UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

ELEONESIO STREY

Construções de reticulados a partir de códigos q-ários

Campinas

2017

Eleonesio Strey

Construções de reticulados a partir de códigos q-ários

Tese 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 Doutor em Matemática Aplicada.

Orientadora: Sueli Irene Rodrigues Costa

Este exemplar corresponde à versão final da Tese defendida pelo aluno Eleonesio Strey e orientada pela Profa. Dra. Sueli Irene Rodrigues Costa.

Campinas

2017

Agência(s) de fomento e nº(s) de processo(s): Não se aplica.

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

St83c

Strey, Eleonesio, 1982-
Construções de reticulados a partir de códigos q-ários / Eleonesio Strey. – Campinas, SP : [s.n.], 2017.

Orientador: Sueli Irene Rodrigues Costa.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos reticulados. 2. Códigos corretores de erros (Teoria da informação). 3. Teoria da informação em matemática. I. Costa, Sueli Irene Rodrigues,1949-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Constructions of lattices from q-ary codes
Palavras-chave em inglês:
Lattice theory
Correcting codes (Information theory)
Information theory in mathematics
Área de concentração: Matemática Aplicada
Titulação: Doutor em Matemática Aplicada
Banca examinadora:
Sueli Irene Rodrigues Costa [Orientador]
João Eloir Strapasson
Danilo Silva
Emerson Luiz do Monte Carmelo
Grasiele Cristiane Jorge
Data de defesa: 26-04-2017
Programa de Pós-Graduação: Matemática Aplicada

Tese de Doutorado defendida em 26 de abril de 2017 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). SUELI IRENE RODRIGUES COSTA

Prof(a). Dr(a). JOÃO ELOIR STRAPASSON

Prof(a). Dr(a). DANILO SILVA

Prof(a). Dr(a). EMERSON LUIZ DO MONTE CARMELO

Prof(a). Dr(a). GRASIELE CRISTIANE JORGE

A Ata da defesa com as respectivas assinaturas dos membros encontra-se no processo de vida acadêmica do aluno.

Agradecimentos

- A Deus, por ter me dado força em todos os momentos.
- Ao Programa de Pós-Graduação em Matemática Aplicada da Unicamp, pela oportunidade de realização do Doutorado.
- À minha orientadora, Dra. Sueli Irene Rodrigues Costa, pela orientação e ajuda nesta empreitada.
- Aos professores do IMECC-Unicamp pela minha formação durante o Doutorado.
- Em especial, agradeço à minha esposa Giselle por todo apoio, pelo carinho e pela compreensão durante a realização deste trabalho.
- Aos amigos e colegas, pela ajuda atribuída sempre que necessário e pelos momentos de descontração.
- A todos amigos e colegas do Laboratório de Matemática Discreta e Códigos do IMECC-Unicamp.
- Aos meus colegas do Departamento de Matemática Pura e Aplicada da Universidade Federal do Espírito Santo, que apoiaram o meu afastamento para qualificação e, em particular, a realização deste trabalho.
- Aos professores, Dr. João Eloir Strapasson, Dr. Danilo Silva, Dr. Emerson Luiz do Monte Carmelo e Dra. Grasiele Jorge por aceitarem participar da minha banca de defesa e por todas as sugestões e observações, que contribuíram muito para melhorar esse trabalho.
- Enfim, agradeço a todos que de alguma forma contribuíram direta ou indiretamente para a realização deste trabalho.

Resumo

Reticulados vêm sendo utilizados na abordagem de vários problemas em códigos corretores de erros e criptografia. Este trabalho foca em construções de reticulados a partir de códigos lineares q-ários. Construções D, D$'$ e $\overline{\mathrm{D}}$ e vários resultados são estendidos de códigos lineares binários para códigos lineares q-ários, $q \in \mathbb{N}$. Definimos a adição zero-um em $\mathbb{Z}_q^n$ e mostramos que a Construção $\overline{\mathrm{D}}$ produz um reticulado se, e somente se, a cadeia de códigos utilizada é fechada sob esta adição. Fórmulas fechadas ou limitantes para a distância da soma mínima de reticulados obtidos via Construções D, D$'$ e $\overline{\mathrm{D}}$ são fornecidos. Introduzimos a Construção A$'$ a partir de códigos lineares sobre o anel quociente $\mathbb{Z}_q[X]/(X^a)$ e mostramos que a mesma produz um reticulado se, e somente se, o código utilizado é fechado sob a adição zero-um deslocada. Conexões entre as construções supracitadas também são fornecidas.

Palavras-chave: Reticulados. Códigos q-ários. Construções D, D$'$, $\overline{\mathrm{D}}$ e A$'$.

Abstract

Lattices have been used in the approach of several problems in error correcting codes and cryptography. This work focuses on lattice constructions from q-ary linear codes. Constructions D, D$'$ and $\overline{\text{D}}$ and several results are extended from binary linear codes to q-ary linear codes, $q \in \mathbb{N}$. We define the zero-one addition in $\mathbb{Z}_q^n$ and show that the extended Construction $\overline{\text{D}}$ produces a lattice if and only if the nested codes are closed under this addition. Closed formulas or bounds for the minimum sum distance of lattices obtained via Constructions D, D$'$ and $\overline{\text{D}}$ are derived. We introduce the Construction A$'$ from linear codes over the quotient ring $\mathbb{Z}_q[X]/(X^a)$ and show it produces a lattice if and only if the used code is closed under shifted zero-one addition. Connections between the aforementioned constructions are also provided.

Keywords: Lattices. q-ary codes. Constructions D, D$'$, $\overline{\text{D}}$ and A$'$.

Sumário

Introdução

Um reticulado Λ é um subgrupo aditivo e discreto de $\mathbb{R}^n$. Equivalentemente, $\Lambda \subseteq \mathbb{R}^n$ é um reticulado se, e somente se, existem vetores linearmente independentes $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbb{R}^n$ tais que Λ consiste de todas as combinações lineares inteiras de $\boldsymbol{v}_i$, $i = 1, \ldots, m$, isto é,

$$\Lambda = \{\alpha_1 \boldsymbol{v}_1 + \cdots + \alpha_m \boldsymbol{v}_m;\ \alpha_1, \ldots, \alpha_m \in \mathbb{Z}\}.$$

Reticulados têm sido relacionados com códigos lineares sobre anéis finitos e usados para correção de erros em diferentes contextos [53] e também na proposição de esquemas criptográficos [32, 36]. A relação entre códigos e reticulados mais conhecida é a chamada "Construção A", que associa a cada código linear $C \subseteq \mathbb{Z}_q^n$ (onde $\mathbb{Z}_q$ é o anel dos inteiros módulo q) a imagem inversa de C pela aplicação módulo q, a qual sempre é um reticulado [9,24,28]. Neste trabalho, estudamos as Construções D, D$'$, $\overline{\text{D}}$ e A$'$. As Construções D e D$'$ foram propostas por Barnes e Sloane em [2] para códigos binários. Estas construções fornecem reticulados a partir de cadeias de códigos binários encaixados. Reticulados com boas propriedades, tais como reticulados LDPC [37] e reticulados turbo [38], podem ser descritos usando as Construções D' e D, respectivamente. Já a Construção $\overline{\text{D}}$ é uma reformulação da fómula código de Forney introduzida em [15,16]. A partir de uma cadeia de códigos lineares $\mathbb{Z}_p^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ (p primo), o conjunto gerado pela Construção $\overline{\text{D}}$ é dado por

$$\Gamma_{\overline{D}} = C_a + pC_{a-1} + p^2 C_{a-2} + \cdots + p^{a-1} C_1 + p^a \mathbb{Z}^n.$$

Esta construção tem atraído muita atenção desde sua introdução [19, 20, 22, 25, 26, 51]. A Construção $\overline{\text{D}}$ nem sempre produz um reticulado. Quando $p = 2$, a Construção $\overline{\text{D}}$ produz um reticulado se, e somente se, a cadeia de códigos utilizada é fechada sob o produto de Schur [25]. Finalmente, a Construção A$'$ definida em [19, 20] produz reticulados a partir de códigos lineares sobre o anel quociente $\mathbb{Z}_2[X]/(X^a)$. Em [20] é demonstrado que esta construção é equivalente à construção multinível de reticulados Barnes-Wall a partir de códigos de Reed-Muller.

Organização do trabalho

O Capítulo 1 é dedicado à apresentação dos conceitos básicos da teoria de reticulados. Nele, definimos reticulado, base, matriz geradora, determinante e volume de um reticulado, região de Voronoi, densidade de empacotamento, número de vizinhos, reticulado dual, etc. Consideramos métricas em reticulados provindas de normas e na Seção 1.4 mostramos que a região de Voronoi de um reticulado Λ na métrica da soma e na métrica do máximo nem sempre são regiões fundamentais de Λ.

O Capítulo 2 destina-se ao estudo de códigos lineares sobre $\mathbb{Z}_q$, $q \in \mathbb{N}$. Neste capítulo são apresentados alguns conceitos básicos tais como base, matriz geradora, distância mínima, código dual e a cota de Singleton de um código linear.

No Capítulo 3, são apresentadas nossas principais contribuições que incluem os resultados de [41–44]. Na Seção 3.1, estudamos a Construção A para códigos lineares q-ários ($q \in \mathbb{N}$) e mostramos que o reticulado tridimensional de maior densidade na métrica da soma pode ser obtido via Construção A. Na Seção 3.2.1, estendemos a Construção D para códigos lineares q-ários ($q \in \mathbb{N}$) e mostramos que a mesma sempre produz um reticulado. Mostramos que um reticulado obtido via Construção D a partir de uma cadeia composta por k códigos lineares sobre $\mathbb{Z}_q$, a menos de um fator de escala, sempre pode ser obtido via Construção A a partir de um código linear sobre $\mathbb{Z}_{q^k}$. Além destes, vários resultados apresentados em [2,9] para reticulados obtidos via Construção D a partir de códigos lineares binários são estendidos para reticulados obtidos via Construção D a partir de códigos lineares q-ários. As Construções D$'$ e $\overline{\text{D}}$ para códigos q-ários ($q \in \mathbb{N}$) são apresentadas nas Seções 3.2.2 e 3.2.3, respectivamente. Mostramos que a Construção D$'$ sempre produz um reticulado enquanto que a Construção $\overline{\text{D}}$ nem sempre fornece um reticulado. Na Seção 3.2.4 são apresentadas algumas conexões entre as Construções D, D$'$ e $\overline{\text{D}}$. Além disso, definimos a adição zero-um em $\mathbb{Z}_q^n$, mostramos que para $q = 2$ esta operação coincide com o produto de Schur e que Construção $\overline{\text{D}}$ produz um reticulado se, e somente se, a cadeia de códigos utilizada é fechada sob a adição zero-um. Resultados sobre a distância mínima na métrica da soma em reticulados obtidos via Construções D, D$'$ e $\overline{\text{D}}$ são apresentados na Seção 3.2.5. Na Seção 3.3, propomos uma generalização da Construção A$'$ e mostramos que esta produz um reticulado se, e somente se, o código correspondente sobre $\mathbb{Z}_q[X]/(X^a)$ é fechado sob a adição zero-um deslocada. Uma conexão entre as Construções A e A' também é fornecida. Observações finais e perspectivas futuras estão incluídas no último capítulo.

Capítulo 1

Reticulados

Neste capítulo, apresentamos os conceitos iniciais e alguns resultados preliminares sobre reticulados. Para tornar o texto o mais autossuficiente possível também fornecemos demonstrações de vários resultados apresentados. O objetivo deste capítulo é estabelecer a base teórica e notações para o desenvolvimento do restante do trabalho. As principais referências utilizadas neste capítulo foram [5], [9], [23], [47] e [52].

1.1 Conceitos e resultados iniciais

No decorrer deste texto, o espaço vetorial normado $(\mathbb{R}^n, \|\cdot\|)$ será denotado simplesmente por $\mathbb{R}^n$. Neste trabalho só consideramos métricas em $\mathbb{R}^n$ provindas de normas. Salvo menção em contrário, $\|\cdot\|$ será assumida como uma norma arbitrária no $\mathbb{R}^n$, sendo d a métrica induzida por esta noma, isto é, $d(\boldsymbol{x}, \boldsymbol{y}) = \|\boldsymbol{x} - \boldsymbol{y}\|$. Entre as normas mais conhecidas no $\mathbb{R}^n$ temos as normas ℓ_p, $1 \leq p \leq \infty$, descritas abaixo.

Para cada $1 \leq p < \infty$, a **norma $\boldsymbol{\ell_p}$** de um vetor $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$ é definida como

$$\|\boldsymbol{x}\|_p = \left(\sum_{i=1}^{n} |x_i|^p \right)^{1/p}$$

e a métrica induzida por esta norma é dada por

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

em que $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{R}^n$. A métrica induzida pela norma ℓ_1 também é conhecida como **métrica da soma**, **métrica de Manhattan** ou **métrica do táxi**. A métrica induzida pela norma ℓ_2 é a **métrica euclidiana**.

A **norma $\boldsymbol{\ell_\infty}$** (também conhecida como **norma do máximo**) de um vetor $\boldsymbol{x} =$

$(x_1, \ldots, x_n) \in \mathbb{R}^n$ é definida como

$$\|\boldsymbol{x}\|_\infty = \max\{|x_1|, \ldots, |x_n|\}$$

e a métrica induzida por esta norma é dada por

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

em que $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{R}^n$.

Dados $\boldsymbol{x} \in \mathbb{R}^n$ e $r > 0$, a **bola aberta** e a **bola fechada** com centro em $\boldsymbol{x}$ e raio $r > 0$ são, respectivamente, definidas como

$$B_d(\boldsymbol{x}, r) = B(\boldsymbol{x}, r) = \{\boldsymbol{y} \in \mathbb{R}^n;\ \|\boldsymbol{x} - \boldsymbol{y}\| < r\}$$

e

$$B_d[\boldsymbol{x}, r] = B[\boldsymbol{x}, r] = \{\boldsymbol{y} \in \mathbb{R}^n;\ \|\boldsymbol{x} - \boldsymbol{y}\| \leq r\}.$$

Todas as normas no $\mathbb{R}^n$ são equivalentes [30], isto é, dadas duas normas $\|\cdot\|_a$ e $\|\cdot\|_b$, sempre existem constantes positivas c_1 e c_2 tais que para qualquer $\boldsymbol{x} \in \mathbb{R}^n$,

$$c_1\|\boldsymbol{x}\|_a \leq \|\boldsymbol{x}\|_b \leq c_2\|\boldsymbol{x}\|_a.$$

Isto garante que todas as normas no $\mathbb{R}^n$ induzem a mesma topologia, ou seja, conjuntos abertos numa norma $\|\cdot\|_a$ também são abertos numa norma $\|\cdot\|_b$ e vice-versa.

Definição 1.1.1. *Um conjunto $D \subseteq \mathbb{R}^n$ é dito **discreto** quando não possui pontos de acumulação. Isto significa que para cada $\boldsymbol{x} \in D$, existe $r > 0$ tal que $B(\boldsymbol{x}, r) \cap D = \{\boldsymbol{x}\}$.*

Exemplo 1.1.1. *Os conjuntos $\mathbb{N}$, $\mathbb{Z}$ e $\{1/n;\ n \in \mathbb{N}^*\}$ são discretos em $\mathbb{R}$.*

Observação 1.1.1. *Todo subconjunto de um conjunto discreto é também discreto.*

Observação 1.1.2. *A Definição 1.1.1 não depende da norma em $\mathbb{R}^n$, ou seja, conjuntos discretos numa norma $\|\cdot\|_a$ também são discretos numa norma $\|\cdot\|_b$ e vice-versa. Isto ocorre pois todas as normas no $\mathbb{R}^n$ induzem a mesma topologia, conforme mencionado anteriormente.*

Definição 1.1.2. *Chamamos de **reticulado** qualquer subgrupo aditivo e discreto de $\mathbb{R}^n$.*

Exemplo 1.1.2. *$\mathbb{Z}^n$ é um reticulado.*

Teorema 1.1.1. *Se Λ é um reticulado em $\mathbb{R}^n$, então existe $r > 0$ tal que $B(\boldsymbol{x}, r) \cap \Lambda = \{\boldsymbol{x}\}$ para todo $\boldsymbol{x} \in \Lambda$.*

Demonstração. Seja $\Lambda \subseteq \mathbb{R}^n$ 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 $B(\mathbf{0}, r) \cap \Lambda = \{\mathbf{0}\}$. Logo para cada $\boldsymbol{x} \in \Lambda$, tem-se

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

e portanto $B(\boldsymbol{x}, r) \cap \Lambda = \{\boldsymbol{x}\}$ para todo $\boldsymbol{x} \in \Lambda$. □

Corolário 1.1.1. *Todo reticulado Λ em $\mathbb{R}^n$ é um conjunto fechado.*

Demonstração. Pelo Teorema 1.1.1, existe $r > 0$ tal que $B(\boldsymbol{x}, r) \cap \Lambda = \{\boldsymbol{x}\}$ para todo $\boldsymbol{x} \in \Lambda$. Seja $(\boldsymbol{z}_n) \subseteq \Lambda$ uma sequência convergente em $\mathbb{R}^n$, digamos $\boldsymbol{z}_n \to \boldsymbol{z}$, $\boldsymbol{z} \in \mathbb{R}^n$. Logo existe $n_0 \in \mathbb{N}$ tal que

$$\|\boldsymbol{z}_n - \boldsymbol{z}_m\| = \|\boldsymbol{z}_n - \boldsymbol{z} + \boldsymbol{z} - \boldsymbol{z}_m\| \leq \|\boldsymbol{z}_n - \boldsymbol{z}\| + \|\boldsymbol{z}_m - \boldsymbol{z}\| < \frac{r}{2} + \frac{r}{2} = r$$

sempre que $n, m \geq n_0$. Como $B(\boldsymbol{z}_n, r) \cap \Lambda = \{\boldsymbol{z}_n\}$, segue que $\boldsymbol{z}_n = \boldsymbol{z}_{n_0}$, para todo $n \geq n_0$, isto é, exceto por um número finito de termos, a sequência $(\boldsymbol{z}_n)$ é constante. Como $(\boldsymbol{z}_n) \subseteq \Lambda$, segue que $\boldsymbol{z} \in \Lambda$. Isto mostra que $\Lambda \subseteq \mathbb{R}^n$ é fechado. □

Corolário 1.1.2. *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado. Toda bola centrada em zero possui finitos elementos de Λ, isto é, o conjunto $B(\mathbf{0}, R) \cap \Lambda$ é finito, para todo $R > 0$.*

Demonstração. Pelo Teorema 1.1.1, existe $r > 0$ tal que $B(\boldsymbol{x}, r) \cap \Lambda = \{\boldsymbol{x}\}$ para todo $\boldsymbol{x} \in \Lambda$. As bolas $B(\boldsymbol{x}, r)$, com $\boldsymbol{x} \in B[\mathbf{0}, R] \cap \Lambda$, formam uma cobertura aberta de $B[\mathbf{0}, R] \cap \Lambda$. Como $B[\mathbf{0}, R] \cap \Lambda$ é compacto (todo subconjunto limitado e fechado de $\mathbb{R}^n$ é compacto), existem $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k \in B[\mathbf{0}, R] \cap \Lambda$ tais que

$$B[\mathbf{0}, R] \cap \Lambda \subseteq \bigcup_{i=1}^{k} B(\boldsymbol{x}_i, r),$$

donde segue que $B[\mathbf{0}, R] \cap \Lambda = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$, uma vez que $B(\boldsymbol{x}_i, r) \cap \Lambda = \{\boldsymbol{x}_i\}$ para todo $i = 1, \ldots, k$. Isto mostra que $B[\mathbf{0}, R] \cap \Lambda$ é finito. Logo $B(\mathbf{0}, R) \cap \Lambda$ também é finito. □

Corolário 1.1.3. *Todo reticulado $\Lambda \subseteq \mathbb{R}^n$, $\Lambda \neq \{\mathbf{0}\}$, possui um vetor não nulo de norma mínima.*

Demonstração. Segue imediatamente do Corolário 1.1.2. □

Teorema 1.1.2. *Um subconjunto $\Lambda \neq \{\mathbf{0}\}$ de $\mathbb{R}^n$ é um reticulado se, e somente se, existem $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m \in \mathbb{R}^n$ linearmente independentes tais que Λ consiste de todas as com-*

binações lineares inteiras destes vetores, isto é,

$$\Lambda = \big\{\alpha_1\boldsymbol{b}_1 + \cdots + \alpha_m\boldsymbol{b}_m;\ \alpha_1, \ldots, \alpha_m \in \mathbb{Z}\big\}.$$

Demonstração. ($\Rightarrow$) Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado não nulo e $S = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ um subconjunto maximal linearmente independente de Λ. A prova será feita por indução sobre m. Suponha inicialmente que $m = 1$ (isto é, $S = \{\boldsymbol{v}_1\}$) e seja $r > 0$ tal que $B(\boldsymbol{0}, r) \cap \Lambda \neq \{\boldsymbol{0}\}$. O Corolário 1.1.2 garante que o conjunto $B(\boldsymbol{0}, r) \cap \Lambda$ é finito. Logo podemos escolher $\boldsymbol{b}_1 \in B(\boldsymbol{0}, r) \cap \Lambda$, $\boldsymbol{b}_1 \neq \boldsymbol{0}$, tal que a norma de $\boldsymbol{b}_1$ seja mínima. Para cada $\boldsymbol{x}$ de Λ, existe $\alpha_1 \in \mathbb{R}$ tal que $\boldsymbol{x} = \alpha_1\boldsymbol{b}_1$. Se α_1 é inteiro então $\alpha_1\boldsymbol{b}_1 \in \Lambda$, pois $\boldsymbol{b}_1 \in \Lambda$ e Λ é um subgrupo aditivo de $\mathbb{R}^n$. Agora, se α_1 não é inteiro temos que $\alpha_1\boldsymbol{b}_1 \notin \Lambda$, pois se existisse um número real não inteiro α_1 tal que $\alpha_1\boldsymbol{b}_1 \in \Lambda$ teríamos

$$\alpha_1\boldsymbol{b}_1 - \lfloor\alpha_1\rfloor\,\boldsymbol{b}_1 = (\alpha_1 - \lfloor\alpha_1\rfloor)\boldsymbol{b}_1 \in \Lambda$$

e

$$\|(\alpha_1 - \lfloor\alpha_1\rfloor)\boldsymbol{b}_1\| = (\alpha_1 - \lfloor\alpha_1\rfloor)\|\boldsymbol{b}_1\| < \|\boldsymbol{b}_1\|$$

(o símbolo $\lfloor\alpha_1\rfloor$ denota o maior inteiro menor ou igual a α_1). Porém, isto contradiz a minimalidade de $\|\boldsymbol{b}_1\|$. Logo

$$\Lambda = \big\{\alpha_1\boldsymbol{b}_1;\ \alpha_1 \in \mathbb{Z}\big\}.$$

Agora, suponha que $m > 1$ e que o resultado vale para todo reticulado que contém um subconjunto maximal linearmente independente com $m-1$ vetores. Sejam V o subespaço de $\mathbb{R}^n$ gerado pelos vetores $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{m-1}$ e $\Lambda_0 = \Lambda \cap V$. Claramente Λ_0 é um reticulado. Logo, por hipótese de indução, existem $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{m-1} \in \mathbb{R}^n$ linearmente independentes tais que

$$\Lambda_0 = \big\{\alpha_1\boldsymbol{b}_1 + \cdots + \alpha_{m-1}\boldsymbol{b}_{m-1};\ \alpha_1, \ldots, \alpha_{m-1} \in \mathbb{Z}\big\}.$$

Seja X o conjunto formado por todos os elementos $\boldsymbol{x}$ de Λ da forma

$$\boldsymbol{x} = \alpha_1\boldsymbol{b}_1 + \cdots + \alpha_{m-1}\boldsymbol{b}_{m-1} + \alpha_m\boldsymbol{v}_m,$$

com $\alpha_i \in \mathbb{R}$, $0 \leq \alpha_m \leq 1$ e $0 \leq \alpha_i < 1$ para $i = 1, \ldots, m-1$. Do Corolário 1.1.2, temos que X é finito, já que é limitado. Por outro lado, $X \neq \emptyset$ pois $\boldsymbol{v}_m \in X$. Assim, podemos escolher $\boldsymbol{b}_m = \tilde{\alpha}_1\boldsymbol{b}_1 + \cdots + \tilde{\alpha}_{m-1}\boldsymbol{b}_{m-1} + \tilde{\alpha}_m\boldsymbol{v}_m \in X$ tal que o coeficiente $\tilde{\alpha}_m$ seja não nulo e mínimo. Obviamente $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{m-1}, \boldsymbol{b}_m\}$ é linearmente independente. Dado $\boldsymbol{v} \in \Lambda$, pela maximalidade de m, o conjunto $\{\boldsymbol{v}, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ é linearmente dependente, isto é, existem números reais β_i, $1 \leq i \leq m$, tais que

$$\boldsymbol{v} = \sum_{i=1}^{m} \beta_i\boldsymbol{b}_i = \sum_{i=1}^{m-1} (\beta_i + \beta_m\tilde{\alpha}_i)\boldsymbol{b}_i + \beta_m\tilde{\alpha}_m\boldsymbol{v}_m,$$

uma vez que $\boldsymbol{b}_m = \tilde{\alpha}_1\boldsymbol{b}_1 + \cdots + \tilde{\alpha}_{m-1}\boldsymbol{b}_{m-1} + \tilde{\alpha}_m\boldsymbol{v}_m$. Tomando $\gamma_m = \lfloor\beta_m\rfloor$ e $\gamma_i = \lfloor\beta_i + (\beta_m - \lfloor\beta_m\rfloor)\rfloor$, $1 \leq i \leq m$, temos o vetor $\boldsymbol{w} = \boldsymbol{v} - \sum_{i=1}^{m-1}\gamma_i\boldsymbol{b}_i - \gamma_m\boldsymbol{b}_m$ pertence a Λ e pode ser reescrito da seguinte forma $\boldsymbol{w} = \boldsymbol{v} - \sum_{i=1}^{m-1}(\gamma_i + \gamma_m\tilde{\alpha}_i)\boldsymbol{b}_i - \gamma_m\tilde{\alpha}_m\boldsymbol{v}_m$, isto é,

$$\boldsymbol{w} = \sum_{i=1}^{m-1}(\beta_i + \beta_m\tilde{\alpha}_i)\boldsymbol{b}_i + \beta_m\tilde{\alpha}_m\boldsymbol{v}_m - \sum_{i=1}^{m-1}(\gamma_i + \lfloor\beta_m\rfloor\tilde{\alpha}_i)\boldsymbol{b}_i - \lfloor\beta_m\rfloor\tilde{\alpha}_m\boldsymbol{v}_m.$$

Donde segue que $\boldsymbol{w} = \sum_{i=1}^{m-1}\mu_i\boldsymbol{b}_i + \mu_m\boldsymbol{v}_m$, onde $\mu_i = \beta_i + (\beta_m - \lfloor\beta_m\rfloor)\tilde{\alpha}_i - \lfloor\beta_i + (\beta_m - \lfloor\beta_m\rfloor)\tilde{\alpha}_i\rfloor$ e $\mu_m = (\beta_m - \lfloor\beta_m\rfloor)\tilde{\alpha}_m$. Observe que $0 \leq \mu_i \leq 1$ e $0 \leq \mu_m < \tilde{\alpha}_m < 1$. Isto mostra que $\boldsymbol{w}$ pertence a X. Como o coeficiente de $\boldsymbol{v}_m$ em $\boldsymbol{w}$ é menor do que $\tilde{\alpha}_m$ e não é negativo, temos que ele é zero (pela escolha de $\boldsymbol{b}_m$), isto é, $\beta_m \in \mathbb{Z}$. Logo $\boldsymbol{w} \in \Lambda \cap V = \Lambda_0$ e consequentemente $\boldsymbol{v} \in \Lambda$, já que $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m \in \Lambda$, $\gamma_1, \ldots, \gamma_m, \beta_m \in \mathbb{Z}$, Λ é um reticulado e

$$\boldsymbol{v} = \boldsymbol{w} + \sum_{i=1}^{m-1}\gamma_i\boldsymbol{b}_i + \gamma_m\boldsymbol{b}_m$$

Isto mostra que

$$\Lambda = \big\{\alpha_1\boldsymbol{b}_1 + \cdots + \alpha_m\boldsymbol{b}_m;\ \alpha_1, \ldots, \alpha_m \in \mathbb{Z}\big\}.$$

($\Leftarrow$) Sejam $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m \in \mathbb{R}^n$ linearmente independentes tais que

$$\Lambda = \big\{\alpha_1\boldsymbol{b}_1 + \cdots + \alpha_m\boldsymbol{b}_m;\ \alpha_1, \ldots, \alpha_m \in \mathbb{Z}\big\}.$$

Considere a matriz B cujas linhas são os vetores $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$. Podemos reescrever Λ da seguinte forma

$$\Lambda = \{\boldsymbol{x}B;\ \boldsymbol{x} \in \mathbb{Z}^m\}.$$

Observe que Λ é um subgrupo aditivo de $\mathbb{R}^n$. De fato, $\Lambda \subseteq \mathbb{R}^n$, $\mathbf{0} \in \Lambda$ e dados $\boldsymbol{v}, \boldsymbol{w} \in \Lambda$, existem $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}^m$ tais que $\boldsymbol{v} = \boldsymbol{x}B$ e $\boldsymbol{w} = \boldsymbol{y}B$. Donde segue que $\boldsymbol{v} - \boldsymbol{w} = \boldsymbol{x}B - \boldsymbol{y}B = (\boldsymbol{x} - \boldsymbol{y})B \in \Lambda$, já que $(\boldsymbol{x} - \boldsymbol{y}) \in \mathbb{Z}^m$. Agora, vamos mostrar que Λ é um conjunto discreto. Com efeito, todo vetor $\boldsymbol{v} \in \Lambda$ pode ser escrito de forma única como

$$\boldsymbol{v} = \lambda_1\boldsymbol{b}_1 + \cdots + \lambda_m\boldsymbol{b}_m$$

com $\lambda_i \in \mathbb{Z}$. Como $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\} \subseteq \mathbb{R}^n$ é linearmente independente, existem $\boldsymbol{b}_{m+1}, \ldots, \boldsymbol{b}_n \in \mathbb{R}^n$ tais que $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m, \boldsymbol{b}_{m+1}, \ldots, \boldsymbol{b}_n\}$ é uma base de $\mathbb{R}^n$. Considere a transformação linear $T : \mathbb{R}^n \to \mathbb{R}^n$ dada por $T(\alpha_1\boldsymbol{b}_1 + \cdots + \alpha_n\boldsymbol{b}_n) = (\alpha_1, \ldots, \alpha_n)$. Temos que $T\big(B(\mathbf{0}, r)\big)$ é limitado, digamos

$$\|T(\boldsymbol{v})\| < k, \forall \boldsymbol{v} \in B(\mathbf{0}, r).$$

Logo $T(\boldsymbol{v}) \in B(\mathbf{0}, k) \cap \mathbb{Z}^n$ para todo $\boldsymbol{v} \in B(\mathbf{0}, r) \cap \Lambda$. Mas $B(\mathbf{0}, k) \cap \mathbb{Z}^n$ é finito (Corolário 1.1.2) e T é bijetora, logo $B(\mathbf{0}, r) \cap \Lambda$ é finito. Seja $r > 0$ tal que $\Lambda \cap B(\mathbf{0}, r) \neq \{\mathbf{0}\}$. O conjunto $\{\|\boldsymbol{x}\|;\ \boldsymbol{x} \in \Lambda \cap B(\mathbf{0}, r) \text{ e } \boldsymbol{x} \neq \mathbf{0}\} \subseteq \mathbb{R}$ é não vazio e finito, logo possui menor

elemento. Seja $\boldsymbol{x}_0 \in \Lambda$, $\boldsymbol{x}_0 \neq \mathbf{0}$, tal que

$$\|\boldsymbol{x}_0\| = \min\{\|\boldsymbol{x}\|;\ \boldsymbol{x} \in \Lambda \cap B(\mathbf{0}, r) \text{ e } \boldsymbol{x} \neq \mathbf{0}\}.$$

Para $0 < \epsilon \leq \|\boldsymbol{x}_0\|$ tem-se $B(\boldsymbol{x}, \epsilon) \cap \Lambda = \{\boldsymbol{x}\}$ para todo $\boldsymbol{x} \in \Lambda$. Caso contrário, existiria $\boldsymbol{y} \in \Lambda$ tal que $\boldsymbol{x} \neq \boldsymbol{y}$ e

$$\|\boldsymbol{x} - \boldsymbol{y}\| < \epsilon \leq \|\boldsymbol{x}_0\|,$$

contrariando a minimalidade de $\|\boldsymbol{x}_0\|$, já que $\mathbf{0} \neq \boldsymbol{x} - \boldsymbol{y} \in \Lambda$. Isto mostra que Λ é discreto. □

Observação 1.1.3. *Se $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m \in \mathbb{R}^n$ são linearmente dependentes, então o conjunto formado por todas as combinações lineares inteiras destes vetores nem sempre é um reticulado. Por exemplo, pode-se mostrar que $\{a + b\sqrt{2};\ a, b \in \mathbb{Z}\} \subset \mathbb{R}$ não é discreto (logo não é um reticulado) e $\{1, \sqrt{2}\} \subset \mathbb{R}$ é linearmente dependente.*

Definição 1.1.3. *Um conjunto $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\} \subseteq \mathbb{R}^n$ linearmente independente é dito uma **base** de um reticulado $\Lambda \subseteq \mathbb{R}^n$ quando $\Lambda = \{\alpha_1\boldsymbol{b}_1 + \cdots + \alpha_m\boldsymbol{b}_m;\ \alpha_1, \ldots, \alpha_m \in \mathbb{Z}\}$.*

Observação 1.1.4. *Todo reticulado possui uma base (Teorema 1.1.2). Um reticulado pode ser gerado por mais de uma base, conforme podemos conferir no próximo exemplo.*

Exemplo 1.1.3. *Na Figura 1.1 estão ilustrados um reticulado $\Lambda \subseteq \mathbb{R}^2$ e duas bases do mesmo, a saber $\alpha = \{(2,0), (-1,1)\}$ e $\beta = \{(3,1), (1,1)\}$.*

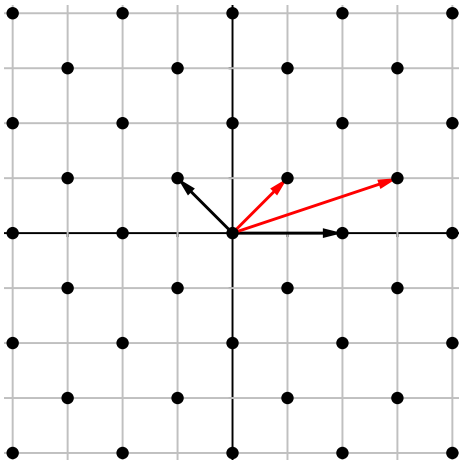


Figura 1.1: Reticulado Λ

Teorema 1.1.3. *Duas bases de um mesmo reticulado possuem a mesma quantidade de vetores.*

Demonstração. Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado. Suponha que $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ e $\{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k\}$ são bases de Λ. Para provar que $m = k$, basta mostrar que o espaço vetorial real gerado por $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ é igual ao espaço vetorial real gerado por $\{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k\}$, isto é,

$\text{span}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\} = \text{span}\{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k\}$. Com efeito, seja $\boldsymbol{x} \in \text{span}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$. Assim, existem números reais $\alpha_1, \ldots, \alpha_m$ tais que

$$\boldsymbol{x} = \sum_{i=1}^{m} \alpha_i \boldsymbol{b}_i. \tag{1.1}$$

Como cada $\boldsymbol{b}_i$ pertence ao reticulado Λ e $\{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k\}$ é uma base de Λ, segue que existem $\lambda_{ij} \in \mathbb{Z}$ tais que

$$\boldsymbol{b}_i = \sum_{j=1}^{k} \lambda_{ij} \boldsymbol{c}_j. \tag{1.2}$$

De (1.1) e (1.2), obtemos

$$\boldsymbol{x} = \sum_{i=1}^{m} \sum_{j=1}^{k} \alpha_i \lambda_{ij} \boldsymbol{c}_j.$$

Portanto $\boldsymbol{x} \in \text{span}\{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k\}$. Isto mostra que $\text{span}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\} \subseteq \text{span}\{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k\}$. De forma análoga podemos obter a outra inclusão $\text{span}\{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k\} \subseteq \text{span}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$. □

Definição 1.1.4. *O número de vetores de uma base qualquer de um reticulado Λ é chamado de* ***posto*** *ou* ***dimensão*** *de Λ. Dizemos que um reticulado $\Lambda \subseteq \mathbb{R}^n$ possui* ***posto completo*** *quando o posto de Λ é n.*

Definição 1.1.5. *Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ uma base de Λ tal que $\boldsymbol{b}_i = (b_{i1}, \ldots, b_{in})$, para $i = 1, \ldots, m$. Dizemos que a matriz*

$$B = \begin{pmatrix} b_{11} & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{m1} & b_{m2} & \ldots & b_{mn} \end{pmatrix}$$

é uma ***matriz geradora*** *de Λ. A matriz $G = BB^t$ é chamada de* ***matriz de Gram*** *de Λ associada à base $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$.*

Um reticulado $\Lambda \subseteq \mathbb{R}^n$ com matriz geradora $B \in \mathbb{R}^{m \times n}$ pode ser representado matricialmente da seguinte forma

$$\Lambda = \Lambda(B) = \{\boldsymbol{u}B;\ \boldsymbol{u} \in \mathbb{Z}^m\}.$$

Definição 1.1.6. *Uma matriz quadrada U com entradas inteiras é chamada de* ***matriz unimodular*** *se* $\det(U) = \pm 1$.

Lema 1.1.1. *A inversa de uma matriz unimodular também é uma matriz unimodular.*

Demonstração. Seja $A \in \mathbb{Z}^{n \times n}$ tal que $\det(A) = \pm 1$. O Teorema 3.5.5 de [4], garante que A possui inversa e $A^{-1} = [1/\det(A)](\text{Adj}(A))$, onde $\text{Adj}(A)$ denota a matriz adjunta de

A. Por outro lado, temos que $\mathrm{Adj}(A) \in \mathbb{Z}^{n\times n}$, uma vez que $A \in \mathbb{Z}^{n\times n}$. Logo todas as entradas da matriz A^{-1} também são inteiras, já que $\det(A) = \pm 1$. Para concluir a prova, basta mostrar que $\det(A^{-1}) = \pm 1$. Com efeito, temos que $AA^{-1} = I_n$ e consequentemente $\det(A)\det(A^{-1}) = 1$. Mas $\det(A) = \pm 1$, logo $\det(A^{-1}) = \pm 1$. □

Observação 1.1.5. *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 $Gl_n(\mathbb{Z})$.*

Teorema 1.1.4. *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 B_1 e B_2 matrizes geradoras de um reticulado Λ e sejam $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ as linhas da matriz B_2. Para cada $i \in \{1, \ldots, m\}$, existe $\boldsymbol{u}_i \in \mathbb{Z}^m$ tal que $\boldsymbol{b}_i = \boldsymbol{u}_i B_1$. Assim, existe uma matriz $U \in \mathbb{Z}^{m\times m}$ tal que $B_2 = UB_1$. Analogamente, podemos mostrar que existe uma matriz $V \in \mathbb{Z}^{m\times m}$ tal que $B_1 = VB_2$. Logo $B_1 = VUB_1$. Multiplicando ambos os lados desta igualdade à direita por $B_1^t(B_1B_1^t)^{-1}$ ($B_1B_1^t$ possui inversa pelo Lema 1.2.1), obtemos $VU = I_m$ e consequentemente $\det U \det V = 1$. Por outro lado, os números $\det U$ e $\det V$ são inteiros, pois $U, V \in \mathbb{Z}^{m\times m}$. Logo $\det U = \pm 1$. Portanto existe uma matriz quadrada U com entradas inteiras e $\det(U) = \pm 1$ tal que $B_2 = UB_1$. ($\Leftarrow$) Seja U uma matriz unimodular tal que $B_2 = UB_1$. Como $U \in \mathbb{Z}^{m\times m}$, segue que $\Lambda(B_2) \subseteq \Lambda(B_1)$. Por outro lado, da igualdade $B_2 = UB_1$ segue que $B_1 = U^{-1}B_2$, o que implica $\Lambda(B_1) \subseteq \Lambda(B_2)$, uma vez que U^{-1} também é uma matriz unimodular (Lema 1.1.1). Portanto B_1 e B_2 geram o mesmo reticulado. □

Teorema 1.1.5. *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 Λ. Pelo Teorema 1.1.4, existe uma matriz unimodular U tal que $B_2 = UB_1$. Logo $G_2 = B_2B_2^t = UB_1B_1^tU^t = UG_1U^t$. Portanto

$$\det(G_1) = \det(U)\det(G_2)\det(U^t) = \det(G_2),$$

uma vez que $\det(U) = \det(U^t) = \pm 1$. □

Definição 1.1.7. *Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e G uma matriz de Gram de Λ. O **determinante** ou **discriminante** de Λ é definido como $\det(\Lambda) = \det(G)$.*

1.2 O reticulado dual

Definição 1.2.1. *Seja $\Lambda = \Lambda(B)$ um reticulado em $\mathbb{R}^n$. O **reticulado dual** de Λ é definido como*

$$\Lambda^* = \left\{\boldsymbol{w} \in span(B);\ \langle \boldsymbol{v}, \boldsymbol{w}\rangle \in \mathbb{Z}, \forall \boldsymbol{v} \in \Lambda\right\},$$

onde span(B) *é o espaço vetorial real gerado pelas linhas de* B *e* $\langle\,,\rangle$ *é o produto interno usual em* $\mathbb{R}^n$.

O conjunto Λ^* é de fato um reticulado (ver Teorema 1.2.1 a seguir). Do ponto de vista geométrico, o reticulado dual pode ser visto como a interseção entre determinadas famílias de hiperplanos. De fato, seja $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ uma base de um reticulado Λ. Temos que

$$\Lambda^* = \big\{\boldsymbol{w} \in \text{span}(B);\ \langle \boldsymbol{b}_i, \boldsymbol{w}\rangle \in \mathbb{Z} \text{ para } i = 1, \ldots, m\big\}.$$

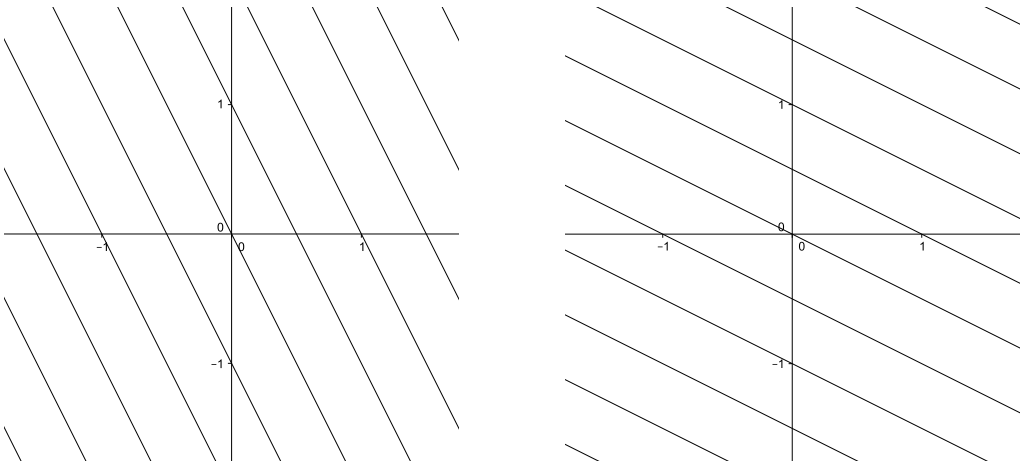
Dessa forma, podemos escrever $\Lambda^* = \bigcap_{i=1}^{m} H_i$, em que

$$H_i = \bigcup_{k\in\mathbb{Z}} \big\{\boldsymbol{w} \in \text{span}(B);\ \langle \boldsymbol{b}_i, \boldsymbol{w}\rangle = k\big\},$$

isto é, H_i é a união de todos os hiperplanos no span(B) que são perpendiculares ao vetor $\boldsymbol{b}_i$ e cuja distância euclidiana até a origem é $k/\|\boldsymbol{b}_i\|_2$, para algum $k \in \mathbb{N}$. Para cada $k \in \mathbb{N}$, $k \neq 0$, existem dois hiperplanos no span(B) que são perpendiculares ao vetor $\boldsymbol{b}_i$ e cuja distância euclidiana até a origem é $k/\|\boldsymbol{b}_i\|_2$, a saber

$$\{\boldsymbol{w} \in \text{span}(B);\ \langle \boldsymbol{b}_i, \boldsymbol{w}\rangle = -k\} \text{ e } \{\boldsymbol{w} \in \text{span}(B);\ \langle \boldsymbol{b}_i, \boldsymbol{w}\rangle = k\}.$$

Exemplo 1.2.1. *Seja* $\Lambda \subseteq \mathbb{R}^2$ *o reticulado gerado pela matriz* B*, cujas linhas são* $\boldsymbol{b}_1 = (2,1)$ *e* $\boldsymbol{b}_2 = (1,2)$*. Temos que span*$(B) = \mathbb{R}^2$*. Para cada* $i \in \{1,2\}$*, seja* H_i *a união de todos os hiperplanos (que neste caso são retas) no* $\mathbb{R}^2$ *que são perpendiculares ao vetor* $\boldsymbol{b}_i$ *e cuja distância euclidiana até a origem é* $k/\|\boldsymbol{b}_i\|_2$*, para algum* $k \in \mathbb{N}$*. Os conjuntos* H_1 *e* H_2 *estão representados nas Figuras 1.2(a) e 1.2(b), respectivamente. Na Figura 1.3(a)*

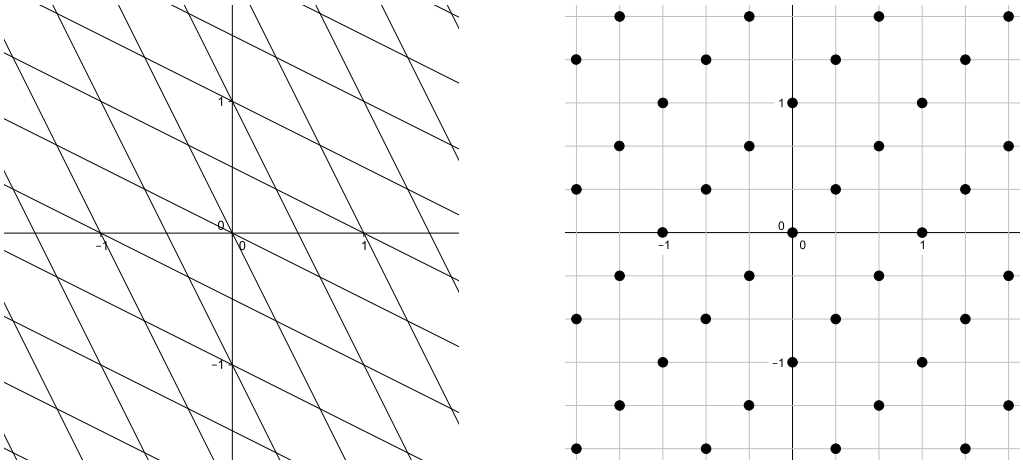


(a) H_1 (b) H_2

Figura 1.2: Famílias de hiperplanos associadas aos vetores $\boldsymbol{b}_1 = (2,1)$ e $\boldsymbol{b}_2 = (1,2)$

podemos observar as sobreposições entre as famílias de retas H_1 *e* H_2*. O reticulado dual de* Λ *pode ser visto como a interseção entre os conjuntos* H_1 *e* H_2 *e este está representado*

na Figura 1.3(b).



