Construções de reticulados densos via polinômios

Antonio Aparecido de Andrade [1]
Departamento de Matemática, Ibilce - Unesp, São José do Rio Preto - SP.
Agnaldo José Ferrari [2]
Departamento de Matemática, FC - Unesp, Bauru - SP
Robson Ricardo de Araujo [3]
Doutorando em Matemática, Departamento de Matemática, Imecc - Unicamp, Campinas - SP.

Resumo. O estudo de reticulados surgiu a partir do problema de como cobrir o espaço $\mathbb{R}^n$ com esferas de mesmo raio de forma que quaisquer duas esferas se toquem em apenas um ponto e ocupem o maior espaço possível. Na teoria de reticulados algébricos um dos principais problemas é a obtenção de reticulados com alta densidade e que sejam ao mesmo tempo de fácil manipulação. No presente trabalho apresentamos construções de reticulados de dimensões 2 e 3 via polinômios de graus 2 e 3 no corpo de números reais, e dessa forma obtemos versões rotacionadas dos reticulados Λ_2 e Λ_3. Desse modo, apresentamos alguns fatos sobre os reticulados, definindo-os e apresentamos suas principais propriedades. Apresentamos a matriz de Gram de um reticulado e seu determinante, o conceito de discriminante de uma equação e fornecemos de maneira explícita o discriminante de uma equação quadrática e de uma cúbica. Em seguida, apresentamos construções de reticulados de dimensão 2 via polinômios de grau 2 com raízes reais, com raízes complexas e com raízes duplas Em seguida apresentamos construções de reticulados de dimensão 3 via polinômios de grau 3 com raízes reais (podendo uma delas ser dupla), com uma raiz real e duas raízes complexas, e finalmente, com uma raiz tripla. Em todos os casos obtemos exemplos de reticulados com densidade de centro ótima de dimensões 2 e 3.

1 Resultados básicos

O problema clássico do empacotamento esférico consiste em encontrar um arranjo de esferas idênticas no espaço euclidiano n-dimensional de forma que a fração do espaço coberto por essas esferas seja a maior possível. Ao estudar a densidade de empacotamento, um dos principais problemas é a obtenção de reticulados com alta densidade e que sejam ao mesmo tempo manipuláveis.

O volume no $\mathbb{R}^n$ é bem conhecido e pode ser facilmente transferido para o $\mathbb{R}$-espaço V através do isomorfismo natural entre $\mathbb{R}^n$ e V, e definido por meio de uma base $\{v_1, \cdots, v_n\}$.

Um empacotamento esférico, ou simplesmente um empacotamento no $\mathbb{R}^n$, é uma distribuição de esferas de mesmo raio no $\mathbb{R}^n$ de forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio. Um empacotamento reticulado é um empacotamento em que o conjunto dos centros das esferas formam um reticulado $\mathcal{H}_\beta$ de $\mathbb{R}^n$. Dado um empacotamento no

[1] andrade@ibilce.unesp.br. Agradecimentos a Fapesp, Proc. 2013/25977-7.
[2] ferrari@fc.unesp.br
[3] ra162215@ime.unicamp.br.

$\mathbb{R}^n$, associado a um reticulado $\mathcal{H}_\beta$, com $\beta = \{v_1, \cdots, v_n\}$ uma $\mathbb{Z}$-base, definimos a sua densidade de empacotamento como sendo a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas.

Estamos interessados no empacotamento associado a um reticulado $\mathcal{H}_\beta$ em que as esferas tenham raio máximo. Para a determinação deste raio, observe que fixado $k > 0$, a intersecção do conjunto compacto $\{x \in \mathbb{R}^n;\ |x| \leq k\}$ com o reticulado $\mathcal{H}_\beta$ é um conjunto finito, de onde segue que o número $\mathcal{H}_{\beta_{min}} = min\{|\lambda|;\ \lambda \in \mathcal{H}_\beta,\ \lambda \neq 0\}$ está bem definido e $(\mathcal{H}_{\beta_{min}})^2$ é chamado de norma mínima. Observamos que $\rho = \mathcal{H}_{\beta_{min}}/2$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de $\mathcal{H}_\beta$ e obter um empacotamento, assim ρ é chamado raio de empacotamento do reticulado. Dessa forma, estudar os empacotamentos reticulados equivale ao estudo dos reticulados. Denotando por $\mathcal{B}(\rho)$ a esfera com centro na origem e raio ρ, temos que a densidade de empacotamento de $\mathcal{H}_\beta$ é igual a

$$\Delta(\mathcal{H}_\beta) = \frac{\text{Volume da esfera}}{\text{Volume da região fundamental}} = \frac{\mathcal{V}ol(\mathcal{B}(\rho))}{\mathcal{V}ol(\mathcal{H}_\beta)} = \frac{\mathcal{V}ol(\mathcal{B}(1))\rho^n}{\mathcal{V}ol(\mathcal{H}_\beta)}. \tag{1}$$

Portanto, o problema se reduz ao estudo de um outro parâmetro, chamado de densidade de centro, que é dado por

$$\delta(\mathcal{H}_\beta) = \frac{\rho^n}{\mathcal{V}ol(\mathcal{H}_\beta)}. \tag{2}$$

Logo, tiramos a seguinte relação

$$\Delta(\mathcal{H}_\beta) = \mathcal{V}ol(\mathcal{B}(1))\delta(\mathcal{H}_\beta), \tag{3}$$

ou seja, a densidade de empacotamente de $\mathcal{H}_\beta$ é igual ao produto entre o volume da esfera com centro na origem e raio 1 e a densidade de centro $\delta(\mathcal{H}_\beta)$.

