Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Classificação dos sub-reticulados do reticulado hexagonal

por

Geraldo Lúcio Tardin

sob orientação do

Prof. Dr. Antônio de Andrade e Silva

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para a obtenção do título de Mestre em Matemática.

João Pessoa - PB

Março/2002

Classificação dos sub-reticulados do reticulado hexagonal

por

Geraldo Lúcio Tardin

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para a obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Antônio de Andrade e Silva

Prof. Dr. Martinho da Costa Araújo

Prof. Dr. Hélio Pires de Almeida

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Março/2002

Agradecimentos

1. Ao meu orientador, Prof. Dr. Antônio de Andrade e Silva, pela eficaz orientação, pela paciência, pelo incentivo e principalmente pela amizade.

2. Aos demais professores do Departamento de Matemática - UFPB, pela experiência transmitida, especialmente ao Prof. Dr. Hélio Pires de Almeida, por ter contribuído mais diretamente.

3. A todos os colegas do Curso de Mestrado, pelo incentivo e amizade, especialmente aos que contribuíram mais diretamente no decorrer do curso: Almir César Ferreira Cavalcanti, Paulo Roberto Lemos de Messias, Cícero José da Silva, Delano Klinger Alves de Souza, Luciana Rôze de Freitas, Luis Lima de Oliveira Júnior e Claudilene Gomes da Costa.

4. Ao amigo Adelmo Carvalho da Silva, pelo companheirismo e pelas habilidades gastronômicas.

5. Aos colegas do Departamento de Matemática-UFMT, Campus de Rondonópolis, pelo apoio, especialmente aos que me confiaram a vinda para este curso: Martinho da Costa Araújo e Antônio Gonçalves Vicente.

6. À Marizete Gregório Tardin e à Ana Line Gregório Tardin, pela compreensão e pelo apoio.

7. A Antônio Gregório Neto e Hilda Rodrigues Gregório, pelo grande apoio à minha família, durante minha ausência.

Dedicatória

À minha mãe
Maria do Carmo Viana Tardin
Ao meu pai
Luiz José Tardin "in memoriam"
À minha filha
Ana Line Gregório Tardin e
À minha esposa Marizete Gregório Tardin.

Resumo

Classificamos os sub-reticulados não equivalentes do reticulado hexagonal, de índice N. Além disso, introduzimos uma classe de códigos multinível baseada na iteração da construção A generalizada de reticulados de Leech, de um único nível.

Abstract

We classify the inequivalent sublattices of index N of the hexagonal lattice. Moreover, we introduce a class of multilevel codes, based on iterating the single-level generalized Construction A lattices of Leech.

Notação

$\mathbb{F}$ - Alfabeto

R - Anel

$\mathbb{Z}[\omega]$ - Anel dos inteiros de Eisenstein-Jacobi

$\mathbb{Z}_n$ - Anel dos inteiros módulo n

$\mathbb{Z}[x]$ - Anel dos polinômios sobre $\mathbb{Z}$

$\mathcal{C}$ - Código

$(n, k, d)_q$ - Código

$E_{\mathcal{C}}$ - Código do espaço Euclidiano

$[n, k, d]_q$ - Código linear

$\equiv$ - Congruente

$\mathbb{I}$ - Conjunto de índices

$[\Lambda/\Gamma]$ - Conjunto de representantes das classes laterais de Γ em Λ

$\mathbb{Z}$ - Conjunto dos números inteiros

$\mathbb{Q}$ - Conjunto dos números racionais

$\mathbb{R}$ - Conjunto dos números reais

$\langle S \rangle$ - Conjunto gerado por S

A - Construção de Leech

$GF(p)$ - Corpo de Galois com p elementos

$\mathbb{F}_p$ - Corpo finito com p elementos

$\Delta(\Lambda)$ - Densidade de Λ

$\delta(\Lambda)$ - Densidade de centro de Λ

$\det \Lambda$ - Determinante de Λ

$d_H(\mathbf{c}, \mathbf{c}')$ - Distância de Hamming entre $\mathbf{c}$ e $\mathbf{c}'$

$d^2(\mathbf{u}, \mathbf{v})$ - Distância Euclidiana quadrática entre $\mathbf{u}$ e $\mathbf{v}$

$d^2_{\min}(\mathcal{C})$ - Distância Euclidiana quadrática mínima de $\mathcal{C}$

$d_H(\mathcal{C})$ - Distância mínima de Hamming de $\mathcal{C}$

$\Lambda_{\mathcal{C}}$ - Empacotamento esférico em $\mathbb{R}^n$

$E_\rho(\mathbf{c})$ - Esfera de centro $\mathbf{c}$ e raio ρ

$\mathbb{F}^{\mathbb{I}}$ - Espaço de seqüências

$\lambda(\Lambda)$ - Expoente de densidade de Λ

X_x - Função característica

G - Grupo

$t(\Lambda)$ - Grupo das translações por elementos de Λ

φ - Homomorfismo

$[\Lambda : \Gamma]$ - Índice de Γ em Λ

$\inf S$ - Ínfimo do conjunto S

$\cap$ - Interseção

$\cong$ - Isomorfo

$\mathbf{A}$ - Matriz

$\mathbf{M}$ - Matriz geradora de Λ

$\mathbf{M}^*$ - Matriz geradora de Λ^*

$\mathbf{I}_n$ - Matriz identidade de ordem n

$\mathbf{A}^{-1}$ - Matriz inversa de $\mathbf{A}$

$\mathbf{A}^t$ - Matriz transposta de $\mathbf{A}$

$\mathrm{mdc}(a, m)$ - Máximo divisor comum entre a e m

$\min S$ - Mínimo do conjunto S

V - Módulo

V/W - Módulo quociente de V por W

$\|\mathbf{u}\|$ - Norma de $\mathbf{u}$

$N(\mathbf{v})$ - Norma quadrática do vetor $\mathbf{v}$

$\ker \varphi$ - Núcleo do homomorfismo φ

$|S|$ - Número de elementos do conjunto S

p - Número primo

$\forall$ - Para todo

$\gamma(\Lambda)$ - Parâmetro de Hermite de Λ

$W_H(\mathbf{c})$ - Peso de Hamming de $\mathbf{c}$

$W_H(\mathcal{C})$ - Peso mínimo de Hamming de $\mathcal{C}$

$\prod$ - Produto

$(\mathbf{u}, \mathbf{v})$ - Produto interno de $\mathbf{u}$ e $\mathbf{v}$

β - Raio de cobertura

ω - Raíz cúbica da unidade

$R_v(\mathbf{u})$ - Região de Voronoi associada ao vetor $\mathbf{u}$

$\mathbf{F}$ - Região fundamental

Λ - Reticulado

Λ^* - Reticulado dual

A_2 - Reticulado hexagonal

$\mathbf{c}$ - Seqüência

$\left(\frac{a}{p}\right)$ - Símbolo de Legendre

$\sum$ - Soma

T - Transformação linear

$\cup$ - União

$\dot{\cup}$ - União disjunta

$V(\Lambda)$ - Volume da região fundamental de Λ

Sumário

Introdução

O problema clássico do empacotamento esférico, ainda sem solução até hoje, é descobrir como juntar o maior número de esferas idênticas em uma grande região vazia. Se tomarmos como exemplo um hangar, por mais engenhosamente que as esferas sejam arranjadas, em torno de 25% do espaço não será preenchido. Quando os centros das esferas formam um subgrupo discreto de $\mathbb{R}^n$, o empacotamento recebe o nome de reticulado, que é o mais importante conceito no estudo da geometria dos números. Um arranjo familiar é aquele em que os centros das esferas formam o reticulado cúbico de face centrada (usualmente encontrado em bancas de frutas), onde o espaço ocupado pelas esferas é

$$\frac{\pi}{\sqrt{18}} = 0,7405\ldots$$

do espaço total, isto é, o número de esferas é $0,7405\ldots$.do volume do hangar, dividido pelo volume de uma esfera. Por isso dizemos que este empacotamento tem densidade $0,7405\ldots$. Gauss mostrou, em 1831, que dentre os empacotamentos reticulados em $\mathbb{R}^3$, este é o mais denso. Uma observação interessante é que este reticulado é constituído dos pontos de $\mathbb{Z}^3$ cuja soma de suas coordenadas é um número par. Em uma dimensão, o empacotamento mais denso é obviamente o reticulado $\mathbb{Z}$ e em duas dimensões é o reticulado hexagonal, que é gerado pela matriz

$$\begin{pmatrix} 1 & 0 \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$$

e cuja densidade é

$$\frac{\pi}{\sqrt{12}} = 0,9069\ldots$$

Mas este problema não se reduz a 2 ou 3 dimensões, e tem considerável importância prática em dimensões maiores que 3, e isto o torna um dois mais famosos problemas abertos em matemática.

Esta dissertação é constituída de três capítulos. O capítulo 1 destina-se aos conceitos básicos necessários ao desenvolvimento do trabalho, começando por módulos, para daí definirmos reticulado como módulo sobre $\mathbb{Z}$. Ainda, neste capítulo, apresentamos algumas caracterizações algébricas e geométricas sobre reticulados e estudamos seus parâmetros.

No segundo capítulo, apresentamos um método para classificar os sub-reticulados não equivalentes do reticulado hexagonal, tendo como base o artigo intitulado "On sublattices of the hexagonal lattice" de M. Bernstein, N. J. A. Sloane e Paul E. Wright. Antes porém, fornecemos alguns resultados da teoria dos números, que são pré-requisitos para uma melhor compreensão.

O terceiro capítulo tem início com uma seção sobre códigos, porque o principal objetivo é construir empacotamentos esféricos a partir de códigos dados. Existe um grande número de construções dessa natureza, porém enfatizamos a construção A de Leech, que é a mais simples e pode ser obtida a partir de um código binário, e por isso, o empacotamento é uma união de classes laterais de $2\mathbb{Z}^n$. Se esse código for linear, o empacotamento é um reticulado. Para obtermos empacotamentos em dimensões superiores, a construção A é generalizada, tendo como base o código dado e uma partição de reticulados, onde são dados vários exemplos de construções de um único nível, isto é, construções baseadas em partições do tipo Λ/Γ; e para finalizar, apresentamos uma construção ainda mais geral, que é chamada de Construção Multinível, isto é, construção baseada em partição do tipo $\Lambda_0/\Lambda_1/\Lambda_2/\cdots$, para a obtenção de empacotamentos ainda melhores.

Capítulo 1

Resultados Básicos

Neste capítulo apresentaremos alguns resultados básicos sobre anéis, módulos e reticulados que serão necessários ao desenvolvimento deste trabalho. O leitor interessado em mais detalhes pode consultar Cassels [1], Conway e Sloane [2], Forney e Vardy [5], Garcia e Lequain [6], ou Milies [11].

1.1 Módulos

Um *anel* é um conjunto não vazio R munido de duas operações binárias, a adição

$$(r, s) \longmapsto r + s$$

e a multiplicação

$$(r, s) \longmapsto rs$$

tais que as seguintes propriedades valem:

1. R é um grupo comutativo com relação à operação de adição.
2. $r(st) = (rs)t$ para quaisquer $r, s, t \in R$.
3. $r(s + t) = rs + rt, (r + s)t = rt + st$, para quaisquer $r, s, t \in R$.

Se em um anel R, as propriedades

4. Existe $1 \in R$ tal que $r1 = 1r = r$, para todo $r \in R$ e
5. $rs = sr$, para quaisquer $r, s \in R$

são verificadas, dizemos que R é um *anel comutativo com unidade*.

Um anel R cujos elementos não nulos formam um grupo com relação à multiplicação é chamado um *anel de divisão*. Se além disso, R é um anel comutativo, então R é chamado um *corpo*. Um exemplo importante de anel é o *anel dos inteiros módulo* n, denotado por $\mathbb{Z}_n$.

Seja R um anel comutativo com unidade. Um *módulo* V sobre R é um grupo comutativo aditivo, junto com uma função

$$R \times V \longrightarrow V, (r, \mathbf{v}) \longmapsto r\mathbf{v},$$

tal que as seguintes propriedades valem:

1. $r(s\mathbf{v}) = (rs)\mathbf{v}$, para quaisquer $r, s \in R$ e $\mathbf{v} \in V$.
2. $r(\mathbf{u} + \mathbf{v}) = r\mathbf{u} + r\mathbf{v}$, para quaisquer $r \in R$ e $\mathbf{u}, \mathbf{v} \in V$.
3. $(r + s)\mathbf{v} = r\mathbf{v} + s\mathbf{v}$, para quaisquer $r, s \in R$ e $\mathbf{v} \in V$.
4. $1\mathbf{v} = \mathbf{v}$, para todo $\mathbf{v} \in V$.

Note que, se R é um corpo, então um módulo V sobre R é um *espaço vetorial* sobre R.

Denotamos o número de elementos de V, ou *cardinalidade* de V, por $|V|$.

Exemplo 1.1 *Seja V um grupo comutativo aditivo. Então é fácil verificar que V é um módulo sobre $\mathbb{Z}$ com a operação*

$$\mathbb{Z} \times V \to V, (r, \mathbf{v}) \mapsto r\mathbf{v},$$

onde

$$r\mathbf{v} = \begin{cases} (r-1)\mathbf{v} + \mathbf{v} & se\ r > 0 \\ 0 & se\ r = 0 \\ (-r)(-\mathbf{v}) & se\ r < 0. \end{cases}$$

Em particular, se $|V| = n$, então $n\mathbf{v} = 0$, para todo $\mathbf{v} \in V$. Note então que V é um módulo sobre $\mathbb{Z}_n$, fazendo $\bar{r}\mathbf{v} = r\mathbf{v}$, para todo $r \in \mathbb{Z}$ e $\mathbf{v} \in V$.

Um subconjunto W de um módulo V sobre R é um *submódulo* de V se:

1. Para quaisquer $\mathbf{w}_1, \mathbf{w}_2 \in W$, tem-se $\mathbf{w}_1 - \mathbf{w}_2 \in W$,

2. Para quaisquer $r \in R$ e $\mathbf{w} \in W$, tem-se $r\mathbf{w} \in W$.

Sejam S um subconjunto de um módulo V sobre R e

$$\mathcal{A} = \{W : W \text{ é submódulo de } V \text{ e } S \subset W\}.$$

Então

$$\langle S \rangle = \bigcap_{W \in \mathcal{A}} W$$

é o menor submódulo de V contendo S e será chamado de *submódulo gerado por* S sobre R.

Seja V um módulo sobre R. Se $\mathbf{v} \in V$ pode ser escrito como

$$\mathbf{v} = \sum\nolimits_{i=1}^{n} r_i \mathbf{v}_i : r_i \in R \text{ e } \mathbf{v}_i \in V,$$

então dizemos que $\mathbf{v}$ é uma *combinação linear* dos elementos $\mathbf{v}_1, \ldots, \mathbf{v}_n$ sobre R. Neste caso, o conjunto de todas as combinações lineares de $\mathbf{v}_1, \ldots, \mathbf{v}_n$ é o submódulo

$$\langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle = \left\{ \sum_{i=1}^{n} r_i \mathbf{v}_i : r_i \in R \right\},$$

gerado por $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Quando existe um subconjunto finito S de um módulo V sobre R tal que $V = \langle S \rangle$, dizemos que V é um *módulo finitamente gerado* sobre R. Se $S = \{\mathbf{v}\}$, isto é, S consiste de um único elemento, temos

$$\langle \mathbf{v} \rangle = \{r\mathbf{v} : r \in R\}$$

e $\langle \mathbf{v} \rangle$ será chamado de *submódulo cíclico gerado por* $\mathbf{v}$ sobre R.

