

Constelações de Sinais Provenientes de Corpos de Números

Edson Donizete de Carvalho,
 Departamento de Matemática, FEIS, UNESP
 Alameda Rio de Janeiro 26
 15385-000 Ilha Solteira-SP
 E-mail: edson@mat.feis.unesp.br

1 Resumo Extendido

Uma *constelação de sinais* é um subconjunto S de pontos em \mathbb{R}^n . Na qual cada ponto é chamado *ponto de sinal* e a constelação é dita ser *geometricamente uniforme* se para quaisquer sinais $s_0, s_1 \in S$, existir uma isometria $T \in U(S)$ tal que $T(s_0) = s_1$, ou seja, $U(S)$ age transitivamente em S , equivalentemente,

$$U(s_0) = \{T(s_0) : \forall T \in U(S)\} = S.$$

Dentre todos os possíveis conjuntos de sinais com cardinalidade m finita, aquele que apresenta a menor energia média é denominada de *constelação de sinais*. A energia média mínima E_{min} , de um conjunto de sinais $\{s_0, s_1, \dots, s_{m-1}\}$ é uma função dada por $\prod_{i=0}^{m-1} d_i^2 \frac{(\bar{s}, s_i)}{m}$, onde $d(\bar{s}, s_i)$, denota a distância entre os pontos de sinais s_i e \bar{s} onde \bar{s} é o centro de massa da constelação.

Definição 1.1. A região de Voronoi $R_V(s)$ associada a um dado ponto de sinal $s \in S$ é o conjunto $R_V(s) = \{\mathbf{x} \in \mathbb{R}^n : d(\mathbf{x}, s) \leq d(\mathbf{x}, T(s)), \forall T \in U\}$.

Definição 1.2. O perfil de distância global com relação a $s \in S$, denotado por $PD(s)$, é definido como sendo o conjunto das distâncias dos pontos de S com relação a s .

O teorema a seguir relaciona constelações de sinais geometricamente uniformes com regiões de Voronoi.

Teorema 1.1. [3] Se S for uma constelação de sinais geometricamente uniforme, então:

- 1) Todas as regiões de Voronoi são do mesmo tipo, isto é, são congruentes;
- 2) O perfil de distância global $PD(s)$ é o mesmo para qualquer ponto de sinal em S .

Nestas condições dizemos que uma constelação de sinais do tipo S está *casada* a um grupo G , se existe, uma aplicação μ de G sobre S tal que $d(\mu(g), \mu(h)) = d(\mu(e), \mu(g^{-1}h))$, para todo $g, h \in G$, onde e é o elemento neutro de G e $d(\cdot, \cdot)$ é uma distância em S . O grupo G nestas condições é denominado de *grupo de rótulos de S* . A aplicação μ é chamada *aplicação casada*. Além disso, se μ é injetiva, dizemos que μ^{-1} é um *rotulamento casado*, isto é, se G é isomorfo a $G(S)$ então μ é uma *rotulamento isométrico*. [6]

Em [4] e [5], Huber considerou códigos de blocos a partir dos anéis de inteiros $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$ módulo ideais primos $\langle \gamma \rangle$. Em [4], também foi introduzida a *métrica de Mannheim* w_M em $\mathbb{Z}[i]/\langle \gamma \rangle$, ou seja, dado $\delta = x + yi \in \mathbb{Z}[i]/\langle \gamma \rangle$, tem-se que

$w_M(\delta) = |x| + |y|$, o que permite definir a distância entre dois elementos $\alpha, \beta \in \mathbb{Z}[i]/\langle \gamma \rangle$, por $d_M = w_M(\delta)$, onde $\delta \equiv \alpha - \beta \pmod{\gamma}$ com $\delta \in \mathbb{Z}[i]/\langle \gamma \rangle$. Em [7], Nóbrega *et. alii* estenderam a definição da métrica de Mannheim ao anel $\mathbb{Z}[\omega]$.