2 Construções de reticulados

Seja uma equação $p(x) = a_0 + a_1x + a_2x^2 + \cdots + x^n$ com coeficientes reais. O produto dos quadrados das diferenças das raízes da equação onde o coeficiente dominante é 1 é chamado discriminante da equação e denotado por Δ. Assim, se $\alpha_1, \alpha_2, \cdots, \alpha_n$ são as raízes de $p(x) = 0$, então $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2$. Em particular, o discriminante de uma equação quadrática $p(x) = x^2 + ax + b = 0$ é dada por $\Delta = a^2 - 4b$ e o discriminante de uma equação cúbica $p(x) = x^3 + ax^2 + bx + c = 0$ é dada por $\Delta = 18abc - 4a^3c + a^2b^2 - 4b^3 - 27c^2$.

Nas construções de reticulados em dimensões 2 e 3 tratamos de equações quadráticas e equações cúbicas com um olhar sobre os seus discriminantes e seus coeficientes. Para isso, apresentamos condições sobre seus discriminantes e sobre seus coeficientes para as construções de reticulados densos nessas dimensões, quando $\Delta > 0$, $\Delta = 0$ e $\Delta < 0$. Finalmente, apresentamos construções de reticulados densos em dimensões superiores, que generaliza as construções nas dimensões 2 e 3.

Referências

[1] L.E. Dickson, *First course in the theory of equations*, John Wiley & Sons, Inc, London, 1922.

[2] T.M Souza, *Reticulados algébricos em corpos de números abelianos*. Dissertação de Mestrado em Matemática, Instituto de Biociências, Letras e Ciências Exatas (Ibilce), Universidade Estadual Paulista (Unesp), São José do Rio Preto - SP, 2004.

Construção do reticulado hexagonal via o método de Krüskemper

Agnaldo José Ferrari [1]
Departamento de Matemática, FC - Unesp, Bauru - SP.
Antonio Aparecido de Andrade [2]
Departamento de Matemática, Ibilce - Unesp, São José do Rio Preto - SP.

Resumo. O objetivo deste trabalho é a construção do reticulado hexagonal via ideais reticulados em alguma algebra $\mathbb{Z}[x]/(f(x))$, onde $f(x)$ é um polinômio mônico e irredutível. A construção é baseada no Método de Krüskemper [2], [4]. Os reticulados construídos, via este método, possuem diversidade máxima, representando assim constelações eficientes para transmissão sobre os canais com desvanecimento do tipo Rayleigh. Além disso, através da distância produto mínima, um relevante parâmetro de performance, obtemos constelações mais eficientes das conhecidas até o momento.

1 Preliminares

Seja M um $\mathbb{Z}$-módulo livre finitamente gerado de posto n e $b : M \times M \to \mathbb{Z}$ uma forma bilinear simétrica. Seja $f(x) \in \mathbb{Z}[x]$ um polinômio mônico irredutível de grau n e θ uma raíz de f. Assim, $\mathbb{Z}[x]/(f(x)) = \mathbb{Z}[\theta]$ com base $\{1, \theta, \cdots, \theta^{n-1}\}$. Seja $\mathcal{A}$ um ideal de $\mathbb{Z}[\theta]$. Definimos $\mathcal{A}^{\#} = \{c \in \mathbb{Q}(\theta) \mid Tr(c\mathcal{A}) \subseteq \mathbb{Z}\}$. Sejam $B \in \mathcal{M}_n(\mathbb{Z})$ uma matriz simétrica não singular e $A \in \mathcal{M}_n(\mathbb{Z})$ tal que seu polinômio característico χ_A é irredutível e $B^{-1}AB = A^T$, então B é a matriz de um ideal reticulado [2]. Seja (M, b) um reticulado integral, então existe um inteiro algébrico θ, um ideal $\mathcal{A}$ de $\mathbb{Z}[\theta]$ e $\alpha \in (\mathcal{A}^2)^{\#} \subseteq \mathbb{Q}(\theta)$ tal que b é isomorfo a $\varphi : \mathcal{A} \times \mathcal{A} \to \mathbb{Z}$ dado por $\varphi(x, y) = Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha xy)$. O elemento θ pode ser considerado totalmente real [4].

2 Construção do reticulado hexagonal

Uma matriz geradora para o reticulado hexagonal A_2 e sua matriz de Gram são dadas, respectivamente, por

$$M = \begin{bmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix} \quad \text{e} \quad G = \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}.$$

. Seja o polinîomio irredutível $p(x) = x^3 - 2$ sobre $\mathbb{Q}$. A matriz $A = \begin{bmatrix} -1 & 1 \\ 2 & 1 \end{bmatrix}$ é raiz do polinômio $p_A(x) = x^3 - 3I$, onde I é a matriz identidade de ordem 3, $G^{-1}AG = A^t$, onde A^t é a transposta de A. Agora, computamos duas matrizes V e G do seguinte modo: sejam $v_\theta = \{v_1, v_2\}$, onde $v_j = (-1)^{i+j}\Delta_{ij}(A - \theta I_n)$ e $i = 1$. Assim, $v_\theta = \{(1 - \theta, -2)\}$. Se $V =$

[1] ferrari@fc.unesp.br
[2] andrade@ibilce.unesp.br. Agradecimentos a Fapesp - Processo 2013/25977-7.

