# CONSTRUÇÃO E ROTULAGEM DE CONSTELAÇÕES DE SINAIS GEOMETRICAMENTE UNIFORMES EM $\mathbb{R}^N$ CASADAS A GRUPOS

**Edson Donizete de Carvalho, Reginaldo Palazzo Jr. e Marcelo Firer**

**Resumo** - Neste trabalho estabelecemos as condições necessárias para a construção de constelações de sinais que sejam geometricamente uniformes e também casadas a grupos quocientes aditivos. Tais constelações fazem parte do espaço de sinais em $\mathbb{R}^n$ cuja identificação dos pontos de sinais são dados por elementos dos correspondentes anéis de inteiros. A rotulagem casada decorrerá da ação transitiva dos $p$-grupos aditivos $G_{p^m}$ ou de grupos aditivos do corpo de Galois $GF(p^m)$.

**Palavras-chave:** Códigos geometricamente uniformes, conjunto de sinais, rotulagem casada, anéis de inteiros.

**Abstract** - In this paper we establish the conditions under which it is possible to construct signal sets satisfying the properties of being geometrically uniform and matched to additive quotient groups. Such signal sets consist of subsets of signal spaces in $\mathbb{R}^n$ such that the sinal points are identified with the elements of the corresponding integer rings. The matched labelling is a conseguence of the transitive action either of the additive $p$-groups $G_{p^m}$ or of the additive groups of the Galois field $GF(p^m)$.

**Keywords:** Geometrically uniform codes, signal sets, matched labelling, integer ring.

## 1. INTRODUÇÃO

O problema de construção de constelações de sinais que possuam inerentemente propriedades geométricas e estruturas algébricas é fundamental e relevante tanto no aspecto da sistematicidade de geração de tais constelações como no de implementação prática dos moduladores e demoduladores. É portanto neste contexto que se coloca a seguinte questão: Quando é possível construir constelações com $p^m$ sinais, onde $m$ é um inteiro positivo qualquer, que sejam geometricamente uniformes e também casadas a grupos (rotulagem), preferencialmente aditivos? Sob esta condição, tais constelações devem fazer parte de reticulados em $\mathbb{R}^n$ que tenham como identificação os elementos dos anéis de inteiros $\mathbb{Z}[\theta]$.

Edson Donizete de Carvalho está com a Universidade Vale do Rio Verde de Três Corações - UNINCOR, Três Corações, MG, Brasil. Reginaldo Palazzo está com o Departamento de Telemática da Unicamp - DT-FEEC-UNICAMP, Campinas, SP, Brasil. Marcelo Firer está com o Departamento de Matemática - IMECC-UNICAMP, Campinas, SP, Brasil. Emails: edsondonizete@yahoo.com.br, palazzo@dt.fee.unicamp.br, mfirer@ime.unicamp.br. Editor de Área responsável: Ricardo Campello. Artigo submetido em 09/Jun/2003, revisado em 05/Abr/2004, aceito em 05/Abr/2004.

Em [5], Egri e Horrigan propuseram a construção de um grupo multiplicativo finito de inteiros complexos para o uso em detecção diferencial de sinais de uma constelação de sinais 16-QAM.

Em [6], Rifà estendeu o resultado de [5] através da classificação, caracterização e construção dos grupos multiplicativos $G_m$ de cardinalidade $2^m$ e dos grupos das unidades de $G_m$, que podem ser utilizados em detecção diferencialmente coerente de sinais do tipo QAM.

Em [12], Dong *et.ali.* propuseram a construção de constelações de sinais QAM com $4p^{2m-2}$ e $6p^{2m-2}$ sinais casadas a subgrupos dos grupos multiplicativos das unidades dos quocientes $\mathbb{Z}[i]/(p^m)$ e $\mathbb{Z}[\omega]/(p^m)$, para $p$ primo e $p > 2$, respectivamente.

Nos trabalhos [5], [6] e [12] foram propostos códigos corretores de erros não lineares tendo como alfabetos elementos dos grupos multiplicativos associados aos correspondentes anéis de inteiros. Sob a operação de multiplicação, tais grupos não dão origem a reticulados.

Em [3] e [4], Huber propos um método de construção de códigos de bloco lineares tendo como alfabeto elementos do corpo de Galois $GF(p)$ obtido via classes de resíduos de um anel de inteiros de Gauss ou de Eisenstein-Jacobi módulo ideais primos.

Nóbrega *et.ali.* [9] propuseram um procedimento algébrico de rotulagem casada, dos sinais de uma constelação de sinais em $\mathbb{R}^2$ por elementos do grupo aditivo de $GF(p)$, para os casos em que um inteiro primo $p$ seja fatorável como elementos irredutíveis em um anel de inteiros.

Neste trabalho iremos considerar as possibilidades de construção e rotulagem de constelações de sinais geometricamente uniformes com cardinalidade $M = p^k$, com $k \geq 2$, a partir de reticulados identificados por anéis de inteiros, que não foram consideradas nos trabalhos anteriores. A seguir discriminamos os casos a serem considerados.

Caso I: É possível construir constelações de sinais geometricamente uniformes com $p^k$ sinais, $k \geq 2$ e $p$ primo, casadas ao grupo aditivo de $GF(p^k)$? Em caso afirmativo, quais são os possíveis valores de $k$?

Caso II: É possível construir constelações de sinais geometricamente uniformes com $p^k$ sinais, cujo grupo de rótulos possua uma estrutura aditiva que não faça parte de $GF(p^k)$? Caso seja possível, que estrutura algébrica poderá ser esta?

Caso III: É possível construir constelações de sinais geometricamente uniformes de mesma cardinalidade, no entanto, casadas a diferentes grupos?

Em relação ao Caso I, para $k = 2$, Huber, [4], fornece exemplos de constelações com $p^2$ sinais provenientes do reticulado identificado por $\mathbb{Z}[\omega]$.

Todavia, não foram considerados em [3], [4] e [9] os seguintes casos: 1) $k = 2$ e as constelações com $p^2$ sinais provenientes do reticulado identificado por $\mathbb{Z}[i]$; e 2) no caso geral para $k \geq 3$.

Neste trabalho mostramos que no caso em que as constelações de sinais são provenientes do reticulado identificado por $\mathbb{Z}[i]$ e $k = 2$, se $p = 4t + 3$, $t$ inteiro, é possível construir constelações de sinais geometricamente uniformes com $p^2$ sinais casadas a grupos aditivos de $GF(p^2)$. Similarmente, mostramos que no caso $\mathbb{Z}[\omega]$ e $k = 2$, se $p \neq 6t + 1$, $t$ inteiro, então é possível construir constelações de sinais geometricamente uniformes com $p^2$ sinais casadas a grupos aditivos de $GF(p^2)$. Para $k \geq 3$, tanto em $\mathbb{Z}[i]$ quanto em $\mathbb{Z}[\omega]$ mostramos que não é possível obter tais constelações.

Chamamos a atenção ao fato de que em [3], [4], e [9] não foram considerados os Casos II e III.