(a) H_1 e H_2 (b) $\Lambda^* = H_1 \cap H_2$

Figura 1.3: Reticulado dual

Lema 1.2.1. *Seja B uma matriz $m \times n$ de posto m. Temos que*

(i) BB^t possui inversa.

(ii) $span(B) = span\big((BB^t)^{-1}B\big)$.

Demonstração. (i) As linhas a matriz B são linearmente independentes, uma vez que B é uma matriz $m \times n$ de posto m. Assim,

$$\boldsymbol{x}(BB^t) = \mathbf{0} \;\Rightarrow\; \boldsymbol{x}(BB^t)\boldsymbol{x}^t = 0 \;\Rightarrow\; \|\boldsymbol{x}B\|_2^2 = 0 \;\Rightarrow\; \boldsymbol{x}B = \mathbf{0} \;\Rightarrow\; \boldsymbol{x} = \mathbf{0}.$$

Isto mostra que linhas da matriz BB^t também são linearmente independentes. Por outro lado, temos que BB^t é uma matriz quadrada. Logo BB^t possui inversa.
(ii) Seja $\boldsymbol{y} \in \text{span}(B)$, isto é, $\boldsymbol{y} = \boldsymbol{x}B$ para algum $\boldsymbol{x} \in \mathbb{R}^m$. Pelo item (i), a matriz BB^t possui inversa, logo podemos escrever $\boldsymbol{y} = \boldsymbol{z}(BB^t)^{-1}B$, em que $\boldsymbol{z} = \boldsymbol{x}(BB^t) \in \mathbb{R}^m$. Isto mostra que $\boldsymbol{y} \in \text{span}\big((BB^t)^{-1}B\big)$ e consequentemente $\text{span}(B) \subseteq \text{span}\big((BB^t)^{-1}B\big)$. Por outro lado, a inclusão $\text{span}\big((BB^t)^{-1}B\big) \subseteq \text{span}(B)$ é trivial. Portanto $\text{span}(B) = \text{span}\big((BB^t)^{-1}B\big)$. □

Teorema 1.2.1. *Se $B \in \mathbb{R}^{m\times n}$ é uma matriz geradora de Λ, então a matriz $(BB^t)^{-1}B$ (isto é, a pseudoinversa de B^t) é uma matriz geradora de Λ^*.*

Demonstração. Seja $B \in \mathbb{R}^{m\times n}$ uma matriz geradora de Λ. Para cada $\boldsymbol{v} \in \Lambda$, isto é, $\boldsymbol{v} = \boldsymbol{u}B$ com $\boldsymbol{u} \in \mathbb{Z}^m$ temos que

$$\big\langle \boldsymbol{v}, \boldsymbol{w}(BB^t)^{-1}B \big\rangle = \boldsymbol{w}(BB^t)^{-1}B\boldsymbol{v}^t = \boldsymbol{w}(BB^t)^{-1}B(\boldsymbol{u}B)^t = \boldsymbol{w}\boldsymbol{u}^t \in \mathbb{Z}, \forall \boldsymbol{w} \in \mathbb{Z}^m.$$

Logo $\{\boldsymbol{w}(BB^t)^{-1}B;\ \boldsymbol{w} \in \mathbb{Z}^m\} \subseteq \Lambda^*$. Agora, vamos mostrar a inclusão $\Lambda^* \subseteq \{\boldsymbol{w}(BB^t)^{-1}B;\ \boldsymbol{w} \in \mathbb{Z}^m\}$. Com efeito, seja $\boldsymbol{w} \in \Lambda^*(B)$. Temos que $\boldsymbol{w} \in \text{span}(B)$ e $\langle \boldsymbol{v}, \boldsymbol{w}\rangle \in \mathbb{Z}$ para todo $\boldsymbol{v} \in \Lambda$. Como $\text{span}(B) = \text{span}((BB^t)^{-1}B)$, existe $\boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{R}^n$ tal que $\boldsymbol{w} = \boldsymbol{u}(BB^t)^{-1}B$. Para concluir, basta mostrar que $\boldsymbol{u} \in \mathbb{Z}^n$. Com efeito, temos que $\langle \boldsymbol{v}, \boldsymbol{u}(BB^t)^{-1}B\rangle \in \mathbb{Z}$ para todo $\boldsymbol{v} \in \Lambda$. Em particular, $u_i = \boldsymbol{u}(BB^t)^{-1}B\boldsymbol{b}_i^t = \langle \boldsymbol{b}_i, \boldsymbol{u}(BB^t)^{-1}B\rangle \in \mathbb{Z}$, em que $\boldsymbol{b}_i$ é a i-ésima linha de B. □

Corolário 1.2.1. *Para qualquer reticulado Λ, tem-se $(\Lambda^*)^* = \Lambda$.*

Demonstração. Seja $B \in \mathbb{R}^{m\times n}$ uma matriz geradora de Λ. Pelo Teorema 1.2.1, $(BB^t)^{-1}B$ é uma matriz geradora de Λ^* e

$$\left[(BB^t)^{-1}B((BB^t)^{-1}B)^t\right]^{-1}(BB^t)^{-1}B = B$$

é uma matriz geradora de $(\Lambda^*)^*$. Portanto $(\Lambda^*)^* = \Lambda$. □

Corolário 1.2.2. *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado. Para cada $0 \neq k \in \mathbb{R}$, temos que o dual de $k\Lambda$ é $(1/k)\Lambda^*$.*

Demonstração. Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e $0 \neq k \in \mathbb{R}$. Se B é uma matriz geradora de Λ, kB é uma matriz geradora de $k\Lambda$. O Teorema 1.2.1 garante que $(BB^t)^{-1}B$ e

$$(kB(kB)^t)^{-1}kB = (1/k)(BB^t)^{-1}B$$

são matrizes geradoras de Λ^* e $(k\Lambda)^*$, respectivamente. Portanto $(k\Lambda)^* = (1/k)\Lambda^*$. □

Corolário 1.2.3. *Para qualquer reticulado Λ, tem-se* $\det(\Lambda^*) = 1/\det(\Lambda)$.

Demonstração. Seja $B \in \mathbb{R}^{m\times n}$ uma matriz geradora de Λ. O Teorema 1.2.1 afirma que $(BB^t)^{-1}B$ é uma matriz geradora de Λ^* e portanto

$$\det(\Lambda^*) = \det\left[(BB^t)^{-1}B\big((BB^t)^{-1}B\big)^t\right] = \det\left(BB^t\right)^{-1} = 1/\det(BB^t) = 1/\det(\Lambda).$$

□

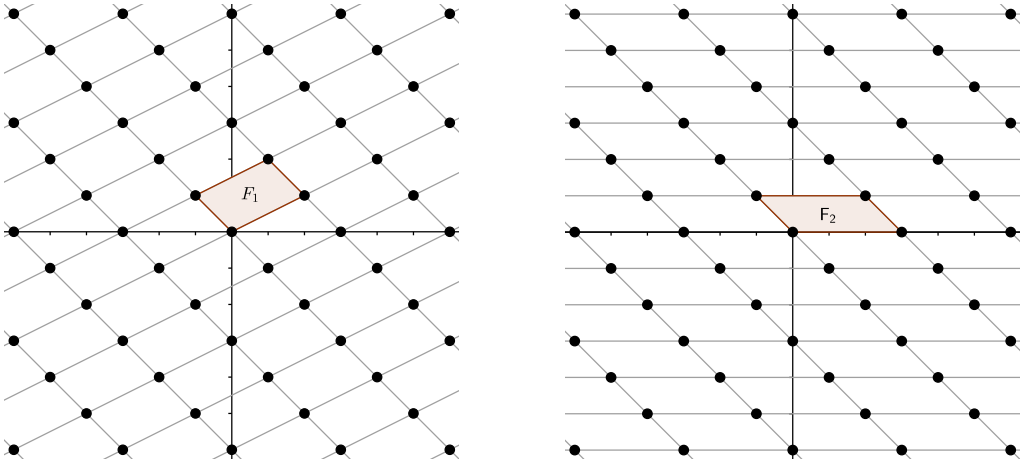
1.3 Região fundamental

Definição 1.3.1. *Uma **região fundamental** F de um reticulado $\Lambda = \Lambda(B) \subseteq \mathbb{R}^n$ de posto m é um subconjunto de span(B) que ladrilha span(B) por translações $\boldsymbol{v} + F$ com $\boldsymbol{v} \in \Lambda$, isto é,*

$$\textit{span}(B) = \bigcup_{\boldsymbol{v}\in\Lambda} \big(\boldsymbol{v} + F\big)$$

e dois ladrilhos $\boldsymbol{v}_1 + F$ e $\boldsymbol{v}_2 + F$, com $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \Lambda$ e $\boldsymbol{v}_1 \neq \boldsymbol{v}_2$, ou não se interceptam ou se interceptam apenas nos bordos.

Exemplo 1.3.1. *Considere o reticulado* Λ *com base* $\beta = \{(2,1),(-1,1)\}$. *Na Figura 1.4 estão ilustradas duas regiões fundamentais de* Λ, *a saber* $F_1 = \{\alpha_1(2,1) + \alpha_2(-1,1);\ 0 \leq \alpha_1, \alpha_2 < 1\}$ *e* $F_2 = \{\alpha_1(3,0) + \alpha_2(-1,1);\ 0 \leq \alpha_1, \alpha_2 < 1\}$.



(a) Ladrilhamento por F_1 (b) Ladrilhamento por F_2

Figura 1.4: Ladrilhamentos do reticulado Λ

Teorema 1.3.1. *[3] Seja* $\Lambda = \Lambda(B) \subseteq \mathbb{R}^n$ *um reticulado de posto* m. *Se* F_1 *e* F_2 *são regiões fundamentais de* Λ, *então* F_1 *e* F_2 *possuem o mesmo volume euclidiano (m-dimensional).*

Definição 1.3.2. *O* ***volume*** *de um reticulado* $\Lambda \subseteq \mathbb{R}^n$ *de posto* m, *denotado por vol*(Λ), *é definido como o volume euclidiano* m*-dimensional de uma região fundamental (qualquer) de* Λ.

Exemplo 1.3.2. *O volume do reticulado* Λ *apresentado no Exemplo 1.3.1 é vol*$(\Lambda) = 3/2$.

Definição 1.3.3. *Sejam* $\Lambda = \Lambda(B) \subseteq \mathbb{R}^n$ *um reticulado de posto* m *e* $\beta = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_m\}$ *uma base de* Λ. *O conjunto*

$$P_\beta = \left\{ \sum_{i=1}^{m} \alpha_i \boldsymbol{b}_i;\ 0 \leq \alpha_i < 1, \forall\ i \in \{1, \ldots, m\} \right\}$$

é denominado ***paralelotopo fundamental*** *de* Λ *associado à base* β.

Exemplo 1.3.3. *Considere novamente o reticulado* Λ *apresentado no Exemplo 1.3.1. Os conjuntos* F_1 *e* F_2 *(Figura 1.4) são paralelotopos fundamentais de* Λ *associados, respectivamente, às bases* $\{(2,1),(-1,1)\}$ *e* $\{(3,0),(-1,1)\}$ *de* Λ.

Teorema 1.3.2. *Qualquer paralelotopo fundamental de um reticulado* Λ *é uma região fundamental de* Λ.

Demonstração. Seja $\beta = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_m\}$ uma base de Λ e considere o paraletotopo fundamental associado a esta base, isto é,

$$P_\beta = \left\{ \sum_{i=1}^{m} \alpha_i \boldsymbol{b}_i;\ 0 \leq \alpha_i < 1, \forall\ i \in \{1, \ldots, m\} \right\}.$$

Seja B a matriz geradora de Λ associada à base β. Devemos mostrar que

(i) $\text{span}(B) = \bigcup_{\boldsymbol{v}\in\Lambda} \big(\boldsymbol{v} + P_\beta\big)$.

(ii) Se $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \Lambda$ e $\boldsymbol{v}_1 \neq \boldsymbol{v}_2$, então os ladrilhos $\boldsymbol{v}_1 + P_\beta$ e $\boldsymbol{v}_2 + P_\beta$ ou são disjuntos ou se interceptam apenas nos bordos.

(i) A inclusão $\bigcup_{\boldsymbol{v}\in\Lambda} \big(\boldsymbol{v} + P_\beta\big) \subseteq \text{span}(B)$ é trivial. Assim, resta mostrar a outra inclusão, isto é, $\text{span}(B) \subseteq \bigcup_{\boldsymbol{v}\in\Lambda} \big(\boldsymbol{v} + P_\beta\big)$. Com efeito, para cada $\boldsymbol{w} \in \text{span}(B)$ existem $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$ tais que $\boldsymbol{w} = \sum_{i=1}^{m} \alpha_i \boldsymbol{b}_i$. Logo

$$\boldsymbol{w} = \sum_{i=1}^{m} \alpha_i \boldsymbol{b}_i = \sum_{i=1}^{m} \lfloor \alpha_i \rfloor \boldsymbol{b}_i + \sum_{i=1}^{m} (\alpha_i - \lfloor \alpha_i \rfloor) \boldsymbol{b}_i \in \bigcup_{\boldsymbol{v}\in\Lambda} \big(\boldsymbol{v} + P_\beta\big),$$

uma vez que

$$\sum_{i=1}^{m} \lfloor \alpha_i \rfloor \boldsymbol{b}_i \in \Lambda \ \text{ e } \ \sum_{i=1}^{m} (\alpha_i - \lfloor \alpha_i \rfloor) \boldsymbol{b}_i \in P_\beta.$$

Isto mostra que $\text{span}(B) = \bigcup_{\boldsymbol{v}\in\Lambda} \big(\boldsymbol{v} + P_\beta\big)$.
(ii) Observe que o interior do conjunto $\boldsymbol{v} + P_\beta$ é dado por

$$\text{int}\big(\boldsymbol{v} + P_\beta\big) = \left\{ \boldsymbol{v} + \sum_{i=1}^{m} \alpha_i \boldsymbol{b}_i;\ 0 < \alpha_i < 1, \forall\ i \in \{1, \ldots, m\} \right\}.$$

Sejam $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \Lambda$ tais que $\text{int}\big(\boldsymbol{v}_1 + P_\beta\big) \cap \text{int}\big(\boldsymbol{v}_2 + P_\beta\big) \neq \emptyset$. Seja

$$\boldsymbol{x} \in \text{int}\big(\boldsymbol{v}_1 + P_\beta\big) \cap \text{int}\big(\boldsymbol{v}_2 + P_\beta\big).$$

Existem $s_1, \ldots, s_m, k_1, \ldots, k_m \in \mathbb{Z}$ e $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m \in \mathbb{R}$ tais que $0 < \alpha_i, \beta_i < 1$,

$$\boldsymbol{v}_1 = \sum_{i=1}^{m} s_i \boldsymbol{b}_i, \boldsymbol{v}_2 = \sum_{i=1}^{m} k_i \boldsymbol{b}_i \text{ e } \boldsymbol{x} = \sum_{i=1}^{m} s_i \boldsymbol{b}_i + \sum_{i=1}^{m} \alpha_i \boldsymbol{b}_i = \sum_{i=1}^{m} k_i \boldsymbol{b}_i + \sum_{i=1}^{m} \beta_i \boldsymbol{b}_i.$$

Como $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$ são linearmente independentes, segue que $s_i + \alpha_i = k_i + \beta_i$, isto é, $s_i - k_i = \beta_i - \alpha_i$. Logo $s_i = k_i$ e $\alpha_i = \beta_i$, uma vez que $s_i - k_i \in \mathbb{Z}$ e $-1 < \beta_i - \alpha_i < 1$. Portanto $\boldsymbol{v}_1 = \boldsymbol{v}_2$. □

Definição 1.3.4. *Um conjunto limitado $X \subseteq \mathbb{R}^m$ é dito* ***J-mensurável*** *(mensurável segundo Jordan) se, tomando-se um bloco $B = [a_1, b_1] \times \cdots \times [a_m, b_m] \subseteq \mathbb{R}^m$ que contenha*

*X, a função característica $\mathcal{X}_X : B \to \mathbb{R}$, que é dada por $\mathcal{X}_X(\boldsymbol{x}) = 1, \forall \boldsymbol{x} \in X$ e $\mathcal{X}_X(\boldsymbol{x}) = 0, \forall \boldsymbol{x} \in B \setminus X$, é integrável. Neste caso, o **volume** euclidiano m-dimensional de X é definido como*

$$vol_m(X) = \int_B \mathcal{X}_X(x)dx.$$

Teorema 1.3.3. *[29] Um conjunto limitado $X \subseteq \mathbb{R}^m$ é J-mensurável se, e somente se, sua fronteira $Fr(X)$ tem medida nula.*

Observação 1.3.1. *Qualquer paralelotopo fundamental de um reticulado é um conjunto J-mensurável e seu volume é dado pelo Teorema 1.3.5 a seguir.*

Teorema 1.3.4. *[29] Sejam $T : \mathbb{R}^m \to \mathbb{R}^m$ uma transformação linear e $A \in \mathbb{R}^{m\times m}$ tal que $T(\boldsymbol{x}) = \boldsymbol{x}A$, para todo $\boldsymbol{x} \in \mathbb{R}^m$. Se $\Omega \subseteq \mathbb{R}^m$ é um conjunto J-mensurável, então $T(\Omega)$ também é J-mensurável e*

$$vol_m(T(\Omega)) = |\det A| \cdot vol_m(\Omega).$$

Teorema 1.3.5. *O volume euclidiano m-dimensional de um paralelotopo fundamental de um reticulado Λ de posto m é dado por $\sqrt{\det \Lambda}$.*

Demonstração. Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado, $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ uma base de Λ e B a matriz geradora de Λ associada a esta base. Aplicando o processo de ortogonalização de Gram-Schmidt (ver Seção 8.4 de [4]) aos vetores $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ e normalizando os vetores gerados por este processo, obtemos vetores ortonormais $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ tais que

$$\text{span}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\} = \text{span}\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m\}.$$

Agora, sejam $\boldsymbol{a}_{m+1}, \ldots, \boldsymbol{a}_n \in \mathbb{R}^n$ tais que $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{a}_{m+1}, \ldots, \boldsymbol{a}_n\}$ é uma base ortonormal de $\mathbb{R}^n$ e considere a matriz

$$A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$$

em que A_1 é a matriz $m \times n$, cujas linhas são os vetores $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ e A_2 é a matriz $(n-m) \times n$, cujas linhas são os vetores $\boldsymbol{a}_{m+1}, \ldots, \boldsymbol{a}_n$. Note que $AA^t = A^tA = I_n$, $A_1A_1^t = I_m$ e $BA_2^t = 0$. Defina $T : \text{span}(B) \to \mathbb{R}^m$ pondo $T(\boldsymbol{x}) = \boldsymbol{x}A_1^t$. A aplicação T preserva a distância euclidiana, isto é, $\|T(\boldsymbol{x})\|_2 = \|\boldsymbol{x}\|_2$, $\forall \boldsymbol{x} \in \text{span}(B)$. De fato, para cada $\boldsymbol{x} \in \text{span}(B)$, existe $\boldsymbol{y} \in \mathbb{R}^m$ tal que $\boldsymbol{x} = \boldsymbol{y}A_1$ (já que $\text{span}(B) = \text{span}(A_1)$) e consequentemente

$$\begin{aligned} \|T(\boldsymbol{x})\|_2^2 &= \langle T(\boldsymbol{x}), T(\boldsymbol{x})\rangle = \left\langle \boldsymbol{x}A_1^t, \boldsymbol{x}A_1^t \right\rangle = (\boldsymbol{x}A_1^t)(\boldsymbol{x}A_1^t)^t = \boldsymbol{x}A_1^tA_1\boldsymbol{x}^t \\ &= (\boldsymbol{y}A_1)A_1^tA_1\boldsymbol{x}^t = \boldsymbol{y}(A_1A_1^t)A_1\boldsymbol{x}^t = (\boldsymbol{y}A_1)\boldsymbol{x}^t = \boldsymbol{x}\boldsymbol{x}^t = \|\boldsymbol{x}\|_2^2. \end{aligned}$$

Logo a aplicação T preserva o volume euclidiano (Teorema 10.53 de [1]). O Teorema 1.3.4 juntamente com a Observação 1.3.1 garantem que se $P_\beta = [0,1)^m B = \{\boldsymbol{x}B;\ \boldsymbol{x} \in [0,1)^m\}$

(isto é, P_β é o paralelotopo fundamental de Λ associado à base $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$), então

$$\begin{aligned} \mathrm{vol}_m(P_\beta) &= \mathrm{vol}_m\big(T(P_\beta)\big) = \mathrm{vol}_m\big([0,1)^m B A_1^t\big) \\ &= |\det(BA_1^t)| \cdot \mathrm{vol}_m\big([0,1)^m\big) = |\det(BA_1^t)|. \end{aligned}$$

Por outro lado, temos que $A^tA = A_1^tA_1 + A_2^tA_2$, isto é, $A_1^tA_1 = A^tA - A_2^tA_2$ e consequentemente

$$BA_1^tA_1B^t = B(A^tA - A_2^tA_2)B^t = BA^tAB^t - BA_2^tA_2B^t = BB^t,$$

já que $A^tA = I_n$ e $BA_2^t = 0$. Logo

$$\det(BA_1^t)^2 = \det(BA_1^t)\det(BA_1^t)^t = \det(BA_1^tA_1B^t) = \det(BB^t) = \det\Lambda.$$

Portanto $\mathrm{vol}_m(P_\beta) = \sqrt{\det\Lambda}$. □

Corolário 1.3.1. *O volume de um reticulado Λ é dado por $\sqrt{\det\Lambda}$.*

Demonstração. Basta aplicar os Teoremas 1.3.2 e 1.3.5. □

Exemplo 1.3.4. *Considere o reticulado Λ gerado pela matriz*

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

Temos que

$$G = BB^t = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$$

é uma matriz de Gram de Λ. Logo o volume de Λ é vol$(\Lambda) = \sqrt{\det\Lambda} = \sqrt{\det G} = \sqrt{3}$.

1.4 Região de Voronoi

Nesta seção, introduzimos o conceito de região de Voronoi. Recordamos algumas de suas propriedades já conhecidas quando a métrica considerada é a euclidiana. Discutimos também o fato de que algumas destas propriedades não são válidas para as métricas da soma e do máximo.

Definição 1.4.1. *Dado um elemento $\boldsymbol{v}$ de um reticulado $\Lambda = \Lambda(B) \subseteq \mathbb{R}^n$, a **região de Voronoi** de $\boldsymbol{v}$ (em relação à métrica d) é definida como*

$$\mathcal{R}_d(\boldsymbol{v}) = \{\boldsymbol{x} \in span(B);\ d(\boldsymbol{x}, \boldsymbol{v}) \leq d(\boldsymbol{x}, \boldsymbol{u}), \forall \boldsymbol{u} \in \Lambda\},$$

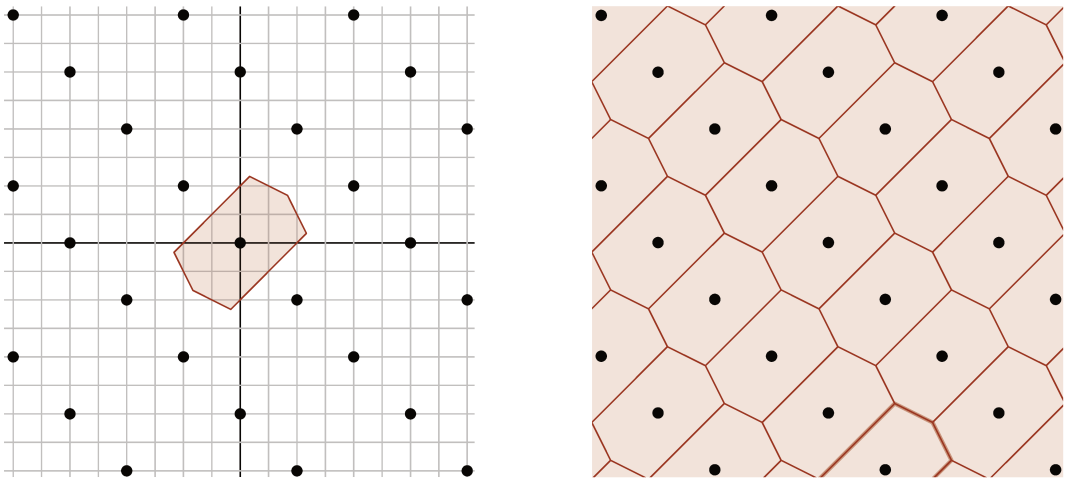
isto é,

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

Observação 1.4.1. *$\mathcal{R}_d(\boldsymbol{v})$ é o conjunto de todos os pontos de $span(B)$ que estão mais próximos de $\boldsymbol{v}$ do que de qualquer outro ponto de Λ (considerando a métrica d). Neste trabalho abordamos apenas métricas induzidas por uma norma, conforme mencionado anteriormente.*

No que segue, as regiões de Voronoi de $\boldsymbol{v}$ considerando a métrica da soma, a métrica euclidiana e a métrica do máximo são, respectivamente, denotadas por $\mathcal{R}_1(\boldsymbol{v})$, $\mathcal{R}_2(\boldsymbol{v})$ e $\mathcal{R}_\infty(\boldsymbol{v})$.

Exemplo 1.4.1. *Seja $\Lambda \subseteq \mathbb{R}^2$ o reticulado determinado pela base $\{(3,0),(-1,1)\}$. Na Figura 1.5(a) ilustramos a região de Voronoi $\mathcal{R}_2(\mathbf{0})$. Observe que $\mathcal{R}_2(\mathbf{0})$ é uma região fundamental de Λ, isto é, $\mathcal{R}_2(\mathbf{0})$ ladrilha $\mathbb{R}^2$ por translações $\boldsymbol{v} + \mathcal{R}_2(\mathbf{0})$ com $\boldsymbol{v} \in \Lambda$ (Figura 1.5(b)).*



(a) $\mathcal{R}_2(\mathbf{0})$ (b) $\mathcal{R}_2(\mathbf{0})$ é uma região fundamental de Λ

Figura 1.5: Região de Voronoi na métrica euclidiana

Observação 1.4.2. *Seja $\Lambda = \Lambda(B) \subset \mathbb{R}^n$ um reticulado. A região de Voronoi $\mathcal{R}_2(\mathbf{0})$ é uma região fundamental de Λ (Teorema 1.4.2). Porém, nas métricas da soma e do máximo a região de Voronoi de um reticulado nem sempre é uma região fundamental de Λ (Exemplo 1.4.2).*

Teorema 1.4.1. *Seja $\Lambda = \Lambda(B) \subseteq \mathbb{R}^n$ um reticulado. Para cada $\boldsymbol{v} \in \Lambda$, temos que*

$$\mathcal{R}_d(\boldsymbol{v}) = \boldsymbol{v} + \mathcal{R}_d(\mathbf{0}).$$

Demonstração. Como a métrica d é induzida por uma norma, segue que $d(\boldsymbol{w}+\boldsymbol{u}, \boldsymbol{w}+\boldsymbol{v}) = d(\boldsymbol{u}, \boldsymbol{v})$ quaisquer que sejam $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^n$. Assim, para cada $\boldsymbol{v} \in \Lambda$ tem-se

$$\begin{aligned} \boldsymbol{x} \in \mathcal{R}_d(\mathbf{0}) &\iff \boldsymbol{x} \in \operatorname{span}(B) \text{ e } d(\boldsymbol{x}, \mathbf{0}) \leq d(\boldsymbol{x}, \boldsymbol{u}) \text{ para todo } \boldsymbol{u} \in \Lambda. \\ &\iff (\boldsymbol{v}+\boldsymbol{x}) \in \operatorname{span}(B) \text{ e } d(\boldsymbol{v}+\boldsymbol{x}, \boldsymbol{v}) \leq d(\boldsymbol{v}+\boldsymbol{x}, \boldsymbol{w}) \text{ para todo } \boldsymbol{w} \in \Lambda. \\ &\iff (\boldsymbol{v}+\boldsymbol{x}) \in \mathcal{R}_d(\boldsymbol{v}). \end{aligned}$$

Isto mostra que $\mathcal{R}_d(\boldsymbol{v}) = \boldsymbol{v} + \mathcal{R}_d(\mathbf{0})$. □

Definição 1.4.2. *Dado um reticulado $\Lambda \subseteq \mathbb{R}^n$, a região $\mathcal{R}_d(\mathbf{0})$ é chamada* ***região de Voronoi*** *de Λ. A região de Voronoi de Λ também é denotada por $\mathcal{R}_d(\Lambda)$.*

Teorema 1.4.2. *Seja $\Lambda = \Lambda(B) \subseteq \mathbb{R}^n$ um reticulado. Temos que $\mathcal{R}_2(\Lambda)$ é uma região fundamental de Λ.*

Demonstração. Observe que $\operatorname{span}(B) = \bigcup_{\boldsymbol{v}\in\Lambda} \mathcal{R}_2(\boldsymbol{v})$. Do Teorema 1.4.1, obtemos

$$\operatorname{span}(B) = \bigcup_{\boldsymbol{v}\in\Lambda} \big(\boldsymbol{v} + \mathcal{R}_2(\mathbf{0})\big).$$

Agora, sejam $\boldsymbol{v} \in \Lambda$ e $X = \{\boldsymbol{u} \in \Lambda;\ \boldsymbol{u} \neq \boldsymbol{v} \text{ e } \|\boldsymbol{u}-\boldsymbol{v}\|_2 \text{ é mínimo}\}$. Dos Corolários 1.1.2 e 1.1.3, segue que X é não vazio e finito, digamos $X = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k\}$. Pode-se mostrar que

$$\mathcal{R}_2(\boldsymbol{v}) = \big\{\boldsymbol{x} \in \operatorname{span}(B);\ d(\boldsymbol{x}, \boldsymbol{v}) \leq d(\boldsymbol{x}, \boldsymbol{u}_i), \forall i \in \{1, \ldots, k\}\big\},$$

o interior do conjunto $\mathcal{R}_2(\boldsymbol{v})$ é dado por

$$\operatorname{Int}\big(\mathcal{R}_2(\boldsymbol{v})\big) = \big\{\boldsymbol{x} \in \operatorname{span}(B);\ d(\boldsymbol{x}, \boldsymbol{v}) < d(\boldsymbol{x}, \boldsymbol{u}_i), \forall i \in \{1, \ldots, k\}\big\}$$

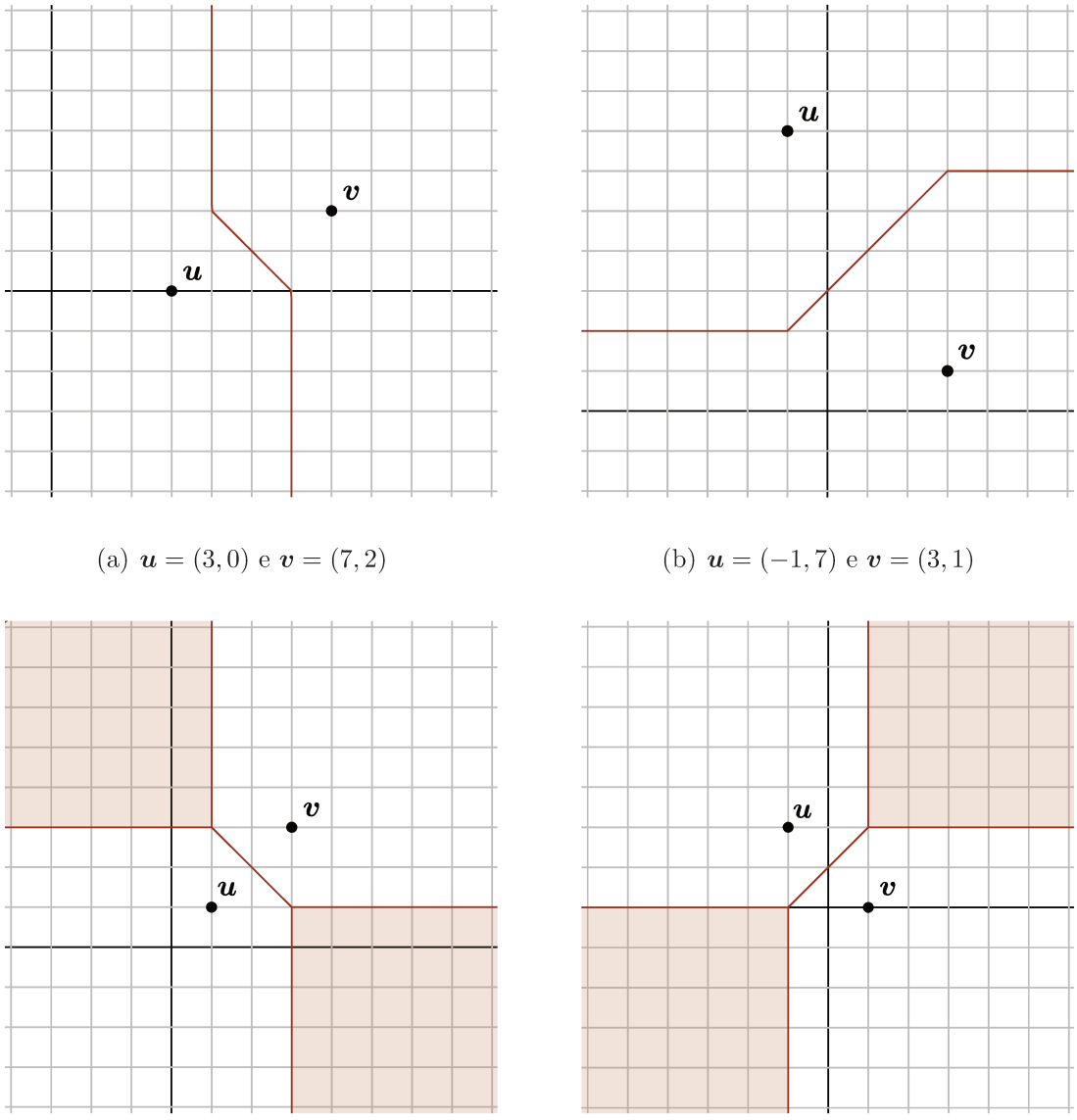
e sua fronteira (isto é, o bordo) é dado por

$$\operatorname{Fr}\big(\mathcal{R}_2(\boldsymbol{v})\big) = \left\{\boldsymbol{x} \in \operatorname{span}(B) \,\middle|\, \begin{array}{l} d(\boldsymbol{x}, \boldsymbol{v}) = d(\boldsymbol{x}, \boldsymbol{u}_i), \text{ para algum } i \in \{1, \ldots, k\} \\ \text{e } d(\boldsymbol{x}, \boldsymbol{v}) \leq d(\boldsymbol{x}, \boldsymbol{u}_i), \text{ para todo } i \in \{1, \ldots, k\} \end{array} \right\}.$$

Para qualquer $\boldsymbol{u} \in \Lambda$, temos que $\mathcal{R}_2(\boldsymbol{u}) \cap \mathcal{R}_2(\boldsymbol{v}) \neq \emptyset$ se, e somente se, $\boldsymbol{u} = \boldsymbol{u}_i$ para algum $i \in \{1, \ldots, k\}$. Renomeando os vetores, se necessário, podemos supor sem perda de generalidade que $\boldsymbol{u} = \boldsymbol{u}_1$. Assim, $\boldsymbol{x} \in \mathcal{R}_2(\boldsymbol{u}) \cap \mathcal{R}_2(\boldsymbol{v})$ implica que $\boldsymbol{x} \in \operatorname{span}(B)$, $d(\boldsymbol{x}, \boldsymbol{v}) = d(\boldsymbol{x}, \boldsymbol{u}_1)$ e $d(\boldsymbol{x}, \boldsymbol{v}) \leq d(\boldsymbol{x}, \boldsymbol{u}_j)$, para todo $j \in \{2, \ldots, k\}$. Logo $\boldsymbol{x} \in \operatorname{Fr}\big(\mathcal{R}_2(\boldsymbol{v})\big)$. Isto mostra que $\mathcal{R}_2(\boldsymbol{u}) \cap \mathcal{R}_2(\boldsymbol{v}) \subseteq \operatorname{Fr}\big(\mathcal{R}_2(\boldsymbol{v})\big)$. Analogamente, podemos mostrar que $\mathcal{R}_2(\boldsymbol{u}) \cap \mathcal{R}_2(\boldsymbol{v}) \subseteq \operatorname{Fr}\big(\mathcal{R}_2(\boldsymbol{u})\big)$. Portanto ladrilhos distintos $\mathcal{R}_2(\boldsymbol{u})$ e $\mathcal{R}_2(\boldsymbol{v})$ ou não se interceptam ou se interceptam apenas nos bordos. □

Observação 1.4.3. *Dado um reticulado Λ, o volume da região de Voronoi $\mathcal{R}_2(\Lambda)$ é dado por $(\det \Lambda)^{1/2}$, pois é uma região fundamental de Λ.*

Observação 1.4.4. *Sejam $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^2$ tais que $\boldsymbol{u} \neq \boldsymbol{v}$. O conjunto dos pontos equidistantes de $\boldsymbol{u}$ e $\boldsymbol{v}$ na métrica euclidiana é uma reta (a mediatriz do segmento $[\boldsymbol{u}, \boldsymbol{v}]$). Por outro lado, observamos que o conjunto dos pontos equidistantes de $\boldsymbol{u}$ e $\boldsymbol{v}$ na métrica da soma (e também na métrica do máximo) nem sempre é uma "curva", às vezes é uma "região". Nas Figuras 1.6 e 1.7 ilustramos o conjunto dos pontos que são equidistantes aos pontos $\boldsymbol{u}$ e $\boldsymbol{v}$ na métrica da soma e na métrica do máximo, respectivamente.*



(a) $\boldsymbol{u} = (3, 0)$ e $\boldsymbol{v} = (7, 2)$

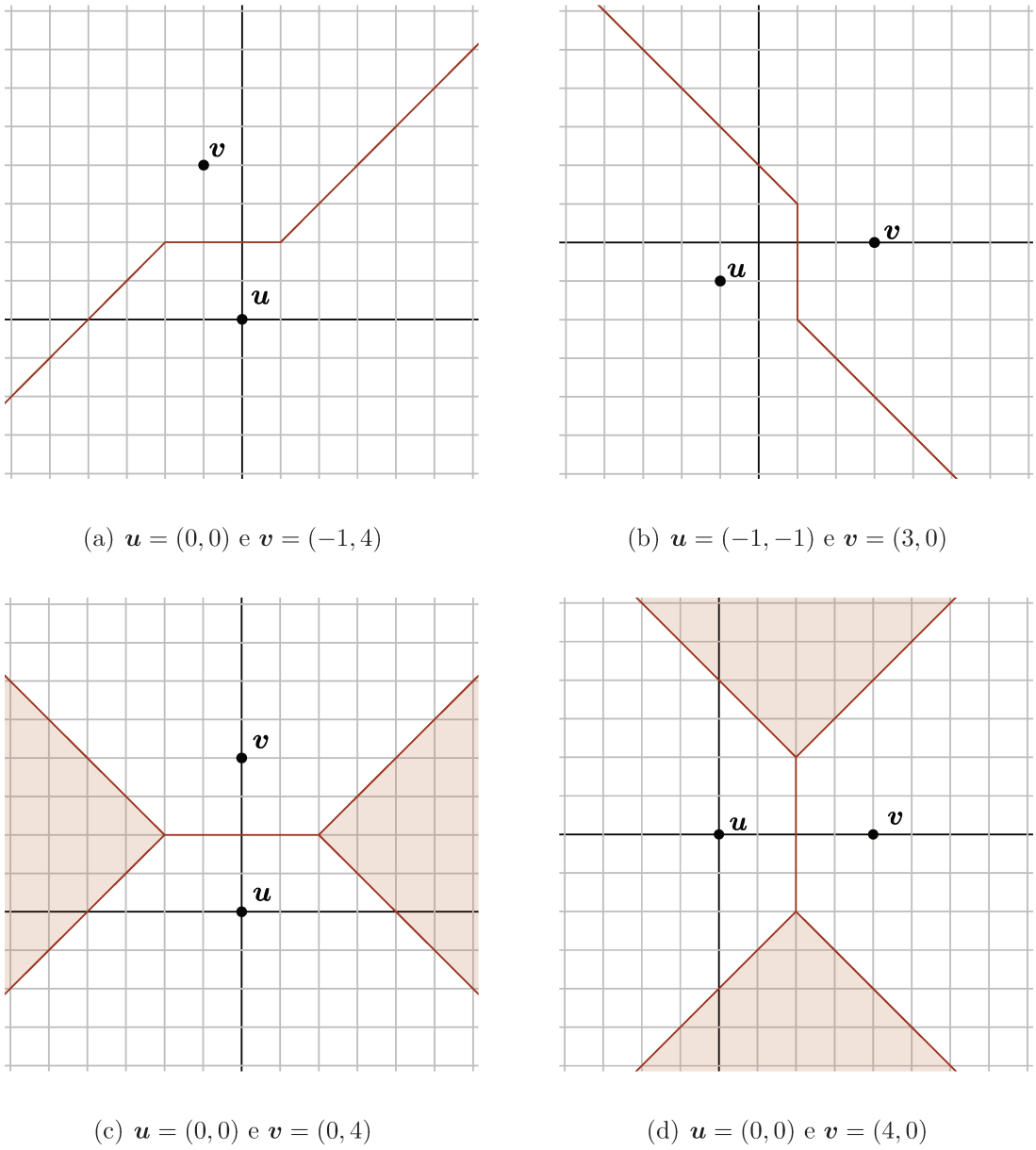
(b) $\boldsymbol{u} = (-1, 7)$ e $\boldsymbol{v} = (3, 1)$

(c) $\boldsymbol{u} = (1, 1)$ e $\boldsymbol{v} = (3, 3)$

(d) $\boldsymbol{u} = (-1, 2)$ e $\boldsymbol{v} = (1, 0)$

Figura 1.6: Lugar geométrico dos pontos equidistantes de $\boldsymbol{u}$ e $\boldsymbol{v}$ na métrica da soma

O conjunto dos pontos equidistantes de $\boldsymbol{u}$ e $\boldsymbol{v}$ na métrica da soma (resp. na métrica do máximo) não é uma "curva" quando $\boldsymbol{u}-\boldsymbol{v} = (\pm t, t)$ (resp. $\boldsymbol{u}-\boldsymbol{v} = (0, t)$ ou $\boldsymbol{u}-\boldsymbol{v} = (t, 0)$) para algum $t \in \mathbb{R}$.