$\{(v_{11}, v_{12}), (v_{21}, v_{22})\}$ e $\{(1, \theta)\}V = \{(v_1, v_2)\}$, então $V = \{(1, -2), (-1, 0)\}$, e consequentemente, $(V^T)^{-1} = \{(\frac{1}{2}, 0), (0, \frac{1}{6})$.

Agora, $G = (Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^{i-1}\theta^{j-1}))_{i,j=1}^{2} = \{(2, 0), (0, 6)\}$, uma vez que θ é uma raiz de $p_A x$. O conjunto das raizes de $p_A(x)$ é $\left\{-\sqrt{3}, \sqrt{3}\right\}$,e isto significa que os homomorfismos reais de θ são $\sigma_1(\theta) = -\sqrt{3}$ e $\sigma_2(\theta) = \sqrt{3}$. Além disso, $d_{\mathbb{K}} = det(G) = 12$.

Sejam $v_\theta^{'} = \{(v_1^{'}, v_2^{'})\}$, onde $v_1^{'} = \sum_{i=1}^{2} m_{i1}\theta^{i-1}$, $v_2^{'} = \sum_{i=1}^{2} m_{i2}\theta^{i-1}$ e

$$(m_{ij})_{i,j=1}^{2} = G^{-1}(V^T)^{-1} = \left\{\left(0, -\frac{1}{4}\right), \left(-\frac{1}{6}, -\frac{1}{12}\right)\right\}.$$

Portanto, $v_\theta^{'} = \{(v_1^{'}, v_2^{'})\} = \left\{\left(-\frac{1}{6}\theta, -\frac{1}{4} - \frac{1}{12}\theta\right)\right\}$. O elemento α é dado por $\alpha v_\theta = G v_\theta^{'}$, i.e., $\alpha\{(1 - \theta, -2)\} = \{(2, -1), (-1, 2)\}\{(-\frac{1}{6}\theta, -\frac{1}{4} - \frac{1}{12}\theta)\}$. Usando, por exemplo, a última linha, computamos $\alpha = \frac{1}{4}$. Assim, a matriz geradora do reticulado é dada por

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(v_1) & \sqrt{\alpha_2}\sigma_2(v_1) \\ \sqrt{\alpha_1}\sigma_1(v_2) & \sqrt{\alpha_2}\sigma_2(v_2) \end{pmatrix} = \begin{pmatrix} \frac{1+\sqrt{3}}{2} & \frac{1-\sqrt{3}}{2} \\ -1 & -1 \end{pmatrix}.$$

Assim, $det(b_\alpha) = det(G) = 3$, $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]] = 1$ e $h(\mathbb{K}) = 1$, onde $\mathbb{K} = \mathbb{Q}(\sqrt{3})$. Como a norma mínima de A_2 é $\mu = 2$, segue que o reticulado construído sobre o anel $\mathcal{O}_{\mathbb{K}}$ tem distância produto mínima relativa dada por

$$\sqrt{d_{p,rel}(A_2)} = \left(\frac{1}{(\sqrt{\mu})^2}\sqrt{\frac{det(b_\alpha)}{d_{\mathbb{K}}}}\frac{min\{\mathcal{A}\}}{[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]]}\right)^{1/2} = \left(\frac{1}{(\sqrt{2})^2}\sqrt{\frac{3}{12}}\right)^{1/2} = 0.5.$$

Referências

[1] J. Boutros, E. Viterbo, C. Rastello, J.C. Belfiore. *Good lattice constellations for both Rayleigh fading and Gaussian channels*, *IEEE Transactions on Information Theory*, v. 42, n. 2, pp. 502-518, 1996.

[2] E.P. Conner, R. Perlis. *A survey of trace forms of algebraic number fields*, Series in Pure Mathematics, v. 2, 1984.

[3] J.H. Conway, N.J.A. Sloane. *Sphere packings, lattices and groups*, 3rd edition, *Spring-Verlag*, New York, 1999.

[4] M. Krüskemper. *Algebraic construction of bilinear forms over* $\mathbb{Z}$. *Pub. Math. de Besancon, Théorie des nombres*, 1996/97 - 1997/98.

[5] F. Oggier. *Algebraic methods for channel coding. Tese de doutorado*, École Polytechnique fédérale de Laisanne, 2005.

[6] F. Oggier, E.B. Fluckiger. *Best rotated cubic lattice constellations for Rayleigh fading channel. Proc. Int. Symposium of Information Theory - ISIT 2003*, Yokohama, Japan, July 2003.

Reticulados algébricos via corpos de números abelianos de grau primo

Robson Ricardo de Araujo [1]
Doutorando em Matemática, Imecc - Unicamp, Campinas - SP
Sueli Irene Rodrigues Costa [2]
Departamento de Matemática, Imecc - Unicamp, Campinas - SP.

Resumo Um corpo de números abeliano $\mathbb{K}$ de grau primo p está contido em um corpo ciclotômico $Q(\zeta_n)$ em que $n = p^2\tilde{n}$ ou $n = \tilde{n}$, onde $\tilde{n}$ é livre de quadrados. Em cada caso é possível estudar e descrever explicitamente qual é a base do anel de inteiros de $\mathbb{K}$ e qual é a expressão da forma traço integral $Tr_{\mathbb{K}}(x\overline{x})$ em função de p e de n, com x nesse anel de inteiros. Nesta apresentação pretendemos apresentar esses resultados e a relação deles com a densidade de reticulados algébricos construídos pelo mergulho canônico sobre $\mathbb{Z}$-módulos do anel de inteiros de $\mathbb{K}$.