Em relação ao Caso II, mostramos que é possível construir constelações de sinais geometricamente uniformes com $p^k$ sinais casadas a $p$-grupos aditivos $G_{p^k}$ que não fazem parte de $GF(p^k)$ para $k \geq 3$. Mostramos também que no caso em que $k = 2$, se $p = 4t + 1$ e a constelação de sinais está identificada em $\mathbb{Z}[i]$ ou $p = 6t + 1$ e a constelação de sinais está identificada em $\mathbb{Z}[\omega]$, para $t$ um inteiro positivo, então é possível construir constelações de sinais geometricamente uniformes com $p^2$ sinais casadas a $p$-grupos aditivos $G_{p^2}$ que não fazem parte de $GF(p^2)$.

Observamos, através da Figura 2, que eventualmente poderá ocorrer constelações com $p^k$ sinais casadas a diferentes grupos de tal forma que os correspondentes arranjos geométricos dos sinais são também diferentes. Isto ocorrerá se $p^k$ puder ser representado por diferentes formas quadráticas. Dessa forma, o Caso III fica especificado.

Uma contribuição deste trabalho está relacionada ao processo de determinação do gerador $\gamma = a + b\theta$ do ideal $I$ em $\mathbb{Z}[\theta]$ de norma relativa $p^k$. A determinação do ideal $I$ é relevante pois o mesmo é utilizado na obtenção do grupo quociente $\mathbb{Z}[\theta]/I$, que por sua vez é isomorfo ao grupo de rótulos de uma constelação com $p^k$ sinais. Apesar de [3], [4] e [9] fazerem uso desta concepção, tal procedimento não foi considerado.

Observamos que o gerador $\gamma = a + b\theta$ pode ser determinado através das soluções inteiras $(X, Y) = (a, b)$ da forma quadrática $h(X, Y) = p^k$, onde $h(X, Y)$ provém da norma relativa do anel de inteiros $\mathbb{Z}[\theta]$. Portanto, quando $p^k$ for representável por uma forma quadrática, então é possível construir uma constelação geometricamente uniforme com $p^k$ sinais a partir de $\mathbb{Z}[\theta]$.

Em particular, mostramos através do Exemplo 4.3 que a proposta de construção de constelações de sinais geometricamente uniformes casadas a grupos aditivos de $GF(p^m)$ feita por Interlando e Elia em [13] pode ser estendida a $p$-grupos aditivos $G_{p^m}$ que não fazem parte de grupos aditivos de $GF(p^m)$.

Este trabalho está organizado da seguinte maneira. Na Seção 2, faremos uma revisão de conceitos da teoria dos números tais como corpo de números, anéis de inteiros, norma de um ideal e grupo de Galois bem como os conceitos de constelações de sinais geometricamente uniformes e a definição da função de rotulagem casada entre os sinais de uma constelação de sinais e os elementos de um grupo $G$. Na Seção 3, a definição de reticulado em $\mathbb{R}^n$ e os procedimentos para a identificação dos pontos dos reticulados em $\mathbb{R}^2$ e $\mathbb{R}^n$ por elementos dos anéis de inteiros são apresentados. Na Seção 4, fornecemos procedimentos para a construção de constelações com $p^m$ sinais em $\mathbb{R}^2$ e $\mathbb{R}^n$, com exemplos em $\mathbb{R}^2$ e $\mathbb{R}^3$. Finalmente, na Seção 5 as conclusões deste trabalho são apresentadas.

## 2. PRELIMINARES

### 2.1 TEORIA DOS NÚMEROS

Sejam $\mathbb{E}$ e $\mathbb{F}$ subcorpos de $\mathbb{C}$, o corpo dos números complexos. Se $\mathbb{E}$ é um subcorpo de $\mathbb{F}$, então $\mathbb{F}$ é uma extensão de $\mathbb{E}$, denotada por $\mathbb{F}/\mathbb{E}$. A dimensão de $\mathbb{F}$, este visto como espaço vetorial sobre $\mathbb{E}$, é chamada de grau de $\mathbb{F}$ sobre $\mathbb{E}$ e será denotada por $[\mathbb{F} : \mathbb{E}]$.

Considere $p(X)$ um polinômio irredutível sobre $\mathbb{E}$. Pelo Teorema Fundamental da Álgebra é sempre possível obter um subcorpo $\mathbb{F}$ de $\mathbb{C}$, que seja uma extensão do corpo $\mathbb{E}$, chamado *corpo de fatoração* de $p(X)$, como sendo o menor corpo $\mathbb{F}$ contendo todas as raízes de $p(X)$.

Chamamos de *número algébrico* qualquer elemento $\alpha \in \mathbb{C}$ que é raiz de algum polinômio não nulo $p(X)$ sobre $\mathbb{Q}$, o corpo dos números racionais. Podemos e iremos sempre considerar $p(X)$ mônico. Qualquer extensão finita de $\mathbb{Q}$ é chamada de *corpo de números*, em particular $\mathbb{F} = \mathbb{Q}(\alpha) = \{a + \alpha b : a, b \in \mathbb{Q}\}$, é uma extensão quadrática de $\mathbb{Q}$ com $\alpha$ uma raiz de $p(X)$.

Sejam $\mathbb{F}$ um corpo de números e $\alpha \in \mathbb{F}$ raiz de um polinômio $p(X)$ mônico com coeficientes em $\mathbb{Z}$, diremos que $\alpha$ é um *inteiro algébrico* e o conjunto desses inteiros algébricos constitui um anel denominado *anel de inteiros de* $\mathbb{F}$, [7], denotado por $\mathcal{D}_{\mathbb{F}}$. Exemplos de corpos de números são as extensões quadráticas imaginárias, isto é, subcorpos $\mathbb{F}$ de $\mathbb{C}$ de grau 2 caracterizados por:

$$\mathbb{F} = \mathbb{Q}(\sqrt{-m}) = \left\{a + ib\sqrt{m} : a, b \in \mathbb{Q}\right\},$$

onde $m$ é um inteiro positivo livre de quadrados.

Já os anéis de inteiros $\mathcal{D}_{\mathbb{F}}$ são caracterizados por $\mathbb{Z}[\theta] = \{a + b\theta : a, b \in \mathbb{Z}\}$, onde $\theta$ é dado por

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

**Exemplo 2.1** *Considere os seguintes casos:*

i) *Se a extensão quadrática é* $\mathbb{F} = \mathbb{Q}(\sqrt{-1})$, *então o anel de inteiros* $\mathbb{Z}[\theta]$ *de* $\mathbb{F}$ *é dado por* $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, *onde* $i = \sqrt{-1}$, *também conhecido como o anel de inteiros de Gauss.*

ii) *Se a extensão quadrática é* $\mathbb{F} = \mathbb{Q}(\sqrt{-3})$, *então o anel de inteiros* $\mathbb{Z}[\theta]$ *de* $\mathbb{F}$ *é dado por* $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$, *onde* $\omega = \frac{1+\sqrt{-3}}{2}$, *também conhecido como o anel de inteiros de Eisenstein-Jacobi.*

O Teorema 2.1 relaciona polinômios $p(X)$, tendo uma das raízes um inteiro algébrico, com extensões de corpos.