Uma seqüência finita $\mathbf{v}_1, \ldots, \mathbf{v}_n$ de elementos de um módulo V sobre R é chamada *linearmente independente* se

$$\sum_{i=1}^{n} r_i \mathbf{v}_i = 0 \Longrightarrow r_1 = r_2 = \cdots = r_n = 0.$$

Caso contrário, dizemos que a seqüência é *linearmente dependente*. Um subconjunto S de um módulo V sobre R é dito *linearmente independente* se qualquer seqüência finita de elementos distintos de S é linearmente independente. Caso contrário, S é dito de *linearmente dependente*.

Um subconjunto S de um módulo V sobre R é dito uma *base* sobre R se as seguintes propriedades valem:

1. $V = \langle S \rangle$.

2. S é linearmente independente.

Um módulo V sobre R é chamado de *módulo livre* sobre R se possui uma base. Quaisquer duas bases de um módulo livre sobre R têm a mesma cardinalidade. A cardinalidade da base sobre R é chamada de *posto* de V sobre R.

Sejam U e V módulos sobre R. Uma aplicação $\varphi : U \to V$ é um *homomorfismo de módulos* sobre R se as seguintes condições são satisfeitas:

1. $\varphi(\mathbf{u} + \mathbf{v}) = \varphi(\mathbf{u}) + \varphi(\mathbf{v}), \forall \mathbf{u}, \mathbf{v} \in U$.

2. $\varphi(r\mathbf{u}) = r\varphi(\mathbf{u}), \forall \mathbf{u} \in U$ e $r \in R$.

Denotamos o conjunto destes homomorfismos sobre R por

$$\text{Hom}_R(U, V) = \{\varphi : U \longrightarrow V : \varphi \text{ é um homomorfismo sobre } R\}.$$

Um homomorfismo de módulos sobre R, $\varphi : U \longrightarrow V$ é um *isomorfismo* sobre R se φ é bijetora. Em particular, quando $U = V$, temos $\text{Hom}_R(U, V) = \text{End}_R(U)$, onde $\text{End}_R(U)$ é o conjunto dos *endomorfismos* de U.

Teorema 1.1 *Sejam U e V módulos livres sobre R e n o posto de U. Sejam $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ uma base de U sobre R e $\mathbf{v}_1, \ldots, \mathbf{v}_n$ elementos arbitrários de V. Então existe um único homomorfismo de módulos sobre R, $\varphi : U \to V$ tal que $\varphi(\mathbf{u}_i) = \mathbf{v}_i$, para todo $i = 1, 2, \ldots, n$.*

Prova. Dado $\mathbf{u} \in U$, existem únicos $r_1, \cdots, r_n \in R$ tais que

$$\mathbf{u} = r_1\mathbf{u}_1 + \cdots + r_n\mathbf{u}_n.$$

Definamos $\varphi : U \to V$ por

$$\varphi(\mathbf{u}) = r_1\mathbf{v}_1 + \cdots + r_n\mathbf{v}_n.$$

Sendo $r_1, \cdots, r_n$ únicos, a função φ é bem definida e $\varphi(\mathbf{u}_i) = \mathbf{v}_i$, pois

$$\mathbf{u}_i = 0\mathbf{u}_1 + \cdots + 1\mathbf{u}_i + \cdots + 0\mathbf{u}_n, i = 1, \ldots, n.$$

Seja $\mathbf{u}' = s_1\mathbf{u}_1 + \cdots + s_n\mathbf{u}_n$. Então

$$\mathbf{u} + \mathbf{u}' = (r_1 + s_1)\mathbf{u}_1 + \cdots + (r_n + s_n)\mathbf{u}_n.$$

Logo,

$$\begin{aligned}
\varphi(\mathbf{u} + \mathbf{u}') &= (r_1 + s_1)\mathbf{v}_1 + \cdots + (r_n + s_n)\mathbf{v}_n \\
&= r_1\mathbf{v}_1 + s_1\mathbf{v}_1 + \cdots + r_n\mathbf{v}_n + s_n\mathbf{v}_n \\
&= (r_1\mathbf{v}_1 + \cdots + r_n\mathbf{v}_n) + (s_1\mathbf{v}_1 + \cdots + s_n\mathbf{v}_n) \\
&= \varphi(\mathbf{u}) + \varphi(\mathbf{u}').
\end{aligned}$$

Agora, seja $t \in R$. Então

$$tu = (tr_1)\mathbf{u}_1 + \cdots + (tr_n)\mathbf{u}_n.$$

Portanto,

$$\begin{aligned}
\varphi(t\mathbf{u}) &= (tr_1)\mathbf{v}_1 + \cdots + (tr_n)\mathbf{v}_n \\
&= t(r_1\mathbf{v}_1 + \cdots + r_n\mathbf{v}_n) \\
&= t\varphi(\mathbf{u})
\end{aligned}$$

Finalmente, se $\psi : U \to V$ é um homomorfismo tal que $\psi(\mathbf{u}_i) = \mathbf{v}_i$, para todo $i = 1, 2, \ldots, n$, então

$$\begin{aligned}
\psi(\mathbf{u}) &= \psi(r_1\mathbf{u}_1 + \cdots + r_n\mathbf{u}_n) \\
&= r_1\psi(\mathbf{u}_1) + \cdots + r_n\psi(\mathbf{u}_n) \\
&= r_1\mathbf{v}_1 + \cdots + r_n\mathbf{v}_n \\
&= \varphi(\mathbf{u}).
\end{aligned}$$

Como $\psi(\mathbf{u}) = \varphi(\mathbf{u})$ para todo $\mathbf{u} \in U$ temos que $\psi = \varphi$. ■

Sejam U e V módulos livres sobre R e $\varphi : U \to V$ um isomorfismo sobre R. Se $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ é uma base sobre R de V e $\varphi(\mathbf{u}_i) = \mathbf{v}_i$, $i = 1, \ldots, n$, então é fácil verificar que $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ é uma base de U sobre R.

Sejam V um módulo sobre R e W um submódulo de V sobre R. Se $\mathbf{v}$ é um elemento arbitrário de V, escrevemos $W + \mathbf{v}$ para representar o conjunto de somas $\mathbf{w} + \mathbf{v}$, com $\mathbf{w} \in W$, isto é,

$$W + \mathbf{v} = \{\mathbf{w} + \mathbf{v} : \mathbf{w} \in W\}.$$

Estes conjuntos são chamados *classes laterais à direita* de W em V. De forma análoga, definimos classes laterais à esquerda. Estas classes particionam V em subconjuntos mutuamente disjuntos de mesma cardinalidade.

Exemplo 1.2 *Seja W o submódulo sobre $\mathbb{R}$ em $\mathbb{R}^2$ definido por*

$$W = \left\{(r, s) \in \mathbb{R}^2 : r = s\right\},$$

isto é, W é a reta dada pela equação $r - s = 0$. Podemos ver $W + \mathbf{v}$ como uma translação da reta, obtida somando-se cada ponto de W a $\mathbf{v}$. A classe lateral $W + \mathbf{v}$ é também uma reta e é paralela a W. Assim, as classes laterais de W em $\mathbb{R}^2$ são precisamente todas as retas paralelas a W.

No teorema seguinte, utilizaremos as classes laterais de um submódulo W sobre R de um módulo V sobre R em V, para definir um novo módulo, chamado *módulo quociente de V por W*, que será denotado por V/W.

Teorema 1.2 *Sejam V um módulo sobre R e W um submódulo de V. Então as classes laterais de W em V formam um módulo sobre R com as seguintes operações de adição e multiplicação escalar*:

1. $(W + \mathbf{w}_1) + (W + \mathbf{w}_2) = W + (\mathbf{w}_1 + \mathbf{w}_2)$, *para quaisquer* $\mathbf{w}_1, \mathbf{w}_2 \in W$.

2. $r\,(W + \mathbf{v}) = W + r\mathbf{v}$, *para qualquer* $r \in R$ *e* $\mathbf{v} \in V$. ■

1.2 Reticulados

Seja $\mathbb{R}^n$ o espaço Euclidiano n-dimensional. A *norma quadrática*

$$\mathbf{N}(\mathbf{v}) = \| \mathbf{v} \|^2$$

de um vetor $\mathbf{v} \in \mathbb{R}^n$ é a soma dos quadrados de suas componentes, isto é,

$$\mathbf{N}(\mathbf{v}) = (\mathbf{v}, \mathbf{v}) = \mathbf{v}\mathbf{v}^t,$$

onde $(\mathbf{v}, \mathbf{v})$ é o produto interno de $\mathbf{v}$ por $\mathbf{v}$. A *distância Euclidiana quadrática* entre dois vetores $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ é a norma quadrática de sua diferença, isto é,

$$d^2(\mathbf{u}, \mathbf{v}) = \mathbf{N}(\mathbf{u} - \mathbf{v}) = \|\mathbf{u} - \mathbf{v}\|^2 .$$

Uma *esfera* em $\mathbb{R}^n$, com centro $\mathbf{c}$ e raio ρ, consiste de todos os pontos $\mathbf{v} \in \mathbb{R}^n$ tais que $\mathbf{N}(\mathbf{v} - \mathbf{c}) = \rho^2$, isto é,

$$E_\rho(\mathbf{c}) = \{\mathbf{v} \in \mathbb{R}^n : \mathbf{N}(\mathbf{v} - \mathbf{c}) = \rho^2\}.$$

Um *empacotamento esférico* Λ em $\mathbb{R}^n$ de raio ρ consiste de uma seqüência infinita de pontos $\mathbf{c}_1, \mathbf{c}_2, \ldots$ em $\mathbb{R}^n$, os centros das esferas, tais que

$$\mathbf{N}(\mathbf{c}_i - \mathbf{c}_j) \geq 4\rho^2, \forall i \neq j.$$

O raio ρ é chamado de *raio de empacotamento* e, neste caso,

$$d^2_{\min}(\Lambda) = 4\rho^2,$$

onde $d^2_{\min}(\Lambda)$ é a distância Euclidiana quadrática mínima entre os elementos de Λ.

Um subgrupo aditivo de $\mathbb{R}^n$ é *discreto* se sua interseção com qualquer subconjunto limitado em $\mathbb{R}^n$ é finita. Um *reticulado* Λ é um subgrupo aditivo discreto de $\mathbb{R}^n$, ou equivalentemente, os centros do empacotamento esférico Λ formam um grupo aditivo sob a adição de vetores. Em outras palavras, todo reticulado é um módulo sobre $\mathbb{Z}$. Um *sub-reticulado* Γ de um reticulado Λ é um subconjunto de elementos de Λ, que é também um reticulado. Um *código reticulado* é um subconjunto finito de pontos de um reticulado

Λ ou de uma translação $\mathbf{v} + \Lambda$.

Exemplo 1.3 *$\Lambda = \mathbb{Z}^n$ é um reticulado em $\mathbb{R}^n$.*

Teorema 1.3 *Seja Λ um reticulado em $\mathbb{R}^n$. Então Λ é gerado, como módulo sobre $\mathbb{Z}$, por m vetores linearmente independentes sobre $\mathbb{R}$, neste caso, $m \leq n$.*

Prova. Se $m = 1$ e $\Lambda \neq \{0\}$, então $\Lambda_+^* \neq \{0\}$, pois se $v \in \Lambda$ e $v \neq 0$, então $-v \in \Lambda$ e $v > 0$ ou $-v > 0$. Seja $0 < u = \inf \Lambda_+$.

Afirmação. $u \in \Lambda_+$ e $\Lambda = \mathbb{Z}u$.

De fato, se $u \notin \Lambda_+$, então

$$u < u + \frac{u}{2}.$$

Assim, por definição, existem $v, w \in \Lambda_+$ tais que

$$u < v < w < u + \frac{u}{2} \Rightarrow w - v < \frac{u}{2} < u.$$

Logo, $w - v \in \Lambda_+$, com $w - v < u$, que é uma contradição. Como todo $v \in \Lambda$ pode ser escrito na forma

$$v = qu + r, \text{ com } q \in \mathbb{Z} \text{ e } 0 \leq r < u,$$

temos pela escolha de u, que $r = 0$, pois $r = v - qu \in \Lambda$. Portanto, $v \in \mathbb{Z}u$, isto é, $\Lambda = \mathbb{Z}u$.

Sejam $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ um subconjunto maximal de vetores linearmente independentes de Λ, sobre $\mathbb{R}$ e

$$\Gamma = \langle \mathbf{u}_1, \ldots, \mathbf{u}_m \rangle, \Gamma_{m-1} = \langle \mathbf{u}_1, \ldots, \mathbf{u}_{m-1} \rangle \text{ e } \Lambda_{m-1} = \Lambda \cap \Gamma_{m-1}.$$

Então é claro que Λ_{m-1} é discreto. Se $m > 1$, podemos supor, como hipótese de indução, que Λ_{m-1} é gerado como módulo sobre $\mathbb{Z}$, por l vetores linearmente independentes sobre $\mathbb{R}$, digamos $\mathbf{v}_1, \ldots, \mathbf{v}_l$. Como $\mathbf{u}_1, \ldots, \mathbf{u}_{m-1} \in \Lambda_{m-1}$, temos que $l = m-1$. Assim, podemos substituir $\mathbf{v}_1, \ldots, \mathbf{v}_{m-1}$ por $\mathbf{u}_1, \ldots, \mathbf{u}_{m-1}$. Seja

$$S = \{\mathbf{u} \in \Lambda : \mathbf{u} = s_1\mathbf{u}_1 + \cdots + s_m\mathbf{u}_m, \ 0 \leq s_i < 1 \text{ e } 0 \leq s_m \leq 1\}.$$

Então é claro que S é limitado, finito e $\mathbf{u}_m \in S$, pois Λ é discreto. Assim, podemos

escolher $\mathbf{v}_m \in S$, com o último coeficiente s_m menor possível e positivo, digamos,

$$\mathbf{v}_m = t_1\mathbf{u}_1 + \cdots + t_m\mathbf{u}_m, 0 < t_m \leq 1.$$

Afirmação. $\{\mathbf{u}_1, \ldots, \mathbf{u}_{m-1}, \mathbf{v}_m\}$ é uma base sobre $\mathbb{Z}$ de Λ.
De fato, é fácil verificar que $\{\mathbf{u}_1, \ldots, \mathbf{u}_{m-1}, \mathbf{v}_m\}$ é linearmente independente sobre $\mathbb{R}$. Dado qualquer vetor $\mathbf{u} \in \Lambda$, temos

$$\mathbf{u} = x_1\mathbf{u}_1 + \cdots + x_{m-1}\mathbf{u}_{m-1} + x_m\mathbf{v}_m, x_i \in \mathbb{R}.$$

Como para cada i, $x_i = y_i + z_i$, onde $y_i \in \mathbb{Z}$ e $0 \leq z_i < 1$, temos $\mathbf{u} = \mathbf{w}_1 + \mathbf{w}_2$, onde

$$\mathbf{w}_1 = y_1\mathbf{u}_1 + \cdots + y_{m-1}\mathbf{u}_{m-1} + y_m\mathbf{v}_m \text{ e } \mathbf{w}_2 = z_1\mathbf{u}_1 + \cdots + z_{m-1}\mathbf{u}_{m-1} + z_m\mathbf{v}_m.$$

Sendo $\mathbf{w}_2 \in S$ e $z_m < x_m$, temos pela escolha de x_m, que $z_m = 0$. Portanto, $\{\mathbf{u}_1, \ldots, \mathbf{u}_{m-1}, \mathbf{v}_m\}$ gera Λ. ■