(a) $\boldsymbol{u} = (0, 0)$ e $\boldsymbol{v} = (-1, 4)$

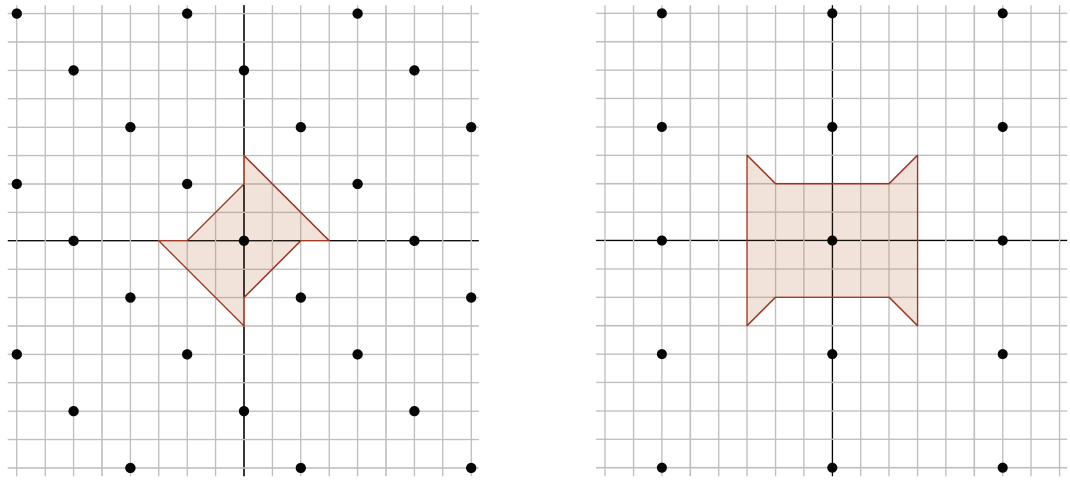
(b) $\boldsymbol{u} = (-1, -1)$ e $\boldsymbol{v} = (3, 0)$

(c) $\boldsymbol{u} = (0, 0)$ e $\boldsymbol{v} = (0, 4)$

(d) $\boldsymbol{u} = (0, 0)$ e $\boldsymbol{v} = (4, 0)$

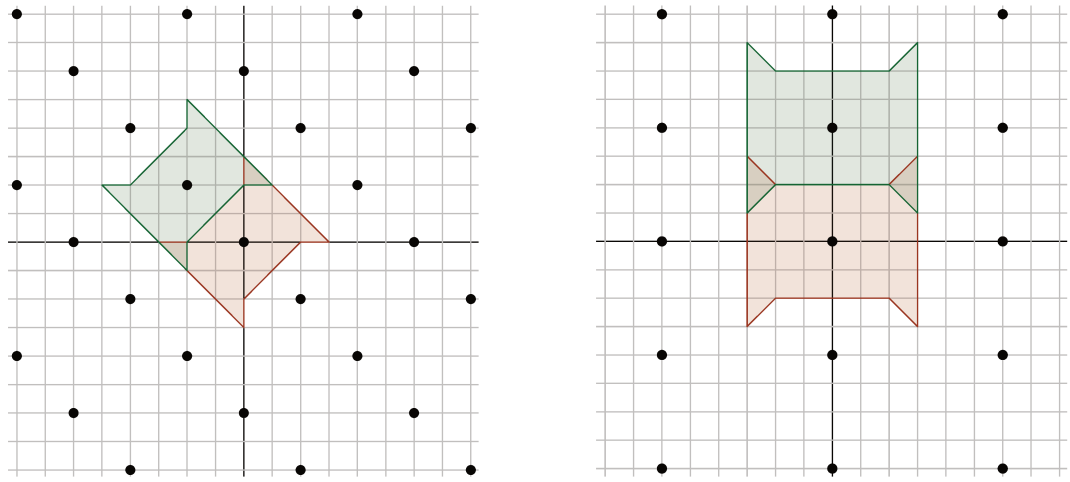
Figura 1.7: Lugar geométrico dos pontos equidistantes de $\boldsymbol{u}$ e $\boldsymbol{v}$ na métrica do máximo

Exemplo 1.4.2. *Sejam* $\Lambda_\alpha, \Lambda_\beta \subseteq \mathbb{R}^2$ *os reticulados gerados pelas bases* $\alpha = \{(3, 0), (-1, 1)\}$ *e* $\beta = \{(3, 0), (0, 2)\}$*, respectivamente. Nas Figuras 1.8(a)e 1.8(b) estão representadas as regiões de Voronoi* $\mathcal{R}_1(\Lambda_\alpha)$ *e* $\mathcal{R}_\infty(\Lambda_\beta)$*, respectivamente. Observe que* $(\det \Lambda_\alpha)^{1/2} = 3$*,* $(\det \Lambda_\beta)^{1/2} = 6$*, a área euclidiana de* $\mathcal{R}_1(\Lambda_\alpha)$ *é* $13/4$ *e a de* $\mathcal{R}_\infty(\Lambda_\beta)$ *é* $13/2$*. Pelo Corolário 1.3.1, temos que* $\mathcal{R}_1(\Lambda_\alpha)$ *e* $\mathcal{R}_\infty(\Lambda_\beta)$ *não são regiões fundamentais de* Λ_α *e* Λ_β*, respectivamente. Em cada caso, ladrilhos que não são disjuntos e não se interceptam apenas nos bordos estão ilustrados na Figura 1.9.*



(a) $\mathcal{R}_1(\Lambda_\alpha)$ (b) $\mathcal{R}_\infty(\Lambda_\beta)$

Figura 1.8: Região de Voronoi



(a) Reticulado Λ_α (b) Reticulado Λ_β

Figura 1.9: $\mathcal{R}_1(\Lambda_\alpha)$ e $\mathcal{R}_\infty(\Lambda_\beta)$ não são regiões fundamentais de Λ_α e Λ_β, respectivamente

1.5 Empacotamento esférico

Definição 1.5.1. *Um* ***empacotamento esférico*** *no* $\mathbb{R}^n$ *é uma coleção de esferas/bolas no* $\mathbb{R}^n$*, todas de mesmo raio, de modo que quaisquer duas esferas/bolas ou não se interceptam ou se interceptam apenas no bordo. Um* ***empacotamento reticulado*** *no* $\mathbb{R}^n$ *é empacotamento esférico tal que o conjunto dos centros das esferas/bolas formam um reticulado.*

Observação 1.5.1. *Dado um reticulado* $\Lambda \subseteq \mathbb{R}^n$*, sempre existe um empacotamento*

esférico cujos centros das esferas/bolas são os elementos de Λ *(Teorema 1.1.1).*

Definição 1.5.2. *O* ***raio de empacotamento*** ρ *de um reticulado* Λ *não nulo é o maior número real* r *tal que* $\Lambda + B[\mathbf{0}, r]$ *é um empacotamento reticulado.*

Teorema 1.5.1. *Seja* $\Lambda \subseteq \mathbb{R}^n$ *um reticulado não nulo. O raio de empacotamento de* Λ *é dado por* $\rho = \|\boldsymbol{x}_0\|/2$*, em que* $\|\boldsymbol{x}_0\| = \min\{\|\boldsymbol{x}\|;\ \boldsymbol{x} \in \Lambda \text{ e } \boldsymbol{x} \neq \mathbf{0}\}$.

Demonstração. Seja $\boldsymbol{x}_0 \in \Lambda$ tal que $\|\boldsymbol{x}_0\| = \min\{\|\boldsymbol{x}\|;\ \boldsymbol{x} \in \Lambda \text{ e } \boldsymbol{x} \neq \mathbf{0}\}$ (a existência é garantida pelo Corolário 1.1.3). Note que $\Lambda + B[\mathbf{0}, \|\boldsymbol{x}_0\|/2]$ é um empacotamento de Λ. Com efeito, suponha que $\boldsymbol{u}, \boldsymbol{v} \in \Lambda$ e

$$\big(\boldsymbol{u} + B[\mathbf{0}, \|\boldsymbol{x}_0\|/2]\big) \cap \big(\boldsymbol{v} + B[\mathbf{0}, \|\boldsymbol{x}_0\|/2]\big) \neq \emptyset.$$

Sejam $\boldsymbol{x}, \boldsymbol{y} \in B[\mathbf{0}, \|\boldsymbol{x}_0\|/2]$ tais que $\boldsymbol{u} + \boldsymbol{x} = \boldsymbol{v} + \boldsymbol{y}$, isto é, $\boldsymbol{v} - \boldsymbol{u} = \boldsymbol{x} - \boldsymbol{y}$. Donde segue que

$$\|\boldsymbol{v} - \boldsymbol{u}\| = \|\boldsymbol{x} - \boldsymbol{y}\| \leq \|\boldsymbol{x}\| + \|\boldsymbol{y}\| \leq \frac{\|\boldsymbol{x}_0\|}{2} + \frac{\|\boldsymbol{x}_0\|}{2} = \|\boldsymbol{x}_0\|.$$

Porém, $\boldsymbol{x}_0$ e $\boldsymbol{v} - \boldsymbol{u}$ pertencem ao reticulado Λ e $\|\boldsymbol{x}_0\| = \min\{\|\boldsymbol{x}\|;\ \boldsymbol{x} \in \Lambda \text{ e } \boldsymbol{x} \neq \mathbf{0}\}$. Logo $\|\boldsymbol{v} - \boldsymbol{u}\| = \|\boldsymbol{x} - \boldsymbol{y}\| = \|\boldsymbol{x}_0\|$. Da igualdade $\|\boldsymbol{x} - \boldsymbol{y}\| = \|\boldsymbol{x}_0\|$, obtemos

$$\|\boldsymbol{x}\| = \|\boldsymbol{y}\| = \frac{\|\boldsymbol{x}_0\|}{2},$$

uma vez que $\|\boldsymbol{x}\| \leq \|\boldsymbol{x}_0\|/2$ e $\|\boldsymbol{y}\| \leq \|\boldsymbol{x}_0\|/2$. Isto mostra que as bolas $\boldsymbol{u} + B[\mathbf{0}, \|\boldsymbol{x}_0\|/2]$ e $\boldsymbol{v} + B[\mathbf{0}, \|\boldsymbol{x}_0\|/2]$ se interceptam apenas no bordo. Para concluir a prova, basta observar que quando $r > \|\boldsymbol{x}_0\|/2$ a coleção de bolas $\Lambda + B[\mathbf{0}, r]$ não é um empacotamento esférico, pois $\boldsymbol{x}_0/2 \in B(\mathbf{0}, r) \cap B(\boldsymbol{x}_0, r)$. □

Definição 1.5.3. *Seja* $\Lambda \subseteq \mathbb{R}^n$ *um reticulado de posto* m*. Definimos a* ***densidade de empacotamento*** *esférico de* Λ *em relação a uma métrica* d *como*

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

ou seja,

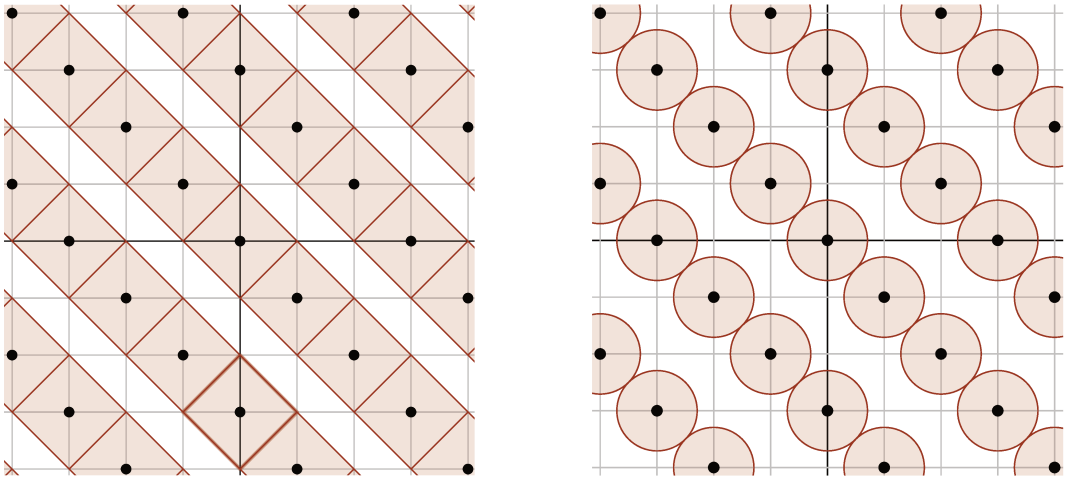
$$\Delta_d(\Lambda) = \frac{vol_m(B_d[\mathbf{0}, \rho])}{vol(\Lambda)} = \frac{vol_m(B_d[\mathbf{0}, 1])\rho^n}{\sqrt{\det(\Lambda)}}.$$

Observação 1.5.2. *A densidade de empacotamento de um reticulado* $\Lambda = \Lambda(B) \subseteq \mathbb{R}^n$ *é a proporção do espaço gerado pelas linhas de* B *que é coberta pela união das esferas/bolas centradas nos pontos de* Λ *e de raio* ρ*.*

Definição 1.5.4. *A* ***densidade de centro*** *de um reticulado* Λ *de posto* m *em relação a métrica* d *é o número* $\delta_d(\Lambda) = \rho^n / vol(\Lambda)$.

Observação 1.5.3. *Utilizamos ρ_1, $\Delta_1(\Lambda)$, $\delta_1(\Lambda)$ para denotar o raio de empacotamento, a densidade de empacotamento e a densidade de centro de Λ em relação à métrica da soma. Analogamente, usamos ρ_2, $\Delta_2(\Lambda)$, $\delta_2(\Lambda)$ para representar o raio de empacotamento, a densidade de empacotamento e a densidade de centro de Λ em relação à métrica euclidiana.*

Exemplo 1.5.1. *Considere o reticulado $\Lambda \subseteq \mathbb{R}^2$ gerado pela base $\{(2,1),(-1,1)\}$. Nas Figuras 1.10(a) e 1.10(b) estão representados empacotamentos esféricos deste reticulado, respectivamente, em relação à métrica da soma e em relação à métrica euclidiana. Observe que $vol(\Lambda) = 3$, $\rho_1 = 1$, $\rho_2 = \sqrt{2}/2$, $vol_2(B_1[\mathbf{0}, \rho_1]) = 2$, $vol_2(B_2[\mathbf{0}, \rho_2]) = \pi/2$. Logo $\Delta_1(\Lambda) = 2/3$, $\Delta_2(\Lambda) = \pi/6$, $\delta_1(\Lambda) = 1/3$ e $\delta_2(\Lambda) = 1/6$.*



(a) Métrica da soma (b) Métrica euclidiana

Figura 1.10: Empacotamento esférico do reticulado Λ gerado pela base $\{(2,1),(-1,1)\}$

Observação 1.5.4. *Fixados uma métrica e um inteiro positivo n, um problema clássico é a busca pelo reticulado n-dimensional com a maior densidade possível. São poucas as dimensões em que tais reticulados são conhecidos. Por exemplo, na métrica euclidiana são conhecidos os reticulados mais densos nas dimensões de 1 até 8 [9] e na dimensão 24 [8] (ver Seção 1.7). Enquanto que na métrica da soma, são conhecidos apenas os reticulados mais densos nas dimensões 1, 2 e 3 [12].*

1.6 Número de vizinhos

Um problema clássico relacionado com empacotamentos reticulados é o problema do número de vizinhos (*kissing number*).

Definição 1.6.1. *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado. Para cada $\boldsymbol{x} \in \Lambda$, o número de vetores $\boldsymbol{y} \in \Lambda$ tais que $\boldsymbol{x} \neq \boldsymbol{y}$ e $d(\boldsymbol{x}, \boldsymbol{y}) = \|\boldsymbol{x} - \boldsymbol{y}\|$ seja mínima, que denotamos por $\tau_d(\boldsymbol{x})$, é dito o* ***número de vizinhos*** *de $\boldsymbol{x}$.*

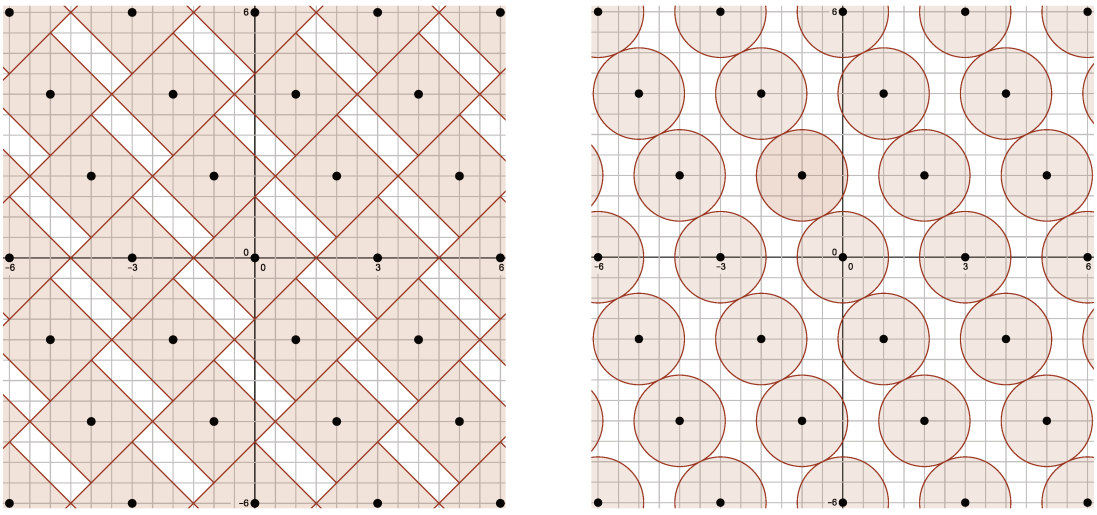
Teorema 1.6.1. *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado. Dados $\boldsymbol{x}, \boldsymbol{y} \in \Lambda$, o número de vizinhos de $\boldsymbol{x}$ é igual ao número de vizinhos de $\boldsymbol{y}$.*

Demonstração. Se $\Lambda = \{\mathbf{0}\}$, o resultado é trivial. Suponha que $\Lambda \neq \{\mathbf{0}\}$ e sejam $V_x = \{\boldsymbol{z} \in \Lambda;\ \boldsymbol{x} \neq \boldsymbol{z}$ e $d(\boldsymbol{x}, \boldsymbol{z}) = \|\boldsymbol{x} - \boldsymbol{z}\|$ é mínima$\}$ e $V_y = \{\boldsymbol{z} \in \Lambda;\ \boldsymbol{y} \neq \boldsymbol{z}$ e $d(\boldsymbol{y}, \boldsymbol{z}) = \|\boldsymbol{y} - \boldsymbol{z}\|$ é mínima$\}$. Para obter o resultado desejado, basta observar que a aplicação $\varphi : V_x \to V_y$ dada por $\varphi(\boldsymbol{z}) = \boldsymbol{z} + (\boldsymbol{y} - \boldsymbol{x})$ é bem definida e bijetora. □

Definição 1.6.2. *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado. O número $\tau_d(\mathbf{0})$ é chamado* ***número de vizinhos*** *(ou* ***kissing number****) de Λ.*

Observação 1.6.1. *O número número de vizinhos de Λ também será denotado por $\tau_d(\Lambda)$ ou simplesmente τ_d. O número de vizinhos em relação às métricas da soma e euclidiana serão denotados por τ_1 e τ_2, respectivamente. No próximo exemplo podemos observar que o número de vizinhos de um reticulado depende da norma utilizada.*

Exemplo 1.6.1. *Seja $\Lambda \subseteq \mathbb{R}^2$ o reticulado gerado pela base $\{(3, 0), (2, 2)\}$. Nas Figuras 1.11(a) e 1.11(b) estão representados empacotamentos esféricos deste reticulado, respectivamente, em relação à métrica da soma e em relação à métrica euclidiana. Observamos que o reticulado Λ possui kissing number igual a $\tau_1 = 4$ na métrica da soma e kissing number igual a $\tau_2 = 2$ na métrica euclidiana.*



(a) Métrica da soma (b) Métrica euclidiana

Figura 1.11: Empacotamentos esféricos de Λ

Observação 1.6.2. *O kissing number na métrica euclidiana define o segundo termo da chamada série teta do reticulado [9, 45].*

1.7 Reticulados importantes

Nesta seção, todos os resultados informados (raio de empacotamento, norma mínima, densidade, etc) são relativos à norma euclidiana. Dados referentes às outras métricas são escassos na literatura.

O reticulado $\mathbb{Z}^n$

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

$$\mathbb{Z}^n = \{(x_1, \ldots, x_n);\ x_1, \ldots, x_n \in \mathbb{Z}\}.$$

Qualquer matriz unimodular de ordem n gera $\mathbb{Z}^n$. Em particular, a matriz identidade I_n é uma matriz geradora de $\mathbb{Z}^n$. O reticulado $\mathbb{Z}^n$ é autodual (isto é, $(\mathbb{Z}^n)^* = \mathbb{Z}^n$), sua norma mínima é 1, seu *kissing number* é $2n$, seu raio de empacotamento é $1/2$ e sua densidade de centro é 2^{-n}.

O reticulado A_n

O reticulado A_n é definido como

$$A_n = \{(x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1};\ x_0 + x_1 + \cdots + x_n = 0\}.$$

Geometricamente A_n pode ser visto como a interseção entre o reticulado cúbico $\mathbb{Z}^{n+1}$ e o hiperplano perpendicular ao vetor $\boldsymbol{e} = (1, \ldots, 1)$. Uma matriz geradora é dada por

$$\begin{pmatrix} -1 & 1 & 0 & 0 & \ldots & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & \ldots & 0 & -1 & 1 \end{pmatrix}.$$

Pode-se mostrar que A_n tem norma mínima igual a $\sqrt{2}$, seu *kissing number* é $n(n+1)$, seu raio de empacotamento é $1/\sqrt{2}$ e sua densidade de centro é $2^{-n/2}(n+1)^{-1/2}$.

O reticulado D_n

O reticulado D_n é conjunto formado por todos os vetores do $\mathbb{R}^n$ que possuem coordenadas inteiras e cuja soma das mesmas é par, isto é,

$$D_n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n;\ x_1 + \cdots + x_n \text{ é par}\}.$$

Uma matriz geradora para D_n é dada por

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

Pode-se mostrar que D_n tem norma mínima igual a $\sqrt{2}$, seu *kissing number* é $2n(n-1)$, seu raio de empacotamento é $1/\sqrt{2}$ e sua densidade de centro $2^{-(n+2)/2}(n+1)$.

O reticulado E_8

O reticulado E_8 é formado por todos os pontos $(x_1, \dots, x_8) \in \mathbb{R}^8$ tais que $\{x_1, \dots, x_8\} \subset \mathbb{Z}$ ou $\{x_1, \dots, x_8\} \subset \mathbb{Z} + 1/2$ e $x_1 + \cdots + x_8 \equiv 0 \mod 2$, isto é,

$$E_8 = \{(x_1, \dots, x_8) \in \mathbb{R}^8;\ \text{todo } x_i \in \mathbb{Z} \text{ ou todo } x_i \in \mathbb{Z} + 1/2,\ x_1 + \cdots + x_8 \equiv 0 \mod 2\}.$$

Este é o reticulado mais denso em dimensão 8. Uma matriz geradora de E_8 é dada por

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

Pode-se mostrar que E_8 é autodual (isto é, $(E_8)^* = E_8$), sua norma mínima igual a $\sqrt{2}$, seu *kissing number* é 240, seu raio de empacotamento é $1/\sqrt{2}$ e sua densidade de centro é $1/16$.

O reticulado E_7

O reticulado E_7 é constituído pelos pontos de E_8 que são perpendiculares ao vetor $\boldsymbol{e} = (1, \dots, 1)$, isto é,

$$E_7 = \{(x_1, \dots, x_8) \in E_8;\ x_1 + \cdots + x_8 = 0\}.$$

Uma matriz geradora de E_7 é dada por

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

Pode-se mostrar que o determinante de E_7 é 2, sua norma mínima igual a $\sqrt{2}$, seu *kissing number* é 126, seu raio de empacotamento é $1/\sqrt{2}$ e sua densidade de centro é $1/16$.

O reticulado E_6

O reticulado E_6 é constituído pelos vetores de E_8 que pertencem ao complemento ortogonal do subespaço vetorial gerado por $(1, 0, \ldots, 0, 1)$ e $(0, 1, \ldots, 1, 0)$, isto é,

$$E_6 = \{(x_1, \ldots, x_8) \in E_8;\ x_1 + x_8 = x_2 + \cdots + x_7 = 0\}.$$

Uma matriz geradora de E_6 é dada por

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

Pode-se mostrar que o determinante de E_6 é 3, sua norma mínima igual a $\sqrt{2}$, seu *kissing number* é 72, seu raio de empacotamento é $1/\sqrt{2}$ e sua densidade de centro é $1/(8\sqrt{3})$.

O reticulado de Barnes-Wall Λ_{16} (ou $BW16$)

O reticulado de Barnes-Wall Λ_{16} é constituído por todas as combinações lineares inteiras das linhas da seguinte matriz

$$\frac{1}{\sqrt{2}}\begin{pmatrix}
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}.$$

Pode-se mostrar que o determinante de Λ_{16} é 256, sua norma mínima é igual a 2, seu *kissing number* é 4320, seu raio de empacotamento é 1 e sua densidade de centro é 1/16.

O reticulado de Leech Λ_{24}

O reticulado de Leech Λ_{24} é constituído por todas as combinações lineares inteiras das linhas da seguinte matriz

$$\frac{1}{\sqrt{8}}\begin{pmatrix}
8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
4 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
4 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
4 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0\\
2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0\\
0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0\\
-3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}.$$

Pode-se mostrar que o determinante de Λ_{24} é 1, sua norma mínima é igual a 2, seu *kissing number* é 196560, seu raio de empacotamento é 1 e sua densidade de centro é 1.

Concluímos esta seção apresentando uma tabela com os reticulados mais densos (considerando a métrica euclidiana) nas dimensões de 1 até 8 [9] e na dimensão 24 [8]. Estas são as únicas dimensões em que os reticulados mais densos são conhecidos.

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

Tabela 1.1: Reticulados mais densos (norma euclidiana)

Capítulo 2

Códigos lineares q-ários

Neste capítulo, apresentamos uma breve introdução a códigos lineares q-ários. Novamente, para tornar o texto o mais autossuficiente possível fornecemos demonstrações de vários resultados apresentados. As principais referências utilizadas neste capítulo foram [11], [21], [34] e [35].

2.1 Códigos lineares

Sejam q um inteiro positivo, $\mathbb{Z}_q$ o anel dos inteiros módulo q e $\mathbb{Z}_q^n$ o conjunto formado por todas as n-uplas sobre $\mathbb{Z}_q$, isto é,

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

Definição 2.1.1. *Chamamos de* ***código linear*** q***-ário*** *de comprimento n a um subgrupo aditivo de $\mathbb{Z}_q^n$.*

Observação 2.1.1. *Um código linear q-ário também é chamado de código linear sobre $\mathbb{Z}_q$, ou simplesmente, código linear.*

Definição 2.1.2. *Sejam $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k \in \mathbb{Z}_q^n$. Dizemos que $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$ são* ***linearmente independentes*** *sobre $\mathbb{Z}_q$ quando*

$$\alpha_1\boldsymbol{b}_1 + \cdots + \alpha_k\boldsymbol{b}_k = \mathbf{0}\ (\alpha_1, \ldots, \alpha_k \in \mathbb{Z}_q) \implies \alpha_1 = \cdots = \alpha_k = 0.$$

Caso contrário, os vetores $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$ são ditos ***linearmente dependentes*** *sobre $\mathbb{Z}_q$.*

Definição 2.1.3. *Sejam $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k \in \mathbb{Z}_q^n$ e $\{\mathbf{0}\} \neq C \subseteq \mathbb{Z}_q^n$ um código linear. Dizemos que os vetores $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$* ***geram*** *$C$, quando $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k \in C$ e qualquer vetor $\boldsymbol{v} \in C$ pode ser escrito como uma combinação linear (em geral, não única) destes vetores, isto é, quando existem $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}_q$ tais que $\boldsymbol{v} = \alpha_1\boldsymbol{b}_1 + \cdots + \alpha_k\boldsymbol{b}_k$. Neste caso, escrevemos*

$$C = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_k \rangle .$$

Por convenção, dizemos que o código linear nulo $C = \{\mathbf{0}\} \subseteq \mathbb{Z}_q^n$ é gerado pelo conjunto vazio. Em outras palavras, $C = \{\mathbf{0}\} = \langle \emptyset \rangle$.

Definição 2.1.4. *Chamamos de **base**[1] de um código linear $C \subseteq \mathbb{Z}_q^n$ qualquer subconjunto S de $\mathbb{Z}_q^n$ formado por vetores linearmente independentes que geram C.*

Observação 2.1.2. *Se $S = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k\} \subseteq \mathbb{Z}_q^n$ é uma base de um código linear $C \subseteq \mathbb{Z}_q^n$, então qualquer elemento $\boldsymbol{v} \in C$ pode ser escrito de forma única como uma combinação linear dos elementos de S.*

Exemplo 2.1.1. *O código linear $C = \langle (2,4) \rangle = \{(0,0), (2,4), (4,2)\} \subseteq \mathbb{Z}_6^2$ não possui base, uma vez que todo subconjunto não vazio de C é linearmente dependente.*

Observação 2.1.3. *Quando q é primo, temos que $\mathbb{Z}_q$ é um corpo e um código linear q-ário pode ser visto como um subespaço vetorial de $\mathbb{Z}_q^n$ e, consequentemente, possui uma base com $k \leq n$ vetores. Caso contrário, se q não é primo, podemos apenas garantir a existência de um conjunto minimal de geradores.*

Teorema 2.1.1. *[23] Todo código linear q-ário possui um conjunto minimal de geradores.*

Teorema 2.1.2. *Sejam C_1 e C_2 códigos lineares tais que $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2$. Existem números inteiros $k_1 \geq k_2 \geq 0$ e um conjunto de vetores $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1}\}$ em $\mathbb{Z}_q^n$ tais que*

$$C_1 = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1} \rangle \text{ e } C_2 = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_2} \rangle .$$

Demonstração. Sejam C_1 e C_2 códigos lineares q-ários tais que $C_1 \supseteq C_2$. Pelo Teorema 2.1.1, existem vetores $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_2} \in \mathbb{Z}_q^n$, para algum $k_2 \geq 0$, tais que $C_2 = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_2} \rangle$. Se $C_1 = C_2$, o resultado é imediato. Caso contrário, escolhemos $\boldsymbol{b}_{k_2+1} \in C_1 \setminus C_2$ (é possível fazer tal escolha pois $C_1 \supsetneq C_2$). Se $C_1 = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_2}, \boldsymbol{b}_{k_2+1} \rangle$, obtemos o resultado desejado. Caso contrário, prosseguimos com este processo. Como a cardinalidade de C_1 é finita, após um número finito de passos encontraremos $\boldsymbol{b}_{k_2+1}, \boldsymbol{b}_{k_2+2}, \ldots, \boldsymbol{b}_{k_1} \in \mathbb{Z}_q^n$, para algum $k_1 \geq k_2$, de modo que $C_1 = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1} \rangle$, o que completa a demonstração. □

Observação 2.1.4. *O conjunto $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1}\}$ no Teorema 2.1.2 pode ser vazio. Isto ocorre quando $C_1 = C_2 = \{\mathbf{0}\}$ e $k_1 = k_2 = 0$.*

Observação 2.1.5. *Sejam C_1 e C_2 códigos lineares sobre $\mathbb{Z}_q$ tais que $C_1 \supseteq C_2$. Se q é primo, então existem parâmetros $k_1 \geq k_2 \geq 0$ e $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1} \in \mathbb{Z}_q^n$ tais que $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_2}\}$ e $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1}\}$ são, respectivamente, conjuntos minimais de geradores de C_1 e C_2. Porém, quando q não é primo nem sempre existem parâmentros com estas propriedades (ver Exemplo 2.1.2).*

[1] Em [35] é apresentada a noção de independência modular e uma nova definição de base de um código linear, a qual não é equivalente a definição apresentada neste trabalho.

Exemplo 2.1.2. *Considere a cadeia de códigos lineares* $\mathbb{Z}_4^2 \supseteq C_1 \supseteq C_2$ *tal que*

$$C_1 = \{(0,0),(1,1),(2,2),(3,3)\}$$

e

$$C_2 = \{(0,0),(2,2)\}.$$

Escolhendo $k_1 = 2, k_2 = 1, \boldsymbol{b}_1 = (2,2)$ *e* $\boldsymbol{b}_2 = (1,1)$*, temos que* $C_1 = \langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle$ *e* $C_2 = \langle \boldsymbol{b}_1 \rangle$*. Observe que não existem* $k_1 \geq k_2 \geq 0$ *e* $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1} \in \mathbb{Z}_4^2$ *tais que* $C_2 = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_2} \rangle$ *e* $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1}\}$ *seja um conjunto minimal de geradores de* C_1*.*

Corolário 2.1.1. *Seja* $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ *uma cadeia de códigos lineares. Temos que existem números inteiros* $k_1 \geq k_2 \geq \cdots \geq k_a \geq 0$ *e um conjunto de vetores* $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1}\}$ *em* $\mathbb{Z}_q^n$ *tais que*

$$C_\ell = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_\ell} \rangle \text{ para todo } \ell \in \{1, \ldots, a\}.$$

Demonstração. Segue imediatamente do Teorema 2.1.2. □

Observação 2.1.6. *Seja* $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ *uma cadeia de códigos lineares. Se* q *é primo e a dimensão de* C_ℓ *como espaço vetorial sobre* $\mathbb{Z}_q$ *é* k_ℓ*, sempre existe um conjunto* $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1}\} \subseteq \mathbb{Z}_q^n$ *linearmente independente tal que*

$$C_\ell = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_\ell} \rangle \text{ para todo } \ell \in \{1, \ldots, a\}.$$

2.2 O código dual

Definição 2.2.1. *Para* $\boldsymbol{x} = (x_1, \ldots, x_n)$ *e* $\boldsymbol{y} = (y_1, \ldots, y_n)$ *em* $\mathbb{Z}_q^n$*, o* ***produto interno*** *entre* $\boldsymbol{x}$ *e* $\boldsymbol{y}$ *é definido como* $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = x_1 y_1 + \cdots + x_n y_n$*.*

Teorema 2.2.1. *Seja* C *um código linear* q*-ário de comprimento* n*. O conjunto*

$$C^\perp = \{\boldsymbol{y} \in \mathbb{Z}_q^n;\ \langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0, \forall \boldsymbol{x} \in C\} \tag{2.1}$$

também é um código linear q*-ário de comprimento* n*.*

Demonstração. Observe que $C^\perp \subseteq \mathbb{Z}_q^n$, $\mathbf{0} \in C^\perp$ e dados $\boldsymbol{y}_1, \boldsymbol{y}_2 \in C^\perp$ tem-se $\langle \boldsymbol{x}, \boldsymbol{y}_1 - \boldsymbol{y}_2 \rangle = \langle \boldsymbol{x}, \boldsymbol{y}_1 \rangle - \langle \boldsymbol{x}, \boldsymbol{y}_2 \rangle = 0 - 0 = 0$, para todo $\boldsymbol{x} \in C$. Logo $C^\perp$ é um subgrupo aditivo de $\mathbb{Z}_q^n$. □

Definição 2.2.2. *Seja* C *um código linear* q*-ário. O código linear* q*-ário* $C^\perp$ *definido em (2.1) é chamado* ***código dual*** *de* C*.*

No que segue, a cardinalidade de um conjunto S é representada por $|S|$.

Teorema 2.2.2. *[49] Dado um código linear $C \subseteq \mathbb{Z}_q^n$, temos que $|C||C^\perp| = q^n$.*

Teorema 2.2.3. *Dado um código linear $C \subseteq \mathbb{Z}_q^n$, temos que $(C^\perp)^\perp = C$.*

Demonstração. Aplicando o Teorema 2.2.2 aos códigos C e $C^\perp$, obtemos $|C||C^\perp| = q^n$ e $|C^\perp||(C^\perp)^\perp| = q^n$. Logo $|C| = |(C^\perp)^\perp|$. Por outro lado, temos que $C \subseteq (C^\perp)^\perp$, já que para cada $\boldsymbol{x} \in C$ tem-se $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0, \forall \boldsymbol{y} \in C^\perp$ e logo $\boldsymbol{x} \in (C^\perp)^\perp$. Portanto $(C^\perp)^\perp = C$. □

Definição 2.2.3. *Um código linear $C \subseteq \mathbb{Z}_q^n$ é dito* ***auto-ortogonal*** *se $C \subseteq C^\perp$ e é dito* ***autodual*** *quando $C = C^\perp$.*

Exemplo 2.2.1. *Considere os códigos lineares $C_1 = \{(0,0),(2,2)\} \subseteq \mathbb{Z}_4^2$ e*

$$C_2 = \{(0,0),(1,2),(2,4),(3,1),(4,3)\} \subseteq \mathbb{Z}_5^2.$$

Temos que

$$\begin{aligned} C_1^\perp &= \{(x,y) \in \mathbb{Z}_4^2;\ 2x + 2y = 0\} \\ &= \{(0,0),(0,2),(1,1),(1,3),(2,2),(2,0),(3,3),(3,1)\} \end{aligned}$$

e

$$\begin{aligned} C_2^\perp &= \{(x,y) \in \mathbb{Z}_5^2;\ x + 2y = 0\} \\ &= \{(0,0),(1,2),(2,4),(3,1),(4,3)\}. \end{aligned}$$

Observe que $C_1 \subseteq C_1^\perp$ e $C_2 = C_2^\perp$, isto é, C_1 é auto-ortogonal e C_2 é autodual (em particular, também é auto-ortogonal).

Lema 2.2.1. *Se C_1 e C_2 são códigos lineares q-ários tais que $C_1 \supseteq C_2$, então $C_1^\perp \subseteq C_2^\perp$.*

Demonstração. Seja $\boldsymbol{y} \in C_1^\perp$. Temos que $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0$ para todo $\boldsymbol{x} \in C_1$. Em particular, $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0$ para todo $\boldsymbol{x} \in C_2$, já que $C_1 \supseteq C_2$. Logo $\boldsymbol{y} \in C_2^\perp$. Portanto $C_1^\perp \subseteq C_2^\perp$. □

Teorema 2.2.4. *Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ uma cadeia de códigos lineares. Existem números inteiros $0 \leq r_1 \leq r_2 \leq \cdots \leq r_a$ e um conjunto de vetores $\{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_a}\}$ em $\mathbb{Z}_q^n$ tais que*

$$C_\ell^\perp = \langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_\ell} \rangle \text{ para todo } \ell \in \{1, \ldots, a\}.$$

Demonstração. Dada uma cadeia de códigos lineares $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$, podemos considerar a cadeia de códigos duais associada $\mathbb{Z}_q^n \supseteq C_a^\perp \supseteq C_{a-1}^\perp \supseteq \cdots \supseteq C_1^\perp$ (Lema 2.2.1). O resultado segue do Teorema 2.1.2 aplicado a esta cadeia de códigos duais. □

Observação 2.2.1. *Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ uma cadeia de códigos lineares. Se q é primo e a dimensão de C_ℓ como espaço vetorial sobre $\mathbb{Z}_q$ é k_ℓ, sempre existe um conjunto $\{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_a}\} \subseteq \mathbb{Z}_q^n$ ($r_\ell = n - k_\ell$) linearmente independente tal que*

$$C_\ell^\perp = \langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_\ell} \rangle \text{ para todo } \ell \in \{1, \ldots, a\}.$$

2.3 Matriz geradora

Para cada $k > 0$, I_k denota a matriz identidade de ordem $k \times k$.

Definição 2.3.1. *Seja $C \subseteq \mathbb{Z}_q^n$ um código linear. Uma matriz G cujas linhas formam um conjunto minimal de geradores de C é chamada* ***matriz geradora*** *de C.*

Observação 2.3.1. *A matriz G não é univocamente determinada por C, uma vez que depende da escolha de um conjunto minimal de geradores de C.*

Teorema 2.3.1. *Sejam $C \subseteq \mathbb{Z}_q^n$ um código linear e $G \in \mathbb{Z}_q^{k\times n}$ uma matriz geradora de C, isto é, $C = \{\boldsymbol{u}G;\ \boldsymbol{u} \in \mathbb{Z}_q^k\}$. Temos que $C^\perp = \{\boldsymbol{y} \in \mathbb{Z}_q^n;\ \boldsymbol{y}G^t = \boldsymbol{0}\}$.*

Demonstração. Seja $D = \{\boldsymbol{y} \in \mathbb{Z}_q^n;\ \boldsymbol{y}G^t = \boldsymbol{0}\}$. Para cada $\boldsymbol{y} \in D$,

$$\langle \boldsymbol{u}G, \boldsymbol{y}\rangle = \boldsymbol{y}(\boldsymbol{u}G)^t = (\boldsymbol{y}G^t)\boldsymbol{u}^t = 0, \forall \boldsymbol{u} \in \mathbb{Z}_q^k$$

e logo $\boldsymbol{y} \in C^\perp$. Isto mostra que $D \subseteq C^\perp$. Agora, vamos mostrar que $C^\perp \subseteq D$. Com efeito, dado $\boldsymbol{y} \in \mathbb{Z}_q^n$ tal que $\boldsymbol{y} \notin D$, o vetor $\boldsymbol{y}G^t$ é não nulo. Logo, existe $i \in \{1, \ldots, k\}$ tal que $\langle \boldsymbol{e}_i G, \boldsymbol{y}\rangle = (\boldsymbol{y}G^t)\boldsymbol{e}_i^t \neq 0$. Portanto $\boldsymbol{y} \notin C^\perp$. Isto conclui a demonstração. □

Observação 2.3.2. *Seja $C \subseteq \mathbb{Z}_q^n$ um código linear. Se $G \in \mathbb{Z}_q^{k\times n}$ e $H \in \mathbb{Z}_q^{m\times n}$ são, respectivamente, matrizes geradoras de C e $C^\perp$, então $HG^t = 0$. Além disso, se q é primo, então qualquer matriz geradora de $C^\perp$ é $(n-k) \times n$. Porém, quando q não é primo isto nem sempre é verdade, conforme podemos no Exemplo 2.3.1.*

Exemplo 2.3.1. *Considere novamente o código linear $C = \{(0,0),(2,2)\} \subseteq \mathbb{Z}_4^2$. No Exemplo 2.2.1, vimos que $C^\perp = \{(0,0),(0,2),(1,1),(1,3),(2,2),(2,0),(3,3),(3,1)\}$. Logo*

$$G = \begin{pmatrix} 2 & 2 \end{pmatrix} \text{ e } H = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}$$

são, respectivamente, matrizes geradoras de C e $C^\perp$.

Observação 2.3.3. *Sejam G_1 e G_2 matrizes geradoras de códigos lineares C_1 e C_2, respectivamente. Se G_1 e G_2 são matrizes de mesma ordem e G_2 pode ser obtida de G_1 por uma sequência finita de operações do tipo*

(L1) Permutação de duas linhas

(L2) Multiplicação de uma linha por um escalar inversível em $\mathbb{Z}_q$

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

então $C_1 = C_2$. Além disso, G_1 também pode ser obtida de G_2 por uma sequência finita de operações do tipo $(L1), (L2)$ e $(L3)$.

No que segue, apresentamos resultados referentes às matrizes geradoras de códigos lineares sobre $\mathbb{Z}_{p^a}$, onde os números a e p são inteiros positivos, sendo p primo. Também denotamos por (C1) a operação permutação de duas colunas.

Lema 2.3.1. *Sejam $C \subseteq \mathbb{Z}_{p^a}^n$ um código linear e $G = (\overline{g}_{ij}) \in \mathbb{Z}_{p^a}^{k\times n}$ uma matriz geradora de C. Aplicando uma sequência finita de operações do tipo $(L1), (L2), (L3)$ e $(C1)$ à matriz G, é possível obter uma matriz da forma*

$$\begin{pmatrix} p^s I_\ell & p^s B \\ 0 & p^s D \end{pmatrix},$$

em que $0 \leq s \leq a-1$, $1 \leq \ell \leq k$ e a matriz D de ordem $(k-\ell)\times(n-\ell)$ não possui entradas inversíveis em $\mathbb{Z}_{p^a}$.