**Teorema 2.1** *[10] Sejam $\mathbb{F}/\mathbb{E}$ uma extensão de corpos e $\alpha \in \mathbb{F}$ um inteiro algébrico sobre $\mathbb{E}$.*

i) *Existe um polinômio mônico irredutível $p(X) \in \mathbb{E}[X]$ tendo $\alpha$ como raiz;*

ii) *$p(X)$ é o polinômio mônico de menor grau em $\mathbb{E}[X]$ tendo $\alpha$ como raiz e é único;*

iii) *A dimensão $[\mathbb{F} : \mathbb{E}]$ é igual ao grau de $p(X)$.*

**Lema 2.1** *[10] Seja $p(X) \in \mathbb{E}[X]$ um polinômio não constante. Seja $\mathbb{F}$ o corpo de fatoração de $p(X)$. Se $\sigma : \mathbb{F} \to \mathbb{F}$ é um automorfismo e se $\alpha$ é uma raiz de $p(X)$, então $\sigma(\alpha)$ também é uma raiz de $p(X)$.*

**Definição 2.1** *Seja $\mathbb{F}/\mathbb{E}$ uma extensão de corpos. O grupo de Galois $\mathbb{F}/\mathbb{E}$, denotado por $G(\mathbb{F}/\mathbb{E})$, é o conjunto de todos os automorfismos de $\mathbb{F}$ que deixam fixos os elementos de $\mathbb{E}$. Se o polinômio $p(X) \in \mathbb{E}[X]$ tiver como corpo de fatoração $\mathbb{F}$, então o grupo de Galois de $p(X)$ é $G(\mathbb{F}/\mathbb{E})$.*

**Teorema 2.2** *[10] Seja $p(X)$ um polinômio com coeficientes sobre $\mathbb{E}$. Se $p(X)$ é separável (isto é, possui todas raízes distintas no corpo de fatoração), então a cardinalidade do grupo de Galois $G(\mathbb{F}/\mathbb{E})$, iguala a dimensão do espaço vetorial $\mathbb{F}$ com relação a $\mathbb{E}$.*

Seja $G(\mathbb{F}/\mathbb{E}) = \{\sigma_0, \ldots, \sigma_{n-1}\}$ o grupo de Galois $\mathbb{F}/\mathbb{E}$. Chamamos de *norma relativa* de um elemento $z \in \mathbb{F}$ a aplicação $N_{\mathbb{F}/\mathbb{E}}(z) = \prod_{i=0}^{n-1} \sigma_i(z)$ com valores em $\mathbb{E}$.

Como exemplo, considere uma extensão quadrática racional imaginária do tipo $\mathbb{Q}(\sqrt{-m})/\mathbb{Q}$, onde $m$ é um inteiro positivo livre de quadrados. O grupo de Galois associado a esta extensão é $G(\mathbb{Q}(\sqrt{-m})/\mathbb{Q}) = \{\sigma_0, \sigma_1\}$, onde $\sigma_0$ é a identidade e $\sigma_1(a + b\sqrt{-m}) = a - b\sqrt{-m}$.

Avaliando a norma dos elementos nos anéis de inteiros $\mathbb{Z}[\theta]$ provenientes dessas extensões quadráticas imaginárias, concluímos que

$$N_{\mathbb{Q}(\sqrt{-m})/\mathbb{Q}}(a + b\theta) = (a + b\theta)(\overline{a + b\theta}) = \begin{cases} a^2 - mb^2, & se \ -m \equiv 2, 3 \ mod 4 \\ a^2 + ab + \frac{(1-m)}{4}b^2, & se \ -m \equiv 1 \ mod 4 \end{cases}$$

É conhecido que o algoritmo da divisão de Euclides é válido nos anéis $\mathbb{Z}[\theta]$ para $\theta = \sqrt{-m}$, se $m = 1, 2$ e para $\theta = \frac{1+\sqrt{-m}}{2}$, se $m = 3, 7, 11$ através do uso da aplicação norma, [7], isto é, dados $a, b \in \mathbb{Z}[\theta]$, sempre existem $q, r \in \mathbb{Z}[\theta]$ satifazendo a condição de que $a = bq + r$, com $r = 0$ ou $N_{\mathbb{Q}(\sqrt{-m})/\mathbb{Q}}(r) < N_{\mathbb{Q}(\sqrt{-m})/\mathbb{Q}}(b)$.

Os anéis onde o algoritmo da divisão de Euclides é aplicável são denominados **anéis euclidianos**.

**Proposição 2.1** *[7] Sejam $\mathbb{F}$ um corpo de números, $\mathcal{D}_{\mathbb{F}}$ seu anel de inteiros algébricos e $\mathcal{P}$ um ideal não nulo de $\mathcal{D}_{\mathbb{F}}$, então são válidas as seguintes afirmações:*

**(i)** *$\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$, onde $p$ é o único número primo em $\mathcal{P}$;*

**(ii)** *O quociente $\mathcal{D}_{\mathbb{F}}/\mathcal{P}$ é uma extensão finita do corpo $GF(p)$ cujo grau $[\mathcal{D}_{\mathbb{F}}/\mathcal{P} : GF(p)] \leq n$.*

Sejam $R$ um anel comutativo e $I$ um ideal de $R$. Em $R/I$ a operação $(a + I) + (b + I) = (a + b) + I$ para $a, b \in R$, está bem definida e as seguintes condições são verificadas:

**i)** A classe $0 + I$ é o elemento neutro para esta operação.

**ii)** $a + I = b + I$ se, e somente se, $a - b \in I$, neste caso denotamos por $a \equiv b(mod\ I)$.

Assim fica estabelecida uma estrutura de grupo aditivo em $R$. A notação $a \equiv b(mod\ I)$ significa que os elementos $a$ e $b$ de $R$ estão na mesma classe lateral (isto é, representam o mesmo elemento em $R/I$). Chamamos $R/I$ de **grupo quociente aditivo** de $R$ sobre $I$.

O número de elementos de $R/I$ é chamado de **norma do ideal** $I$.

Outro fato conhecido é que anéis euclidianos são **anéis principais**, isto é, todo ideal é gerado por um elemento que é único a menos de associados.

## 2.2 CONSTELAÇÕES DE SINAIS GEOMETRICAMENTE UNIFORMES

Um conjunto discreto de pontos em $\mathbb{R}^n$ em que seja possível realizar uma identificação destes pontos por sinais é chamado de *espaço de sinais*.

Uma *constelação de sinais* é um subconjunto finito de sinais em um espaço de sinais.

**Definição 2.2** *Um conjunto de sinais $K$ é uma constelação de sinais geometricamente uniforme se para quaisquer sinais $k_0, k_1 \in K$, existir uma isometria $T \in U(K)$ tal que $T(k_0) = k_1$, ou seja, $U(K)$ age transitivamente em $K$, equivalentemente,*

$$U(k_0) = \{T(k_0) : \forall T \in U(K)\} = K.$$

Dentre todos os possíveis conjuntos de sinais com cardinalidade $m$ finita, aquele que apresenta a menor energia média é denominado de *constelação de sinais* associada aos $m$ pontos de sinais. A energia média mínima, $E_{min}$, de uma constelação de sinais $\{x_0, x_1, \ldots, x_{m-1}\}$ é a função $\sum_{i=1}^{m-1} \frac{d^2(x_0, x_i)}{m}$, onde $d(x_0, x_i)$ denota a distância do sinal $x_i$ a $x_0$, e $x_0$ é o baricentro da constelação. Note que $d(.,.)$ depende do espaço métrico em consideração. Se for o Euclidiano, então $d(.,.)$ é a distância Euclidiana. Se for o espaço hiperbólico, então $d(.,.)$ é a distância hiperbólica.

