolas em A_2

Como o conceito de código perfeito está relacionado ao conceito de cobertura, precisamos definir o raio de empacotamento para seguirmos com o estudo dos códigos perfeitos.

Definição 3.3.2. Definimos o **raio de empacotamento (discreto)**, denotado por $r(\Lambda)$, como sendo o maior r tal que

- (i) $((\tilde{B}_p(r) + \boldsymbol{\lambda}) \cap \tilde{B}_p(r)) \cap \Lambda_a = \emptyset, \forall \mathbf{0} \neq \boldsymbol{\lambda} \in \Lambda;$
- (ii) $r \in \mathcal{D}_n(\Lambda_a).$

Além disso, se Λ também cumprir a seguinte propriedade

- (iii) $\tilde{B}_p(r) + \Lambda = \Lambda_a$

Λ será dito um **código r -perfeito** em Λ_a .

Considere a seguinte aplicação:

$$\begin{aligned} \Phi : \mathbb{R}_+ &\longrightarrow \mathcal{D}_n \\ x &\longmapsto \max\{y \in \mathcal{D}_n : y \leq x\}. \end{aligned}$$

Definição 3.3.3. O **raio de cobertura discreto** de um código Λ , denotado por \tilde{R}_Λ , é o menor raio $r \in \mathcal{D}_n$ tal que $\bigcup_{\mathbf{x} \in \Lambda} \tilde{B}_p(\mathbf{x}, r) = \Lambda_a$.

O raio de empacotamento discreto é um elemento do conjunto de distâncias realizáveis \mathcal{D}_n . Além do mais, a última propriedade da Definição 3.3.2 nos diz que, num código r -perfeito o raio de empacotamento discreto deve coincidir com o raio de cobertura

discreto \tilde{R} . Em palavras, se o código for perfeito, vai existir uma bola $\tilde{B}_p(r)$, de tal forma que, quando centrada nos pontos do código Λ não há sobreposição e a união delas cobre todo o \mathbb{R}^n . Da perspectiva de códigos, essa é a situação mais adequada, uma vez que, quando o receptor receber a mensagem, garantimos que ela vai estar em alguma das bolas. E assim, a mensagem pode ser decodificada corretamente. Em situações em que esse caso não acontece, pode-se verificar se é possível utilizar os chamados códigos quase-perfeitos como alternativa de obter ladrilhamento.

A [Figura 19](#) apresenta dois exemplos de ladrilhamentos em A_2 , por meio da translação de poli-Voronoi pelos pontos do código. Vale ressaltar que, cada ladrilhamento apresentado é associado a uma bola discreta em A_2 na métrica l_2 .

Definição 3.3.4. *Sejam V um espaço vetorial normado e f uma função de V em \mathbb{R} . Definimos o $\operatorname{argmin}_{x \in V} f(x)$ como o conjunto de todos os pontos de V que minimizam f , isto é, $\operatorname{argmin}_{x \in V} f(x) = \{x \in V : f(x) \leq f(y), \forall y \in V\}$.*

É importante destacar que em reticulados ambientes gerais, o raio de empacotamento discreto não é exclusivamente determinado pela distância mínima, mas pode ser usado para definir limitantes, como podemos ver no seguinte teorema:

Teorema 3.3.1. *(STREY, 2020) A distância mínima $d(\Lambda)$ e o raio de empacotamento $r(\Lambda)$ de um reticulado $\Lambda \subset \Lambda_a$ satisfazem*

$$\Phi \left(\frac{d(\Lambda)}{2} \right) \leq r(\Lambda) \leq \frac{d(\Lambda)}{2} + M \leq \frac{d(\Lambda)}{2} + R_{\Lambda_a},$$

em que $M = \|\mathbf{x}/2 - \mathbf{u}\|$, $\mathbf{u} \in \operatorname{argmin}_{\mathbf{z} \in \Lambda_a} \|\mathbf{x}/2 - \mathbf{z}\|$, e \mathbf{x} é um vetor de norma mínima em Λ .

A prova do teorema acima pode ser encontrada em [\(STREY, 2020\)](#).

Vimos até o momento que, o problema de encontrar códigos perfeitos em Λ_a está associado ao problema de encontrar uma cobertura para este reticulado ambiente. E saber como identificar quando um código é perfeito, é o primeiro ponto de partida para que possamos listar esses códigos. Nesse sentido, veremos condições para se obter códigos perfeitos.

3.4 Condição de Existência

Teorema 3.4.1. *(STREY, 2020) Para $\Lambda \subset \Lambda_a$ ser um código r -perfeito uma condição necessária é que $N_{\Lambda_a}(r) \operatorname{vol}(\Lambda_a) = \operatorname{vol}(\Lambda)$.*

No [Teorema 3.4.1](#), $N_{\Lambda_a}(r) = \#(\tilde{B}_p(r) \cap \Lambda_a)$ é o número de pontos do reticulado Λ_a que pertencem a $\tilde{B}_p(r)$, e $vol(\Lambda_a)$ é o volume do reticulado ambiente. O resultado acima diz que se um código é r -perfeito, então $N_{\Lambda_a}(r)vol(\Lambda_a) = vol(\Lambda)$.

Observação 3.4.1. *Entretanto, a volta do [Teorema 3.4.1](#) nem sempre é verdadeira.*

Teorema 3.4.2. ([HORAK; ALBDAIWI, 2012](#)) *Seja $P \subset \mathbb{Z}^n$, tal que, $|P| = m$. Existe um reticulado que ladrilha o \mathbb{Z}^n por translações de P se, e somente se, existe um grupo abeliano G de ordem m e um homomorfismo $\phi : \mathbb{Z}^n \rightarrow G$ tal que a restrição de ϕ em P é uma bijeção.*

Em outras palavras o [Teorema 3.4.1](#) diz que, para o código que estamos analisando ladrilha o reticulado ambiente, precisamos verificar se as bolas centradas em um ponto do código e de raio r são disjuntas. Ou seja, precisamos verificar se existe um empacotamento.

É importante termos bons limitantes superiores para o raio de um código perfeito, para sabermos quando parar as buscas pois a partir daquele limitante não encontraremos mais nenhum perfeito. Aqui, vamos trabalhar com limitantes obtidos por ([STRAPASSON; STREY, 2021](#)) para ter apenas uma noção de onde parar as buscas. Esses limitantes são uma generalização feita para trabalhar com reticulados ambientes gerais na métrica euclidiana (l_2). Sendo assim, não podemos garantir que são bons limitantes para valores gerais de p e, portanto, não podemos afirmar que contemplamos todos os códigos perfeitos para algum valor de p . Embora esses limitantes não sejam os ideais, eles nos permitem limitar as buscas com certa segurança.

Teorema 3.4.3. ([STRAPASSON; STREY, 2021](#)) *Em um espaço ambiente Λ_a , um código r -perfeito Λ na métrica l_2 deve satisfazer*

$$r \leq M \frac{1 + \sqrt[n]{\Delta^{(n)}}}{1 - \sqrt[n]{\Delta^{(n)}}} \quad \text{ou} \quad r \leq \tilde{R}_{\Lambda_a} \frac{1 + \sqrt[n]{\Delta^{(n)}}}{1 - \sqrt[n]{\Delta^{(n)}}} \quad (3.1)$$

em que, $M = \min_{\mathbf{u} \in \Lambda_a} \|\mathbf{x}/2 - \mathbf{u}\| \leq \tilde{R}_{\Lambda_a}$, \mathbf{x} é um vetor de norma mínima em Λ e \tilde{R}_{Λ_a} é o raio de cobertura contínuo do reticulado ambiente Λ_a . E $\Delta^{(n)}$ é a densidade de empacotamento máxima na dimensão n .

Teorema 3.4.4. ([STRAPASSON; STREY, 2021](#)) *Em um espaço ambiente Λ_a , um código r -perfeito Λ na métrica l_2 deve satisfazer*

$$r \leq \tilde{R}_{\Lambda_a} \frac{\sqrt[n]{\Theta^{(n)}} + 1}{\sqrt[n]{\Theta^{(n)}} - 1} \quad (3.2)$$

em que, \tilde{R}_{Λ_a} é o raio de cobertura contínuo do reticulado ambiente Λ_a . E $\Theta^{(n)}$ é o ínfimo das densidades de cobertura sobre todos os reticulados n -dimensionais.

O limitante (3.1) depende da densidade de empacotamento máxima sobre todos os reticulados n -dimensionais de posto completo. Já o (3.2) depende do ínfimo das densidades de cobertura sobre os mesmos reticulados.

A seguir, no Capítulo 4 buscaremos por todos os códigos perfeitos no reticulado ambiente A_n (os valores de n serão especificados).

4 Resultados Computacionais

Iniciaremos esse capítulo com um pseudo-código apresentado em (STREY, 2020). Tal algoritmo visa listar todos os códigos perfeitos em reticulados ambientes quaisquer até um determinado raio de empacotamento r , satisfazendo os limitantes mostrados no capítulo anterior. Para finalidade deste trabalho, vamos nos ater ao reticulado ambiente A_n .

Com o algoritmo, vamos buscar para quais raios são obtidos códigos perfeitos e listar os códigos perfeitos no reticulado ambiente em questão.

4.1 Algoritmo

Antes de mais nada devemos fixar valores para p , n e escolher o reticulado ambiente que iremos utilizar. Como dito anteriormente, nosso foco é trabalhar com o ambiente A_n , então basta fixarmos os valores de n e p . Feito isso, utilizamos o Algoritmo SVP para obter todos os pontos de A_n que possuem norma menor ou igual a r , ou seja, o conjunto de distâncias realizáveis em A_n .

O **problema do vetor mais curto** (*Shortest Vector Problem*) - SVP, consiste em dada a matriz B , encontrar o vetor de norma mínima do reticulado Λ gerado por B .

Para cada raio atingível em Λ_a , $r_i \in \mathcal{D}(\Lambda_a)$ ($0 \neq r_i \leq r$), o algoritmo verifica se existe um sub-reticulado $\Lambda \subset \Lambda_a$ tal que $vol(\Lambda) = vol(\Lambda_a)N_{\Lambda_a}(r_i)$.

Algoritmo 1 – TESTE DOS CÓDIGOS PERFEITOS**Entrada:** Λ_a é o reticulado ambiente; $0 \neq r_i \leq r$;**Saída:** Lista de todos os códigos r_i -perfeitos em Λ_a ;

```

1 início
2   inicialização;
3    $\tilde{B}_p \leftarrow \tilde{B}_p^n(r_i)$ ;
4   Lattices  $\leftarrow \{\Lambda \subset \Lambda_a : vol(\Lambda) = vol(\Lambda_a)N_{\Lambda_a}(r_i)\}$ ;
5    $C \leftarrow \#Lattices$ ;
6   enquanto  $C > 0$  faça
7     se “Teste de Injetividade” no  $C$ -ésimo elemento de Lattices é negativo
8       então
9         delete o  $C$ -ésimo elemento de Lattices;
10      fim
11      $C \leftarrow C - 1$ ;
12  fim
13   $C \leftarrow \#Lattices$ ;
14  enquanto  $C > 0$  faça
15    se “Teste de Empacotamento” no  $C$ -ésimo elemento de Lattices é negativo
16      então
17        delete o  $C$ -ésimo elemento de Lattices;
18    fim
19     $C \leftarrow C - 1$ ;
20  fim
21 fim

```

O algoritmo acima lista todos os códigos r_i -perfeitos em A_n . Dados o reticulado ambiente, a dimensão e o valor de p , usando o SVP vamos listar todos os valores possíveis para o raio r_i . Esses possíveis valores de raios são os valores da norma dos pontos de A_n , normas essas que possuem valores menores ou iguais a r . Em que, r é uma estimativa satisfazendo os limitantes mostrados no capítulo anterior.