Em se tratando de constelações de sinais S do tipo QAM como proposto por Huber em [4], [5] e [7], tem-se que a métrica de Mannheim é mais apropriada que a *métrica de Hamming e de Lee*.

Em particular, as constelações de sinais S consideradas em [4] e [5] e [7] são *geometricamente uniformes*,

Neste contexto coloca-se as seguinte questões:

Questão I: Quando é possível construir constelações com p^t sinais, com $t \in \mathbb{Z}$ e $t > 0$, e p um inteiro primo qualquer, que tenha como rótulos grupos preferencialmente aditivos?

Questão II: Quando é possível construir constelações com p^t sinais geometricamente uniformes, com $t \in \mathbb{Z}$ e $t > 0$, como abordadas na Questão I com rotulamento casado pela distância de Mannheim?

Sob estas condições, tais constelações devem fazer parte de reticulados em \mathbb{R}^2 que tenham como identificação elementos dos anéis de inteiros $\mathbb{Z}[\theta] = \{a + b\theta \mid a, b \in \mathbb{Z}\}$ provenientes de corpos de números quadráticos imaginários $\mathbb{Q}(\sqrt{-m}) = \{a + b\sqrt{-m} \mid a, b \in \mathbb{Q}\}$, com m um inteiro livre de quadrados.

Já θ é caracterizado por

$$\theta = \begin{cases} \sqrt{-m}, & \text{se } -m \equiv 2, 3 \pmod{4} \\ \frac{1+\sqrt{-m}}{2}, & \text{se } -m \equiv 1 \pmod{4} \end{cases}$$

Como exemplos desta caracterização temos que $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$ são anéis de inteiros dos corpos de números $\mathbb{Q}(\sqrt{-1})$ e $\mathbb{Q}(\sqrt{-3})$, respectivamente.

A função que estabelece o rotulamento casado entre os pontos de sinais das constelações (identificados por elementos de anéis dos inteiros de energia mínima) e os elementos de um grupo aditivo G é dada por:

Um elemento $l \in G$ (G um grupo com p^t elementos) é um rótulo para o ponto $x + y\theta \in \mathbb{Z}[\theta]$ se $x + yr \equiv l \pmod{p^t}$, onde $r \in \mathbb{Z}$ é a única solução (em s) da equação $a + bs \equiv 0 \pmod{p^t}$, onde $0 \leq s < p^t - 1$.

Em [1], Carvalho *et. alii* forneceram resposta a Questão I para o caso dos anéis de $\mathbb{Z}[i]$ ou $\mathbb{Z}[\omega]$.

Foi mostrado que se p for da forma $p = 4k + 1$ ou $p = 6k + 1$, k inteiro, e os reticulados forem $\mathbb{Z}[i]$ ou $\mathbb{Z}[\omega]$, respectivamente, então existem constelações de p sinais com rótulos dados por grupos

aditivos dos corpos de Galois $GF(p)$. Além disso, se $t \geq 2$ então existem constelações com p^t sinais com rótulos dados por p -grupos aditivos G_{p^t} não fazem parte dos corpos de Galois $GF(p^t)$.

Caso p seja da forma $p \neq 4k + 1$ ou $p \neq 6k + 1$, k inteiro, e os reticulados forem $\mathbb{Z}[i]$ ou $\mathbb{Z}[\omega]$, respectivamente, então existem constelações com p^2 sinais casadas com rótulos dados por grupos aditivos que fazem parte da estrutura aditiva dos corpos de Galois $GF(p^2)$. Além disso, se $t \geq 2$ e t for par, então existem constelações de sinais com p^t sinais com rótulos dados por p -grupos aditivos de G_{p^t} que não fazem parte de $GF(p^t)$.

Neste trabalho, estendemos os resultados obtidos em [1]. Caracterizando o processo de rotulamento de constelações provenientes de reticulados dados pelos anéis de $\mathbb{Z}[\theta]$ por grupos aditivos.

