Minissimpósio
Códigos e reticulados algébricos

Coordenador: Antonio Aparecido de Andrade

1 Introdução

O CNMAC é um excelente evento da SBMAC, onde congrega um grande número de participantes, entre pesquisadores, professores, profissionais de empresas e centros de pesquisas e estudantes das mais diversas áreas da Matemática e da Matemática Aplicada e Computacional. Constitui-se em uma oportunidade ímpar para discutir trabalhos em andamento, divulgar resultados e ficar a par da produção científica em desenvolvimento nas principais instituições nacionais, que acontece desde 1978. No CNMAC são apresentados minicursos, minissimpósios, conferências, sessões técnicas de comunicações, sessões especiais dedicadas à iniciação científica e ao ensino, exposições e mesas redondas. Também durante o CNMAC são premiados trabalhos de iniciação científica, dissertações de mestrado e teses de doutorado. O CNMAC tem como objetivo reunir a comunidade científica de Matemática Aplicada e Computacional, criando um fórum para o intercâmbio de idéias e surgimento de parcerias entre os participantes, assim como incentivando e inspirando a platéia de estudantes que comparecem ao evento. No ano de 2022 o Imecc - Unicamp, Campinas - SP, está empenhada em sediar o XLI CNMAC, que será realizada no período de 26 à 30 de setembro.

Em 2003, nesta linha, foi organizado o primeiro minissimpósio intitulado *Empacotamento de esferas e códigos lineares* dentro do XXVI CNMAC realizado no período de 08 a 11 de setembro no Ibilce - Unesp - São José do Rio Preto - SP. Em 2004, foi organizado o segundo minissimpósio intitulado *Códigos e reticulados*, dentro do XXVII CNMAC que foi realizado no período de 13 a 16 de setembro na PUC - Porto Alegre - RS, que teve como o objetivo de divulgar algumas técnicas utilizadas no estudo de códigos e reticulados, sobre anéis e corpos, enfocando o estudo de empacotamento de esferas em espaços euclidianos e hiperbólicos. Depois de uma pausa, em 2016 organizamos um minissimpósio intitulado

Códigos e reticulados algébricos dentro da programação do XXXVII CNMAC que foi realizado em Gramado - RS no período de 05 a 09 de setembro. Em 2017, organizamos um minissimpósio intitulado *Código e reticulados algébricos* dentro da programação do XXVII CNMAC que foi realizado no Instituto de Ciência e Tecnologia da Universidade Federal de São Paulo, Campus de São José dos Campos - SP, no período de 19 a 22 de setembro. Em 2018, organizamos um minissimpósio intitulado *Construções de códigos e reticulados algébricos* dentro do XXXVIII CNMAC com o objetivo de divulgar novas técnicas utilizadas no estudo da construção de reticulados algébricos obtidos via corpos de números, enfocando o estudo do empacotamento de esferas em espaços euclidianos e hiperbólicos. No ano de 2019 o Instituto de Matemática da Universidade Federal de Uberlândia sediou o XXIX CNMAC, realizado no período de 16 a 20 de setembro, onde organizamos o minissimpósio códigos e reticulados algébricos. No ano de 2020/21 o primeiro CNMAC on line, XL CNMAC, foi realizado e organizado pala Universidade Federal de Campo Grande, Campo Grande - MS, no período de 13 à 17 de setembro de 2021, onde organizamos o Minissimpósio Códigos e reticulados algébricos. Em 2022 dentro do XLI CNMAC, no período de 26 à 30 de setembro, realizado no Imecc - Unicamp, Campinas - SP, organizamos o mini-simpósio Códigos e reticulados algébricos. Novamente, em 2023, estamos empenhados em organizar um minissimpósio intitulado *Códigos e reticulados algébricos* dentro do XLII CNMAC, que será realizado no período de 18 à 22 de setembro, que será realizado em Bonito - MS, com o objetivo de divulgar novas técnicas utilizadas no estudo da construção de reticulados algébricos obtidos via corpos de números, enfocando o estudo do empacotamento de esferas em espaços euclidianos e hiperbólicos. Neste minissimpósio veremos, também, diferentes métodos de pesquisar os melhores reticulados, visando sempre determinar aqueles de maior densidade de centro, através das técnicas geométricas e também das técnicas algébricas.

2 Programa

1. Prof. Dr. Antonio Aparecido de Andrade.
   Título: Corpos de números puros e aplicações.
   Filiação: Departamento de Matemática, Ibilce - Unesp, São José do Rio Preto - SP.

2. Prof. Dr. Robson Ricardo de Araujo

   Título: Reticulados bem arredondados em dimensão prima ímpar via o mergulho canônico.

   Filiação: Instituto Federal de Educação de São Paulo (IFSP), Catanduva - SP.

3. Profa. Dra. Carina Alves.

   Título: Reticulados circulantes.

   Filiação: Departamento de Matemática, Igce - Unesp, Rio Claro - SP.

4. Profa. Dra. Grasiele Cristiane Jorge.

   Título: Sobre a não existência de códigos lineares perfeitos na métrica l_p para alguns parâmetros.

   Filiação: Instituto de Ciência e Tecnologia - Unifesp, São José dos Campos - SP.

5. Profa. Dra. Cintya Wink de Oliveira Benedito.

   Título: Rotulameneto dos pontos das constelações de sinais $mPolSK - 8PSK$ via Álgebra dos Quatérnios e Partições.

   Filiação: Campus Experimental de São João da Boa Vista (SP) - Unesp, São João da Boa Vista - SP.

6. Prof. Dr. Edson Donizete de Carvalho

   Título: Códigos quocientes provenientes de grupos solúveis.

   Filiação: Departamento de Matemática, Feis - Unesp, Ilha Solteira - SP.

7. Prof. Dr. João Eloir Strapasson.

   Título: Reticulados algébricos construídos via torções por unidades.

   Filiação: Faculdade de Ciências Agronômicas, Unicamp, Limeria - SP.

8. Prof. Dr. Antonio Aparecido de Andrade.

   Título: Trace form via the twisted homomorphism.

   Filiação: Departamento de Matemática, Ibilce - Unesp, São José do Rio Preto - SP.