Demonstração. Podemos assumir sem perda de generalidade que $0 \leq g_{ij} < p^a$, para $1 \leq i \leq k$ e $1 \leq j \leq n$. Para cada $\overline{g}_{ij} \in \mathbb{Z}_{p^a}$, $\overline{g}_{ij} \neq \overline{0}$, existem números inteiros k_{ij} e a_{ij} univocamente determinados tais que $0 \leq k_{ij} < a$, $0 < a_{ij} < p^{a-k_{ij}}$, $\overline{g}_{ij} = p^{k_{ij}}\overline{a}_{ij}$ e $\mathrm{mdc}(p, a_{ij}) = 1$. Note que cada $\overline{a}_{ij}$ é inversível em $\mathbb{Z}_{p^a}$. Seja

$$s = \min_{\substack{1\leq i\leq k\\ 1\leq j\leq n}} \left\{k_{ij};\ \overline{g}_{ij} \neq \overline{0}, \overline{g}_{ij} = p^{k_{ij}}\overline{a}_{ij} \text{ e } \mathrm{mdc}(p, a_{ij}) = 1\right\}.$$

Assim, para cada para (i, j) satisfazendo $1 \leq i \leq k$ e $1 \leq j \leq n$, podemos escolher $\overline{b}_{ij}$ tal que $0 \leq b_{ij} < p^{a-s}$ e $\overline{g}_{ij} = p^s\overline{b}_{ij}$. Ou seja,

$$G = p^s \begin{pmatrix} \overline{b}_{11} & \overline{b}_{12} & \cdots & \overline{b}_{1n} \\ \overline{b}_{21} & \overline{b}_{22} & \cdots & \overline{b}_{2n} \\ \vdots & \vdots & & \vdots \\ \overline{b}_{k1} & \overline{b}_{k2} & \cdots & \overline{b}_{kn} \end{pmatrix}.$$

Por construção, alguma entrada $\overline{b}_{ij}$ é inversível em $\mathbb{Z}_{p^a}$. Assim, por meio de (L1) e (C1), podemos supor sem perda de generalidade que $\overline{b}_{11}$ é inversível em $\mathbb{Z}_{p^a}$. Agora, multiplicando a primeira linha por $\overline{b}_{11}^{-1}$ (operação (L2)) e, para cada $i \in \{2, \ldots, k\}$, adicionando à i-ésima linha a primeira linha multiplicada por $-\overline{b}_{i1}\overline{b}_{11}^{-1}$ (operações do tipo (L3)), obtemos uma matriz da forma

$$G_1 = p^s \begin{pmatrix} \overline{1} & \overline{c}_{12} & \cdots & \overline{c}_{1n} \\ \overline{0} & \overline{c}_{22} & \cdots & \overline{c}_{2n} \\ \vdots & \vdots & & \vdots \\ \overline{0} & \overline{c}_{k2} & \cdots & \overline{c}_{kn} \end{pmatrix}.$$

Se todas as entradas $\overline{c}_{ij}$ com $2 \leq i \leq m$ e $2 \leq j \leq n$ não são inversíveis em $\mathbb{Z}_{p^a}$, encontramos o resultado desejado. Caso contrário, por meio de (L1) e (C1), podemos supor sem perda de generalidade que $\overline{c}_{22}$ é inversível em $\mathbb{Z}_{p^a}$. Assim, multiplicando a

segunda linha de G_1 por $\overline{c}_{22}^{-1}$ (operação (L2)) e, para cada $i \in \{1\} \cup \{3, \ldots, k\}$, adicionando à i-ésima linha a segunda linha multiplicada por $-\overline{c}_{i2}\overline{c}_{22}^{-1}$ (operação (L3)), obtemos uma nova matriz da forma

$$G_2 = p^s \begin{pmatrix} \overline{1} & \overline{0} & \overline{d}_{13} & \cdots & \overline{d}_{1n} \\ \overline{0} & \overline{1} & \overline{d}_{23} & \cdots & \overline{d}_{2n} \\ \overline{0} & \overline{0} & \overline{d}_{33} & \cdots & \overline{d}_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ \overline{0} & \overline{0} & \overline{d}_{k3} & \cdots & \overline{d}_{kn} \end{pmatrix}.$$

Se todas as entradas $\overline{d}_{ij}$ com $3 \leq i \leq m$ e $3 \leq j \leq n$ não são inversíveis em $\mathbb{Z}_{p^a}$, encontramos o resultado desejado. Caso contrário, continuamos este processo até encontrarmos uma matriz da forma

$$p^s \begin{pmatrix} I_\ell & B \\ 0 & D \end{pmatrix},$$

em que $0 \leq s \leq a-1$, $1 \leq \ell \leq k$ e a matriz D é $(k-\ell) \times (n-\ell)$ e não possui entradas inversíveis em $\mathbb{Z}_{p^a}$. □

Teorema 2.3.2. *Todo código linear sobre $\mathbb{Z}_{p^a}$ de comprimento n, a menos de uma permutação de colunas, possui uma matriz geradora da forma*

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,a-1} & A_{0,a} \\ 0 & pI_{k_1} & pA_{1,2} & pA_{1,3} & \cdots & pA_{1,a-1} & pA_{1,a} \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{2,3} & \cdots & p^2 A_{2,a-1} & p^2 A_{2,a} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & p^{a-1} I_{k_{a-1}} & p^{a-1} A_{a-1,a} \end{pmatrix}. \tag{2.2}$$

As colunas de G estão agrupadas em blocos de tamanhos $k_0, k_1, \ldots, k_{a-1}$ e $k_a = n - \sum_{i=0}^{a-1} k_i$, com $k_i \geq 0$ para todo $i \in \{0, 1, \ldots, a\}$.

Demonstração. Seja $G \in \mathbb{Z}_{p^a}^{k \times n}$ uma matriz geradora de C. Aplicando uma sequência conveniente de operações do tipo (L1), (L2), (L3) e (C1) a esta matriz, obtemos uma matriz da forma

$$\begin{pmatrix} p^{s_1} I_{k_{s_1}} & p^{s_1} B_1 \\ 0 & p^{s_1} D_1 \end{pmatrix},$$

em que $0 \leq s_1 \leq a-1$ e a matriz D_1 é $(k-k_{s_1}) \times (n-k_{s_1})$ e não possui entradas inversíveis em $\mathbb{Z}_{p^a}$ (Lema 2.3.1). Se $k_{s_1} = k$, encontramos o resultado desejado. Caso contrário, aplicando uma sequência conveniente de operações do tipo (L1), (L2), (L3) e (C1) a esta nova matriz, obtemos uma matriz da forma

$$\begin{pmatrix} p^{s_1} I_{k_{s_1}} & p^{s_1} A_{s_1,s_2} & p^{s_1} \tilde{B}_1 \\ 0 & p^{s_2} I_{k_{s_2}} & p^{s_2} B_2 \\ 0 & 0 & p^{s_2} D_2 \end{pmatrix}$$

em que $0 \leq s_1 < s_2 \leq a-1$ e a matriz D_2 é $(k-k_{s_1}-k_{s_2}) \times (n-k_{s_1}-k_{s_2})$ e não possui entradas inversíveis em $\mathbb{Z}_{p^a}$ (Lema 2.3.1). Se $k_{s_1}+k_{s_2}=k$, encontramos o resultado desejado. Caso contrário, continuamos com este processo até obtermos uma matriz da forma

$$\begin{pmatrix} p^{s_1}I_{k_{s_1}} & p^{s_1}A_{s_1,s_2} & p^{s_1}A_{s_1,s_3} & \cdots & p^{s_1}A_{s_1,s_r} & p^{s_1}A_{s_1,a} \\ 0 & p^{s_2}I_{k_{s_2}} & p^{s_2}A_{s_2,s_3} & \cdots & p^{s_2}A_{s_2,s_r} & p^{s_2}A_{s_2,a} \\ 0 & 0 & p^{s_3}I_{k_{s_3}} & \cdots & p^{s_3}A_{s_3,s_r} & p^{s_3}A_{s_3,a} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & p^{s_r}I_{k_{s_r}} & p^{s_r}A_{s_r,a} \end{pmatrix},$$

em que $0 \leq s_1 < s_2 < \cdots < s_r \leq a-1$ e $k_{s_1}+k_{s_2}+\cdots+k_{s_r}=k$. □

Definição 2.3.2. *Dizemos que uma matriz geradora G de um código linear $C \subseteq \mathbb{Z}_{p^a}^n$ está na **forma padrão** quando G está na forma (2.2).*

Observação 2.3.4. *Um código linear $C \subseteq \mathbb{Z}_{p^a}^n$ pode ter mais do que uma matriz geradora na forma padrão. Por exemplo,*

$$G_1 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \text{ e } G_2 = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$$

são matrizes geradoras na forma padrão do código linear 4-ário

$$C = \{(0,0),(1,0),(2,0),(3,0),(0,2),(1,2),(2,2),(3,2)\}.$$

Teorema 2.3.3. *[35] Seja $C \subseteq \mathbb{Z}_{p^a}^n$ um código linear. Os parâmetros $k_0, k_1, \ldots, k_a$ são os mesmos qualquer que seja a matriz geradora de C na forma padrão.*

Teorema 2.3.4. *Seja $G \in \mathbb{Z}_{p^a}^{k\times n}$ uma matriz geradora de um código linear $C \subseteq \mathbb{Z}_{p^a}^n$ na forma (2.2). Qualquer $\boldsymbol{v} \in C$ pode ser escrito de forma única como $\boldsymbol{v} = (\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{a-1})G$, com $\boldsymbol{v}_i \in (\mathbb{Z}_{p^a}/p^{a-i}\mathbb{Z}_{p^a})^{k_i} \cong (p^i\mathbb{Z}_{p^a})^{k_i}$. Além disso, o número de elementos C é dado por*

$$|C| = p^{\sum_{i=0}^{a-1}(a-i)k_i}.$$

Demonstração. Seja $\phi : \mathbb{Z}_{p^a}^k \to \mathbb{Z}_{p^a}^n$ o homomorfismo de grupos dado por $\phi(\boldsymbol{v}) = \boldsymbol{v}G$. É imediato que $\phi(\mathbb{Z}_{p^a}^k) = C$. Por outro lado, dado $\boldsymbol{v} \in \mathbb{Z}_{p^a}^k$ podemos escrever $\boldsymbol{v} = (\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{a-1})$ com $\boldsymbol{v}_i \in \mathbb{Z}_{p^a}^{k_i}$. Dessa forma,

$$
\phi(\boldsymbol{v}) = \mathbf{0} \iff \begin{cases} \boldsymbol{v}_0 = \mathbf{0} \\ \boldsymbol{v}_0 A_{0,1} + p\boldsymbol{v}_1 = \mathbf{0} \\ \boldsymbol{v}_0 A_{0,2} + p\boldsymbol{v}_1 A_{1,2} + p^2\boldsymbol{v}_2 = \mathbf{0} \\ \vdots \\ \boldsymbol{v}_0 A_{0,a-1} + p\boldsymbol{v}_1 A_{1,a-1} + p^2\boldsymbol{v}_2 A_{2,a-1} + \cdots + p^{a-1}\boldsymbol{v}_{a-1} = \mathbf{0} \\ \boldsymbol{v}_0 A_{0,a} + p\boldsymbol{v}_1 A_{1,a} + p^2\boldsymbol{v}_2 A_{2,a} + \cdots + p^{a-1}\boldsymbol{v}_{a-1} A_{a-1,a} = \mathbf{0} \end{cases}
$$

$$
\iff \begin{cases} \boldsymbol{v}_0 = \mathbf{0} \\ p\boldsymbol{v}_1 = \mathbf{0} \\ p^2\boldsymbol{v}_2 = \mathbf{0} \\ \vdots \\ p^{a-1}\boldsymbol{v}_{a-1} = \mathbf{0} \end{cases}
$$

$$
\iff \begin{cases} \boldsymbol{v}_0 \in p^a\mathbb{Z}_{p^a}^{k_0} \\ \boldsymbol{v}_1 \in p^{a-1}\mathbb{Z}_{p^a}^{k_1} \\ \boldsymbol{v}_2 \in p^{a-2}\mathbb{Z}_{p^a}^{k_2} \\ \vdots \\ \boldsymbol{v}_{a-1} \in p\mathbb{Z}_{p^a}^{k_{a-1}}. \end{cases}
$$

Logo

$$
\ker(\phi) = \left(p^a\mathbb{Z}_{p^a}\right)^{k_0} \times \left(p^{a-1}\mathbb{Z}_{p^a}\right)^{k_1} \times \cdots \times \left(p\mathbb{Z}_{p^a}\right)^{k_{a-1}}.
$$

Portanto

$$
\begin{aligned}
C \cong \mathbb{Z}_{p^a}^k / \ker(\phi) &\cong \left(\mathbb{Z}_{p^a}^{k_0} \times \mathbb{Z}_{p^a}^{k_1} \times \cdots \times \mathbb{Z}_{p^a}^{k_{a-1}}\right) / \left(p^a\mathbb{Z}_{p^a}^{k_0} \times p^{a-1}\mathbb{Z}_{p^a}^{k_1} \times \cdots \times p\mathbb{Z}_{p^a}^{k_{a-1}}\right) \\
&\cong \left(\mathbb{Z}_{p^a}/p^a\mathbb{Z}_{p^a}\right)^{k_0} \times \left(\mathbb{Z}_{p^a}/p^{a-1}\mathbb{Z}_{p^a}\right)^{k_1} \times \cdots \times \left(\mathbb{Z}_{p^a}/p\mathbb{Z}_{p^a}\right)^{k_{a-1}} \\
&\cong \left(\mathbb{Z}_{p^a}\right)^{k_0} \times \left(p\mathbb{Z}_{p^a}\right)^{k_1} \times \cdots \times \left(p^{a-1}\mathbb{Z}_{p^a}\right)^{k_{a-1}}.
\end{aligned}
$$

Das considerações acima, obtemos que qualquer elemento $\boldsymbol{v}$ de C pode ser escrito de forma única como $\boldsymbol{v} = (\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{a-1})G$ com $\boldsymbol{v}_i \in (\mathbb{Z}_{p^a}/p^{a-i}\mathbb{Z}_{p^a})^{k_i} \cong (p^i\mathbb{Z}_{p^a})^{k_i}$ e, consequentemente, o número de elementos C é dado por $|C| = (p^a)^{k_0}(p^{a-1})^{k_1}\cdots(p)^{k_{a-1}} = p^{\sum_{i=0}^{a-1}(a-i)k_i}$. □

Definição 2.3.3. *Um código linear $C \subseteq \mathbb{Z}_{p^a}^n$ que a menos de uma permutação de colunas possui uma matriz geradora da forma (2.2) é dito do tipo*

$$
(1)^{k_0}(p)^{k_1}\cdots(p^{a-2})^{k_{a-2}}(p^{a-1})^{k_{a-1}}.
$$

Corolário 2.3.1. *[21] Todo código linear sobre $\mathbb{Z}_p$ de comprimento n, a menos de uma permutação de colunas, possui uma matriz geradora da seguinte forma $G = (I_k \mid A)$, em*

que A é uma matriz $k \times (n-k)$.

O próximo teorema fornece uma matriz geradora do código dual $C^{\perp}$ a partir de uma matriz geradora de C na forma (2.2).

Teorema 2.3.5. *Seja $C \subseteq \mathbb{Z}_{p^a}^n$ um código linear com matriz geradora G da forma (2.2). Para cada par (i,j) satisfazendo $0 \leq i < j \leq a$, seja*

$$B_{i,j} = -\sum_{k=i+1}^{j-1} B_{i,k} A_{a-j,a-k}^t - A_{a-j,a-i}^t.$$

Então, uma matriz geradora do código dual de C é dada por

$$H = \begin{pmatrix} B_{0,a} & B_{0,a-1} & \cdots & B_{0,3} & B_{0,2} & B_{0,1} & I_{k_a} \\ pB_{1,a} & pB_{1,a-1} & \cdots & pB_{1,3} & pB_{1,2} & pI_{k_{a-1}} & 0 \\ p^2B_{2,a} & p^2B_{2,a-1} & \cdots & p^2B_{2,3} & p^2I_{k_{a-2}} & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ p^{a-1}B_{a-1,a} & p^{a-1}I_{k_1} & \cdots & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{2.3}$$

As colunas de H estão agrupadas em blocos de tamanhos $k_0, k_1, \ldots, k_{a-1}$ e $k_a = n - \sum_{i=0}^{a-1} k_i$, com $k_i \geq 0$ para todo $i \in \{0,1,\ldots,a\}$.

Demonstração. Seja $D \subseteq \mathbb{Z}_{p^a}^n$ o código linear gerado por H. Escreva

$$G = \begin{pmatrix} G_0 \\ G_1 \\ G_2 \\ \vdots \\ G_{a-1} \end{pmatrix} \text{ e } H = \begin{pmatrix} H_0 \\ H_1 \\ H_2 \\ \vdots \\ H_{a-1} \end{pmatrix},$$

de modo que G_i e H_i sejam matrizes $k_i \times n$ e $k_{a-i} \times n$, respectivamente. Temos que

$$GH^t = \begin{pmatrix} G_0H_0^t & G_0H_1^t & \cdots & G_0H_{a-1}^t \\ G_1H_0^t & G_1H_1^t & \cdots & G_1H_{a-1}^t \\ \vdots & \vdots & & \vdots \\ G_{a-1}H_0^t & G_{a-1}H_1^t & \cdots & G_{a-1}H_{a-1}^t \end{pmatrix}.$$

É imediato que $G_jH_i^t = 0$ sempre que $i + j \geq a$, pois neste caso todas as entradas de $G_jH_i^t$ são múltiplas de p^a. Por outro lado, para $i, j \in \{0,1,\ldots,a-1\}$ tal que $i + j < a$

tem-se

$$\begin{aligned} G_j H_i^t &= p^{i+j}\left(I_{k_j} B_{i,a-j}^t + A_{j,j+1} B_{i,a-j-1}^t + \cdots + A_{j,a-i-1} B_{j,j+1}^t + A_{j,a-i} I_{k_{a-i}}\right) \\ &= p^{i+j}\left(B_{i,a-j}^t + \sum_{k=i+1}^{a-j-1} A_{j,a-k} B_{i,k}^t + A_{j,a-i}\right) = 0, \end{aligned}$$

uma vez que

$$B_{i,a-j} = -\sum_{k=i+1}^{a-j-1} B_{i,k} A_{j,a-k}^t - A_{j,a-i}^t.$$

Logo $GH^t = 0$. Isto mostra que $D \subseteq C^\perp$. Para concluir a demonstração, basta mostrar que $|D| = |C^\perp|$. Do Teorema 2.3.4, obtemos

$$|D| = (p^a)^{k_a}(p^{a-1})^{k_{a-1}} \cdots (p^2)^{k_2}(p)^{k_1} = p^{\sum_{i=1}^{a} i k_i}$$

e

$$|C| = (p^a)^{k_0}(p^{a-1})^{k_1} \cdots (p)^{k_{a-1}} = p^{\sum_{i=0}^{a-1} (a-i) k_i}.$$

Consequentemente

$$|C||D| = \left(p^{\sum_{i=0}^{a-1} (a-i) k_i}\right)\left(p^{\sum_{i=1}^{a} i k_i}\right) = p^{an}.$$

Isto mostra que $|D| = |C^\perp|$, uma vez que $|C||C^\perp| = p^{an}$ (Teorema 2.2.2). □

Corolário 2.3.2. *Sejam $C \subseteq \mathbb{Z}_{p^a}^n$ um código linear do tipo*

$$(1)^{k_0}(p)^{k_1} \cdots (p^{a-2})^{k_{a-2}}(p^{a-1})^{k_{a-1}}$$

e $k_a = n - \sum_{i=0}^{a-1} k_i$. O código linear $C^\perp$ é do tipo $(1)^{k_a}(p)^{k_{a-1}} \cdots (p^{a-2})^{k_2}(p^{a-1})^{k_1}$ e seu número de elementos é dado por

$$|C^\perp| = (p^a)^{k_a}(p^{a-1})^{k_{a-1}} \cdots (p^2)^{k_2}(p)^{k_1} = p^{\sum_{i=1}^{a} i k_i}.$$

Demonstração. Segue imediatamente dos Teoremas 2.3.4 e 2.3.5. □

Corolário 2.3.3. *[21] Se $C \subseteq \mathbb{Z}_p^n$ é um código linear com matriz geradora $G = (I_k \mid A)$, então $H = (A^t \mid I_{n-k})$ é uma matriz geradora de $C^\perp$.*

Em [35] é apresentado o conceito de matrizes geradoras na forma padrão para códigos lineares sobre $\mathbb{Z}_q$, $q \in \mathbb{N}$, generalizando vários resultados mencionados aqui.

2.4 Distâncias em $\mathbb{Z}_q^n$

Nesta seção, apresentamos as distâncias de Hamming e de Lee que foram definidas respectivamente em 1950 [18] e 1957/1958 [27, 48] e têm sido muito estudadas desde que

foram introduzidas.

2.4.1 Distância de Hamming

A distância de Hamming entre dois elementos $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_q^n$ é simplesmente o número de coordenadas distintas entre os mesmos.

Definição 2.4.1. *Dados dois elementos $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_q^n$, a **distância de Hamming** entre $\boldsymbol{x}$ e $\boldsymbol{y}$ é definida como*

$$d_H(\boldsymbol{x}, \boldsymbol{y}) = |\{i;\ x_i \neq y_i, 1 \leq i \leq n\}|.$$

Definição 2.4.2. *Seja $C \subseteq \mathbb{Z}_q^n$ um código linear não nulo. A **distância de Hamming mínima** de C é definida como*

$$d_H(C) = \min\{d_H(\boldsymbol{x}, \boldsymbol{y});\ \boldsymbol{x}, \boldsymbol{y} \in C \text{ e } \boldsymbol{x} \neq \boldsymbol{y}\},$$

ou equivalentemente, $d_H(C) = \min\left\{d_H(\boldsymbol{z}, \boldsymbol{0});\ \boldsymbol{z} \in C \setminus \{\boldsymbol{0}\}\right\}$.

No próximo teorema, o símbolo $\lceil x \rceil$ denota o menor inteiro maior ou igual a x.

Teorema 2.4.1. *(Cota de Singleton) Seja $C \subseteq \mathbb{Z}_q^n$ um código linear não nulo. Temos que*

$$d_H(C) \leq n - \lceil \log_q |C| \rceil + 1.$$

Demonstração. Seja $\phi : C \to \mathbb{Z}_q^n$ o homomorfismo de grupos dado por

$$\phi(x_1, \ldots, x_n) = (x_1, \ldots, x_{n-d_H(C)+1}, \underbrace{0, 0, \ldots, 0}_{d_H(C)-1}).$$

Pode-se ver facilmente que ϕ é injetor (e logo $|C| = |\phi(C)|$) e $|\phi(C)| \leq q^{n-d_H(C)+1}$. Portanto $|C| \leq q^{n-d_H(C)+1}$. Aplicando a função logarítmica de base q (que é crescente, já que $q \geq 2$) em ambos os lados da desigualdade $|C| \leq q^{n-d_H(C)+1}$, obtemos $\log_q |C| \leq n - d_H(C) + 1$ e consequentemente $\lceil \log_q |C| \rceil \leq n - d_H(C) + 1$, já que $n - d_H(C) + 1$ é inteiro. Portanto $d_H(C) \leq n - \lceil \log_q |C| \rceil + 1$. □

Definição 2.4.3. *Um código linear $C \subseteq \mathbb{Z}_q^n$ é dito **MDS** (Maximum Distance Separable) se $d_H(C) = n - \lceil \log_q |C| \rceil + 1$.*

Exemplo 2.4.1. *O código linear $C = \{(0,0), (2,2)\} \subseteq \mathbb{Z}_4^2$ é MDS. De fato, observe que $d_H(C) = 2$, $n = 2$ e $\lceil \log_4 |C| \rceil = \lceil \log_4 2 \rceil = \lceil 1/2 \rceil = 1$. Logo $d_H(C) = n - \lceil \log_q |C| \rceil + 1$.*

2.4.2 Distância de Lee

Definição 2.4.4. *Dados dois elementos* $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_q^n$, *a* ***distância de Lee*** *entre* $\boldsymbol{x}$ *e* $\boldsymbol{y}$ *é definida como*

$$d_{Lee}(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{n} \min\{\sigma(x_i - y_i), q - \sigma(x_i - y_i)\},$$

sendo $\sigma : \mathbb{Z}_q \to \mathbb{Z}$ *a inclusão natural (isto é,* $\sigma(\overline{x})$ *é o resto da divisão de* x *por* q*).*

Observação 2.4.1. *Quando* $q = 2$ *ou* $q = 3$, *as distâncias de Hamming e de Lee são idênticas, isto é,* $d_h(\boldsymbol{x}, \boldsymbol{y}) = d_{Lee}(\boldsymbol{x}, \boldsymbol{y}), \forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_q^n$. *Porém, se* $q > 3$ *a distância de Lee de* $\boldsymbol{x}$ *a* $\boldsymbol{y}$ *é sempre maior ou igual à de Hamming de* $\boldsymbol{x}$ *a* $\boldsymbol{y}$.

Observação 2.4.2. *A distância de Lee foi introduzida em [27,48] na abordagem da transmissão de sinais em determinados canais com ruído. Recentes aplicações na área de comunicações podem ser encontradas em [13] e suas referências.*

Definição 2.4.5. *Seja* $C \subseteq \mathbb{Z}_q^n$ *um código linear não nulo. A* ***distância de Lee mínima*** *de* C *é definida como*

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

Observação 2.4.3. *A distância de Lee é invariante por translações, isto é,*

$$d_{Lee}(\boldsymbol{x}, \boldsymbol{y}) = d_{Lee}(\boldsymbol{x} + \boldsymbol{z}, \boldsymbol{y} + \boldsymbol{z}), \forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \mathbb{Z}_q^n.$$

De fato, para quaisquer $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_n)$ *e* $\boldsymbol{z} = (z_1, \ldots, z_n)$ *em* $\mathbb{Z}_q^n$,

$$\begin{aligned} d_{Lee}(\boldsymbol{x} + \boldsymbol{z}, \boldsymbol{y} + \boldsymbol{z}) &= \sum_{i=1}^{n} \min\left\{\sigma\big((x_i + z_i) - (y_i + z_i)\big), q - \sigma\big((x_i + z_i) - (y_i + z_i)\big)\right\} \\ &= \sum_{i=1}^{n} \min\left\{\sigma\big(x_i - y_i\big), q - \sigma\big(x_i - y_i\big)\right\} \\ &= d_{Lee}(\boldsymbol{x}, \boldsymbol{y}). \end{aligned}$$

Teorema 2.4.2. *Seja* $C \subseteq \mathbb{Z}_q^n$ *um código linear não nulo. Temos que*

$$d_{Lee}(C) = \min\left\{d_{Lee}(\boldsymbol{z}, \boldsymbol{0});\ \boldsymbol{z} \in C \setminus \{\boldsymbol{0}\}\right\}.$$

Demonstração. Sejam $\boldsymbol{x}, \boldsymbol{y} \in C$, $\boldsymbol{x} \neq \boldsymbol{y}$, tais que $d_{Lee}(C) = d_{Lee}(\boldsymbol{x}, \boldsymbol{y})$. Temos que

$$d_{Lee}(C) = d_{Lee}(\boldsymbol{x}, \boldsymbol{y}) = d_{Lee}(\boldsymbol{x} - \boldsymbol{y}, \boldsymbol{0}) \geq \min\left\{d_{Lee}(\boldsymbol{z}, \boldsymbol{0});\ \boldsymbol{z} \in C \setminus \{\boldsymbol{0}\}\right\},$$

já que $\boldsymbol{x} - \boldsymbol{y} \in C \setminus \{\mathbf{0}\}$. Por outro lado, $d_{Lee}(\boldsymbol{z}, \mathbf{0}) \geq d_{Lee}(C), \forall \boldsymbol{z} \in C \setminus \{\mathbf{0}\}$, e logo $\min\{d_{Lee}(\boldsymbol{z}, \mathbf{0});\ \boldsymbol{z} \in C \setminus \{\mathbf{0}\}\} \geq d_{Lee}(C)$. Isto conclui a demonstração. □

Teorema 2.4.3. *Seja $C \subseteq \mathbb{Z}_q^n$ um código linear não nulo. Temos que*

$$d_{Lee}(C) \leq \left\lfloor \frac{q}{2} \right\rfloor \big(n - \lceil \log_q |C| \rceil + 1\big).$$

Demonstração. Para cada $\boldsymbol{z} \in \mathbb{Z}_q^n$,

$$d_{Lee}(\boldsymbol{z}, \mathbf{0}) = \sum_{i=1}^{n} d_{Lee}(z_i, 0) \leq \left\lfloor \frac{q}{2} \right\rfloor d_H(\boldsymbol{z}, \mathbf{0}),$$

já que $d_{Lee}(z_i, 0) = 0$ se $z_i = 0$ e $d_{Lee}(z_i, 0) \leq \lfloor q/2 \rfloor$ se $z_i \neq 0$. Logo

$$d_{Lee}(C) \leq \left\lfloor \frac{q}{2} \right\rfloor d_H(C).$$

Para concluir a demonstração, basta aplicar o Teorema 2.4.1. □

Definição 2.4.6. *Um código linear $C \subseteq \mathbb{Z}_q^n$ é dito **MLDS** (Maximum Lee Distance Separable) se $d_{Lee}(C) = \lfloor q/2 \rfloor (n - \lceil \log_q |C| \rceil + 1)$.*

Exemplo 2.4.2. *O código linear $C = \{(0,0), (2,2)\} \subseteq \mathbb{Z}_4^2$ é MLDS. De fato, observe que $d_{Lee}(C) = 4$, $q = 4$, $n = 2$ e $\lceil \log_4 |C| \rceil = \lceil \log_4 2 \rceil = \lceil 1/2 \rceil = 1$. Logo $d_{Lee}(C) = \lfloor q/2 \rfloor (n - \lceil \log_q |C| \rceil + 1)$.*

Capítulo 3

Reticulados obtidos a partir de códigos lineares

Neste capítulo, abordamos construções de reticulados a partir de códigos. Na Seção 3.1, estudamos a Construção A para códigos lineares q-ários e mostramos que o reticulado tridimensional de maior densidade na métrica da soma pode ser obtido via Construção A. Na Seção 3.2.1, propomos a Construção D para códigos lineares q-ários e estendemos vários resultados de códigos binários para códigos q-ários. As Construções D$'$ e $\overline{\mathrm{D}}$ para códigos q-ários são apresentadas nas Seções 3.2.2 e 3.2.3, respectivamente. Na Seção 3.2.4 são apresentadas algumas conexões entre as construções supracitadas. Também, definimos a adição zero-um em $\mathbb{Z}_q^n$ e mostramos que a Construção $\overline{\mathrm{D}}$ produz um reticulado se, e somente se, a cadeia de códigos utilizada é fechada sob esta adição. Fórmulas e limitantes para a distância da soma mínima de reticulados obtidos via Construções D, D$'$ e $\overline{\mathrm{D}}$ são apresentados na Seção 3.2.5. Na Seção 3.3 introduzimos a Construção A$'$ para códigos lineares sobre o anel quociente $\mathbb{Z}_q[X]/(X^a)$.

Os resultados deste capítulo incluem os apresentados em [41, 42], os quais possuem versões preliminares [43, 44].

No decorrer deste capítulo, utilizamos frequentemente a inclusão natural $\sigma : \mathbb{Z}_q \to \mathbb{Z}$ (isto é, $\sigma(\overline{x})$ é o resto da divisão de x por q), o homomorfismo de anéis $\overline{\sigma} : \mathbb{Z} \to \mathbb{Z}_q$ dado por $\overline{\sigma}(x) = \overline{x}$ e suas extensões $\sigma : \mathbb{Z}_q^n \to \mathbb{Z}^n$ e $\overline{\sigma} : \mathbb{Z}^n \to \mathbb{Z}_q^n$.

3.1 Construção A

Existem várias maneiras de se obter reticulados a partir de códigos lineares q-ários, uma das mais conhecidas é a chamada Construção A, que abordamos nesta seção.

Definição 3.1.1. *(**Construção A**) Dado um código linear $C \subseteq \mathbb{Z}_q^n$, definimos o conjunto $\Lambda_A(C)$ da seguinte forma*

$$\Lambda_A(C) = q\mathbb{Z}^n + \sigma(C).$$

Teorema 3.1.1. *$C \subseteq \mathbb{Z}_q^n$ é um código linear se, e somente se, $\Lambda_A(C) \subseteq \mathbb{Z}^n$ é um reticulado em $\mathbb{R}^n$.*

Demonstração. ($\Rightarrow$) Seja $C \subseteq \mathbb{Z}_q^n$ um código linear. Como $\Lambda_A(C) \subseteq \mathbb{Z}^n$ é um conjunto discreto, basta mostrar que $\Lambda_A(C)$ é um subgrupo aditivo de $\mathbb{R}^n$. Com efeito, $\mathbf{0} \in \Lambda_A(C)$ e dados $\boldsymbol{w}_1, \boldsymbol{w}_2 \in \Lambda_A(C)$ existem $\boldsymbol{z}_1, \boldsymbol{z}_2 \in \mathbb{Z}^n$ e $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C$ tais que $\boldsymbol{w}_1 = q\boldsymbol{z}_1 + \sigma(\boldsymbol{c}_1)$ e $\boldsymbol{w}_2 = q\boldsymbol{z}_2 + \sigma(\boldsymbol{c}_2)$, logo $\boldsymbol{w}_1 - \boldsymbol{w}_2 = q(\boldsymbol{z}_1 - \boldsymbol{z}_2) + \sigma(\boldsymbol{c}_1) - \sigma(\boldsymbol{c}_2)$. Aplicando o algoritmo da divisão, obtemos $\boldsymbol{m} \in \mathbb{Z}^n$ e $\boldsymbol{r} \in \mathbb{Z}^n$ tais que $\boldsymbol{r} \in [0, q)^n$ e $\sigma(\boldsymbol{c}_1) - \sigma(\boldsymbol{c}_2) = \boldsymbol{m}q + \boldsymbol{r}$. Assim, temos que $\boldsymbol{w}_1 - \boldsymbol{w}_2 = q(\boldsymbol{z}_1 - \boldsymbol{z}_2 + \boldsymbol{m}) + \boldsymbol{r}$, com $\boldsymbol{r} = \sigma(\overline{\sigma}(\boldsymbol{r}))$ e $\overline{\sigma}(\boldsymbol{r}) = \boldsymbol{c}_1 - \boldsymbol{c}_2 \in C$. Portanto $\boldsymbol{w}_1 - \boldsymbol{w}_2 \in q\mathbb{Z}^n + \sigma(C) = \Lambda_A(C)$. ($\Leftarrow$) Seja $C \subseteq \mathbb{Z}_q^n$ e suponha que $\Lambda_A(C) = q\mathbb{Z}^n + \sigma(C)$ é um reticulado em $\mathbb{R}^n$. Observe que $C = \overline{\sigma}(\Lambda_A(C))$, $\Lambda_A(C)$ é um subgrupo aditivo de $\mathbb{Z}^n$ e $\overline{\sigma} : \mathbb{Z}^n \to \mathbb{Z}_q^n$ é um homomorfismo de grupos. Logo C é um subgrupo aditivo de $\mathbb{Z}_q^n$, ou seja, $C \subseteq \mathbb{Z}_q^n$ é um código linear. □

Definição 3.1.2. *Um reticulado que pode ser obtido via Construção A a partir de um código linear $C \subseteq \mathbb{Z}_q^n$ é chamado de* ***reticulado q-ário****.*

Um reticulado q-ário $\Lambda_A(C) \subseteq \mathbb{R}^n$ sempre contém $q\mathbb{Z}^n$ e portanto possui posto completo. Também vale a "recíproca", isto é, se um reticulado $\Lambda \subseteq \mathbb{Z}^n$ contém $q\mathbb{Z}^n$, então Λ pode ser obtido via Construção A a partir de algum código q-ário de comprimento n.

Exemplo 3.1.1. *Na Figura 3.1, ilustramos o reticulado 6-ário obtido via Construção A a partir do código linear*

$$C = \{(0,0), (1,2), (2,4), (3,0), (4,2), (5,4)\} \subseteq \mathbb{Z}_6^2.$$

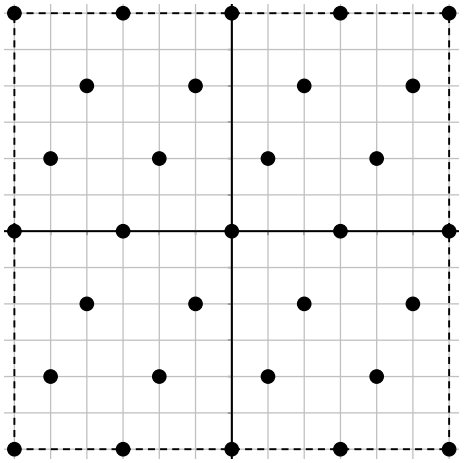


Figura 3.1: $\Lambda_A(C) \cap [-6, 6]^2$

O próximo resultado é apresentado em [40] e uma demonstração alternativa pode ser encontrada em [23, Proposição 3.2.7]. Trata-se de um caso particular do Corolário 3.2.10, por isso omitimos sua demonstração.

Teorema 3.1.2. *Seja $\{\mathbf{0}\} \neq C \subseteq \mathbb{Z}_q^n$ um código linear. Se $d_{Lee}(C)$ denota a distância de Lee mínima do código C, então a distância mínima em relação à métrica da soma do reticulado $\Lambda_A(C)$ é dada por*

$$d_{\min}^1\big(\Lambda_A(C)\big) = \min\big\{q, d_{Lee}(C)\big\}.$$

Exemplo 3.1.2. *Considere o código linear*

$$C = \langle (1, 36, 3), (0, 37, 7) \rangle \subseteq \mathbb{Z}_{38}^3$$

e o reticulado $\Lambda_A(C) = 38\mathbb{Z}^3 + \sigma(C)$. É fácil ver que

$$\begin{bmatrix} 1 & 36 & 3 \\ 0 & -1 & 7 \\ 0 & 0 & 38 \end{bmatrix}$$

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

$$M = \begin{bmatrix} 1 & 38 & -7 \\ -2 & -75 & 14 \\ 3 & 107 & -20 \end{bmatrix} \begin{bmatrix} 1 & 36 & 3 \\ 0 & -1 & 7 \\ 0 & 0 & 38 \end{bmatrix} = \begin{bmatrix} 1 & -2 & 3 \\ -2 & 3 & 1 \\ 3 & 1 & -2 \end{bmatrix}$$

é também uma matriz geradora para $\Lambda_A(C)$, uma vez que

$$\begin{bmatrix} 1 & 38 & -7 \\ -2 & -75 & 14 \\ 3 & 107 & -20 \end{bmatrix}$$

é uma matriz unimodular. Em [33] é mostrado que a densidade de $\Lambda(M)$ (e portanto de $\Lambda_A(C)$) em relação à métrica da soma é $18/19$ e que esta é a maior densidade possível em relação à métrica da soma no $\mathbb{R}^3$. Observamos também que, usando o Teorema 3.1.2, podemos obter a distância de Lee mínima do código C, a saber $d_{Lee}(C) = 6$.

3.2 Construção D e suas variações

3.2.1 Construção D

A Construção D é apresentada em [2, 9] para códigos binários. Em alguns trabalhos encontramos uma versão generalizada desta construção que relaciona reticulados com cadeias de códigos lineares sobre $\mathbb{Z}_p$, p primo (por exemplo [14,22,39]). Nesta seção, estendemos esta construção para códigos lineares q-ários ($q \in \mathbb{N}$) e também vários resultados

de códigos binários para códigos q-ários.

Definição 3.2.1. ***(Construção D)*** *Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$, uma cadeia de códigos lineares. Dados números inteiros $k_1 \geq k_2 \geq \cdots \geq k_a \geq 0$ e um conjunto de vetores $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1}\}$ em $\mathbb{Z}_q^n$ tais que $C_\ell = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_\ell} \rangle$, para $\ell = 1, 2, \ldots, a$. O conjunto Λ_D consiste de todos os vetores da forma*

$$q\boldsymbol{z} + \sum_{\ell=1}^{a} \sum_{j=1}^{k_\ell} \beta_j^{(\ell)} \frac{1}{q^{\ell-1}} \sigma(\boldsymbol{b}_j),$$

em que $\boldsymbol{z} \in \mathbb{Z}^n$ e $\beta_j^{(\ell)} \in \{0, 1, \ldots, q-1\}$.

A existência dos parâmetros $k_1, k_2, \ldots, k_a$ e $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{k_1}$ na definição acima é garantida pelo Corolário 2.1.1. Quando $a = 1$, a Construção D coincide com a Construção A. Se q for primo, cada código linear C_i pode ser visto como um subespaço vetorial de $\mathbb{Z}_q^n$ e sempre podemos escolher como parâmetros $k_i = \dim C_i$ $(i = 1, \ldots, a)$ e um conjunto de vetores $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1}\} \subseteq \mathbb{Z}_q^n$ linearmente independentes tais que $C_i = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_i} \rangle$ (Observação 2.1.6) e, quando $q = 2$, a Definição 3.2.1 restrita a estes parâmetros coincide a versão original da Construção D [2].

O teorema a seguir fornece uma nova representação para o conjunto Λ_D. No restante deste capítulo, salvo menção em contrário, $k_{a+1} := 0$.

Teorema 3.2.1.

$$\Lambda_D = \left\{ \boldsymbol{z} + \sum_{s=1}^{a} \sum_{i=k_{s+1}+1}^{k_s} \alpha_i^{(s)} \frac{1}{q^{s-1}} \sigma(\boldsymbol{b}_i);\ \boldsymbol{z} \in q\mathbb{Z}^n, \alpha_i^{(s)} \in \mathbb{Z} \text{ e } 0 \leq \alpha_i^{(s)} < q^s \right\}.$$

Demonstração. Observe que $k_1 \geq k_2 \geq \cdots \geq k_a \geq 0$, logo

$$\begin{aligned}
&\sum_{\ell=1}^{a} \sum_{j=1}^{k_\ell} \beta_j^{(\ell)} \frac{1}{q^{\ell-1}} \sigma(\boldsymbol{b}_j) \\
= \ &\left(\sum_{\ell=1}^{a} \beta_1^{(\ell)} q^{a-\ell} \right) \frac{1}{q^{a-1}} \sigma(\boldsymbol{b}_1) + \cdots + \left(\sum_{\ell=1}^{a} \beta_{k_a}^{(\ell)} q^{a-\ell} \right) \frac{1}{q^{a-1}} \sigma(\boldsymbol{b}_{k_a}) + \\
&\left(\sum_{\ell=1}^{a-1} \beta_{k_a+1}^{(\ell)} q^{a-1-\ell} \right) \frac{1}{q^{a-2}} \sigma(\boldsymbol{b}_{k_a+1}) + \cdots + \left(\sum_{\ell=1}^{a-1} \beta_{k_{a-1}}^{(\ell)} q^{a-1-\ell} \right) \frac{1}{q^{a-2}} \sigma(\boldsymbol{b}_{k_{a-1}}) \\
&+ \cdots + \\
&\left(\beta_{k_2+1}^{(1)} \right) \frac{1}{q^0} \sigma(\boldsymbol{b}_{k_2+1}) + \cdots + \left(\beta_{k_1}^{(1)} \right) \frac{1}{q^0} \sigma(\boldsymbol{b}_{k_1}) \\
= \ &\sum_{s=1}^{a} \sum_{i=k_{s+1}+1}^{k_s} \alpha_i^{(s)} \frac{1}{q^{s-1}} \sigma(\boldsymbol{b}_i), \text{ onde } \alpha_i^{(s)} = \sum_{\ell=1}^{s} \beta_i^{(\ell)} q^{s-\ell} \text{ para todo } 1 \leq s \leq a.
\end{aligned}$$

Para completar a prova, é suficiente observar que um inteiro m satisfaz $0 \leq m < q^s$ se, e

somente se, existem $\beta_i^{(1)}, \ldots, \beta_i^{(s)} \in \{0, 1, \ldots, q-1\}$ tais que $\sum_{\ell=1}^{s} \beta_i^{(\ell)} q^{s-\ell} = m$. □

Teorema 3.2.2. *O conjunto Λ_D é um reticulado em $\mathbb{R}^n$ de posto completo.*

Demonstração. Observe que Λ_D é um conjunto discreto, uma vez que $q^{a-1}\Lambda_D \subseteq \mathbb{Z}^n$. Assim, para provar que Λ_D é um reticulado, resta mostrar que Λ_D é um subgrupo aditivo de $\mathbb{R}^n$. Com efeito, Λ_D é um subgrupo aditivo de $\mathbb{R}^n$ pois de $\Lambda_D \subseteq \mathbb{R}^n$, $\mathbf{0} \in \Lambda_D$ e dados $\boldsymbol{w}_1, \boldsymbol{w}_2 \in \Lambda_D$ temos, pelo Teorema 3.2.1, que existem $\boldsymbol{z}_1, \boldsymbol{z}_2 \in q\mathbb{Z}^n$ e $0 \leq \alpha_i^{(s)}, \beta_i^{(s)} < q^s$ tais que

$$\boldsymbol{w}_1 = \boldsymbol{z}_1 + \sum_{s=1}^{a} \sum_{i=k_{s+1}+1}^{k_s} \alpha_i^{(s)} \frac{1}{q^{s-1}} \sigma(\boldsymbol{b}_i) \quad \text{e} \quad \boldsymbol{w}_2 = \boldsymbol{z}_2 + \sum_{s=1}^{a} \sum_{i=k_{s+1}+1}^{k_s} \beta_i^{(s)} \frac{1}{q^{s-1}} \sigma(\boldsymbol{b}_i)$$

e consequentemente

$$\boldsymbol{w}_1 - \boldsymbol{w}_2 = \big(\boldsymbol{z}_1 - \boldsymbol{z}_2\big) + \sum_{s=1}^{a} \sum_{i=k_{s+1}+1}^{k_s} \big(\alpha_i^{(s)} - \beta_i^{(s)}\big) \frac{1}{q^{s-1}} \sigma(\boldsymbol{b}_i).$$

Aplicando o algoritmo da divisão obtemos inteiros $\gamma_i^{(s)}$ e $\mu_i^{(s)}$, $1 \leq s \leq a$ e $k_{s+1}+1 \leq i \leq k_s$, tais que $\alpha_i^{(s)} - \beta_i^{(s)} = \gamma_i^{(s)} q^s + \mu_i^{(s)}$ e $0 \leq \mu_i^{(s)} < q^s$. Assim

$$\boldsymbol{w}_1 - \boldsymbol{w}_2 = \boldsymbol{z} + \sum_{s=1}^{a} \sum_{i=k_{s+1}+1}^{k_s} \mu_i^{(s)} \frac{1}{q^{s-1}} \sigma(\boldsymbol{b}_i),$$

em que

$$\boldsymbol{z} = \boldsymbol{z}_1 - \boldsymbol{z}_2 + q \sum_{s=1}^{a} \sum_{i=k_{s+1}+1}^{k_s} \gamma_i^{(s)} \sigma(\boldsymbol{b}_i) \in q\mathbb{Z}^n.$$

Logo, pelo Teorema 3.2.1, temos que $\boldsymbol{w}_1 - \boldsymbol{w}_2 \in \Lambda_D$. Isto mostra que Λ_D é um reticulado. Para concluir, basta observar que Λ_D tem posto completo, uma vez que $q\mathbb{Z}^n \subseteq \Lambda_D$. □

Exemplo 3.2.1. *Seja $\mathbb{Z}_4^2 \supseteq C_1 \supseteq C_2$ a cadeia de código lineares tal que*

$$\begin{aligned} C_1 &= \langle (2,2), (0,1) \rangle \ \textit{e} \\ C_2 &= \langle (2,2) \rangle . \end{aligned}$$

Dados $k_1 = 2$, $k_2 = 1$, $\boldsymbol{b}_1 = (2,2), \boldsymbol{b}_2 = (0,1) \in \mathbb{Z}_4^2$, temos que $C_1 = \langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle$ e $C_2 = \langle \boldsymbol{b}_1 \rangle$. Aplicando o Teorema 3.2.1, obtemos

$$\Lambda_D = \big\{ \boldsymbol{z} + \alpha_1^{(2)}(1/2, 1/2) + \alpha_2^{(1)}(0,1);\ \boldsymbol{z} \in 4\mathbb{Z}^n, 0 \leq \alpha_2^{(1)} < 4 \ \textit{e}\ 0 \leq \alpha_1^{(2)} < 4^2 \big\},$$

isto é,

$$\Lambda_D = \bigcup_{\boldsymbol{z} \in 4\mathbb{Z}^2} \big(\boldsymbol{z} + \Lambda_D \cap [0,4)^2 \big)$$

e os elementos de $\Lambda_D \cap [0,4)^2$ estão representados na Figura 3.2.

