

Constelações de sinais via os anéis de inteiros de Gauss e de Eisenstein-Jacobi

Antonio Aparecido de Andrade,

Tatiane da Silva Evangelista*

Depto de Matemática, IBILCE, UNESP,

15054-000, São José do Rio Preto, SP

E-mail: andrade@ibilce.unesp.br, tatilista@bol.com.br

1 Introdução

O problema de construção de sinais que possuam boas propriedades geométricas e boas estruturas algébricas é fundamental e relevante tanto no aspecto da sistematicidade de geração como na implementação prática dos moduladores e demoduladores. Este trabalho, está organizado da seguinte maneira. Na Seção 2, faremos uma breve revisão de corpos quadráticos, decomposição de ideais em uma extensão quadrática. Na Seção 3, veremos as constelações de sinais casadas a $GF(p)$ e definiremos a distância de Mannheim via corpos quadráticos. Na Seção 4, fornecemos o algoritmo para rotular os elementos dos corpos quadráticos. Na Seção 5, veremos a região de Voronoi e a distância máxima entre os elementos de $A_p[\rho]$, onde $\rho = w = \frac{1+\sqrt{-3}}{2}$, isto é, no caso em que $d = -3$ (para $A_p[i]$ é análogo). Finalmente, na Seção 6, as conclusões deste trabalho são apresentadas.

2 Conceitos preliminares

Nesta seção, veremos os conceitos de elemento inteiro, norma de um elemento, corpos quadráticos e a decomposição de ideais estendidos.

Definição 1 *Sejam $A \subseteq B$ anéis. Dizemos que um elemento $\alpha \in B$ é inteiro sobre A , se α é uma raiz de um polinômio mônico com coeficientes em A .*

O conjunto dos elementos de B que são inteiros sobre A é um anel que denotamos por \mathcal{O}_B .

Definição 2 *Sejam $\mathbb{K} \subset \mathbb{L}$ uma extensão finita de corpos de grau n e $\alpha \in \mathbb{L}$. Definimos a norma de α sobre \mathbb{K} como $N(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$, onde $\sigma_i : \mathbb{L} \rightarrow \mathbb{C}$, para $i = 1, \dots, n$, são os \mathbb{K} -homomorfismos.*

Definição 3 *Um corpo quadrático é uma extensão de grau 2 de \mathbb{Q} .*

Sejam A um anel de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão finita de \mathbb{K} de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de A em \mathbb{L} . Se $\mathcal{P} \subset \mathcal{A}$ é um ideal primo, então $\mathcal{P}\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{L}}$, é um ideal e pode ser expresso de modo único na forma $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g \mathcal{Q}_i^{e_i}$, onde os \mathcal{Q}_i são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e os e_i são elementos de \mathbb{Z} , para $i = 1, \dots, g$.

Proposição 1 *Os ideais primos \mathcal{Q}_i da fatoração $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g \mathcal{Q}_i^{e_i}$ são os únicos ideais primos de $\mathcal{O}_{\mathbb{L}}$ tais que $\mathcal{Q}_i \cap A = \mathcal{P}$, para $i = 1, \dots, g$.*

Definição 4 *Se $\mathcal{P} \subset A$ e $\mathcal{Q} \subset \mathcal{O}_{\mathbb{L}}$ são ideais primos tal que $\mathcal{P} = A \cap \mathcal{Q}$, dizemos que \mathcal{Q} está acima de \mathcal{P} .*

Lema 1 *Com as notações anteriores temos que*

- $\frac{A}{\mathcal{P}}$ e $\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i}$ são corpos e que $\frac{A}{\mathcal{P}}$ pode ser identificado como um subcorpo de $\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i}$, para $i = 1, 2, \dots, g$.
- $\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i}$ é um espaço vetorial de dimensão finita sobre $\frac{A}{\mathcal{P}}$, para $i = 1, \dots, g$.

Teorema 1 *(Teorema da Igualdade Fundamental)*
 $\sum_{i=1}^g e_i f_i = [\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}\mathcal{O}_{\mathbb{L}}} : \frac{A}{\mathcal{P}}] = n$, onde $f_i = [\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{Q}_i} : \frac{A}{\mathcal{P}}]$ chamado grau residual.

Sejam $d \in \mathbb{Z}$ livre de quadrados, $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de \mathbb{K} e p um número primo. Seja $p\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^g \mathcal{Q}_i^{e_i}$ a decomposição do ideal $p\mathcal{O}_{\mathbb{K}}$ como um produto de ideais primos de $\mathcal{O}_{\mathbb{K}}$. Pelo Teorema 1, segue que $\sum_{i=1}^g e_i f_i = 2$. Assim, $g \leq 2$ e temos os seguintes casos:

- Se $g = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$, então p se decompõe em $\mathcal{O}_{\mathbb{K}}$, ou seja, $p\mathcal{O}_{\mathbb{K}} = \mathcal{Q}_1\mathcal{Q}_2$, onde $\mathcal{Q}_1, \mathcal{Q}_2$ são ideais primos distintos de $\mathcal{O}_{\mathbb{K}}$ acima de $p\mathbb{Z}$.