Para cada r_i , deve-se calcular a cardinalidade da bola discreta $\tilde{B}_p(r_i)$ para obter o $vol(\Lambda)$ e na sequência listar todos os sub-reticulados Λ com o volume que foi dado nesse passo. Lembrando que, $vol(\Lambda) = N_{\Lambda_a} vol(\Lambda_a)$. Dessa lista de reticulados só nos interessam os que são códigos perfeitos para A_n . Assim, para avaliar cada potencial código perfeito, aplicaremos o “Teste de Injetividade”. Este teste consiste em verificar se as bolas centradas em pontos do código e de raio r são disjuntas. Ou seja, dadas as bolas discretas centradas em pontos do sub-reticulado, queremos obter o raio de empacotamento. O raio de empacotamento é o maior raio de tal maneira que, a bola centrada em um ponto de Λ

não intercepte as bolas de mesmo raio, centradas em outros pontos de Λ . Como estamos trabalhando com empacotamento discreto, os pontos de coordenadas inteiras de uma bola não estão contidos em outras bolas discretas de mesmo raio.

O “Teste de Injetividade” é baseado no [Teorema 3.4.2](#). No qual, para cada $\Lambda \subset \Lambda_a$ vamos considerar um homomorfismo $\phi : A_2 \rightarrow G$, onde G é um grupo abeliano de cardinalidade igual ao determinante do código ($|G| = \det(\Lambda)$). Dada a bola \tilde{B}_{r_i} , vamos analisar a ação quando aplicamos a função ϕ nos pontos da bola \tilde{B}_{r_i} de maneira que, cada ponto seja levado em um único representante da sua classe dentro de um paralelepípedo fundamental de Λ_a . Se essa aplicação não for bijetora, descartamos o reticulado, e seguimos testando os próximos candidatos. Caso a aplicação seja bijetora, pelo teorema temos que esse código é perfeito. No “Teste de Empacotamento” verifica-se se as bolas de raio r_i centradas em pontos de $\Lambda \subset \Lambda_a$ são disjuntas.

Sabemos por ([STREY, 2020](#)) que para $p = 2$ existem 10 raios para quais existem códigos perfeitos em A_2 e a maior cardinalidade de bola onde obtemos perfeitos é 127. Então faremos uma análise mantendo a dimensão 2 inicialmente para analisar se existe certo padrão conforme aumentamos o valor de p .

Exemplo 4.1.1. *Dados o reticulado ambiente Λ_a , que possui matriz de Gram $G = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$ e $r_i = \sqrt{8}$ um candidato a raio de empacotamento. Para $r_i = \sqrt{8}$, executando o algoritmo proposto por Fincke e Pohst em ([FINCKE; POHST, 1985](#)), encontramos a bola $\tilde{B}_2(\sqrt{8})$, $\tilde{B}_2(\sqrt{8}) = \{(0,0)M, \pm(1,0)M, \pm(0,1)M, \pm(1,1)M, \pm(-1,1)M, \pm(1,2)M, \pm(2,1)M, \pm(2,0)M, \pm(0,2)M, \pm(2,2)M\}$, em que M é uma matriz geradora para Λ_a . Logo, $\#\tilde{B}_2(\sqrt{8}) = 19$. Seguindo para o próximo passo do algoritmo, precisamos obter um sub-reticulado de Λ_a tal que $\text{vol}(\Lambda) = 19 \text{ vol}(\Lambda_a)$. Para que isso ocorra, precisamos obter uma matriz $A \in \mathbb{R}^{2 \times 2}$ tal que $\det(A) = 19$ e AM gere Λ .*

Utilizando a Fórmula Normal de Hermite, temos:

$$A_{19,x} = \begin{pmatrix} 1 & x \\ 0 & 19 \end{pmatrix} \quad A_{1,x} = \begin{pmatrix} 19 & x \\ 0 & 1 \end{pmatrix}$$

em que $x \in \{0, 1, \dots, 18\}$ e $x \in \{0\}$.

Nesse momento, todos os candidatos a sub-reticulados fazem parte da lista “Lattices” e cada um deles irá passar pelo “Teste de Injetividade”. Considere o candidato cuja matriz é $A_{19,7} = \begin{pmatrix} 1 & 7 \\ 0 & 19 \end{pmatrix}$. A matriz $A_{19,7}$ caracteriza o núcleo do homomorfismo $\Phi_{A_{19,7}}$ e agora iremos analisar a aplicação de $\Phi_{A_{19,7}}$ nos elementos da bola $\tilde{B}_2(\sqrt{8})$. Observe na [Figura 20](#) as seguintes situações:

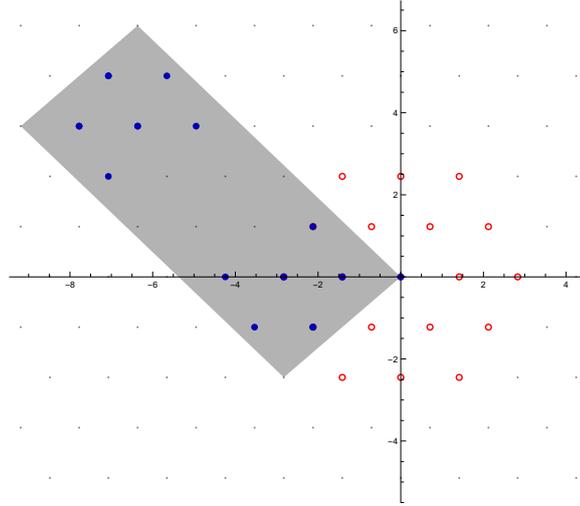


Figura 20 – Ação do homomorfismo $\Phi_{A_{19,7}}$ nos elementos da bola $\tilde{B}_2(\sqrt{8})$

- Em $\tilde{B}_2(\sqrt{8})$ os elementos $(1, 0)M$ e $(-2, -2)M$ correspondem ao elemento $(-4, 3)M$ no paralelogramo fundamental;
- Em $\tilde{B}_2(\sqrt{8})$ os elementos $(1, 1)M$ e $(-2, -1)M$ correspondem ao elemento $(-2, -1)M$ no paralelogramo fundamental;
- Em $\tilde{B}_2(\sqrt{8})$ os elementos $(-1, 0)M$ e $(2, 2)M$ correspondem ao elemento $(-1, 0)M$ no paralelogramo fundamental;
- Em $\tilde{B}_2(\sqrt{8})$ os elementos $(-1, -1)M$ e $(2, 1)M$ correspondem ao elemento $(-3, 4)M$ no paralelogramo fundamental;
- Em $\tilde{B}_2(\sqrt{8})$ os elementos $(1, 2)M$ e $(-2, 0)M$ correspondem ao elemento $(-2, 0)M$ no paralelogramo fundamental;
- Em $\tilde{B}_2(\sqrt{8})$ os elementos $(-1, -2)M$ e $(2, 0)M$ correspondem ao elemento $(-3, 3)M$ no paralelogramo fundamental.

Portanto, a aplicação $\Phi_{A_{19,7}}$ não é injetora, e $A_{19,7}$ será deletado do conjunto “Lattices”. Logo o reticulado gerado pela matriz $A_{19,7}M$ não é um código perfeito em Λ_a .

Agora considere o candidato $A_{19,8} = \begin{pmatrix} 1 & 8 \\ 0 & 19 \end{pmatrix}$. Ao aplicar $\Phi_{A_{19,8}}$ em $\tilde{B}_2(\sqrt{8})$, percebemos que cada elemento de $\tilde{B}_2(\sqrt{8})$ tem um correspondente distinto no paralelogramo fundamental, como é possível observar na [Figura 21](#). Isto significa que, nesse caso temos que $\Phi_{A_{19,8}}$ é injetora, e portanto, a matriz $A_{19,8}$ passou no “Teste de Injetividade”.

Finalizamos fazendo o “Teste de Empacotamento”. Ao final dos testes, concluímos que para $A = \begin{pmatrix} 1 & 8 \\ 0 & 19 \end{pmatrix}$ o único sub-reticulado gerado por AM é um código perfeito em Λ_a .

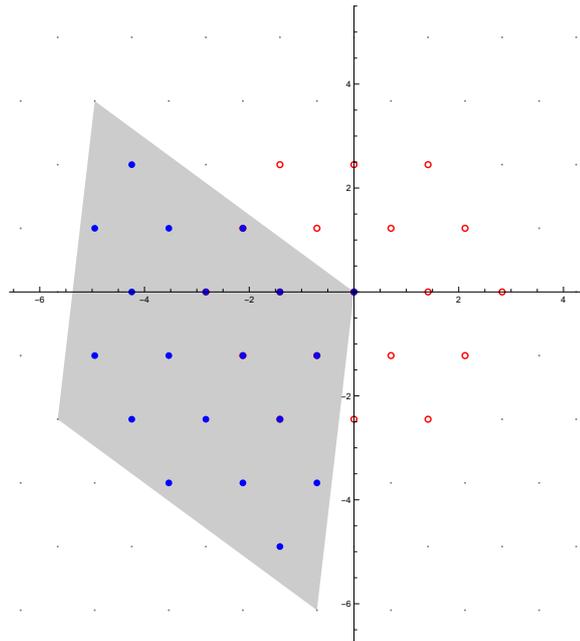


Figura 21 – Ação do homomorfismo $\Phi_{A_{19,8}}$ nos elementos da bola $\tilde{B}_2(\sqrt{8})$

Observação 4.1.1. Colocamos a matriz do sub-reticulado na forma padrão para não correr o risco de pegar reticulados equivalentes e não fazer contas repetidas. Então, para não haver essa redundância, colocamos a matriz na forma triangular superior, com o determinante igual ao que estamos analisando. Fazemos esse procedimento no algoritmo descartamos os sub-reticulados equivalentes.

4.2 Resultados

Executando o algoritmo apresentado na Seção 4.1, a busca foi realizada no espaço ambiente A_n , nas dimensões 2 e 3. Fixando nosso reticulado ambiente e a dimensão, para cada valor de p o algoritmo buscou, para cada r_i , uma matriz inteira A , de modo que, quando multiplicada por M (matriz geradora do reticulado ambiente) obtemos uma matriz AM que gera o sub-reticulado $\Lambda \subset \Lambda_a$. Esses códigos perfeitos ($\Lambda \subset \Lambda_a$) são únicos para o ambiente escolhido, a menos de congruência.