1 Preliminares

Um subgrupo discreto aditivo de $\mathbb{R}^n$ é o que chamamos de reticulado, o qual possui uma base com $m \leq n$ vetores. Se $m = n$ dizemos que o reticulado é de posto máximo ou completo. Um reticulado é, portanto, o conjunto das combinações lineares sobre $\mathbb{Z}$ de m vetores linearmente independentes. Os reticulados têm sido já há algum tempo aplicados à Teoria de Códigos e à Criptografia, devido à sua simetria e às suas inúmeras propriedades. Na maioria das vezes os pesquisadores da área se preocupam em produzir reticulados com alta densidade de centro (ou seja, com bom empacotamento esférico) para serem utilizados em canais Gaussianos ou com máxima diversidade e boa distância produto mínima para serem aplicados em canais do tipo Rayleigh com desvanecimento. Classicamente sabe-se que reticulados podem ser obtidos via Teoria Algébrica dos Números através do mergulho canônico. O mergulho canônico (ou homomorfismo de Minkowski) é uma aplicação que realiza geometricamente os elementos de um corpo de números, produzindo um reticulado quando aplicado em um $\mathbb{Z}$-módulo de um anel de inteiros.

2 Reticulados algébricos

Se M é um $\mathbb{Z}$-módulo de um anel de inteiros de um corpo de números $\mathbb{K}$ de grau n, então o mergulho canônico é a aplicação $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^n$ definida por

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), Re(\sigma_{r_1+1}(x)), Im(\sigma_{r_1+1}(x)), \ldots, Re(\sigma_{r_2}(x)), Im(\sigma_{r_2}(x)))$$

[1] ra162215@ime.unicamp.br.
[2] sueli@ime.unicamp.br. Agradecimentos a Fapesp, Proc. 2013/25977-7.

em que $\sigma_i : \mathbb{K} \longrightarrow \mathbb{C}$ são os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$, (r_1, r_2) é a assinatura do corpo $\mathbb{K}$, e o conjunto $\sigma(M)$ é um reticulado completo em $\mathbb{R}^n$. Neste caso, a densidade de centro do reticulado $\sigma(M)$ é dada pela expressão

$$\delta(\sigma(M)) = \frac{2^{r_2}\rho^n}{[\mathcal{O}_{\mathbb{K}} : M]\sqrt{D(\mathbb{K})}}$$

em que $[\mathcal{O}_{\mathbb{K}} : M]$ é o índice do $\mathbb{Z}$-módulo M em $\mathcal{O}_{\mathbb{K}}$, $D(\mathbb{K})$ é o discriminante do corpo $\mathbb{K}$ e

$$\rho \triangleq \min_{0 \neq x \in M} Tr_{\mathbb{K}}(x\overline{x})$$

é o mínimo da força traço integral $Tr_{\mathbb{K}}(x\overline{x})$ em M.

Quando $\mathbb{K}$ é um corpo de números de grau primo $p > 2$ podemos calcular a expressão da forma traço integral $Tr_{\mathbb{K}}(x\overline{x})$ (note que $\overline{x} = x$ neste caso), para x no anel de inteiros de $\mathbb{K}$. Tal expressão está em função de p e do condutor de $\mathbb{K}$, que é o menor inteiro m tal que $\mathbb{K} \subset \mathbb{Q}(\zeta_m)$. Para obter essa expressão é necessário notar que há duas possibilidades para m: ou $m = p^2\tilde{m}$ ou $m = \tilde{m}$, em que $m = p_1 p_2 \dots p_r$, com $p_i \equiv 1 \ (mod\ p)$ distintos entre si.

Nesta apresentação vamos apresentar as propriedades do corpo de números $\mathbb{K}$ de grau primo $p > 2$ para cada um dos casos mencionados acima. Em particular, explicitaremos uma base integral de $\mathbb{K}$ em cada caso. Posteriormente apresentaremos a expressão da forma traço integral $Tr_{\mathbb{K}}(x\overline{x})$ em cada caso e veremos aplicações desses resultados a fim de produzir reticulados algébricos com boa densidade.

Referências

[1] Conway, J.H., Sloane, N.J.A. *Sphere packings, lattices and group*. Springer-Verlag, Nova Iorque, 3ª edição, 1998.

[2] A.L. Flores. **Lattices in Abelian Fields**. PhD Thesis (in portuguese), Campinas, 2000.

[3] V.H. Leopoldt. **Ûber die Hauptordnung der Ganzen Elemente Eines Abelschen Zahlkörpers**. J. Reine Angew. Math., 201, 119-149, 1959.

[4] G. Lettl. **The Ring of Integers of an Abelian Number Field**. J. Reine Angew. Math., 404, 162-170, 1990.

[5] T.P.N. Neto, J.O.D. Lopes, J.C. Interlando. **The Discriminant of Abelian Number Fields**. Journal of Algebra and its Applications, 5(1), 1-7, 2006.

[6] J.V.L. Nunes, J.C. Interlando, T.P.N. Neto, J.O.D. Lopes. **New p-dimensional Lattices from Cyclic Extensions**. Journal of Algebra and Its Applications, p. 1750186, (9 pages) 2016.

[7] E.L. Oliveira. **Towers of Abelian Extensions of Unramified Prime Degree**. PhD Thesis (in Portuguese), São José do Rio Preto, 2015.

[8] E.L. Oliveira, J.C. Interlando, J.C., T.P.N. Neto, J.O.D. Lopes. **The Integral Trace Form of Cyclic Extensions of Odd Prime Degree**. To appear in Rocky Mountain J. Math.

Alguns resultados sobre reticulados bem arredondados

Carina Alves [1]
Departamento de Matemática, Igce - Unesp, Rio Claro - SP.