Teorema 1.4 *Sejam V um módulo livre sobre $\mathbb{Z}$ de posto n e W um submódulo próprio sobre $\mathbb{Z}$ de V. Então W tem uma base sobre $\mathbb{Z}$ com m elementos e $m \leq n$.*

Prova. Seja $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ uma base sobre $\mathbb{Z}$ de V. Então existe um único homomorfismo $\varphi : V \to \mathbb{R}^n$ sobre $\mathbb{Z}$ tal que

$$\varphi(\mathbf{v}_i) = \mathbf{e}_i, \forall i = 1, \ldots, n \text{ e } \mathbf{e}_i \in \mathbb{R}^n.$$

É fácil verificar que φ é injetor. Logo, $V \cong \varphi(V)$. Todo vetor $\mathbf{u} \in \mathbb{R}^n$ pode ser escrito de modo único na forma

$$\mathbf{u} = r_1\mathbf{e}_1 + \cdots + r_n\mathbf{e}_n, r_i \in \mathbb{R}.$$

Definamos $\psi : \mathbb{R}^n \to \mathbb{R}^n$ por

$$\psi(\mathbf{u}) = (r_1, \ldots, r_n).$$

Então $\psi(B_\rho[\mathbf{0}])$ é limitada, onde $B_\rho[\mathbf{0}]$ é a bola fechada de centro $\mathbf{0}$ e raio ρ. Assim, existe $k \in \mathbb{R}$ tal que

$$\|\psi(\mathbf{u})\| \leq k, \forall \mathbf{u} \in B_\rho[\mathbf{0}].$$

Agora, se $s_1\mathbf{e}_1 + \cdots + s_n\mathbf{e}_n \in B_\rho[\mathbf{0}]$ e $s_i \in \mathbb{Z}$, então

$$\|(s_1, \ldots, s_n)\| \leq k.$$

Logo,

$$|s_i| \leq \|(s_1, \ldots, s_n)\| \leq k, \forall i = 1, \ldots, n.$$

O número de soluções inteiras desta desigualdade é finito e assim, $\varphi(V) \cap B_\rho[\mathbf{0}]$ também o é. Portanto, $\varphi(V)$ é discreto. Pelo Teorema 1.3, W tem uma base sobre $\mathbb{Z}$ com m elementos e $m \leq n$. ■

Como todo reticulado de dimensão $m \leq n$ pode ser mergulhado (imerso como sub-reticulado) em um reticulado de dimensão n, então salvo menção explícita em contrário, todos os reticulados e sub-reticulados deste trabalho são de dimensão n

Seja $\Lambda = \langle \mathbf{u}_1, \ldots, \mathbf{u}_n \rangle$ um reticulado em $\mathbb{R}^n$ gerado por n vetores linearmente independentes $\mathbf{u}_1, \ldots, \mathbf{u}_n$ sobre $\mathbb{R}$. Se

$$\mathbf{u}_i = (r_{i1}, \ldots, r_{in}),$$

então a matriz

$$\mathbf{M} = (\mathbf{u}_i, 1 \leq i \leq n),$$

cujas linhas são os vetores $\mathbf{u}_i$ é chamada uma *matriz geradora* do reticulado Λ, e os elementos do reticulado Λ consistem de todos os vetores $\mathbf{vM}$, onde $\mathbf{v} \in \mathbb{Z}^n$.

Seja $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ uma base qualquer sobre $\mathbb{Z}$ de Λ. Então existem únicos $b_{ij} \in \mathbb{Z}$ tais que

$$\mathbf{v}_j = \sum_{i=1}^{n} b_{ij}\mathbf{u}_i, 1 \leq j \leq n.$$

De modo análogo, existem únicos $a_{ij} \in \mathbb{Z}$ tais que

$$\mathbf{u}_j = \sum_{i=1}^{n} a_{ij}\mathbf{v}_i, 1 \leq j \leq n.$$

Logo,

$$\begin{aligned}\mathbf{u}_j &= \sum_{i=1}^{n} a_{ij}\mathbf{v}_i \\ &= \sum_{i=1}^{n}\left(a_{ij}\sum_{k=1}^{n} b_{ki}\mathbf{u}_k\right) \\ &= \sum_{k=1}^{n}\left(\sum_{i=1}^{n} a_{ij}b_{ki}\right)\mathbf{u}_k.\end{aligned}$$

Assim,

$$\sum_{i=1}^{n} a_{ij}b_{ki} = \begin{cases} 1 & \text{se } j = k \\ 0 & \text{se } j \neq k. \end{cases}$$

Se $\mathbf{A} = (a_{ij})$ é a matriz de mudança da base $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ sobre $\mathbb{Z}$ para a base $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ sobre $\mathbb{Z}$ e $\mathbf{B} = (b_{ij})$ é a matriz de mudança da base $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ sobre $\mathbb{Z}$ para a base $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ sobre $\mathbb{Z}$, então

$$\mathbf{AB} = \mathbf{I}_n,$$

onde $\mathbf{I}_n$ é a matriz quadrada de ordem n. Logo,

$$\det \mathbf{A} \det \mathbf{B} = \det(\mathbf{AB}) = 1.$$

Portanto,

$$\det \mathbf{A} = \det \mathbf{B} = \pm 1.$$

Conclusão. Toda base $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ sobre $\mathbb{Z}$ de Λ pode ser obtida a partir de uma dada base $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ sobre $\mathbb{Z}$ de Λ, onde

$$\mathbf{v}_j = \sum_{i=1}^{n} b_{ij}\mathbf{u}_i, 1 \leq j \leq n,$$

com $b_{ij} \in \mathbb{Z}$ e $\det \mathbf{B} = \pm 1$.

O *determinante* do reticulado Λ é o valor absoluto do determinante da matriz geradora $\mathbf{M}$, isto é,

$$\det \Lambda = |\det \mathbf{M}|.$$

Note, do exposto acima, que $\det \Lambda$ é independente da base sobre $\mathbb{Z}$ escolhida para Λ.

Sejam Λ um reticulado em $\mathbb{R}^n$, Γ um sub-reticulado de Λ, $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ uma base sobre

$\mathbb{Z}$ de Λ e $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ uma base sobre $\mathbb{Z}$ de Γ. Como $\mathbf{v}_j \in \Lambda$, existem únicos $b_{ij} \in \mathbb{Z}$ tais que

$$\mathbf{v}_j = \sum_{i=1}^{n} b_{ij}\mathbf{u}_i, 1 \leq j \leq n.$$

Se $\mathbf{B} = (b_{ij})$, então

$$N = |\det \mathbf{B}| = \frac{\det \Gamma}{\det \Lambda}$$

é chamado de *índice* de Γ em Λ. Note que N depende somente de Λ e Γ, não das bases sobre $\mathbb{Z}$ escolhidas para Λ e Γ. Pela Regra de Cramer, obtemos

$$N\mathbf{u}_j = \sum_{i=1}^{n} a_{ij}\mathbf{v}_i, 1 \leq j \leq n,$$

onde $a_{ij} \in \mathbb{Z}$. Assim,

$$N\Lambda \subseteq \Gamma \subseteq \Lambda,$$

onde $N\Lambda = \{N\mathbf{u} : \mathbf{u} \in \Lambda\}$ é um reticulado. Portanto, $\{N\mathbf{u}_1, \ldots, N\mathbf{u}_n\}$ é uma base sobre $\mathbb{Z}$ de $N\Lambda$.

Teorema 1.5 *Sejam Λ um reticulado em $\mathbb{R}^n$ e Γ um sub-reticulado de Λ. Então*:

1. *Para cada base $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ sobre $\mathbb{Z}$ de Λ, existe uma base $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ sobre $\mathbb{Z}$ de Γ tal que*

$$\mathbf{v}_i = \sum_{j=1}^{i} b_{ij}\mathbf{u}_j,$$

onde $b_{ij} \in \mathbb{Z}$, $b_{ii} \neq 0$ e $1 \leq i \leq n$.

2. *Para cada base $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ sobre $\mathbb{Z}$ de Γ, existe uma base $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ sobre $\mathbb{Z}$ de Λ tal que*

$$\mathbf{v}_i = \sum_{j=1}^{i} b_{ij}\mathbf{u}_j,$$

onde $b_{ij} \in \mathbb{Z}$, $b_{ii} \neq 0$ e $1 \leq i \leq n$.

Prova. 1. Seja N o índice de Γ em Λ. Como $N\mathbf{u}_j \in \Gamma$, temos que existem vetores $\mathbf{v}_i \in \Gamma$ tais que

$$\mathbf{v}_i = \sum_{j=1}^{i} b_{ij}\mathbf{u}_j,$$

onde $b_{ij} \in \mathbb{Z}$, $b_{ii} \neq 0$ e $1 \leq i \leq n$. Assim, para cada i, podemos escolher $\mathbf{v}_i \in \Gamma$, com o último coeficiente $|b_{ii}|$ menor possível e $b_{ii} \neq 0$.

Afirmação. $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ é uma base sobre $\mathbb{Z}$ de Γ.

De fato, é claro que $\langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle \subseteq \Gamma$. Suponhamos por absurdo, que exista $\mathbf{w} \in \Gamma - \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$. Como $\mathbf{w} \in \Lambda$, temos que existem únicos $a_i \in \mathbb{Z}$, tais que

$$\mathbf{w} = \sum_{i=1}^{n} a_i \mathbf{u}_i.$$

Seja k, $1 \leq k \leq n$, o menor inteiro tal que

$$\mathbf{w} = \sum_{i=1}^{k} a_i \mathbf{u}_i \text{ e } a_k \neq 0.$$

Desde que $b_{kk} \neq 0$, podemos escolher $c \in \mathbb{Z}$ tal que

$$|a_k - cb_{kk}| < |b_{kk}|.$$

O vetor

$$\mathbf{w} - c\mathbf{v}_k = \sum_{i=1}^{k} (a_i - cb_{ki})\mathbf{u}_i \in \Gamma - \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle,$$

pois $\mathbf{w} \in \Gamma - \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$. Logo, $a_k - cb_{kk} \neq 0$, que é uma contradição. Portanto, $\Gamma = \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$.

2. Seja $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ uma base de Γ sobre $\mathbb{Z}$, fixada. Como $N\Lambda$ é um sub-reticulado de Γ, onde N é o índice de Γ em Λ, pelo item anterior, existe uma base $\{N\mathbf{u}_1, \ldots, N\mathbf{u}_n\}$ sobre $\mathbb{Z}$ de $N\Lambda$ tal que

$$N\mathbf{u}_i = \sum_{j=1}^{i} c_{ij} \mathbf{v}_j,$$

onde $c_{ij} \in \mathbb{Z}$, $c_{ii} \neq 0$ e $1 \leq i \leq n$. Logo,

$$\mathbf{v}_i = \sum_{j=1}^{i} b_{ij} \mathbf{u}_j,$$

onde $b_{ij} \in \mathbb{Q}$, $b_{ii} \neq 0$ e $1 \leq i \leq n$. É claro que $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ é uma base sobre $\mathbb{Z}$ de Λ.

Como $\mathbf{v}_i \in \Lambda$ e todo $\mathbf{u} \in \Lambda$ pode ser escrito de modo único na forma

$$\mathbf{u} = b_1\mathbf{u}_1 + \cdots + b_n\mathbf{u}_n, b_i \in \mathbb{R},$$

temos que $b_{ij} \in \mathbb{Z}$. ■

Observação 1.1 *Sejam Λ e Γ reticulados em $\mathbb{R}^n$ com matrizes geradoras $\mathbf{M}$ e $\mathbf{N}$, respectivamente. Então Γ é um sub-reticulado de Λ se, e somente se, $\mathbf{N} = \mathbf{BM}$, onde*

$$\mathbf{B} = \begin{pmatrix} b_{11} & 0 & 0 & \cdots & 0 \\ b_{21} & b_{22} & 0 & \cdots & 0 \\ b_{31} & b_{32} & b_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & b_{n3} & \cdots & b_{nn} \end{pmatrix}$$

com $b_{ij} \in \mathbb{Z}$. A matriz $\mathbf{B}$ é chamada matriz particionadora *do sub-reticulado Γ.*

Corolário 1.1 *Sejam Λ um reticulado em $\mathbb{R}^n$ e Γ um sub-reticulado de Λ. Então*:

1. *Para cada base $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ sobre $\mathbb{Z}$ de Λ, existe uma base $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ sobre $\mathbb{Z}$ de Γ tal que*

$$\mathbf{v}_i = \sum_{j=1}^{i} b_{ij}\mathbf{u}_j,$$

onde $b_{ij} \in \mathbb{Z}$, $b_{ii} > 0$, $0 \leq b_{ij} < b_{jj}$ e $1 \leq i \leq n$,

2. *Para cada base $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ sobre $\mathbb{Z}$ de Γ, existe uma base $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ sobre $\mathbb{Z}$ de Λ tal que*

$$\mathbf{v}_i = \sum_{j=1}^{i} b_{ij}\mathbf{u}_j,$$

onde $b_{ij} \in \mathbb{Z}$, $b_{ii} > 0$, $0 \leq b_{ij} < b_{ii}$ e $1 \leq i \leq n$.

Prova. 1. Para mostrar que $b_{ii} > 0$, basta substituir $\mathbf{u}_i$ por $-\mathbf{u}_i$ se $b_{ii} < 0$. Agora, substituamos $\mathbf{v}_i$ por

$$\mathbf{w}_i = \sum_{j=1}^{i-1} a_{ij}\mathbf{v}_j + \mathbf{v}_i,$$

onde $a_{ij} \in \mathbb{Z}$ será determinado, $2 \leq i \leq n$ e $\mathbf{w}_1 = \mathbf{v}_1$. Note que, para qualquer escolha de a_{ij}, o conjunto $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ é uma base sobre $\mathbb{Z}$ de Γ. Logo,

$$\mathbf{w}_i = \sum_{j=1}^{i} c_{ij}\mathbf{u}_j,$$

onde $c_{ii} = b_{ii}$. Assim, para $j < i$, temos

$$c_{ij} = a_{ij}b_{jj} + a_{i(j+1)}b_{(j+1)j} + \cdots + a_{i(i-1)}b_{(i-1)j} + b_{ij}.$$

Portanto, para cada i, podemos escolher $a_{i1}, a_{i2}, \ldots, a_{i(i-1)}$ de modo que

$$0 \leq c_{ij} < c_{jj} = b_{jj}.$$

A prova de 2. é análoga. ■

Corolário 1.2 *Sejam Λ um reticulado em $\mathbb{R}^n$ e Γ um sub-reticulado de Λ. Então o índice de Γ em Λ é o número das classes laterais de Γ em Λ, denotado por $[\Lambda : \Gamma]$.*

Prova. Seja N o índice de Γ em Λ. Então, pelo Corolário 1.1, temos

$$N = \prod_{i=1}^{n} b_{ii}.$$

Afirmação. O conjunto

$$[\Lambda/\Gamma] = \{c_1\mathbf{u}_1 + \cdots + c_n\mathbf{u}_n, 0 \leq c_i < b_{ii}, 1 \leq i \leq n\}$$

é um sistema completo de representantes de classes laterais de Γ em Λ.
De fato, seja

$$\mathbf{u} = a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n$$

um elemento qualquer de Λ. Dividindo a_1 por b_{11}, obtemos

$$a_1 = b_{11}q_1 + r_1, 0 \leq r_1 < b_{11}.$$

Então

$$\mathbf{u} - q_1\mathbf{v}_1 - r_1\mathbf{u}_1 = a_2\mathbf{u}_2 + \cdots + a_n\mathbf{u}_n.$$