4.2.1 Códigos Perfeitos em A_2

Caso $p = 2$

Para o reticulado ambiente A_2 , temos M uma matriz geradora de A_2 tal que $G = MM^t = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$.

Considerando o caso onde $p = 2$, obtemos 10 raios para os quais existem códigos perfeitos em A_2 . Podemos observar na Tabela 9 os raios com suas respectivas

cardinalidades das bolas discretas e matriz A . Note que, para $p = 2$, a maior cardinalidade da bola discreta é 127, quando $r = \sqrt{72}$.

Caso $p = 2$		
r^2	$N_{A_2}(r)$	A
2	7	$\begin{pmatrix} 1 & 3 \\ 0 & 7 \end{pmatrix}$
6	13	$\begin{pmatrix} 1 & 4 \\ 0 & 13 \end{pmatrix}$
8	19	$\begin{pmatrix} 1 & 8 \\ 0 & 19 \end{pmatrix}$
14	31	$\begin{pmatrix} 1 & 6 \\ 0 & 31 \end{pmatrix}$
18	37	$\begin{pmatrix} 1 & 11 \\ 0 & 37 \end{pmatrix}$
24	43	$\begin{pmatrix} 1 & 7 \\ 0 & 43 \end{pmatrix}$
32	61	$\begin{pmatrix} 1 & 14 \\ 0 & 61 \end{pmatrix}$
38	73	$\begin{pmatrix} 1 & 9 \\ 0 & 73 \end{pmatrix}$
50	91	$\begin{pmatrix} 1 & 17 \\ 0 & 91 \end{pmatrix}$
72	127	$\begin{pmatrix} 1 & 20 \\ 0 & 127 \end{pmatrix}$

Tabela 9 – $p = 2$

Caso $p = 3$

Para $p = 3$ existem 11 raios para os quais existem códigos perfeitos em A_2 . Na [Tabela 10](#) vemos cada raio e suas respectivas cardinalidade da bola discreta e matriz A . No caso $p = 3$, a maior cardinalidade da bola discreta é 45. É possível perceber comparando as tabelas [9](#) e [10](#) que perdemos as cardinalidades de bola iguais a 43, 61, 73, 91 e 127 quando saímos de $p = 2$ para $p = 3$. Contudo, ganhamos outras cardinalidades intermediárias que não ladrilhavam em $p = 2$, como 5, 11, 17, 23, 27 e 45.

Caso $p = 3$		
r^2	$N_{A_2}(r)$	A
$\sqrt{\frac{7}{2} + \frac{3\sqrt{3}}{4}}$	5	$\begin{pmatrix} 1 & 3 \\ 0 & 5 \end{pmatrix}$
$2\sqrt{2}$	7	$\begin{pmatrix} 1 & 3 \\ 0 & 7 \end{pmatrix}$
$\frac{3(9 + \sqrt{3})}{2\sqrt{2}}$	11	$\begin{pmatrix} 1 & 3 \\ 0 & 11 \end{pmatrix}$
$6\sqrt{6}$	13	$\begin{pmatrix} 1 & 4 \\ 0 & 13 \end{pmatrix}$
$2(\sqrt{2} + 3\sqrt{6})$	17	$\begin{pmatrix} 1 & 11 \\ 0 & 17 \end{pmatrix}$
$16\sqrt{2}$	19	$\begin{pmatrix} 1 & 8 \\ 0 & 19 \end{pmatrix}$
$2\sqrt{2}(8 + 3\sqrt{3})$	23	$\begin{pmatrix} 1 & 14 \\ 0 & 23 \end{pmatrix}$
$\frac{125 + 3\sqrt{3}}{2\sqrt{2}}$	27	$\begin{pmatrix} 1 & 16 \\ 0 & 27 \end{pmatrix}$
$\frac{\sqrt{2} + 81\sqrt{6}}{4}$	31	$\begin{pmatrix} 1 & 6 \\ 0 & 31 \end{pmatrix}$
$54\sqrt{2}$	37	$\begin{pmatrix} 1 & 11 \\ 0 & 37 \end{pmatrix}$
$\frac{125 + 81\sqrt{3}}{2\sqrt{2}}$	45	$\begin{pmatrix} 1 & 13 \\ 0 & 45 \end{pmatrix}$

Tabela 10 – $p = 3$ **Caso $p = 4$**

Dando continuidade, para $p = 4$ existem 13 raios para os quais existem códigos perfeitos em A_2 . Na [Tabela 11](#) vemos cada raio e suas respectivas cardinalidade da bola discreta e a matriz A . No caso $p = 4$, a maior cardinalidade da bola discreta é 67. Comparando esse caso com os casos acima vemos que a quantidade de raios para os quais existem códigos perfeitos aumenta conforme aumentamos o valor de p . Comparando também os casos $p = 3$ e $p = 4$, vemos que a maior cardinalidade da bola discreta também aumentou, de 45 para 67. Outro fato interessante a respeito das cardinalidades das bolas discretas foi a repetição de todas as cardinalidades do caso $p = 3$ para $p = 4$. Ou seja, todas as bolas do caso anterior também ladrilham A_2 quando $p = 4$ e ainda encontramos

uma nova bola de cardinalidade 67. Perceba que, o fato das cardinalidades se repetirem não implica que seus raios correspondentes sejam iguais, o que faz sentido, já que são métricas distintas.

Caso $p = 4$		
r^2	$N_{A_2}(r)$	A
$\frac{5}{2}$	5	$\begin{pmatrix} 1 & 3 \\ 0 & 5 \end{pmatrix}$
4	7	$\begin{pmatrix} 1 & 3 \\ 0 & 7 \end{pmatrix}$
$\frac{45}{2}$	11	$\begin{pmatrix} 1 & 3 \\ 0 & 11 \end{pmatrix}$
36	13	$\begin{pmatrix} 1 & 4 \\ 0 & 13 \end{pmatrix}$
40	17	$\begin{pmatrix} 1 & 11 \\ 0 & 17 \end{pmatrix}$
64	19	$\begin{pmatrix} 1 & 8 \\ 0 & 19 \end{pmatrix}$
100	23	$\begin{pmatrix} 1 & 14 \\ 0 & 23 \end{pmatrix}$
$\frac{317}{2}$	27	$\begin{pmatrix} 1 & 16 \\ 0 & 27 \end{pmatrix}$
$\frac{365}{2}$	31	$\begin{pmatrix} 1 & 6 \\ 0 & 31 \end{pmatrix}$
324	37	$\begin{pmatrix} 1 & 11 \\ 0 & 37 \end{pmatrix}$
$\frac{677}{2}$	41	$\begin{pmatrix} 1 & 12 \\ 0 & 41 \end{pmatrix}$
360	45	$\begin{pmatrix} 1 & 13 \\ 0 & 45 \end{pmatrix}$
900	67	$\begin{pmatrix} 1 & 19 \\ 0 & 67 \end{pmatrix}$

Tabela 11 – $p = 4$

Caso $p = 5$

Para $p = 5$ existem 15 raios para os quais existem códigos perfeitos em A_2 . Na Tabela 12 vemos cada raio e suas respectivas cardinalidade da bola discreta e matriz A . Nesse caso, a maior cardinalidade da bola discreta é 149. Veja que, a quantidade de códigos perfeitos segue aumentando conforme aumentamos o valor de p . E desde $p = 3$ até o caso atual temos todas as bolas de mesma cardinalidade dos casos anteriores ladrilhando A_2 para $p = 5$ e ganhamos novas bolas com cardinalidades maiores.

Caso $p = 5$		
r^2	$N_{A_2}(r)$	A
$\frac{\sqrt{2} + 9\sqrt{6}}{8}$	5	$\begin{pmatrix} 1 & 3 \\ 0 & 5 \end{pmatrix}$
$4\sqrt{2}$	7	$\begin{pmatrix} 1 & 3 \\ 0 & 7 \end{pmatrix}$
$\frac{9(27 + \sqrt{3})}{4\sqrt{2}}$	11	$\begin{pmatrix} 1 & 3 \\ 0 & 11 \end{pmatrix}$
$36\sqrt{6}$	13	$\begin{pmatrix} 1 & 4 \\ 0 & 13 \end{pmatrix}$
$4(\sqrt{2} + 9\sqrt{6})$	17	$\begin{pmatrix} 1 & 11 \\ 0 & 17 \end{pmatrix}$
$128\sqrt{2}$	19	$\begin{pmatrix} 1 & 8 \\ 0 & 19 \end{pmatrix}$
$4\sqrt{2}(32 + 9\sqrt{3})$	23	$\begin{pmatrix} 1 & 14 \\ 0 & 23 \end{pmatrix}$
$\frac{3125 + 9\sqrt{3}}{4\sqrt{2}}$	27	$\begin{pmatrix} 1 & 16 \\ 0 & 27 \end{pmatrix}$
$\frac{\sqrt{2} + 2187\sqrt{6}}{8}$	31	$\begin{pmatrix} 1 & 6 \\ 0 & 31 \end{pmatrix}$
$\frac{3125 + 2187\sqrt{3}}{4\sqrt{2}}$	39	$\begin{pmatrix} 1 & 31 \\ 0 & 39 \end{pmatrix}$
$972\sqrt{2}$	41	$\begin{pmatrix} 1 & 12 \\ 0 & 41 \end{pmatrix}$
$36\sqrt{2}(27 + \sqrt{3})$	45	$\begin{pmatrix} 1 & 13 \\ 0 & 45 \end{pmatrix}$
$36\sqrt{2}(27 + 32\sqrt{3})$	67	$\begin{pmatrix} 1 & 19 \\ 0 & 67 \end{pmatrix}$
$4\sqrt{2}(3125 + 288\sqrt{3})$	115	$\begin{pmatrix} 1 & 21 \\ 0 & 115 \end{pmatrix}$

Caso $p = 5$		
r^2	$N_{A_2}(r)$	A
$4\sqrt{2}(3125 + 2187\sqrt{3})$	149	$\begin{pmatrix} 1 & 27 \\ 0 & 149 \end{pmatrix}$

Tabela 12 – $p = 5$

Caso $p = 6$

Continuando, para $p = 6$ existem 18 raios para os quais existem códigos perfeitos em A_2 . Na [Tabela 13](#) vemos cada raio e suas respectivas cardinalidade da bola discreta e matriz A . A maior cardinalidade da bola discreta é 149, assim como no caso $p = 5$. A quantidade de códigos perfeitos segue aumentando conforme aumentamos o valor de p , entretanto, obtivemos o mesmo valor referente à maior cardinalidade da bola discreta, quando comparado ao caso anterior.