3 Resumos das palestras

Corpos de números puros e aplicações

Antonio Aparecido de Andrade [1]
Departamento de Matemática, Ibilce, Unesp
São José do Rio Preto - SP

1 Introdução

Um problema clássico na matemá¡tica é o de obter um empacotamento de esferas de mesmo raio em $\mathbb{R}^n$ de tal modo que as esferas ocupem o maior espaço possível ou, equivalentemente, que a densidade deste empacotamento seja máxima. Isto pode ser visto como uma versão do 18^o problema de Hilbert, proposto em 1900 no Congresso Internacional de Matemá¡tica em Paris. Dentre os empacotamentos esféricos, o empacotamento reticulado, que é um tipo de empacotamento onde o conjunto formado pelos centros das esferas formam um conjunto discreto no $\mathbb{R}^n$, chamado de reticulado. Um dos parâmetros matemáticos que medem a densidade do empacotamento é a densidade de centro, definida como a razão entre o raio e o volume das esferas. Para os espaços $\mathbb{R}^n$ de dimensões 2 a 8 e 24 são conhecidos empacotamentos reticulados com densidade de centro máxima. Reticulados com alta densidade de centro possuem aplicações na teoria da informação.

Seja $\mathbb{K}$ um corpo de números de grau n. Assim existem n $\mathbb{Q}$-monomorfismos $\sigma_1, \sigma_2, \ldots, \sigma_n$ de $\mathbb{K}$ em $\mathbb{C}$. Podemos reordenar tais monomofismos de tal forma que $\sigma_1, \ldots, \sigma_{r_1}$ sejam reais e que os monomorfismos não reais satisfaçam $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $j = 1, \ldots, r_2$, onde $n = r_1 + 2r_2$. Defina a função $\sigma : \mathbb{K} \to \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2} = \mathbb{R}^n$ por

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

A função σ é um homomorfismo injetivo de anéis de $\mathbb{K}$ em $\mathbb{R}^n$, chamado de homomorfismo canônico (ou homomorfismo de Minkowski). Se M é um $\mathbb{Z}$-módulo de $\mathbb{K}$, então $\sigma(M)$ é um reticulado em $\mathbb{R}^n$. Tais reticulados são chamados de reticulados algébricos e possuem o diferencial de poder usar resultados da teoria algébrica dos números para analisar as suas propriedades. Além disso, diversos trabalhos mostram a existência de reticulados algébricos com densidade de centro ótima.

2 Resultados

Uma extensão finita dos racionais, $\mathbb{Q} \subseteq \mathbb{K}$ é chamado um corpo de números. Neste trabalho, exploramos alguns corpos de números, chamados corpos puros, onde diferentemente dos corpos quadráticos e ciclotômicos, não é simples de identificar o seu anel de inteiros Por isso, chamamos

[1] antonio.andrade@unesp.br. Agradecimentos a Fapesp, Proc. 2013/25977-7 e 2022/02303-0

a atenção para os corpos onde o elemento primitivo tem como polinômio minimal $p(x) = x^n - d$, com d um inteiro livre de cubos.

Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[n]{d}$, com $d \in \mathbb{Z}$ livre de potências n-ésimas e $n \in \mathbb{N}$, e $\mathcal{O}_{\mathbb{K}}$ o seu anel de inteiros algébricos de $\mathbb{K}$.

1. Se d é livre de quadrados, então $\theta\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = d\mathbb{Z}$.

2. Se $d \in \mathbb{Z}$ é livre de quadrados, então

$$\mathcal{T}r(\theta^k) = \begin{cases} 0, \text{ se } k = 1, 2, \ldots, n-1, \\ nd^s, \text{ se } k = ns, \text{ com } s \in \mathbb{N}, \\ 0, \text{ se } k > n \text{ e } k \not\equiv 0 (mod\ n). \end{cases}$$

3. Se $n = 3$ e $d \in \mathbb{Z}$ é livre de quadrados, então

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2, \text{ se } d \not\equiv \pm 1 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2-2\theta+\theta^2}{3}\right), \text{ se } d \equiv 1 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2-\theta+\theta^2}{3}\right), \text{ se } d \equiv -1 (mod\ 9). \end{cases}$$

4. Se $n = 3$ e d não é livre de quadrados e livre de cubos, ou seja, com $d = m^2 n$, onde m e n são livres de quadrados e $mdc(m, n) = 1$, então

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\frac{\theta^2}{m}) & \text{se} \quad d \not\equiv \pm 1 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\frac{\theta^2 + m\theta + m}{3m}) & \text{se} \quad d \equiv 1 (mod\ 9) \text{ e } m \equiv 1, -2 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\frac{\theta^2 + 2m\theta + 2m}{3m}) & \text{se} \quad d \equiv 1 (mod\ 9) \text{ e } m \not\equiv 1, -2 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\frac{\theta^2 + 2m\theta + m}{3m}) & \text{se} \quad d \equiv -1 (mod\ 9) \text{ e } m \equiv 1, -2 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\frac{\theta^2 + m\theta + 2m}{3m}) & \text{se} \quad d \equiv -1 (mod\ 9) \text{ e } m \not\equiv 1, -2 (mod\ 9). \end{cases}$$

Referências

[1] L. S. Facini, *Uma introdução aos corpos não abelianos de grau menor ou igual a 6*, Dissertação de Mestrado, Ibilce - Unesp, São José do Rio Preto - SP, 2021.

[2] D. A. Marcus, *Number fields*. Springer-Verlag, New York, 1977.

Reticulados bem arredondados em dimensão prima ímpar via o mergulho canônico

Robson Ricardo de Araujo [1]
Instituto Federal de São Paulo, Catanduva - SP.

1 Introdução

Reticulados bem arredondados são aqueles de posto máximo em $\mathbb{R}^n$ que possuem um conjunto com n vetores linearmente independentes de normas coincidentes à norma mínima do reticulado. Recentemente algumas vantagens para codificação e criptografia têm sido apontadas sobre a utilização desses reticulados, tais como seu uso para transmissão de sinais em canais *SISO do tipo Rayleigh com desvanecimento* e em canais *wiretap MIMO* [4, 5].