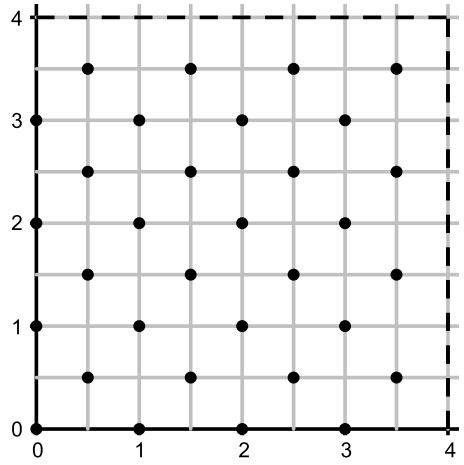


Figura 3.2: $\Lambda_D \cap [0,4)^2$

Observação 3.2.1. *Seja $\mathbb{Z}_3^2 \supseteq C_1 \supseteq C_2$ tal que $C_1 = C_2 = \{(0,0),(1,2),(2,1)\}$. Aplicando a Construção D a esta cadeia usando $k_1 = 2$, $k_2 = 1$, $\boldsymbol{b}_1 = (1,2), \boldsymbol{b}_2 = (2,1) \in \mathbb{Z}_3^2$, obtemos*

$$\Lambda_D = \left\{\boldsymbol{z} + \alpha_1^{(2)}(1/3, 2/3) + \alpha_2^{(1)}(2,1);\ \boldsymbol{z} \in 3\mathbb{Z}^n, 0 \leq \alpha_2^{(1)} < 3 \text{ e } 0 \leq \alpha_1^{(2)} < 3^2\right\}.$$

Por outro lado, utilizando $\hat{k}_1 = 2$, $\hat{k}_2 = 1$, $\hat{\boldsymbol{b}}_1 = (2,1), \hat{\boldsymbol{b}}_2 = (1,2) \in \mathbb{Z}_3^2$, temos

$$\hat{\Lambda}_D = \left\{\boldsymbol{z} + \alpha_1^{(2)}(2/3, 1/3) + \alpha_2^{(1)}(1,2);\ \boldsymbol{z} \in 3\mathbb{Z}^n, 0 \leq \alpha_2^{(1)} < 3 \text{ e } 0 \leq \alpha_1^{(2)} < 3^2\right\}.$$

Note que $\Lambda_D \neq \hat{\Lambda}_D$, pois $(1/3, 2/3) \in \Lambda_D \setminus \hat{\Lambda}_D$. Isto mostra que um reticulado obtido via Construção D depende dos parâmetros $k_1, \ldots, k_a$ e $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1}$.

Lema 3.2.1. *Se o conjunto $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k\} \subseteq \mathbb{Z}_q^n$ é linearmente independente sobre $\mathbb{Z}_q$, então $\{\sigma(\boldsymbol{b}_1), \ldots, \sigma(\boldsymbol{b}_k)\} \subseteq \mathbb{Z}^n$ é linearmente independente sobre $\mathbb{Z}$.*

Demonstração. Suponha que $\{\sigma(\boldsymbol{b}_1), \ldots, \sigma(\boldsymbol{b}_k)\}$ é linearmente dependente sobre $\mathbb{Z}$, isto é, que existem inteiros $\alpha_1, \ldots, \alpha_k$ não todos nulos tais que $\alpha_1\sigma(\boldsymbol{b}_1) + \cdots + \alpha_k\sigma(\boldsymbol{b}_k) = 0$. Seja $s = \min\{t \in \mathbb{Z};\ \alpha_i q^{-t} \in \mathbb{Z} \text{ e } \alpha_i q^{-(t+1)} \in \mathbb{Z}, \forall i = 1, \ldots, k\}$. Dividindo os inteiros $\alpha_1, \ldots, \alpha_k$ por q^s, obtemos inteiros $\beta_1, \ldots, \beta_k$, não todos múltiplos de q, tais que $\alpha_1 = q^s\beta_1, \ldots, \alpha_k = q^s\beta_k$ e logo $\beta_1\sigma(\boldsymbol{b}_1) + \cdots + \beta_k\sigma(\boldsymbol{b}_k) = \mathbf{0}$. Logo $\overline{\beta}_1\boldsymbol{b}_1 + \cdots + \overline{\beta}_k\boldsymbol{b}_k = \mathbf{0}$ com $\overline{\beta}_i \neq 0$ para algum $i \in \{1, \ldots, k\}$. Portanto $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k\} \subseteq \mathbb{Z}_q^n$ é linearmente dependente sobre $\mathbb{Z}_q$. □

Teorema 3.2.3. *Se $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1} \in \mathbb{Z}_q^n$ são vetores linearmente independentes, então*

$$|\Lambda_D \cap [0,q)^n| = \prod_{s=1}^{a} \left(q^s\right)^{k_s - k_{s+1}}.$$

Demonstração. Pelo Lema 3.2.1, $\sigma(\boldsymbol{b}_1), \ldots, \sigma(\boldsymbol{b}_{k_1})$ são vetores linearmente independentes

sobre $\mathbb{Z}$. Logo existem exatamente $\prod_{s=1}^{a}\left(q^s\right)^{k_s-k_{s+1}}$ vetores da forma

$$\sum_{s=1}^{a}\sum_{i=k_{s+1}+1}^{k_s}\alpha_i^{(s)}\frac{1}{q^{s-1}}\sigma(\boldsymbol{b}_i) \quad (0\leq\alpha_i^{(s)}<q^s).$$

Devemos mostrar que estes vetores também são distintos quando considerados módulo q. Logo, para completar a demonstração é suficiente observar que se

$$\boldsymbol{w}_1=\sum_{s=1}^{a}\sum_{i=k_{s+1}+1}^{k_s}\alpha_i^{(s)}\frac{1}{q^{s-1}}\sigma(\boldsymbol{b}_i) \quad \text{e} \quad \boldsymbol{w}_2=\sum_{s=1}^{a}\sum_{i=k_{s+1}+1}^{k_s}\beta_i^{(s)}\frac{1}{q^{s-1}}\sigma(\boldsymbol{b}_i),$$

$0\leq\alpha_i^{(s)}<q^s$ e $0\leq\beta_i^{(s)}<q^s$, são congruentes módulo q, então $\boldsymbol{w}_1=\boldsymbol{w}_2$. De fato, $\boldsymbol{w}_1\equiv\boldsymbol{w}_2 \mod q$ se, e somente se,

$$\sum_{s=1}^{a}\sum_{i=k_{s+1}+1}^{k_s}\left(\alpha_i^{(s)}-\beta_i^{(s)}\right)\frac{1}{q^{s-1}}\sigma(\boldsymbol{b}_i)\in q\mathbb{Z}^n.$$

Como os vetores $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_{k_1}$ são linearmente independentes (sobre $\mathbb{Z}_q$), segue que

$$\left(\alpha_i^{(s)}-\beta_i^{(s)}\right)\frac{1}{q^{s-1}}\in q\mathbb{Z}.$$

Por outro lado, $0\leq\alpha_i^{(s)}<q^s$ e $0\leq\beta_i^{(s)}<q^s$, isto é, $-q<\left(\alpha_i^{(s)}-\beta_i^{(s)}\right)\frac{1}{q^{s-1}}<q$. Logo

$$\left(\alpha_i^{(s)}-\beta_i^{(s)}\right)\frac{1}{q^{s-1}}=0,$$

isto é, $\alpha_i^{(s)}=\beta_i^{(s)}$, para todo par (i,s) satisfazendo $1\leq s\leq a$ e $k_{s+1}+1\leq i\leq k_s$. Portanto $\boldsymbol{w}_1=\boldsymbol{w}_2$. □

Observação 3.2.2. *No Exemplo 3.2.1, os vetores $\boldsymbol{b}_1=(2,2)$ e $\boldsymbol{b}_2=(0,1)$ são linearmente dependentes sobre $\mathbb{Z}_4$ e $|\Lambda_D\cap[0,4)^2|=32\neq 64=\prod_{s=1}^{2}\left(4^s\right)^{k_s-k_{s+1}}$. Isto mostra que a hipótese do Teorema 3.2.3 é fundamental para garantir a conclusão do mesmo.*

O próximo teorema estende um resultado de reticulados obtidos via Construção D a partir de códigos p-ários (p primo) [14] para códigos q-ários, $q\in\mathbb{N}$.

Teorema 3.2.4. *Sejam G_1 a matriz cujas linhas são os vetores $\sigma(\boldsymbol{b}_1),\ldots,\sigma(\boldsymbol{b}_{k_1})$ e C o código linear q^a-ário gerado pelas linhas da matriz $G=DG_1$, em que $D=(d_{ij})$ é a matriz diagonal tal que*

$$d_{jj} = \begin{cases} 1, \ se\ 1 \leq j \leq k_a \\ q, \ se\ k_a < j \leq k_{a-1} \\ \vdots \\ q^{a-1}, \ se\ k_2 < j \leq k_1. \end{cases}$$

Temos que $q^{a-1}\Lambda_D = \Lambda_A(C)$.

Demonstração. Seja $\boldsymbol{w} \in \Lambda_A(C)$. Existem $\alpha_j^{(i)} \in \{0, 1, \ldots, q^a - 1\}$, $1 \leq i \leq a$ e $k_{i+1}+1 \leq j \leq k_i$, e $\boldsymbol{z} \in \mathbb{Z}^n$ tais que

$$\boldsymbol{w} = q^a \boldsymbol{z} + \sum_{i=1}^{a} \sum_{j=k_{i+1}+1}^{k_i} \alpha_j^{(i)} q^{a-i} \sigma(\boldsymbol{b}_j).$$

Por outro lado, $q^{a-1}\Lambda_D$ é um reticulado e $q^a\boldsymbol{z}, q^{a-i}\sigma(\boldsymbol{b}_j) \in q^{a-1}\Lambda_D$ para todo $1 \leq i \leq a$ e $k_{i+1} < j \leq k_i$, logo $\boldsymbol{w} \in q^{a-1}\Lambda_D$. Isto mostra que $\Lambda_A(C) \subseteq q^{a-1}\Lambda_D$. Agora, vamos mostrar que $q^{a-1}\Lambda_D \subseteq \Lambda_A(C)$. Com efeito, seja $\boldsymbol{w} \in q^{a-1}\Lambda_D$. Pelo Teorema 3.2.1, existem $\alpha_j^{(i)} \in \{0, 1, \ldots, q^i - 1\} \subseteq \{0, 1, \ldots, q^a - 1\}$, $1 \leq i \leq a$ e $k_{i+1} + 1 \leq j \leq k_i$, e $\boldsymbol{z} \in \mathbb{Z}^n$ tais que

$$\boldsymbol{w} = q^a \boldsymbol{z} + \sum_{i=1}^{a} \sum_{j=k_{i+1}+1}^{k_i} \alpha_j^{(i)} q^{a-i} \sigma(\boldsymbol{b}_j).$$

Portanto $\boldsymbol{w} \in \Lambda_A(C)$. □

Corolário 3.2.1. *O conjunto* $q^{a-1}\Lambda_D$ *é um reticulado* q^a*-ário.*

Exemplo 3.2.2. *Considere novamente a cadeia de códigos lineares* $\mathbb{Z}_3^2 \supseteq C_1 \supseteq C_2$ *tal que* $C_1 = C_2 = \{(0,0), (1,2), (2,1)\}$. *Escolhendo* $k_1 = 2$, $k_2 = 1$, $\boldsymbol{b}_1 = (1,2), \boldsymbol{b}_2 = (2,1) \in \mathbb{Z}_3^2$, *obtemos*

$$\Lambda_D = \left\{ \boldsymbol{z} + \alpha_1^{(2)}(1/3, 2/3) + \alpha_2^{(1)}(2,1); \ \boldsymbol{z} \in 3\mathbb{Z}^n, 0 \leq \alpha_2^{(1)} < 3 \ e\ 0 \leq \alpha_1^{(2)} < 3^2 \right\}.$$

O reticulado $3\Lambda_D$ *é* 9*-ário, pois pode ser obtido via Construção A a partir do código linear* 9*-ário determinado pela matriz*

$$G = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 6 & 3 \end{pmatrix}.$$

Observação 3.2.3. *O reticulado* Λ_D *do exemplo anterior não pode ser obtido via Construção D a partir de uma cadeia de códigos lineares binários.*

O resultado a seguir estende o Teorema 13 da página 232 de [9] para a Construção D a partir de códigos q-ários, $q \in \mathbb{N}$.

Teorema 3.2.5. *Sejam* $k_1 \geq k_2 \geq \cdots \geq k_a \geq 0$ *e* $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1} \in \mathbb{Z}_q^n$ *não nulos tais que*

1. *$C_\ell = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_\ell} \rangle$, para $\ell = 1, \ldots, a$.*

2. *Alguma permutação das linhas da matriz $M = [\sigma(\boldsymbol{b}_1) \ \cdots \ \sigma(\boldsymbol{b}_{k_1})]^t$ forma uma matriz triangular superior (resp. inferior) na forma escalonada.*

3. *Para cada $j \in \{1, \ldots, k_1\}$, a primeira (resp. última) componente não nula do vetor $\sigma(\boldsymbol{b}_j)$, que denotamos por α_j, divide q e todas as demais componentes do mesmo.*

Se Λ_D é o reticulado obtido via Construção D a partir da cadeia $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ usando os parâmetros $k_1, k_2, \ldots, k_a$ e $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1}$, então existe uma base para Λ_D formada pelos k_1 vetores $(1/q^{i-1})\sigma(\boldsymbol{b}_j)$, $1 \leq i \leq a$ e $k_{i+1} < j \leq k_i$, mais $n - k_1$ vetores da forma $(0, \ldots, 0, q, 0, \ldots, 0)$.

Demonstração. Podemos assumir sem perda de generalidade que alguma permutação das linhas da matriz M forma uma matriz triangular superior. Seja $\tilde{M}$ a (única) matriz triangular superior de ordem n cujas linhas são os k_1 vetores

$$\frac{1}{q^{i-1}}\sigma(\boldsymbol{b}_j) \quad (1 \leq i \leq a \ \text{ e } \ k_{i+1} < j \leq k_i)$$

e as demais $n - k_1$ linhas são da forma $(0, \ldots, 0, q, 0, \ldots, 0)$. A existência e unicidade da matriz $\tilde{M}$ é garantida pela Hipótese 2, uma vez que $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1}$ são vetores não nulos. As linhas da matriz $\tilde{M}$ são linearmente independentes pois

$$\det \tilde{M} = q^{n-k_1}\left(\prod_{j=1}^{k_1} \alpha_j\right) \prod_{i=1}^{a} \left(\frac{1}{q^{i-1}}\right)^{k_i - k_{i+1}} \neq 0.$$

Para concluir a demonstração, vamos mostrar que $\Lambda(\tilde{M}) = \Lambda_D$, em que $\Lambda(\tilde{M})$ é o reticulado gerado pelas linhas da matriz $\tilde{M}$. Com efeito, dado $\boldsymbol{w} \in \Lambda(\tilde{M})$, existem números inteiros $\beta_j^{(i)}$, $1 \leq i \leq a$ e $k_{i+1} + 1 \leq j \leq k_i$, e $\boldsymbol{z} \in q\mathbb{Z}^n$ tais que

$$\boldsymbol{w} = \boldsymbol{z} + \sum_{i=1}^{a} \sum_{j=k_{i+1}+1}^{k_i} \beta_j^{(i)} \frac{1}{q^{i-1}} \sigma(\boldsymbol{b_j}).$$

Dividindo $\beta_j^{(i)}$ por q^i obtemos inteiros $\mu_j^{(i)}$ e $\alpha_j^{(i)}$, $1 \leq i \leq a$ e $k_{i+1} + 1 \leq j \leq k_i$, tais que $\beta_j^{(i)} = \mu_j^{(i)} q^i + \alpha_j^{(i)}$ e $0 \leq \alpha_j^{(i)} < q^i$. Assim,

$$\boldsymbol{w} = \tilde{\boldsymbol{z}} + \sum_{i=1}^{a} \sum_{j=k_{i+1}+1}^{k_i} \alpha_j^{(i)} \frac{1}{q^{i-1}} \sigma(\boldsymbol{b}_j),$$

em que

$$\tilde{\boldsymbol{z}} = \boldsymbol{z} + q \sum_{i=1}^{a} \sum_{j=k_{i+1}+1}^{k_i} \mu_j^{(i)} \sigma(\boldsymbol{b}_j) \in q\mathbb{Z}^n.$$

Portanto $\boldsymbol{w} \in \Lambda_D$ (Teorema 3.2.1). Reciprocamente, dado $\boldsymbol{w} \in \Lambda_D$ temos que existem inteiros $\alpha_j^{(i)} \in \{0, 1, \ldots, q^i - 1\}$, $1 \leq i \leq a$ e $k_{i+1} + 1 \leq j \leq k_i$, e $\boldsymbol{z} \in q\mathbb{Z}^n$ tais que

$$\boldsymbol{w} = \boldsymbol{z} + \sum_{i=1}^{a} \sum_{j=k_{i+1}+1}^{k_i} \alpha_j^{(i)} \frac{1}{q^{i-1}} \sigma(\boldsymbol{b}_j).$$

Por outro lado,

$$\sum_{i=1}^{a} \sum_{j=k_{i+1}+1}^{k_i} \alpha_j^{(i)} \frac{1}{q^{i-1}} \sigma(\boldsymbol{b}_j) \in \Lambda(\tilde{M}),$$

uma vez que os vetores $(1/q^{i-1})\sigma(\boldsymbol{b}_j)$, $1 \leq i \leq a$ e $k_{i+1} < j \leq k_i$, são linhas da matriz $\tilde{M}$. Logo, para mostrar que $\boldsymbol{w} \in \Lambda(\tilde{M})$ é suficiente mostrar que $\boldsymbol{z} \in \Lambda(\tilde{M})$. De fato, sejam $\boldsymbol{d}_1, \ldots, \boldsymbol{d}_n$ as linhas da matriz $\tilde{M}$ e $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ os vetores canônicos do $\mathbb{R}^n$. Como a primeira componente não nula de cada vetor $\sigma(\boldsymbol{b}_i)$, $i = 1, \ldots, k_1$, divide q e todas as demais componentes do mesmo e a matriz $\tilde{M}$ é triangular superior, temos que cada um dos vetores $q\boldsymbol{e}_i$, $1 \leq i \leq n$, pode ser escrito como combinação linear inteira das linhas $\boldsymbol{d}_i, \boldsymbol{d}_{i+1}, \ldots, \boldsymbol{d}_n$. Logo $q\mathbb{Z}^n \subseteq \Lambda(\tilde{M})$ e portanto $\boldsymbol{z} \in \Lambda(\tilde{M})$. Isto mostra que $\Lambda(\tilde{M}) = \Lambda_D$. □

Corolário 3.2.2. *Sejam $k_1 \geq k_2 \geq \cdots \geq k_a \geq 0$ e $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1} \in \mathbb{Z}_q^n$ vetores não nulos satisfazendo as Condições 1, 2 e 3 do Teorema 3.2.5. Temos que*

$$\det \Lambda_D = \left(\prod_{j=1}^{k_1} \alpha_j \right)^2 \left(q^2\right)^{n - \sum_{\ell=1}^{a} k_\ell}.$$

Demonstração. Do Teorema 3.2.5, existe uma matriz triangular $\tilde{M} \in \mathbb{R}^{n \times n}$, cujas linhas são os k_1 vetores $(1/q^{i-1})\sigma(\boldsymbol{b_j})$, $1 \leq i \leq a$ e $k_{i+1} < j \leq k_i$, mais $n - k_1$ vetores da forma $(0, \ldots, 0, q, 0, \ldots, 0)$ tal que $\Lambda_D = \Lambda(\tilde{M})$. Portanto

$$\det \Lambda_D = \det(\tilde{M}\tilde{M}^t) = \left(\prod_{j=1}^{k_1} \alpha_j \right)^2 \left(q^2\right)^{n - \sum_{\ell=1}^{a} k_\ell},$$

uma vez que

$$\begin{aligned} \det \tilde{M} &= q^{n-k_1} \left(\prod_{j=1}^{k_1} \alpha_j \right) \prod_{i=1}^{a} \left(\frac{1}{q^{i-1}} \right)^{k_i - k_{i+1}} \\ &= \left(\prod_{j=1}^{k_1} \alpha_j \right) q^{n-k_1} \cdot q^{-(k_a + k_{a-1} + \cdots + k_3 + k_2)} \\ &= \left(\prod_{j=1}^{k_1} \alpha_j \right) q^{n - \sum_{\ell=1}^{a} k_\ell}. \end{aligned}$$

Isto conclui a demonstração. □

Corolário 3.2.3. *[9] Sejam $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1} \in \mathbb{Z}_2^n$ vetores não nulos tais que*

1. *$C_\ell = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_\ell} \rangle$ para $\ell = 1, \ldots, a$.*
2. *Alguma permutação das linhas da matriz M, cujas linhas são $\sigma(\boldsymbol{b}_1), \ldots, \sigma(\boldsymbol{b}_{k_1})$, forma uma matriz triangular superior (resp. inferior) na forma escalonada.*

Então existe uma base para o reticulado Λ_D formada pelos k_1 vetores $(1/2^{i-1})\sigma(\boldsymbol{b}_j)$, $1 \leq i \leq a$ e $k_{i+1} < j \leq k_i$, mais $n - k_1$ vetores da forma $(0, \ldots, 0, 2, 0, \ldots, 0)$. Além disso,

$$\det \Lambda_D = 4^{n - \sum_{\ell=1}^{a} k_\ell}.$$

Demonstração. Para cada $j \in \{1, \ldots, k_1\}$ a primeira componente não nula de $\sigma(\boldsymbol{b_i})$ é igual a 1 e portanto divide 2 e todas as demais componentes deste vetor. Aplicando o Teorema 3.2.5 e o Corolário 3.2.2 obtemos o resultado desejado. □

O próximo corolário estende a Proposição 3.2.4 da referência [23].

Corolário 3.2.4. *Sejam $C \subseteq \mathbb{Z}_{p^r}^n$ um código linear e G uma matriz geradora de C na forma padrão, isto é,*

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,r-1} & A_{0,r} \\ 0 & pI_{k_1} & pA_{1,2} & pA_{1,3} & \cdots & pA_{1,r-1} & pA_{1,r} \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{2,3} & \cdots & p^2 A_{2,r-1} & p^2 A_{2,r} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & p^{r-1} I_{k_{r-1}} & p^{r-1} A_{r-1,r} \end{pmatrix},$$

na qual as colunas estão agrupadas em blocos de tamanhos $k_0, k_1, \ldots, k_{r-1}$ e $k_r = n - \sum_{i=0}^{r-1} k_i$, com $k_i \geq 0$ para todo $i \in \{0, 1, \ldots, r\}$. Uma matriz geradora do reticulado $\Lambda_A(C)$ é dada por

$$\begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,r-1} & A_{0,r} \\ 0 & pI_{k_1} & pA_{1,2} & pA_{1,3} & \cdots & pA_{1,r-1} & pA_{1,r} \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{2,3} & \cdots & p^2 A_{2,r-1} & p^2 A_{2,r} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & p^{r-1} I_{k_{r-1}} & p^{r-1} A_{r-1,r} \\ 0 & 0 & 0 & 0 & \cdots & 0 & p^r I_{k_r} \end{pmatrix}.$$

Demonstração. Segue imediatamente do Teorema 3.2.5. □

Observação 3.2.4. *Um fato importante que pode ser inferido do último teorema é descrito a seguir. Se um reticulado $\Lambda \subseteq \mathbb{R}^n$ de posto completo possui uma matriz geradora do tipo λM com $\lambda \in \mathbb{R}$ e $M \in \mathbb{Z}^{n \times n}$ sendo uma matriz triangular superior (resp. inferior) tal*

que a primeira entrada não nula de cada linha (resp. última) divide todas as demais entradas de sua linha, então exceto por um fator de escala Λ pode ser obtido via Construção D. Em particular, os reticulados $\mathbb{Z}^n, D_n, E_8, \Lambda_{16}$ e Λ_{24} (ver Seção 1.7) podem ser obtidos via Construção D. Para ilustrar tal afirmação, nos próximos exemplos construímos os reticulados E_8, Λ_{16} e Λ_{24}.

Exemplo 3.2.3. *Seja $\mathbb{Z}_4^8 \supseteq C_1 \supseteq C_2$ a cadeia códigos lineares tal que*

$$C_1 = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_8 \rangle \;\; e \;\; C_2 = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_7 \rangle ,$$

em que

$$\begin{aligned}
\boldsymbol{b}_1 &= (2,2,0,0,0,0,0,0),\\
\boldsymbol{b}_2 &= (0,2,2,0,0,0,0,0),\\
\boldsymbol{b}_3 &= (0,0,2,2,0,0,0,0),\\
\boldsymbol{b}_4 &= (0,0,0,2,2,0,0,0),\\
\boldsymbol{b}_5 &= (0,0,0,0,2,2,0,0),\\
\boldsymbol{b}_6 &= (0,0,0,0,0,2,2,0),\\
\boldsymbol{b}_7 &= (1,1,1,1,1,1,1,1),\\
\boldsymbol{b}_8 &= (1,0,0,0,0,0,0,0).
\end{aligned}$$

Seja Λ_D o reticulado obtido via Construção D, utilizando como parâmetros $k_1 = 8, k_2 = 7$ e os vetores $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_8$. O Teorema 3.2.5 afirma que

$$\left\{ \frac{1}{4}\sigma(\boldsymbol{b}_1), \frac{1}{4}\sigma(\boldsymbol{b}_2), \frac{1}{4}\sigma(\boldsymbol{b}_3), \frac{1}{4}\sigma(\boldsymbol{b}_4), \frac{1}{4}\sigma(\boldsymbol{b}_5), \frac{1}{4}\sigma(\boldsymbol{b}_6), \frac{1}{4}\sigma(\boldsymbol{b}_7), \frac{1}{4^0}\sigma(\boldsymbol{b}_8) \right\}$$

é uma base para Λ_D. Assim,

$$\begin{pmatrix}
1/2 & 1/2 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1/2 & 1/2 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1/2 & 1/2 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1/2 & 1/2 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1/2 & 1/2 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1/2 & 1/2 & 0\\
1/4 & 1/4 & 1/4 & 1/4 & 1/4 & 1/4 & 1/4 & 1/4\\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

é uma matriz geradora para Λ_D e, consequentemente, a matriz

$$M = \begin{pmatrix} -1/2 & 1/2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1/2 & 1/2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1/2 & 1/2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1/2 & 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1/2 & 1/2 & 0 \\ 1/4 & 1/4 & 1/4 & 1/4 & 1/4 & 1/4 & 1/4 & 1/4 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

também é uma matriz geradora para Λ_D. Por outro lado, temos que $2M$ é uma matriz geradora de E_8 (ver Seção 1.7). Logo $2\Lambda_D = E_8$.

Exemplo 3.2.4. *Seja $\mathbb{Z}_4^{16} \supseteq C_1 \supseteq C_2$ a cadeia códigos lineares tal que $C_1 = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{16} \rangle$ e $C_2 = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_5 \rangle$, em que*

$$\begin{aligned}
\boldsymbol{b}_1 &= (2,2,2,2,0,2,0,2,2,0,0,2,0,0,0,0),\\
\boldsymbol{b}_2 &= (0,2,2,2,2,0,2,0,2,2,0,0,2,0,0,0),\\
\boldsymbol{b}_3 &= (0,0,2,2,2,2,0,2,0,2,2,0,0,2,0,0),\\
\boldsymbol{b}_4 &= (0,0,0,2,2,2,2,0,2,0,2,2,0,0,2,0),\\
\boldsymbol{b}_5 &= (2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2),\\
\boldsymbol{b}_6 &= (2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),\\
\boldsymbol{b}_7 &= (1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0),\\
\boldsymbol{b}_8 &= (1,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0),\\
\boldsymbol{b}_9 &= (1,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0),\\
\boldsymbol{b}_{10} &= (1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0),\\
\boldsymbol{b}_{11} &= (1,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0),\\
\boldsymbol{b}_{12} &= (1,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0),\\
\boldsymbol{b}_{13} &= (1,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0),\\
\boldsymbol{b}_{14} &= (1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0),\\
\boldsymbol{b}_{15} &= (1,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0),\\
\boldsymbol{b}_{16} &= (1,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0).
\end{aligned}$$

Seja Λ_D o reticulado obtido via Construção D, utilizando como parâmetros $k_1 = 16, k_2 = 5$ e os vetores $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{16}$. Aplicando o Teorema 3.2.5, obtemos que

$$\left\{ \frac{1}{4}\sigma(\boldsymbol{b}_1), \frac{1}{4}\sigma(\boldsymbol{b}_2), \ldots, \frac{1}{4}\sigma(\boldsymbol{b}_5), \frac{1}{4^0}\sigma(\boldsymbol{b}_6), \frac{1}{4^0}\sigma(\boldsymbol{b}_7), \ldots, \frac{1}{4^0}\sigma(\boldsymbol{b}_{16}) \right\}$$

é uma base para Λ_D. Logo uma matriz geradora para Λ_D é dada por

$$M = \begin{pmatrix}
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1/2 & 1/2 & 1/2 & 1/2 & 0 & 1/2 & 0 & 1/2 & 1/2 & 0 & 0 & 1/2 & 0 & 0 & 0 & 0 \\
0 & 1/2 & 1/2 & 1/2 & 1/2 & 0 & 1/2 & 0 & 1/2 & 1/2 & 0 & 0 & 1/2 & 0 & 0 & 0 \\
0 & 0 & 1/2 & 1/2 & 1/2 & 1/2 & 0 & 1/2 & 0 & 1/2 & 1/2 & 0 & 0 & 1/2 & 0 & 0 \\
0 & 0 & 0 & 1/2 & 1/2 & 1/2 & 1/2 & 0 & 1/2 & 0 & 1/2 & 1/2 & 0 & 0 & 1/2 & 0 \\
1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2
\end{pmatrix}$$

Agora, observe que

$$\sqrt{2}M = \frac{1}{\sqrt{2}} \begin{pmatrix}
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}$$

e que esta é uma matriz geradora do reticulado Λ_{16} *(ver Seção 1.7). Portanto* $\sqrt{2}\Lambda_D = \Lambda_{16}$.

Exemplo 3.2.5. *Seja $\mathbb{Z}_8^{24} \supseteq C_1 \supseteq C_2$ uma cadeia códigos lineares tal que*

$$\begin{aligned} C_1 &= \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{24} \rangle \quad e \\ C_2 &= \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{23} \rangle, \end{aligned}$$

em que cada $\boldsymbol{b}_i$ corresponde a i-ésima linha da seguinte matriz

$$\begin{pmatrix}
4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 \\
5 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

Se Λ_D é o reticulado obtido via Construção D, utilizando como parâmetros $k_1 = 24, k_2 = 23$ e os vetores $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{24}$, então $\Lambda_D = \frac{\sqrt{8}}{8}\Lambda_{24}$.

3.2.2 Construção D′

A Construção D′ é apresentada em [2, 9] apenas para códigos lineares binários. Nesta seção, estendemos esta construção para códigos lineares q-ários, $q \in \mathbb{N}$.

Definição 3.2.2. ***(Construção D′)*** *Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ uma cadeia*

de códigos lineares. Dados números inteiros $r_1, r_2, \ldots, r_a$ *satisfazendo* $0 \leq r_1 \leq r_2 \leq \cdots \leq r_a$ *e um conjunto de vetores* $\{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_a}\}$ *em* $\mathbb{Z}_q^n$ *tais que* $C_\ell^\perp = \langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_\ell} \rangle$ *para* $\ell = 1, 2, \ldots, a$*, em que* $C_\ell^\perp$ *é o código dual de* C_ℓ*, o conjunto* $\Lambda_{D'}$ *consiste de todos os vetores* $\boldsymbol{x} \in \mathbb{Z}^n$ *tais que*

$$\boldsymbol{x} \cdot \sigma(\boldsymbol{h}_j) \equiv \boldsymbol{0} \mod q^{i+1}$$

para todo par de inteiros (i, j) *satisfazendo* $0 \leq i < a$ *e* $r_{a-i-1} < j \leq r_{a-i}$ *(*$r_0 := 0$*).*

A existência dos parâmetros $r_1, r_2, \ldots, r_a$ e $\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_{r_a}$ na definição acima é garantida pelo Teorema 2.2.4. Quando $a = 1$, a Construção D′ coincide com a Construção A. Se q é primo, cada código linear C_i pode ser visto como um subespaço vetorial de $\mathbb{Z}_q^n$ e sempre podemos escolher como parâmetros $r_i = n - \dim C_i$ $(i = 1, \ldots, a)$ e um conjunto de vetores $\{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_a}\} \subseteq \mathbb{Z}_q^n$ linearmente independente tal que $C_i^\perp = \langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_i} \rangle$ (Observação 2.2.1) e, quando $q = 2$, a Definição 3.2.2 restrita a estes parâmetros coincide a versão original da Construção D′ [2].

Teorema 3.2.6. *O conjunto* $\Lambda_{D'}$ *é um reticulado em* $\mathbb{R}^n$ *de posto completo.*

Demonstração. $\Lambda_{D'}$ é um conjunto discreto, pois $\Lambda_{D'} \subseteq \mathbb{Z}^n$. Para ver que $\Lambda_{D'}$ é um subgrupo aditivo de $\mathbb{R}^n$ note que $\Lambda_{D'} \subseteq \mathbb{R}^n$, $\boldsymbol{0} \in \Lambda_{D'}$ e dados $\boldsymbol{x}, \boldsymbol{y} \in \Lambda_{D'}$ temos que

$$(\boldsymbol{x} - \boldsymbol{y}) \cdot \sigma(\boldsymbol{h_j}) \equiv \boldsymbol{0} \mod q^{i+1}$$

para todo par de inteiros (i, j) satisfazendo $0 \leq i < a$ e $r_{a-i-1} < j \leq r_{a-i}$, uma vez que $\boldsymbol{x} \cdot \sigma(\boldsymbol{h_j}) \equiv \boldsymbol{0} \mod q^{i+1}$ e $\boldsymbol{y} \cdot \sigma(\boldsymbol{h_j}) \equiv \boldsymbol{0} \mod q^{i+1}$. Isto mostra que $\boldsymbol{x} - \boldsymbol{y} \in \Lambda_{D'}$. Como $q^a \mathbb{Z}^n \subseteq \Lambda_{D'}$, segue que $\Lambda_{D'}$ é um reticulado de posto completo. □

Exemplo 3.2.6. *Seja* $\mathbb{Z}_4^2 \supseteq C_1 \supseteq C_2$ *a cadeia de códigos lineares tal que*

$$C_1 = \langle (2,2), (0,1) \rangle \;\; e \;\; C_2 = \langle (2,2) \rangle .$$

Observe que

$$\begin{aligned} C_1^\perp &= \{(x,y) \in \mathbb{Z}_4^2;\ 2x + 2y = 0 \ e \ y = 0\} \\ &= \{(0,0), (2,0)\} \\ &= \langle (2,0) \rangle \end{aligned}$$

e

$$\begin{aligned} C_2^\perp &= \{(x,y) \in \mathbb{Z}_4^2;\ 2x + 2y = 0\} \\ &= \{(0,0), (2,0), (0,2), (2,2), (3,1), (1,1), (1,3), (3,3)\} \\ &= \langle (3,1), (2,0) \rangle . \end{aligned}$$

Tomando $r_1 = 1$, $r_2 = 2$, $\boldsymbol{h}_1 = (2,0)$ *e* $\boldsymbol{h}_2 = (3,1)$, *temos que* $0 \leq r_1 \leq r_2$, $C_1^{\perp} = \langle \boldsymbol{h}_1 \rangle$, $C_2^{\perp} = \langle \boldsymbol{h}_1, \boldsymbol{h}_2 \rangle$ *e*

$$\begin{aligned} \Lambda_{D'} &= \{\boldsymbol{x} \in \mathbb{Z}^2;\ \boldsymbol{x} \cdot \sigma(\boldsymbol{h}_1) \equiv \boldsymbol{0} \mod 16 \ e\ \boldsymbol{x} \cdot \sigma(\boldsymbol{h}_2) \equiv \boldsymbol{0} \mod 4\} \\ &= \{(x,y) \in \mathbb{Z}^2;\ 2x \equiv 0 \mod 16 \ e\ 3x + y \equiv 0 \mod 4\}. \end{aligned}$$

Logo $\Lambda_{D'} \cap [0,16)^2 = \{(0,0),(0,4),(0,8),(0,12),(8,0),(8,4),(8,8),(8,12)\}$. *Os elementos de* $\Lambda_{D'} \cap [0,16)^2$ *estão representados na Figura 3.3.*

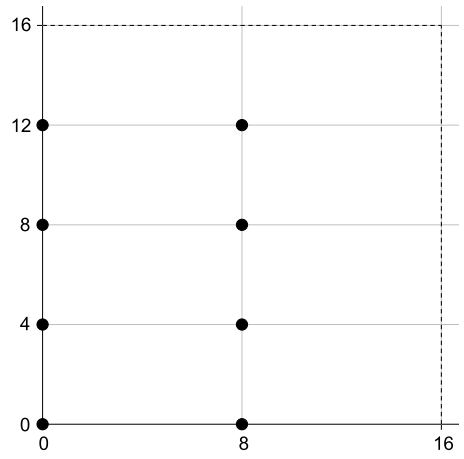


Figura 3.3: $\Lambda_{D'} \cap [0,16)^2$

3.2.3 Construção $\overline{\mathrm{D}}$

A Construção $\overline{\mathrm{D}}$, também chamada de *construção pela fórmula código*, é uma reformulação da fórmula código de Forney, que foi introduzida em [15, 16]. Nesta seção, estendemos esta construção para códigos lineares q-ários, $q \in \mathbb{N}$.

Definição 3.2.3. *(**Construção** $\overline{\boldsymbol{D}}$) Seja* $\mathbb{Z}_q^n \supseteq C_1 \supseteq \cdots \supseteq C_a$ *uma cadeia de códigos lineares. O conjunto* $\Gamma_{\overline{D}}$ *é definido da seguinte forma*

$$\Gamma_{\overline{D}} = q^a \mathbb{Z}^n + q^{a-1}\sigma(C_1) + \cdots + q^1 \sigma(C_{a-1}) + \sigma(C_a).$$

Observação 3.2.5. *Quando* $a = 1$, *temos que* $\Gamma_{\overline{D}} = \Lambda_A(C_1)$ *e, neste caso,* $\Gamma_{\overline{D}}$ *é um reticulado. Para* $a \geq 2$, *temos que* $\Gamma_{\overline{D}} \subseteq \mathbb{Z}^n$ *é um conjunto discreto, mas nem sempre é um reticulado (ver Exemplo 3.2.7).*

Definição 3.2.4. *Dada uma cadeia de códigos lineares* $\mathbb{Z}_q^n \supseteq C_1 \supseteq \cdots \supseteq C_a$, *denotamos por* $\Lambda_{\overline{D}}$ *o "menor" reticulado (com relação a inclusão) que contém o conjunto* $\Gamma_{\overline{D}}$ *dado na Definição 3.2.3. Em outras palavras,* $\Lambda_{\overline{D}}$ *é o (único) reticulado que contém* $\Gamma_{\overline{D}}$ *e satisfaz a seguinte propriedade: Se* Λ *é um reticulado em* $\mathbb{R}^n$ *que contém* $\Gamma_{\overline{D}}$, *então* $\Lambda_{\overline{D}} \subseteq \Lambda$.