Caso $p = 6$		
r^2	$N_{A_2}(r)$	A
$\frac{7}{2}$	5	$\begin{pmatrix} 1 & 3 \\ 0 & 5 \end{pmatrix}$
8	7	$\begin{pmatrix} 1 & 3 \\ 0 & 7 \end{pmatrix}$
$\frac{189}{2}$	11	$\begin{pmatrix} 1 & 3 \\ 0 & 11 \end{pmatrix}$
216	13	$\begin{pmatrix} 1 & 4 \\ 0 & 13 \end{pmatrix}$
224	17	$\begin{pmatrix} 1 & 11 \\ 0 & 17 \end{pmatrix}$
512	19	$\begin{pmatrix} 1 & 8 \\ 0 & 19 \end{pmatrix}$
728	23	$\begin{pmatrix} 1 & 14 \\ 0 & 23 \end{pmatrix}$
$\frac{3913}{2}$	27	$\begin{pmatrix} 1 & 16 \\ 0 & 27 \end{pmatrix}$
$\frac{4921}{2}$	31	$\begin{pmatrix} 1 & 6 \\ 0 & 31 \end{pmatrix}$

Caso $p = 6$		
r^2	$N_{A_2}(r)$	A
$\frac{8827}{2}$	39	$\begin{pmatrix} 1 & 31 \\ 0 & 39 \end{pmatrix}$
5832	41	$\begin{pmatrix} 1 & 12 \\ 0 & 41 \end{pmatrix}$
6048	45	$\begin{pmatrix} 1 & 13 \\ 0 & 45 \end{pmatrix}$
19656	67	$\begin{pmatrix} 1 & 19 \\ 0 & 67 \end{pmatrix}$
46592	77	$\begin{pmatrix} 1 & 48 \\ 0 & 77 \end{pmatrix}$
$\frac{134881}{2}$	97	$\begin{pmatrix} 1 & 18 \\ 0 & 97 \end{pmatrix}$
$\frac{238329}{2}$	105	$\begin{pmatrix} 3 & 23 \\ 0 & 35 \end{pmatrix}$
138824	115	$\begin{pmatrix} 1 & 21 \\ 0 & 115 \end{pmatrix}$
282464	149	$\begin{pmatrix} 1 & 27 \\ 0 & 149 \end{pmatrix}$

Tabela 13 – $p = 6$ **Caso $p = 7$**

Para $p = 7$ existem 22 raios para os quais existem códigos perfeitos em A_2 . Na [Tabela 14](#) vemos cada raio e suas respectivas cardinalidade da bola discreta e matriz A . Neste caso, a maior cardinalidade da bola discreta é 313. A quantidade de códigos perfeitos segue aumentando conforme aumentamos o valor de p , assim como o valor referente à maior cardinalidade da bola discreta.

Caso $p = 7$		
r^2	$N_{A_2}(r)$	A
$\frac{\sqrt{2} + 27\sqrt{6}}{16}$	5	$\begin{pmatrix} 1 & 3 \\ 0 & 5 \end{pmatrix}$
$8\sqrt{2}$	7	$\begin{pmatrix} 1 & 3 \\ 0 & 7 \end{pmatrix}$

Caso $p = 7$		
r^2	$N_{A_2}(r)$	A
$\frac{27(81 + \sqrt{3})}{8\sqrt{2}}$	11	$\begin{pmatrix} 1 & 3 \\ 0 & 11 \end{pmatrix}$
$216\sqrt{6}$	13	$\begin{pmatrix} 1 & 4 \\ 0 & 13 \end{pmatrix}$
$8(\sqrt{2} + 27\sqrt{6})$	17	$\begin{pmatrix} 1 & 11 \\ 0 & 17 \end{pmatrix}$
$1024\sqrt{2}$	19	$\begin{pmatrix} 1 & 8 \\ 0 & 19 \end{pmatrix}$
$8\sqrt{2}(128 + 27\sqrt{3})$	23	$\begin{pmatrix} 1 & 14 \\ 0 & 23 \end{pmatrix}$
$\frac{78125 + 27\sqrt{3}}{8\sqrt{2}}$	27	$\begin{pmatrix} 1 & 16 \\ 0 & 27 \end{pmatrix}$
$\frac{\sqrt{2} + 59049\sqrt{6}}{16}$	31	$\begin{pmatrix} 1 & 6 \\ 0 & 31 \end{pmatrix}$
$\frac{78125 + 59049\sqrt{3}}{8\sqrt{2}}$	39	$\begin{pmatrix} 1 & 31 \\ 0 & 39 \end{pmatrix}$
$17496\sqrt{2}$	41	$\begin{pmatrix} 1 & 12 \\ 0 & 41 \end{pmatrix}$
$216\sqrt{2}(81 + \sqrt{3})$	45	$\begin{pmatrix} 1 & 13 \\ 0 & 45 \end{pmatrix}$
$216\sqrt{2}(81 + 128\sqrt{3})$	67	$\begin{pmatrix} 1 & 19 \\ 0 & 67 \end{pmatrix}$
$1024\sqrt{2}(128 + 27\sqrt{3})$	77	$\begin{pmatrix} 1 & 48 \\ 0 & 77 \end{pmatrix}$
$\frac{823543 + 2109375\sqrt{3}}{8\sqrt{2}}$	93	$\begin{pmatrix} 1 & 58 \\ 0 & 93 \end{pmatrix}$
$\frac{27(177147 + \sqrt{3})}{8\sqrt{2}}$	97	$\begin{pmatrix} 1 & 18 \\ 0 & 97 \end{pmatrix}$
$\frac{27(177147 + 78125\sqrt{3})}{8\sqrt{2}}$	105	$\begin{pmatrix} 3 & 23 \\ 0 & 35 \end{pmatrix}$
$8\sqrt{2}(78125 + 3456\sqrt{3})$	115	$\begin{pmatrix} 1 & 21 \\ 0 & 115 \end{pmatrix}$
$\frac{19487171 + 2109375\sqrt{3}}{8\sqrt{2}}$	149	$\begin{pmatrix} 1 & 27 \\ 0 & 149 \end{pmatrix}$
$\frac{19487171 + 22235661\sqrt{3}}{8\sqrt{2}}$	187	$\begin{pmatrix} 1 & 72 \\ 0 & 187 \end{pmatrix}$

Caso $p = 7$		
r^2	$N_{A_2}(r)$	A
$\frac{27(6328125 + 823543\sqrt{3})}{8\sqrt{2}}$	263	$\begin{pmatrix} 1 & 35 \\ 0 & 263 \end{pmatrix}$
$\frac{2187(78125 + 59049\sqrt{3})}{8\sqrt{2}}$	313	$\begin{pmatrix} 1 & 176 \\ 0 & 313 \end{pmatrix}$

Tabela 14 – $p = 7$

Caso $p = 8$

Para $p = 8$ existem 25 raios para os quais existem códigos perfeitos em A_2 . Na [Tabela 15](#) vemos cada raio e suas respectivas cardinalidade da bola discreta e matriz A . No caso $p = 8$, a maior cardinalidade da bola discreta é 485.

Caso $p = 8$		
r^2	$N_{A_2}(r)$	A
$\frac{41}{8}$	5	$\begin{pmatrix} 1 & 3 \\ 0 & 5 \end{pmatrix}$
16	7	$\begin{pmatrix} 1 & 3 \\ 0 & 7 \end{pmatrix}$
$\frac{3321}{8}$	11	$\begin{pmatrix} 1 & 3 \\ 0 & 11 \end{pmatrix}$
1296	13	$\begin{pmatrix} 1 & 4 \\ 0 & 13 \end{pmatrix}$
1312	17	$\begin{pmatrix} 1 & 11 \\ 0 & 17 \end{pmatrix}$
4096	19	$\begin{pmatrix} 1 & 8 \\ 0 & 19 \end{pmatrix}$
5392	23	$\begin{pmatrix} 1 & 14 \\ 0 & 23 \end{pmatrix}$
$\frac{195353}{8}$	27	$\begin{pmatrix} 1 & 16 \\ 0 & 27 \end{pmatrix}$
$\frac{265721}{8}$	31	$\begin{pmatrix} 1 & 6 \\ 0 & 31 \end{pmatrix}$
$\frac{461033}{8}$	39	$\begin{pmatrix} 1 & 31 \\ 0 & 39 \end{pmatrix}$

Caso $p = 8$		
r^2	$N_{A_2}(r)$	A
104976	41	$\begin{pmatrix} 1 & 12 \\ 0 & 41 \end{pmatrix}$
106272	45	$\begin{pmatrix} 1 & 13 \\ 0 & 45 \end{pmatrix}$
436752	67	$\begin{pmatrix} 1 & 19 \\ 0 & 67 \end{pmatrix}$
1380352	77	$\begin{pmatrix} 1 & 48 \\ 0 & 77 \end{pmatrix}$
$\frac{18702713}{8}$	93	$\begin{pmatrix} 1 & 58 \\ 0 & 93 \end{pmatrix}$
$\frac{21523401}{8}$	97	$\begin{pmatrix} 1 & 18 \\ 0 & 97 \end{pmatrix}$
$\frac{37343673}{8}$	105	$\begin{pmatrix} 3 & 23 \\ 0 & 35 \end{pmatrix}$
6581776	115	$\begin{pmatrix} 1 & 21 \\ 0 & 115 \end{pmatrix}$
$\frac{122999753}{8}$	149	$\begin{pmatrix} 1 & 27 \\ 0 & 149 \end{pmatrix}$
$\frac{340653881}{8}$	187	$\begin{pmatrix} 1 & 72 \\ 0 & 187 \end{pmatrix}$
$\frac{641339801}{8}$	203	$\begin{pmatrix} 1 & 78 \\ 0 & 203 \end{pmatrix}$
$\frac{1514919753}{8}$	263	$\begin{pmatrix} 1 & 35 \\ 0 & 263 \end{pmatrix}$
$\frac{3024837513}{8}$	313	$\begin{pmatrix} 1 & 176 \\ 0 & 313 \end{pmatrix}$
$\frac{17173316201}{8}$	471	$\begin{pmatrix} 1 & 259 \\ 0 & 471 \end{pmatrix}$
2176887312	485	$\begin{pmatrix} 1 & 231 \\ 0 & 485 \end{pmatrix}$

Tabela 15 – $p = 8$

Caso $p = 9$

Para $p = 9$ existem 25 raios para os quais existem códigos perfeitos em A_2 , assim como no caso $p = 8$. Na [Tabela 16](#) vemos cada raio e suas respectivas cardinalidade da bola discreta e matriz A. Neste caso, a maior cardinalidade da bola discreta também é 485, bem como no caso anterior.