*bolsista da Fundação de Amparo à Pesquisa FAPESP, processo: 03/09445-3

2. Se $g = 1$, $e_1 = 1$, $f_1 = 2$, então p é inerte em $\mathcal{O}_{\mathbb{K}}$, ou seja, $p\mathcal{O}_{\mathbb{K}} = \mathcal{Q}$, onde \mathcal{Q} é um ideal primo de $\mathcal{O}_{\mathbb{K}}$ acima de $p\mathbb{Z}$.
3. Se $g = 1$, $e_1 = 2$, $f_1 = 1$, então p ramifica em $\mathcal{O}_{\mathbb{K}}$, ou seja, $p\mathcal{O}_{\mathbb{K}} = \mathcal{Q}^2$, onde \mathcal{Q} é um ideal primo de $\mathcal{O}_{\mathbb{K}}$ acima de $p\mathbb{Z}$.

Proposição 2

1. Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{-1})$ e $p \equiv 1 \pmod{4}$ onde p é um primo ímpar, então p se decompõe em $\mathcal{O}_{\mathbb{K}}$.
2. Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$ e $p \equiv 1 \pmod{6}$ onde p é um primo ímpar, então p se decompõe em $\mathcal{O}_{\mathbb{K}}$.

3 Constelações de sinais

Nesta seção, apresentamos o conceito de constelações de sinais e a distância de Mannheim via corpos quadráticos.

Definição 5 Uma constelação de sinais é um subconjunto finito discreto de pontos no \mathbb{R}^2 em que seja possível realizar uma identificação destes pontos por sinais.

Definição 6 Uma constelação de sinais S é dita casada com um grupo G , mediante a uma distância d , se existe uma aplicação μ de G sobre S tal que $d(\mu(g_1), \mu(g_2)) = d(\mu(e), \mu(g_1^{-1} * g_2))$, para todo g_1 e g_2 pertencentes a G , onde e é o elemento neutro de G e $d(\cdot, \cdot)$ é uma distância em S . Neste caso, a aplicação μ é chamada de aplicação casada. Além disso, se μ for injetora chamamos μ^{-1} de rotulamento casado.

Sejam $\mathbb{Q}(\sqrt{d})$ um extensão quadrática, com d livre de quadrados e $\mathbb{Z}[\rho]$ o anel dos inteiros de $\mathbb{Q}(\sqrt{d})$. Assim, se $d = -1$, então $\mathbb{Z}[\rho] = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$, é o anel dos inteiros de Gauss, e se $d = -3$, então $\mathbb{Z}[\rho] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \mathbb{Z}[w]$, é o anel dos inteiros de Eisenstein-Jacobi. Além disso, temos que $\mathbb{Z}[\rho]$, onde $\rho = i$ ou $\rho = w$, é um domínio de ideais principais. Assim, todo ideal primo \mathcal{I} de $\mathbb{Z}[\rho]$ é escrito na forma

$$\mathcal{I} = \langle \pi \rangle = \pi \mathbb{Z}[\rho] = \{\pi\alpha : \alpha \in \mathbb{Z}[\rho]\},$$

onde $\pi = a + b\rho \in \mathbb{Z}[\rho]$ é um elemento primo. Temos que i é uma raiz quarta primitiva da unidade e w é uma raiz sexta primitiva da unidade.

Observação 1 Se $\pi = a + b\rho \in \mathbb{Z}[\rho]$, então a norma de π é dada por:

$$N(\pi) = N(a + b\rho) = (a + b\rho)\overline{(a + b\rho)} = \begin{cases} a^2 - db^2 & \text{se } d \equiv 2, 3 \pmod{4} \\ a^2 + ab + \frac{1-d}{4}b^2 & \text{se } d \equiv 1 \pmod{4}, \end{cases}$$

onde $\overline{a + b\rho}$ denota a conjugação complexa de $a + b\rho$. Assim, temos que se $d = -1$, então $N(\pi) = a^2 + b^2$ e se $d = -3$, então $N(\pi) = a^2 + ab + b^2$.

Se p é um número ímpar tal que $p \equiv 1 \pmod{4}$ se $d = -1$ ou $p \equiv 1 \pmod{6}$ se $d = -3$, então p se decompõe em $\mathbb{Z}[\rho]$. Nosso objetivo é determinar um rotulamento casado entre o grupo aditivo de $GF(p)$ e um subconjunto conveniente do \mathbb{R}^2 . Em ambos os casos temos que p fatora-se como $p = \pi\bar{\pi}$, onde $N(\pi) = p$, e que o ideal primo $p\mathbb{Z}$ de \mathbb{Z} fatora-se completamente em $\mathbb{Z}[\rho]$, isto é, $p\mathbb{Z}[\rho] = \mathcal{I}\bar{\mathcal{I}}$, onde $\mathcal{I} = \langle \pi \rangle$ e $\bar{\mathcal{I}} = \langle \bar{\pi} \rangle$ são dois ideais primos distintos de $\mathbb{Z}[\rho]$. Como $\mathbb{Z}[\rho]$ é um domínio principal segue que seus ideais primos \mathcal{I} não nulos são maximais. Portanto, o quociente $\frac{\mathbb{Z}[\rho]}{\mathcal{I}}$ é um corpo de ordem p , que denotamos por $A_p[\rho]$.