Basta observar o seguinte fato.

As constelações com p^t sinais em \mathbb{R}^2 , são constituídas por representantes de classes laterais provenientes de ideais I de norma relativa p^t nos anéis de inteiros $\mathbb{Z}[\theta]$, de tal forma que a energia média correspondente seja mínima.

Para que uma constelação de sinais de cardinalidade p proveniente dos reticulados $\mathbb{Z}[\theta]$ apresentem como grupos de rótulos, que sejam grupos aditivos provenientes dos corpos de Galois $G(p)$, basta analisar se p é fatorável no anel de inteiros $\mathbb{Z}[\theta]$ em questão, ou melhor se existe um elemento $\gamma = a + b\theta$ irredutível em $\mathbb{Z}[\theta]$. Em caso afirmativo, basta tomar o ideal primo em $\mathbb{Z}[\theta]$ gerado por γ e verificar se é possível aplicar a função de rotulamento.

Desse modo, indiretamente fica estabelecido um procedimento de se encontrar ideais primos \mathcal{P} em $\mathbb{Z}[\theta]$ gerados por γ .

Tomando as extensões destes ideais \mathcal{P} , ou melhor, potências do gerador γ^t , obteremos os ideais I não primos de norma relativas p^t .

No caso em que isto ocorra, basta tomar γ^t como sendo o gerador de um ideal I em $\mathbb{Z}[\theta]$. Caso a função de rotulamento seja satisfeita, obtemos o grupo quociente $G \simeq \mathbb{Z}[\theta]/I$, como o grupo de rótulos das constelações com p^t sinais obtida a partir do reticulado $\mathbb{Z}[\theta]$.

Desta forma é possível estabelecer um critério de construção constelações de sinais de cardinalidade p^t , que tenha como rótulos p -grupo aditivo G_{p^t} , a partir de $\mathbb{Z}[\theta]$ e desde que satisfaça as condições impostas pela função de rotulamento. Basta que satisfaçam os seguintes casos:

Caso I: Se o inteiro primo p seja irredutível em $\mathbb{Z}[\theta]$, então existe constelação de sinais de cardinalidade p^2 , cujos sinais tenham como rótulos elementos de p -grupo aditivo G_{p^2} proveniente do corpo de Galois $GF(p^2)$. Neste caso, para qualquer inteiro $t > 2$, existe constelação de sinais, cujos sinais tenham como rótulos elementos de p -grupos aditivos G_{p^t} , no entanto não é proveniente do corpo de Galois $GF(p^t)$ por este processo.

Caso II: Se o inteiro primo p seja redutível em $\mathbb{Z}[\theta]$, então existe constelação de sinais de cardinalidade p^t para t par, cujos sinais tenham rótulos elementos de um p -grupo aditivos G_{p^t} , que no entanto, não é proveniente do corpo de Galois $GF(p^t)$.

Caso III : Apenas as as constelações de sinais provenientes dos anéis de inteiros $\mathbb{Z}[i]$ ou $\mathbb{Z}[\omega]$ respondem a *Questão II*, isto é, são geometricamente

uniformes, com grupos de rótulos casados pela distância de Mannheim, satisfazendo o Teorema 1.1.

Nas demais situações é possível apenas fazer a rotulamento dos sinais por elementos de um grupo aditivo G , no entanto, não é obtido o casamento da distância de Mannheim ao grupo G .