Caso $p = 9$		
r^2	$N_{A_2}(r)$	A
$\frac{\sqrt{2} + 81\sqrt{6}}{32}$	5	$\begin{pmatrix} 1 & 3 \\ 0 & 5 \end{pmatrix}$
$16\sqrt{2}$	7	$\begin{pmatrix} 1 & 3 \\ 0 & 7 \end{pmatrix}$
$\frac{81(243 + \sqrt{3})}{16\sqrt{2}}$	11	$\begin{pmatrix} 1 & 3 \\ 0 & 11 \end{pmatrix}$
$1296\sqrt{6}$	13	$\begin{pmatrix} 1 & 4 \\ 0 & 13 \end{pmatrix}$
$16(\sqrt{2} + 81\sqrt{6})$	17	$\begin{pmatrix} 1 & 11 \\ 0 & 17 \end{pmatrix}$
$8192\sqrt{2}$	19	$\begin{pmatrix} 1 & 8 \\ 0 & 19 \end{pmatrix}$
$16\sqrt{2}(512 + 81\sqrt{3})$	23	$\begin{pmatrix} 1 & 14 \\ 0 & 23 \end{pmatrix}$
$\frac{1953125 + 81\sqrt{3}}{16\sqrt{2}}$	27	$\begin{pmatrix} 1 & 16 \\ 0 & 27 \end{pmatrix}$
$\frac{\sqrt{2} + 1594323\sqrt{6}}{32}$	31	$\begin{pmatrix} 1 & 6 \\ 0 & 31 \end{pmatrix}$
$\frac{1953125 + 1594323\sqrt{3}}{16\sqrt{2}}$	39	$\begin{pmatrix} 1 & 31 \\ 0 & 39 \end{pmatrix}$
$314928\sqrt{2}$	41	$\begin{pmatrix} 1 & 12 \\ 0 & 41 \end{pmatrix}$
$1296\sqrt{2}(243 + \sqrt{3})$	45	$\begin{pmatrix} 1 & 13 \\ 0 & 45 \end{pmatrix}$
$1296\sqrt{2}(243 + 512\sqrt{3})$	67	$\begin{pmatrix} 1 & 19 \\ 0 & 67 \end{pmatrix}$
$8192\sqrt{2}(512 + 81\sqrt{3})$	77	$\begin{pmatrix} 1 & 48 \\ 0 & 77 \end{pmatrix}$
$\frac{40353607 + 158203125\sqrt{3}}{16\sqrt{2}}$	93	$\begin{pmatrix} 1 & 58 \\ 0 & 93 \end{pmatrix}$

Caso $p = 9$		
r^2	$N_{A_2}(r)$	A
$\frac{81(4782969 + \sqrt{3})}{16\sqrt{2}}$	97	$\begin{pmatrix} 1 & 18 \\ 0 & 97 \end{pmatrix}$
$\frac{81(4782969 + 1953125\sqrt{3})}{16\sqrt{2}}$	105	$\begin{pmatrix} 3 & 23 \\ 0 & 35 \end{pmatrix}$
$16\sqrt{2}(1953125 + 41472\sqrt{3})$	115	$\begin{pmatrix} 1 & 21 \\ 0 & 115 \end{pmatrix}$
$\frac{2357947691 + 158203125\sqrt{3}}{16\sqrt{2}}$	149	$\begin{pmatrix} 1 & 27 \\ 0 & 149 \end{pmatrix}$
$\frac{2357947691 + 3268642167\sqrt{3}}{16\sqrt{2}}$	187	$\begin{pmatrix} 1 & 72 \\ 0 & 187 \end{pmatrix}$
$\frac{10604499373 + 3268642167\sqrt{3}}{16\sqrt{2}}$	203	$\begin{pmatrix} 1 & 78 \\ 0 & 203 \end{pmatrix}$
$\frac{81(474609375 + 40353607\sqrt{3})}{16\sqrt{2}}$	263	$\begin{pmatrix} 1 & 35 \\ 0 & 263 \end{pmatrix}$
$\frac{19683(1953125 + 1594323\sqrt{3})}{16\sqrt{2}}$	313	$\begin{pmatrix} 1 & 176 \\ 0 & 313 \end{pmatrix}$
$\frac{322687697779 + 190993762971\sqrt{3}}{16\sqrt{2}}$	471	$\begin{pmatrix} 1 & 259 \\ 0 & 471 \end{pmatrix}$
$314928(\sqrt{2} + 41472\sqrt{6})$	485	$\begin{pmatrix} 1 & 231 \\ 0 & 485 \end{pmatrix}$

Tabela 16 – $p = 9$

Caso $p = 10$

Para $p = 10$ existem 32 raios para os quais existem códigos perfeitos em A_2 . Na [Tabela 17](#) vemos cada raio e suas respectivas cardinalidade da bola discreta e matriz A . Neste caso, a maior cardinalidade da bola discreta é 739. Perceba que, a quantidade de códigos perfeitos segue aumentando conforme aumentamos o valor de p , assim como o valor referente à maior cardinalidade da bola discreta.

Caso $p = 10$		
r^2	$N_{A_2}(r)$	A
$\frac{61}{8}$	5	$\begin{pmatrix} 1 & 3 \\ 0 & 5 \end{pmatrix}$

Caso $p = 10$		
r^2	$N_{A_2}(r)$	A
32	7	$\begin{pmatrix} 1 & 3 \\ 0 & 7 \end{pmatrix}$
$\frac{14823}{8}$	11	$\begin{pmatrix} 1 & 3 \\ 0 & 11 \end{pmatrix}$
7776	13	$\begin{pmatrix} 1 & 4 \\ 0 & 13 \end{pmatrix}$
7808	17	$\begin{pmatrix} 1 & 11 \\ 0 & 17 \end{pmatrix}$
32768	19	$\begin{pmatrix} 1 & 8 \\ 0 & 19 \end{pmatrix}$
40544	23	$\begin{pmatrix} 1 & 14 \\ 0 & 23 \end{pmatrix}$
$\frac{2441467}{8}$	27	$\begin{pmatrix} 1 & 16 \\ 0 & 27 \end{pmatrix}$
$\frac{3587227}{8}$	31	$\begin{pmatrix} 1 & 6 \\ 0 & 31 \end{pmatrix}$
$\frac{6028633}{8}$	39	$\begin{pmatrix} 1 & 31 \\ 0 & 39 \end{pmatrix}$
1889568	41	$\begin{pmatrix} 1 & 12 \\ 0 & 41 \end{pmatrix}$
1897344	45	$\begin{pmatrix} 1 & 13 \\ 0 & 45 \end{pmatrix}$
9852192	67	$\begin{pmatrix} 1 & 19 \\ 0 & 67 \end{pmatrix}$
41517056	77	$\begin{pmatrix} 1 & 48 \\ 0 & 77 \end{pmatrix}$
$\frac{663880531}{8}$	93	$\begin{pmatrix} 1 & 58 \\ 0 & 93 \end{pmatrix}$
$\frac{871696161}{8}$	97	$\begin{pmatrix} 1 & 18 \\ 0 & 97 \end{pmatrix}$
$\frac{1464957819}{8}$	105	$\begin{pmatrix} 3 & 23 \\ 0 & 35 \end{pmatrix}$
320462624	115	$\begin{pmatrix} 1 & 21 \\ 0 & 115 \end{pmatrix}$
771665024	137	$\begin{pmatrix} 1 & 25 \\ 0 & 137 \end{pmatrix}$

Caso $p = 10$		
r^2	$N_{A_2}(r)$	A
$\frac{6484356211}{8}$	141	$\begin{pmatrix} 1 & 22 \\ 0 & 141 \end{pmatrix}$
$\frac{7077617869}{8}$	149	$\begin{pmatrix} 1 & 27 \\ 0 & 149 \end{pmatrix}$
$\frac{23644727527}{8}$	187	$\begin{pmatrix} 1 & 72 \\ 0 & 187 \end{pmatrix}$
$\frac{51624994339}{8}$	203	$\begin{pmatrix} 1 & 78 \\ 0 & 203 \end{pmatrix}$
17192934944	247	$\begin{pmatrix} 1 & 33 \\ 0 & 247 \end{pmatrix}$
$\frac{161322969033}{8}$	263	$\begin{pmatrix} 1 & 35 \\ 0 & 263 \end{pmatrix}$
$\frac{355984750017}{8}$	313	$\begin{pmatrix} 1 & 176 \\ 0 & 313 \end{pmatrix}$
110297238368	367	$\begin{pmatrix} 1 & 102 \\ 0 & 367 \end{pmatrix}$
187514600832	389	$\begin{pmatrix} 1 & 41 \\ 0 & 389 \end{pmatrix}$
395937500000	471	$\begin{pmatrix} 1 & 259 \\ 0 & 471 \end{pmatrix}$
470186874144	485	$\begin{pmatrix} 1 & 231 \\ 0 & 485 \end{pmatrix}$
790184984576	537	$\begin{pmatrix} 1 & 415 \\ 0 & 537 \end{pmatrix}$
4177883191392	739	$\begin{pmatrix} 1 & 199 \\ 0 & 739 \end{pmatrix}$

Tabela 17 – $p = 10$ Caso $p = 11$

Para $p = 11$ existem 32 raios para os quais existem códigos perfeitos em A_2 . Na [Tabela 18](#) vemos cada raio e suas respectivas cardinalidade da bola discreta e matriz A . No caso $p = 11$, a maior cardinalidade da bola discreta é 739. Note que, a quantidade de códigos perfeitos e o valor referente à cardinalidade da maior bola discreta são iguais nos casos $p = 10$ e $p = 11$.

Caso $p = 11$		
r^2	$N_{A_2}(r)$	A
$\frac{\sqrt{2} + 243\sqrt{6}}{64}$	5	$\begin{pmatrix} 1 & 3 \\ 0 & 5 \end{pmatrix}$
$32\sqrt{2}$	7	$\begin{pmatrix} 1 & 3 \\ 0 & 7 \end{pmatrix}$
$\frac{243(729 + \sqrt{3})}{32\sqrt{2}}$	11	$\begin{pmatrix} 1 & 3 \\ 0 & 11 \end{pmatrix}$
$7776\sqrt{6}$	13	$\begin{pmatrix} 1 & 4 \\ 0 & 13 \end{pmatrix}$
$32(\sqrt{2} + 243\sqrt{6})$	17	$\begin{pmatrix} 1 & 11 \\ 0 & 17 \end{pmatrix}$
$65536\sqrt{2}$	19	$\begin{pmatrix} 1 & 8 \\ 0 & 19 \end{pmatrix}$
$32\sqrt{2}(2048 + 243\sqrt{3})$	23	$\begin{pmatrix} 1 & 14 \\ 0 & 23 \end{pmatrix}$
$\frac{48828125 + 243\sqrt{3}}{32\sqrt{2}}$	27	$\begin{pmatrix} 1 & 16 \\ 0 & 27 \end{pmatrix}$
$\frac{\sqrt{2} + 43046721\sqrt{6}}{64}$	31	$\begin{pmatrix} 1 & 6 \\ 0 & 31 \end{pmatrix}$
$\frac{48828125 + 43046721\sqrt{3}}{32\sqrt{2}}$	39	$\begin{pmatrix} 1 & 31 \\ 0 & 39 \end{pmatrix}$
$5668704\sqrt{2}$	41	$\begin{pmatrix} 1 & 12 \\ 0 & 41 \end{pmatrix}$
$7776\sqrt{2}(729 + \sqrt{3})$	45	$\begin{pmatrix} 1 & 13 \\ 0 & 45 \end{pmatrix}$
$7776\sqrt{2}(729 + 2048\sqrt{3})$	67	$\begin{pmatrix} 1 & 19 \\ 0 & 67 \end{pmatrix}$
$65536\sqrt{2}(2048 + 243\sqrt{3})$	77	$\begin{pmatrix} 1 & 48 \\ 0 & 77 \end{pmatrix}$
$\frac{1977326743 + 11865234375\sqrt{3}}{32\sqrt{2}}$	93	$\begin{pmatrix} 1 & 58 \\ 0 & 93 \end{pmatrix}$
$\frac{243(129140163 + \sqrt{3})}{32\sqrt{2}}$	97	$\begin{pmatrix} 1 & 18 \\ 0 & 97 \end{pmatrix}$
$\frac{243(129140163 + 48828125\sqrt{3})}{32\sqrt{2}}$	105	$\begin{pmatrix} 3 & 23 \\ 0 & 35 \end{pmatrix}$
$32\sqrt{2}(48828125 + 497664\sqrt{3})$	115	$\begin{pmatrix} 1 & 21 \\ 0 & 115 \end{pmatrix}$