Dividindo a_2 por b_{22}, obtemos

$$a_2 = b_{22}q_2 + r_2, 0 \leq r_2 < b_{22}.$$

Então

$$\mathbf{u} - q_1\mathbf{v}_1 - r_1\mathbf{u}_1 - q_2\mathbf{v}_2 - r_2\mathbf{u}_2 = a_3\mathbf{u}_3 + \cdots + a_n\mathbf{u}_n.$$

Continuando este processo, obtemos

$$\mathbf{u} - (\sum_{i=1}^{n} q_i\mathbf{v}_i) - (\sum_{i=1}^{n} r_i\mathbf{u}_i) = 0,$$

isto é,

$$\mathbf{u} = \mathbf{v} + \mathbf{w},$$

onde $\mathbf{v} \in \Gamma$ *e* $\mathbf{w} \in [\Lambda/\Gamma]$. Suponhamos que

$$(\Gamma + \mathbf{w}) \cap (\Gamma + \mathbf{w}') \neq \emptyset.$$

Então existem

$$\mathbf{w} = \sum_{i=1}^{n} r_i\mathbf{u}_i, \mathbf{w}' = \sum_{i=1}^{n} r_i'\mathbf{u}_i \in [\Lambda/\Gamma],$$

distintos, tais que $\mathbf{w} - \mathbf{w}' \in \Gamma$. Seja s o primeiro índice $(1 \leq s \leq n)$ tal que $r_s \neq r_s'$. Então,

$$\sum_{i=s}^{n}(r_i - r_i')\mathbf{u}_i = \sum_{i=1}^{n} b_i\mathbf{v}_i.$$

Como

$$\mathbf{v}_i = \sum_{j=1}^{i} b_{ij}\mathbf{u}_j,$$

temos que $b_1 = \cdots = b_{s-1} = 0$ e $b_{ss}b_s = r_s - r_s'$, que é uma contradição, pois

$$0 < |r_s - r_s'| < b_{ss} \Rightarrow 0 < b_s < 1.$$

Portanto, $N = [\Lambda : \Gamma]$. ■

Observação 1.2 *Sejam G um grupo abeliano livre de posto n e H um subgrupo próprio de G. Então $[G : H]$ é finito se, e somente se, os postos de G e H são iguais.*

Seja $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ uma transformação linear não singular. Então o reticulado Λ em $\mathbb{R}^n$ é transformado por T no reticulado

$$T(\Lambda) = \{T(\mathbf{u}) : \mathbf{u} \in \Lambda\}$$

em $\mathbb{R}^n$. Se $T(\Lambda) \subseteq \Lambda$, dizemos que T é um *endomorfismo* de Λ. Em particular; se $T(\Lambda) = \Lambda$, dizemos que T é um *automorfismo* de Λ.

Teorema 1.6 *Seja $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ uma transformação linear. Então as seguintes afirmações são equivalentes*:

1. *Existe $r > 0$ tal que $(T(\mathbf{u}), T(\mathbf{v})) = r^2 (\mathbf{u}, \mathbf{v})$, quaisquer que sejam $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$.*
2. *$\|T(\mathbf{u})\| = r \|\mathbf{u}\|$, para todo $\mathbf{u} \in \mathbb{R}^n$ (r constante).*
3. *Se $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ é uma base ortonormal, então $(T(\mathbf{e}_i), T(\mathbf{e}_j)) = 0$ para $i \neq j$ e $\|T(\mathbf{e}_i)\| = r$, para quaisquer $i, j = 1, \ldots, n$.* ■

Uma transformação que satisfaz pelo menos uma das afirmações acima chama-se *similaridade*.

Seja Λ um reticulado em $\mathbb{R}^n$. Então o conjunto

$$\Lambda^* = \{\mathbf{u} \in \mathbb{R}^n : (\mathbf{u}, \mathbf{v}) \in \mathbb{Z}, \forall \mathbf{v} \in \Lambda\}$$

é um reticulado em $\mathbb{R}^n$ chamado *reticulado dual* de Λ. Se $\mathbf{M}$ é uma matriz geradora de Λ, então $\mathbf{M}^* = (\mathbf{M}^{-1})^t$ é uma matriz geradora de Λ^*. Quando $\Lambda \subseteq \Lambda^*$, dizemos que Λ é um *reticulado inteiro* e neste caso,

$$\Lambda^* = \bigcup_{i=0}^{N-1} (\Lambda + \mathbf{w}_i),$$

onde N é o índice de Λ em Λ^* e $w_i \in [\Lambda^*/\Lambda],\ 0 \leq i \leq N-1$. Em particular, quando $\Lambda = \Lambda^*$, dizemos que Λ é um *reticulado auto-dual*.

Uma matriz quadrada $\mathbf{A} = (a_{ij})$, com $a_{ij} \in \mathbb{Z}$ e $\det \mathbf{A} = \pm 1$ é chamada *unimodular*. Assim, $\mathbf{A}$ é unimodular se, e somente se, $\mathbf{A}^{-1} = (a'_{ij})$ existe e $a'_{ij} \in \mathbb{Z}$.

Uma transformação linear $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ é chamada *ortogonal* se a mesma preserva o produto interno, isto é,

$$(T(\mathbf{u}), T(\mathbf{v})) = (\mathbf{u}, \mathbf{v}),$$

para quaisquer $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$.

Sejam Λ e Γ reticulados em $\mathbb{R}^m$ e $\mathbb{R}^n$, respectivamente, com matrizes geradoras $\mathbf{M}$ e $\mathbf{N}$. Dizemos que Λ é *similar* a Γ se

$$\mathbf{M} = r\mathbf{ANB},$$

onde $r \in \mathbb{R} - \{0\}$, $\mathbf{A}$ é uma matriz unimodular e $\mathbf{B}$ é uma matriz ortogonal. Quando $r = 1$, dizemos que Λ é *equivalente* a Γ.

Exemplo 1.4 *Sejam $\Lambda = A_2$ o reticulado hexagonal em $\mathbb{R}^2$, com uma matriz geradora*

$$\mathbf{M} = \begin{pmatrix} 1 & 0 \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$$

e

$$\Gamma = \{(r, s, t) \in \mathbb{Z}^3 : r + s + t = 0\}$$

um reticulado em $\mathbb{R}^3$, com uma matriz geradora

$$\mathbf{N} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & -1 & 1 \end{pmatrix}.$$

Então $\mathbf{M} = r\mathbf{ANB}$, onde $r = \frac{\sqrt{2}}{2}, \mathbf{A} = I_2$ e

$$\mathbf{B} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ 0 & -\frac{2}{\sqrt{6}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \end{pmatrix}.$$

Portanto, o reticulado A_2 é similar ao reticulado Γ.

1.3 Parâmetros de um Reticulado

Seja Λ um empacotamento esférico em $\mathbb{R}^n$. A *região de Voronoi* $R_v(\mathbf{u})$ associada ao ponto $\mathbf{u} \in \Lambda$ é o conjunto

$$R_v(\mathbf{u}) = \{\mathbf{w} \in \mathbb{R}^n : \mathbf{N}(\mathbf{w} - \mathbf{u}) \leq \mathbf{N}(\mathbf{w} - \mathbf{u}'), \forall \mathbf{u}' \in \Lambda\}.$$

Um *buraco* de um empacotamento esférico Λ em $\mathbb{R}^n$ é um ponto de $\mathbb{R}^n - \Lambda$ cuja distância de Λ é um máximo local, isto é, um ponto $\mathbf{w}_0 \in R_v(\mathbf{u})$ tal que $\mathbf{N}(\mathbf{w} - \mathbf{u}) \leq \mathbf{N}(\mathbf{w}_0 - \mathbf{u})$, para todo $\mathbf{w} \in v(\mathbf{w}_0) \cap R_v(\mathbf{u})$, onde $v(\mathbf{w}_0)$ é uma vizinhança de $\mathbf{w}_0$. Um *buraco profundo* de um empacotamento esférico Λ em $\mathbb{R}^n$ é um ponto de $\mathbb{R}^n - \Lambda$ cuja distância de Λ é um máximo absoluto, isto é, um ponto $\mathbf{w}_0 \in R_v(\mathbf{u})$ tal que $\mathbf{N}(\mathbf{w} - \mathbf{u}) \leq \mathbf{N}(\mathbf{w}_0 - \mathbf{u})$, para todo $\mathbf{w} \in R_v(\mathbf{u})$. O *raio de cobertura* de Λ é dado por

$$\beta = \mathbf{N}(\mathbf{w}_0 - \mathbf{u}),$$

onde $\mathbf{w}_0$ é um buraco profundo de Λ.

Uma *translação* por um vetor $\mathbf{u}_0 \in \mathbb{R}^n$ é uma função

$$t_{\mathbf{u}_0} : \mathbb{R}^n \to \mathbb{R}^n$$

dada por

$$t_{\mathbf{u}_0}(\mathbf{u}) = \mathbf{u} + \mathbf{u}_0,$$

para todo $\mathbf{u} \in \mathbb{R}^n$.

Dizemos que um conjunto limitado $X \subset \mathbb{R}^n$ é mensurável quando, tomando-se um bloco $A \subset \mathbb{R}^n$ que contenha X, a função característica $\chi_X : A \to \mathbb{R}$ é integrável. Quando X é mensurável, seu *volume* é dado pela integral múltipla

$$V(X) = \int_X \cdots \int dx_1 dx_2 \cdots dx_n,$$

sobre o conjunto X.

O volume de $E_\rho(\mathbf{0})$ é dado por

$$V(E_\rho(\mathbf{0})) = \frac{\pi^{\frac{n}{2}} \rho^n}{G\left(\frac{n+2}{2}\right)},$$

onde

$$G(\alpha) = \int_0^\infty e^{-\mathbf{v}} \mathbf{v}^{\alpha-1} d\mathbf{v}, \alpha > 0,$$

é a função Gama. Sendo n um inteiro positivo, há dois casos a serem considerados:

1. Se n é par, digamos $n = 2k$, então

$$V(E_\rho(\mathbf{0})) = \frac{\pi^k \rho^{2k}}{k!}.$$

2. Se n é ímpar, digamos $n = 2k + 1$, então

$$V(E_\rho(\mathbf{0})) = \frac{2^{2k+1} k! \pi^k \rho^{2k+1}}{(2k+1)!}.$$

Note que $V(E_\rho(\mathbf{c})) = V(E_\rho(\mathbf{0}))$, pois o volume é invariante por translação.

Uma região em $\mathbb{R}^n$ que contém um e somente um ponto de cada classe lateral à direita de Λ em $\mathbb{R}^n$ é chamada de *região fundamental*. Note que região fundamental não é única, mas toda região fundamental tem o mesmo volume, pois o volume é invariante por translação. O *volume fundamental* de um reticulado Λ é o volume de uma região fundamental, o qual será denotado por $V(\Lambda)$.

Seja $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ uma base sobre $\mathbb{Z}$ do reticulado Λ. Então o conjunto

$$\mathbf{F} = F(\mathbf{u}_1, \ldots, \mathbf{u}_n) = \left\{ \sum_{i=1}^{n} r_i \mathbf{u}_i : 0 \leq r_i < 1 \right\}$$

é uma região fundamental de Λ. De fato, dado $\mathbf{u} \in \mathbb{R}^n$, digamos $\mathbf{u} = s_1\mathbf{u}_1 + \cdots + s_n\mathbf{u}_n$, $s_i \in \mathbb{R}$; como para cada i, $s_i = r_i + t_i$, onde $0 \leq r_i < 1$ e $t_i \in \mathbb{Z}$, temos $\mathbf{u} = \mathbf{w} + \mathbf{v}$ com $\mathbf{w} \in \mathbf{F}$ e $\mathbf{v} \in \Lambda$. Finalmente, se $\mathbf{u} = \mathbf{w}' + \mathbf{v}'$ com $\mathbf{w}' \in \mathbf{F}$ e $\mathbf{v}' \in \Lambda$, então $\mathbf{w} + \mathbf{v} = \mathbf{w}' + \mathbf{v}'$ se, e somente se, $\mathbf{w} = \mathbf{w}'$ e $\mathbf{v} = \mathbf{v}'$, pois $t_i - t_i' \in \mathbb{Z}$ e $0 \leq |r_i - r_i'| < 1$. A região fundamental $\mathbf{F}$ é chamada *região fundamental básica* de Λ.

Seja Λ um reticulado em $\mathbb{R}^n$. Então obtemos uma partição de $\mathbb{R}^n$ em classes de equivalência módulo Λ, isto é, dados $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, $\mathbf{u} \equiv \mathbf{v} \pmod{\Lambda}$ se, e somente se, $\mathbf{v} - \mathbf{u} \in \Lambda$. Assim, a classe de equivalência de $\mathbf{u}$ ou a translação do reticulado Λ por $\mathbf{u}$ é o conjunto

$$\Lambda + \mathbf{u} = \{\mathbf{w} + \mathbf{u} : \mathbf{w} \in \Lambda\}.$$

Note que, $\Lambda + \mathbf{u}$ pode ser caracterizado como o conjunto de pontos em $\mathbb{R}^n$ que são gerados pelo grupo das translações por elementos de Λ,

$$t(\Lambda) = \{t_{\mathbf{w}} : \mathbf{v} \longmapsto \mathbf{w} + \mathbf{v} : \mathbf{w} \in \Lambda, \mathbf{v} \in \mathbb{R}^n\},$$

agindo no ponto inicial $\mathbf{u}$, isto é,

$$\begin{array}{rccc} t: & \Lambda \times \mathbb{R}^n & \to & \mathbb{R}^n \\ & (t_{\mathbf{w}}, \mathbf{u}) & \mapsto & t_{\mathbf{w}}(\mathbf{u}) = \mathbf{w} + \mathbf{u} \end{array}.$$

Logo,

$$\Lambda + \mathbf{u} = \{t_{\mathbf{w}}(\mathbf{u}) : t_{\mathbf{w}} \in t(\Lambda)\}.$$

Em outras palavras, $\Lambda + \mathbf{u}$ é a órbita de $\mathbf{u}$ sob o grupo $t(\Lambda)$.

Lema 1.1 *Seja Λ um reticulado de $\mathbb{R}^n$. Então $\mathbb{R}^n = \dot{\cup}_{\mathbf{w}\in\Lambda}(\mathbf{F} + \mathbf{w})$.*

Prova. Seja $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ uma base sobre $\mathbb{Z}$ do reticulado Λ. Então $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ é uma base sobre $\mathbb{R}$ de $\mathbb{R}^n$. Assim, para cada $\mathbf{u} \in \mathbb{R}^n$, obtemos

$$\mathbf{u} = a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n, a_i \in \mathbb{R}.$$

Como, para cada $i = 1, \ldots, n$, temos $a_i = b_i + c_i$, onde $b_i \in \mathbb{Z}$ e $0 \leq a_i < 1$, segue-se que $\mathbf{u} = \mathbf{v} + \mathbf{x}$ com $\mathbf{v} \in \Lambda$ e $\mathbf{x} \in \mathbf{F}$. Portanto, $\mathbf{u} \in \dot{\cup}_{\mathbf{w}\in\Lambda}(\mathbf{F} + \mathbf{w})$. ■

Lema 1.2 *Seja Λ um reticulado em $\mathbb{R}^n$. Então $V(\Lambda) = \det\Lambda = V(\mathbf{F})$.*

Prova. Seja $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ uma base sobre $\mathbb{Z}$ do reticulado Λ em $\mathbb{R}^n$. Por definição,

$$V(\mathbf{F}) = \int_{\mathbf{F}} \cdots \int dr_1 dr_2 \cdots dr_n.$$

Se $\mathbf{u}_i = (u_{1i}, \ldots, u_{ni})$, então fazendo a mudança de variáveis

$$r_i = \sum_{j=1}^{n} u_{ji} r'_j,$$

onde $0 \leq r'_j < 1$, obtemos

$$V(\mathbf{F}) = \int_0^1 \cdots \int_0^1 |\det(u_{ji})|\, dr'_1 \cdots dr'_n = |\det(u_{ji})|.$$

Portanto, $V(\Lambda) = \det\Lambda = V(\mathbf{F})$. ■

A *densidade* $\Delta(\Lambda)$ de um reticulado Λ em $\mathbb{R}^n$ é a relação entre o volume ocupado pelas esferas na região fundamental e o volume da região fundamental, isto é,

$$\Delta(\Lambda) = \frac{V(E_\rho(\mathbf{0}))}{\det \Lambda}.$$

A *densidade de centro* é

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

Exemplo 1.5 *Seja $\Lambda = \mathbb{Z}^2$ um reticulado em $\mathbb{R}^2$. Então o conjunto $\{(1,0),(0,1)\}$ é uma base sobre $\mathbb{Z}$ de Λ. O raio de empacotamento é $\rho = \frac{1}{2}$ e*

$$V(\Lambda) = \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1.$$

Assim, temos $\Delta(\Lambda) = \frac{\pi}{4}$ e $\delta(\Lambda) = \frac{1}{4}$.