Teorema 2 Se $p \in \mathbb{Z}$ é um número primo ímpar, que fatora-se num produto de dois primos conjugados $\pi = a + b\rho$ e $\bar{\pi}$ no anel dos inteiros algébricos $\mathbb{Z}[\rho]$, isto é, $p = \pi\bar{\pi}$, então em cada classe lateral $l + \mathcal{I}$, onde $\mathcal{I} = \langle \pi \rangle$ e $l = 0, 1, \dots, p-1$, existe um único elemento $\alpha_l = l + \mu\pi$ com norma euclidiana mínima.

Pelo Teorema 2, podemos considerar $A_p[\rho] = \{\alpha_0, \alpha_1, \dots, \alpha_{p-1}\} \subset \mathbb{C}$ um conjunto de representantes de \mathcal{I} em $\mathbb{Z}[\rho]$, satisfazendo $\alpha_l \equiv l \pmod{\mathcal{I}}$ e $N(\alpha_l)$ mínima, munido das seguintes operações de adição e multiplicação, definidas por: $\alpha_i + \alpha_j = \alpha_k$ e $\alpha_i\alpha_j = \alpha_k$, onde $k \equiv i + j \pmod{p}$ e $k = ij \pmod{p}$ tal que $i, j = 0, 1, \dots, p-1$. Assim, $A_p[\rho]$ com essas operações é um corpo com p elementos, isomorfo a $GF(p)$.

Definição 7 Sejam $\alpha, \beta \in A_p[\rho]$ tal que $\alpha - \beta \equiv \gamma \pmod{\mathcal{I}}$, com $\gamma \in A_p[\rho]$. Definimos a distância de Mannheim, entre α e β como $d_{\mathcal{M}}(\alpha, \beta) = w_{\mathcal{M}}(\gamma) = |\alpha| + |\beta|$, onde $\gamma = a + b\rho \in A_p[\rho]$.

Assim, temos que $d_{\mathcal{M}}(\cdot, \cdot)$ é uma métrica em $A_p[\rho]$, e portanto temos definido, de modo natural um rotulamento casado do conjunto de sinais $A_p[\rho] = \{\alpha_0, \alpha_1, \dots, \alpha_{p-1}\} \subset \mathbb{Z}[\rho]$ com o grupo aditivo de $GF(p)$. A aplicação casada μ de $GF(p)$ sobre $A_p[\rho]$ é definida por $\mu(\bar{r}) = \alpha_r$, para $r = 0, 1, \dots, p-1$. Para determinar o rótulo de cada elemento do conjunto de sinais $A_p[\rho] = \{\alpha_0, \dots, \alpha_{p-1}\} \subset \mathbb{Z}[\rho]$ por um elemento do corpo $GF(p)$, usamos o procedimento dado na Seção 4.

4 Algoritmo para rotular os elementos de $A_p[\rho]$

Nesta seção, apresentamos os passos do algoritmo para rotular os elementos de $A_p[\rho]$ por elementos de $GF(p)$ e damos exemplos via os anéis de inteiros de Eisenstein-Jacobi e Gauss. O algoritmo para rotular os elementos de $A_p[\rho]$ consiste dos seguintes passos:

1. Tome um número primo p que se decompõe-se completamente em $\mathbb{Z}[\rho]$, e seja $\pi = a+b\rho \in \mathbb{Z}[\rho]$ tal que $N(\pi) = p$.
2. Tome $s \in \mathbb{Z}$ a única solução na variável r da equação $a+br \equiv 0 \pmod{p}$, onde $0 \leq r \leq p-1$.
3. O elemento $l \in GF(p)$ é o rótulo do ponto $\alpha_l = x+yp \in \mathbb{Z}[\rho]$ se $x+ys \equiv l \pmod{p}$ e se $N(\alpha_l)$ for mínima.

Garantimos a unicidade do ponto α_l pelo Teorema 2. Para melhorar o processo de rotulamento devemos ordenar os valores de l em ordem crescente, e em seguida, para cada ponto $\alpha_l = x+yp \in A_p[\rho]$ atribuímos o rótulo l , onde $l \equiv x+ys \pmod{p}$, sendo $N(\alpha_l)$ mínima.

Exemplo 1 Sejam $d = -3$ e $p = 13 \equiv 1 \pmod{6}$. Aplicando o algoritmo temos:

1. Uma solução da equação $N(\pi) = a^2+ab+b^2 = p = 13$ é dada por $(a,b) = (-1,4)$. Assim, podemos tomar $\pi = -1+4w \in \mathbb{Z}[w]$.
2. A única solução da equação $a+br = -1+4r \equiv 0 \pmod{13}$, onde $0 \leq r \leq 12$, é $r = 10$.
3. Assim, $l \in GF(13)$ será o rótulo do ponto $\alpha_l = x+yw$ de $A_{13}[w]$, se $x+10y \equiv l \pmod{13}$ e se $N(\alpha_l)$ for mínimo.