Caso $p = 11$		
r^2	$N_{A_2}(r)$	A
$32\sqrt{2}(48828125 + 43046721\sqrt{3})$	137	$\begin{pmatrix} 1 & 25 \\ 0 & 137 \end{pmatrix}$
$\frac{243\sqrt{3/2}}{32} + (\frac{1}{\sqrt{2}} + 5\sqrt{2})^1 1$	141	$\begin{pmatrix} 1 & 22 \\ 0 & 141 \end{pmatrix}$
$\frac{285311670611 + 11865234375\sqrt{3}}{32\sqrt{2}}$	149	$\begin{pmatrix} 1 & 27 \\ 0 & 149 \end{pmatrix}$
$\frac{285311670611 + 480490398549\sqrt{3}}{32\sqrt{2}}$	187	$\begin{pmatrix} 1 & 72 \\ 0 & 187 \end{pmatrix}$
$\frac{1792160394037 + 480490398549\sqrt{3}}{32\sqrt{2}}$	203	$\begin{pmatrix} 1 & 78 \\ 0 & 203 \end{pmatrix}$
$32\sqrt{2}(1977326743 + 1019215872\sqrt{3})$	247	$\begin{pmatrix} 1 & 33 \\ 0 & 247 \end{pmatrix}$
$\frac{243(35595703125 + 1977326743\sqrt{3})}{32\sqrt{2}}$	263	$\begin{pmatrix} 1 & 35 \\ 0 & 263 \end{pmatrix}$
$\frac{177147(48828125 + 43046721\sqrt{3})}{32\sqrt{2}}$	313	$\begin{pmatrix} 1 & 176 \\ 0 & 313 \end{pmatrix}$
$32\sqrt{2}(8589934592 + 11865234375\sqrt{3})$	367	$\begin{pmatrix} 1 & 102 \\ 0 & 367 \end{pmatrix}$
$7776\sqrt{2}(129140163 + 48828125\sqrt{3})$	389	$\begin{pmatrix} 1 & 41 \\ 0 & 389 \end{pmatrix}$
$1562500000\sqrt{2}(2048 + 243\sqrt{3})$	471	$\begin{pmatrix} 1 & 259 \\ 0 & 471 \end{pmatrix}$
$5668704(\sqrt{2} + 497664\sqrt{6})$	485	$\begin{pmatrix} 1 & 231 \\ 0 & 485 \end{pmatrix}$
$65536\sqrt{2}(48828125 + 43046721\sqrt{3})$	537	$\begin{pmatrix} 1 & 415 \\ 0 & 537 \end{pmatrix}$
$7776\sqrt{2}(3057647616 + 1977326743\sqrt{3})$	739	$\begin{pmatrix} 1 & 199 \\ 0 & 739 \end{pmatrix}$

Tabela 18 – $p = 11$

Caso $p = 12$

Dando continuidade, para $p = 12$ existem 32 raios para os quais existem códigos perfeitos em A_2 . Na [Tabela 19](#) vemos cada raio e suas respectivas cardinalidade da bola discreta e matriz A. No caso $p = 12$, a maior cardinalidade da bola discreta é 739. Para

valores de $p = 10$, $p = 11$ e $p = 12$, obtemos a mesma quantidade de códigos perfeitos e o mesmo valor da maior cardinalidade da bola discreta. Isso pode nos levar a crer que, as bolas discretas para os próximos valores de p possam ter um formato igual ao desses últimos casos. E assim, para os próximos valores de p já teríamos a quantidade de códigos perfeitos e quantos pontos possui a bola discreta de cada um deles. Tendo em vista que, o número de pontos das bolas discretas a partir de $p = 5$ se repetem em todos os próximos casos de $p > 5$. Ou seja, a partir de $p = 5$ apenas são acrescentadas cardinalidades de bolas discreta distintas e se mantém as cardinalidades encontradas no caso $p = 5$.

Caso $p = 12$		
r^2	$N_{A_2}(r)$	A
$\frac{365}{32}$	5	$\begin{pmatrix} 1 & 3 \\ 0 & 5 \end{pmatrix}$
64	7	$\begin{pmatrix} 1 & 3 \\ 0 & 7 \end{pmatrix}$
$\frac{266085}{32}$	11	$\begin{pmatrix} 1 & 3 \\ 0 & 11 \end{pmatrix}$
46656	13	$\begin{pmatrix} 1 & 4 \\ 0 & 13 \end{pmatrix}$
46720	17	$\begin{pmatrix} 1 & 11 \\ 0 & 17 \end{pmatrix}$
262144	19	$\begin{pmatrix} 1 & 8 \\ 0 & 19 \end{pmatrix}$
308800	23	$\begin{pmatrix} 1 & 14 \\ 0 & 23 \end{pmatrix}$
$\frac{122070677}{32}$	27	$\begin{pmatrix} 1 & 16 \\ 0 & 27 \end{pmatrix}$
$\frac{193710245}{32}$	31	$\begin{pmatrix} 1 & 6 \\ 0 & 31 \end{pmatrix}$
$\frac{315780557}{32}$	39	$\begin{pmatrix} 1 & 31 \\ 0 & 39 \end{pmatrix}$
34012224	41	$\begin{pmatrix} 1 & 12 \\ 0 & 41 \end{pmatrix}$
34058880	45	$\begin{pmatrix} 1 & 13 \\ 0 & 45 \end{pmatrix}$
225115200	67	$\begin{pmatrix} 1 & 19 \\ 0 & 67 \end{pmatrix}$

Caso $p = 12$		
r^2	$N_{A_2}(r)$	A
1264844800	77	$\begin{pmatrix} 1 & 48 \\ 0 & 77 \end{pmatrix}$
$\frac{95909901413}{32}$	93	$\begin{pmatrix} 1 & 58 \\ 0 & 93 \end{pmatrix}$
$\frac{141214768605}{32}$	97	$\begin{pmatrix} 1 & 18 \\ 0 & 97 \end{pmatrix}$
$\frac{230204026053}{32}$	105	$\begin{pmatrix} 3 & 23 \\ 0 & 35 \end{pmatrix}$
15816102976	115	$\begin{pmatrix} 1 & 21 \\ 0 & 115 \end{pmatrix}$
40419911296	137	$\begin{pmatrix} 1 & 25 \\ 0 & 137 \end{pmatrix}$
$\frac{1569214188725}{32}$	141	$\begin{pmatrix} 1 & 22 \\ 0 & 141 \end{pmatrix}$
$\frac{1658203446173}{32}$	149	$\begin{pmatrix} 1 & 27 \\ 0 & 149 \end{pmatrix}$
$\frac{6614363373125}{32}$	187	$\begin{pmatrix} 1 & 72 \\ 0 & 187 \end{pmatrix}$
$\frac{16694191746005}{32}$	203	$\begin{pmatrix} 1 & 78 \\ 0 & 203 \end{pmatrix}$
1668600170560	247	$\begin{pmatrix} 1 & 33 \\ 0 & 247 \end{pmatrix}$
$\frac{69918318130077}{32}$	263	$\begin{pmatrix} 1 & 35 \\ 0 & 263 \end{pmatrix}$
$\frac{167818734992637}{32}$	313	$\begin{pmatrix} 1 & 176 \\ 0 & 313 \end{pmatrix}$
15788671511104	367	$\begin{pmatrix} 1 & 102 \\ 0 & 367 \end{pmatrix}$
29466115334784	389	$\begin{pmatrix} 1 & 41 \\ 0 & 389 \end{pmatrix}$
75390625000000	471	$\begin{pmatrix} 1 & 259 \\ 0 & 471 \end{pmatrix}$
101559990680640	485	$\begin{pmatrix} 1 & 231 \\ 0 & 485 \end{pmatrix}$
165559956668416	537	$\begin{pmatrix} 1 & 415 \\ 0 & 537 \end{pmatrix}$

Caso $p = 12$		
r^2	$N_{A_2}(r)$	A
1216409524338240	739	$\begin{pmatrix} 1 & 199 \\ 0 & 739 \end{pmatrix}$

Tabela 19 – $p = 12$

Caso $p = 13$

Para $p = 13$ existem 33 raios para os quais existem códigos perfeitos em A_2 . Na [Tabela 20](#) vemos cada raio e suas respectivas cardinalidade da bola discreta e matriz A . Neste caso, a maior cardinalidade da bola discreta é 821. Logo, a hipótese levantada anteriormente não se sustenta, uma vez que a quantidade de raios para os quais existem códigos perfeitos aumentou novamente, assim como o valor da maior cardinalidade da bola discreta.

Caso $p = 13$		
r^2	$N_{A_2}(r)$	A
$\frac{\sqrt{2} + 729\sqrt{6}}{128}$	5	$\begin{pmatrix} 1 & 3 \\ 0 & 5 \end{pmatrix}$
$64\sqrt{2}$	7	$\begin{pmatrix} 1 & 3 \\ 0 & 7 \end{pmatrix}$
$\frac{729(2187 + \sqrt{3})}{64\sqrt{2}}$	11	$\begin{pmatrix} 1 & 3 \\ 0 & 11 \end{pmatrix}$
$46656\sqrt{6}$	13	$\begin{pmatrix} 1 & 4 \\ 0 & 13 \end{pmatrix}$
$64(\sqrt{2} + 729\sqrt{6})$	17	$\begin{pmatrix} 1 & 11 \\ 0 & 17 \end{pmatrix}$
$524288\sqrt{2}$	19	$\begin{pmatrix} 1 & 8 \\ 0 & 19 \end{pmatrix}$
$64\sqrt{2}(8192 + 729\sqrt{3})$	23	$\begin{pmatrix} 1 & 14 \\ 0 & 23 \end{pmatrix}$
$\frac{1220703125 + 729\sqrt{3}}{64\sqrt{2}}$	27	$\begin{pmatrix} 1 & 16 \\ 0 & 27 \end{pmatrix}$
$\frac{\sqrt{2} + 1162261467\sqrt{6}}{128}$	31	$\begin{pmatrix} 1 & 6 \\ 0 & 31 \end{pmatrix}$