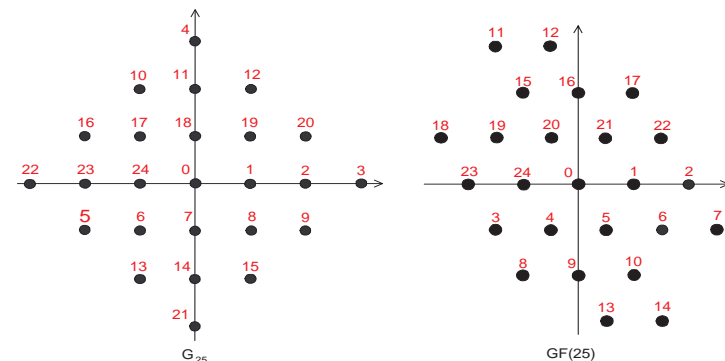


Figura 1: Constelações de Sinais

Exemplo 1.1. Considere $p = 5$, $t = 2$ e $\mathbb{Z}[\omega]$. Sob estas condições, temos que $25 = (5 + 5\omega)(5 - 5\omega)$ e que $5 - 5\omega$ é irredutível em $\mathbb{Z}[\omega]$. Uma das soluções inteiras é dada por $5 - 5\omega$. Seja I o ideal primo gerado por $I = \langle 5 - 5\omega \rangle$. Então, $r = -4$ é solução inteira de $5 - s5 = 25$. Com isso, o rótulo do elemento $x + y\omega$ em $\mathbb{Z}[\omega]$ é obtido de $x - 4y \equiv l \pmod{25}$ como sendo o elemento do grupo aditivo do corpo $GF(25)$.

Exemplo 1.2. Considere $25 = (3 + 4i)(3 - 4i)$. Sob estas condições, temos que $3 - 4i = (1 + 2i)^2$ e que $1 + 2i$ é irredutível em $\mathbb{Z}[i]$. Assim, tomando Seja I o ideal gerado por $I = \langle 3 - 4i \rangle$, temos que I não é um ideal primo em $\mathbb{Z}[i]$. Então, $r = 7$ é solução inteira de $3 - 4s = 25$. Com isso, o rotulo do elemento $x + yi$ em $\mathbb{Z}[i]$ é obtido de $x - 7y \equiv l \pmod{25}$ como sendo o elemento do grupo G_{25} , que não faz parte de $GF(25)$, uma vez que o ideal I não é primo em $\mathbb{Z}[i]$.

A Figura 1 ilustra as constelações de sinais de energia mínima, provenientes de $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, respectivamente. Os sinais destas constelações são rotulados pelos elementos do grupo aditivo G_{25} e pelos elementos do grupo aditivo de $GF(25)$, respectivamente. Estas constelações além de possuírem grupos de rótulos distintos o arranjo geométrico destas constelações de sinais são diferentes.

Referências

- [1] E.D.Carvalho,R.Palazzo Jr. e M.Firer, Construção e Rotulagem de Constelações de Sinais Geometricamente Uniformes em R^n Casadas a Grupos, *Revista da Sociedade Brasileira de Telecomunicações*, Vol.19, No.1 pp. 13-20, Abril 2004.
- [2] H.Cohn, *Advanced Number Theory*, Dover Publications, Inc., New York, 1962.
- [3] G.D.Forney, Geometrically Uniform Codes *IEEE Trans. Inform.Theory*, Vol. IT-37, No.6 pp. 1241-1256, Sept. 1991.

- [4] K. Huber, Codes over Gaussian Integers *IEEE Trans. Inform. Theory* , Vol. IT-40, No.6 pp. 207-216, Jan. 1994.
- [5] K. Huber, Codes over Eisenstein-Jacobi Integers *Contemporary Mathematics* , Vol.168, pp. 165-179, 1994.
- [6] H.A.Loeliger, Signal Sets Matched to Groups *IEEE Trans. Inform. Theory* , Vol. IT-37, No.6 pp. 1675-1682, Nov. 1991.
- [7] T.P.Nobrega Neto, J.C. Interlando, O.M. Favareto, M. Elia, and R. Palazzo Jr., Lattices Constellations and Codes from Quadratic Algebraic Number Fields *IEEE Trans. Inform. Theory* , Vol. IT-47, No.6 pp. 1514-1527, May 2001.