Observação 3.2.6. *Uma caracterização dos elementos do reticulado $\Lambda_{\overline{D}}$ será apresentada no Teorema 3.2.7.*

Exemplo 3.2.7. *Considere novamente a cadeia de códigos lineares apresentada no Exemplo 3.2.6, isto é, $\mathbb{Z}_4^2 \supseteq C_1 \supseteq C_2$ tal que*

$$C_1 = \langle (2,2), (0,1) \rangle \ \ e \ \ C_2 = \langle (2,2) \rangle .$$

Observe que

$$\begin{aligned} \sigma(C_1) &= \{(0,0),(2,2),(0,1),(0,2),(0,3),(2,3),(2,0),(2,1)\} \ e \\ \sigma(C_2) &= \{(0,0),(2,2)\}. \end{aligned}$$

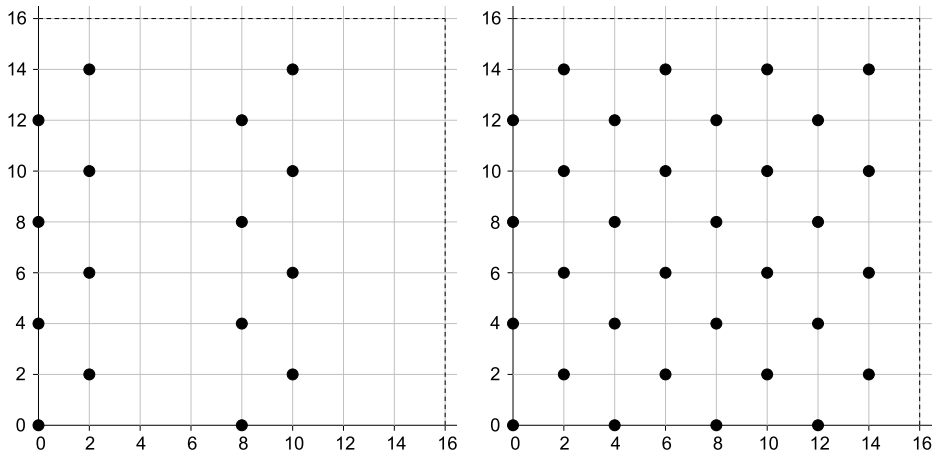
Como $\Gamma_{\overline{D}} = 4^2\mathbb{Z}^2 + 4^1\sigma(C_1) + 4^0\sigma(C_2)$, segue que

$$\Gamma_{\overline{D}} = \bigcup_{\boldsymbol{z} \in 16\mathbb{Z}^2} \left(\boldsymbol{z} + \Gamma_{\overline{D}} \cap [0,16)^2\right),$$

em que

$$\begin{aligned} \Gamma_{\overline{D}} \cap [0,16)^2 &= \{(0,0),(8,8),(0,4),(0,8),(0,12),(8,12),(8,0),(8,4),(2,2), \\ &\quad (10,10),(2,6),(2,10),(2,14),(10,14),(10,2),(10,6)\}. \end{aligned}$$

*Os elementos de $\Gamma_{\overline{D}} \cap [0,16)^2$ e $\Lambda_{\overline{D}} \cap [0,16)^2$ estão reprentados na Figura 3.4. Neste exemplo, temos que $\Gamma_{\overline{D}} \subsetneq \Lambda_{\overline{D}}$, isto é, $\Gamma_{\overline{D}}$ **não** é um reticulado.*



(a) $\Gamma_{\overline{D}} \cap [0,16)^2$ (b) $\Lambda_{\overline{D}} \cap [0,16)^2$

Figura 3.4: Elementos de $\Gamma_{\overline{D}}$ e $\Lambda_{\overline{D}}$ na caixa $[0,16)^2$

Exemplo 3.2.8. *Seja $\mathbb{Z}_4^2 \supseteq C_1 \supseteq C_2$ a cadeia de códigos lineares tal que $C_1 = \langle (1,1), (0,2) \rangle$*

e $C_2 = \langle (2,2) \rangle$. *Observe que*

$$\begin{aligned} \sigma(C_1) &= \{(0,0),(1,1),(2,2),(3,3),(0,2),(1,3),(2,0),(3,1)\} \text{ e} \\ \sigma(C_2) &= \{(0,0),(2,2)\}. \end{aligned}$$

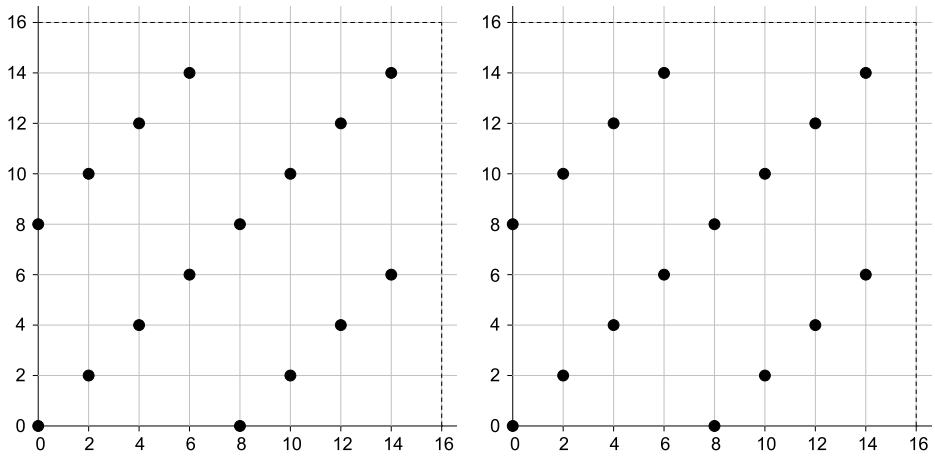
Como $\Gamma_{\overline{D}} = 4^2\mathbb{Z}^2 + 4^1\sigma(C_1) + 4^0\sigma(C_2)$, *segue que*

$$\Gamma_{\overline{D}} = \bigcup_{\boldsymbol{z} \in 16\mathbb{Z}^2} \left(\boldsymbol{z} + \Gamma_{\overline{D}} \cap [0,16)^2\right),$$

em que

$$\begin{aligned} \Gamma_{\overline{D}} \cap [0,16)^2 &= \{(0,0),(4,4),(8,8),(12,12),(0,8),(4,12),(8,0),(12,4), \\ &\quad (2,2),(6,6),(10,10),(14,14),(2,10),(6,14),(10,2),(14,6)\}. \end{aligned}$$

Os elementos de $\Gamma_{\overline{D}} \cap [0,16)^2$ *e* $\Lambda_{\overline{D}} \cap [0,16)^2$ *estão reprentados na Figura 3.5. Neste exemplo, temos que* $\Gamma_{\overline{D}} = \Lambda_{\overline{D}}$, *isto é,* $\Gamma_{\overline{D}}$ *é um reticulado.*



(a) $\Gamma_{\overline{D}} \cap [0,16)^2$ (b) $\Lambda_{\overline{D}} \cap [0,16)^2$

Figura 3.5: Elementos de $\Gamma_{\overline{D}}$ e $\Lambda_{\overline{D}}$ na caixa $[0,16)^2$

Observação 3.2.7. *O conjunto* $\Lambda_{\overline{D}}$ *é sempre um reticulado* q^a*-ário. Se* $\Gamma_{\overline{D}}$ *é um reticulado, então* $\Lambda_{\overline{D}} = \Gamma_{\overline{D}}$.

3.2.4 Conexões entre as Construções D, D′ e $\overline{\mathrm{D}}$

No próximo exemplo exploramos algumas relações entre as Construções D, D′ e $\overline{\mathrm{D}}$.

Exemplo 3.2.9. *Considere a cadeia de códigos lineares* $\mathbb{Z}_6^2 \supseteq C_1 \supseteq C_2$ *tal que* $C_1 =$

$\langle(1,2)\rangle$ *e* $C_2 = \langle(2,4)\rangle$. *Observe que*

$$\begin{aligned} C_1^{\perp} &= \{(x,y) \in \mathbb{Z}_6^2;\ x+2y=0\} \\ &= \{(0,0),(4,1),(2,2),(0,3),(4,4),(2,5)\} \\ &= \langle(4,1)\rangle \end{aligned}$$

e

$$\begin{aligned} C_2^{\perp} &= \{(x,y) \in \mathbb{Z}_6^2;\ 2x+4y=0\} \\ &= \{(0,0),(1,1),(4,1),(2,2),(5,2),(0,3), \\ &\quad (3,3),(1,4),(4,4),(2,5),(5,5),(3,0)\} \\ &= \langle(4,1),(3,0)\rangle\,. \end{aligned}$$

Escolhendo os parâmetros $k_1 = 2, k_2 = 1$, $r_1 = 1$, $r_2 = 2$ *e* $\boldsymbol{b}_1 = (2,4), \boldsymbol{b}_2 = (3,0), \boldsymbol{h}_1 = (4,1), \boldsymbol{h}_2 = (3,0) \in \mathbb{Z}_6^2$, *temos* $0 \leq k_2 \leq k_1$, $0 \leq r_1 \leq r_2$, $C_1 = \langle \boldsymbol{b}_1, \boldsymbol{b}_2\rangle$, $C_2 = \langle \boldsymbol{b}_1\rangle$, $C_1^{\perp} = \langle \boldsymbol{h}_1\rangle$ *e* $C_2^{\perp} = \langle \boldsymbol{h}_1, \boldsymbol{h}_2\rangle$. *Assim,*

$$\Lambda_D = \left\{ \boldsymbol{z} + \alpha_2^{(1)}(3,0) + \alpha_1^{(2)}\frac{1}{6}(2,4);\ \boldsymbol{z} \in 6\mathbb{Z}^2, 0 \leq \alpha_2^{(1)} \leq 5 \text{ e } 0 \leq \alpha_1^{(2)} \leq 35 \right\}$$

e

$$\Lambda_{D'} = \left\{ (x,y) \in \mathbb{Z}^2;\ 4x+y \equiv 0 \mod 36 \ \text{ e } \ 3x \equiv 0 \mod 6 \right\}.$$

Também,

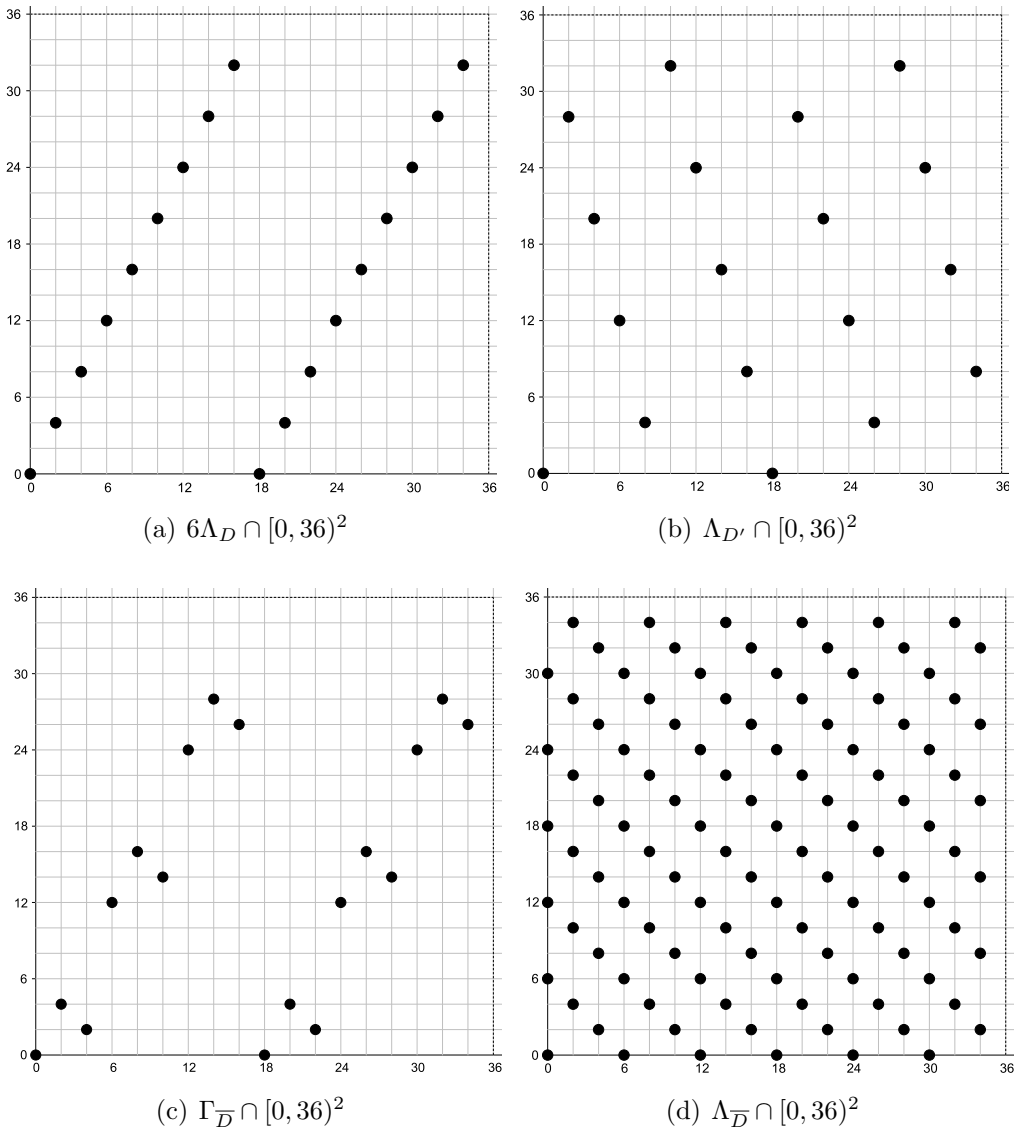
$$\Gamma_{\overline{D}} = 6^2\mathbb{Z}^2 + 6^1\sigma(C_1) + 6^0\sigma(C_2),$$

em que

$$\begin{aligned} \sigma(C_1) &= \{(0,0),(1,2),(2,4),(3,0),(4,2),(5,4)\} \\ \sigma(C_2) &= \{(0,0),(2,4),(4,2)\}. \end{aligned}$$

Portanto,

$$\begin{aligned} 6\Lambda_D &= \bigcup_{\boldsymbol{z} \in 36\mathbb{Z}^2} \left(\boldsymbol{z} + (6\Lambda_D) \cap [0,36)^2\right), \\ \Lambda_{D'} &= \bigcup_{\boldsymbol{z} \in 36\mathbb{Z}^2} \left(\boldsymbol{z} + \Lambda_{D'} \cap [0,36)^2\right), \\ \Gamma_{\overline{D}} &= \bigcup_{\boldsymbol{z} \in 36\mathbb{Z}^2} \left(\boldsymbol{z} + \Gamma_{\overline{D}} \cap [0,36)^2\right) \text{ e} \\ \Lambda_{\overline{D}} &= \bigcup_{\boldsymbol{z} \in 36\mathbb{Z}^2} \left(\boldsymbol{z} + \Lambda_{\overline{D}} \cap [0,36)^2\right), \end{aligned}$$



(a) $6\Lambda_D \cap [0,36)^2$ (b) $\Lambda_{D'} \cap [0,36)^2$

(c) $\Gamma_{\overline{D}} \cap [0,36)^2$ (d) $\Lambda_{\overline{D}} \cap [0,36)^2$

Figura 3.6: (Exemplo 3.2.9) Elementos de $6\Lambda_D$, $\Lambda_{D'}$, $\Gamma_{\overline{D}}$ e $\Lambda_{\overline{D}}$ na caixa $[0,36)^2$

Neste exemplo, observamos que (i) $\Gamma_{\overline{D}} \subsetneqq \Lambda_{\overline{D}}$, (ii) $6\Lambda_D \subsetneqq \Lambda_{\overline{D}}$, (iii) $6\Lambda_D \not\subset \Lambda_{D'}$, (iv) $\Lambda_{D'} \not\subset 6\Lambda_D$ *e* (v) $\Lambda_{D'} \subsetneqq \Lambda_{\overline{D}}$ *(ver Figura 3.6).*

Observação 3.2.8. *O reticulado* $\Lambda_{\overline{D}}$ *sempre contém* $q^{a-1}\Lambda_D$ *(Teorema 3.2.7), mas* $\Lambda_{D'}$ *nem sempre está contido em* $\Lambda_{\overline{D}}$*, conforme podemos verificar no próximo exemplo.*

Exemplo 3.2.10. *Seja* $\mathbb{Z}_4^2 \supseteq C_1 \supseteq C_2$ *a cadeia de códigos lineares tal que* $C_1 = \langle (1,1) \rangle$ *e* $C_2 = \langle (2,2) \rangle$ *. Observe que*

$$\begin{aligned} C_1^{\perp} &= \{(x,y) \in \mathbb{Z}_4^2; x+y=0\} \\ &= \{(0,0),(1,3),(2,2),(3,1)\} \\ &= \langle (1,3) \rangle \end{aligned}$$

e

$$\begin{aligned} C_2^{\perp} &= \{(x,y) \in \mathbb{Z}_4^2; 2x+2y=0\} \\ &= \{(0,0),(1,1),(1,3),(2,0),(2,2),(3,1),(3,3),(0,2)\} \\ &= \langle (1,3),(1,1) \rangle . \end{aligned}$$

Escolhendo $r_1 = 1$, $r_2 = 2$ *e* $\boldsymbol{h}_1 = (1,3), \boldsymbol{h}_2 = (1,1) \in \mathbb{Z}_4^2$, *temos que* $0 \leq r_1 \leq r_2$, $C_1^{\perp} = \langle \boldsymbol{h}_1 \rangle$ *e* $C_2^{\perp} = \langle \boldsymbol{h}_1, \boldsymbol{h}_2 \rangle$. *Assim,*

$$\Lambda_{D'} = \big\{(x,y) \in \mathbb{Z}^2;\ x+3y \equiv 0 \mod 16 \ \ e \ \ 2x \equiv 0 \mod 4\big\}.$$

Também,

$$\Gamma_{\overline{D}} = 4^2\mathbb{Z}^2 + 4^1\sigma(C_1) + 4^0\sigma(C_2),$$

em que

$$\begin{aligned} \sigma(C_1) &= \{(0,0),(1,1),(2,2),(3,3)\} \\ \sigma(C_2) &= \{(0,0),(2,2)\} \end{aligned}$$

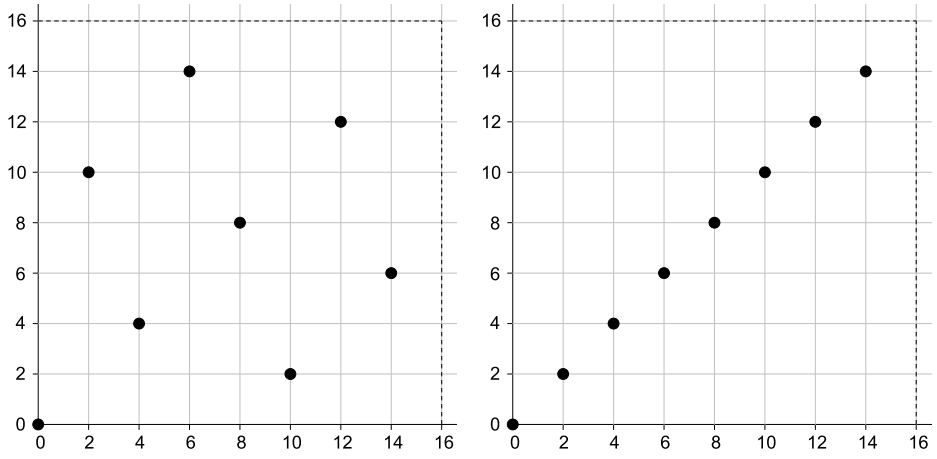
Temos que $\Gamma_{\overline{D}} = \Lambda_{\overline{D}}$,

$$\Lambda_{D'} \cap [0,16)^2 = \{(0,0),(2,10),(4,4),(6,14),(8,8),(10,2),(12,12),(14,6)\}$$

e

$$\Gamma_{\overline{D}} \cap [0,16)^2 = \{(0,0),(2,2),(4,4),(6,6),(8,8),(10,10),(12,12),(14,14)\}.$$

Os elementos de $\Gamma_{\overline{D}} \cap [0,16)^2$ *e* $\Lambda_{\overline{D}} \cap [0,16)^2$ *estão representados na Figura 3.7. Neste exemplo, temos que* $\Lambda_{D'} \not\subset \Lambda_{\overline{D}}$.



(a) $\Lambda_{D'} \cap [0,16)^2$ (b) $\Lambda_{\overline{D}} \cap [0,16)^2$

Figura 3.7: Elementos de $\Lambda_{D'}$ e $\Lambda_{\overline{D}}$ na caixa $[0,16)^2$

O próximo teorema e seu corolário estendem resultados de reticulados obtidos a partir de códigos binários [25] para reticulados obtidos a partir de códigos q-ários.

Teorema 3.2.7. *Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ uma cadeia de códigos lineares. Temos que (i) $q^{a-1}\Lambda_D \subseteq \Lambda_{\overline{D}}$ e (ii) $\Lambda_{\overline{D}}$ consiste de todos os vetores da forma*

$$q^a \boldsymbol{z} + \sum_{i=1}^{a} q^{a-i} \sum_{\boldsymbol{c}_j \in C_i} \alpha_j^{(i)} \sigma(\boldsymbol{c}_j),$$

em que $\alpha_j^{(i)} \in \{0, 1, \ldots, q-1\}$ e $\boldsymbol{z} \in \mathbb{Z}^n$.

Demonstração. (i) Dados $k_1 \geq k_2 \geq \cdots \geq k_a \geq 0$ e vetores $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1} \in \mathbb{Z}_q^n$ tais que $C_i = \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_i} \rangle$ para $i = 1, 2, \ldots, a$, considere o reticulado

$$\Lambda_D = \left\{ \boldsymbol{z} + \sum_{i=1}^{a} \sum_{j=1}^{k_i} \alpha_j^{(i)} \frac{1}{q^{i-1}} \sigma(\boldsymbol{b}_j);\ \boldsymbol{z} \in q\mathbb{Z}^n \text{ e } \alpha_j^{(i)} \in \{0, 1, \ldots, q-1\} \right\}.$$

Dado $\boldsymbol{w} \in q^{a-1}\Lambda_D$, existem $\boldsymbol{z} \in \mathbb{Z}^n$ e $\alpha_j^{(i)} \in \{0, 1, \ldots, q-1\}$ tais que

$$\boldsymbol{w} = q^a \boldsymbol{z} + \sum_{i=1}^{a} \sum_{j=1}^{k_i} \alpha_j^{(i)} q^{a-i} \sigma(\boldsymbol{b}_j).$$

Como $\Lambda_{\overline{D}}$ é um reticulado, $q^a \boldsymbol{z} \in q^a\mathbb{Z}^n \subseteq \Gamma_{\overline{D}} \subseteq \Lambda_{\overline{D}}$ e $q^{a-i}\sigma(\boldsymbol{b}_j) \in q^{a-i}\sigma(C_i) \subseteq \Gamma_{\overline{D}} \subseteq \Lambda_{\overline{D}}$, para $1 \leq i \leq a$ e $1 \leq j \leq k_i$, temos que $\boldsymbol{w} \in \Lambda_{\overline{D}}$.
(ii) Seja

$$\Lambda = \left\{ q^a \boldsymbol{z} + \sum_{i=1}^{a} q^{a-i} \sum_{\boldsymbol{c}_j \in C_i} \alpha_j^{(i)} \sigma(\boldsymbol{c}_j);\ \alpha_j^{(i)} \in \{0, 1, \ldots, q-1\} \text{ e } \boldsymbol{z} \in \mathbb{Z}^n \right\}.$$

É imediato que $\Gamma_{\overline{D}} \subseteq \Lambda$. Da igualdade

$$\sum_{i=1}^{a} q^{a-i} \sum_{\boldsymbol{c}_j \in C_i} \alpha_j^{(i)} \sigma(\boldsymbol{c}_j) = \sum_{i=1}^{a} q^{a-i} \sum_{\boldsymbol{c}_j \in C_i \setminus C_{i+1}} \mu_j^{(i)} \sigma(\boldsymbol{c}_j),$$

em que $\mu_j^{(i)} = \alpha_j^{(i)} + \alpha_j^{(i-1)} q + \cdots + \alpha_j^{(1)} q^{i-1}$, obtemos

$$\Lambda = \left\{ q^a \boldsymbol{z} + \sum_{i=1}^{a} q^{a-i} \sum_{\boldsymbol{c}_j \in C_i \setminus C_{i+1}} \mu_j^{(i)} \sigma(\boldsymbol{c}_j);\ \mu_j^{(i)} \in \{0, 1, \ldots, q^i - 1\} \text{ e } \boldsymbol{z} \in \mathbb{Z}^n \right\}.$$

Agora, note que $\mathbf{0} \in \Lambda$ e que dados $\boldsymbol{x}, \boldsymbol{y} \in \Lambda$, existem $\lambda_j^{(i)}, \mu_j^{(i)} \in \{0, 1, \ldots, q^i - 1\}$ e $\boldsymbol{z}_1, \boldsymbol{z}_2 \in \mathbb{Z}^n$ tais que

$$\boldsymbol{x} = q^a \boldsymbol{z}_1 + \sum_{i=1}^{a} q^{a-i} \sum_{\boldsymbol{c}_j \in C_i \setminus C_{i+1}} \mu_j^{(i)} \sigma(c_j) \quad \text{e} \quad \boldsymbol{y} = q^a \boldsymbol{z}_2 + \sum_{i=1}^{a} q^{a-i} \sum_{\boldsymbol{c}_j \in C_i \setminus C_{i+1}} \lambda_j^{(i)} \sigma(\boldsymbol{c}_j).$$

Assim,

$$\boldsymbol{x}-\boldsymbol{y}=q^a(\boldsymbol{z}_1-\boldsymbol{z}_2)+\sum_{i=1}^{a}q^{a-i}\sum_{\boldsymbol{c}_j\in C_i\setminus C_{i+1}}(\mu_j^{(i)}-\lambda_j^{(i)})\sigma(\boldsymbol{c}_j).$$

Aplicando o algoritmo da divisão, obtemos inteiros $\beta_j^{(i)}$ e $r_j^{(i)}$ tais que $0\leq r_j^{(i)}<q^i$ e $\mu_j^{(i)}-\lambda_j^{(i)}=\beta_j^{(i)}q^i+r_j^{(i)}$ e logo

$$\boldsymbol{x}-\boldsymbol{y}=q^a\boldsymbol{z}+\sum_{i=1}^{a}q^{a-i}\sum_{\boldsymbol{c}_j\in C_i\setminus C_{i+1}}r_j^{(i)}\sigma(\boldsymbol{c}_j),$$

em que

$$\boldsymbol{z}=\boldsymbol{z}_1-\boldsymbol{z}_2+\sum_{i=1}^{a}\sum_{\boldsymbol{c}_j\in C_i\setminus C_{i+1}}\beta_j^{(i)}\sigma(\boldsymbol{c}_j)\in\mathbb{Z}^n.$$

Logo $\boldsymbol{x}-\boldsymbol{y}\in\Lambda$ e portanto Λ é um reticulado. Resta mostrar que Λ é o menor reticulado em $\mathbb{R}^n$ que contém $\Gamma_{\overline{D}}$. Com efeito, seja $\Lambda'\subseteq\mathbb{R}^n$ um reticulado tal que $\Gamma_{\overline{D}}\subseteq\Lambda'$. Para cada $\boldsymbol{v}\in\Lambda$, existem $\alpha_j^{(i)}\in\{0,1,\ldots,q-1\}$ e $\boldsymbol{z}\in\mathbb{Z}^n$ tais que

$$\boldsymbol{v}=q^a\boldsymbol{z}+\sum_{i=1}^{a}q^{a-i}\sum_{\boldsymbol{c}_j\in C_i}\alpha_j^{(i)}\sigma(\boldsymbol{c}_j).$$

Como $q^a\boldsymbol{z}\in\Gamma_{\overline{D}}\subseteq\Lambda'$ e $q^{a-i}\sigma(\boldsymbol{c}_j)\in q^{a-i}\sigma(C_i)\subseteq\Gamma_{\overline{D}}\subseteq\Lambda'$ para todo $i\in\{1,2,\ldots,a\}$ e $\boldsymbol{c}_j\in C_i$, temos que $\boldsymbol{v}\in\Lambda'$. Isto mostra que Λ é o menor reticulado contendo $\Gamma_{\overline{D}}$. □

Definição 3.2.5. *(**Produto de Schur em** $\mathbb{Z}_q^n$) Dados* $\boldsymbol{x}=(x_1,\ldots,x_n)$ *e* $\boldsymbol{y}=(y_1,\ldots,y_n)$ *em* $\mathbb{Z}_q^n$*, o produto de Schur entre* $\boldsymbol{x}$ *e* $\boldsymbol{y}$ *é definido como*

$$\boldsymbol{x}\star\boldsymbol{y}=(x_1y_1,\ldots,x_ny_n),$$

onde a operação no lado direito da igualdade acima denota o produto usual em $\mathbb{Z}_q$*.*

Observação 3.2.9. *O produto de Schur também é conhecido como* ***multiplicação componente a componente****.*

Definição 3.2.6. *Uma cadeia de códigos lineares* $\mathbb{Z}_q^n\supseteq C_1\supseteq C_2\supseteq\cdots\supseteq C_a$ *é dita* ***fechada sob o produto de Schur*** *quando o produto de Schur de quaisquer dois elementos de* C_i *sempre pertence a* C_{i-1} *para* $i=2,\ldots,a$*, isto é, se* $\boldsymbol{c}_1,\boldsymbol{c}_2\in C_i$ *então* $\boldsymbol{c}_1\star\boldsymbol{c}_2\in C_{i-1}$ *para* $i=2,\ldots,a$*.*

Observação 3.2.10. *O conjunto* $\Gamma_{\overline{D}}$ *obtido via Construção* $\overline{D}$ *a partir de uma cadeia de códigos binários encaixados é um reticulado se, e somente se, a cadeia utilizada é fechada sob o produto de Schur [25]. No próximo exemplo mostramos que quando* $q\neq 2$ *este resultado nem sempre é válido. Observamos que nem mesmo quando* q *é primo (e consequentemente* $\mathbb{Z}_q$ *é um corpo) podemos garantir o resultado.*

Exemplo 3.2.11. *Considere a cadeia de códigos lineares* $\mathbb{Z}_5^4 \supseteq C_1 \supseteq C_2$ *tal que*

$$\begin{aligned} C_1 &= \langle (1,2,3,4),(1,4,4,1)\rangle \ \ e \\ C_2 &= \langle (1,2,3,4)\rangle . \end{aligned}$$

Esta cadeia de códigos é fechada sob o produto de Schur, mas o conjunto $\Gamma_{\overline{D}}$ *obtido via Construção* $\overline{D}$ *a partir desta cadeia não é um reticulado. De fato, note que*

$$C_2 = \{(0,0,0,0),(1,2,3,4),(2,4,1,3),(3,1,4,2),(4,3,2,1)\}$$

e logo

$$\begin{aligned} \{\boldsymbol{x} \star \boldsymbol{y};\ \boldsymbol{x},\boldsymbol{y} \in C_2\} &= \{(0,0,0,0),(1,4,4,1),(2,3,3,2),(3,2,2,3),(4,1,1,4)\} \\ &= \langle (1,4,4,1)\rangle \subseteq C_1. \end{aligned}$$

Logo a cadeia $\mathbb{Z}_5^4 \supseteq C_1 \supseteq C_2$ *é fechada sob o produto de Schur. Por outro lado,* $\boldsymbol{v} = (1,2,3,4)$, $\boldsymbol{w} = (1,4,4,1) \in C_1$ *e* $\sigma(\boldsymbol{v}), \sigma(\boldsymbol{w}), \sigma(\boldsymbol{v}+\boldsymbol{w}) \in \Gamma_{\overline{D}}$, *mas* $\sigma(\boldsymbol{v}) + \sigma(\boldsymbol{w}) - \sigma(\boldsymbol{v} + \boldsymbol{w}) = (0,5,5,5) \notin \Gamma_{\overline{D}}$. *Caso contrário, existiriam* $\boldsymbol{c}_1 \in C_1, \boldsymbol{c}_2 \in C_2$ *e* $\boldsymbol{z} \in \mathbb{Z}^n$ *tais que* $(0,5,5,5) = 25\boldsymbol{z} + 5\sigma(\boldsymbol{c}_1) + \sigma(\boldsymbol{c}_2)$ *e logo teríamos* $\boldsymbol{c}_1 = (0,1,1,1)$, *mas* $(0,1,1,1) \notin C_1$. *Portanto* $\Gamma_{\overline{D}}$ *não é um reticulado.*

Tendo em vista as observações acima, propomos a seguinte operação em $\mathbb{Z}_q^n$.

Definição 3.2.7. *(**Adição zero-um em** $\mathbb{Z}_q^n$) Dados* $\boldsymbol{x} = (x_1,\ldots,x_n)$ *e* $\boldsymbol{y} = (y_1,\ldots,y_n)$ *em* $\mathbb{Z}_q^n$, *a adição zero-um entre* $\boldsymbol{x}$ *e* $\boldsymbol{y}$ *é dada por*

$$\boldsymbol{x} * \boldsymbol{y} = (x_1 * y_1, \ldots, x_n * y_n) \in \mathbb{Z}_q^n,$$

onde

$$x_i * y_i = \begin{cases} 0, & se \quad \sigma(x_i) + \sigma(y_i) < q \\ 1, & se \quad \sigma(x_i) + \sigma(y_i) \geq q, \end{cases}$$

para todo $i \in \{1,\ldots,n\}$.

Lema 3.2.2. *Para* $\boldsymbol{x},\boldsymbol{y} \in \mathbb{Z}_q^n$, *tem-se* $\sigma(\boldsymbol{x}) + \sigma(\boldsymbol{y}) = \sigma(\boldsymbol{x}+\boldsymbol{y}) + q\sigma(\boldsymbol{x} * \boldsymbol{y})$.

Demonstração. Dados $\boldsymbol{x} = (x_1,\ldots,x_n), \boldsymbol{y} = (y_1,\ldots,y_n) \in \mathbb{Z}_q^n$, temos que

$$\sigma(x_i) + \sigma(y_i) = \sigma(x_i + y_i) + q\sigma(x_i * y_i).$$

Logo

$$\begin{aligned} q\sigma(\boldsymbol{x}*\boldsymbol{y}) &= q\big(\sigma(x_1*y_1),\ldots,\sigma(x_n*y_n)\big) = \big(q\sigma(x_1*y_1),\ldots,q\sigma(x_n*y_n)\big) \\ &= \big(\sigma(x_1)+\sigma(y_1)-\sigma(x_1+y_1),\ldots,\sigma(x_n)+\sigma(y_n)-\sigma(x_n+y_n)\big) \\ &= \big(\sigma(x_1),\ldots,\sigma(x_n)\big)+\big(\sigma(y_1),\ldots,\sigma(y_n)\big)-\big(\sigma(x_1+y_1),\ldots,\sigma(x_n+y_n)\big) \\ &= \sigma(\boldsymbol{x})+\sigma(\boldsymbol{y})-\sigma(\boldsymbol{x}+\boldsymbol{y}). \end{aligned}$$

Isto mostra o resultado. □

Observação 3.2.11. *Quando $q=2$ a adição zero-um coincide com o produto de Schur.*

Definição 3.2.8. *Uma cadeia de códigos lineares $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ é dita* ***fechada sob a adição zero-um*** *quando a adição zero-um de quaisquer dois elementos de C_i sempre pertence a C_{i-1} para $i=2,\ldots,a$, isto é, se $\boldsymbol{c}_1,\boldsymbol{c}_2 \in C_i$ então $\boldsymbol{c}_1*\boldsymbol{c}_2 \in C_{i-1}$ para $i=2,\ldots,a$.*

Exemplo 3.2.12. *A cadeia $\mathbb{Z}_3^2 \supseteq C_1 \supseteq C_2$ tal que $C_1=C_2=\langle(1,2)\rangle$ não é fechada sob a adição zero-um, pois $(1,2)\in C_2$ e $(1,2)*(1,2)=(0,1)\notin C_1$.*

Exemplo 3.2.13. *A cadeia de códigos lineares $\mathbb{Z}_5^4 \supseteq C_1 \supseteq C_2$ apresentada no Exemplo 3.2.11 não é fechada sob a adição zero-um. Caso contrário, como $(1,2,3,4)$, $(2,4,1,3)$, $(3,1,4,2)\in C_2$ e*

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

teríamos $(1,0,1,0),(0,1,0,1),(0,0,1,1)\in C_1$ e portanto $\dim C_1 \geq 3$ (Contradição!).

Lema 3.2.3. *Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ uma cadeia de códigos lineares. Se $\boldsymbol{w}\in\mathbb{Z}_q^n \setminus C_i$, então $q^{a-i}\sigma(\boldsymbol{w})\notin \Gamma_{\overline{D}}$.*

Demonstração. Seja $\boldsymbol{w}\in\mathbb{Z}_q^n$ e suponha que $q^{a-i}\sigma(\boldsymbol{w})\in\Gamma_{\overline{D}}$, isto é, que existem $\boldsymbol{c}_\ell\in C_\ell$, $1\leq\ell\leq a$, e $\boldsymbol{z}\in\mathbb{Z}^n$ tais que

$$q^{a-i}\sigma(\boldsymbol{w}) = q^a\boldsymbol{z}+q^{a-1}\sigma(\boldsymbol{c}_1)+\cdots+q^{a-i+1}\sigma(\boldsymbol{c}_{i-1})+q^{a-i}\sigma(\boldsymbol{c}_i)+\cdots+q^0\sigma(\boldsymbol{c}_0). \quad (3.1)$$

Dividindo cada uma das componentes de ambos os membros da Igualdade (3.1) por q^{a-i+1} e usando a unicidade da divisão em $\mathbb{Z}$, obtemos

$$q^{a-i}\sigma(\boldsymbol{w}) = q^{a-i}\sigma(\boldsymbol{c}_i)+\cdots+q^0\sigma(\boldsymbol{c}_0). \quad (3.2)$$

Agora, dividindo ambos os membros da Igualdade (3.2) por q^{a-i} e usando novamente a unicidade da divisão em $\mathbb{Z}$, obtemos

$$\sigma(\boldsymbol{w}) = \sigma(\boldsymbol{c}_i).$$

Isto mostra que $\boldsymbol{w} \in C_i$, pois $\boldsymbol{c}_i \in C_i$. □

No próximo teorema, fornecemos uma condição necessária e suficiente para que o conjunto $\Gamma_{\overline{D}}$ obtido via Construção $\overline{\mathrm{D}}$ seja um reticulado. Este teorema e seus corolários estendem para reticulados obtidos a partir de códigos q-ários resultados apresentados em [25] para reticulados obtidos a partir de códigos binários.

Teorema 3.2.8. *Dada uma cadeia de códigos lineares $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$, as seguintes afirmações são equivalentes:*

1. *$\Gamma_{\overline{D}}$ é um reticulado.*
2. *$\Gamma_{\overline{D}} = \Lambda_{\overline{D}}$.*
3. *$\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ é fechada sob a adição zero-um.*
4. *$\Gamma_{\overline{D}} = q^{a-1}\Lambda_D$.*

Demonstração. É fácil ver que $4 \Rightarrow 1 \Rightarrow 2$. Assim, basta mostrar que $2 \Rightarrow 3$ e $3 \Rightarrow 4$.
$(2 \Rightarrow 3)$ Suponha que a cadeia $\mathbb{Z}_q^n = C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ não é fechada sob a adição zero-um. Ou seja, existem $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C_i$ tais que $\boldsymbol{c}_1 * \boldsymbol{c}_2 \notin C_{i-1}$ para algum $i \in \{2, 3, \ldots, a\}$. Aplicando o Lema 3.2.3, obtemos

$$q^{a-i+1}\sigma(\boldsymbol{c}_1 * \boldsymbol{c}_2) \notin \Gamma_{\overline{D}}.$$

Por outro lado, usando o Lema 3.2.2, temos que

$$q\sigma(\boldsymbol{c}_1 * \boldsymbol{c}_2) = \sigma(\boldsymbol{c}_1) + \sigma(\boldsymbol{c}_2) - \sigma(\boldsymbol{c}_1 + \boldsymbol{c}_2).$$

Multiplicando ambos os membros da igualdade acima por q^{a-i}, obtemos

$$q^{a-i+1}\sigma(\boldsymbol{c}_1 * \boldsymbol{c}_2) = q^{a-i}\sigma(\boldsymbol{c}_1) + q^{a-i}\sigma(\boldsymbol{c}_2) - q^{a-i}\sigma(\boldsymbol{c}_1 + \boldsymbol{c}_2) \in \Lambda_{\overline{D}},$$

uma vez que $\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_1 + \boldsymbol{c}_2 \in C_i$. Portanto $\Gamma_{\overline{D}} \neq \Lambda_{\overline{D}}$.
$(3 \Rightarrow 4)$ Esta demonstração será feita por indução sobre a. Se $a = 1$ o resultado é trivial, pois Λ_D e $\Gamma_{\overline{D}}$ coincidem com o reticulado obtido via Construção A a partir de C_1. Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ uma cadeia de códigos lineares fechada sob a adição zero-um. Aplicando a hipótese de indução para $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_{a-1}$, obtemos

$$\Gamma'_{\overline{D}} = q^{a-1}\Lambda'_D, \tag{3.3}$$

em que

$$\Gamma'_{\overline{D}} = q^a\mathbb{Z}^n + q^{a-1}\sigma(C_1) + \cdots + q^{a-i}\sigma(C_i) + \cdots + q^1\sigma(C_{a-1}).$$

e

$$q^{a-1}\Lambda'_D = \left\{ q^a\boldsymbol{z} + \sum_{i=1}^{a-1} q^{a-i} \sum_{j=1}^{k_i} \alpha_j^{(i)}\sigma(\boldsymbol{b}_j);\ \alpha_j^{(i)} \in \{0,1,\ldots,q-1\} \text{ e } \boldsymbol{z} \in \mathbb{Z}^n \right\}.$$

A partir daqui denotaremos por Λ o reticulado dado em (3.3). Para finalizar a demonstração, devemos mostrar que o conjunto

$$\Gamma_{\overline{D}} = \Lambda + \sigma(C_a) = \{\boldsymbol{v} + \sigma(\boldsymbol{c});\ \boldsymbol{v} \in \Lambda \text{ e } \boldsymbol{c} \in C_0\}$$

é igual a

$$q^{a-1}\Lambda_D = \left\{ \boldsymbol{v} + \sum_{j=1}^{k_a} \alpha_j^{(a)}\sigma(b_j);\ \boldsymbol{v} \in \Lambda \text{ e } \alpha_j^{(a)} \in \{0,1,\ldots,q-1\} \right\}.$$

E para isto, basta mostrar que se $\boldsymbol{c} \in C_a$, ou seja, se existem índices $1 \leq j_1, \ldots, j_s \leq k_a$ tais que $\boldsymbol{c} = \boldsymbol{b}_{j_1} + \cdots + \boldsymbol{b}_{j_s}$, então

$$\sigma(\boldsymbol{b}_{j_1}) + \cdots + \sigma(\boldsymbol{b}_{j_s}) = \boldsymbol{v} + \sigma(\boldsymbol{c}),$$

para algum $\boldsymbol{v} \in \Lambda$. Com efeito, o caso $s = 1$ é trivial, pois $\boldsymbol{c} = \boldsymbol{b}_{j_1} \in C_a$, $\mathbf{0} \in \Lambda$ e

$$\sigma(\boldsymbol{b}_{j_1}) = \mathbf{0} + \sigma(\boldsymbol{b}_{j_1}).$$

Agora, seja $\boldsymbol{c} = \boldsymbol{b}_{j_1} + \cdots + \boldsymbol{b}_{j_s}$, com $s > 1$ e $1 \leq j_1, \ldots, j_s \leq k_a$. Pela hipótese de indução, existe um vetor $\boldsymbol{v}' \in \Lambda$ tal que

$$\sigma(\boldsymbol{b}_{j_1}) + \cdots + \sigma(\boldsymbol{b}_{j_{s-1}}) = \boldsymbol{v}' + \sigma(\boldsymbol{c}'),$$

em que $\boldsymbol{c}' = \boldsymbol{b}_{j_1} + \cdots + \boldsymbol{b}_{j_{s-1}}$. Aplicando o Lema 3.2.2, obtemos

$$\begin{aligned} \sigma(\boldsymbol{b}_{j_1}) + \cdots + \sigma(\boldsymbol{b}_{j_{s-1}}) + \sigma(\boldsymbol{b}_{j_s}) &= \boldsymbol{v}' + \sigma(\boldsymbol{c}') + \sigma(\boldsymbol{b}_{j_s}) \\ &= \boldsymbol{v}' + \sigma(\boldsymbol{c}' + \boldsymbol{b}_{j_s}) + q\sigma(\boldsymbol{c}' * \boldsymbol{b}_{j_s}) \\ &= \boldsymbol{v}' + \sigma(\boldsymbol{c}) + q\sigma(\boldsymbol{c}' * \boldsymbol{b}_{j_s}). \end{aligned}$$

Como $C_{a-1} \supseteq C_a$ é fechada sob a adição zero-um, temos que $\boldsymbol{c}' * \boldsymbol{b}_{j_s} \in C_{a-1}$ e consequentemente $q\sigma(\boldsymbol{c}' * \boldsymbol{b}_{j_s}) \in \Lambda$. Portanto

$$\sigma(\boldsymbol{b}_{j_1}) + \cdots + \sigma(\boldsymbol{b}_{j_s}) = \boldsymbol{v} + \sigma(\boldsymbol{c}),$$

em que $\boldsymbol{v} = \boldsymbol{v}' + q\sigma(\boldsymbol{c}' * \boldsymbol{b}_{j_s}) \in \Lambda$. □

Corolário 3.2.5. *Se uma cadeia de códigos lineares $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ é fechada sob a adição zero-um, salvo por um fator de escala, as Construções D e $\overline{D}$ geram o mesmo reticulado.*

Corolário 3.2.6. *Se uma cadeia de códigos lineares $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ é fechada sob a adição zero-um, então o reticulado obtido via Construção D não depende da escolha dos parâmetros $k_1, k_2, \ldots, k_a$ e $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1}$.*

Exemplo 3.2.14. *Considere a cadeia de códigos lineares $\mathbb{Z}_5^4 \supseteq C_1 \supseteq C_2$ tal que*

$$\begin{aligned} C_1 &= \langle (1,0,1,0), (0,1,0,1), (0,0,1,1) \rangle \text{ e} \\ C_2 &= \langle (1,2,3,4) \rangle . \end{aligned}$$

Temos que $C_2 = \{(0,0,0,0), (1,2,3,4), (2,4,1,3), (3,1,4,2), (4,3,2,1)\}$ e consequentemente

$$\begin{aligned} \{\boldsymbol{x} * \boldsymbol{y};\ \boldsymbol{x}, \boldsymbol{y} \in C_2\} &= \{(0,0,0,0), (1,0,1,0), (0,1,0,1), \\ &\quad (0,0,1,1), (1,1,1,1), (1,1,0,0)\} \subseteq C_1. \end{aligned}$$

Logo a cadeia $\mathbb{Z}_5^4 \supseteq C_1 \supseteq C_2$ é fechada sob a adição zero-um. Do Teorema 3.2.8, segue que o conjunto $\Gamma_{\overline{D}}$ obtido a partir desta cadeia é um reticulado e $\Gamma_{\overline{D}} = 5\Lambda_D$. Além disso, o reticulado Λ_D não depende da escolha dos parâmetros (Corolário 3.2.6). Assim, escolhendo como parâmetros $k_1 = 3$, $k_2 = 1$,

$$\begin{aligned} \boldsymbol{b}_1 &= (1,2,3,4), \\ \boldsymbol{b}_2 &= (0,1,0,1) \text{ e} \\ \boldsymbol{b}_3 &= (0,0,1,1), \end{aligned}$$

temos que $C_1 = \langle \boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3 \rangle$ e $C_1 = \langle \boldsymbol{b}_1 \rangle$. Note que estes vetores satisfazem as hipóteses do Teorema 3.2.5. Logo

$$\{(1/5, 2/5, 3/5, 4/5), (0,1,0,1), (0,0,1,1), (0,0,0,5)\}$$

é uma base para Λ_D e consequentemente

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 5 & 0 & 5 \\ 0 & 0 & 5 & 5 \\ 0 & 0 & 0 & 25 \end{pmatrix}$$

é uma matriz geradora para $\Gamma_{\overline{D}} = \Lambda_{\overline{D}}$.