Uma maneira bem considerada nas últimas décadas para obtenção de reticulados é via mergulhos algébricos de $\mathbb{Z}$-módulos (em particular, ideais) de anéis de inteiros de corpos de números para o espaço euclidiano. Reticulados obtidos dessa maneira costumam ser chamados de reticulados algébricos. Em [3] os autores analisam determinadas situações em que reticulados algébricos são ou não bem arredondados. Destacadamente, sendo σ o mergulho canônico e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de um corpo de números, prova-se nesse artigo que $\sigma(\mathcal{O}_{\mathbb{K}})$ é bem arredondado se, e somente se, $\mathbb{K}$ é um corpo ciclotômico. Neste trabalho apresentamos uma iniciativa de expansão desses resultados, provando que é possível obter reticulados bem arredondados através de determinada família de $\mathbb{Z}$-módulos de anéis de inteiros de corpos de números abelianos de grau primo p ímpar via o mergulho canônico, mesmo que esses corpos não sejam abelianos [2]. Ao final apontaremos alguns caminhos para pesquisa futura e problemas em aberto relacionados a este assunto.

2 Resultados

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 a sua simetria e as suas inúmeras propriedades geométricas e algébricas. Um problema muito comum na área consiste em produzir reticulados com alta densidade (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.

[1] robson.ricardo@ifsp.edu.br.
Agradecimentos a Fapesp, Proc. 2021/11311-3 e Proc. 2013/25977-7.

Recentemente, reticulados chamados *bem arredondados* têm ganhado destaque por apresentarem vantagens em canais SISO do tipo Rayleigh com desvanecimento e em canais MIMO Wiretap. Os reticulados bem arredondados são aqueles completos em $\mathbb{R}^n$ que possuem um conjunto com n vetores linearmente independentes cuja norma coincide com a norma mínima do reticulado. Se eles geram o reticulado, dizemos que o reticulado é fortemente bem arredondado.

Classicamente sabe-se também 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. Precisamente, 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

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

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 $\mathbb{R}^n$. Em [3] são apresentados resultados envolvendo reticulados algébricos obtidos pelo mergulho canônico que tenham a propriedade de serem bem arredondados. Um deles menciona a existência de infinitos corpos de números cuja realização geométrica através do mergulho canônico seja um reticulado bem arredondado. Outro dá condições para que um reticulado completo em $\mathbb{R}^2$ seja bem arredondado e para ser equivalente ao reticulado hexagonal. No entanto, destacamos o teorema que diz que, sendo $\mathcal{O}_\mathbb{K}$ o anel de inteiros de um corpo de números $\mathbb{K}$, o reticulado $\sigma(\mathcal{O}_\mathbb{K})$ é bem arredondado se, e somente se, $\mathbb{K}$ é um corpo ciclotômico.

Seja $\mathbb{K}$ um corpo de números abeliano de grau primo ímpar p de modo que seu condutor não seja divisível por p (ou seja, $\mathbb{K}$ é não-ramificado). Mostraremos, construtivamente, uma maneira de obter uma infinidade de $\mathbb{Z}$-módulos M tais que $\sigma(M)$ são bem-arredondados. Com isso, em particular observamos ser possível obter sub-reticulados bem arredondados de $\sigma(\mathcal{O}_\mathbb{K})$, mesmo que este último não seja bem arredondado [2]. Neste trabalho, apresentaremos precisamente os resultados mencionados anteriormente, faremos discussões sobre a geração de reticulados bem arredondados via corpos de números e apontaremos alguns problemas em aberto.

Referências

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

[2] de Araujo, R.R., Costa, S.I.R. *Well-rounded algebraic lattices in odd prime dimension.* Arch. Math. 112, pp. 138-148, 2019.

[3] Fukshansky, L., Petersen, K. *On well-rounded ideal lattices.* Int. J. Number Theory, vol. 8, no. 1, pp. 189-206, 2012.

[4] Gnilke, O.W., Tran, H.T.N., Karilla, A., Hollanti, C. *Well-Rounded Lattices for Reliability and Security in Rayleigh Fading SISO Channels.* IEEE Information Theory Workshop (ITW), 2016, p. 359-363.

[5] Gnilke, O.W., Barreal, A., Karrila, A., Tran, H.T.N., Karpuk, D., Hollanti, C. *Well-Rounded Lattices for Coset Coding in MIMO Wiretap Channels.* Accepted to IEEE Int. Telecommunication Newtworks and Applications Conf. (ITNAC). Dunedin, New Zeland, Dec. 2016.

Reticulados circulantes

Carina Alves [1]
João Gabriel Oliveira de Jesus [2]
William Lima da Silva Pinto [3]
Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de Rio Claro

1 Introdução

Reticulados circulantes são aqueles que admitem uma matriz circulante como matriz geradora, isto é, que admitem como base um vetor real e suas $n-1$ rotações uma coordenada à direita. Neste trabalho será feito um estudo sobre reticulados circulantes, em particular, investigamos condições para que a expressão da norma de um vetor arbitrário de um reticulado circulante seja substancialmente simplificada.

2 Resultados

Seja $n \geq 2$ e defina o operador

$$\mathrm{rot} : \mathbb{R}^n \to \mathbb{R}^n$$

por $\mathrm{rot}(x_1, x_2, \cdots, x_{n-1}, x_n) = (x_n, x_1, x_2, \cdots, x_{n-1})$.

Dizemos que um reticulado $\Lambda_{\mathbf{u}} \subset \mathbb{R}^n$ é *circulante* se ele admite uma base da forma

$$\{\mathbf{u}, \mathrm{rot}(\mathbf{u}), \cdots, \mathrm{rot}^{n-1}(\mathbf{u})\}$$

para algum $\mathbf{u} = (\rho_1, \rho_2, \cdots, \rho_n) \in \mathbb{R}^n$. O vetor $\mathbf{u}$ determina uma matriz circulante $G_{\mathbf{u}}$ da forma

$$G_{\mathbf{u}} = \begin{pmatrix} \rho_1 & \rho_2 & \cdots & \rho_n \\ \rho_n & \rho_1 & \cdots & \rho_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_2 & \rho_3 & \cdots & \rho_1 \end{pmatrix}.$$

A caracterização de reticulados através de matrizes geradoras circulantes tem algumas consequências relevantes, como o cálculo facilitado do determinante, e consequentemente da densidade de centro.

O reticulado A_n, por exemplo, admite uma matriz geradora circulante. Uma classe de reticulados que são preservados pelo operador de rotação para entradas inteiras, foram abordados em [3].