Caso $p = 13$		
r^2	$N_{A_2}(r)$	A
$\frac{1220703125 + 1162261467\sqrt{3}}{64\sqrt{2}}$	39	$\begin{pmatrix} 1 & 31 \\ 0 & 39 \end{pmatrix}$
$102036672\sqrt{2}$	41	$\begin{pmatrix} 1 & 12 \\ 0 & 41 \end{pmatrix}$
$46656\sqrt{2}(2187 + \sqrt{3})$	45	$\begin{pmatrix} 1 & 13 \\ 0 & 45 \end{pmatrix}$
$\frac{96889010407 + 1162261467\sqrt{3}}{64\sqrt{2}}$	67	$\begin{pmatrix} 1 & 19 \\ 0 & 67 \end{pmatrix}$
$524288\sqrt{2}(8192 + 729\sqrt{3})$	77	$\begin{pmatrix} 1 & 48 \\ 0 & 77 \end{pmatrix}$
$\frac{889892578125\sqrt{3/2}}{64} + \left(\frac{5}{\sqrt{2}} + \sqrt{2}\right)^{13}$	93	$\begin{pmatrix} 1 & 58 \\ 0 & 93 \end{pmatrix}$
$\frac{729(3486784401 + \sqrt{3})}{64\sqrt{2}}$	97	$\begin{pmatrix} 1 & 18 \\ 0 & 97 \end{pmatrix}$
$\frac{729(3486784401 + 1220703125\sqrt{3})}{64\sqrt{2}}$	105	$\begin{pmatrix} 3 & 23 \\ 0 & 35 \end{pmatrix}$
$64\sqrt{2}(1220703125 + 5971968\sqrt{3})$	115	$\begin{pmatrix} 1 & 21 \\ 0 & 115 \end{pmatrix}$
$64\sqrt{2}(1220703125 + 1162261467\sqrt{3})$	137	$\begin{pmatrix} 1 & 25 \\ 0 & 137 \end{pmatrix}$
$\frac{729\sqrt{3/2}}{64} + \left(\frac{1}{\sqrt{2}} + 5\sqrt{2}\right)^{13}$	141	$\begin{pmatrix} 1 & 22 \\ 0 & 141 \end{pmatrix}$
$\frac{889892578125\sqrt{3/2}}{64} + \left(\frac{5}{\sqrt{2}} + 3\sqrt{2}\right)^{13}$	149	$\begin{pmatrix} 1 & 27 \\ 0 & 149 \end{pmatrix}$
$\frac{70632088586703\sqrt{3/2}}{64} + \left(\frac{7}{\sqrt{2}} + 2\sqrt{2}\right)^{13}$	187	$\begin{pmatrix} 1 & 72 \\ 0 & 187 \end{pmatrix}$
$\frac{70632088586703\sqrt{3/2}}{64} + \left(\frac{7}{\sqrt{2}} + 3\sqrt{2}\right)^{13}$	203	$\begin{pmatrix} 1 & 78 \\ 0 & 203 \end{pmatrix}$
$64\sqrt{2}(96889010407 + 48922361856\sqrt{3})$	247	$\begin{pmatrix} 1 & 33 \\ 0 & 247 \end{pmatrix}$
$\frac{729(2669677734375 + 96889010407\sqrt{3})}{64\sqrt{2}}$	263	$\begin{pmatrix} 1 & 35 \\ 0 & 263 \end{pmatrix}$
$4294967296\sqrt{2}(8192 + 729\sqrt{3})$	313	$\begin{pmatrix} 1 & 176 \\ 0 & 313 \end{pmatrix}$
$64\sqrt{2}(549755813888 + 889892578125\sqrt{3})$	367	$\begin{pmatrix} 1 & 102 \\ 0 & 367 \end{pmatrix}$

Caso $p = 13$		
r^2	$N_{A_2}(r)$	A
$46656\sqrt{2}(3486784401 + 1220703125\sqrt{3})$	389	$\begin{pmatrix} 1 & 41 \\ 0 & 389 \end{pmatrix}$
$78125000000\sqrt{2}(8192 + 729\sqrt{3})$	471	$\begin{pmatrix} 1 & 259 \\ 0 & 471 \end{pmatrix}$
$102036672(\sqrt{2} + 5971968\sqrt{6})$	485	$\begin{pmatrix} 1 & 231 \\ 0 & 485 \end{pmatrix}$
$524288\sqrt{2}(1220703125 + 1162261467\sqrt{3})$	537	$\begin{pmatrix} 1 & 415 \\ 0 & 537 \end{pmatrix}$
$46656\sqrt{2}(146767085568 + 96889010407\sqrt{3})$	739	$\begin{pmatrix} 1 & 199 \\ 0 & 739 \end{pmatrix}$
$\frac{1220703125(1220703125 + 1162261467\sqrt{3})}{64\sqrt{2}}$	821	$\begin{pmatrix} 1 & 221 \\ 0 & 821 \end{pmatrix}$

Tabela 20 – $p = 13$

4.2.2 Códigos Perfeitos em A_3

Agora vamos analisar os casos de códigos perfeitos em dimensão 3. Para cada valor de p vamos apresentar o conjunto $N_{A_3}(r_i)$, que lista todas as cardinalidades de bolas discretas que ladrilham o reticulado ambiente A_3 .

$p = 2$	$N_{A_3}(r_i) = \{13, 19\}$
$p = 3$	$N_{A_3}(r_i) = \{9, 13, 17, 19, 27, 59\}$
$p = 4$	$N_{A_3}(r_i) = \{9, 13, 17, 19, 27, 59, 139\}$
$p = 5$	$N_{A_3}(r_i) = \{9, 13, 17, 19, 27, 35, 59, 139\}$
$p = 6$	$N_{A_3}(r_i) = \{9, 13, 17, 19, 27, 35, 59, 139\}$
$p = 7$	$N_{A_3}(r_i) = \{9, 13, 17, 19, 27, 35, 59, 139\}$
$p = 8$	$N_{A_3}(r_i) = \{9, 13, 17, 19, 27, 35, 59, 139\}$

Tabela 21 – Códigos perfeitos em A_3

Analisando a [Tabela 21](#) facilmente vemos em comparação com a dimensão 2, que o número de códigos perfeitos para A_3 é menor quando olhamos para os respectivos valores de p . Contudo, é possível observar o mesmo padrão da dimensão anterior, em que bolas intermediárias que antes não ladrilhavam o reticulado A_3 , agora com o aumento do valor de p passaram a ser ladrilhos.

4.3 Conclusões

Para analisar o formato das bolas discretas, vamos observar as Figuras 22, 23 e 24, que apresentam as bolas discretas que ladrilham A_2 . Escolhemos a cardinalidade 13 que está presente nos casos de $p = 2$, $p = 4$ e $p = 10$, e a bola com a maior cardinalidade de cada caso para ilustrarmos.

Na Figura 22 temos a representação das bolas com cardinalidades 13 e 127, que ladrilham o reticulado A_2 . Perceba que a bola com maior cardinalidade tem um formato mais arredondado que a bola de cardinalidade 13.

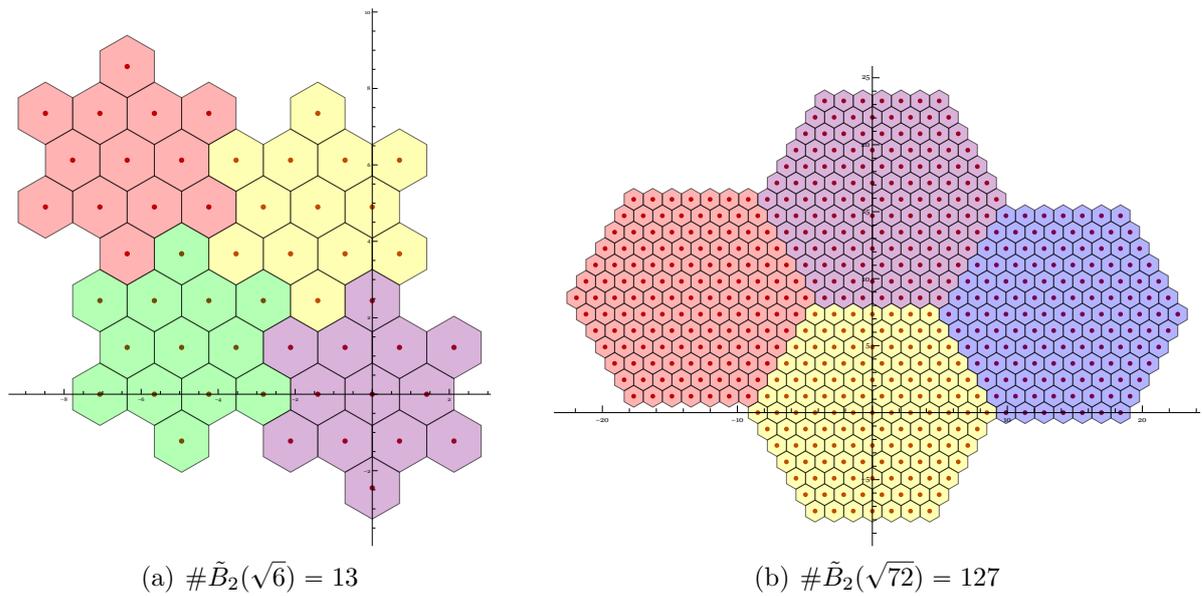


Figura 22 – Códigos perfeitos em A_2 na métrica l_2

Na Figura 23 também temos a representação da bola discreta com cardinalidade 13, só que considerando a métrica l_4 . Vale lembrar que da métrica l_2 para as demais, perdemos algumas cardinalidades de bolas intermediárias. E nesta figura, é possível observar que a bola que representa a maior cardinalidade tem um formato mais parecido com um quadrado, enquanto na métrica l_2 , o formato da bola com maior cardinalidade é mais próxima de um círculo. Ou seja, ganhamos raios intermediários com formato mais quadrado que ladrilham o reticulado ambiente A_2 .

Na Figura 24 temos a representação das bolas com cardinalidades 13 e 739, que ladrilham o reticulado A_2 na métrica l_{10} . Perceba que, quando aumentamos o valor de p aumentamos também a quantidade de códigos perfeitos e o valor da maior cardinalidade da bola discreta. Perceba nas Figuras 22, 23 e 24 que a subfigura (a) que representam as bolas discretas com cardinalidade 13 são idênticas. Isso se repete nos demais casos quando a mesma cardinalidade de bola também for ladrilho de A_2 nas próximas métricas.