Resumo. Os reticulados bem arredondados (do inglês, *Well Rounded Lattices* (WR)) têm sido um tópico de estudo recente, com aplicações em canais grampeados e em criptografia. Os reticulados WR são aqueles que possuem uma base em que todos os vetores têm norma coincidindo com a norma mínima do reticulado. Neste trabalho será feito um estudo de reticulados WR a partir de ideais no anel dos inteiros de corpos de números quadráticos, mostrando que existe uma infinidade de corpos de números quadráticos reais ou imaginários contendo ideais que produzem reticulados WR no plano. Serão abordadas também questões relacionadas a reticulados WR, quando corpos ciclotômicos são considerados.

1 Resultados básicos

Seja Λ um reticulado de posto total no espaço euclidiano n-dimensional. A norma mínima de Λ é definida como $|\Lambda| := \min\{||x||^2 : x \in \Lambda \setminus \{0\}\}$, onde $||\,||$ denota a norma euclidiana usual em $\mathbb{R}^n$ e o conjunto de vetores mínimos de Λ é denotado por

$$S(\Lambda) := \{x \in \Lambda : ||x||^2 = |\Lambda|\}.$$

O reticulado Λ é WR se o conjunto $S(\Lambda)$ gera $\mathbb{R}^n$.

Sejam $\mathbb{K}$ um corpo de números de grau n sobre $\mathbb{Q}$ e $\mathcal{O}_\mathbb{K}$ o seu anel de inteiros. Para cada $x \in \mathbb{K}$, seja $\sigma_\mathbb{K} : \mathbb{K} \to \mathbb{R}^n$ o homomorfismo canônico definido por

$$\sigma_\mathbb{K}(x) = (\sigma_1, \cdots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \cdots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)),$$

onde as notações $\Re(x)$ e $\Im(x)$ representam as partes real e imaginária do número complexo x, respectivamente. Assim, $\Lambda_\mathbb{K} := \sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})$ é um reticulado de posto total em $\mathbb{R}^n$, onde $n = r_1 + 2r_2$. Mais geralmente, para qualquer ideal fracionário não nulo I de $\mathcal{O}_\mathbb{K}$, $\Lambda_\mathbb{K}(I) := \sigma_\mathbb{K}(I)$ é um reticulado de posto total em $\mathbb{R}^n$.

2 Resultados

Neste trabalho, veremos que existem infinitos corpos de números quadráticos reais e imaginários $\mathbb{K}$, cujo anel dos inteiros contém um ideal I, tal que o reticulado $\sigma_\mathbb{K}(I)$ é WR. Outro importante resultado é que o reticulado Λ_D é WR se, e somente se, $D = -1, -3$, onde Λ_D denota o reticulado $\Lambda_\mathbb{K}$.

No entanto, quando consideramos corpos ciclotômicos veremos que reticulados obtidos a partir de corpos ciclotômicos são sempre WR. Os resultados apresentados neste trabalho são baseados nas referências [1, 2].

[1] carina@rc.unesp.br. Agradecimentos à Fapesp, Proc. 2013/25977-7.

Referências

[1] O. W. Gnilke, H. T. N. Tran, A. Karrila and C. Hollanti *Well-Rounded Lattices for Reliability and Security in Rayleigh Fading SISO Channels*, *Information Theory Workshop (ITW), 2016 IEEE*.

[2] L. Fukshansky and K. Petersen, *On Well-Rounded Ideal Lattice*, *International Journal of Number Theory*, 8 (1), 2012, 189-2206.

Códigos na métrica p-Lee

Grasiele Cristiane Jorge [1]
Instituto de Ciência e Tecnologia - Unifesp, São José dos Campos - SP.
Antonio Carlos de Andrade Campello Junior [2]
Imperial College London, Londres, Inglaterra
João Eloir Strapasson [3]
Faculdade de Ciências Aplicadas, Unicamp, Limeira - SP.
Sueli Irene Rodrigues Costa [4]
Departamento de Matemática, Imecc - Unicamp, Campinas - SP.

Resumo Códigos são frequentemente estudados nas métricas de Hamming e de Lee. Neste trabalho, apresentamos resultados sobre códigos q-ários perfeitos e quase perfeitos na métrica p-Lee para $p = 2$.

1 Preliminares

Um código q-ário C é um subconjunto de $\mathbb{Z}_q^n$, $q \in \mathbb{N}$. Um código $C \subset \mathbb{Z}_q^n$ é chamado linear se é um subgrupo aditivo de $\mathbb{Z}_q^n$.

Dados $\overline{x}, \overline{y} \in \mathbb{Z}_q^n$, a métrica p-Lee é definida como $d_{p,Lee}(\overline{x}, \overline{y}) = \left(\sum_{i=1}^{n} (d_{Lee}(\overline{x}_i, \overline{y}_i))^p \right)^{1/p}$ se $1 \leq p < \infty$ e $d_{\infty,Lee}(\overline{x}, \overline{y}) = \max\{d_{Lee}(\overline{x}_i, \overline{y}_i),\ i = 1, \ldots, n\}$, onde $d_{Lee}(\overline{x_i}, \overline{y_i}) = \min\{|\overline{x_i} - \overline{y_i}|, q - |\overline{x_i} - \overline{y_i}|\}$.