[1] e-mail: carina.alves@unesp.br. Agradecimentos à FAPESP, Proc. 2019/20800-8 e 2013/25977-7.
[2] email: jg.jesus@unesp.br
[3] email: william.lima@unesp.br

Reticulados gerados via polinômios possuem matrizes circulantes e foram propostos até a dimensão 3 em [2]. O método enfrenta um problema a partir da dimensão 4, a qual foi explorada em [1], que é o fato de que não se consegue de maneira geral a norma de um vetor arbitrário do reticulado em função dos coeficientes do polinômio. A solução para isso pode ser, por exemplo, restringir os coeficientes do polinômio, e consequentemente suas raízes, a uma condição. Isso torna possível generalizar a construção de reticulados através de polinômios.

Neste trabalho veremos que simplificando a norma de um vetor arbitrário de um reticulado circulante determinado por $\mathbf{u}$, podemos construir alguns reticulados tão densos quanto classes conhecidas, como D_n e A_n. Encontrar empacotamentos esféricos densos no espaço euclidiano equivale a encontrar bons códigos. Códigos que tem sido amplamente utilizados são os códigos espaço-tempo, devido a sua facilidade de codificação e decodificação [4].

Referências

[1] C. Alves, W. L. S. Pinto, A. A. Andrade, *Well-rounded lattices via polynomials with real roots.* International Journal of Applied Mathematics, v. 33, n. 4, p. 663-672, 2020.

[2] A.L. Flores, J. C. Interlando, J. V. L. Nunes, *Optimal families of two and three-dimensional lattice packings from polynomials with integer coefficients.* JP Journal of Algebra, Number Theory and Applications, v. 15, n. 1, p. 45-51, 2009.

[3] L. Fukshansky and X. Sun, *On the geometry of cyclic lattices.* Discrete Comput. Geom, v. 52, p. 240-259, 2014.

[4] G. Wang, J.K. Zhang and M. Amin, *Space-time block code designs based on quadratic field extension for two-transmitter antennas.* IEEE Transaction on Information Theory, v. 58(6), p. 4005-4013, 2012.

Sobre a não existência de códigos lineares perfeitos na métrica ℓ_p para alguns parâmetros

Grasiele Cristiane Jorge e Lucas Eduardo Nogueira Gonçalves [1]
Departamento de Ciência e Tecnologia, Universidade Federal de São Paulo
São José dos Campos - SP

1 Introdução

Um reticulado $\Lambda \subset \mathbb{R}^n$ é um subgrupo aditivo e discreto de $\mathbb{R}^n$. Dado um reticulado $\Lambda \subset \mathbb{Z}^n$, dizemos que Λ é um código linear perfeito para uma dada métrica se existir um raio $r > 0$ (raio de empacotamento) de forma que ao traçarmos esferas com este raio ao redor de todos os elementos de Λ estas esferas não se intersectam em $\mathbb{Z}^n$ e a união delas resulta em $\mathbb{Z}^n$.

Em [2], Golomb e Welch consideraram a métrica da soma e apresentaram famílias de códigos lineares perfeitos para alguns parâmetros: dimensão 2 com qualquer raio natural e qualquer dimensão com raio igual a 1. Eles conjecturaram que na métrica da soma não existem códigos lineares perfeitos em $\mathbb{Z}^n$ para $n \geq 3$ e $r \geq 2$. Embora a conjectura já tenha sido abordada de várias formas, nenhuma delas resultou na demonstração do caso geral e até o momento ela permanece em aberto.

2 Resultados

Pelo fato de existirem pouquíssimos códigos lineares perfeitos em $\mathbb{Z}^n$ na métrica da soma e pela métrica euclidiana ser muito utilizada em aplicações práticas, em [1] foram considerados códigos lineares perfeitos em $\mathbb{Z}^n$ na métrica ℓ_p, $1 < p < \infty$. A métrica ℓ_p é definida para $x, y \in \mathbb{R}^n$ e $p \geq 1$ como

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

Para $p = 1$, ℓ_1 é a métrica da soma e para $p = 2$, ℓ_2 é a métrica euclidiana. Em [1] foi encontrado um limitante para o raio de empacotamento máximo atingível para um código linear perfeito em $\mathbb{Z}^n$ e com o auxílio de um algoritmo computacional foi feita uma busca nas dimensões 2 e 3 considerando a métrica euclidiana (ℓ_2). Foi mostrado que, para a métrica euclidiana, só existem códigos lineares perfeitos em $\mathbb{Z}^2$ para raios 1, $\sqrt{2}$, 2 e $2\sqrt{2}$ e só existem códigos lineares perfeitos em $\mathbb{Z}^3$ para raios $1, \sqrt{3}$. Foi conjecturado que esses são os únicos parâmetros (dimensão e raio) para os quais existem códigos lineares perfeitos na métrica ℓ_2. Considerando $1 < p < \infty$, foi provado que para $n = 2$ e r inteiro não existem códigos perfeitos na métrica ℓ_p se $r > 2$.

[1] grasiele.jorge@unifesp.br. Agradecimentos à Fapesp, Proc. 2019/14390-1 e 2013/25977-7

Em [4] os autores obtiveram outros parâmetros para os quais não existem códigos lineares perfeitos na métrica ℓ_p. Considerando apenas a métrica da soma ($p = 1$), foi provado que se $n \equiv 12$ ou $21 \pmod{27}$ e o número de pontos de $\mathbb{Z}^n$ na bola de raio 3 é livre de quadrados, então não existe um código linear perfeito com raio 3. Mais ainda, se $n \equiv 3, 5, 21$ ou $23 \pmod{27}$, $n \geq 4$, e o número de pontos de $\mathbb{Z}^n$ na bola de raio 4 é livre de quadrados, então não existe um código linear perfeito com raio 4. Agora, considerando a métrica ℓ_p para $2 \leq p < \infty$, foi demonstrado que se $n \equiv 5$ ou $8 \pmod{9}$ e o número de pontos de $\mathbb{Z}^n$ na bola de raio $2^{1/p}$ é livre de quadrados, então não existe um código linear perfeito com raio $2^{1/p}$. Mais ainda, se $n \equiv 11, 12, 20$ ou $21 \pmod{27}$ e o número de pontos de $\mathbb{Z}^n$ na bola de raio $3^{1/p}$ é livre de quadrados, então não existe um código linear perfeito com raio $3^{1/p}$. Todas as demonstrações foram feitas de forma algébrica utilizando a técnica utilizada em [1] com auxílio computacional.

Nesta palestra apresentaremos alguns resultados sobre a classificação de códigos perfeitos na métrica ℓ_p considerando as técnicas utilizadas em [1] e [4].