Observação 3.2.12. *A cadeia usada no exemplo anterior não é fechada sob o produto de Schur, uma vez que* $(1,2,3,4) \in C_2$ *e*

$$(1,2,3,4) \star (1,2,3,4) = (1,4,4,1) \notin C_1.$$

Os próximos dois lemas estendem para códigos q-ários resultados conhecidos anteriormente para Construções D e D′ a partir de códigos binários [37, 50].

Lema 3.2.4. *Seja* H *a matriz* $k_1 \times n$*, cujas linhas são*

$$\sigma(\boldsymbol{b}_1), \ldots, \sigma(\boldsymbol{b}_{k_a}), q\sigma(\boldsymbol{b}_{k_a+1}), \ldots, q\sigma(\boldsymbol{b}_{k_{a-1}}), \ldots, q^{a-1}\sigma(\boldsymbol{b}_{k_2+1}), \ldots, q^{a-1}\sigma(\boldsymbol{b}_{k_1}).$$

Temos que $\boldsymbol{x} \in \Lambda_D^*$ *se, e somente se,* $q\boldsymbol{x} \in \mathbb{Z}^n$ *e* $H\boldsymbol{x}^t \equiv \boldsymbol{0} \mod q^{a-1}$.

Demonstração. Por definição, $\Lambda_D^* = \{\boldsymbol{x} \in \mathbb{R}^n; \langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z}, \forall \boldsymbol{y} \in \Lambda_D\}$. Usando o Teorema 3.2.1, obtemos que $\boldsymbol{x} \in \Lambda_D^*$ se, e somente se, $\langle \boldsymbol{x}, q\boldsymbol{z} \rangle \in \mathbb{Z}$ e $\langle \boldsymbol{x}, (1/q^{i-1})\sigma(b_j) \rangle \in \mathbb{Z}$ para $1 \leq i \leq a$, $k_{i+1} < j \leq k_i$ e para todo $\boldsymbol{z} \in \mathbb{Z}^n$. Logo

$$\boldsymbol{x} \in \Lambda_D^* \quad \text{se, e somente se,} \quad q^{a-i} \langle \boldsymbol{x}, \sigma(\boldsymbol{b}_j) \rangle \equiv q^a \langle \boldsymbol{x}, \boldsymbol{e}_t \rangle \equiv \boldsymbol{0} \mod q^{a-1}$$

para $1 \leq i \leq a$, $k_{i+1} < j \leq k_i$ e $1 \leq t \leq n$, em que $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ é a base canônica do $\mathbb{R}^n$. Portanto $\boldsymbol{x} \in \Lambda_D^*$ se, e somente se, $q\boldsymbol{x} \in \mathbb{Z}^n$ e $H\boldsymbol{x}^t \equiv \boldsymbol{0} \mod q^{a-1}$. □

Lema 3.2.5. *Seja* H *a matriz* $r_a \times n$*, cujas linhas são*

$$\sigma(\boldsymbol{h}_1), \ldots, \sigma(\boldsymbol{h}_{r_1}), q\sigma(\boldsymbol{h}_{r_1+1}), \ldots, q\sigma(\boldsymbol{h}_{r_2}), \ldots, q^{a-1}\sigma(\boldsymbol{h}_{r_{a-1}+1}), \ldots, q^{a-1}\sigma(\boldsymbol{h}_{r_a}).$$

Temos que $\boldsymbol{x} \in \Lambda_{D'}$ *se, e somente se,* $\boldsymbol{x} \in \mathbb{Z}^n$ *e* $H\boldsymbol{x}^t \equiv \boldsymbol{0} \mod q^a$.

Demonstração. Basta observar que $\boldsymbol{x} \in \Lambda_{D'}$ se, e somente se, $\boldsymbol{x} \in \mathbb{Z}^n$ e $q^{a-i}\boldsymbol{x} \cdot \sigma(\boldsymbol{h}_j) \equiv \boldsymbol{0} \mod q^a$ para $0 < i \leq a$ e $r_{a-i} < j \leq r_{a-i+1}$. Logo $\boldsymbol{x} \in \Lambda_{D'}$ se, e somente se, $\boldsymbol{x} \in \mathbb{Z}^n$ e $H\boldsymbol{x}^t \equiv \boldsymbol{0} \mod q^a$. □

Dada uma cadeia $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ de códigos lineares e parâmetros $0 \leq r_1 \leq r_2 \leq \cdots \leq r_a$ e $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_a} \in \mathbb{Z}_q^n$ tais que $C_i^\perp = \langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_i} \rangle$ para $i = 1, 2, \ldots, a$, considere o reticulado $\Lambda_{D^\perp}$ obtido via Construção D a partir da cadeia $C_1^\perp \subseteq C_2^\perp \subseteq \cdots \subseteq C_a^\perp \subseteq \mathbb{Z}_q^n$ (usando os parâmetros $r_1, r_2, \ldots, r_a, \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_a}$), isto é,

$$\Lambda_{D^\perp} = \left\{ q\boldsymbol{z} + \sum_{i=1}^{a} \sum_{j=r_{a-i}+1}^{r_{a-i+1}} \alpha_j^{(i)} \frac{1}{q^{i-1}} \sigma(\boldsymbol{h}_j);\ \boldsymbol{z} \in \mathbb{Z}^n \text{ e } \alpha_j^{(i)} \in \{0, 1, \ldots, q^i - 1\} \right\}.$$

Considere também o reticulado $\Lambda_{D'}$ obtido via Construção D′ a partir da cadeia $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ (usando os mesmos parâmetros $r_1, r_2, \ldots, r_a, \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_a}$), isto é,

$$\Lambda_{D'} = \left\{ \boldsymbol{x} \in \mathbb{Z}^n;\ \boldsymbol{x} \cdot \sigma(\boldsymbol{h}_j) \equiv \boldsymbol{0} \mod q^{i+1}, 0 \leq i < a \text{ e } r_{a-i-1} < j \leq r_{a-i} \right\}$$

no qual $r_0 = 0$. Nestas condições, obtemos os seguintes resultados.

Teorema 3.2.9. *Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ uma cadeia de códigos lineares. Temos que $\Lambda_{D'} = q\Lambda_{D^\perp}^*$. Além disso, M é uma matriz geradora de $\Lambda_{D^\perp}$ se, e somente se, $q(M^t)^{-1}$ é uma matriz geradora de $\Lambda_{D'}$.*

Demonstração. Seja H a matriz, cujas linhas são

$$\sigma(\boldsymbol{h}_1), \ldots, \sigma(\boldsymbol{h}_{r_1}), q\sigma(\boldsymbol{h}_{r_1+1}), \ldots, q\sigma(\boldsymbol{h}_{r_2}), \ldots, q^{a-1}\sigma(\boldsymbol{h}_{r_{a-1}+1}), \ldots, q^{a-1}\sigma(\boldsymbol{h}_{r_a}).$$

Temos que

$$\begin{aligned} \boldsymbol{y} \in q\Lambda_{D^\perp}^* &\overset{\text{Lema 3.2.4}}{\iff} \boldsymbol{y} = q\boldsymbol{x}, q\boldsymbol{x} \in \mathbb{Z}^n \text{ e } H\boldsymbol{x}^t \equiv \boldsymbol{0} \mod q^{a-1} \\ &\iff \boldsymbol{y} \in \mathbb{Z}^n \text{ e } H\boldsymbol{y}^t \equiv \boldsymbol{0} \mod q^a \\ &\overset{\text{Lema 3.2.5}}{\iff} \boldsymbol{y} \in \Lambda_{D'}. \end{aligned}$$

Logo $\Lambda_{D'} = q\Lambda_{D^\perp}^*$. Pelo Teorema 1.2.1, temos que M é uma matriz geradora de $\Lambda_{D^\perp}$ se, e somente se, $(M^t)^{-1}$ é uma matriz geradora de $\Lambda_{D^\perp}^*$. Portanto M é uma matriz geradora de $\Lambda_{D^\perp}$ se, e somente se, $q(M^t)^{-1}$ é uma matriz geradora de $\Lambda_{D'}$, já que $\Lambda_{D'} = q\Lambda_{D^\perp}^*$. □

Corolário 3.2.7. *A cadeia $C_1^\perp \subseteq C_2^\perp \subseteq \cdots \subseteq C_a^\perp \subseteq \mathbb{Z}_q^n$ é fechada sob a adição zero-um se, e somente se, $\Lambda_{D'} = q^a\Gamma_{\overline{D}^\perp}^* = q^a\Lambda_{\overline{D}^\perp}^*$, onde $\Gamma_{\overline{D}^\perp}$ e $\Lambda_{\overline{D}^\perp}$ são obtidos via Construção $\overline{D}$ a partir da cadeia $C_1^\perp \subseteq C_2^\perp \subseteq \cdots \subseteq C_a^\perp \subseteq \mathbb{Z}_q^n$.*

Demonstração. O Teorema 3.2.8 afirma que a cadeia $C_1^\perp \subseteq C_2^\perp \subseteq \cdots \subseteq C_a^\perp \subseteq \mathbb{Z}_q^n$ é fechada sob a adição zero-um se e, somente se, $\Lambda_{\overline{D}^\perp} = \Gamma_{\overline{D}^\perp} = q^{a-1}\Lambda_{D^\perp}$. Por outro lado, do Corolário 1.2.2 e Teorema 3.2.9 temos que $\Gamma_{\overline{D}^\perp} = \Lambda_{\overline{D}^\perp} = q^{a-1}\Lambda_{D^\perp}$ se, e somente se, $\Gamma_{\overline{D}^\perp}^* = \Lambda_{\overline{D}^\perp}^* = (q^{a-1}\Lambda_{D^\perp})^* = (1/q^{a-1})\Lambda_{D^\perp}^* = (1/q^a)\Lambda_{D'}$. Logo a cadeia $C_1^\perp \subseteq C_2^\perp \subseteq \cdots \subseteq C_a^\perp \subseteq \mathbb{Z}_q^n$ é fechada sob a adição zero-um se, e somente se, $\Lambda_{D'} = q^a\Gamma_{\overline{D}^\perp}^* = q^a\Lambda_{\overline{D}^\perp}^*$. □

Corolário 3.2.8. *Sejam $0 \leq r_1 \leq \cdots \leq r_a$ e $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_a} \in \mathbb{Z}_q^n$ vetores não nulos tais que*

1. *$C_\ell^\perp = \langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_\ell} \rangle$ para $\ell = 1, \ldots, a$.*
2. *Alguma permutação das linhas da matriz $[\sigma(\boldsymbol{h}_1) \ \cdots \ \sigma(\boldsymbol{h}_{r_a})]^t$ forma uma matriz triangular superior (resp. inferior) na forma escalonada.*
3. *Para cada $j \in \{1, \ldots, r_a\}$, a primeira (resp. última) componente não nula do vetor $\sigma(\boldsymbol{h}_j)$, denotada por α_j, divide q e todas as demais componentes do mesmo.*

Seja M a (única) matriz triangular superior (resp. inferior) cujas linhas são os r_a vetores $(1/q^{i-1})\sigma(\boldsymbol{h}_j)$, $1 \leq i \leq a$ e $r_{a-i} < j \leq r_{a-i+1}$, mais $n - r_a$ vetores do tipo $(0, \ldots, 0, q, 0, \ldots, 0)$. Nestas condições, $q(M^t)^{-1}$ é uma matriz geradora para $\Lambda_{D'}$ e

$$\det \Lambda_{D'} = \left(\prod_{j=1}^{r_a} \alpha_j \right)^{-2} \left(q^2 \right)^{\sum_{\ell=1}^{a} r_\ell}.$$

Em particular, quando $q = 2$ temos $\det \Lambda_{D'} = 4^{\sum_{\ell=1}^{a} r_\ell}$.

Demonstração. Pelos Teoremas 3.2.5 e 3.2.9, M é uma matriz geradora de $\Lambda_D^\perp$ e $q(M^t)^{-1}$ é uma matriz geradora de $\Lambda_{D'}$. Aplicando o Corolário 3.2.2, obtemos

$$\det \Lambda_D^\perp = \det (MM^t) = \left(\prod_{j=1}^{r_a} \alpha_j \right)^2 \left(q^2 \right)^{n - \sum_{\ell=1}^{a} r_\ell}.$$

Como $\det \Lambda_{D'} = \det [q(M^t)^{-1}(q(M^t)^{-1})^t] = (q^2)^n \det (MM^t)^{-1} = (q^2)^n (\det \Lambda_{D^\perp})^{-1}$, segue que

$$\det \Lambda_{D'} = \left(\prod_{j=1}^{r_a} \alpha_j \right)^{-2} \left(q^2 \right)^{\sum_{\ell=1}^{a} r_\ell}.$$

Em particular, quando $q = 2$ temos $\alpha_j = 1$ para $1 \leq j \leq r_a$ e logo $\det \Lambda_{D'} = 4^{\sum_{\ell=1}^{a} r_\ell}$. □

Exemplo 3.2.15. *Seja $\mathbb{Z}_6^2 \supseteq C_1 \supseteq C_2$ a cadeia de códigos lineares tal que $C_1 = \langle (1,2) \rangle$ e $C_2 = \langle (2,4) \rangle$. Temos que $C_1^\perp = \{(x,y) \in \mathbb{Z}_6^2;\ x + 2y = 0\} = \langle (4,1) \rangle$ e*

$$C_2^\perp = \{(x,y) \in \mathbb{Z}_6^2;\ 2x + 4y = 0\} = \langle (4,1), (3,0) \rangle .$$

Considere o reticulado $\Lambda_{D^\perp}$ obtido via Construção D a partir da cadeia $\mathbb{Z}_6^2 \supseteq C_2^\perp \supseteq C_1^\perp$ usando $r_1 = 1, r_2 = 2, \boldsymbol{h}_1 = (4,1)$ e $\boldsymbol{h}_2 = (3,0)$. Como estes parâmetros satisfazem as hipóteses do Corolário 3.2.8, segue que

$$\det \Lambda_{D^\perp} = \big(3 \cdot 1\big)^2 \big(6^2\big)^{2-(1+2)} = 1/4,$$

$$\det \Lambda_{D'} = \big(3 \cdot 1\big)^{-2} \big(6^2\big)^{1+2} = (6^3/3)^2 = 72^2$$

e matrizes geradoras para $\Lambda_{D^\perp}$ e $\Lambda_{D'}$ são dadas respectivamente por

$$M = \begin{bmatrix} \sigma(\boldsymbol{h}_2) \\ (1/6)\sigma(\boldsymbol{h}_1) \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 4/6 & 1/6 \end{bmatrix} \quad e \quad 6(M^t)^{-1} = \begin{bmatrix} 2 & -8 \\ 0 & 36 \end{bmatrix}.$$

3.2.5 Distância mínima dos reticulados $\Lambda_D, \Lambda_{D'}$ e $\Lambda_{\overline{D}}$

Nesta seção, apresentamos resultados que obtivemos sobre as distâncias mínimas (em relação à métrica da soma) dos reticulados $\Lambda_D, \Lambda_{D'}$ e $\Lambda_{\overline{D}}$.

Lema 3.2.6. *Se $\{\mathbf{0}\} \neq C \subseteq \mathbb{Z}_q^n$ é um código linear, então existem $\boldsymbol{x}, \boldsymbol{y} \in C$ tais que*

$$\|\sigma(\boldsymbol{x}) - \sigma(\boldsymbol{y})\|_1 = d_{Lee}(C).$$

Demonstração. Seja $\boldsymbol{z} \in C$ tal que $d_{Lee}(\boldsymbol{z}, \mathbf{0}) = d_{Lee}(C)$. Logo $2\boldsymbol{z} \in C$ e $\sigma(2\boldsymbol{z}) - \sigma(\boldsymbol{z}) =$

$(\alpha_1, \ldots, \alpha_n)$, sendo

$$\alpha_i = \begin{cases} \sigma(z_i), & \text{se } \sigma(z_i) < q/2 \\ \sigma(z_i) - q, & \text{se } \sigma(z_i) \geq q/2. \end{cases}$$

Portanto

$$\|\sigma(2\boldsymbol{z}) - \sigma(\boldsymbol{z})\|_1 = \sum_{i=1}^{n} |\alpha_i| = \sum_{i=1}^{n} \min\{\sigma(z_i), q - \sigma(z_i)\} = d_{Lee}(\boldsymbol{z}, \boldsymbol{0}) = d_{Lee}(C).$$

Isto mostra que existem $\boldsymbol{x}, \boldsymbol{y} \in C$ tais que $\|\sigma(\boldsymbol{x}) - \sigma(\boldsymbol{y})\|_1 = d_{Lee}(C)$. □

Teorema 3.2.10. *Sejam $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a \neq \{\boldsymbol{0}\}$ uma cadeia de códigos lineares e $\Gamma_{\overline{D}}$ o conjunto discreto obtido via Construção $\overline{D}$ a partir desta cadeia. Se a distância de Lee mínima em C_ℓ é d_{Lee}^ℓ, para $\ell = 1, 2, \ldots, a$, então*

$$d_{\min}^1(\Gamma_{\overline{D}}) = \min\{q^a, q^{a-1}d_{Lee}^1, \ldots, d_{Lee}^a\}.$$

Demonstração. Para cada $\ell \in \{1, 2, \ldots, a\}$, o Lema 3.2.6 garante que existem $\boldsymbol{x}_\ell, \boldsymbol{y}_\ell \in C_\ell$ tais que $\|\sigma(\boldsymbol{x}_\ell) - \sigma(\boldsymbol{y}_\ell)\|_1 = d_{Lee}^\ell$. Como $q^{a-\ell}\sigma(C_\ell) \subseteq \Gamma_{\overline{D}}$, segue que $q^{a-\ell}\sigma(\boldsymbol{x}_\ell), q^{a-\ell}\sigma(\boldsymbol{y}_\ell) \in \Gamma_{\overline{D}}$ e

$$\|q^{a-\ell}\sigma(\boldsymbol{x}_\ell) - q^{a-\ell}\sigma(\boldsymbol{y}_\ell)\|_1 = q^{a-\ell}\|\sigma(\boldsymbol{x}_\ell) - \sigma(\boldsymbol{y}_\ell)\|_1 = q^{a-\ell}d_{Lee}^\ell.$$

Além disso, temos que $d_{\min}^1(\Gamma_{\overline{D}}) \leq q^a$ pois $q^a\mathbb{Z}^n \subseteq \Gamma_{\overline{D}}$. Logo

$$d_{\min}^1(\Gamma_{\overline{D}}) \leq \min\{q^a, q^{a-1}d_{Lee}^1, \ldots, d_{Lee}^a\}.$$

Para completar a prova, resta mostrar que $d_{\min}^1(\Gamma_{\overline{D}}) \geq \min\{q^a, q^{a-1}d_{Lee}^1, \ldots, d_{Lee}^a\}$. Com efeito, dados $\boldsymbol{x}, \boldsymbol{y} \in \Gamma_{\overline{D}}$, escrevemos $\boldsymbol{x} = q^\ell\boldsymbol{v}$ e $\boldsymbol{y} = q^k\boldsymbol{w}$ de modo que $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{Z}^n$, $\boldsymbol{v} \not\equiv \boldsymbol{0} \mod q$ e $\boldsymbol{w} \not\equiv \boldsymbol{0} \mod q$. Podemos assumir sem perda de generalidade que $\ell \geq k$. Temos que: (i) Se $k \geq a$ então

$$d^1(\boldsymbol{x}, \boldsymbol{y}) = q^k d^1(q^{\ell-k}\boldsymbol{v}, \boldsymbol{w}) \geq q^a, \text{ pois } \boldsymbol{0} \neq q^{\ell-k}\boldsymbol{v} - \boldsymbol{w} \in \mathbb{Z}^n.$$

(ii) Se $0 \leq k \leq a-1$ e $0 \leq \ell \leq a-1$, então existem $\boldsymbol{c}_1 \in C_1, \ldots, \boldsymbol{c}_{a-k} \in C_{a-k}$ e $\boldsymbol{z} \in \mathbb{Z}^n$ tais que $\boldsymbol{y} = q^a\boldsymbol{z} + q^{a-1}\sigma(\boldsymbol{c}_1) + \cdots + q^k\sigma(\boldsymbol{c}_{a-k})$ e consequentemente

$$\boldsymbol{w} = q^{a-k}\boldsymbol{z} + q^{a-1-k}\sigma(\boldsymbol{c}_1) + \cdots + q^0\sigma(\boldsymbol{c}_{a-k}).$$

Observe que $\boldsymbol{0} \neq q^{\ell-k}\overline{\boldsymbol{v}} - \overline{\boldsymbol{w}} \in C_{a-k}$ (pois $\overline{\boldsymbol{v}} \in C_{a-\ell}$ e $\overline{\boldsymbol{w}} \in C_{a-k}$) e

$$\begin{aligned} d^1(\boldsymbol{x}, \boldsymbol{y}) &= q^k d^1(q^{\ell-k}\boldsymbol{v}, \boldsymbol{w}) = q^k \sum_{i=1}^{n} |q^{\ell-k}v_i - w_i| \\ &\geq q^k \sum_{i=1}^{n} \min\{\sigma(q^{\ell-k}\overline{v}_i - \overline{w}_i), q - \sigma(q^{\ell-k}\overline{v}_i - \overline{w}_i)\} \geq q^k d_{Lee}^{a-k}, \end{aligned}$$

pois $|q^{\ell-k}v_i - w_i| \geq \min\{\sigma(q^{\ell-k}\overline{v}_i - \overline{w}_i), q - \sigma(q^{\ell-k}\overline{v}_i - \overline{w}_i)\}$ para $i = 1, \ldots, n$.
(iii) Se $0 \leq k \leq a-1$ e $\ell \geq a$, então $\mathbf{0} \neq \overline{\boldsymbol{w}} \in C_{a-k}$ e $\boldsymbol{x} = q^a\boldsymbol{z}$ com $\boldsymbol{z} = q^{\ell-a}\boldsymbol{v} \in \mathbb{Z}^n$. Logo

$$\begin{aligned} d^1(\boldsymbol{x}, \boldsymbol{y}) &= q^k d^1(q^{a-k}\boldsymbol{z}, \boldsymbol{w}) = q^k \sum_{i=1}^{n} |q^{a-k}z_i - w_i| \\ &\geq q^k \sum_{i=1}^{n} \min\{\sigma(-\overline{w}_i), q - \sigma(-\overline{w}_i)\} \\ &= q^k d_{Lee}(-\overline{\boldsymbol{w}}, \mathbf{0}) \geq q^k d_{Lee}^{a-k}. \end{aligned}$$

Portanto $d^1(\boldsymbol{x}, \boldsymbol{y}) \geq \min\{q^a, q^{a-1}d_{Lee}^1, \ldots, d_{Lee}^a\}, \forall \boldsymbol{x}, \boldsymbol{y} \in \Gamma_{\overline{D}}$. □

Corolário 3.2.9. *Sejam $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a \neq \{\mathbf{0}\}$ uma cadeia de códigos lineares, $\Gamma_{\overline{D}}$ o conjunto obtido via Construção $\overline{D}$ a partir desta cadeia e $\Lambda_{\overline{D}}$ o menor reticulado que contém $\Gamma_{\overline{D}}$. Se a distância de Lee mínima em C_ℓ é d_{Lee}^ℓ, para $\ell = 1, 2, \ldots, a$, então*

$$d_{\min}^1(\Lambda_{\overline{D}}) \leq \min\{q^a, q^{a-1}d_{Lee}^1, \ldots, d_{Lee}^a\}.$$

Além disso, quando a cadeia de códigos lineares é fechada sob a adição zero-um, temos

$$d_{\min}^1(\Lambda_{\overline{D}}) = \min\{q^a, q^{a-1}d_{Lee}^1, \ldots, d_{Lee}^a\}.$$

Demonstração. Do Teorema 3.2.10, obtemos $d_{\min}^1(\Lambda_{\overline{D}}) \leq \min\{q^a, q^{a-1}d_{Lee}^1, \ldots, d_{Lee}^a\}$, uma vez que $\Gamma_{\overline{D}} \subseteq \Lambda_{\overline{D}}$. Quando a cadeia utilizada é fechada sob a adição zero-um, temos que $\Gamma_{\overline{D}}$ é um reticulado e $\Gamma_{\overline{D}} = \Lambda_{\overline{D}}$. Assim, aplicando novamente o Teorema 3.2.10, obtemos

$$d_{\min}^1(\Lambda_{\overline{D}}) = d_{\min}^1(\Gamma_{\overline{D}}) = \min\{q^a, q^{a-1}d_{Lee}^1, \ldots, d_{Lee}^a\}.$$

□

Acreditamos que a segunda parte do Corolário 3.2.9 possa ser refinada, retirando-se a hipótese de que a cadeia $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ é fechada sob a adição zero-um. Propomos, portanto, a seguinte conjectura:

Conjectura 3.2.1. *Sejam $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a \neq \{\mathbf{0}\}$ uma cadeia de códigos lineares, $\Gamma_{\overline{D}}$ o conjunto obtido via Construção $\overline{D}$ a partir desta cadeia e $\Lambda_{\overline{D}}$ o menor reticulado que contém $\Gamma_{\overline{D}}$. Se a distância de Lee mínima em C_ℓ é d_{Lee}^ℓ, para $\ell = 1, 2, \ldots, a$, então*

$$d_{\min}^1(\Lambda_{\overline{D}}) = \min\{q^a, q^{a-1}d_{Lee}^1, \ldots, d_{Lee}^a\}.$$

Corolário 3.2.10. *Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a \neq \{\mathbf{0}\}$ uma cadeia de códigos lineares fechada sob a adição zero-um e seja Λ_D o reticulado obtido via Construção D a partir*

desta cadeia. Se a distância de Lee mínima em C_ℓ é d^ℓ_{Lee}, para $\ell = 1, 2, \ldots, a$, então

$$d^1_{\min}(\Lambda_D) = \min_{1\leq \ell \leq a} \left\{ q, \frac{1}{q^{\ell-1}} d^\ell_{Lee} \right\}.$$

Demonstração. Como a cadeia de códigos usada é fechada sob a adição zero-um, temos que $q^{a-1}\Lambda_D = \Lambda_{\overline{D}}$ e logo $d^1_{\min}(\Lambda_D) = (1/q^{a-1}) \min\{q^a, q^{a-1}d^1_{Lee}, \ldots, d^a_{Lee}\}$. □

Observação 3.2.13. *Quando $a = 1$, o Teorema 3.2.10 coincide com o Teorema 3.1.2. De fato, neste caso temos que $\Gamma_{\overline{D}} = \Lambda_A(C_1)$ e logo*

$$d^1_{\min}\big(\Lambda_A(C_1)\big) = d^1_{\min}\big(\Gamma_{\overline{D}}\big) = \min\big\{q, d_{Lee}(C_1)\big\}.$$

No exemplo a seguir mostramos que a condição de que a cadeia de códigos lineares é fechada sob a adição zero-um não pode ser omitida no Corolário 3.2.10.

Exemplo 3.2.16. *Seja $\mathbb{Z}_3^2 \supseteq C_1 \supseteq C_2$ a cadeia de códigos lineares, na qual $C_1 = C_2 = \langle (1,2) \rangle$. Escolhendo os parâmetros $k_1 = 2, k_2 = 1$ e $\boldsymbol{b}_1 = (1,2), \boldsymbol{b}_2 = (2,1) \in \mathbb{Z}_3^2$, temos $0 \leq k_2 \leq k_1$, $C_1 = \langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle$, $C_2 = \langle \boldsymbol{b}_1 \rangle$ e, consequentemente, Λ_D consiste de todos os vetores da forma*

$$z + \alpha_2^{(1)}(2,1) + \alpha_1^{(2)}\frac{1}{3}(1,2),$$

em que $z \in 3\mathbb{Z}^2, 0 \leq \alpha_2^{(1)} < 3$ e $0 \leq \alpha_1^{(2)} < 9$. Portanto,

$$\Lambda_D = \bigcup_{\boldsymbol{z} \in 3\mathbb{Z}^2} \big(\boldsymbol{z} + \Lambda_D \cap [0,3)^2\big).$$

Os elementos de $\Lambda_D \cap [0,3)^2$ estão representados na Figura 3.8. Neste exemplo, observamos

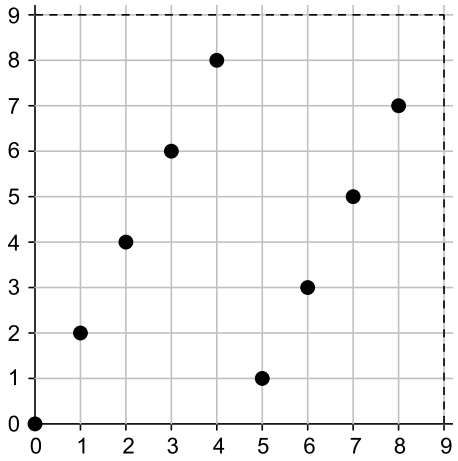


Figura 3.8: Elementos de $3\Lambda_D$ na caixa $[0,9)^2$.

que $d^1_{Lee} = d^2_{Lee} = 2$, $d^1_{\min}(\Lambda_D) = 1$,

$$\min_{1\leq \ell \leq 2}\left\{3, \frac{1}{3^{\ell-1}} d^{\ell}_{Lee}\right\} = \frac{2}{3}$$

e que a cadeia $C_1 \supseteq C_2$ *não é fechada sob a adição zero-um, uma vez que* $(1,2) \in C_2$ *e* $(1,2) * (1,2) = (0,1) \notin C_1$.

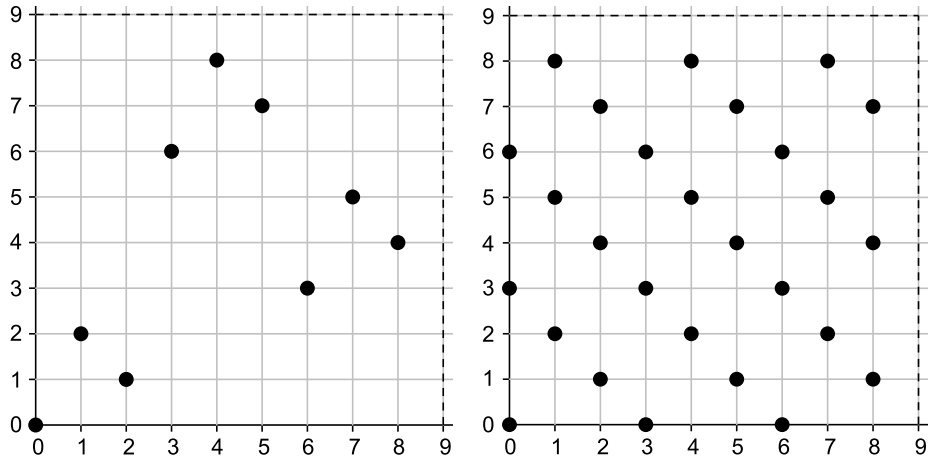
Observação 3.2.14. *O Exemplo 3.2.16 está de acordo com a Conjectura 3.2.1. De fato, temos que* $\Gamma_{\overline{D}} = 3^2\mathbb{Z}^2 + 3^1\sigma(C_1) + 3^0\sigma(C_2)$ *com* $\sigma(C_1) = \sigma(C_2) = \{(0,0),(1,2),(2,1)\}$, *isto é,*

$$\Gamma_{\overline{D}} = 3^2\mathbb{Z}^2 + \Gamma_{\overline{D}} \cap [0,9)^2$$

e

$$\Gamma_{\overline{D}} \cap [0,9)^2 = \{(0,0),(3,6),(6,3),(1,2),(4,8),(7,5),(2,1),(5,7),(8,4)\}.$$

Os elementos de $\Gamma_{\overline{D}} \cap [0,9)^2$ *estão representados na Figura 3.9(a). O conjunto* $\Gamma_{\overline{D}}$ *não*



(a) $\Gamma_{\overline{D}} \cap [0,9)^2$ (b) $\Lambda_{\overline{D}} \cap [0,9)^2$

Figura 3.9: Elementos de $\Gamma_{\overline{D}}$ e $\Lambda_{\overline{D}}$ na caixa $[0,9)^2$

é um reticulado (evidentemente este resultado não poderia ser diferente, pois a cadeia utilizada nesta construção não é fechada sob a adição zero-um - Teorema 3.2.8). Na Figura 3.9(b), está ilustrado o reticulado $\Lambda_{\overline{D}}$ *(isto é, o menor reticulado que contém* $\Gamma_{\overline{D}}$*). Observe que* $d^1_{\min}(\Lambda_{\overline{D}}) = 2$ *(ver Figura 3.9(b)) e* $\min\{3^2, 3d^1_{Lee}, d^2_{Lee}\} = \min\{9,6,2\} = 2$.

Corolário 3.2.11. *Seja* $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a \neq \{\mathbf{0}\}$ *uma cadeia de códigos lineares fechada sob a adição zero-um. Se a distância mínima* d^{ℓ}_{Lee} *de* C_ℓ *satisfaz* $d^{\ell}_{Lee} \geq q^{\ell}$, $\ell = 1,2,\ldots,a$, *então* $d^1_{\min}(\Lambda_{\overline{D}}) = q^a$ *e* $d^1_{\min}(\Lambda_D) = q$.

Demonstração. Basta observar que $q^{a-\ell} d^{\ell}_{Lee} \geq q^a$ e $(1/q^{\ell-1}) d^{\ell}_{Lee} \geq q$, para $\ell = 1,2,\ldots,a$. Consequentemente, aplicando o Teorema 3.2.10 e o Corolário 3.2.10, obtemos $d^1_{\min}(\Lambda_D) = q$ e $d^1_{\min}(\Lambda_{\overline{D}}) = \min\{q^a, q^{a-1}d^1_{Lee}, \ldots, d^a_{Lee}\} = q^a$. □

Corolário 3.2.12. *Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a \neq \{\mathbf{0}\}$ uma cadeia de códigos lineares fechada sob a adição zero-um. Suponhamos que os vetores $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k_1} \in \mathbb{Z}_q^n$ usados na Construção D sejam não nulos e satisfaçam as seguintes condições:*

1. *Alguma permutação das linhas da matriz $[\sigma(\boldsymbol{b}_1) \cdots \sigma(\boldsymbol{b}_{k_1})]^t$ forma uma matriz triangular superior (resp. inferior) na forma escalonada.*

2. *Para cada $j \in \{1, \ldots, k_1\}$, a primeira (resp. última) componente não nula do vetor $\sigma(\boldsymbol{b}_j)$, denotada por α_j, divide q e todas as demais componentes do mesmo.*

Seja $\lambda = \min_{1 \leq \ell \leq a}\{q, (1/q^{\ell-1})d_{Lee}^{\ell}\}$, onde d_{Lee}^{ℓ} denota a distância de Lee mínima em C_ℓ, $\ell = 1, 2, \ldots, a$. Nestas condições, a densidade de empacotamento de Λ_D (e logo de $\Lambda_{\overline{D}}$) na métrica da soma é dada por

$$\Delta_1(\Lambda_{\overline{D}}) = \Delta_1(\Lambda_D) = \frac{\lambda^n q^{\sum_{\ell=1}^{a} k_\ell - n}}{n! \prod_{i=1}^{k_1} \alpha_i} \tag{3.4}$$

e a densidade de centro

$$\delta_1(\Lambda_{\overline{D}}) = \delta_1(\Lambda_D) = \frac{\lambda^n q^{\sum_{\ell=1}^{a} k_\ell - n}}{2^n \prod_{i=1}^{k_1} \alpha_i}. \tag{3.5}$$

Além disso, temos que $d_{Lee}^{\ell} \geq q^{\ell}$ se, e somente se,

$$\Delta_1(\Lambda_D) = \frac{q^{\sum_{\ell=1}^{a} k_\ell}}{n! \prod_{i=1}^{k_1} \alpha_i} \quad e \quad \delta_1(\Lambda_D) = \frac{q^{\sum_{\ell=1}^{a} k_\ell}}{2^n \prod_{i=1}^{k_1} \alpha_i}. \tag{3.6}$$

Demonstração. Basta observar que o volume euclidiano da bola n-dimensional de raio 1 na métrica da soma é $2^n/n!$ [40] e aplicar os Teoremas 3.2.10 e 3.2.8. □

No exemplo a seguir mostramos que a condição de que a cadeia de códigos lineares é fechada sob a adição zero-um não pode ser omitida no Corolário 3.2.12.

Exemplo 3.2.17. *Seja $\mathbb{Z}_6^2 \supseteq C_1 \supseteq C_2$ a cadeia de códigos lineares tal que $C_1 = \langle (4,2), (3,0) \rangle$ e $C_2 = \langle (4,2) \rangle$. Escolhendo $k_1 = 2, k_2 = 1$ e $\boldsymbol{b}_1 = (4,2), \boldsymbol{b}_2 = (3,0) \in \mathbb{Z}_6^2$, temos $0 \leq k_2 \leq k_1$, $C_1 = \langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle$, $C_2 = \langle \boldsymbol{b}_1 \rangle$ e, consequentemente, Λ_D consiste de todos os vetores da forma*

$$\boldsymbol{z} + \alpha_2^{(1)}(3,0) + \alpha_1^{(2)} \frac{1}{6}(4,2),$$

em que $\boldsymbol{z} \in 6\mathbb{Z}^2, 0 \leq \alpha_2^{(1)} < 6$ e $0 \leq \alpha_1^{(2)} < 36$. Observe que $d_{Lee}^1 = 3$, $d_{Lee}^2 = 4$ e os vetores $\boldsymbol{b}_1$ e $\boldsymbol{b}_2$ são não nulos e satisfazem as hipóteses do Corolário 3.2.12. Considere também o conjunto

$$\Gamma_{\overline{D}} = 36\mathbb{Z}^2 + 6\sigma(C_1) + \sigma(C_2)$$

e o reticulado $\Lambda_{\overline{D}}$ (menor reticulado que contém $\Gamma_{\overline{D}}$). Pode-se mostrar que $\Delta_1(\Lambda_{\overline{D}}) = 2/3$ e $\Delta_1(\Lambda_D) = 1/2$. Logo neste exemplo não vale a Igualdade (3.4), caso contrário teríamos $\Delta_1(\Lambda_{\overline{D}}) = \Delta_1(\Lambda_D) = 2/9$. Evidentemente isto não contradiz o Corolário 3.2.12, pois a cadeia de códigos utilizada neste exemplo não é fechada sob a adição zero-um.

Teorema 3.2.11. *Sejam $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a \neq \{\mathbf{0}\}$ uma cadeia de códigos lineares, $0 \leq r_1 \leq r_2 \leq \cdots \leq r_a$ e $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_a} \in \mathbb{Z}_q^n$ tais que $C_\ell^\perp = \langle \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r_\ell} \rangle$ para $\ell = 1, 2, \ldots, a$. Se $\Lambda_{D'}$ é o reticulado obtido via Construção D' usando os parâmetros descritos acima, então*

$$\min\{q^a, q^{a-1}d_{Lee}^1, \ldots, d_{Lee}^a\} \leq d_{\min}^1(\Lambda_{D'}) \leq q^a,$$

em que d_{Lee}^ℓ é a distância de Lee mínima em C_ℓ, para $\ell = 1, 2, \ldots, a$.

Demonstração. Se $\boldsymbol{x} \in \mathbb{Z}^n$ é um vetor com uma componente que não é múltipla de q e $\boldsymbol{x} \cdot \sigma(\boldsymbol{h}_j) \equiv \mathbf{0} \mod q$, $1 \leq j \leq r_k$, então $\|\boldsymbol{x}\|_1 \geq d_{Lee}^k$. De fato, podemos escrever $\boldsymbol{x} = \boldsymbol{c} + q\boldsymbol{z}$, onde $\boldsymbol{z} \in \mathbb{Z}^n$, $\boldsymbol{c} = (c_1, \ldots, c_n)$ e $c_i \in \{0, 1, \ldots, q-1\}$, para todo $i \in \{1, 2, \ldots, n\}$. Como $\boldsymbol{x}$ tem uma componente que não é múltipla de q, temos $\boldsymbol{c} \neq \mathbf{0}$. Além disso, $\boldsymbol{c} \cdot \sigma(\boldsymbol{h}_j) \equiv \mathbf{0} \mod q$, $1 \leq j \leq r_k$, logo $\overline{\mathbf{0}} \neq \overline{\boldsymbol{c}} \in C_k$ e consequentemente $\|\boldsymbol{c}\|_1 \geq d_{Lee}^k$. Portanto

$$\|\boldsymbol{x}\|_1 = \|\boldsymbol{c} + q\boldsymbol{z}\|_1 = \sum_{i=1}^n |c_i + qz_i| \geq \sum_{i=1}^n \min\{c_i, q - c_i\} \geq d_{Lee}^k.$$

Agora, seja $\mathbf{0} \neq \boldsymbol{x} \in \Lambda_{D'}$. Como $\boldsymbol{x} \neq \mathbf{0}$, existe $k \geq 0$ tal que $q^{-k}\boldsymbol{x} \in \mathbb{Z}^n$ e $q^{-k-1}\boldsymbol{x} \notin \mathbb{Z}^n$. Se $k < a$ então $q^{-k}\boldsymbol{x} \cdot \sigma(\boldsymbol{h}_j) \equiv \mathbf{0} \mod q$ para $1 \leq j \leq r_{a-k}$, uma vez que

$$\begin{aligned}
\boldsymbol{x} \in \Lambda_{D'} &\iff \boldsymbol{x} \cdot \sigma(\boldsymbol{h}_j) \equiv \mathbf{0} \mod q^{i+1}, \text{ para } 0 \leq i < a \text{ e } r_{a-i-1} < j \leq r_{a-i}. \\
&\implies \boldsymbol{x} \cdot \sigma(\boldsymbol{h}_j) \equiv \mathbf{0} \mod q^{k+1}, \text{ para } k \leq i < a \text{ e } r_{a-i-1} < j \leq r_{a-i}. \\
&\iff q^{-k}\boldsymbol{x} \cdot \sigma(\boldsymbol{h}_j) \equiv \mathbf{0} \mod q, \text{ para } 1 < j \leq r_{a-k}.
\end{aligned}$$

Logo $\|\boldsymbol{x}\|_1 \geq q^k d_{Lee}^{a-k}$. Se $k \geq a$ então $\boldsymbol{x} = q^k\boldsymbol{z} = q^a(q^{k-a}\boldsymbol{z})$, para algum $\mathbf{0} \neq \boldsymbol{z} \in \mathbb{Z}^n$, e logo $\|\boldsymbol{x}\|_1 \geq q^a$. Portanto $\min\{q^a, q^{a-1}d_{Lee}^1, \ldots, d_{Lee}^a\} \leq d_{\min}^1(\Lambda_{D'})$. Para obter a desigualdade $d_{\min}^1(\Lambda_{D'}) \leq q^a$, é suficiente observar que $q^a\mathbb{Z}^n \subseteq \Lambda_{D'}$. □

Exemplo 3.2.18. *Seja $\mathbb{Z}_3^2 \supseteq C_1 \supseteq C_2$ a cadeia de códigos lineares tal que $C_1 = C_2 = \langle (1,1) \rangle$. Assim, $C_1^\perp = C_2^\perp = \{(x,y) \in \mathbb{Z}_3^2; x + y = 0\} = \{(0,0), (1,2), (2,1)\} = \langle (1,2) \rangle$. Para $r_1 = 1$, $r_2 = 2$ e $\boldsymbol{h}_1 = (1,2), \boldsymbol{h}_2 = (1,2) \in \mathbb{Z}_3^2$, temos $0 \leq r_1 \leq r_2$, $C_1^\perp = \langle \boldsymbol{h}_1 \rangle$, $C_2^\perp = \langle \boldsymbol{h}_1, \boldsymbol{h}_2 \rangle$ e, consequentemente,*

$$\Lambda_{D'} = \big\{(x,y) \in \mathbb{Z}^2;\ x + 2y \equiv 0 \mod 9\big\}.$$

Portanto

$$\Lambda_{D'} = \bigcup_{\boldsymbol{z}\in 9\mathbb{Z}^2} \big(\boldsymbol{z} + \Lambda_{D'} \cap [0,9)^2\big).$$

Os elementos de $\Lambda_{D'} \cap [0,9)^2$ *estão representados na Figura 3.10. Neste exemplo, observamos que* $d^1_{Lee} = d^2_{Lee} = 2$ *e portanto* $\min\{d^2_{Lee}, 3d^1_{Lee}, 3^2\} = 2 < 3 = d^1_{\min}(\Lambda_{D'}) < 3^2$.