Os elementos de $A_{13}[w]$ são dados pela Tabela 1, assim como sua representação geométrica pela Figura 1.

| (x, y) | $N(\alpha)$ | $x + 10y \equiv l \pmod{13}$ |
|----------|-------------|------------------------------|
| (0, 0) | 0 | 0 |
| (1, 0) | 1 | 1 |
| (-2, -1) | 3 | 2 |
| (-1, -1) | 1 | 3 |
| (1, -1) | 1 | 4 |
| (2, -1) | 3 | 5 |
| (0, 2) | 3 | 6 |
| (0, -2) | 3 | 7 |
| (-2, 1) | 3 | 8 |
| (-1, 1) | 1 | 9 |
| (1, 1) | 1 | 10 |
| (2, 1) | 3 | 11 |
| (-1, 0) | 1 | 12 |

Tabela 1: Constelação com 13 sinais rotulados por $GF(13)$ e $d = -3$

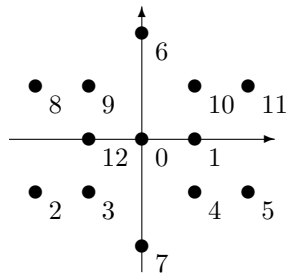


Figura 1

Exemplo 2 Sejam $d = -1$ e $p = 17 \equiv 1 \pmod{4}$. Aplicando o algoritmo, temos:

1. Uma solução da equação $N(\pi) = a^2+b^2 = p = 17$ é dada por $(a,b) = (4,1)$. Assim, podemos tomar $\pi = 4+i \in \mathbb{Z}[i]$.
2. A única solução da equação $a+br = 4+r \equiv 0 \pmod{17}$, onde $0 \leq r \leq 16$, é $r = 13$.
3. Assim, $l \in GF(17)$ será o rótulo do ponto $\alpha_l = x+yi$ de $A_{17}[i]$, se $x+13y \equiv l \pmod{17}$ e $N(\alpha_l)$ é mínima.

Os elementos de $A_{17}[i]$ são dados na Tabela 2 e sua representação geométrica na Figura 2.

| (x, y) | $N(\alpha)$ | $x + 13y \equiv l \pmod{17}$ |
|----------|-------------|------------------------------|
| (0, 0) | 0 | 0 |
| (1, 0) | 1 | 1 |
| (2, 0) | 4 | 2 |
| (-1, -1) | 2 | 3 |
| (0, -1) | 1 | 4 |
| (1, -1) | 2 | 5 |
| (2, -1) | 5 | 6 |
| (-1, -2) | 5 | 7 |
| (0, -2) | 4 | 8 |
| (0, 2) | 4 | 9 |
| (1, 2) | 5 | 10 |
| (-2, 1) | 5 | 11 |
| (-1, 1) | 2 | 12 |
| (0, 1) | 1 | 13 |
| (1, 1) | 2 | 14 |
| (-2, 0) | 4 | 15 |
| (-1, 0) | 1 | 16 |

Tabela 2: Constelação com 17 sinais rotulados por $GF(17)$ e $d = -1$

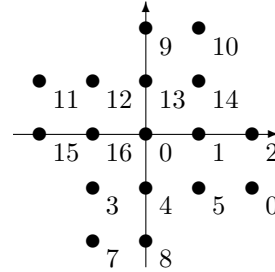


Figura 2

Observação 2 As constelações são simétricas em relação ao primo p considerado.

5 Região de Voronoi

Nesta seção, determinamos a distância máxima de Mannheim entre os elementos de $A_p[\rho]$, onde $\rho = w = \frac{1+\sqrt{-3}}{2}$, isto é no caso em que $d = -3$ (para $A_p[i]$ é análogo).

Definição 8 Dizemos que um subconjunto discreto Λ de pontos do \mathbb{R}^2 é um reticulado de dimensão n se este for um \mathbb{Z} -módulo, gerado através de uma base $\{e_1, \dots, e_n\}$.

Sejam $\mathbb{Z}[w]$, onde $w = \frac{1+\sqrt{-3}}{2}$, o anel de inteiros algébricos de $\mathbb{Q}(\sqrt{-3})$ e um elemento $\pi = a + bw \in \mathbb{Z}[w]$ tal que $N(\pi) = a^2 + ab + b^2 = p$, onde $p \equiv 1 \pmod{6}$. Assim, o ideal $p\mathbb{Z}$ decompõe-se completamente em $\mathbb{Z}[w]$. Podemos assumir sempre que $a, b > 0$, se $\pi = a + bw$, uma vez que o anel dos inteiros algébricos $\mathbb{Z}[w]$ é um domínio em que vale a fatoração única a menos das unidades.

Definição 9 *Sejam \mathcal{S} um subconjunto discreto do \mathbb{R}^n e $X_0 \in \mathcal{S}$. A região de Voronoi de X_0 em \mathcal{S} consiste dos pontos do \mathbb{R}^n que estão mais próximos de X_0 do que qualquer outro ponto de \mathcal{S} , ou seja, $\mathcal{V}(X_0) = \{X \in \mathbb{R}^n : d(X, X_0) \leq d(X, Y), \forall Y \in \mathcal{S}, Y \neq X_0\}$. Dizemos que um ponto Y de \mathcal{S} , $Y \neq X$, é um vizinho de X se $d(X, Y) \leq d(X, Z)$, para todo Z de \mathcal{S} .*

Estamos interessados nos casos em que o subconjunto discreto \mathcal{S} do \mathbb{R}^2 tenha estrutura de \mathbb{Z} -módulo, ou seja, quando \mathcal{S} é um reticulado. Assim, quando X é um ponto do reticulado \mathcal{S} , temos que $\mathcal{V}(X) = X + \mathcal{V}(0)$ e Y é um vizinho de X se, e somente se, $Y - X$ é um vizinho de zero.