O *parâmetro de Hermite* é

$$\gamma(\Lambda) = 4(\delta(\Lambda))^{\frac{2}{n}} \text{ e } \lambda(\Lambda) = -\log_2\left(\frac{\Delta(\Lambda)}{n}\right)$$

é o *expoente de densidade* de Λ.

Um empacotamento esférico Λ em $\mathbb{R}^n$ que é obtido colocando-se uma configuração fixa de s esferas em cada região fundamental de Λ é chamado um *empacotamento periódico*. Neste caso,

$$\Delta(\Lambda) = \frac{sV(E_\rho(\mathbf{0}))}{\det \Lambda}.$$

Corolário 1.3 *Sejam Λ um reticulado em $\mathbb{R}^n$ e Γ um sub-reticulado de Λ. Então*

$$[\Lambda : \Gamma] = \frac{V(\Gamma)}{V(\Lambda)}.$$

Em particular, $[\Lambda : r\Lambda] = r^n$, para todo $r \in \mathbb{Z}$. ■

Corolário 1.4 *Sejam Λ, Γ e Π reticulados em $\mathbb{R}^n$ tais que $\Pi \subseteq \Gamma \subseteq \Lambda$. Então*

$$[\Lambda : \Pi] = [\Lambda : \Gamma][\Gamma : \Pi].$$

■

Lema 1.3 *Sejam Λ um reticulado em $\mathbb{R}^n$ e Γ um sub-reticulado de Λ. Então existe um número finito de reticulados Π entre Γ e Λ.*

Prova. Sejam $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ uma base sobre $\mathbb{Z}$ de Γ e

$$\mathbf{F} = \left\{ \sum_{i=1}^{n} r_i \mathbf{u}_i : 0 \leq r_i < 1 \right\}.$$

Então existe um número finito de elementos de Λ pertencentes a $\mathbf{F}$, pois $\mathbf{F}$ é limitado. Assim, se Π é um reticulado entre Γ e Λ, então o conjunto $\Pi \cap \mathbf{F}$ tem um número finito de elementos. Seja $\Pi \cap \mathbf{F} = S$.

Afirmação. S e Γ determinam Π.

De fato. Seja $\mathbf{v} \in \Pi$. Então existe $\mathbf{u} \in \Gamma$ tal que $\mathbf{v} - \mathbf{u} \in \mathbf{F}$. Logo, $\mathbf{v} - \mathbf{u} \in S$. Portanto, $\Pi = S + \Gamma$. ■

Corolário 1.5 *Sejam Γ um reticulado em $\mathbb{R}^n$ e $N \in \mathbb{Z}_+$. Então existe um número finito de reticulados Λ em $\mathbb{R}^n$ que contêm Γ, tais que $[\Lambda : \Gamma] = N$.*

Prova. Seja Λ um reticulado em $\mathbb{R}^n$ tal que $[\Lambda : \Gamma] = N$. Então $N\Lambda \subseteq \Gamma \subseteq \Lambda$. Pelo Lema 1.3, existe um número finito de reticulados Λ em $\mathbb{R}^n$ que contêm Γ, tais que $[\Lambda : \Gamma] = N$. ■

Capítulo 2

Classificação dos sub-reticulados não equivalentes do reticulado hexagonal

Neste capítulo apresentaremos um método para classificar todos os sub-reticulados de índice N não equivalentes do reticulado hexagonal. Antes de iniciarmos daremos alguns resultados da teoria dos números que serão necessários para uma melhor compreensão.

2.1 Resíduos Quadráticos

Esta seção será destinada ao estudo dos pré-requisitos sobre a teoria dos números, especialmente os resíduos quadráticos, fundamentais para o desenvolvimento da seção subsequente, sobre o reticulado hexagonal. Ao leitor interessado em mais informações, recomendamos Santos [14].

Sejam p um número primo e $\mathbb{F}_p$ um corpo finito. Dizemos que $a \in \mathbb{F}_p$ é um *quadrado* (resíduo quadrático módulo p) se existir $x \in \mathbb{F}_p$ tal que

$$x^2 = a,$$

ou, equivalentemente, a congruência

$$x^2 \equiv a \,(\mathrm{mod}\, p)$$

tem solução. Esta definição pode ser estendida para qualquer inteiro positivo m tal que $\mathrm{mdc}(a, m) = 1$. Suponhamos que $p > 2$ e $\mathrm{mdc}(a, p) = 1$. O *símbolo de Legendre* é definido

por

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ é resíduo quadrático módulo } p \\ -1 & \text{caso contrário} \end{cases}.$$

Pode ser mostrado o critério de Euler:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Além disso,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Note que, se $p = 8k \pm 1$, então $\frac{1}{8}(p^2-1)$ é par. Se $p = 8k \pm 3$, então $\frac{1}{8}(p^2-1)$ é ímpar. Logo,

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

Pode ser provado que

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1, 7 \pmod{8} \\ -1 & \text{se } p \equiv 3, 5 \pmod{8}. \end{cases}$$

Portanto,

$$\left(\frac{4}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{2}{p}\right) = 1 \text{ se } p \equiv 1, 3, 5 \text{ ou } 7 \pmod{8}.$$

Lema 2.1 *Seja* $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ *tal que* $\text{mdc}(a, p) = 1$. *Então*

$$f(x) \equiv 0 \pmod{p}$$

tem no máximo duas raízes.

Prova. Suponhamos, por absurdo, que a congruência

$$f(x) \equiv 0 \pmod{p}$$

tenha três soluções não congruentes módulo p, digamos x_1, x_2 e x_3. Então

$$\begin{aligned} f(x) - f(x_1) &= a(x^2 - x_1^2) + b(x - x_1) \\ &= (x - x_1)[a(x + x_1) + b]. \end{aligned}$$

Como

$$f(x_j) \equiv f(x_1) \pmod{p}, j = 2, 3,$$

temos que

$$f(x_j) - f(x_1) = (x_j - x_1)[a(x_j + x_1) + b] \equiv 0 \pmod{p}.$$

Logo, a congruência linear

$$[ax + (b + ax_1)] \equiv 0 \pmod{p}$$

tem duas soluções não congruentes módulo p, o que é uma contradição. ■

Como $\text{mdc}(a, p) = 1$ temos que

$$ax^2 + bx + c \equiv 0 \pmod{p} \Leftrightarrow x^2 + a^{-1}bx + a^{-1}c \equiv 0 \pmod{p}.$$

Logo,

$$\begin{aligned} x^2 + a^{-1}bx + a^{-1}c &\equiv x^2 + a^{-1}bx + \left[2^{-1}a^{-1}b\right]^2 - \left[2^{-1}a^{-1}b\right]^2 + a^{-1}c \\ &\equiv (x + 2^{-1}a^{-1}b)^2 - 2^{-2}a^{-2}(b^2 - 4ac). \end{aligned}$$

Portanto, a congruência

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

tem soluções se, e somente se,

$$\Delta = b^2 - 4ac$$

é um resíduo quadrático módulo p, isto é,

$$\left(\frac{\Delta}{p}\right) \equiv \Delta^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Teorema 2.1 (Teorema Chinês dos Restos) *Se* $\text{mdc}(a_i, m_i) = \text{mdc}(m_i, m_j) = 1$,

para $i \neq j$ e c_i inteiro, então o sistema

$$\begin{aligned} a_1x &\equiv c_1 (\mathrm{mod}\, m_1) \\ a_2x &\equiv c_2 (\mathrm{mod}\, m_2) \\ a_3x &\equiv c_3 (\mathrm{mod}\, m_3) \\ &\vdots \\ a_rx &\equiv c_r (\mathrm{mod}\, m_r) \end{aligned}$$

possui solução e a solução é única módulo $m = m_1 m_2 \cdots m_r$. ■

Observação 2.1 *Note que o número de soluções da congruência*

$$x^2 + x + 1 \equiv 0 \,(\mathrm{mod}\, p)$$

pode ser escrito na forma

$$\left(1 + \left(\frac{p}{3}\right)\right),$$

se $p > 3$, pois $\Delta = -3$. Por exemplo, se $p = 7$, então $2^2 \equiv -3 \,(\mathrm{mod}\, 7)$ e $x_1 = 2$, $x_2 = 4$ são as soluções não congruentes. Portanto, se

$$N = \prod_{i=1}^{n} p_i^{k_i},$$

onde os p_i são números primos distintos, então pelo Teorema Chinês dos Restos o número de soluções da congruência

$$x^2 + x + 1 \equiv 0 \,(\mathrm{mod}\, N)$$

é dado por

$$\nu_1 = \begin{cases} 0 & \text{se } 2 \mid N \text{ ou } 9 \mid N \\ \prod\limits_{i=1, p_i>3}^{n} \left(1 + \left(\frac{p_i}{3}\right)\right) & \text{caso contrário} \end{cases}. \tag{2.1}$$

Observação 2.2 *Note que o número de soluções da congruência*

$$x^2 - 1 \equiv 0 \,(\mathrm{mod}\, p)$$

pode ser escrito na forma

$$\left(1+\left(\frac{4}{p}\right)\right),$$

se $p \geq 3$, *pois* $\Delta = 4$. *Por exemplo, se* $p = 7$, *então* $2^2 \equiv 4 \pmod 7$ *e* $x_1 = -1$, $x_2 = 1$ *são as soluções não congruentes. Portanto, se*

$$N = \prod_{i=1}^{n} p_i^{k_i},$$

onde os p_i *são números primos distintos, então pelo Teorema Chinês dos Restos, o número de soluções da congruência*

$$x^2 - 1 \equiv 0 \pmod N$$

é dado por

$$\mu = 2^{n-1+v_2},$$

onde

$$v_2 = \begin{cases} 2 & se\ N \equiv 0 \pmod 8 \\ 1 & se\ N \equiv 1,3,4,5\ ou\ 7 \pmod 8 \\ 0 & se\ N \equiv 2\ ou\ 6 \pmod 8 \end{cases}, \tag{2.2}$$

pois na fatoração de N *pode ocorrer primo par.*

2.2 O Reticulado Hexagonal

Nesta seção apresentaremos um método para classificar todos os sub-reticulados de índice N não equivalentes do reticulado hexagonal.

O reticulado hexagonal $\Lambda = A_2$ é gerado pelos vetores

$$\mathbf{u}_1 = (1,0) \text{ e } \mathbf{u}_2 = (-\frac{1}{2}, \frac{\sqrt{3}}{2}).$$

Note que, podemos identificar

$$(1,0) \leftrightarrow 1, (-\frac{1}{2}, \frac{\sqrt{3}}{2}) \leftrightarrow \omega \text{ e } (-\frac{1}{2}, -\frac{\sqrt{3}}{2}) \leftrightarrow \omega^2,$$

onde ω é a raiz cúbica da unidade

$$\omega = \exp(\frac{2\pi i}{3}).$$

Portanto, a função

$$\varphi : \mathbb{Z}[\omega] \to A_2$$

definida por

$$\varphi(1) = (1, 0) \text{ e } \varphi(\omega) = (-\frac{1}{2}, \frac{\sqrt{3}}{2})$$

é um homomorfismo injetor de módulos sobre $\mathbb{Z}$, isto é, podemos identificar A_2 com o anel dos inteiros de Eisenstein-Jacobi $\mathbb{Z}[\omega]$.

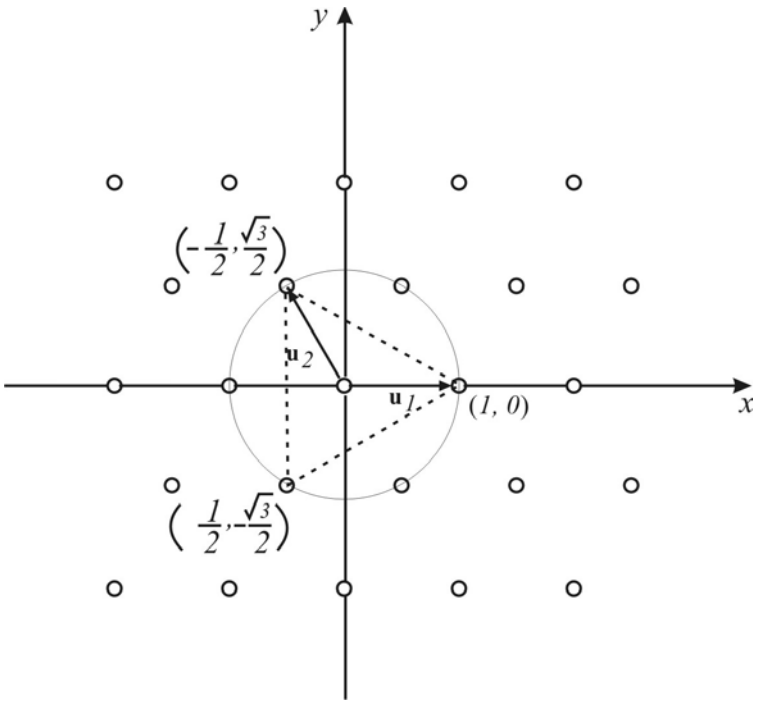

Figura 2-1: O reticulado hexagonal $\Lambda = A_2$.