Referências

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

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

[3] C. C. Lavor, M. M. S. Alves, R. M. Siqueira e S. I. R. Costa, Uma introdução à teoria de códigos, Notas em Matemática Aplicada, SBMAC, 2006.

[4] T. Zhang e G. Ge, Perfect and quasi-perfect codes under the ℓ_p metric, IEEE Transactions on Information Theory, 63(7), pp. 4325-4331, 2017.

Rotulamento dos Pontos das Constelações de Sinais mPolSK−8PSK via Álgebra dos Quatérnios e Partições QAM

Cintya Wink de Oliveira Benedito, Danyel Morais Doval e Ivan Aritz Aldaya Garde [1]
Faculdade de Engenharia, Unesp
São João da Boa Vista - SP

1 Introdução

Modulações de alta ordem vêm ganhando destaque através do uso de alguns formatos que utilizam a polarização da luz para transmitir dados e, além disso, podem ser otimizadas utilizando operações de rotação e translação dos símbolos das constelações definidas por politopos, [1, 2]. Dentre elas, o uso da técnica de modulação digital conhecida como modulação por chaveamento de polarização - PolSK (*Polarization-Shift Keying*) chama a atenção na área das comunicações ópticas, pelo fato de que o estado de polarização é o parâmetro mais estável de um feixe de laser durante a sua propagação na atmosfera.

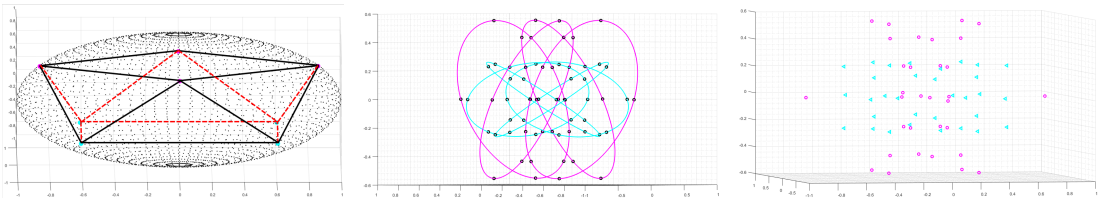
Neste contexto, este trabalho tem como objetivo inicial apresentar modulações em quatro dimensões utilizando os conceitos de códigos esféricos ótimos, álgebra dos quatérnios e fibração de Hopf. A partir da junção da modulação PolSK com a modulação PSK (*Phase-Shift Keying*), iremos construir a modulação mPolSK-nPSK, em que m é a quantidade de pontos tomados em uma esfera de Poincaré e n é a quantidade de amostras consideradas na modulação PSK. A importância de se considerar códigos esféricos ótimos na esfera de Poincaré está no fato de em transmissões de sinais ruidosos, os pontos espalhados pelo ruído terão menor probabilidade de serem associados ao ponto errado devido ao fato da distância mínima ser a maior possível entre os m pontos considerados, este é um diferencial deste trabalho aos demais conhecidos pelos autores na literatura. Além disso, utilizaremos os conceitos de fibração de Hopf para transformar as coordenadas de três dimensões para quatro dimensões e vice-versa. Por fim, iremos realizar o rotulamento das constelações de sinais mPolSK−8PSK para $m = \{4, 6, 8, 12, 16\}$, pelas modulações 4D. E, em seguida, através da relação entre a álgebra dos quatérnios e o espaço quadridimensional iremos obter as partições bidimensionais QAM das modulações.

2 Resultados

Consideremos constelações de sinais obtidas a partir das modulações mPolSK-8PSK para $m = \{4, 6, 8, 12, 16\}$. De modo a exemplificar as construções realizadas, apresentamos na Figura 1 a modulação 8PolSK-8PSK. Na Figura 1(a) temos a configuração ótima no S^2 para oito pontos, a qual é dada por um antiprisma quadrado. Aplicando o mapeamento inverso da fibração de Hopf nas coordenadas obtidas a partir do código esférico ótimo considerado e em seguida a

[1] cintya.benedito@unesp.br. Agradecimentos a Fapesp, Proc. 2020/03613-7 e 2013/25977-7

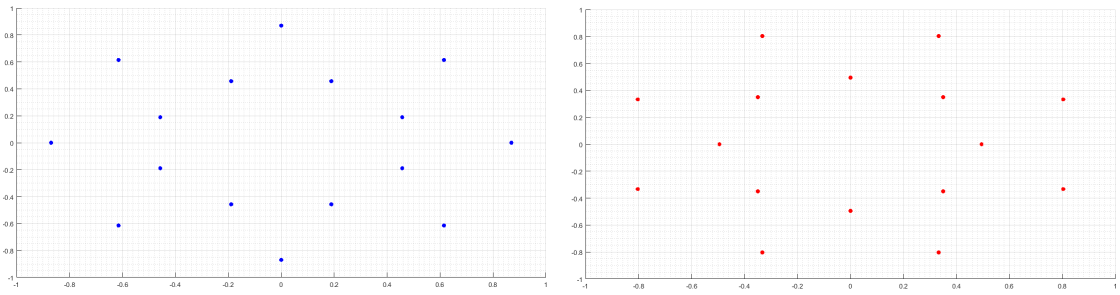
projeção estereográfica, obtemos os 8 círculos da esfera S^3 na esfera S^2 apresentado na Figura 1(b), de modo que em cada círculo é considerado 8 amostras da modulação PSK, gerando assim a modulação 8PolSK-8PSK. Por fim, excluindo os círculos, na Figura 1(c), temos a constelação de sinais ótima da modulação 8PolSK-8PSK, onde cada cor está associada ao respectivo ponto na esfera S^2 de acordo com a Figura 1(a).



(a) Código esférico ótimo 8pts (b) Modulação 8PolSK-8PSK (c) Constelação de sinais

Figura 1: Modulação 8PolSK-8PSK utilizando códigos esféricos ótimos.