A imagem via o homomorfismo de Minkowsk do anel de inteiros $\mathbb{Z}[\rho]$ de uma extensão quadrática $\mathbb{Q}(\sqrt{d})$ de \mathbb{Q} pode ser visto como um reticulado no \mathbb{R}^2 , gerado por $\{1, \rho\}$, onde $\rho = \sqrt{-1} = i$ se $d = -1$ e $\rho = w = \frac{1+\sqrt{-3}}{2}$ se $d = -3$. Seja \mathcal{S} um subreticulado de $\mathbb{Z}[w]$ gerado por $\{\pi, w\pi\}$, com $\pi = a + bw$, $a, b \in \mathbb{Z}$ tal que $N(\pi) = p$, com $p \equiv 1 \pmod{6}$. Em $\mathbb{Z}[w]$, os vizinhos da origem são as raízes sextas da unidade, isto é, w^j para $j = 0, 1, \dots, 5$.

Nosso objetivo agora é determinar a distância máxima de Mannheim entre os pontos de $A_p[w]$. Para isso identificamos $\mathbb{Z}[w]$ com um subconjunto de \mathbb{R}^2 . Se $\pi \in \mathbb{Z}[w]$ com $\pi \neq 0$, então $\pi = a + bw$, para $a, b \in \mathbb{Z}$. Consideramos os segmentos de reta com extremidades na origem e nos pontos $w^j\pi$, para $j = 0, 1, \dots, 5$. Tomemos a reta perpendicular passando pelo ponto médio de cada um desses segmentos de reta. As intersecções das retas traçadas, formam os vértices de um hexágono \mathcal{H} , que chamamos de C_l , para $l = 1, 2, \dots, 6$. Temos que $\pi = a + bw$, com $w = \frac{1+\sqrt{-3}}{2}$, tem coordenadas (a, b) na base $\{1, w\}$ e $(\frac{2a+b}{2}, \frac{b\sqrt{3}}{2})$ na base canônica $\{1, i\}$, na qual é associado com as coordenadas C_l . Consideramos $\pi' = (\frac{-b\sqrt{3}}{2}, \frac{2a+b}{2})$, na base $\{1, i\}$, um vetor ortogonal a π . Queremos agora, determinar as coordenadas dos pontos C_l , para $l = 1, 2, \dots, 6$, na base $\{1, w\}$, que são os vértices do hexágono \mathcal{H} . Temos que $O\vec{C}_1 = \frac{\pi}{2} + \frac{1}{2} \frac{|\pi'|}{|\pi|} \frac{\sqrt{3}}{3} \pi' = \frac{\pi}{2} + \frac{\sqrt{3}}{6} \pi' = \frac{1}{2}(\frac{2a+b}{2}, \frac{b\sqrt{3}}{2}) + \frac{\sqrt{3}}{6}(\frac{-b\sqrt{3}}{2}, \frac{2a+b}{2})$. Assim, $2O\vec{C}_1 = 2[\frac{1}{2}(\frac{2a+b}{2}, \frac{b\sqrt{3}}{2}) + \frac{\sqrt{3}}{6}(\frac{-b\sqrt{3}}{2}, \frac{2a+b}{2})] = (\frac{2a+b}{2}, \frac{b\sqrt{3}}{2}) + \frac{\sqrt{3}}{3}(\frac{-b\sqrt{3}}{2}, \frac{2a+b}{2})$. Agora, $4O\vec{C}_1 = 2(2O\vec{C}_1) = 2[(\frac{2a+b}{2}, \frac{b\sqrt{3}}{2}) + \frac{\sqrt{3}}{3}(\frac{-b\sqrt{3}}{2}, \frac{2a+b}{2})] = (2a + b, b\sqrt{3}) + (-b, \frac{(2a+b)\sqrt{3}}{3}) =$

$(2a, \frac{2(a+b)\sqrt{3}}{3})$. Logo,

$$O\vec{C}_1 = (\frac{a}{2}, \frac{(a+2b)}{6}\sqrt{3}).$$

Também, podemos escrever $O\vec{C}_1 = \frac{a}{2} + \frac{(a+2b)}{2}w = \frac{a}{2} + (\frac{a+2b}{2})(\frac{1+\sqrt{-3}}{2}) = \frac{a}{2} + \frac{(a+2b)\sqrt{3}}{2} = \frac{a}{2} + \frac{a+2b}{3}(\frac{-\sqrt{-3}}{2}) + \frac{a+2b}{6} - \frac{(a+2b)}{6} = (\frac{a+2b}{3})(\frac{1+\sqrt{-3}}{2}) + \frac{3a-a-2b}{6} = \frac{a-b}{3} + \frac{(a+2b)}{3}w$.