Como $\mathbb{Z}[\omega]$ é um domínio de ideais principais, temos que todo ideal de $\mathbb{Z}[\omega]$ é da forma

$$\langle \alpha \rangle = \{z\alpha : z \in \mathbb{Z}[\omega]\}.$$

É fácil verificar que, para cada ideal I de $\mathbb{Z}[\omega]$ o conjunto $\varphi(I)$ é um reticulado de $\mathbb{R}^2$. Mas a recíproca é, em geral, falsa. Mas temos o seguinte resultado:

Proposição 2.1 *Seja Λ um reticulado qualquer de $\mathbb{R}^2$. Se $\omega\beta \in I$, para todo $\beta \in I = \varphi^{-1}(\Lambda)$, então I é um ideal de $\mathbb{Z}[\omega]$. Neste caso, dizemos que Λ é um* reticulado ideal *de $\mathbb{R}^2$.*

Prova. Dados $\alpha, \beta \in I$, existem $\mathbf{x}, \mathbf{y} \in \Lambda$ tais que $\mathbf{x} = \varphi(\alpha)$ e $\mathbf{y} = \varphi(\beta)$. Logo,

$$\mathbf{x} - \mathbf{y} = \varphi(\alpha) - \varphi(\beta) = \varphi(\alpha - \beta),$$

isto é, $\alpha - \beta \in I$. Como $\omega\alpha \in I$, para todo $\alpha \in I$, temos que $(a+b\omega)\alpha \in I$, para quaisquer $a, b \in \mathbb{Z}$. Portanto, I é um ideal de $\mathbb{Z}[\omega]$. ■

Seja Γ um sub-reticulado de A_2 tal que $[A_2 : \Gamma] = N$. Então pela Observação 1.1 existe uma matriz particionadora

$$\mathbf{B} = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$$

tal que $\det \mathbf{B} = N$. Se

$$\mathbf{M} = \begin{pmatrix} 1 & 0 \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$$

é a matriz geradora de A_2 e $\mathbf{N}$ é a matriz geradora de Γ, então

$$\begin{aligned} \mathbf{N} &= \mathbf{BM} \\ &= \begin{pmatrix} a & 0 \\ b - \frac{1}{2}c & \frac{\sqrt{3}}{2}c \end{pmatrix}, \end{aligned}$$

isto é, Γ é gerado pelos vetores

$$\mathbf{v}_1 = (a, 0) \text{ e } \mathbf{v}_2 = (b - \frac{1}{2}c, \frac{\sqrt{3}}{2}c).$$

Como A_2/Γ é um grupo abeliano finitamente gerado, temos que A_2/Γ é um grupo cíclico de ordem N ou A_2/Γ é isomorfo a um produto direto $\mathbb{Z}_{\frac{N}{m}} \times \mathbb{Z}_m$ de grupos cíclicos, onde m é um fator de $\frac{N}{m}$. Neste caso, $m^2 \mid N$. Dizemos que Γ é um *sub-reticulado primitivo* de A_2 se A_2/Γ é cíclico.

Teorema 2.2 *Seja $N = \prod_{i=1}^{n} p_i^{k_i}$, onde os p_i são números primos distintos. Então o*

número de sub-reticulados primitivos não equivalentes de $\Lambda = A_2$ *de índice* N *é*

$$f_1(N) = \frac{1}{6}N\prod_{i=1}^{n}(1+\frac{1}{p_i}) + \frac{\nu_1}{3} + 2^{n-2+\nu_2},$$

onde ν_1 *é dado por* (2.1) *e* ν_2 *é dado por* (2.2).

Prova. Nosso problema é equivalente a determinar todos os homomorfismos de módulos sobre $\mathbb{Z}$

$$\varphi : A_2 \to \mathbb{Z}/N\mathbb{Z} = \mathbb{Z}_N,$$

pois $\ker\varphi = \Gamma$ é um sub-reticulado de A_2. Como A_2 é gerado por 1 e ω temos que φ é completamente determinado por $\varphi(1)$ e $\varphi(\omega)$. Note que,

$$\ker(r\varphi) = \ker\varphi, \forall r \in U(\mathbb{Z}_N).$$

O número de sub-reticulados primitivos de índice N em um reticulado qualquer em $\mathbb{R}^2$ é dado pela função ψ (cf. [15, Theorem 8, p. 134])

$$\psi(N) = N\prod_{p|N}(1+\frac{1}{p}). \tag{2.3}$$

Como sub-reticulados equivalentes são invariantes por rotação e reflexão, temos que dividir a expressão (2.3) por 6. Além disso, devemos adicionar os sub-reticulados de A_2 que já tenham sido rotacionados ou reflexionados: neste caso, devemos dividir somente por 2 ou 3, respectivamente. Assim, há dois casos a serem considerados:

1º Caso. Suponhamos que Γ tenha somente rotação. Então, sem perda de generalidade, podemos assumir que

$$\varphi(1) = 1, \varphi(\omega) = x \text{ e } \varphi(\omega^2) = x^2,$$

onde

$$x^2 + x + 1 \equiv 0 \,(\mathrm{mod}\, N),$$

pois

$$\varphi(\omega^2 + \omega + 1) = \varphi(0) = 0.$$

O número de soluções desta congruência, pela Observação 2.1, é dada por ν_1. Assim, o

termo adicional é dado por

$$(\frac{1}{2}-\frac{1}{6})\nu_1=\frac{1}{3}\nu_1.$$

2º Caso. Suponhamos que Γ tenha somente reflexão. Então, sem perda de generalidade, temos as seguintes possibilidades:

$$\begin{aligned}\varphi(1) &= 1, \varphi(\omega)=x \text{ e } \varphi(\omega^2)=-x-1,\\ \varphi(1) &= -x-1, \varphi(\omega)=1 \text{ e } \varphi(\omega^2)=x,\\ \varphi(1) &= x, \varphi(\omega)=-x-1 \text{ e } \varphi(\omega^2)=1,\end{aligned}$$

onde

$$x^2-1\equiv 0\,(\mathrm{mod}\,N).$$

Assim, pela Observação 2.2, o número de sub-reticulados não equivalentes é dado por

$$3\cdot 2^{n-1+\nu_2}.$$

Logo, o termo adicional é dado por

$$(\frac{1}{3}-\frac{1}{6})3\cdot 2^{n-1+\nu_2}=2^{n-2+\nu_2}.$$

Portanto,

$$f_1(N)=\frac{1}{6}N\prod_{i=1}^{n}(1+\frac{1}{p_i})+\frac{\nu_1}{3}+2^{n-2+\nu_2}$$

é o número de sub-reticulados primitivos não equivalentes de A_2 de índice N. ■

Teorema 2.3 *O número de sub-reticulados não equivalentes de $\Lambda=A_2$ com índice N é*

$$f(N)=\sum_{m^2|N} f_1(\frac{N}{m^2}).$$

Prova. Seja Γ um sub-reticulado qualquer de A_2 com índice N. Então Γ pode ser escrito de modo único como

$$\Gamma=m\Gamma',$$

N	$f_1(N)$	$f(N)$
1	1	1
2	1	1
3	2	2
4	2	3
5	2	2
6	3	3
7	3	3
8	4	5
9	3	4
10	4	4
11	3	3
12	6	8
13	4	4
14	5	5
15	6	6
16	6	9
17	4	4
18	7	8
19	5	5
20	8	10

Tabela 2.1: Número de sub-reticulados primitivos e não equivalentes de Λ

onde Γ' é um sub-reticulado primitivo de A_2 com índice $\frac{N}{m^2}$ em A_2, pois

$$[A_2 : \Gamma] = N = m^2 \cdot \frac{N}{m^2},$$

e se

$$\mathbf{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

é a matriz geradora de Γ, então

$$\mathbf{M}' = \begin{pmatrix} \frac{a}{m} & \frac{b}{m} \\ \frac{c}{m} & \frac{d}{m} \end{pmatrix},$$

onde $\mathbf{M} = m\mathbf{M}'$, é a matriz geradora de Γ'. Portanto,

$$f(N) = \sum_{m^2|N} f_1(\frac{N}{m^2})$$

é o número de sub-reticulados não equivalentes de A_2 com índice N. ■

Teorema 2.4 *Seja* Γ *um reticulado em* $\mathbb{R}^2$ *com matriz geradora*

$$\mathbf{N} = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}, a, b, c \in \mathbb{Z}.$$

Então:

1. *O reticulado hexagonal* A_2 *contém uma cópia similar de* Γ *se, e somente se,*

$$4ac - b^2 = 3m^2, m \in \mathbb{Z}.$$

2. *O reticulado hexagonal* A_2 *contém uma cópia de* Γ *se, e somente se,*

$$4ac - b^2 = 3m^2, m \in \mathbb{Z}$$

e

$$a = 3^k \prod_{p_i \equiv 1 \pmod 3} p_i^{l_i} \prod_{q_i \equiv -1 \pmod 3} q_i^{2m_i}.$$

Prova. 1. Seja Γ' uma cópia similar de Γ. Então existe $r \in \mathbb{Q}$ $(\mathbb{Z})$ tal que

$$ac - \frac{b^2}{4} = r^2 \det \Gamma' \Leftrightarrow 4ac - b^2 = 3m^2, m \in \mathbb{Z}.$$

2. Como

$$4a \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} = \begin{pmatrix} 2a & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 3m^2 \end{pmatrix} \begin{pmatrix} 2a & b \\ 0 & 1 \end{pmatrix},$$

temos que $4a\Gamma \subseteq A_2$. Portanto, $\Gamma \subseteq A_2$. ■

Teorema 2.5 *Seja* Γ *um sub-reticulado qualquer de* A_2 *com índice* N. *Então* $d^2_{\min}(\Gamma) \leq N$. *Além disso,* $d^2_{\min}(\Gamma) = N$ *se, e somente se,* Γ *é um reticulado ideal.*

Prova. Como A_2 é o reticulado mais denso em $\mathbb{R}^2$ temos que $d^2_{\min}(\Gamma) \leq N$, para todo sub-reticulado Γ de A_2. ■

Capítulo 3

Construções multinível

Neste capítulo apresentaremos algumas definições e resultados básicos sobre códigos, com o objetivo de construir reticulados a partir de um dado código corretor de erro, o qual generaliza a construção de Leech. Como referência indicamos MacWilliams e Sloane [10] ou Silva [16].

3.1 Códigos

Consideremos um *alfabeto* (conjunto) $\mathbb{F}$ com q elementos e $\mathbb{I} \subseteq \mathbb{Z}$. Um *espaço de seqüências* $\mathbb{F}^{\mathbb{I}}$ é o conjunto de todas as seqüências $\mathbf{c} = (c_i)_{i\in\mathbb{I}}$, cujos elementos c_i pertencem ao alfabeto $\mathbb{F}$. Quando

$$\mathbb{I} = \{i : 1 \leq i \leq n\},$$

denotamos $\mathbb{F}^{\mathbb{I}}$ por $\mathbb{F}^n$ e chamamos de conjunto de todas as n-uplas $\mathbf{c} = (c_i)_{i\in\mathbb{I}}$, onde $c_i \in \mathbb{F}$. Um *código* $\mathcal{C}$ sobre um alfabeto $\mathbb{F}$ é qualquer subconjunto não vazio do espaço de seqüências $\mathbb{F}^{\mathbb{I}}$. Quando $\mathcal{C}$ é um subconjunto do conjunto $\mathbb{F}^n$, dizemos que $\mathcal{C}$ é um *código de bloco de comprimento* n.

Exemplo 3.1 *Se* $\mathbb{I} = \{1, 2, 3\}$ *e* $\mathbb{F} = \{0, 1, 2\}$, *então*

$$\mathcal{C} = \{(0, 0, 0), (0, 1, 2)\}$$

é um código de bloco de comprimento $n = 3$.

A *dimensão* do código $\mathcal{C}$ é o número $k = \log_{|\mathbb{F}|} \mid \mathcal{C} \mid$. Note que k não é necessariamente inteiro. A *distância de Hamming* $d_H(\mathbf{c}, \mathbf{c}')$ entre duas seqüências $\mathbf{c}, \mathbf{c}' \in \mathbb{F}^n$ é o número de

componentes onde elas diferem:

$$d_H(\mathbf{c}, \mathbf{c}') = \mid \{i \in \mathbb{I} : c_i \neq c_i'\} \mid .$$

O *peso de Hamming* de $\mathbf{c} \in \mathbb{F}^n$, denotado por $w_H(\mathbf{c})$, é definido por

$$w_H(\mathbf{c}) = d_H(\mathbf{c}, \mathbf{0}),$$

onde $\mathbf{0}$ é a seqüência nula. Observe que $w_H(\mathbf{c})$ é igual ao número de componentes não nulas de $\mathbf{c}$.

Exemplo 3.2 *Se* $\mathbb{F} = \{0, 1, 2\}$, $\mathbf{c} = (2, 1, 1, 1, 2)$ *e* $\mathbf{c}' = (0, 1, 2, 2, 0)$, *então* $d_H(\mathbf{c}, \mathbf{c}') = 4$, $w_H(\mathbf{c}) = 5$ *e* $w_H(\mathbf{c}') = 3$.

Se $|\mathcal{C}| > 2$, então a *distância mínima de Hamming* de $\mathcal{C}$ é definida por

$$d_H(\mathcal{C}) = \min \{d_H(\mathbf{c}, \mathbf{c}') : \mathbf{c}, \mathbf{c}' \in \mathcal{C}, \mathbf{c} \neq \mathbf{c}'\},$$

e o *peso mínimo de Hamming*, é definido por

$$w_H(\mathcal{C}) = \min \{w(\mathbf{c}) : \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq \mathbf{0}\}.$$

Um código de bloco $\mathcal{C}$ de comprimento n sobre um grupo G é um *código de grupo* se $\mathcal{C}$ é um subgrupo do produto direto G^n. Se $\mathcal{C}$ é um código de grupo sobre G, então a mínima distância de Hamming é o peso mínimo de Hamming. Um código linear $\mathcal{C}$ sobre $\mathbb{F}_q = GF(q)$, onde $GF(q)$ é o corpo de Galois com q elementos, é um código de grupo sobre o grupo aditivo de $\mathbb{F}_q$, ou seja, um subgrupo de $\mathbb{F}_q^n$.

Se $\mathcal{C}$ é um código de bloco linear sobre $\mathbb{F}_q$ de comprimento n, dimensão k e distância mínima de Hamming $d_H(\mathcal{C})$, então dizemos que $\mathcal{C}$ é um $[n, k, d]_q$-código, ou o código $\mathcal{C} = [n, k, d]_q$.

Exemplo 3.3 *Se* $\mathbb{F}_2 = \mathbb{Z}_2 = \{0, 1\}$, *então*

$$\mathcal{C} = \{(0, 0, 0), (1, 1, 0), (1, 0, 1), (0, 1, 1)\}$$

é um $[3, 2, 2]_2$*-código.*

Note que em um $[n,k,d]_q$-código, $d_H(\mathbb{C}) = w_H(\mathbb{C})$ e k é necessariamente inteiro.

Seja

$$\varphi : \{0,1\} \to \{-1,1\}$$

a função definida por

$$\varphi(0) = +1 \text{ e } \varphi(1) = -1.$$

Portanto, qualquer $[n,k,d]_2$-código $\mathcal{C}$ pode ser transformado em um código do espaço Euclidiano através da função

$$\begin{array}{rccc} \varphi : & \mathbb{F}_2^n & \to & \mathbb{R}^n \\ & (c_1,\ldots,c_n) & \mapsto & (\varphi(c_1),\ldots,\varphi(c_n)) \end{array}.$$

O código resultante $E_{\mathcal{C}} = \varphi(\mathcal{C})$ é um subconjunto, de ordem $|\mathcal{C}| = 2^k$, de

$$[-1,+1]^n = [-1,+1] \times \cdots \times [-1,+1].$$

Exemplo 3.4 *Seja*

$$\mathcal{C} = \{(0,0),(0,1),(1,0),(1,1)\}.$$

Então

$$E_{\mathcal{C}} = \{(1,1),(1,-1),(-1,1),(-1,-1)\}$$

são os quatro vértices de um quadrado. Observe que $k = n$, o que não ocorrerá se tomarmos o código do Exemplo 3.3*, onde $E_{\mathcal{C}}$ será um subconjunto de ordem* 4 *do cubo.*

Se $\mathbf{c} = (c_1, c_2, \ldots, c_n), \mathbf{c}' = (c_1', c_2', \ldots, c_n') \in \mathcal{C}$, onde $\mathcal{C}$ é um $[n,k,d]_2$-código, então

$$\begin{aligned} \|\varphi(\mathbf{c}) - \varphi(\mathbf{c}')\|^2 &= (\varphi(c_1) - \varphi(c_1'))^2 + \cdots + (\varphi(c_n) - \varphi(c_n'))^2 \\ &= 4d_H(\mathbf{c},\mathbf{c}'), \end{aligned}$$

pois

$$(\varphi(c_i) - \varphi(c_i'))^2 = \begin{cases} 4 & \text{se } c_i \neq c_i' \\ 0 & \text{se } c_i = c_i' \end{cases}.$$

Portanto,

$$d_{\min}^2(E_{\mathcal{C}}) = 4d_H(\mathcal{C}).$$

3.2 Construção de Leech

A construção mais simples de um reticulado de um código de bloco linear é a construção A de Leech [2], a qual passaremos a descrever.