**Definição 2.3** *A região de Voronoi $R_V(k)$ associada a um dado ponto de sinal $k \in K$ é o conjunto $R_V(k) = \{\mathbf{x} \in \mathbb{R}^n : d(\mathbf{x}, k) \leq d(\mathbf{x}, T(k)), \forall T \in U\}$.*

**Definição 2.4** *O perfil de distância global com relação a $k \in K$, denotado por $PD(k)$, é definido como sendo o conjunto das distâncias dos pontos de $K$ com relação a $k$.*

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

**Teorema 2.3** *[1] Se $K$ 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 $PD(k)$ é o mesmo para qualquer ponto de sinal em $K$.*

Dizemos que uma constelação de sinais $S$ está *casada* a um grupo $G$, se existe uma aplicação $\mu$ 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 $d(.,.)$ é uma distância em $S$. A aplicação $\mu$ é chamada *aplicação casada* [2]. Além disso, se $\mu$ é injetiva, dizemos que $\mu^{-1}$ é uma *rotulagem casada*, isto é, se $G$ é isomorfo a $G(S)$ então $\mu$ é uma *rotulagem isométrica*.

## 3. RETICULADOS EM $\mathbb{R}^N$

Dizemos que um subconjunto discreto $\Lambda$ de pontos de $\mathbb{R}^n$ é um *reticulado de dimensão* $n$ se este for um $\mathbb{Z}$-módulo, gerado através de uma base $\{e_1,\ldots,e_n\}$. Note que $e_1,\ldots,e_n$ podem ser vistos como linhas de uma matriz geradora $M$. Um vetor $x = (x_1,\ldots,x_n) \in \Lambda$, é escrito como $x = x_1e_1 + \cdots + x_ne_n = x.M$, onde $x_i$ são inteiros. A norma de $x$ é $N(x) = N(x_1e_1 + \cdots + x_ne_n) = \Sigma_{i=1}^{n}\Sigma_{j=1}^{n} x_ix_je_ie_j = x.M.M^tx^t = x.A.x^t = f(x)$, onde a matriz $A = M.M^t$ é chamada *matriz Gram de* $\Lambda$.

A função $f(x)$ de $n$ variáveis inteiras $x_1,\ldots,x_n$ é uma forma quadrática associada ao reticulado $\Lambda$.

### 3.1 RETICULADOS EM $\mathbb{R}^2$ IDENTIFICADOS PELOS ANÉIS DE INTEIROS $\mathbb{Z}[i]$ E $\mathbb{Z}[\omega]$

É fato conhecido que o recobrimento de $\mathbb{R}^2$ por polígonos do tipo $\{p,q\}$, isto é, um polígono de $p$ lados onde cada vértice é recoberto por $q$ polígonos, é necessário que a equação $(p-2)(q-2) = 4$ tenha soluções inteiras. Disto segue que $\mathbb{R}^2$ admite apenas recobrimentos do tipo $\{4,4\}$, $\{6,3\}$ e $\{3,6\}$.

Mostraremos, pelo Teorema 3.1, que os elementos do anel de inteiros $\mathbb{Z}[\theta]$ proveniente de uma extensão quadrática imaginária $\mathbb{Q}(\sqrt{-m})$, onde $m$ é um inteiro positivo livre de quadrados, são identificados pelos baricentros ou vértices dos correspondentes polígonos.

**Teorema 3.1** *[8] Seja $\alpha_{(a,b)} = a + b\theta$ um elemento de um anel de inteiros $\mathbb{Z}[\theta]$ proveniente de uma extensão quadrática $\mathbb{Q}(\sqrt{-m})$, onde $m$ é um inteiro positivo livre de quadrados. Temos dois casos a considerar:*

1) *Caso em que $-m \equiv 2,3 \bmod 4$.*

   *Seja $\alpha_{(a,b)}$ o baricentro de um paralelogramo. Então, $\alpha_{(a+1,b)}$ e $\alpha_{(a-1,b)}$ são identificados como sendo os vértices opostos do paralelogramo cuja distância euclidiana de $\alpha_{(a,b)}$ vale 1, enquanto que $\alpha_{(a,b+1)}$ e $\alpha_{(a,b-1)}$ são identificados como sendo o par de vértices opostos do paralelogramo cuja distância euclidiana de $\alpha_{(a,b)}$ vale $\sqrt{m}$;*

2) *Caso em que $-m \equiv 1 \bmod 4$.*

   *Seja $\alpha_{(a,b)}$ o baricentro de um hexágono. Então, $\alpha_{(a+1,b)}$ e $\alpha_{(a-1,b)}$ são identificados como sendo os vértices opostos de um hexágono cuja distância euclidiana de $\alpha_{(a,b)}$ vale 1, equanto que $\alpha_{(a-1,b+1)}$ e $\alpha_{(a+1,b-1)}$; e $\alpha_{(a,b-1)}$ e $\alpha_{(a,b+1)}$ são identificados como sendo os demais pares de vértices opostos do hexágono com distância euclidiana $\frac{\sqrt{m+1}}{2}$ de $\alpha_{(a,b)}$.*

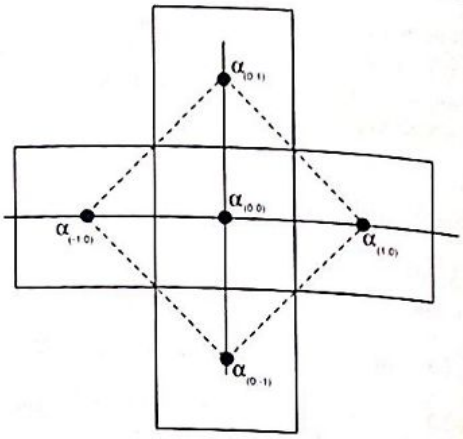


**Figura 1**. Tesselação por quadrados

**Corolário 3.1** *[8]*

1) *O recobrimento de $\mathbb{R}^2$ por quadrados de área unitária é obtido através da identificação dos baricentros dos quadrados unitários com os elementos do anel de inteiros de Gauss;*

2) *O recobrimento de $\mathbb{R}^2$ por hexágonos regulares de área mínima é obtido através da identificação dos baricentros de hexágonos de área mínima com os elementos do anel de inteiros de Eisenstein-Jacobi.*

Note que o reticulado obtido a partir da tesselação de quadrados de área unitária é identificado pelo anel de inteiros $\mathbb{Z}[i]$ cuja forma quadrática associada é $f(X,Y) = X^2 + Y^2$, ou seja, a norma relativa dos elementos de $\mathbb{Z}[i]$.

Analogamente, temos que o reticulado obtido a partir da tesselação de $\mathbb{R}^2$ por hexágonos regulares de área mínima é identificado pelo anel de inteiros $\mathbb{Z}[\omega]$ cuja forma quadrática associada é $g(X,Y) = X^2 + XY + Y^2$, ou seja, a norma relativa dos elementos de $\mathbb{Z}[\omega]$.

O objetivo desta identificação é prover uma estrutura de grupo, com a operação de grupo sendo aditiva, aos pontos destes reticulados em $\mathbb{R}^2$. Neste caso, em particular, a estrutura aditiva do grupo provém da parte aditiva do anel de inteiros.