Portanto, na base $\{1, w\}$, as coordenadas de C_1 são $C_1 = (\frac{a-b}{3}, \frac{a+2b}{3})$. As coordenadas dos pontos C_l , para $l = 2, 3, \dots, 6$, podem ser obtidos das coordenadas C_1 como $C_l = w^{l-1}C_1$. Assim, obtemos as seguintes coordenadas do hexágono \mathcal{H} .

$$\begin{aligned} C_2 &= (\frac{-(a+2b)}{3}, \frac{2a+b}{3}), \\ C_3 &= (\frac{-(2a+b)}{3}, \frac{a-b}{3}), \\ C_4 &= (\frac{-(a-b)}{3}, \frac{-(a+2b)}{3}), \\ C_5 &= (\frac{a+2b}{3}, \frac{-(2a+b)}{3}) \text{ e} \\ C_6 &= (\frac{2a+b}{3}, \frac{-(a-b)}{3}). \end{aligned}$$

Teorema 3 *Se $\pi = a + bw \in \mathbb{Z}[w]$ é tal que $N(\pi) = a^2 + ab + b^2 = p$, onde p é um primo tal que $p \equiv 1 \pmod{6}$, então a distância máxima de Mannheim entre os elementos de $A_p[w]$ é dado por $d_{\mathcal{M}, \max}(A_p[w]) = \max\{|a|, |b|, |a+b|\} - 1$.*

Teorema 4 *Se $\pi = a + bi \in \mathbb{Z}[i]$ é tal que $N(\pi) = a^2 + b^2 = p$, onde p é primo tal que $p \equiv 1 \pmod{4}$, então a distância máxima de Mannheim entre os elementos de $A_p[i]$ é dada por $d_{\mathcal{M}, \max}(A_p[i]) = \max\{|a|, |b|\} - 1$.*

Sejam as regiões semi-abertas R_1, R_2 e R_3 limitadas, respectivamente, pelos pares de retas determinadas por C_1C_6 e C_3C_4 , C_1C_2 e C_4C_5 , C_2C_3 e C_5C_6 , isto é, $R_1 = \{(x, y) \in \mathbb{R}^2 : -N(\pi) < (a+2b)y + (2a+b)x \leq N(\pi)\}$, $R_2 = \{(x, y) \in \mathbb{R}^2 : -N(\pi) < (2a+b)y + (a-b)x \leq N(\pi)\}$ e $R_3 = \{(x, y) \in \mathbb{R}^2 : -N(\pi) < (a-b)y - (a+2b)x \leq N(\pi)\}$. Seja R a intersecção dessas regiões, ou seja, $R = \bigcap_{i=1}^3 R_i$. O conjunto R tem como fronteira o hexágono \mathcal{H} . Agora, queremos determinar as coordenadas inteiras, na base $\{1, w\}$, dos pontos de R mais próximos dos vértices de \mathcal{H} e assim, mais distantes da origem. Deste modo, dado $\pi = a + bw \in \mathbb{Z}[w]$, precisamos analisar três casos da diferença $a - b$. Podemos considerar o caso $a, b > 0$ e sem perda de generalidade, podemos supor que $a > b$, pois os resultados para o caso $b > a$ são obtidos somente trocando a por b .

1. Se $a - b \equiv 0 \pmod{3}$, então $a - b \equiv 0 \pmod{3}$ e $p = a^2 + ab + b^2 = 3a^2 \pmod{3}$. Isto implica, que p não é primo. Logo, este caso é excluído.
2. Se $a - b \equiv 1 \pmod{3}$, então tomando C_j^1 , para $j = 1, 2, \dots, 6$, os pontos de coordenadas inteiras na base $\{1, w\}$ mais próximos de C_j , temos que

$$\begin{aligned} C_1^1 &= \left(\frac{a-b-1}{3}, \frac{a+2b-1}{3} \right), \\ C_2^1 &= \left(\frac{-a-2b+1}{3}, \frac{2a+b-2}{3} \right), \\ C_3^1 &= \left(\frac{-2a-b+2}{3}, \frac{a-b-1}{3} \right), \\ C_4^1 &= \left(\frac{-a+b+1}{3}, \frac{-a-2b+1}{3} \right), \\ C_5^1 &= \left(\frac{a+2b-1}{3}, \frac{-2a-b+2}{3} \right) \text{ e} \\ C_6^1 &= \left(\frac{2a+b-2}{3}, \frac{-a+b+1}{3} \right). \end{aligned}$$

3. Se $a - b \equiv 2 \pmod{3}$, então tomando C_j^2 , para $j = 1, 2, \dots, 6$, os pontos de coordenadas inteiras da base $\{1, w\}$ mais próximos de C_j , temos que

$$\begin{aligned} C_1^2 &= \left(\frac{a-b-2}{3}, \frac{a+2b-2}{3} \right), \\ C_2^2 &= \left(\frac{-a-2b+2}{3}, \frac{2a+b-1}{3} \right), \\ C_3^2 &= \left(\frac{-2a-b+1}{3}, \frac{a-b-2}{3} \right), \\ C_4^2 &= \left(\frac{-a+b+2}{3}, \frac{-a-2b+2}{3} \right), \\ C_5^2 &= \left(\frac{a+2b-2}{3}, \frac{-2a-b+1}{3} \right) \text{ e} \\ C_6^2 &= \left(\frac{2a+b-1}{3}, \frac{-a+b+2}{3} \right). \end{aligned}$$