Com base nas tabelas e figuras acima, podemos observar que à medida que

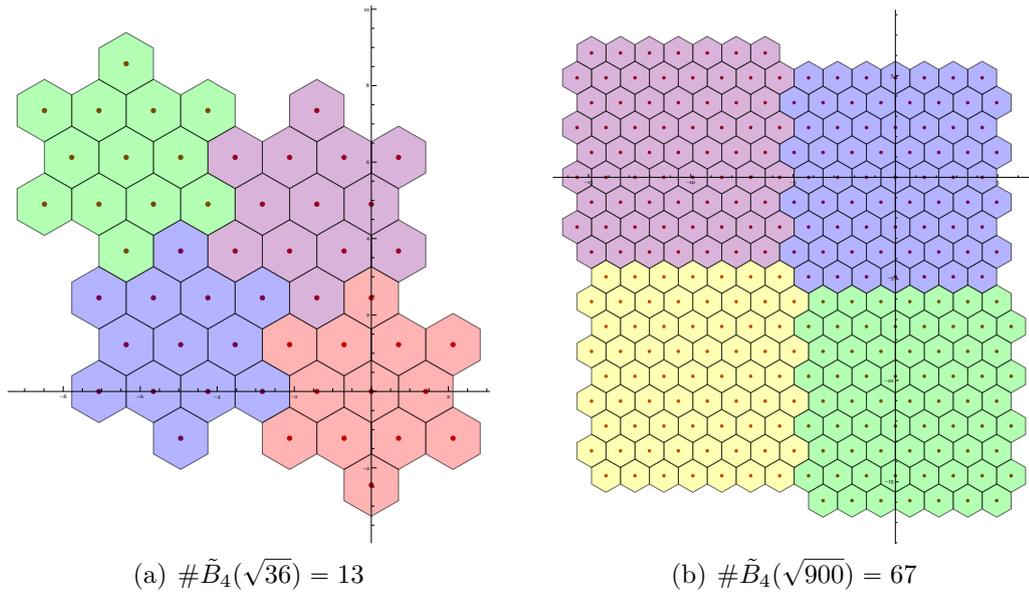


Figura 23 – Códigos perfeitos em A_2 na métrica l_4

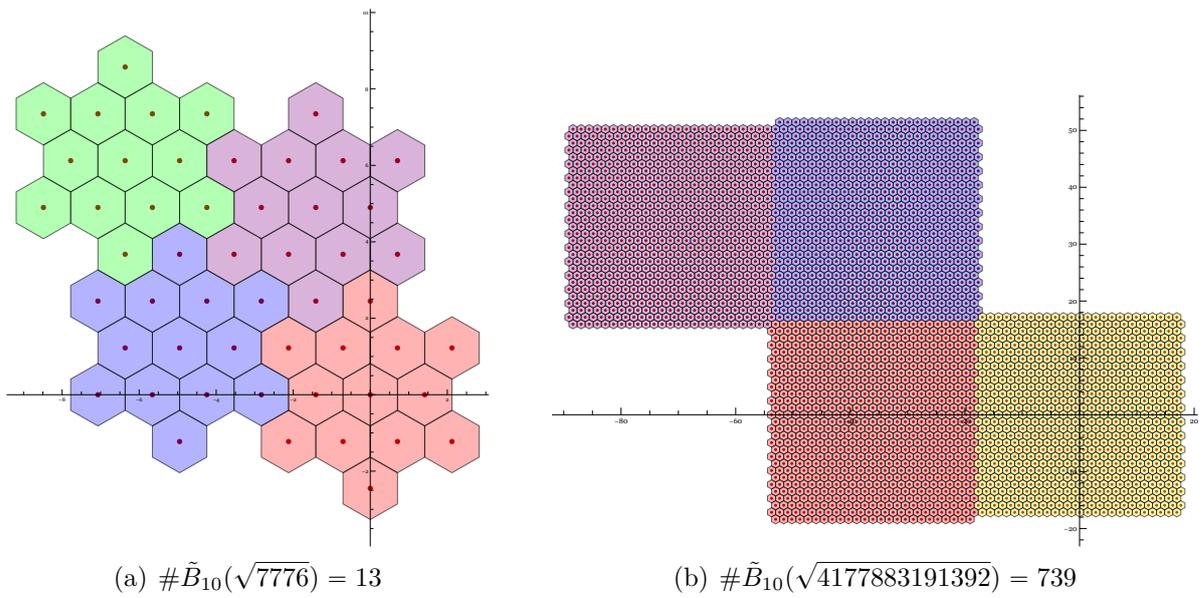


Figura 24 – Códigos perfeitos em A_2 na métrica l_{10}

o valor de p cresce, as bolas ficam com formato cada vez mais quadrado. Sendo assim, espera-se que conforme aumentarmos o valor de p , a quantidade de códigos perfeitos em A_2 também aumente. Visto que, o aumento do valor de p implica em bolas com o formato mais quadrado. Além disso, podemos “ganhar” bolas discretas intermediárias que anteriormente não ladrilhavam o reticulado A_2 para valores de p inferiores. Assim como as bolas de cardinalidade superior podem por ventura ladrilhar A_2 para valores de p superiores. Ainda podemos afirmar que quando alteramos o valor de p , permitimos outros formatos de ladrilhos.

Retomando os casos de $p = 2$ para $p = 3$, vimos que perdemos algumas

cardinalidades de bola discreta e ganhamos outras. Essas cardinalidades que foram perdidas são dos formatos mais arredondados. Visto que, conforme aumentamos o valor de p aumentamos a quantidade de códigos perfeitos. Esse padrão também acontece para os demais casos, quando ganhamos os ladrilhos intermediários.

4.4 Considerações Finais

Com base nas simulações realizadas, concluímos que conforme crescemos o valor de p temos uma quantidade maior de ladrilhos para o reticulado ambiente A_2 associados às bolas discretas.

Outra coisa que notamos foi a existência de simetria nos códigos perfeitos de A_2 , ou seja, nos dados obtidos pelo algoritmo há duas soluções (ou mais) possíveis para um mesmo raio. Nesses casos, consideramos os códigos perfeitos cuja matriz A está vide o [Exemplo 4.1.1](#).

Uma perspectiva futura é realizar ajustes no algoritmo para cortar as soluções simétricas, visando assim diminuir o tempo de busca. Esse ajuste se faz necessário quando for subir a dimensão e para valores de p grandes.

Referências

- ALVES, C.; ANDRADE, A. A. d. *Reticulados via corpos ciclotômicos*. [S.l.]: São Paulo: Editora UNESP Digital, 2014. Citado na página 44.
- CAMPELLO, A.; JORGE, G. C.; COSTA, S. I. Reticulados q -ários na norma l_p e uma generalização da métrica de lee. *XXX Simpósio Brasileiro de Telecomunicações (SBrT), Brasília-DF*, 2012. Citado 3 vezes nas páginas 41, 43 e 44.
- CONWAY, J. H.; SLOANE, N. J. A. *Sphere packings, lattices and groups*. [S.l.]: Springer Science & Business Media, 2013. v. 290. Citado 10 vezes nas páginas 18, 27, 28, 30, 31, 32, 33, 34, 35 e 41.
- COSTA, S. I.; CAMPELLO, A.; JORGE, G. C.; STRAPASSON, J. E.; QURESHI, C. Codes and lattices in the l_p metric. In: IEEE. *2014 Information Theory and Applications Workshop (ITA)*. [S.l.], 2014. p. 1–4. Citado na página 37.
- COSTA, S. I.; OGGIER, F.; CAMPELLO, A.; BELFIORE, J.-C.; VITERBO, E. *Lattices applied to coding for reliable and secure communications*. [S.l.]: Springer, 2017. Citado 11 vezes nas páginas 17, 25, 29, 30, 31, 32, 33, 34, 35, 37 e 42.
- FINCKE, U.; POHST, M. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of computation*, v. 44, n. 170, p. 463–471, 1985. Citado na página 54.
- FIRER, M.; ALVES, M. M. S.; PINHEIRO, J. A.; PANEK, L. *Poset codes: partial orders, metrics and coding theory*. [S.l.]: Springer, 2018. Citado na página 39.
- GOLOMB, S. W.; WELCH, L. R. Perfect codes in the lee metric and the packing of polyominoes. *SIAM Journal on Applied Mathematics*, SIAM, v. 18, n. 2, p. 302–317, 1970. Citado 2 vezes nas páginas 11 e 44.
- HEFEZ, A.; VILLELA, M. L. T. *Códigos corretores de erros*. [S.l.]: Instituto de Matematica Pura e Aplicada, 2008. Citado 2 vezes nas páginas 37 e 39.
- HORAK, P.; ALBDAIWI, B. F. Diameter perfect lee codes. *IEEE transactions on information theory*, IEEE, v. 58, n. 8, p. 5490–5499, 2012. Citado na página 50.
- HUFFMAN, W. C.; PLESS, V. *Fundamentals of error-correcting codes*. [S.l.]: Cambridge university press, 2010. Citado na página 40.
- JORGE, G. C. *Reticulados q -ários e algébricos*. Tese (Doutorado). Citado na página 28.
- JÚNIOR, A. C. d. A. C. *Reticulados, projeções e aplicações à teoria da informação*. Tese (Doutorado) — IMECC - UNICAMP, 2014. Citado na página 41.
- LAVOR, C.; ALVES, M.; SIQUEIRA, R.; COSTA, S. Uma introdução a teoria de códigos. *Notas em Matemática Aplicada*, v. 21, 2006. Citado 4 vezes nas páginas 20, 21, 23 e 37.
- LEE, C. Some properties of nonbinary error-correcting codes. *IRE Transactions on Information Theory*, IEEE, v. 4, n. 2, p. 77–82, 1958. Citado na página 40.

- LINT, J. H. V. A survey of perfect codes. *The Rocky Mountain Journal of Mathematics*, JSTOR, v. 5, n. 2, p. 199–224, 1975. Citado 2 vezes nas páginas 11 e 44.
- MACWILLIAMS, F. J.; SLOANE, N. J. A. *The theory of error-correcting codes*. [S.l.]: Elsevier, 1977. v. 16. Citado 2 vezes nas páginas 37 e 40.
- MATOS, R. da S. *Um estudo sobre códigos perfeitos com as métricas lp e do grafo*. Tese (Doutorado) — [sn], 2018. Citado na página 44.
- MICCIANCIO, D.; GOLDWASSER, S. *Complexity of lattice problems: a cryptographic perspective*. [S.l.]: Springer Science & Business Media, 2002. v. 671. Citado na página 26.
- NAVES, L. R. B. A densidade de empacotamentos esféricos em reticulados. *UNICAMP, Campinas, SP*, 2009. Citado na página 26.
- ROGERS, C. Packing and covering, cambridge university press. *London, England*, 1964. Citado na página 21.
- RUSH, J. A.; SLOANE, N. An improvement to the minkowski-hiawka bound for packing superballs. *Mathematika*, London Mathematical Society, v. 34, n. 1, p. 8–18, 1987. Citado na página 27.
- SHANNON, C. E. A mathematical theory of communication. *The Bell system technical journal*, Nokia Bell Labs, v. 27, n. 3, p. 379–423, 1948. Citado 2 vezes nas páginas 11 e 37.
- STRAPASSON, J. E.; STREY, G. Códigos perfeitos bidimensionais em reticulados algébricos. *Proceeding Series of the Brazilian Society of Computational and Applied Mathematics*, v. 8, n. 1, 2021. Citado na página 50.
- STREY, E. *Construções de reticulados a partir de códigos q -ários*. Tese (Doutorado) — Tese de Doutorado, Imecc-Unicamp, 2017. Citado na página 22.
- STREY, G. R. d. A. S. *Códigos perfeitos e ladrilhamentos em diversos reticulados ambientes*. Tese (Doutorado) — [sn], 2020. Citado 5 vezes nas páginas 44, 45, 49, 52 e 54.
- TSUCHIYA, L. Y. *Um estudo de reticulados q -ários com a métrica da soma*. Dissertação (Mestrado) — IMECC - UNICAMP, 2012. Citado 2 vezes nas páginas 37 e 39.