### 3.2 RETICULADOS EM $\mathbb{R}^N$ IDENTIFICADOS POR ANÉIS DE INTEIROS

Em [13], Interlando e Elia propuseram uma maneira natural de se obter reticulados em $\mathbb{R}^n$, onde os pontos destes reticulados são identificados como sendo os elementos de um anel de inteiros proveniente de corpos de números de grau $n$.

Para estabelecer esta identificação foi considerado em [13] a aplicação estabelecida em (1). Esta aplicação realiza o mergulho dos elementos de um corpo de números $\mathbb{F}$ em $\mathbb{R}^n$ onde cada coordenada, desta identificação em $\mathbb{R}^n$, é a imagem dos $n$ distintos mergulhos associados ao corpo de números $\mathbb{F}$ aplicados num elemento de $\mathbb{F}$, isto é,

$$\sigma_{\mathbb{F}} : \mathbb{F} \longrightarrow \mathbb{R}^n$$

$$x \longrightarrow (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x) \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)). \quad (1)$$

sendo que $\sigma_j$, para $j = 1, \ldots, r_1$, são mergulhos reais de $\mathbb{F}$ em $\mathbb{C}$, e $\sigma_j$, para $j = r_1 + 1, \ldots, r_1 + r_2$ são mergulhos complexos de $\mathbb{F}$ em $\mathbb{C}$ com $\overline{\sigma_{j+r_1}} = \sigma_{j+r_1+r_2}$.

Não é difícil mostrar que $\sigma_{\mathbb{F}}$ é um monomorfismo, que chamamos de *mergulho canônico* de $\mathbb{F}$ em $\mathbb{R}^n$.

Por outro lado, o anel de inteiros $\mathcal{D}_{\mathbb{F}}$ associado a um corpo de números $\mathbb{F}$ é um $\mathbb{Z}$-módulo livre com uma base integral do tipo $\beta = \{\omega_1, \ldots, \omega_n\}$. Chamamos a atenção ao fato de que, em geral, a determinação da base integral para extensões de grau maior ou igual a 3 é significativamente difícil.

Para cada $\omega_i \in \beta$, consideraremos os pontos $u_i = \sigma_{\mathbb{F}}(\omega_i)$ dados por

$$u_i = (\sigma_1(\omega_i), \ldots, \sigma_{r_1}(\omega_i), \Re\sigma_{r_1}(\omega_i), \Im\sigma_{r_1}(\omega_i), \ldots, \Re\sigma_{r_1+r_2}(\omega_i), \Im\sigma_{r_1+r_2}(\omega_i)). \quad (2)$$

Assim, $\sigma_{\mathbb{F}}(\beta) = \{u_1, \ldots, u_n\}$ será uma base para um reticulado $\Lambda$ em $\mathbb{R}^n$. Avaliando $\sigma_{\mathbb{F}}$ em $y \in \mathcal{D}_{\mathbb{F}}$, onde $y = a_1\omega_1 + \cdots + a_n\omega_n$, e $a_1, \ldots, a_n \in \mathbb{Z}$, temos que

$$\sigma_{\mathbb{F}}(y) = a_1\sigma_{\mathbb{F}}(\omega_1) + \cdots + a_n\sigma_{\mathbb{F}}(\omega_n) = a_1u_1 + \cdots + a_nu_n.$$

O que torna a identificação completa.

## 4. CONSTRUÇÃO E ROTULAGEM DE CONSTELAÇÕES GEOMETRICAMENTE UNIFORMES COM $P^M$ SINAIS

Nesta seção apresentaremos procedimentos de construção de constelações de sinais em $\mathbb{R}^2$ casadas a grupos aditivos de $GF(p)$ ou $GF(p^2)$ e a $p$-grupos aditivos que não fazem parte de um corpo de Galois e as correspondentes rotulagens conduzindo a constelações geometricamente uniformes. Mostraremos que este fato ocorre de maneira similar em $\mathbb{R}^n$ com uma única ressalva de que os grupos aditivos de $GF(p^k)$ ocorram para $k \leq n$.

### 4.1 CONSTELAÇÕES GEOMETRICAMENTE UNIFORMES COM $P^M$ SINAIS EM $\mathbb{R}^2$

As constelações geometricamente uniformes com $p^m$ sinais em $\mathbb{R}^2$, cuja construção será descrita nesta seção, serão constituídas por representantes de classes laterais provenientes de ideais $I$ de norma relativa $p^m$ nos anéis de inteiros $\mathbb{Z}[\theta]$, para $\theta = i$ e $\theta = \omega$, de tal forma que a energia média correspondente seja mínima.

Em [3] e [9], foram estabelecidas as condições de quando é possível construir constelações com $p$ sinais, cada uma casada ao correspondente grupo aditivo de $GF(p)$.

Para tal, foi analisado se $p$ é fatorável no anel de inteiros $\mathbb{Z}[\theta]$, para $\theta = i$ ou $\omega$, 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 $\gamma$.

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

Por outro lado, convém observar neste processo que existe um elemento $\gamma = a + b\theta$ de norma relativa $p$, se o par de inteiros $(a, b)$ for a solução inteira da forma quadrática $h(X, Y) = p$, onde $h(X, Y)$ é a norma relativa de um elemento $\mathbb{Z}[\theta]$. Para maiores detalhes, referimos o leitor à referência [11].

Através do estudo da representatividade de potências de primo $p^m$ por uma forma quadrática $h(X, Y)$ associada a norma relativa de um anel de inteiros $\mathbb{Z}[\theta]$, estabelecemos as condições necessárias para construir constelações geometricamente uniformes com $p^m$ sinais a partir de reticulados indentificados por $\mathbb{Z}[\theta]$.

No caso em que é possível tal construção, basta tomar $\gamma$ como sendo o gerador de um ideal $I$ em $\mathbb{Z}[\theta]$. Através do quociente $G \simeq \mathbb{Z}[\theta]/I$, obtemos o grupo quociente aditivo casado à constelação com $p^m$ sinais obtida a partir do reticulado identificado por $\mathbb{Z}[\theta]$.

A estrutura algébrica de tais grupos quocientes aditivos, $G$, dependerá das congruências $p$ módulo 4 ou $p$ módulo 6 para os reticulados identificados por $\mathbb{Z}[i]$ ou por $\mathbb{Z}[\omega]$ e do valor de $m$.

Foi mostrado em [3], [4] e [9] que é possível construir constelações com $p$ sinais, estas identificadas por $\mathbb{Z}[i]$, somente nos casos em que $p = 2$ ou $p = 4t + 1$, onde $t$ é um inteiro positivo. Quando as constelações são identificadas por $\mathbb{Z}[\omega]$ é possível construir constelações com $p$ sinais nos casos $p = 3$ ou $p = 6t + 1$, para $t$ inteiro positivo. Em todos esses casos as constelações são casadas a grupos aditivos de $GF(p)$.

As Proposições 4.1 e 4.2 fornecem respostas gerais de quando é possível construir constelações geometricamente uniformes com $p^m$ sinais casadas a grupos, constelações essas identificadas por $\mathbb{Z}[i]$ e por $\mathbb{Z}[\omega]$, bem como explicita quem são os grupos aditivos.