Nosso objetivo, agora, é encontrar as relações entre os conjuntos $\mathbb{Z}[\rho]$, R , \mathcal{S} e \mathcal{H} . Assim consideremos os seguintes resultados:

Lema 2 Se $\mathcal{V} = \mathcal{V}_{\mathcal{S}}(0) = \{x \in \mathbb{R}^2 : d(x, 0) \leq d(x, y), \forall y \in \mathcal{S}, y \neq 0\}$ é a região de Voronoi da origem \mathcal{S} , então $\mathcal{V} = R$.

Lema 3 Os pontos de coordenadas inteiras de R formam um conjunto completo de representantes das classes laterais módulo o ideal gerado por π , onde $\pi \in \mathbb{Z}[w]$.

Lema 4 O conjunto \mathcal{S} é obtido a partir de $\mathbb{Z}[w]$ através de uma rotação seguida de uma homotetia. Além disso, a região de Voronoi da origem de \mathcal{S} é obtida da região de Voronoi da origem de $\mathbb{Z}[w]$ pela mesma ação. A rotação é determinada por $\theta = \arg(\pi)$ e a homotetia sendo a multiplicação por $\sqrt{N(\pi)}$, onde $\pi = a + bw \in \mathbb{Z}[w]$, com $a, b \in \mathbb{Z}$.

O próximo teorema estabelece as relações entre $\mathbb{Z}[\rho]$, R , \mathcal{S} e \mathcal{H} .

Teorema 5

1. Os pontos de coordenadas inteiras na base $\{1, w\}$ localizados no interior de \mathcal{H} formam um conjunto completo de representantes das classes laterais módulo o ideal gerado por π , onde $\pi \in \mathbb{Z}[w]$.
2. O conjunto R pode ser visto como uma região de Voronoi da origem do subreticulado \mathcal{S} .
3. A região R pode ser vista como uma rotação seguida de uma homotetia da região de Voronoi da origem do reticulado $\mathbb{Z}[w]$.

Observação 3

1. Se \mathcal{D} é um quadrado de vértices:

$$\begin{aligned} C_1 &= \left(\frac{a-b}{2}, \frac{a+2b}{2} \right); \\ C_2 &= \left(\frac{-(a+2b)}{2}, \frac{2a+b}{2} \right); \\ C_3 &= \left(\frac{-(a-b)}{2}, \frac{-(a+2b)}{2} \right) \text{ e} \\ C_4 &= \left(\frac{a+2b}{2}, \frac{-(2a+b)}{2} \right), \end{aligned}$$

então as coordenadas de R mais próximos do vértices de \mathcal{D} e mais distantes da origem são:

- Se $a - b \equiv 1 \pmod{2}$, então

$$\begin{aligned} C_1^1 &= \left(\frac{a-b-1}{2}, \frac{a+2b-1}{2} \right); \\ C_2^1 &= \left(\frac{-a-2b+1}{2}, \frac{2a+b-2}{2} \right); \\ C_3^1 &= \left(\frac{-a+b+1}{2}, \frac{-a-2b+1}{2} \right) \text{ e} \\ C_4^1 &= \left(\frac{a+2b-1}{2}, \frac{-2a-b+2}{2} \right). \end{aligned}$$

- Se $a - b \equiv 2 \pmod{2}$, então

$$\begin{aligned} C_1^2 &= \left(\frac{a-b-2}{2}, \frac{a+2b-2}{2} \right); \\ C_2^2 &= \left(\frac{-a-2b+2}{2}, \frac{2a+b-1}{2} \right); \\ C_3^2 &= \left(\frac{-a+b+2}{2}, \frac{-a-2b+2}{2} \right) \text{ e} \\ C_4^2 &= \left(\frac{a+2b-2}{2}, \frac{-2a-b+1}{2} \right). \end{aligned}$$

2. Para os corpos quadráticos $\mathbb{Q}(\sqrt{d})$, com $d \equiv 2, 3 \pmod{4}$, temos que as regiões R são retângulos.

Exemplo 3 Pelo Exemplo 1, podemos tomar $\pi = -1 + 4w = (-1, 4)$, onde $a = -1$ e $b = 4$. Consideramos os segmentos de reta com extre-midades na origem e nos pontos $\pm\pi = \pm(-1, 4)$, $\pm w\pi = \pm(-4, 3)$, $\pm w^2\pi = \pm(-3, -1)$. Como $a - b \equiv 1 \pmod{3}$, segue que a região Voronoi R é um hexágono de vértices: $C_1^1 = (-2, 2)$, $C_2^1 = (-2, 0)$, $C_3^1 = (0, -2)$, $C_4^1 = (2, -2)$, $C_5^1 = (2, 0)$ e $C_6^1 = (0, 2)$, e que os vetores π , $w\pi$ e $w^2\pi$ possuem o mesmo comprimento, uma vez que $N(w) = 1$ e

$\theta = \arg(w) = 60^\circ$, sendo \mathcal{H} o hexágono de coordenadas: $A = (\frac{-5}{3}, \frac{7}{3})$, $B = (\frac{-7}{3}, \frac{2}{3})$, $C = (\frac{-2}{3}, \frac{-5}{3})$, $D = (\frac{5}{3}, \frac{-7}{3})$, $E = (\frac{7}{3}, \frac{-2}{3})$ e $F = (\frac{2}{3}, \frac{5}{3})$. A Figura 3, mostra o conjunto de sinais $A_{13}[w]$ representado na região R .