Agora, iremos realizar o rotulamento das coordenadas $(x_1, x_2, x_3, x_4) \in \mathbb{R}^4$ dos $m \cdot 8$ símbolos das constelações de sinais via álgebra dos quatérnios, para todas as modulações em quatro dimensões com $m = \{4, 6, 8, 12, 16\}$ pontos. E, em seguida, representar os símbolos em partições bidimensionais QAM. Sabe-se que existe um isomorfismo entre a álgebra dos quatérnios e o espaço $\mathbb{R}^4$. Através dessa relação, no caso de $m = 8$ pontos, podemos escrever cada um dos 64 símbolos da constelação de sinais da modulação 8PolSK-8PSK, como um quatérnio na forma $x = x_1 + x_2 \cdot i + x_3 \cdot j + x_4 \cdot k$. Para construir os respectivos símbolos em partições QAM, utilizamos a representação de Cayley-Dickson obtendo dois conjuntos de coordenadas complexas na forma $z_1 = x_1 + x_2 \cdot i$ e $z_2 = x_3 + x_4 \cdot i$ para cada um dos 64 símbolos. Na Figura 2, representamos tais símbolos das partições QAM para a configuração ótima utilizando 8 pontos.



(a) $x_1 + i \cdot x_2$ (b) $x_3 + i \cdot x_4$

Figura 2: Partições QAM para 8 pontos ótimos.

Referências

[1] Rodrigues, F. A., Temporão, G. and Weid, J. P. Constructive methods for the design and labeling of four-dimensional modulations, *Journal of Communication and Information Systems*, volume 33, no. 1, pages 257-270, 2018. DOI: 10.14209/jcis.2018.26.

[2] Karlsson, M. Four-dimensional rotations in coherent optical communications, *Journal of Lightwave Technology*,v. 32, n. 6, p. 1246–1257, 2014.

Códigos quocientes provenientes de grupos solúveis

Edson Donizete de Carvalho [1]
Departamento de Matemática, Feis, Unesp - Ilha Solteira - SP

1 Introdução

A transmissão de informação em sistemas de comunicação está sujeito de forma frequente a ação do ruído que é tratada por meio de modelos probabilísticos. A componente chave na transmissão é o modulador que faz uso de constelações de sinais, isto é, conjuntos discretos finitos de pontos em um espaço métrico.

Em particular, conjuntos discretos de pontos de um espaço métrico podem serem caracterizados pela existência de simetrias internas que são de fundamental importância para a implementação prática de moduladores e demoduladores.

A técnica denominada na literatura de partição de Ungerboeck [1] despertou grande interesse na comunidade de Teoria de Informação e Códigos, onde foram propostos esquemas conhecidos por modulação codificada que combina a codificação e modulação em uma única etapa, o que garantiu uma maior proteção contra a ação do ruído em sistemas de transmissão digital e foram obtidos ganhos de codificação da ordem de $3-6$ dB, sem que houvesse a necessidade de sacrificar a taxa da informação ou mesmo no aumento da largura de banda. Esta técnica introduzida por Ungerboeck é conhecida por mapeamento de partição de conjuntos, foram feito uso das constelações de sinais 2^m-QAM e 2^m PSK, a modulação de sinais que foi gerada por sequências de sinais codificados, isto é, palavras códigos de um código quociente $\mathcal{C}$, que hoje conhecemos por códigos-reticulados.

Forney [2] propos uma maneira prática de codificação de bits de informação e de bits não codificados para um código quociente $\mathcal{C}$ a partir de constelações de sinais a partir de da técnica de partição de reticulados, obtidos por meio de cadeias de reticulados binários dados pela Equação (1).

$$\mathbb{Z}^{2m}/2\mathbb{Z}^{2m}/2^2\mathbb{Z}^{2m}/\cdots/2^n\mathbb{Z}^{2m} \tag{1}$$

2 Resultados

Mostraremos que a ténica proposta por Forney em [2] de construção de códigos quocientes binários $\mathcal{C}$ também podem serem expandida por meio de constelações de sinais 2^m-QAM proveniente do bitoro, isto é, uma superfície compacta de gênero $g = 2$ [3].

Neste sentido, consideraremos uma cadeia de subgrupos

$$\Lambda_1/\Lambda_2/\cdots/\Lambda_n \tag{2}$$

[1] edson.donizete@unesp.br. Agradecimentos a Fapesp, Proc. 2013/25977-7 e 2019/22368-6

onde, $|\Lambda_i/\Lambda_{i-1}| = 2$ para todo $i \in \{1, \ldots, n\}$.

Se Λ é um grupo que pertence a cadeia de subgrupos dadas pela Equação 2, temos que por conseguência de resultados da Teoria de Grupos que Λ/Λ_n tem ordem 2^k algum inteiro positivo k e Λ_1/Λ tem ordem 2^{n-k}. Temos, também que $\Lambda_1/\Lambda_n \simeq \mathbb{Z}_2^n$, isto é, Λ_1/Λ_n tem ordem 2^n.

Um código linear binário $\mathcal{C} = (n, k) \subset \mathbb{Z}_2^n$ é obtido através da seleção dos sinais a partir da cadeia de grupos descritas na Equação (2), ao se considerar um grupo Λ na cadeia, seleciona-se os k bits de informação através da seleção dos sinais nas classes laterais do grupo quociente Λ/Λ_n e os $(n-k)$ bits de redundância são tomados a partir da seleção dos sinais das classes laterias do grupo quociente Λ_1/Λ.

Em [3] foi mostrado que o grupo de telling G gerado pelas reflexões de um triângulo hiperbólico no bitoro de ângulos $(\frac{\pi}{l}, \frac{\pi}{m}, \frac{\pi}{n})$ que também é denotado por (l, m, n) é soluvel, isto é, sempre é possível extrair uma cadeia de subgrupos como descrito pela Equação (1).

Em particular, no bitoro quando $G = (2, 8, 8)$, $(4, 4, 4)$ ou $(2, 4, 8)$ [3] é possível extrair cadeias de grupos com $G = \Lambda_1$ como descritas na Equação (2), onde $G/\Lambda_n \simeq \mathbb{Z}_2^n$. Assim ao tomarmos a seleções dos sinais de forma conveniente a partir da cadeia de grupos como descrito na Equação (1), obtemos um código $\mathcal{C} \subset \mathbb{Z}_2^n$.

A Figura 1, ilustra um código $\mathcal{C} \subset \mathbb{Z}_2^4$, obtidos por meio da cadeia de grupos como descrito na Equação (2), ao se considerar o grupo $(G = (4, 4, 4)$.