**Proposição 4.1** *Para qualquer primo p, é possível construir constelações com $p^2$ sinais, tais que*

*1 - Caso $\mathbb{Z}[i]$:*

- *1.1 Se $p = 4t + 1$, com $t \in \mathbb{Z}$, tais constelações estão casadas a $p$-grupos aditivos $G_{p^2}$ que não fazem parte de $GF(p^2)$;*
- *1.2 Se $p = 4t+3$, com $t \in \mathbb{Z}$ em $\mathbb{Z}[i]$, tais constelações estão casadas a grupos aditivos de $GF(p^2)$.*

*2 - Caso $\mathbb{Z}[\omega]$:*

- *2.1 Se $p = 6t + 1$, com $t \in \mathbb{Z}$, tais constelações estão casadas a $p$-grupos aditivos que não fazem parte de $GF(p^2)$;*
- *2.2 Se $p \neq 6t + 1$, com $t \in \mathbb{Z}$, tais constelações estão casadas a grupos aditivos de $GF(p^2)$.*

**Demonstração:**

1.1 Para $p = 4t + 1$, com $t \in \mathbb{Z}$, pelo Teorema de Gauss existe $\alpha = x + iy \in \mathbb{Z}[i]$, tal que $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha) = x^2 + y^2 = p$. Logo, tomando $\alpha^2 = (x + iy)^2 = (x^2 + y^2) + i(2xy)$, tem-se que $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha^2) = N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha)N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha) = p.p = p^2$.

O ideal $I$ tomado em $\mathbb{Z}[i]$ neste caso é $I = \langle\alpha^2\rangle$.

**1.2** Para $p = 4t + 3$, com $t \in \mathbb{Z}$, basta escolher $\alpha = p$, pois $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha) = N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(p) = p.p = p^2$. O ideal $I$ em $\mathbb{Z}[i]$, considerado neste caso, é $I = \langle p \rangle$.

**2.1** Para $p = 6t + 1$, com $t \in \mathbb{Z}$, existe $\alpha = x + \omega y \in \mathbb{Z}[\omega]$, tal que $N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\alpha) = x^2 + xy + y^2 = p$. Neste caso o ideal $I$ tomado em $\mathbb{Z}[\omega]$ é $I = \langle \alpha^2 \rangle$.

**2.2** Para $p \neq 6t + 1$, com $t \in \mathbb{Z}$, basta escolher $\alpha = p$, pois $N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\alpha) = N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(p) = p.p = p^2$. O ideal $I$ em $\mathbb{Z}[\omega]$, considerado neste caso, é $I = \langle p \rangle$.

■

**Proposição 4.2** *Os itens abaixo fornecem as condições suficientes para a construção de constelações com $p^m$ sinais, $m \geq 3$, todas casadas a p-grupos aditivos $G_{p^m}$ que não fazem parte de $GF(p^m)$.*

*1 - Caso $\mathbb{Z}[i]$:*

*1.1 Se o número primo p é da forma $p = 4t + 1$, então é possível construir constelações com $p^m$ sinais para qualquer p;*

*1.2 Para os números primos da forma $p = 4t + 3$ é possível construir constelações com $p^m$ sinais para os casos em que m é par.*

*2 - Caso $\mathbb{Z}[\omega]$:*

*2.1 Se o número primo p é da forma $p = 6t + 1$, então é possível construir constelações com $p^m$ sinais para qualquer p;*

*2.2 Para os números primos da forma $p \neq 6t + 1$ é possível construir constelações com $p^m$ sinais para os casos em que m é par.*

**Demonstração:**

**1.1** No caso em que $p = 4t + 1$, com $t \in \mathbb{Z}$, existe $\alpha = x + iy \in \mathbb{Z}[i]$, tal que $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha) = x^2 + y^2 = p$. Tomando $\gamma = \alpha^n$, temos que $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\gamma) = N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha^n) = p^n$. Neste caso o ideal $I$ em $\mathbb{Z}[i]$, será dado por $I = \langle \alpha^n \rangle$.

**1.2** Caso em que $p = 4t + 3$, com $t \in \mathbb{Z}$. Da Proposição 4.1, com $p = 4t + 3$, seja $\alpha = p$, então $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha) = N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(p) = p.p = p^2$. Tomando $\gamma = \alpha^k$, sua norma será $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\gamma) = N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha^k) = (p^2)^k$. Neste caso o ideal $I$ em $\mathbb{Z}[i]$, é dado por $I = \langle \alpha^k \rangle$.

**2.1** Caso em que $p$ é fatorável em $\mathbb{Z}[\omega]$ existe $\alpha \in \mathbb{Z}[\omega]$ tal que $p = \alpha.\overline{\alpha}$. Neste caso, $N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\alpha) = p$. Logo, tomando-se $\gamma = \alpha^m$, sua norma será $N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\gamma) = N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\alpha^m) = p^m$. Neste caso, o ideal $I$ em $\mathbb{Z}[\omega]$ é dado por $I = \langle \gamma \rangle$.

**2.2** Caso em que $p$ não é fatorável em $\mathbb{Z}[\omega]$. Neste caso para os valores de $m = 2k$, com $k$ inteiro, basta que tomemos $\gamma = p^k(1-\omega)$, que teremos $N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\gamma) = N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(p^k)N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(1-\omega) = p^{2k}.1 = p^m$ Basta tomar o ideal $I$ em $\mathbb{Z}[\omega]$, dado por $I = \langle \gamma \rangle$.

## 4.2 FUNÇÃO DE ROTULAGEM ENTRE UM GRUPO $G$ E CONSTELAÇÕES DE SINAIS EM $\mathbb{R}^2$

A função que estabelecerá a rotulagem casada entre os pontos de sinais das constelações (indentificados 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 $p^m$ elementos) é um rótulo para o ponto $x + y\theta \in \mathbb{Z}[\theta]$ se $x + yr \equiv l \bmod p^m$, onde $r \in \mathbb{Z}$ é a única solução (em s) da equação $a + bs \equiv 0 \bmod p^m$, onde $0 \leq s \leq p^m - 1$.*

**Exemplo 4.1** *Considere $p = 5$, $k = 2$ e $\mathbb{Z}[\omega]$. Sob estas condições, a representação $h(X, Y) = p^k$ é dada por $X^2 + XY + Y^2 = 25$. Uma das soluções inteiras é dada por $5 - 5w$. Seja $I$ o ideal primo gerado por $I = \langle 5 - 5w \rangle$. Então, $r = -4$ é solução inteira de $5 - s5 = 25$. Com isso, o rótulo do elemento $x + yw$ em $\mathbb{Z}[w]$ é obtido de $x - 4y \equiv l \bmod 25$ como sendo o elemento do grupo aditivo do corpo $GF(25)$.*

**Exemplo 4.2** *Considere $25 = (4+3i)(4-3i)$. Seja m ideal gerado por $m = \langle 4 - 3i \rangle$. Então, $r = -7$ é solução inteira de $4 - s3 = 25$. Com isso, o rotulo do elemento $x + yi$ em $\mathbb{Z}[i]$ é obtido de $x - 7y \equiv l \bmod 25$ como sendo o elemento do grupo $G_{25}$.*

A Figura 2 ilustra as constelações de sinais $A_{25}[i]$ e $A_{25}[\omega]$ 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 possuirem grupos de rótulos distintos o arranjo geométrico destas constelações de sinais são diferentes.