2 Resultados

A fim de definir os conceitos de códigos perfeitos e quase perfeitos na métrica p-Lee para $2 \leq p < \infty$, primeiro definimos o conjunto distância como $\mathcal{D}_{p,n,q} = \{d \in \mathbb{R},$ tal que existem $z \in \mathbb{Z}_q^n$ e $c \in C$ com $d_{p,Lee}(z, c) = d\}$. O raio de empacotamento de um código $C \subseteq \mathbb{Z}_q^n$ na métrica p-Lee, denotado por r_p, é o maior $r \in \mathcal{D}_{p,n,q}$ tal que $B_p^n(x, r) \cap B_p^n(y, r) = \emptyset$ para todo $x, y \in C$, onde $B_p^n(a, r)$ denota a bola fechada na métrica p-Lee em $\mathbb{Z}_q^n$ centrada em a com raio r. O raio de cobertura de um código $C \subseteq \mathbb{Z}_q^n$ na métrica p-Lee, denotado por R_p, é o menor $r \in \mathcal{D}_{p,n,q}$ tal que $\bigcup_{c \in C} B_p^n(c, r) = \mathbb{Z}_q^n$. Definimos a distância de dois elementos $r_a, r_b \in \mathcal{D}_{p,n,q}$ com $r_a < r_b$ como $d(r_a, r_b) = \#\left(\mathcal{D}_{p,n,q} \cap [r_a, r_b)\right)$, onde $[r_a, r_b)$ denota um intervalo em $\mathbb{R}$. Dizemos que um código é perfeito quando $r_p = R_p$ e quase perfeito quando $d(r_p, R_p) = 1$.

[1] grasiele.jorge@unifesp.br
[2] accampellojr@gmail.com
[3] joao.strapasson@fca.unicamp.br
[4] sueli@ime.unicamp.br. Agradecimentos à Fapesp, Proc. 2013/25977-7 e 2015/17167-0 e ao CNPq, Proc. 432735/2016-0.

Neste trabalho, apresentamos alguns resultados de [1] e [3] onde, através de uma abordagem computacional, para $p = 2$ e $n = 2, 3$ foram determinados todos os raios para os quais existem códigos lineares perfeitos e quase perfeitos.

Referências

[1] A. Campello, G. C. Jorge, J. E. Strapasson, S. I. R. Costa, *Perfect codes in the l_p metric*, *European Journal of Combinatorics*, vol. 53, p. 72-85, 2016.

[2] S.W. Golomb, L. R. Welch, *Perfect Codes in the Lee Metric and the Packing of Polyominoes*, *SIAM Journal on Applied Mathematics*, vol. 18, p. 302-317, 1970.

[3] J. E. Strapasson, G. C. Jorge, A. Campello, S. I. R. Costa, *Quasi-perfect codes in the l_p metric*, *Computational Applied Mathematics*, p. 1-15, 2016.

Estratégias de codificação para redes 5G

Cintya Wink de Oliveira Benedito [1]
Câmpus Experimental de São João da Boa Vista, Unesp, São João da Boa Vista - SP.
Vanessa Beatriz Martão [2]
Câmpus Experimental de São João da Boa Vista, Unesp, São João da Boa Vista - SP.

Resumo Neste trabalho iremos apresentar estratégias de codificação de canal utilizando códigos polares com o objetivo de aplicá-los no sistema 5G. Para esta estratégia de codificação é utilizada a polarização de canal para um canal discreto e sem memória, onde parâmetros como a capacidade do canal e o limitante de Bhattacharyya podem ser calculados. Dessa forma, a codificação dos códigos polares utilizando o produto de Kronecker de matrizes será apresentada e será mostrado que estes códigos atingem a capacidade do canal para serem utilizados em redes 5G.

1 Resultados

A partir de 2020 acredita-se que começará a ser implementado o sistema de comunicação sem fio de quinta geração (5G) [1], esse sistema trará grandes desafios para os serviços de comunicações, pois por meio dele haverá um crescimento exponencial de dados devido as novas aplicações e ao aumento substancial de dispositivos que ocorrerá a partir da implementação da Internet das Coisas (IoT, Internet of things).

O 5G demanda de diversos fatores para sua implementação, como taxas de transmissão 1000x mais altas do que as taxas de sistemas 4G, uma maior confiabilidade e cobertura no canal de comunicação, diminuir substancialmente a latência na transmissão do sinal e também aumentar a eficiência energética desses dispositivos, entre outros [2]. As novas taxas propostas são de 10Gbps em baixa mobilidade e 100Mbps para as demais, com raio de cobertura de até 50Km para cenários menos densos, com baixo retardo, entre 1ms a 10ms. Para que seja possível alcançar esses objetivos, essa comunicação necessita de um tipo de codificação de canal no qual supra a todos esses requisitos.

Os códigos polares, introduzidos por E. Arikan em 2009 [3], são códigos de bloco lineares baseados no conceito de polarização de canal, onde um canal W é transformado em dois tipos de canais sintetizados, mas com diferentes confiabilidades: o bom (W+) e o ruim (W-). Ao aplicar continuamente a polarizacão sobre os canais sintetizados, grande parte dos canais resultantes tende a dois extremos: os canais ruidosos e os canais quase-livres de ruídos. Portanto, a estratégia é transmitir os bits de informação sobre os canais sem ruído e fixar em zero os bits sobre os canais ruidosos, chamados bits congelados.

Os códigos polares possuem codificadores baseados em simples mapeamentos lineares, [3]. Para uma palavra código de tamanho $N = 2^n, n \geq 1$, definimos $F_N = F^{\otimes n}$, onde $F^{\otimes n}$ é o

[1] cintya.benedito@sjbv.unesp.br. Agradecimentos a Fapesp - Processo 2013/25977-7.
[2] nessa.bia.martao@hotmail.com

n-ésimo produto de Kronecker para a matriz $F = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. A codificação dos códigos polares é feita utilizando a matriz geradora $G_N = B_N \times F_N$, onde B_N é uma matriz de permutação que guarda a seguência de combinação da construção do canal.