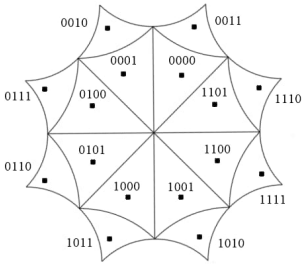


Figura 1:

Referências

[1] G. Ungerboeck, *Channel coding with multilevel/phase signals*, IEEE Trans. Inf. Theory, 28, 55 - 67, 1982

[2] G. D. Forney, *Coset Codes - Part I: Introduction and geometrical classification*, IEEE Trans. Inform. Theory, 34, 1123-1151, 1988.

[3] E. M. V. Gomes, E. D. Carvalho, C. A. R. Martins, W. S. Soares, Jr. and E. B. Silva, *Hyperbolic geometrically uniform codes and Ungerboeck partitioning on the double torus*, Symmetry. vol. 14 (3), 449, 2022.

Reticulados algébricos construídos via torções por unidades

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

1 Introdução

Considere um número natural M, da forma $M = 2^r q$, em que q é um número ímpar, considere o corpo real maximal

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

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). Quando tomamos $\alpha = 1$ temos o mergulho sem torção, também denominado mergulho canônico.

A obtenção do elemento totalmente positivo requer duas etapas fundamentais:

- A primeira é a obtenção de um elemento β que possua uma norma previamente desejada;
- A segunda etapa, a mais complexa, requer a busca de uma unidade u tal que $\alpha = u\,\beta$ seja um elemento totalmente positivo.

Observação 1.1. *A complexidade do problema 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.*

2 Resultados

Conjectura 2.1. *Para todo q um número ímpar composto e $r \geqslant r_0 = 1$, existe duas unidades totalmente positivas, a saber $2+e_1$ e $2-e_1$. O reticulado algébrico obtido pelo mergulho torcido por uma destas unidades é mais denso que o reticulado algébrico do mergulho canônico.*

Conjectura 2.2. *Para todo q um número primo ímpar e $r \geqslant r_0 = 2$, existe duas unidades totalmente positivas, a saber $2+e_1$ e $2-e_1$. O reticulado algébrico obtido pelo mergulho torcido de $\mathcal{O}_\mathbb{K}$ por uma destas unidades é mais denso que o reticulado algébrico do mergulho canônico $\mathcal{O}_\mathbb{K}$.*

[1] strapass@unicamp.br. Agradecimentos a Fapesp, Proc. 2013/25977-7 e 2020/09838-0

Mostraremos que estas conjecturas são válidas para valores pequenos de q e qualquer $r > r_0$. Estas conjecturas podem ser estendidas para mergulhos de ideais principais em $\mathcal{O}_{\mathbb{K}}$ ($\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$) Apresentaremos um estudo de caso considerando diversas dimensões.

Referências

[1] E. B. Fluckiger, Lattices and Number Fields, *Contemp. Math.* 241, 1999, 69-84.

[2] E. B. Fluckiger, F. Oggier, E. Viterbo, New Algebraic Constructions of Rotated $\mathbb{Z}^n$-Lattice Constellations for the Rayleigh Fading Channel, *IEEE Transactions on Information Theory* 50, 2004, 702-714.

[3] J. C. Interlando, J. O. D. Lopes, T. P. N. Neto, The discriminant of abelian number fields, *Journal of Algebra and Its Applications* 05, 2006, 35-41.

[4] 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.

[5] G. C. Jorge, A. A. Andrade, S. I. R. Costa, J. E. Strapasson Algebraic constructions of densest lattices, *Journal of Algebra* (Print), 429, 2015, 218-235.

[6] F. Oggier, Algebraic Methods for Channel Coding, Ph.D. thesis, SB, Lausanne (2005) doi: 10.5075/epfl-thesis-3182.

[7] P. Samuel, Algebraic Theory of Numbers, Hermann, Paris, 1970.

[8] I.N. Stewart, D.O. Tall, Algebraic Number Theory, Chapman & Hall, London, 1987.

[9] 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, *Journal of Algebra and Its Applications*, 20(03), 2021, 2150029.

Trace form via the twisted homomorphism

Antonio Aparecido de Andrade [1]
Departamento de Matemática, Ibilce, Unesp
São José do Rio Preto - SP

1 Introduction

An algebraic number field $\mathbb{K}$ is an extension of $\mathbb{Q}$ of degree finite n, that is, $[\mathbb{K}:\mathbb{Q}]=n$. In this case, $\mathbb{K}=\mathbb{Q}(\theta)$, where $\theta\in\mathbb{C}$ is a root of a monic irreducible polynomial $p(x)\in\mathbb{Q}[x]$ and n is the degree of $p(x)$. The n distinct roots of $p(x)$, namely, $\theta_1,\theta_2,\ldots,\theta_n$, are the conjugates of θ. If $\sigma:\mathbb{K}\to\mathbb{C}$ is a $\mathbb{Q}$-homomorphism, then $\sigma(\theta)=\theta_i$ for some $i=1,2,\ldots,n$. Furthermore, there are exactly n $\mathbb{Q}$-homomorphisms σ_i, for $i=1,2,\ldots,n$, of $\mathbb{K}$ in $\mathbb{C}$.

An element $\alpha\in\mathbb{K}$ is called an algebraic integer if there is a monic polynomial $f(x)$ with integer coefficients such that $f(\alpha)=0$. The set $\mathcal{O}_{\mathbb{K}}=\{\alpha\in\mathbb{K}:\alpha \text{ is an algebraic integer}\}$ is a ring, called ring of algebraic integers of $\mathbb{K}$ and $\mathcal{O}_{\mathbb{K}}$, as a $\mathbb{Z}$-module, has a basis $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ over $\mathbb{Z}$, called integral basis, where n is the degree of $\mathbb{K}$.

The trace and the norm of an element $\alpha\in\mathbb{K}$ over $\mathbb{Q}$ are defined as the rational numbers $Tr_{\mathbb{K}}(\alpha)=\sum_{i=1}^{n}\sigma_i(\alpha)$ and $N_{\mathbb{K}}(\alpha)=\prod_{i=1}^{n}\sigma_i(\alpha)$. If $\alpha\in\mathcal{O}_{\mathbb{K}}$, then $Tr_{\mathbb{K}}(\alpha)$ and $N_{\mathbb{K}}(\alpha)$ are algebraic integers. The discriminant of $\mathbb{K}$ over $\mathbb{Q}$ is defined by $\mathcal{D}_{\mathbb{K}}=\mathcal{D}(\alpha_1,\alpha_2,\ldots,\alpha_n)=\det_{1\le i,j\le n}(Tr_{\mathbb{K}}(\alpha_i\alpha_j))=\det_{1\le i,j\le n}(\sigma_i(\alpha_j))^2$, where $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ is an integral basis of $\mathbb{K}$ [1].