**Observação 4.1** *Constelações geometricamente uniformes com $p^m$ sinais em $\mathbb{R}^n$. Convém observar que também é possível construir constelações geometricamente uniformes com $p^m$ sinais em $\mathbb{R}^n$ rotuladas não apenas por grupos aditivos de $GF(p^m)$, como proposto em [13], mas também por p-grupos aditivos $G_{p^m}$.*

*Antes, no entanto, apresentaremos o Lema de Kummer e uma definição que foram preponderantes para a obtenção da rotulagem em [13].*

***Teorema 4.1** [14](Lema de Kummer) Seja $\mathcal{D}_{\mathbb{F}}$ o anel de inteiros do corpo de números $\mathbb{F} = \mathbb{Q}(\theta)$ e $p(X) \in \mathbb{Z}[X]$ o polinômio minimal de $\theta$ de grau $n$. Um ideal primo $\langle p \rangle$ de $\mathbb{Z}$ se decompõe em produto de ideais primos de $\mathcal{D}_{\mathbb{F}}$ da seguinte maneira: seja $\overline{p}(X) = \overline{p_1}(X)^{e_1} \ldots \overline{p_n}(X)^{e_s}$ a fatoração de $p(X)$ em polinômios mônicos irredutíveis de grau $f_i$, $1 \leq i \leq s$, sobre $\mathbb{Z}_p[X]$ com $e_1 + e_2 + \cdots + e_s = n$, onde a barra denota a classe de resíduos módulo p. Então $p\mathcal{D}_{\mathbb{F}}$ tem uma única fatoração $p\mathcal{D}_{\mathbb{F}} = \mathcal{P}_1^{e_1} \ldots \mathcal{P}_s^{e_s}$ como produto de potências de ideais primos em $\mathcal{D}_{\mathbb{F}}$, onde $\mathcal{P}_i = \langle p, p_i(\theta) \rangle$ e $\mathcal{D}_{\mathbb{F}}/\mathcal{P}_i \simeq GF(p^{f_i})$, para $1 \leq i \leq s$.*

***Proposição 4.3** [13] Sejam $\mathbb{F} = \mathbb{Q}(\theta)$ um corpo de números de grau $n$ com $\theta \in \mathcal{D}_{\mathbb{F}}$ e $\{\omega_1, \ldots, \omega_n\}$ uma base de $\mathbb{F}$ sobre $\mathbb{Q}$. Seja $\Lambda$ um reticulado obtido a partir de $\mathcal{D}_{\mathbb{F}}$.*

*Considere $\varphi$ um isomorfismo de $\mathcal{D}_{\mathbb{F}}/\mathcal{P}_i$ em $GF(p^{f_i})$. Seja $pr$ a projeção de $\mathcal{D}_{\mathbb{F}}$ em $\mathcal{D}_{\mathbb{F}}/\mathcal{P}_i$. Então $l = \varphi(pr)\sigma^{-1}$ é a rotulagem linear de $\Lambda$ em $GF(p^{f_i})$. Além disso, se $\mathcal{D}_{\mathbb{F}} = \mathbb{Z}[\theta]$, então $l$ pode ser completamente especificado*

■

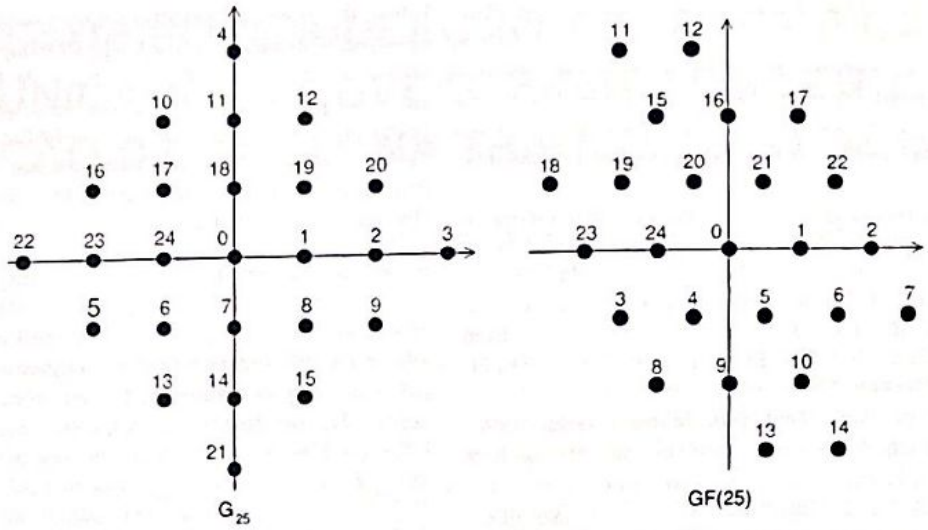


**Figura 2.** Constelações de Sinais.

*por* $l(\sigma(\theta)) = \overline{\theta}$, *com* $\overline{\theta}$ *a raiz do polinômio* $p_i(x)$ *sobre* $GF(p)$, *e* $l : \Lambda \longrightarrow GF(p^t)$ *é a rotulagem linear dada por* $l(\sigma(x_1\omega_1 + \ldots + x_n\omega_n)) = x_1 l(\sigma(\omega_1)) + \ldots + x_n l(\sigma(\omega_n))$, *para quaisquer* $x_i \in \mathbb{Z}$, *com* $1 \leq i \leq n$.

***Exemplo 4.3*** *Considere* $\mathbb{F} = \mathbb{Q}(\alpha)$, *onde* $\alpha$ *é a raiz complexa do polinômio minimal* $p(X) = X^3 - X + 1$. *O anel de inteiros é* $\mathcal{D}_{\mathbb{F}} = \mathbb{Z}[\alpha]$ *com uma base integral* $\beta = \{1, \alpha, -1 + \alpha^2\}$, *[14]. Tomando* $p(X)$ *módulo* 11, *obtemos* $p(X) = (X - 5)(X^2 + 5X + 2)(mod\ 11\ \mathbb{Z}[X])$, *onde o polinômio do segundo grau é irredutível sobre* $\mathbb{Z}_{11}$. *Assim,*

**i)**

$$11\mathbb{Z}[\alpha] = \mathcal{P}_1\mathcal{P}_2,$$

*onde* $\mathcal{P}_1 = \langle 11, \alpha - 5\rangle$ *e* $\mathcal{P}_2 = \langle 11, \alpha^2 - 6\alpha - 9\rangle$. *Temos que* $\mathbb{Z}[\alpha]/\mathcal{P}_1 \simeq GF(11)$, *e portanto,* $\alpha \equiv 5(mod \mathcal{P}_1)$.

*A função de rotulagem é* $l(\sigma(X_0 + X_1\alpha + X_2(-1 + \alpha^2)(mod\ 11\ \mathbb{Z}[X]) = X_0 + 5X_1 + 2X_2, \forall X_i \in \mathbb{Z}$, *com* $0 \leq i \leq 2$.

**ii)** *Considere o ideal* $I = \mathcal{P}_1^2$ *de norma* 121. *Então* $\mathbb{Z}[\alpha]/I \simeq G_{121}$, *e portanto,* $\alpha \equiv 5(mod I)$.

*A função de rotulagem é* $l(\sigma(x_0 + x_1\alpha + x_2(-1 + \alpha^2)(mod\ 121\ \mathbb{Z}[X]) = x_0 + 5x_1 + 24x_2, \forall x_i \in \mathbb{Z}$, *com* $0 \leq i \leq 2$.