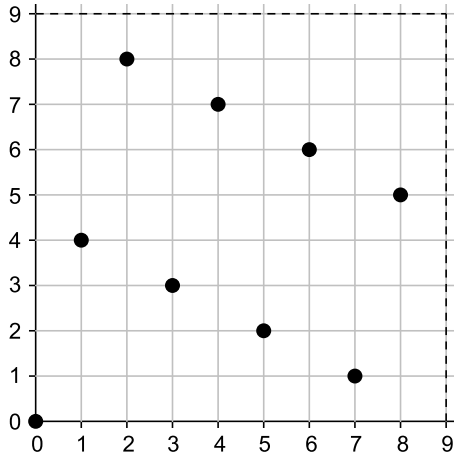


Figura 3.10: Elementos de $\Lambda_{D'}$ na caixa $[0,9)^2$.

Exemplo 3.2.19. *Um exemplo no qual as desigualdades do Teorema 3.2.11 são estritas pode ser obtido considerando novamente a cadeia de códigos lineares* $\mathbb{Z}_6^2 \supseteq C_1 \supseteq C_2$ *tal que* $C_1 = \langle(1,2)\rangle$ *e* $C_2 = \langle(2,4)\rangle$ *juntamente com os parâmetros* $r_1 = 1$, $r_2 = 2$ *e* $\boldsymbol{h}_1 = (4,1), \boldsymbol{h}_2 = (3,0) \in \mathbb{Z}_6^2$ *(Exemplo 3.2.9). Neste exemplo, temos que* $\min\{6^2, 6d^1_{Lee}, d^2_{Lee}\} = 4 < 5 = d^1_{\min}(\Lambda'_D) < 6^2$.

3.3 Construção A′

Nesta seção, $\mathbb{Z}_q[X]$ representa o anel de polinômios na variável X com coeficientes em $\mathbb{Z}_q$, $I_a = (X^a) \subseteq \mathbb{Z}_q[X]$ é o ideal gerado pelo polinômio X^a e $R_{a,q}$ é o anel quociente de $\mathbb{Z}_q[X]$ por I_a, isto é, $R_{a,q} = \mathbb{Z}_q[X]/I_a$. Em outras palavras, $R_{a,q}$ é o conjunto

$$\left\{ \sum_{j=0}^{a-1} b_j X^j;\ b_1, b_2, \ldots, b_{a-1} \in \mathbb{Z}_q \right\},$$

munido com as operações de adição e multiplicação de polinômios sobre $\mathbb{Z}_q$, juntamente com a operação quociente $X^a = 0$, que é equivalente ao cancelamento de todos os termos de grau maior ou igual a a. Também utilizamos a aplicação $\phi : R_{a,q} \to \mathbb{Z}$ dada por

$$\phi\left(\sum_{j=0}^{a-1} b_j X^j \right) = \sum_{j=0}^{a-1} \sigma(b_j) q^j,$$

e sua extensão $\phi : R_{a,q}^n \to \mathbb{Z}^n$ dada por $\phi(p_1, \ldots, p_n) = \big(\phi(p_1), \ldots, \phi(p_n)\big)$.

Definição 3.3.1. *Um subconjunto C de $R_{a,q}^n$ é chamado de* ***código linear*** *de comprimento n sobre $R_{a,q}$ quando C pode ser escrito da seguinte forma*

$$C = \{\boldsymbol{u}G;\ \boldsymbol{u} \in R_{a,q}^{1\times k}\},$$

para alguma matriz $G \in R_{a,q}^{k\times n}$. Neste caso, dizemos que as linhas da matriz G geram o código linear C.

A seguir, apresentamos a Construção A′ associada com códigos lineares sobre $R_{a,q}$, a qual é uma generalização da Construção A′ que foi introduzida em [19, 20] para o caso $q = 2$.

Definição 3.3.2. *(**Construção A′**) Dado um código linear C de comprimento n sobre $R_{a,q}$, definimos o conjunto*

$$\Gamma_{A'} = \phi(C) + q^a\mathbb{Z}^n.$$

Observação 3.3.1. *Para qualquer código linear $C \subseteq R_{a,q}^n$, $\Gamma_{A'} = \phi(C) + q^a\mathbb{Z}^n$ é um conjunto discreto, uma vez que $\Gamma_{A'} \subseteq \mathbb{Z}^n$. Entretanto, conforme podemos ver no próximo exemplo, $\Gamma_{A'}$ nem sempre é um subgrupo aditivo de $\mathbb{R}^n$ e, consequentemente, a Construção A' nem sempre produz um reticulado.*

Exemplo 3.3.1. *Considere o código linear C sobre $R_{2,6}$ gerado pelas linhas da matriz*

$$G = \begin{bmatrix} 2 & 4 \\ X & 2X \end{bmatrix} \in R_{2,6}^{2\times 2}.$$

Ou seja,

$$\begin{aligned} C &= \left\{ \begin{bmatrix} aX+b & cX+d \end{bmatrix} \begin{bmatrix} 2 & 4 \\ X & 2X \end{bmatrix};\ a,b,c,d \in \mathbb{Z}_6 \right\} \\ &= \Big\{(2b + (2a+d)X, 4b + (4a+2d)X);\ a,b,d \in \mathbb{Z}_6\Big\}. \end{aligned}$$

Donde segue que

$$\phi(C) = \big\{(\sigma(2b) + 6\sigma(2a+d), \sigma(4b) + 6\sigma(4a+2d));\ a,b,d \in \mathbb{Z}_6\big\},$$

isto é,

$$\begin{aligned} \phi(C) = \{&(0,0),(6,12),(12,24),(18,0),(24,12),(30,24),(2,4),(8,16),(14,28),\\ &(20,4),(26,16),(32,28),(4,2),(10,14),(16,26),(22,2),(28,14),(34,26)\}. \end{aligned}$$

Os elementos de $\phi(C)$ estão representados na Figura 3.11. Neste exemplo, o conjunto

$$\Gamma_{A'} = \phi(C) + 36\mathbb{Z}^2 = \bigcup_{\boldsymbol{z}\in 36\mathbb{Z}^2} \left[\boldsymbol{z} + \phi(C)\right]$$

***não** é um reticulado. Além disso, temos que $\Gamma_{A'}$ é igual ao conjunto $\Gamma_{\overline{D}}$ obtido via Construção $\overline{D}$ no Exemplo 3.2.9 a partir da cadeia de códigos lineares* 6*-ários*

$$\mathbb{Z}_6^2 \supseteq C_1 = \langle (1,2) \rangle \supseteq C_2 = \langle (2,4) \rangle .$$

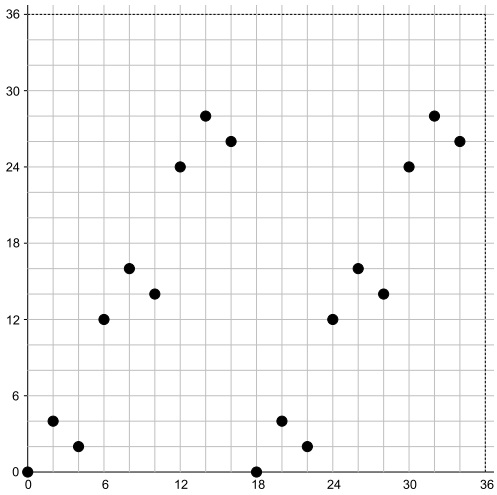


Figura 3.11: $\Gamma_{A'} \cap [0,36)^2$

No próximo teorema mostramos que qualquer conjunto $\Gamma_{\overline{D}} \subseteq \mathbb{Z}^n$ obtido a partir da Construção $\overline{\mathrm{D}}$ também pode ser obtido via Construção A′, ou seja, sempre existe um código linear $C \subseteq R_{a,q}^n$ tal que $\Gamma_{\overline{D}} = \phi(C) + q^a\mathbb{Z}^n$. Este resultado é mostrado em [25] para o caso $q = 2$.

Teorema 3.3.1. *Sejam $\mathbb{Z}_q^n \supseteq C_1 \supseteq \cdots \supseteq C_{a-1} \supseteq C_a$ uma cadeia de códigos lineares e*

$$\Gamma_{\overline{D}} = q^a\mathbb{Z}^n + q^{a-1}\sigma(C_1) + \cdots + q^1\sigma(C_{a-1}) + \sigma(C_a).$$

Existe um código linear $C \subseteq R_{a,q}^n$ tal que $\Gamma_{\overline{D}} = \phi(C) + q^a\mathbb{Z}^n = \Gamma_{A'}$.

Demonstração. Sejam $k = k_1 \geq k_2 \geq \cdots \geq k_a \geq 0$ e uma matriz $G \in \mathbb{Z}_q^{k\times n}$ tal que as primeiras k_i linhas geram C_i. Escrevemos

$$G = \begin{bmatrix} G_a \\ \vdots \\ G_2 \\ G_1 \end{bmatrix} \in \mathbb{Z}_q^{k\times n}$$

de modo que as linhas da matriz $[G_a^t \cdots G_i^t]^t$ geram C_i e consideramos o código linear C sobre $R_{a,q}$ gerado pelas linhas da matriz

$$\tilde{G} = \begin{bmatrix} G_a \\ XG_{a-1} \\ \vdots \\ X^{a-2}G_2 \\ X^{a-1}G_1 \end{bmatrix} \in R_{a,q}^{k\times n}.$$

Afirmação: $\Gamma_{\overline{D}} = \phi(C) + q^a\mathbb{Z}^n$ (isto é, $\Gamma_{\overline{D}}$ pode ser obtido de C via Construção A′). De fato, dado $\boldsymbol{w} \in \Gamma_{\overline{D}}$, existem $\boldsymbol{z} \in \mathbb{Z}^n$ e $\boldsymbol{c}_i \in C_i$, $i = 1, \ldots, a$, tais que

$$\boldsymbol{w} = q^a\boldsymbol{z} + q^{a-1}\sigma(\boldsymbol{c}_1) + \cdots + q^1\sigma(\boldsymbol{c}_{a-1}) + \sigma(\boldsymbol{c}_a).$$

Para cada $i \in \{1, \ldots, a\}$, escolhemos $\boldsymbol{d}_i = (d_{i1}, \ldots, d_{ik_i}) \in \mathbb{Z}_q^{1\times k_i}$ tal que

$$\boldsymbol{d}_i \begin{bmatrix} G_a \\ \vdots \\ G_i \end{bmatrix} = (d_{i1}, \ldots, d_{ik_i}) \begin{bmatrix} G_a \\ \vdots \\ G_i \end{bmatrix} = \boldsymbol{c}_i.$$

Multiplicando as componentes de $\boldsymbol{d}_i$ por potências convenientes de X e acrescentando $k - k_i$ zeros, obtemos um vetor $\tilde{\boldsymbol{d}}_i = (d_{i1}X^{a-i}, \ldots, d_{ik_i}, 0, \ldots, 0) \in R_a^{1\times k}$ satisfazendo

$$\tilde{\boldsymbol{d}}_i\tilde{G} = (d_{i1}X^{a-i}, \ldots, d_{ik_i}, 0, \ldots, 0) \begin{bmatrix} G_a \\ XG_{a-1} \\ \vdots \\ X^{a-2}G_2 \\ X^{a-1}G_1 \end{bmatrix} = \boldsymbol{c}_iX^{a-i}$$

e consequentemente $(\tilde{\boldsymbol{d}}_1 + \cdots + \tilde{\boldsymbol{d}}_{a-1} + \tilde{\boldsymbol{d}}_a)\tilde{G} = \boldsymbol{c}_1X^{a-1} + \cdots + \boldsymbol{c}_{a-1}X + \boldsymbol{c}_a$. Aplicando ϕ em ambos os lados desta última igualdade, obtemos

$$\phi\big((\tilde{\boldsymbol{d}}_1 + \cdots + \tilde{\boldsymbol{d}}_{a-1} + \tilde{\boldsymbol{d}}_a)\tilde{G}\big) = q^{a-1}\sigma(\boldsymbol{c}_1) + \cdots + q\sigma(\boldsymbol{c}_{a-1}) + \sigma(\boldsymbol{c}_a).$$

Como $(\tilde{\boldsymbol{d}}_1 + \cdots + \tilde{\boldsymbol{d}}_{a-1} + \tilde{\boldsymbol{d}}_a)\tilde{G} \in C$, segue que $\boldsymbol{w} \in \phi(C) + q^a\mathbb{Z}^n$. Isto mostra que $\Gamma_{\overline{D}} \subseteq \phi(C) + q^a\mathbb{Z}^n$. Para concluir a prova, resta mostrar que $\phi(C) + q^a\mathbb{Z}^n \subseteq \Gamma_{\overline{D}}$. Com efeito, se $\boldsymbol{w} \in \phi(C) + q^a\mathbb{Z}^n$, então existem $\boldsymbol{z} \in \mathbb{Z}^n$ e $\tilde{\boldsymbol{d}} \in R_a^{1\times k}$ tais que $\boldsymbol{w} = \phi(\tilde{\boldsymbol{d}}\tilde{G}) + q^a\boldsymbol{z}$.

Além disso, para qualquer $\tilde{\boldsymbol{d}} \in R_a^{1\times k}$, o coeficiente de X^{a-i} em

$$\tilde{\boldsymbol{d}}\tilde{G} = \tilde{\boldsymbol{d}} \begin{bmatrix} G_a \\ XG_{a-1} \\ \vdots \\ X^{a-2}G_2 \\ X^{a-1}G_1 \end{bmatrix}$$

é combinação linear das linhas da matriz $[G_a^t \cdots G_i^t]^t$. Logo existem $\boldsymbol{c}_i \in C_i$, $\forall i = 1, \ldots, a$, tais que $\tilde{\boldsymbol{d}}\tilde{G} = \boldsymbol{c}_1 X^{a-1} + \cdots + \boldsymbol{c}_{a-1}X + c_a$ e portanto

$$\boldsymbol{w} = \phi(\tilde{\boldsymbol{d}}\tilde{G}) + q^a\boldsymbol{z} = q^a\boldsymbol{z} + \sigma(\boldsymbol{c}_1)q^{a-1} + \cdots + \sigma(\boldsymbol{c}_{a-1})q + \sigma(\boldsymbol{c}_a) \in \Gamma_{\overline{D}}.$$

Isto mostra que $\Gamma_{\overline{D}} = \phi(C) + q^a\mathbb{Z}^n$. □

Corolário 3.3.1. *Se um código linear C sobre $R_{a,q}$ pode ser escrito como*

$$C_a + XC_{a-1} + \cdots + X^{a-1}C_1$$

e a cadeia $\mathbb{Z}_q^n \supseteq C_1 \supseteq \cdots \supseteq C_{a-1} \supseteq C_a$ é fechada sob a adição zero-um, então o conjunto $\Gamma_{A'} = \phi(C) + q^a\mathbb{Z}^n$ obtido a partir da Construção A' é um reticulado.

Demonstração. Temos que

$$\Gamma_{A'} = \phi(C) + q^a\mathbb{Z}^n = \sigma(C_a) + q\sigma(C_{a-1}) + \cdots + q^{a-1}\sigma(C_1) + q^a\mathbb{Z}^n = \Gamma_{\overline{D}}.$$

Aplicando o Teorema 3.2.8 obtemos o resultado desejado. □

Definição 3.3.3. *(**Adição zero-um em $R_{a,q}^n$**) Dados $p(X) = \alpha_0 + \alpha_1 X + \cdots + \alpha_{a-1}X^{a-1}$ e $\hat{p}(X) = \hat{\alpha}_0 + \hat{\alpha}_1 X + \cdots + \hat{\alpha}_{a-1}X^{a-1}$ em $R_{a,q}$, a adição zero-um entre $p(X)$ e $\hat{p}(X)$ é*

$$p(X) * \hat{p}(X) = (\alpha_0 * \hat{\alpha}_0) + (\alpha_1 * \hat{\alpha}_1)X + \cdots + (\alpha_{a-1} * \hat{\alpha}_{a-1})X^{a-1},$$

na qual a operação $(*)$ no lado direito desta igualdade é a adição zero-um em $\mathbb{Z}_q$. A adição zero-um entre dois elementos $\boldsymbol{p} = (p_1, \ldots, p_n)$ e $\hat{\boldsymbol{p}} = (\hat{p}_1, \ldots, \hat{p}_n)$ de $R_{a,q}^n$ é definida como

$$\boldsymbol{p} * \hat{\boldsymbol{p}} = (p_1 * \hat{p}_1, \ldots, p_n * \hat{p}_n).$$

Observação 3.3.2. *Escrevendo $\boldsymbol{p}, \hat{\boldsymbol{p}} \in R_{a,q}^n$ como $\boldsymbol{p} = \boldsymbol{p}_0 + \boldsymbol{p}_1 X + \cdots + \boldsymbol{p}_{a-1}X^{a-1}$ e $\hat{\boldsymbol{p}} = \hat{\boldsymbol{p}}_0 + \hat{\boldsymbol{p}}_1 X + \cdots + \hat{\boldsymbol{p}}_{a-1}X^{a-1}$ com $\boldsymbol{p}_i, \hat{\boldsymbol{p}}_i \in \mathbb{Z}_q^n$, $i = 0, \ldots, a-1$, temos*

$$\boldsymbol{p} * \hat{\boldsymbol{p}} = (\boldsymbol{p}_0 * \hat{\boldsymbol{p}}_0) + (\boldsymbol{p}_1 * \hat{\boldsymbol{p}}_1)X + \cdots + (\boldsymbol{p}_{a-1} * \hat{\boldsymbol{p}}_{a-1})X^{a-1}.$$

Definição 3.3.4. *Um código linear C sobre $R_{a,q}$ é dito* ***fechado sob a adição zero-um deslocada*** *quando para quaisquer elementos $\boldsymbol{c}_1$ e $\boldsymbol{c}_2$ de C, $(\boldsymbol{c}_1 * \boldsymbol{c}_2)X$ também é um elemento de C.*

Observação 3.3.3. *Se uma cadeia de códigos lineares $\mathbb{Z}_q^n \supseteq C_1 \supseteq \cdots \supseteq C_{a-1} \supseteq C_a$ é fechada sob a adição zero-um, então $C = C_a + XC_{a-1} + \cdots + X^{a-1}C_1$ é um código linear sobre $R_{a,q}$ fechado sob a adição zero-um deslocada.*

Lema 3.3.1. *Seja C um código linear sobre $R_{a,q}$. Se $\boldsymbol{c}_1$ e $\boldsymbol{c}_2$ são elementos de C, então*

$$\phi(\boldsymbol{c}_1) + \phi(\boldsymbol{c}_2) - \phi(\boldsymbol{c}_1 + \boldsymbol{c}_2) = \phi\big((\boldsymbol{c}_1 * \boldsymbol{c}_2)X\big) + q^a\boldsymbol{z}, \text{ para algum } \boldsymbol{z} \in \mathbb{Z}^n.$$

Demonstração. Sejam $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C$. Para cada $i \in \{1, 2\}$, escrevemos $\boldsymbol{c}_i$ da seguinte forma

$$\boldsymbol{c}_i = \boldsymbol{c}_{i,0} + \cdots + \boldsymbol{c}_{i,a-2}X^{a-2} + \boldsymbol{c}_{i,a-1}X^{a-1},$$

em que $\boldsymbol{c}_{i,0}, \ldots, \boldsymbol{c}_{i,a-2}, \boldsymbol{c}_{i,a-1} \in \mathbb{Z}_q^n$. Donde segue que

$$\begin{aligned}
\phi(\boldsymbol{c}_1) &= \sigma(\boldsymbol{c}_{1,0}) + \cdots + \sigma(\boldsymbol{c}_{1,a-2})q^{a-2} + \sigma(\boldsymbol{c}_{1,a-1})q^{a-1}, \\
\phi(\boldsymbol{c}_2) &= \sigma(\boldsymbol{c}_{2,0}) + \cdots + \sigma(\boldsymbol{c}_{2,a-2})q^{a-2} + \sigma(\boldsymbol{c}_{2,a-1})q^{a-1} \quad \text{e} \\
\phi(\boldsymbol{c}_1 + \boldsymbol{c}_2) &= \sigma(\boldsymbol{c}_{1,0} + \boldsymbol{c}_{2,0}) + \cdots + \sigma(\boldsymbol{c}_{1,a-2} + \boldsymbol{c}_{2,a-2})q^{a-2} + \sigma(\boldsymbol{c}_{1,a-1} + \boldsymbol{c}_{2,a-1})q^{a-1}.
\end{aligned}$$

Usando as três igualdades acima e o Lema 3.2.2, obtemos

$$\phi(\boldsymbol{c}_1)+\phi(\boldsymbol{c}_2)-\phi(\boldsymbol{c}_1+\boldsymbol{c}_2) = \sigma(\boldsymbol{c}_{1,0}*\boldsymbol{c}_{2,0})q+\cdots+\sigma(\boldsymbol{c}_{1,a-2}*\boldsymbol{c}_{2,a-2})q^{a-1}+\sigma(\boldsymbol{c}_{1,a-1}*\boldsymbol{c}_{2,a-1})q^a.$$

Porém, $\phi\big((\boldsymbol{c}_1 * \boldsymbol{c}_2)X\big) = \sigma(\boldsymbol{c}_{1,0} * \boldsymbol{c}_{2,0})q + \cdots + \sigma(\boldsymbol{c}_{1,a-2} * \boldsymbol{c}_{2,a-2})q^{a-1}$, logo

$$\phi(\boldsymbol{c}_1) + \phi(\boldsymbol{c}_2) - \phi(\boldsymbol{c}_1 + \boldsymbol{c}_2) = \phi\big((\boldsymbol{c}_1 * \boldsymbol{c}_2)X\big) + q^a\boldsymbol{z},$$

em que $\boldsymbol{z} = \sigma(\boldsymbol{c}_{1,a-1} * \boldsymbol{c}_{2,a-1}) \in \mathbb{Z}^n$. □

Teorema 3.3.2. *Seja C um código linear sobre $R_{a,q}$. O conjunto $\Gamma_{A'} = \phi(C) + q^a\mathbb{Z}^n$ obtido de C via Construção A' é um reticulado se, e somente se, C é fechado sob a adição zero-um deslocada.*

Demonstração. ($\Rightarrow$) Suponha que C que não é fechado sob a adição zero-um deslocada. Então existem $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C$ tais que $(\boldsymbol{c}_1 * \boldsymbol{c}_2)X \notin C$ e, logo, $\phi\big((\boldsymbol{c}_1 * \boldsymbol{c}_2)X\big) \notin \phi(C)$, uma vez que a aplicação ϕ é injetora. Observe que $\phi(\boldsymbol{c}_1), \phi(\boldsymbol{c}_2), \phi(\boldsymbol{c}_1 + \boldsymbol{c}_2) \in \phi(C) \subseteq \Gamma_{A'}$, mas $\phi(\boldsymbol{c}_1)+\phi(\boldsymbol{c}_2)-\phi(\boldsymbol{c}_1+\boldsymbol{c}_2) \notin \Gamma_{A'}$, pois $\phi(\boldsymbol{c}_1)+\phi(\boldsymbol{c}_2)-\phi(\boldsymbol{c}_1+\boldsymbol{c}_2) = \phi\big((\boldsymbol{c}_1*\boldsymbol{c}_2)X\big)+q^a\boldsymbol{z}$, para algum $\boldsymbol{z} \in \mathbb{Z}^n$ (ver Lema 3.3.1) e $\phi\big((\boldsymbol{c}_1 * \boldsymbol{c}_2)X\big) \notin \phi(C)$. Logo $\Gamma_{A'}$ não é um reticulado.
($\Leftarrow$) Suponha que C que é fechado sob a adição zero-um deslocada. Primeiramente temos que $\Gamma_{A'} \subseteq \mathbb{Z}^n$ e, consequentemente, $\Gamma_{A'}$ é um conjunto discreto. Agora, sejam $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C$.

O menor grau de um elemento $p(X) = \alpha_0 + \alpha_1 X + \cdots + \alpha_{a-1}X^{a-1} \in R_{a,q}$ é igual ao menor índice i tal que $\alpha_i \neq 0$. Por convenção o menor grau de 0 é a. Dizemos também que k é o menor grau de $\boldsymbol{c}_2$ se o mínimo entre os menores graus das entradas de $\boldsymbol{c}_2$ é igual a k. Primeiramente vamos mostrar por indução que $\phi(\boldsymbol{c}_1) + \phi(\boldsymbol{c}_2) \in \Gamma_{A'}$. Se o menor grau de $\boldsymbol{c}_2$ é a, então $\boldsymbol{c}_2 = \mathbf{0}$ e o resultado é óbvio. Suponha que o menor grau de $\boldsymbol{c}_2$ é $a-1$. Pelo Lema 3.3.1,

$$\phi(\boldsymbol{c}_1) + \phi(\boldsymbol{c}_2) - \phi(\boldsymbol{c}_1 + \boldsymbol{c}_2) = \phi\big((\boldsymbol{c}_1 * \boldsymbol{c}_2)X\big) + q^a\boldsymbol{z},$$

para algum $\boldsymbol{z} \in \mathbb{Z}^n$. Como $(\boldsymbol{c}_1 * \boldsymbol{c}_2)X = \mathbf{0}$ em $R_{a,q}$, segue que

$$\phi(\boldsymbol{c}_1) + \phi(\boldsymbol{c}_2) = \phi(\boldsymbol{c}_1 + \boldsymbol{c}_2) + q^a\boldsymbol{z} \in \Gamma_{A'}.$$

Agora, suponha que o grau de $\boldsymbol{c}_2$ é $0 \leq k \leq a-1$. Aplicando novamente o Lema 3.3.1, temos

$$\phi(\boldsymbol{c}_1) + \phi(\boldsymbol{c}_2) - \phi(\boldsymbol{c}_1 + \boldsymbol{c}_2) = \phi\big((\boldsymbol{c}_1 * \boldsymbol{c}_2)X\big) + q^a\boldsymbol{z},$$

para algum $\boldsymbol{z} \in \mathbb{Z}^n$. Como o menor grau de $(\boldsymbol{c}_1 * \boldsymbol{c}_2)X$ é maior ou igual a $k+1$, aplicando a hipótese de indução aos vetores $\boldsymbol{c}_1 + \boldsymbol{c}_2$ e $(\boldsymbol{c}_1 * \boldsymbol{c}_2)X$, obtemos

$$\phi(\boldsymbol{c}_1 + \boldsymbol{c}_2) + \phi\big((\boldsymbol{c}_1 * \boldsymbol{c}_2)X\big) \in \Gamma_{A'}.$$

Logo $\phi(\boldsymbol{c}_1) + \phi(\boldsymbol{c}_2) \in \Gamma_{A'}$. Finalmente, para cada $\boldsymbol{c} \in C$, temos

$$-\phi(\boldsymbol{c}) = (q^a - 1)\phi(\boldsymbol{c}) + q^a\phi(\boldsymbol{c}) \in \Gamma_{A'},$$

uma vez que $(q^a - 1)\phi(\boldsymbol{c}) \in \Gamma_{A'}$ e $\phi(\boldsymbol{c}) \in \mathbb{Z}^n$. Logo $\Gamma_{A'}$ é um reticulado. □

Corolário 3.3.2. *Seja $\overline{\sigma}_{q^a} : \mathbb{Z}^n \to \mathbb{Z}_{q^a}^n$ o homomorfismo canônico de anéis. Um código linear C sobre $R_{a,q}$ é fechado sob a adição zero-um deslocada se, e somente se, $\overline{\sigma}_{q^a}(\phi(C))$ é um código linear q^a-ário. Neste caso,*

$$\Gamma_{A'} = \Lambda_A\big(\overline{\sigma}_{q^a}(\phi(C))\big).$$

Demonstração. ($\Rightarrow$) Observe que $\overline{\sigma}_{q^a}(\phi(C)) = \overline{\sigma}_{q^a}(\Gamma_{A'})$ e $\Gamma_{A'}$ é um reticulado, pois C é um código linear sobre $R_{a,q}$ fechado sob a adição zero-um deslocada. Temos que $\overline{\sigma}_{q^a}(\phi(C)) \subseteq \mathbb{Z}_{q^a}^n$, $\mathbf{0} \in \overline{\sigma}_{q^a}(\phi(C))$ e dados $\boldsymbol{w}_1, \boldsymbol{w}_2 \in \overline{\sigma}_{q^a}(\phi(C)) = \overline{\sigma}_{q^a}(\Gamma_{A'})$, existem $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \Gamma_{A'}$ tais que $\boldsymbol{w}_1 = \overline{\sigma}_{q^a}(\phi(\boldsymbol{c}_1))$ e $\boldsymbol{w}_2 = \overline{\sigma}_{q^a}(\phi(\boldsymbol{c}_2))$ e consequentemente

$$\begin{aligned} \boldsymbol{w}_1 - \boldsymbol{w}_2 &= \overline{\sigma}_{q^a}(\phi(\boldsymbol{c}_1)) - \overline{\sigma}_{q^a}(\phi(c_2)) \\ &= \overline{\sigma}_{q^a}\big(\phi(\boldsymbol{c}_1) - \phi(\boldsymbol{c}_2)\big) \in \overline{\sigma}_{q^a}(\phi(C)). \end{aligned}$$

Isto mostra que $\overline{\sigma}_{q^a}(\phi(C))$ é um código linear q^a-ário.

($\Leftarrow$) Suponha que o código linear C não é fechado sob a adição zero-um deslocada. Pelo Teorema 3.3.2, segue que $\Gamma_{A'}$ não é um reticulado. Assim, existem $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \Gamma_{A'}$ tais que $\boldsymbol{v}_1 - \boldsymbol{v}_2 \notin \Gamma_{A'}$, pois $\Gamma_{A'}$ é um conjunto discreto. Como $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \Gamma_{A'}$, existem $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C$ e $\boldsymbol{z}_1, \boldsymbol{z}_2 \in \mathbb{Z}^n$ tais que $\boldsymbol{v}_1 = \phi(\boldsymbol{c}_1) + q^a\boldsymbol{z}_1$ e $v_2 = \phi(\boldsymbol{c}_2) + q^a\boldsymbol{z}_2$. Seja $\boldsymbol{w}_1 = \overline{\sigma}_{q^a}(\boldsymbol{v}_1)$ e $\boldsymbol{w}_2 = \overline{\sigma}_{q^a}(\boldsymbol{v}_2)$,

$$\boldsymbol{w}_1 - \boldsymbol{w}_2 = \overline{\sigma}_{q^a}(\boldsymbol{v}_1) - \overline{\sigma}_{q^a}(\boldsymbol{v}_2) = \overline{\sigma}_{q^a}(\boldsymbol{v}_1 - \boldsymbol{v}_2) \notin \overline{\sigma}_{q^a}(\phi(C)),$$

pois se $\overline{\sigma}_{q^a}(\boldsymbol{v}_1 - \boldsymbol{v}_2) = \overline{\sigma}_{q^a}(\phi(\boldsymbol{c}))$ para algum $\boldsymbol{c} \in C$, então $\boldsymbol{v}_1 - \boldsymbol{v}_2 = \phi(\boldsymbol{c}) + q^a\boldsymbol{z}$ para algum $\boldsymbol{z} \in \mathbb{Z}^n$, isto é, $\boldsymbol{v}_1 - \boldsymbol{v}_2 \in \Gamma_{A'}$. Logo $\overline{\sigma}_{q^a}(\phi(C))$ não é um código linear.

Portanto um código linear C sobre $R_{a,q}$ é fechado sob a adição zero-um deslocada se, e somente se, $\overline{\sigma}_{q^a}(\phi(C))$ é um código linear. Finalmente, note que se $\overline{\sigma}_{q^a}(\phi(C))$ é um código linear, então o reticulado obtido via Construção A usando o código linear $\overline{\sigma}_{q^a}(\phi(C))$ é

$$\Lambda_A\big(\overline{\sigma}_{q^a}(\phi(C))\big) = \sigma_{q^a}\big(\overline{\sigma}_{q^a}(\phi(C))\big) + q^a\mathbb{Z}^n = \phi(C) + q^a\mathbb{Z}^n = \Gamma_{A'}.$$

□

Considerações finais e perspectivas

Nos Capítulos 1 e 2 e na Seção 3.1 procuramos dar uma redação abrangente sobre códigos e reticulados incluindo os principais resultados e discussões originais a serem utilizados no restante do Capítulo 3. Verificamos que a região de Voronoi de um reticulado nas métricas da soma e do máximo nem sempre são regiões fundamentais do mesmo (Exemplo 1.4.2). Mostramos que o reticulado tridimensional de maior densidade na métrica da soma pode ser obtido via Construção A (Exemplo 3.1.2). No Capítulo 3, as Construções D, D′ e $\overline{\mathrm{D}}$ são generalizadas para códigos lineares q-ários ($q \in \mathbb{N}$) e vários resultados de códigos binários são estendidos para códigos q-ários (Seções 3.2.1, 3.2.2 e 3.2.3). Definimos a adição zero-um em $\mathbb{Z}_q^n$ (Definição 3.2.7) e mostramos que a Construção $\overline{\mathrm{D}}$ produz um reticulado se, e somente se, a cadeia de códigos utilizada é fechada sob esta adição (Teorema 3.2.8). Também são fornecidas fórmulas fechadas e limitantes para a distância da soma mínima de reticulados obtidos via Construções D, D′ e $\overline{\mathrm{D}}$ em termos das distâncias de Lee dos códigos utilizados (Seção 3.2.5). Introduzimos a Construção A′ a partir de códigos lineares sobre o anel quociente $\mathbb{Z}_q[X]/(X^a)$ e mostramos que a mesma produz um reticulado se, e somente se, o código utilizado é fechado sob a adição zero-um deslocada (Seção 3.3). Conexões entre as construções supracitadas também são fornecidas (Seções 3.2.4 e 3.3).

Como possíveis perspectivas futuras de pesquisa em continuidade deste trabalho, colocamos:

- Estudar a distância mínima de reticulados obtidos via Construções D, D′ e $\overline{\mathrm{D}}$ a partir de códigos q-ários considerando outras métricas.

- Estudar e discutir possíveis vantagens das construções aqui apresentadas em possíveis aplicações.

- Pesquisar possíveis construções de reticulados densos na métrica euclidiana e da soma via Construção D (resp. D′ ou $\overline{\mathrm{D}}$) a partir de códigos q-ários.

- Seja R um subanel discreto de $\mathbb{C}$ formando um domínio de ideais principais (por exemplo, $R = \mathbb{Z}[i]$ ou $R = \mathbb{Z}[(-1 + i\sqrt{3})/2]$), p um primo em R e $R_p = R/(p)$, isto é, R_p é o anel quociente de R pelo ideal gerado por p (R_p é um corpo). Em [14] é introduzida a "Construção D complexa", a qual relaciona reticulados (R-*lattices*)

com cadeias de códigos lineares sobre R_p. Nesse contexto, surgem as seguintes questões: 1) Podemos generalizar as Construções D′ e $\overline{\mathrm{D}}$ para cadeias de códigos sobre R_p? 2) Dentre os resultados apresentados neste trabalho, quais podem ser estendidos?

Bibliografia

[1] S. Axler. *Linear Algebra Done Right*. Undergraduate Texts in Mathematics, Springer, 3rd Ed., 2015.

[2] E. S. Barnes e N. J. A. Sloane. New lattice packings of spheres. *Canad. J. Math.*, 35: 117–130, 1983.

[3] A. F. Beardon. *The geometry of discrete groups*. Springer, 1995.

[4] J. L. Boldrini, S. I. R. Costa, V. L. Figueiredo e H. G. Wetzler. *Algebra Linear*. 3ª Ed., Harbra, 1986.

[5] A. Campello. Reticulados, Projeções e Aplicações à Teoria da Informação. Tese de Doutorado, Unicamp, 2014.

[6] A. Campello, G. C. Jorge e S. R. I. Costa. Reticulados q-ários na norma l_p e uma generalização da métrica de Lee. *Simpósio Brasileiro de Telecomunicações (SBrT)*, Brasília - DF, 2012.

[7] A. Campello, G. C. Jorge, J. E. Strapasson e S. R. I. Costa. Perfect codes in the l_p metric. *European Journal of Combinatorics*, 53:72–85, 2016.

[8] H. Cohn e A. Kumar. Optimality and uniqueness of the Leech lattice among lattices. *Annals of Mathematics*, Princeton, 170:1003–1050, 2009.

[9] J. H. Conway e N. J. A. Sloane. *Sphere Packings, Lattices and Groups*. Springer Verlag, New York, 3rd Ed., 1998.

[10] S. I. R. Costa, A. Campello, G. C. Jorge, J. E. Strapasson e C. Qureshi. Codes and lattices in the l_p metric, *IEEE Information Theory and Applications Workshop*, 2014.

[11] S. T. Dougherty e H. Liu. Independence of vectors in codes over rings. *Designs, Codes and Cryptography*, 51: 55–68, 2009.

[12] T. Etzion, A. Vardy e E. Yaakobi. Dense Error-Correcting Codes in the Lee Metric. *IEEE Information Theory Workshop*, Dublin, Ireland, 2010.

[13] T. Etzion, A. Vardy e E. Yaakobi. Coding for the lee and manhattan metrics with weighing matrices. *IEEE Transactions on Information Theory*, 59(10):6712–6723, 2013.

[14] C. Feng, D. Silva e F. R. Kschischang. Lattice network coding over finite rings. *Proc. 12th Canadian Workshop Inform. Theory*, Kelowna, BC, 78–81, 2011.

[15] G. D. Forney. Coset Codes-Part I: Introduction and Geometrical Classification, *IEEE Trans. Inform. Theory*, 34(5):1123–1151, 1988.

[16] G. D. Forney. Coset Codes-Part II: Binary Lattices and Related Codes. *IEEE Trans. Inform. Theory*, 34(5):1152–1187, 1988.

[17] S. W. Golomb e L. R. Welch. Perfect codes in the Lee metric and the packing of polyominos. *SIAM Journal Applied Math.*, 18:302–317, 1970.

[18] R. Hamming. Error Detecting and Error Correcting Codes. *Technical Report 2. Bell Syst. Tech. Journal*, 29(2):147–160, 1950.

[19] J. Harshan, E. Viterbo e J.-C. Belfiore. Construction of Barnes-Wall Lattices from Linear Codes over Rings. *Proceedings of the IEEE International Symposium on Information Theory*, Cambridge, MA, 3110–3114, 2012.

[20] J. Harshan, E. Viterbo e J.-C. Belfiore. Practical Encoders and Decoders for Euclidean Codes from Barnes-Wall Lattices. *IEEE Transactions on Communications*, 61(11): 4417–4427, 2013.

[21] A. Hefez e M. L. T. Vitella. *Códigos corretores de erros*. Instituto Nacional de Matemática Pura e Aplicada, IMPA, 2002.

[22] Yu-Chih Huang e Krishna R. Narayanan. Construction π_A and π_D Lattices: Construction, Goodness, and Decoding Algorithms. Available on http://arxiv.org/pdf/1506.08269, 2015.

[23] G. C. Jorge. Reticulados q-ários e Algébricos. Tese de Doutorado, Unicamp, 2012.

[24] G. C. Jorge, A. C. Campello e S. I. R Costa. q-ary lattices in the l_p norm and a generalization of the Lee metric. *International Workshop on Coding and Cryptography*, Bergen, Norway, 2013.

[25] W. Kositwattanarerk e F. Oggier. Connections Between Construction D and Related Constructions of Lattices. *Des. Codes Cryptogr.*, 73:441–455, 2014.

[26] W. Kositwattanarerk e F. Oggier. On Construction D and Related Constructions of Lattices from Linear Codes. *Proc. of the Int. Workshop on Coding and Cryptography*, Bergen, Norway, 428–437, 2013.

[27] C. Y. Lee. Some properties of nonbinary error-correcting code. *IRE Trans. on Inform. Theory*, v. IT-4, 72–82, 1958.

[28] J. Leech e N. J. A. Sloane. Sphere Packings and Error-Correcting Codes. *Can. J. Math.*, 23(4): 718–745, 1971.

[29] E. L. Lima. *Curso de análise* vol. 2. Coleção Projeto Euclides, IMPA, 11ª Ed, 2007.

[30] E. L. Lima. *Espaços métricos*. Coleção Projeto Euclides, IMPA, 5ª Ed, 2015.

[31] S. Liu, Y. Hong e E. Viterbo. Unshared Secret Key Cryptography. *IEEE Transactions on Wireless Communications*, 13(12):6670–6683, 2014.

[32] D. Micciancio e O. Regev. *Lattice-Based Cryptography in Post Quantum Cryptography*, D. J. Bernstein, J. Buchmann, E. Dahmen, Springer, 147–191, 2009.

[33] H. Minkowski. Dichteste gitterformige lagerung kongruenter korper. *Nachrichten Ges. Wiss. Gottingen*, 311–355, 1904.

[34] G. H. Norton e A. Salagean. On the Structure of Linear and Cyclic Codes over a Finite Chain Ring. *Applicable Alg. Eng., Commun. Comput.*, 10:489–506, 2000.

[35] Y. H. Park. Modular independence and generator matrices for codes over $\mathbb{Z}_m$. *Designs, Codes and Cryptography*, 50:147–162, 2009.

[36] C. Peikert. A decade of lattice cryptography. Cryptology ePrint Archive, Report 2015/939. http://eprint.iacr.org/2015/939, 2015.

[37] M.-R. Sadeghi, A. H. Banihashemi e D. Panario. Low-density parity-check lattices: construction and decoding analysis. *IEEE Trans. Inf. Theory*, 52(10):4481–4495, 2006.

[38] A. Sakzad, M.-R. Sadeghi e D. Panario. Turbo Lattices: Construction and Error Decoding Performance. Available on arXiv:1108.1873v3, 2012.

[39] P. R. B. da Silva e D. Silva. Design of Lattice Network Codes Based on Construction D. *International Telecommunications Symposium*, 2014.

[40] J. A. Rush e N. J. A. Sloane. An improvement to the Minkowski-Hlawka bound for packing superballs. *Mathematika*, 34:8–18, 1987.

[41] E. Strey e S. I. R. Costa. Bounds for the ℓ_1-distance of q-ary lattices obtained via Constructions D, D$'$ and $\overline{\text{D}}$. *Comp. and Applied Mathematics*, 2017. DOI 10.1007/s40314-017-0453-x

[42] E. Strey e S. I. R. Costa. Lattices from codes over $\mathbb{Z}_q$: Generalization of Constructions D, D′ and $\overline{\mathrm{D}}$. *Des. Codes Cryptogr.*, 2016. DOI: 10.1007/s10623-016-0289-1.

[43] E. Strey e S. I. R. Costa. Limitantes para a distância da soma em reticulados obtidos via Construção D e suas variações. *Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT)*, Santarém - PA, 548–552, 2016.

[44] E. Strey e S. I. R. Costa. Reticulados a partir de Códigos sobre Anéis Finitos: Conexões entre as Construções D, D′ e $\overline{D}$. *Proc. Ser. Braz. Soc. Appl. Comput. Math.*, 5(1), 2017. DOI: 10.5540/03.2017.005.01.0228

[45] G. Strey. A série teta e a função de sigilo de um reticulado. Dissertação de Mestrado, Unicamp, 2016.

[46] S. Szabo e J. A. Wood. Properties of dual codes defined by nondegenerate forms. *J. Algebra Comb. Discrete Appl.*, 4(2): 105–113, 2017.

[47] L. Y. Tsuchiya. Um estudo de reticulados q-ários com a métrica da soma. Dissertação de Mestrado, Unicamp, 2012.

[48] W. Ulrich. Non-binary error correction codes. *Bell Sys. Journal*, 36:1341–1387, 1957.

[49] J. A. Wood. Duality for modules over finite rings and applications to coding theory. *Amer. J. Math.*, 121(3):555–575, 1999.

[50] I. Woungang, S. Misra e S. Chandra Misra. Selected Topics in Information and Coding Theory. *Series on Coding Theory and Cryptology*, 7:41–76, 2010. ISBN: 978-981-283-716-5.

[51] Y. Yan, C. Ling e X. Wu. Polar Lattices: Where Arikan Meets Forney. *IEEE Int. Symp. Inform. Theory*, Istanbul, Turkey, 1292–1296, 2013.

[52] R. Zamir. *Lattice Coding of Signals and Networks: A Structured Coding Approach to Quantization, Modulation and Multi-user Information Theory*. Cambridge University Press, 2014.

[53] R. Zamir. Lattices are everywhere. *Information Theory and Applications Workshop*, San Diego-CA, 392–421, 2009.

Índice Remissivo