2 Trace form via $\mathbb{Q}(\zeta_n)$

An algebraic number field $\mathbb{L}$ is said to be cyclotomic if $\mathbb{L}=\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity. In this case, $[\mathbb{L}:\mathbb{Q}]=m=\phi(n)$, where ϕ is Euler's phi function, the ring of algebraic integers of $\mathbb{L}$ is given by $\mathcal{O}_{\mathbb{L}}=\mathbb{Z}[\zeta_n]$ and $\{1,\zeta_n,\zeta_n^2,\cdots,\zeta_n^{\phi(n)-1}\}$ is an integral basis for $\mathbb{L}$.

Definition 2.1. *Let $n=p_1^{t_1}p_2^{t_2}\ldots p_s^{t_s}$, where $t_k\ge 1$, for $k=1,2,\ldots,s$. The function*

$$\mu(n)=\begin{cases}(-1)^s, & \text{if } t_k=1, \text{ for all } k.\\ 1, & \text{if } n=1.\\ 0, & \text{if } t_k>1, \text{ for some } k.\end{cases}$$

is called Möbius function.

[1] antonio.andrade@unesp.br. Agradecimentos a Fapesp, Proc. 2013/25977-7 e 2022/02303-0

Let $n = p_1^{t_1} \dots p_s^{t_s}$, with $t_k \geq 1$, for $k = 1, 2, \dots s$, $n \neq 2^r$, $r \geq 2$, $m = \phi(n)$. If $x = b_0 + b_1\zeta_n + \ldots + b_{m-1}\zeta_n^{m-1}$ is an algebraic integer of $\mathbb{L} = \mathbb{Q}(\zeta_n)$, then

$$x\overline{x} = \sum_{i=0}^{m-1} b_i^2 + \sum_{i=0}^{m-1} A_i\beta_i,$$

where $A_i = b_0b_i + b_1b_{i+1} + \ldots + b_{m-1-i}b_{m-1}$ and $\beta_i = \zeta_n^i + \zeta_n^{-i}$, for all $i = 1, 2, \cdots, m-1$.

Theorem 2.1. ([2]) *If $n = p_1^{a_1} \dots p_s^{a_s}$, with $a_k \geq 1$, for $k = 1, 2, \dots s$, $n \neq 2^r$, $r \geq 2$, $m = \phi(n)$ e $x = a_0 + a_1\zeta_n + \ldots + a_{m-1}\zeta_n^{m-1}$ is an algebraic integer of $\mathbb{L} = \mathbb{Q}(\zeta_n)$, then*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = \frac{n}{P}\left\{ \phi(P)\sum_{i=0}^{m-1} a_i^2 + 2\sum_{j=1}^{\phi(P)-1} \mu(\frac{P}{t_j})\phi(t_j)A_{\frac{n}{P}j} \right\},$$

where $P = p_1 \dots p_s$, $t_j = mdc(j, P)$, for $j = 1, 2, \dots, \phi(P) - 1$ and $A_i = a_oa_i + a_1a_{i+1} + \ldots + a_{m-1-i}a_{m-1}$, for $i = 1, 2, \dots, m-1$.

Proposition 2.1. *[3] If $\alpha = a_0 + a_1\zeta_n + \cdots + a_{\phi(n)-1}\zeta_n^{\phi(n)-1} \in \mathcal{O}_{\mathbb{L}}$, then*

$$Tr_{\mathbb{L}}(\alpha) = \frac{n}{P}\left(\phi(P)a_0 + \sum_{k=1}^{\phi(P)-1} a_{\frac{n}{P}k}\mu(\frac{P}{t_k})\phi(t_k) \right).$$

Corollary 2.1. *[3] If $n = 2^r$, where $r \geq 2$, then $Tr_{\mathbb{L}}(\alpha) = \phi(n)a_0$.*

Theorem 2.2. *[3] If $\alpha = a_0 + a_1\zeta_n + \cdots + a_{\phi(n)-1}\zeta_n^{\phi(n)-1} \in \mathcal{O}_{\mathbb{L}}$ and $x = b_0 + b_1\zeta_n + \cdots + b_{\phi(n)-1}\zeta_n^{\phi(n)-1} \in \mathcal{O}_{\mathbb{L}}$, then*

$$\begin{aligned} Tr_{\mathbb{L}}(\alpha x\overline{x}) \;=\; & \sum_{i=0}^{\phi(n)-1} b_i^2\left(\frac{n}{P}\left(\phi(P)a_0 + \sum_{k=1}^{\phi(P)-1} a_{\frac{n}{P}k}\mu(\frac{P}{t_k})\phi(t_k) \right)\right) \\ & + 2a_0 \sum_{k=1}^{\phi(P)-1} B_{\frac{n}{P}k}\mu(\frac{P}{t_k})\frac{1}{\phi(\frac{P}{t_k})}\phi(n) + \sum_{\substack{i+j=\frac{nk}{P} \\ l\leq k\leq r \\ 1\leq i,j\leq\phi(n)-1}} B_ia_j\mu(\frac{P}{t_k})\phi(t_k) \\ & + \sum_{\substack{0\leq|i-j|=\frac{nk}{P} \\ 0\leq k\leq s \\ 1\leq i,j\leq\phi(n)-1}} B_ia_j\mu(\frac{P}{t_k})\phi(t_k), \end{aligned}$$

where $l = \left\lceil \frac{2P}{n} \right\rceil$, $r = \left\lfloor \varphi(P) - \frac{2P}{n} \right\rfloor$ and $s = \left\lfloor \frac{\varphi(P)}{2} - \frac{2P}{n} \right\rfloor$.

Referências

[1] P. Samuel, *Algebraic Theory of Numbers*, Hermann, Paris (1970).

[2] J. C. Interlando, T. P. N. Neto, T. M. Rodrigues, J. O. D. Lopes, A note on the integral trace form in cyclotomic fields, *J. Algebra App.*, **14** (2015), 1550045.

[3] A. A. Andrade, Integral trace form via cyclotomic fields, in preparation.