## 5. CONCLUSÕES

Neste trabalho estendemos os procedimentos de construção e rotulagem de constelações de sinais geometricamente uniformes casadas a grupos aditivos de corpos de Galois a partir dos reticulados identificados pelos anéis de inteiros $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, propostos em [3], [4] e [9].

Mostramos que se $p$ for da forma $p = 4t + 1$ ou $p = 6t + 1$, $t$ inteiro, e os reticulados forem $\mathbb{Z}[i]$ ou $\mathbb{Z}[\omega]$, respectivamente, então existem constelações de sinais geometricamente uniformes com $p$ sinais casadas a grupos aditivos de $GF(p)$. Além disso, se $m \geq 2$ então existem constelações de sinais geometricamente uniformes com $p^m$ sinais casadas a $p$-grupos aditivos $G_{p^m}$ que não fazem parte de $GF(p^m)$.

Mostramos que se $p$ for da forma $p = 6t+1$ ou $p \neq 6t+1$, $t$ inteiro, e os reticulados forem $\mathbb{Z}[i]$ ou $\mathbb{Z}[\omega]$, respectivamente, então existem constelações de sinais geometricamente uniformes com $p^2$ sinais casadas a grupos aditivos de $GF(p^2)$. Além disso, se $m \geq 2$ e $m$ for par, então existem constelações de sinais geometricamente uniformes com $p^m$ sinais casadas a $p$-grupos aditivos de $G_{p^m}$ que não fazem parte de $GF(p^m)$.

Em $\mathbb{R}^n$, verificamos que nos casos em que a proposta apresentada em [13] é satisfeita, isto é, existe uma constelação geometricamente uniforme com $p^k$ sinais casada a um grupo aditivo de $GF(p^k)$ a partir de um reticulado identificado por um anel de inteiros proveniente de um corpo de números de grau $n$, é possível construir uma constelação geometricamente uniforme com $p^m$ sinais casada a um $p$-grupo aditivo de $G_{p^m}$ cuja cardinalidade é $p^m$ e que não faça parte de $GF(p^m)$, onde $p^m$ é uma potência de $p^k$.

## AGRADECIMENTOS

Este trabalho teve o suporte financeiro da Fundação de Amparo à Pesquisa do Estado de São Paulo, FAPESP, processo 95/4720-08, do Conselho Nacional de Desenvolvimento Científico e Tecnológico, CNPq, processo 301416/85-0, e da CAPES-PROCAD, processo 0121/01-0, Brasil.

## REFERÊNCIAS

[1] G.D. Forney, "Geometrically uniform codes," *IEEE Trans. Inform. Theory*, vol.IT-37, No.6, pp. 1241-1259, Sept. 1991.

[2] H.A. Loeliger, "Signal sets matched to groups," *IEEE Trans. Inform. Theory*, vol.IT-37, No.6, pp. 1675-1682, Nov. 1991.

[3] K. Huber, "Codes over gaussian integers," *IEEE Trans. Inform. Theory*, vol.IT-40, pp. 207-216, Jan. 1994.

[4] K. Huber, "Codes over Eisenstein-Jacobi integers," *Contemporary Mathematics*, vol.168, pp. 165-179, 1994.

[5] R.G. Egri, and F.A. Horrigan, "A finite group of complex integers and its application to differentially coherent detection of

QAM signals," *IEEE Trans. Inform. Theory*, vol.IT-40, pp. 216-219, Jan. 1994.

[6] J. Rifà, "Groups of complex integers used as QAM signals," *IEEE Trans. Inform. Theory*, vol.IT-41, pp. 1512-1517, Sept. 1995.

[7] O. Endler, *Teoria dos Núneros Algébricos*, Projeto Euclides, 1986.

[8] E.D. Carvalho, *Construção e Rotulamento de Constelações de Sinais Geometricamente Uniformes em Espaços Euclidianos e Hiperbólicos*, Tese de Doutorado, FECC-UNICAMP, 2001.

[9] T.P. Nóbrega Neto, J.C. Interlando, O.M. Favareto, M. Elia, and R. Palazzo Jr, "Lattice constellations and codes from quadratic number fields,"*IEEE Trans. Inform. Theory*, vol.IT-47, pp. 1514-1527, May 2001.

[10] J. Rotman, *Galois Theory*, New York: Springer-Verlag, 1990.

[11] T.Y. Lam, *The Algebraic Theory of Quadratic Forms*, New York: Benjamim, 1963.

[12] X.D. Dong, C.B. Soh, E. Gunawan, and L.Z. Tang, "Groups of algebraic integers used for coding QAM signal," *IEEE Trans. Inform. Theory*, vol.44, No.5, pp. 1848-1860, Sept. 1998.

[13] J.C. Interlando, and M. Elia, "On the linear labelling of lattice constellations from algebraic numbers fields,"*Combinatorics '2000* Gaeta, Italy, pp. 181.

[14] M. Phost, and H. Zassenhaus, *Algorithmic Algebraic Numbers Theory*, Cambridge University, 1989.

**Edson Donizete de Carvalho** graduou-se em Matemática pela Universidade Estadual Paulista(UNESP) câmpus de São José do Rio Preto SP em 1994. Obteve o título de Mestre em Matemática em 1997 pelo IMECC-UNICAMP e o título de Doutor em Engenharia Elétrica em 2001 pela FEEC-UNICAMP na área de Telecomunicações. Atualmente é professor da Universidade Vale do Rio Verde de Três Corações(UNINCOR). Suas áreas de interesse incluem teoria algébrica dos números, ações des grupos e codificação.

**Reginaldo Palazzo Jr.** Formado em Engenharia Elétrica (1975) pela Faculdade de Engenharia da UNICAMP. Pela mesma escola, obteve em 1977 o título de Mestre em Engenharia Elétrica. Em 1981 e em 1984 obteve o Engineer Degree e o Doctor of Philosophy pela University of California, Los Angeles. Foi consultor da Technology Transfer Institute e da Quotron System Inc, Los Angeles, USA, em 1984. Em 1985, foi contratado pela FEEC-UNICAMP. Em 1987 obteve o título de Livre Docente pela FEEC-UNICAMP. Em 1993 foi professor visitante no Departamento de Engenharia Elétrica da University of Notre Dame, Indiana, USA. É pesquisador 1A do CNPq, desde 1997. Foi promovido para *Senior Member* do Institute of Electric and Electronics Engineers, USA, em 1997. Recebeu o Prêmio de Reconhecimento Acadêmico Zeferino Vaz pela FEEC-UNICAMP em 1998. É membro do Comitê Assessor da Engenharia Elétrica do CNPq (Julho de 2001 a Junho de 2004). Atualmente, é assessor na Pró-reitoria de Pesquisa, UNICAMP. É Professor Titular MS6 da FEEC-UNICAMP desde 1996. Ministrou palestras, cursos e participou de atividades de curta duração em diversas instituições internacionais.

**Marcelo Firer** é matemático, formado pela Unicamp, com doutorado pela Universidade de Jerusalém. Suas áreas de interesse incluem Teorias de Lie, especialmente espaços simétricos, ações de grupos grafos, Edifícios de Tits e relações destas com codificação.