Seja $p \in \mathbb{N}$ um número primo fixado. Sabemos que todo $m \in \mathbb{N}$ pode ser escrito de modo único na forma

$$m = m_0 + m_1 p + \cdots + m_r p^r,$$

onde $0 \leq m_i \leq p-1$, $i = 0, \ldots, r$, isto é, a *expansão de m na base p*. Note que,

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots .$$

Assim, podemos estender a expansão a todo $m \in \mathbb{Z}$.

Sejam $p = 2$ e $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$. Um *arranjo de coordenadas* de $\mathbf{x}$ é dado por

$$\begin{bmatrix} x_{01} & \cdots & x_{0n} \\ x_{11} & \cdots & x_{1n} \\ x_{21} & \cdots & x_{2n} \\ \vdots & \cdots & \vdots \end{bmatrix},$$

onde

$$x_i = x_{0i} + x_{1i}2 + x_{2i}2^2 + \cdots , i = 1, \ldots, n.$$

O número de linhas no arranjo pode ser infinito, mas após um determinado momento elas são todas idênticas.

Exemplo 3.5 *O arranjo de coordenadas do vetor*

$$\mathbf{x} = (4, 3, 2, 1, 0, -1, -2, -3) \in \mathbb{Z}^8$$

é dado por

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

Seja $\mathcal{C}$ um código qualquer (não necessariamente linear). Um empacotamento de esferas em $\mathbb{R}^n$ é definido por

$$\Lambda_{\mathcal{C}} = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \equiv \mathbf{c} \,(\mathrm{mod}\, 2) \text{ para algum } \mathbf{c} \in \mathcal{C}\}.$$

Assim, $\mathbf{x} \in \Lambda_{\mathcal{C}}$ se, e somente se, a primeira linha do arranjo de coordenadas de $\mathbf{x}$ está em $\mathcal{C}$. Portanto, $\Lambda_{\mathcal{C}}$ é um reticulado se, e somente se, $\mathcal{C}$ é um código linear. Além disso,

$$d^2_{\min}(\Lambda_{\mathcal{C}}) \geq \min\{4, d_H(\mathcal{C})\}.$$

Em particular, se $\Lambda_{\mathcal{C}}$ é um reticulado, então

$$d^2_{\min}(\Lambda_{\mathcal{C}}) = \min\{4, d_H(\mathcal{C})\}.$$

De fato, dados $\mathbf{x} = \mathbf{c}+2\mathbb{Z}^n$ e $\mathbf{x}' = \mathbf{c}' + 2\mathbb{Z}^n$ elementos não nulos de $\Lambda_{\mathcal{C}}$, isto é, $\mathbf{x} = \mathbf{c} + \mathbf{v}$ e $\mathbf{x}' = \mathbf{c}' + \mathbf{w}$, onde $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$ e $\mathbf{v}, \mathbf{w} \in 2\mathbb{Z}^n$, há dois casos a serem considerados:

$1^{\underline{0}}$ Caso. Se $\mathbf{c} = \mathbf{c}'$, então $\mathbf{x} - \mathbf{x}' \in 2\mathbb{Z}^n$. Logo,

$$d^2(\mathbf{x}, \mathbf{x}') \geq d^2_{\min}(2\mathbb{Z}^n) = 4,$$

onde a igualdade pode ser alcançada escolhendo-se $\mathbf{x} - \mathbf{x}'$ com uma única componente não nula e igual a um vetor em $2\mathbb{Z}^n$ com norma mínima 4.

$2^{\underline{0}}$ Caso. Se $\mathbf{c} \neq \mathbf{c}'$, então existe um primeiro índice i_0, $1 \leq i_0 \leq n$, tal que $c_{i_0} \neq c'_{i_0}$. Assim, pelo menos $d_H(\mathcal{C})$ componentes de $\mathbf{x} - \mathbf{x}'$ são diferentes de 0, pois $\mathbf{c}$ e $\mathbf{c}'$ representam a primeira linha dos arranjos de coordenadas de $\mathbf{x}$ e $\mathbf{x}'$, respectivamente. Logo,

$$d^2(\mathbf{x}, \mathbf{x}') \geq d_H(\mathcal{C}),$$

onde a igualdade pode ser alcançada escolhendo-se $\mathbf{x} - \mathbf{x}'$ uma seqüência de peso mínimo.

Note que $\Lambda_{\mathcal{C}}$ é dado explicitamente como a união de $|\mathcal{C}|$ classes laterais de $2\mathbb{Z}^n$. Então a região de Voronoi contém $|\mathcal{C}|$ centros de esferas. Como

$$|\mathcal{C}| = [\Lambda_{\mathcal{C}} : 2\mathbb{Z}^n] = \frac{V(2\mathbb{Z}^n)}{V(\Lambda_{\mathcal{C}})},$$

temos que

$$\begin{aligned} V(\Lambda_{\mathcal{C}}) &= \frac{V(2\mathbb{Z}^n)}{|\mathcal{C}|} \\ &= \frac{(V(2\mathbb{Z}))^n}{2^k} \\ &= \frac{2^n}{2^k} \\ &= 2^{n-k}. \end{aligned}$$

Além disso, $\Lambda_{\mathcal{C}}$ é similar a $E_{\mathcal{C}}$. De fato, a função

$$\begin{array}{rccc} \varphi: & \Lambda_{\mathcal{C}} & \to & E_{\mathcal{C}} \\ & (x_1, \ldots, x_n) & \mapsto & (1-2x_1, \ldots, 1-2x_n) \end{array}$$

transforma $\Lambda_{\mathcal{C}}$ em $E_{\mathcal{C}}$.

A Construção A de Leech pode ser generalizada da seguinte maneira: sejam Λ um reticulado em $\mathbb{R}^l$ e Γ um sub-reticulado de Λ de mesmo posto. Então $[\Lambda : \Gamma] = N$. Assim, Λ é a união disjunta das N classes laterais de Γ, isto é,

$$\Lambda = \bigcup_{i=1}^{N} (\Gamma + \mathbf{x}_i), \mathbf{x}_i \in \Lambda.$$

Seja G um *grupo de rótulo* abeliano tal que

$$\varphi : G \to \Lambda/\Gamma$$

seja um isomorfismo. Se

$$\xi : G \to [\Lambda/\Gamma]$$

é a composição de φ com a aplicação natural de Λ/Γ em $[\Lambda/\Gamma]$, então φ leva cada $g \in G$ na classe lateral ou na translação $\Gamma + \xi(g)$. Reciprocamente, existe uma correspondente aplicação de rótulo

$$\pi : \Lambda \to G$$

que leva os elementos das classes laterais $\varphi(g) = \Gamma + \xi(g)$ para as classes laterais de rótulo $g \in G$.

Dado um código de grupo $\mathcal{C}$ sobre G, definimos

$$\Lambda_{\mathcal{C}} = \bigcup_{\mathbf{c}\in\mathcal{C}} \varphi(\mathbf{c}),$$

onde

$$\begin{aligned}\varphi(\mathbf{c}) &= \varphi(\mathbf{c}_1)\times\varphi(\mathbf{c}_2)\times\cdots\times\varphi(\mathbf{c}_n)\\ &= \Gamma^n + \xi(\mathbf{c})\\ &= \Gamma^n + (\xi(\mathbf{c}_1),\xi(\mathbf{c}_2),\ldots,\xi(\mathbf{c}_n))\,.\end{aligned}$$

O empacotamento esférico $\Lambda_{\mathcal{C}}$ em $\mathbb{R}^{nl}$ é chamado de *Construção generalizada A* de reticulados, baseada na partição de um único *nível* Λ/Γ e no código $\mathcal{C}$. Note que, $\Lambda_{\mathcal{C}}$ é dado explicitamente como a união de $|\mathcal{C}|$ classes laterais de Γ, ou $|\mathcal{C}|$ *maneiras*. Então a região de Voronoi contém $|\mathcal{C}|$ centros de esferas. Deste modo, temos

$$V(\Lambda_{\mathcal{C}}) = \frac{V(\Gamma)^n}{|\mathcal{C}|}$$

e

$$d^2_{\min}(\Lambda_{\mathcal{C}}) \geq \min\left\{d^2_{\min}(\Gamma), d_H(\mathcal{C})d^2_{\min}(\Lambda)\right\}.$$

Exemplo 3.6 *Sejam* $\Lambda = \mathbb{Z}$ *e* $\Gamma = 2\mathbb{Z}$. *Então* Λ/Γ *é uma cadeia de partições com* 1*-nível e* 2*-maneiras. Neste caso, tomando*

$$G = \{e, g\} \cong \mathbb{Z}_2, [\Lambda/\Gamma] = \{0,1\}, \xi(e) = 0 \;\; e \;\; \xi(g) = 1,$$

temos que

$$\Lambda_{\mathcal{C}} = \bigcup_{\mathbf{c}\in\mathcal{C}} \varphi(\mathbf{c}),$$

onde

$$\begin{aligned}\varphi(\mathbf{c}) &= \varphi(\mathbf{c}_1)\times\varphi(\mathbf{c}_2)\times\cdots\times\varphi(\mathbf{c}_n)\\ &= \Gamma^n + \xi(\mathbf{c})\\ &= \Gamma^n + (\xi(\mathbf{c}_1),\xi(\mathbf{c}_2),\ldots,\xi(\mathbf{c}_n))\end{aligned}$$

e $\mathcal{C}$ *um* $(n,k,d)_2$ *código sobre* G*, com os seguintes parâmetros:*

$$\begin{aligned} d^2_{\min}(\Lambda_{\mathcal{C}}) &= \min\{4, d_H(\mathcal{C})\}, \\ V(\Lambda_{\mathcal{C}}) &= 2^{n-k}, \\ \gamma(\Lambda_{\mathcal{C}}) &= 2^{\frac{2(k-n)}{n}} \cdot d^2_{\min}(\Lambda_{\mathcal{C}}). \end{aligned}$$

Para o código $\mathcal{C} = [2,1,2]_2$*, obtemos que*

$$d^2_{\min}(\Lambda_{\mathcal{C}}) = 2, V(\Lambda_{\mathcal{C}}) = 2 \ \ e \ \ \gamma(\Lambda_{\mathcal{C}}) = 1.$$

Note que $\Lambda_{\mathcal{C}}$ *é equivalente ao reticulado* D_2 *em* $\mathbb{R}^2$*, (cf. [2]). Para o código* $\mathcal{C} = [4,3,2]_2$*, obtemos que*

$$d^2_{\min}(\Lambda_{\mathcal{C}}) = 2, V(\Lambda_{\mathcal{C}}) = 2 \ \ e \ \ \gamma(\Lambda_{\mathcal{C}}) = \sqrt{2} \approx 1.4142.$$

Note que $\Lambda_{\mathcal{C}}$ *é equivalente ao reticulado* D_4 *em* $\mathbb{R}^4$*, (cf. [2]). Para o código* $\mathcal{C} = [8,4,4]_2$*, obtemos que*

$$d^2_{\min}(\Lambda_{\mathcal{C}}) = 4, V(\Lambda_{\mathcal{C}}) = 2^4 \ \ e \ \ \gamma(\Lambda_{\mathcal{C}}) = 2.$$

Note que $\Lambda_{\mathcal{C}}$ *é equivalente ao reticulado* E_8 *em* $\mathbb{R}^8$*, (cf. [2]).*

Exemplo 3.7 *Sejam* $\Lambda = A_2$ *e* Γ *o sub-reticulado de* Λ *obtido com a matriz particionadora*

$$\mathbf{B} = \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}.$$

Então Λ/Γ *é uma cadeia de partições, com* 1*-nível e* 3*-maneiras. Neste caso, tomando*

$$\begin{aligned} G &= \{e, g, g^2\} \cong \mathbb{Z}_3, [\Lambda/\Gamma] = \{0,1,2\}, \xi(e) = 0, \\ \xi(g) &= 1 \ \ e \ \ \xi(g^2) = 2, \end{aligned}$$

temos que

$$\Lambda_{\mathcal{C}} = \bigcup_{\mathbf{c} \in \mathcal{C}} \varphi(\mathbf{c}),$$

onde

$$\begin{aligned}\varphi(\mathbf{c}) &= \varphi(\mathbf{c}_1)\times\varphi(\mathbf{c}_2)\times\cdots\times\varphi(\mathbf{c}_n)\\ &= \Gamma^n+\xi(\mathbf{c})\\ &= \Gamma^n+(\xi(\mathbf{c}_1),\xi(\mathbf{c}_2),\ldots,\xi(\mathbf{c}_n))\end{aligned}$$

e $\mathcal{C}$ *um* $(n,k,d)_3$ *código sobre* G*, com os seguintes parâmetros:*

$$\begin{aligned}d^2_{\min}(\Lambda_{\mathcal{C}}) &= \min\{3,d_H(\mathcal{C})\},\\ V(\Lambda_{\mathcal{C}}) &= 2^{-n}\cdot 3^{\frac{3n-2k}{2}},\\ \gamma(\Lambda_{\mathcal{C}}) &= 2\cdot 3^{\frac{2k-3n}{2n}}\cdot d^2_{\min}(\Lambda_{\mathcal{C}}).\end{aligned}$$

Para o código $\mathcal{C}=[4,2,3]_3$*, obtemos que*

$$d^2_{\min}(\Lambda_{\mathcal{C}})=3, V(\Lambda_{\mathcal{C}})=2^{-4}\cdot 3^4 \ \ e\ \ \gamma(\Lambda_{\mathcal{C}})=2.$$

Note que $\Lambda_{\mathcal{C}}$ *é similar ao reticulado* E_8 *em* $\mathbb{R}^8$*, (cf. [2]).*

Exemplo 3.8 *Sejam* $\Lambda = A_2$ *e* Γ *o sub-reticulado de* Λ *obtido com a matriz particionadora*

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

Então Λ/Γ *é uma cadeia de partições, com* 1*-nível e* 4*-maneiras. Neste caso, tomando*

$$\begin{aligned}G &= \{e,g,g^2,g^3\},[\Lambda/\Gamma]=\{0,1,2,3\},\xi(e)=0,\\ \xi(g) &= 1,\xi(g^2)=2\ \ e\ \ \xi(g^3)=3,\end{aligned}$$

temos que

$$\Lambda_{\mathcal{C}}=\bigcup_{\mathbf{c}\in\mathcal{C}}\varphi(\mathbf{c}),$$

onde

$$\begin{aligned}\varphi(\mathbf{c}) &= \varphi(\mathbf{c}_1)\times\varphi(\mathbf{c}_2)\times\cdots\times\varphi(\mathbf{c}_n)\\ &= \Gamma^n+\xi(\mathbf{c})\\ &= \Gamma^n+(\xi(\mathbf{c}_1),\xi(\mathbf{c}_2),\ldots,\xi(\mathbf{c}_n))\end{aligned}$$

e $\mathcal{C}$ *um* $(n,k,d)_4$ *código sobre* G*, com os seguintes parâmetros:*

$$\begin{aligned}d^2_{\min}(\Lambda_{\mathcal{C}}) &= \min\{4,d_H(\mathcal{C})\},\\ V(\Lambda_{\mathcal{C}}) &= 2^{n-2k}\cdot 3^{\frac{n}{2}}\\ \gamma(\Lambda_{\mathcal{C}}) &= 4^{\frac{2k-n}{n}}\cdot 3^{-1}\cdot d^2_{\min}(\Lambda_{\mathcal{C}}).\end{aligned}$$

Para o código $\mathcal{C}=[6,3,4]_4$*, obtemos que*

$$d^2_{\min}(\Lambda_{\mathcal{C}})=4, V(\Lambda_{\mathcal{C}})=3^3 \text{ e } \gamma(\Lambda_{\mathcal{C}})=\frac{4}{3}.$$

Note que $\Lambda_{\mathcal{C}}$ *é similar ao reticulado* K_{12} *em* $\mathbb{R}^{12}$*, (cf. [2]).*

3.3 Construções Multinível

Nesta seção, veremos que a construção generalizada A pode ser mais geral, utilizando partições com mais de um nível.