Nosso objetivo é apresentar esta codificação relacionando-a com a polarização de canal apresentada em [3], além de calcular parâmetros relacionados com esta codificação como a capacidade do canal, mostrando que esta é alcançada para ser utilizada em redes 5G, o parâmetro de Bhattacharyya utilizado para verificar a confiabilidade da codificação e a probabilidade de erro.

Referências

[1] M. Shafi, A. F. Molisch, P. J. Smith. *"5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment and Practice"*. IEEE journals on Selected Areas in Commun., Vol. PP, no. 99, April 2017.

[2] Z. Dong. *"Up in the air with 5G"*. Communicate. Huawei Technologies Think Tech. Issue 80, (10) 2016.

[3] E. Arikan. *"Channel polarization: A method for constructing capacity achieving codes for symmetric binary input memoryless channels,"*. IEEE Trans. Inform. Theory, vol. 55, pp. 3051-3073, July 2009.

Modulação codificada 8-QAM via o reticulado D_2

Miller Acosta Osorio [1]
Departamento de Engenharia Elétrica - Unesp Ilha Solteira - SP.
Edson Donizete de Carvalho [2]
Departamento de Matemática - Unesp, Ilha Solteira - SP.
Jozué Vieira Filho [3]
Câmpus Experimental de São João da Boa Vista, Unesp, São João da Boa Vista - SP.

Resumo. Os sistemas de comunicações sem fio têm evoluído de forma extraordinária nos últimos anos. O crescimento nas aplicações, desde que requeira de espectro de frequência limitado, necessita de sistemas que integrem voz e dados em modernos links de comunicação digital de forma eficiente. Os problemas de ruído e multipercuso continuam sendo os que mais limitam a capacidade destes sistemas. Neste sentido, sistemas eficientes de codificação de canal continuam sendo estudados e são, de fato, um dos principais mecanismos que podem melhorar tal eficiência. Esquemas de modulação codificada tem sido propostos na literatura via reticulados [1], [2], [4]. Neste trabalho abordaremos a técnica de modulação codificada por blocos (BCM) de comprimento N para a transmissão de dados através de uma constelação de sinais de 8-PSK obtida via partição do reticulado D_2 para 8 pontos com mesmo esquema BCM. Cada símbolo da sequência codificada corresponde a um ponto da constelação bi-dimensional D_2 de 8 pontos .

1 Resultados básicos

Neste trabalho, apresentamos um estudo da técnica de modulação codificada por blocos (BCM) de comprimento N para a transmissão de dados mediante uma constelação de sinal de 8-PSK apresentada em [3] e se focou na construção de uma constelação de sinais via partição de reticulado bi-dimensionais com 8 pontos que permita a construção de sequências de símbolos codificadas equivalentes a códigos $2N$-dimensionais para canais limitados en largura de banda.

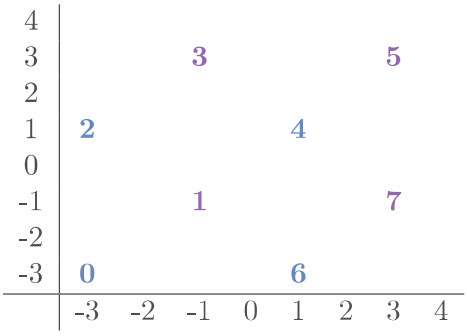
A codificação consiste de m codificadores $E_l, \cdots, E_m$, para códigos de correção de erro binários $C_l, \cdots, C_m$, com taxa $R_1, \cdots, R_m$, respectivamente. Se C_i é um bloco de cumprimento N e k_i bits de informação, a R_i é k_i/n_i. A sequencia de informação previamente é particionada dentro de m componentes de sequencias de informação a taxa R_m. $s_i^{(t)}$ denota a saída (símbolos binários) dos codificadores E_i no tempo t. O símbolo de canal a transmitir no tempo t é o resultado da combinação de $s_1^{(t)}, \cdots, s_m^{(t)}$ como descrito na Equacão 1 e que corresponde a uns dos 2^m símbolos da constelação de sinais do esquema de modulação multinível utilizado.

$$s(t) = \sum_{i=1}^{m} s_i^t \cdot 2^{i-1}. \tag{1}$$

[1] e-mail macosta13@gmail.com.
[2] edson@mat.feis.unesp.br. Agradecimentos a Fapesp - Processo 2013/25977-7.
[3] jozue.vieira@sjbv.unesp.br.

2 Construção

Utilizando a estrutura de codificadores binário de repetição $(8, 1, 8)$, de paridade $(8, 7, 2)$ e universal $(8, 8, 1)$ construiremos uma constelação reticulada, onde o mapeamento é realizado por meio da cadeia de partições dada por $\mathbb{Z}^2/D_2/2\mathbb{Z}^2/2D_2/4\mathbb{Z}^2/\cdots$, e representada por uma constelação de energia media zero.



Assim, para transmitir uma sequencia binaria de 16 bits como [0100011011010101] é realizada através de três blocos de 1 bits, 7 bits e 8 bits e codificadas como $E_1 = [\mathbf{0}000000]$, $E_2 = [\mathbf{1\ 0\ 0\ 0\ 1\ 1\ 0}1]$ e $E_3 = [\mathbf{1\ 1\ 0\ 1\ 0\ 1\ 0\ 1}]$, respectivamente. A sequencia codificada é $s = [64042606]$ que corresponde ao ponto $p = [-1 - 311 - 3 - 311 - 311 - 3 - 3 - 31 - 3]$ em o reticulado D_2^8.