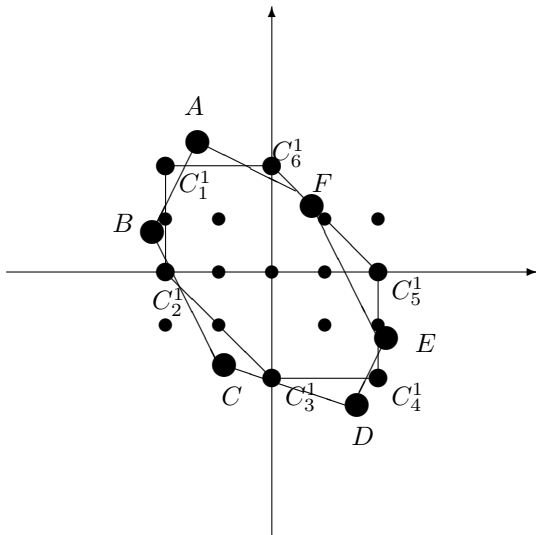


Figura 3

Exemplo 4 Pelo Exemplo 2, podemos tomar $\pi = 4 + i = (4, 1)$, onde $a = 4$ e $b = 1$. Consideramos os segmentos de reta com extremidades na origem e nos pontos $\pm\pi = \pm(4, 1)$ e $\pm\pi i = \pm(-1, 4)$. Como $a - b \equiv 1 \pmod{2}$, segue que a região de Voronoi R é um quadrado regular de vértices $C_1^1 = (1, \frac{5}{2})$, $C_2^1 = (\frac{-5}{2}, \frac{7}{2})$, $C_3^1 = (-1, \frac{-5}{2})$ e $C_4^1 = (\frac{5}{2}, \frac{-7}{2})$, e que os vetores π e πi possuem o mesmo comprimento $\theta = \arg(i) = 90^\circ$, sendo o quadrado \mathcal{Q} de coordenadas $A = (\frac{3}{2}, 2)$, $B = (-3, \frac{9}{2})$, $C = (\frac{-3}{2}, -3)$ e $D = (3, \frac{-9}{2})$. A Figura 4, mostra o conjunto de sinais $A_{17}[i]$ representado na região R .

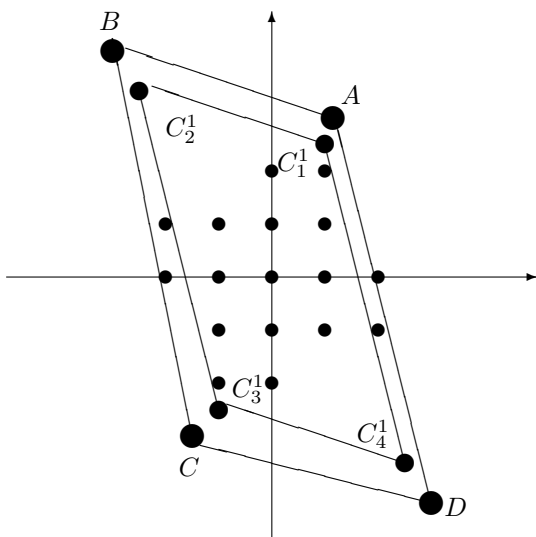


Figura 4

6 Conclusão

Neste trabalho, vimos os procedimentos de construção e rotulagem de constelações de sinais casadas a grupos aditivos de corpos de Galois $GF(p)$ a partir dos anéis de inteiros $\mathbb{Z}[w]$ e $\mathbb{Z}[i]$. Notemos que, para rotular os elementos via classes laterais dos anéis de inteiros de Eisenstein-Jacobi ou de Gauss por elementos de $GF(p)$, tomando o cuidado de sempre procurar ter a norma mínima. Vimos também, que a região Voronoi, tem um formato de hexágono ou retângulo, no caso via anéis de inteiros Eisenstein-Jacobi ou Gauss, respectivamente.

Referências

- [1] Huber, K., Codes over Gaussian integers, IEEE Trans. Inform. Theory, vol. 40, pp. 207 – 216, Jan. 1994.
- [2] Huber, K., Codes over Eisenstein-Jacobi integers, AMS, Contemp. Math., vol. 158, pp. 165 – 179, 1994.
- [3] Lang, S., "Algebraic Number Theory", Addison-Wesley Publishing Company, 1970.
- [4] Nóbrega Neto, T. P.; Favareto, O. M.; Interlando, J. C.; Palazzo Jr., R., Lattice Constellations and Codes from Quadratic Number Fields, IEEE Trans. Inform. Theory, vol. 47, pp. 1514 – 1527, May 2001.