Seja

$$\Lambda_m\subseteq\Lambda_{m-1}\subseteq\cdots\subseteq\Lambda_0$$

uma cadeia de reticulados em $\mathbb{R}^l$ com quocientes

$$\Lambda_{i-1}/\Lambda_i\cong G_i,$$

para $i=1,2,\ldots,m$.

Sejam as funções

$$\begin{aligned}\varphi_i &: G_i \to \Lambda_{i-1}/\Lambda_i,\\ \xi_i &: G_i \to [\Lambda_{i-1}/\Lambda_i],\\ \pi_i &: \Lambda_{i-1} \to G_i.\end{aligned}$$

Então as correspondentes funções produto são respectivamente

$$\begin{aligned}\varphi &: G_1 \times \cdots \times G_m \to \Lambda_0/\Lambda_m,\\ \xi &: G_1 \times \cdots \times G_m \to [\Lambda_0/\Lambda_m],\\ \pi &: \Lambda_0 \to G_1 \times \cdots \times G_m,\end{aligned}$$

e a função φ corresponde a uma cadeia de decomposição em classes laterais dada por

$$\begin{aligned}\varphi(g_1,\ldots,g_m) &= \Lambda_m + \xi(g_1,\ldots,g_m)\\ &= \Lambda_m + \xi_1(g_1) + \cdots + \xi_m(g_m).\end{aligned}$$

A função φ induz uma correspondência biunívoca entre as classes laterais de Λ_m em Λ_0 e o produto cartesiano $G_1 \times \cdots \times G_m$, mas não é necessariamente um isomorfismo entre Λ_0/Λ_m e $G_1 \times \cdots \times G_m$.

Sejam $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_m$ uma seqüência de códigos de grupos de comprimento n sobre os grupos quociente G_i e o empacotamento em $\mathbb{R}^{nl}$

$$\begin{aligned}\Lambda &= \bigcup_{\mathbf{c}_i \in \mathcal{C}_i} \varphi(\mathbf{c}_1,\ldots,\mathbf{c}_m)\\ &= \bigcup_{\mathbf{c}_i \in \mathcal{C}_i} [(\Lambda_m)^n + \xi_1(\mathbf{c}_1) + \cdots + \xi_m(\mathbf{c}_m)],\end{aligned}$$

onde

$$\xi_i(\mathbf{c}_i) = (\xi_i(c_{1i}), \xi_i(c_{2i}), \ldots, \xi_i(c_{ni}))$$

para uma seqüência

$$\mathbf{c}_i = (c_{1i}, c_{2i}, \ldots, c_{ni}) \in \mathcal{C}_i, i = 1, \ldots, m.$$

Note que Λ é um conjunto discreto de pontos em $\mathbb{R}^{nl}$, mas não necessariamente um

reticulado. Como toda região fundamental de $(\Lambda_m)^n$ de volume $V(\Lambda_m)^n$ contém $\prod_{i=1}^m |\mathcal{C}_i|$ classes laterais de $(\Lambda_m)^n$, então

$$V(\Lambda) = \frac{V(\Lambda_m)^n}{\prod_{i=1}^m |\mathcal{C}_i|}.$$

Além disso,

$$d^2_{\min}(\Lambda) \geq \min\left\{d^2_{\min}(\Lambda_m), d_H(\mathcal{C}_m)\, d^2_{\min}(\Lambda_{m-1}), \ldots, d_H(\mathcal{C}_1)\, d^2_{\min}(\Lambda_0)\right\}.$$

De fato, sejam $\mathbf{x}, \mathbf{x}' \in \Lambda$ com seqüências de rótulos $\pi(\mathbf{x}) = (c_1, \ldots, c_m)$ e $\pi(\mathbf{x}') = (c'_1, \ldots, c'_m)$, respectivamente. Se $\pi(\mathbf{x}) = \pi(\mathbf{x}')$, então $\mathbf{x}$ e $\mathbf{x}'$ estão na mesma classe de $(\Lambda_m)^n$. Assim,

$$\|\mathbf{x} - \mathbf{x}'\|^2 \geq d^2_{\min}(\Lambda_m).$$

Se $\pi(\mathbf{x}) \neq \pi(\mathbf{x}')$, então existe um primeiro índice, digamos i_0, tal que $c_{i_0} \neq c'_{i_0}$. Assim, $\mathbf{x}$ e $\mathbf{x}'$ estão na mesma classe de $(\Lambda_{i_0-1})^n$ em $(\Lambda_0)^n$ mas não na mesma classe de $(\Lambda_{i_0})^n$. Como c_{i_0} difere de c'_{i_0} em pelo menos $d_H(\mathcal{C}_{i_0})$ posições temos que $\mathbf{x}$ difere de $\mathbf{x}'$ por pelo menos $d^2_{\min}(\Lambda_{i_0-1})$ em pelo menos $d_H(\mathcal{C}_{i_0})$ coordenadas. Logo,

$$\|\mathbf{x} - \mathbf{x}'\|^2 \geq d_H(\mathcal{C}_{i_0})\, d^2_{\min}(\Lambda_{i_0-1}).$$

Quando os códigos $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_m$ satisfazem a condição

$$\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_m,$$

temos a igualdade.

Exemplo 3.9 *Sejam $\Lambda_0 = \mathbb{Z}^2$, $\Lambda_1 = D_2$ e $\Lambda_2 = 2\mathbb{Z}^2$. Então $\Lambda_0/\Lambda_1/\Lambda_2$ é uma cadeia de partições, com 2-níveis e 2-maneiras. Neste caso, tomando*

$$\begin{aligned} G_1 &= \{e_1, g_1\} \cong \mathbb{Z}_2, G_2 = \{e_2, g_2\} \cong \mathbb{Z}_2, \\ [\Lambda_0/\Lambda_1] &= \{0,1\}, [\Lambda_1/\Lambda_2] = \{0,1\}, \xi_1(e_1) = 0, \\ \xi_1(g_1) &= 1, \xi_2(e_2) = 0 \ \ e \ \ \xi_2(g_2) = 1, \end{aligned}$$

temos que

$$\begin{aligned}\Lambda &= \bigcup_{\mathbf{c}_i \in \mathcal{C}_i} \varphi\left(\mathbf{c}_1, \mathbf{c}_2\right) \\ &= \bigcup_{\mathbf{c}_i \in \mathcal{C}_i} [(\Lambda_m)^n + \xi_1(\mathbf{c}_1) + \xi_2\left(\mathbf{c}_2\right)],\end{aligned}$$

onde

$$\xi_i\left(\mathbf{c}_i\right) = \left(\xi_i\left(c_{1i}\right), \xi_i\left(c_{2i}\right), \ldots \xi_i\left(c_{ni}\right)\right)$$

para uma seqüência

$$\mathbf{c}_i = (c_{1i}, c_{2i}, \ldots, c_{ni}) \in \mathcal{C}_i$$

e $\mathcal{C}_i$ *um* $(n, k_i, d_i)_2$ *código sobre* G_i*, com os seguintes parâmetros:*

$$\begin{aligned}d^2_{\min}(\Lambda) &= \min\{4, 2d_H(\mathcal{C}_2), d_H(\mathcal{C}_1)\}, \\ V(\Lambda) &= 2^{2n-(k_1+k_2)}, \\ \gamma(\Lambda) &= 2^{\frac{(k_1+k_2)-2n}{n}} \cdot d^2_{\min}(\Lambda).\end{aligned}$$

Para os códigos $\mathcal{C}_1 = [8, 4, 4]_2$ *e* $\mathcal{C}_2 = [8, 7, 2]_2$*, obtemos que*

$$d^2_{\min}(\Lambda) = 4, V(\Lambda) = 2^5 \ \ e \ \ \gamma(\Lambda) = 2^{\frac{11}{8}}.$$

Note que Λ *é equivalente ao reticulado* H_{16} *em* $\mathbb{R}^{16}$*, (cf. [17]). Para os códigos* $\mathcal{C}_1 = [16, 11, 4]_2$ *e* $\mathcal{C}_2 = [16, 15, 2]_2$*, obtemos que*

$$d^2_{\min}(\Lambda) = 4, V(\Lambda) = 2^6 \ \ e \ \ \gamma(\Lambda) = 2^{\frac{13}{8}}.$$

Note que Λ *é equivalente ao reticulado* X_{32} *em* $\mathbb{R}^{32}$*, (cf. [17]).*

Exemplo 3.10 *Sejam* $\Lambda_0 = A_2$ *e* Λ_1*,* Λ_2 *obtidos de* Λ_0 *usando a matriz particionadora*

$$\mathbf{B} = \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}.$$

Então $\Lambda_0/\Lambda_1/\Lambda_2$ *é uma cadeia de partições, com* 2*-níveis e* 3*-maneiras. Neste caso,*

tomando

$$\begin{aligned} G_1 &= \{e_1, g_1, g_1^2\} \cong \mathbb{Z}_3, G_2 = \{e_2, g_2, g_2^2\} \cong \mathbb{Z}_3, \\ [\Lambda_0/\Lambda_1] &= \{0,1,2\}, [\Lambda_1/\Lambda_2] = \{0,1,2\}, \xi_1(e_1) = 0, \\ \xi_1(g_1) &= 1, \xi_1(g_1^2) = 2 \ \ e \\ \xi_2(e_2) &= 0, \xi_2(g_2) = 1, \xi_2(g_2^2) = 2, \end{aligned}$$

temos que

$$\begin{aligned} \Lambda &= \bigcup_{\mathbf{c}_i \in \mathcal{C}_i} \varphi\left(\mathbf{c}_1, \mathbf{c}_2\right) \\ &= \bigcup_{\mathbf{c}_i \in \mathcal{C}_i} [(\Lambda_m)^n + \xi_1(\mathbf{c}_1) + \xi_2\left(\mathbf{c}_2\right)], \end{aligned}$$

onde

$$\xi_i\left(\mathbf{c}_i\right) = \left(\xi_i\left(c_{1i}\right), \xi_i\left(c_{2i}\right), \ldots, \xi_i\left(c_{ni}\right)\right)$$

para uma seqüência

$$\mathbf{c}_i = (c_{1i}, c_{2i}, \ldots, c_{ni}) \in \mathcal{C}_i$$

e $\mathcal{C}_i$ *um* $(n, k_i, d_i)_3$ *código sobre* G_i*, com os seguintes parâmetros:*

$$\begin{aligned} d^2_{\min}(\Lambda) &= \min\{9, 3d_H(\mathcal{C}_1), d_H(\mathcal{C}_2)\}, \\ V(\Lambda) &= 2^{-n} \cdot 3^{\frac{5n-2(k_1+k_2)}{2}}, \\ \gamma(\Lambda) &= 2 \cdot 3^{\frac{2(k_1+k_2)-5n}{2n}} \cdot d^2_{\min}(\Lambda). \end{aligned}$$

Para os códigos $\mathcal{C}_1 = [4,4,1]_3$ *e* $\mathcal{C}_2 = [4,2,3]_3$*, obtemos que*

$$d^2_{\min}(\Lambda) = 3, V(\Lambda) = 2^{-4} \cdot 3^4 \ \ e \ \gamma(\Lambda) = 2.$$

Note que Λ *é similar ao reticulado* E_8 *em* $\mathbb{R}^8$*, (cf. [2]). Para os códigos* $\mathcal{C}_1 = [12,6,6]_3$ *e* $\mathcal{C}_2 = [12,11,2]_3$*, obtemos*

$$d^2_{\min}(\Lambda) = 6, V(\Lambda) = 2^{-12} \cdot 3^{13} \ \ e \ \gamma(\Lambda) = 12 \cdot 3^{-\frac{13}{12}} \approx 3.6501.$$

Para os códigos $\mathcal{C}_1 = [18, 10, 6]_3$ *e* $\mathcal{C}_2 = [18, 16, 2]_3$*, obtemos*

$$d^2_{\min}(\Lambda) = 6, V(\Lambda) = 2^{-18} \cdot 3^{19} \text{ e } \gamma(\Lambda) = 12 \cdot 3^{-\frac{19}{18}} \approx 3.7632.$$

Note que os reticulados acima são tão densos quanto os reticulados da Tabela V de ([8]).

Referências Bibliográficas

[1] Cassels, J. W. S., *An Introdution to the Geometry of Number*. Springer-Verlag, 1959.

[2] Conway, J. H. and Sloane, N. J. A., *Sphere Packing, Lattices and Groups.* Springer-Verlag, 1993.

[3] Fell, H., Newman, M. and Ordman, E. "Tables of Genera of Groups of Linear Fractional Transformations," *J. Res. Nat. Bur. Standards,* 67B, 61-68, 1963.

[4] Forney, Jr. G. D., "Coset Codes I: Introduction and Geometrical Classification," *IEEE Trans. Inform. Theory,* vol. 34, 1123-1151, 1988.

[5] Forney, Jr. G. D. and Vardy, A., "Generalized Minimum Distance Decoding of Euclidean-Space Codes and Lattices," Part I, *IEEE Trans. Inform. Theory,* vol. 42, 1992-2026, 1996.

[6] Garcia, A. e Lequain, Y., *Álgebra: Um Curso de Introdução*. IMPA, 1988.

[7] Herstein, I. N., *Abstract Algebra*. Macmillan, 1990.

[8] Kschischang, F. R. and Pasupathy, S., "Some Ternary and Quaternary Codes and Associated Sphere Packings," *IEEE Trans. Inform. Theory,* vol. 38, 227-246, 1992.

[9] Lima, E. L., *Curso de Análise*. IMPA, 1981.

[10] MacWilliams, F. J. and Sloane, N. J A., *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[11] Milies, F. C. P., *Anéis e Módulos*. IME-USP, 1972.

[12] Roman, S., *Advanced Linear Algebra*. Springer-Verlag, 1992.

[13] Rotman, J. J., *Galois Theory*. Springer-Verlag, 1998.

[14] Santos, J. P. O., *Introdução à Teoria dos Números*. IMPA, 2000.

[15] Schoeneberg, B., *Elliptic Modular Functions*. Springer-Verlag, 1974.

[16] Silva, A. A., *Uma Contribuição à Classe dos Códigos Geometricamente Uniformes.* Tese de Doutorado, FEEC-UNICAMP, 1996.

[17] Silva, M. A. O. C., *Reticulados e suas Partições Aplicados à Codificação para Canais AWGN Limitados em Banda.* Tese de Doutorado, FEE-UNICAMP, 1991.

[18] Spindler, K., *Abstract Algebra with Applications*. Dekker, 1994.