Referências

[1] H. Imai, S. Hirakawa, *A new multilevel coding method using error-correcting codes*, *IEEE Transactions on Information Theory*, 23(3) (1977) 371-377.

[2] E.L. Cusack, *Error control codes for QAM signalling*, *Electronics Letters*, 20(2) (1984) 62-63.

[3] S.I. Sayegh, *A Class of Optimum Block Codes in Signal Space*, *Communications, IEEE Transactions on*, 34(10) (1986) 1043-1045.

[4] G. D. Forney, *Coset codes. I. Introduction and geometrical classification*, *IEEE Transactions on Information Theory*, 34(5) (1988) 1123-1151.

Algoritmo heurístico para obtenção de elemento totalmente positivo em corpos totalmente reais.

João Eloir Strapasson [1]
Faculdade de Ciências Aplicadas, Unicamp, Limeira - SP.

Resumo. Neste trabalho, apresentamos o pseudo código de um algoritmo heurístico que visa encontrar, se possível, um elemento totalmente positivo associado ao mergulho torcido de corpos totalmente reais.

1 Introdução

Considere um número natural M, da forma $M = 2^r p_1 p_2 \cdots p_k$, em que p_i's são números primos ímpares e distintos, considere o corpo totalmente

$$\mathbb{K} = \mathbb{Q}\left(\zeta_M + \zeta_M^{-1}\right),$$

em que ζ_M é a M-ésima raiz primitiva da unidade. O mergulho torcido induz no anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ uma métrica dada pela forma bilinear:

$$\langle x, y\rangle = \mathrm{Tr}(xy\alpha)$$

em que α é um elemento totalmente positivo (positivo para cada mergulho canônico).

2 Resultados

A obtenção do elemento totalmente positivo requer duas etapas fundamentais:

- A primeira é a obtenção de um elemento β que possui a mesmo norma produto do elemento α e assim α, se existir, será obtido pela multiplicação do elemento β por alguma unidade;
- A segunda etapa, a mais complexa, requer a geração de unidades. A complexidade está associado ao fato de que a quantidade de unidades crescem exponencialmente com a dimensão, pois as unidades formam um grupo multiplicativo gerado por $n-1$ unidades fundamentais.

As unidades fundamentais em geral não são conhecidas e portanto não existe fórmula fechada para a geração ou obtenção de unidades, sendo assim faz-se necessário um mecanismo eficiente e controlado para geração de um número razoável de unidades. Portanto para segunda etapa

[1] strapass@unicamp.br. Agradecimentos a Fapesp - Processo 2013/25977-7.

sugerimos a utilização de técnicas heurísticas para a geração de um conjunto grande de unidades, uma possibilidade para isso é usar as unidades ciclotômicas ou busca aleatória de unidades.

O Algoritmo a seguir proposto tem obtido sucesso em baixas dimensões e nos casos positivos a resposta é obtida em poucos minutos.

Algoritmo 1: Método heurístico para obtenção de elemento algébrico totalmente positivo.

Entrada: Um número natural M; Número máximo de iterações C;
Saída: Um elemento totalmente positivo "α" ou mensagem "elemento não encontrado".

inicio

1. Obtenha o discriminante de corpo $\mathbb{K}$ e sua fatoração;
2. Obtenha o polinômio minimal;
3. Defina os elementos de $\mathcal{O}_{\mathbb{K}}$ (e_i) e os mergulhos canônicos;
4. Defina funções "sinal" e "norma produto" de elementos de $\mathcal{O}_{\mathbb{K}}$;
5. Encontre um conjunto grande de unidades;
6. Construa uma matriz, U, em que cada linha representa o sinal de alguma unidade gerada;
7. Obtenha, para cada i, os elementos geradores de cada ideal $\prod_l \langle p_{i,l}(e_1), p_i \rangle$ ($p_{i,l}$ é l-ésimo elemento da fatoração do polinômio minimal módulo i-ésimo primo ímpar divisor de M (p_i);
8. Selecione os elementos dos ideais anteriores de forma a satisfazerem a norma produto desejada;
9. Multiplique os elementos anteriores de forma a obter candidatos como a norma produto desejada;
10. Construa uma matriz, A, em que cada linha representa o sinal dos elementos anteriores;

enquanto $u > 0$ **faça**

a. Use algum mecanismo de busca para encontrar linhas iguais entre as matrizes U e A;
b. Se a etapa anterior for positiva, identifique os elementos que geram as respectivas linhas iguais de U e A, multiplique os elementos de forma a obter o elemento α e faça $C = -1$;
c. Caso contrário faça $C = C - 1$ e atualize a matriz A multiplicado cada linha pelo sinal de uma unidade escolhida da maneira aleatória;

se $C=0$ **então**

imprima a mensagem "elemento não encontrado";

senão

imprima α;

Referências

[1] J. C. Interlando, T. P. N. Neto, T. M. Rodrigues, J. O. D. Lopes, A note on the integral trace form in cyclotomic fields, *Journal of Algebra and Its Applications* 14, 2015, 1550045.

[2] J. E. Strapasson, A. J. Ferrari, G. C. Jorge, S. I. R. Costa, Algebraic constructions of rotated unimodular lattices and direct sum of Barnes-Wall lattices (*submetido*).