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.

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 pela 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. Em 2023 organizamos um minissimpósio intitulado *Códigos e reticulados algébricos* dentro do XLII CNMAC, que foi realizado no período de 18 à 22 de setembro em Bonito - MS. Em 2024, organizamos o minissimpósio intitulado *Códigos e reticulados algébricos* dentro do XLIII CNMAC, que foi realizado no período de 16 à 20 de setembro, em Porto de Galinhas - PE. Novamente, em 2025, estamos empenhados em organizar um minissimpósio intitulado *Códigos e reticulados algébricos* dentro do XLIV CNMAC, que será realizado no período de 15 à 19 de setembro, que será realizado no Rio de Janeiro - RJ, 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: Aplicações de corpos puros na teoria da codificação.

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

2. Prof. Dr. Robson Ricardo de Araujo
Título: O problema do isomorfismo de reticulados para módulos e suas conexões com a criptografia pó quântica.
Filiação: Instituto Federal de Educação de São Paulo (IFSP), Catanduva - SP.
3. Profa. Dra. Carina Alves.
Título: Alguns resultados sobre reticulados torcidos bem arredondados via corpos quadráticos imaginários.
Filiação: Departamento de Matemática, Igce - Unesp, Rio Claro - SP.
4. Profa. Dra. Grasielle Cristiane Jorge.
Título: Algumas construções do reticulado de Leech via subcorpos de corpos ciclotômicos.
Filiação: Instituto de Ciência e Tecnologia - Unifesp, São José dos Campos - SP.
5. Profa. Dra. Cintya Wink de Oliveira Benedito.
Título: Códigos de bloco espaço-tempo via álgebra dos quatérnios associativas e não associativas.
Filiação: Campus Experimental de São João da Boa Vista (SP) - Unesp, São João da Boa Vista - SP.
6. Prof. Dr. João Eloir Strapasson.
Título: Algoritmo para obtenção de elemento totalmente positivo em corpos totalmente reais, via SVP-Problem.
Filiação: Faculdade de Ciências Aplicadas, Unicamp, Limeria - SP.
7. Prof. Dr. Edson Donizete de Carvalho
Título: Codificação baseada na teoria das Q -matrizes de Fibonacci
Filiação: Departamento de Matemática, Feis - Unesp, Ilha Solteira - SP.
8. Prof. Dr. Danilo Antonio Caprio.
Título: Um estudo sobre a teoria das Q -matrizes e aplicações.
Filiação: Departamento de Matemática, Feis - Unesp, Ilha Solteira - SP.

3 Resumos das palestras

Aplicações de corpos puros na teoria da codificação.

Antonio Aparecido de Andrade ¹

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

Um problema clássico na matemática 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 18º problema de Hilbert, proposto em 1900 no Congresso Internacional de Matemática 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.

Seja $\mathbb{K}$ um corpo de números puro de grau n . Pela teoria de Galois, segue que existem n $\mathbb{Q}$ -monomorfismos $\sigma_1, \sigma_2, \dots, \sigma_n$ de $\mathbb{K}$ em $\mathbb{C}$. Se n é ímpar, apenas um é real, por exemplo σ_1 , e os demais são complexos. Neste caso,

$$\sigma(\alpha) = (\alpha, \tilde{\alpha}, \operatorname{Re}(\sigma_1(\alpha)), \operatorname{Im}(\sigma_1(\alpha)), \dots, \operatorname{Re}(\sigma_{\frac{n-2}{2}}(\alpha)), \operatorname{Im}(\sigma_{\frac{n-2}{2}}(\alpha))),$$

onde $\alpha \in \mathbb{K}$ e $\sigma_{n/2}(\alpha) = \tilde{\alpha}$. Assim, $\|\sigma(\alpha)\|^2 = \alpha^2 + (\tilde{\alpha})^2 + \sum_{i=1}^{(n-2)/2} \sigma_i(\alpha)\overline{\sigma_i(\alpha)}$. Se n é par, apenas dois são reais, por exemplo σ_1 e $\sigma_{n/2}$, e os demais $n - 2$ são complexos. Neste caso, o homomorfismo canônico é dado por

$$\sigma(\alpha) = (\alpha, \operatorname{Re}(\sigma_1(\alpha)), \operatorname{Im}(\sigma_1(\alpha)), \dots, \operatorname{Re}(\sigma_{\frac{n-1}{2}}(\alpha)), \operatorname{Im}(\sigma_{\frac{n-1}{2}}(\alpha))),$$

onde $\alpha \in \mathbb{K}$. Assim, $\|\sigma(\alpha)\|^2 = \alpha^2 + \sum_{i=1}^{(n-1)/2} \sigma_i(\alpha)\overline{\sigma_i(\alpha)}$.

Se M é um $\mathbb{Z}$ -módulo de $\mathbb{K}$, então $\sigma(M)$ é um reticulado em $\mathbb{R}^n$, chamados 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. Neste trabalho, apresentamos novas construções de reticulados via corpos puros.

Referências

- [1] J. H. Conway and N. J. A Sloane. *Sphere packings, lattices and group*. Springer-Verlag, New York, 1998.
- [2] E. L. Oliveira, J. C. Interlando, T. P. Nóbrega Neto and J. O. D. Lopes, The integral trace form of cyclic extensions of odd prime degree, *Rocky Mountain J. Math.*, **47**(4) (2017) 1075-1088.
- [3] E. M. Moro, A. A. Andrade and C. Alves, Integral trace form of extensions of degree pq , *J. Algebra Appl.* **29** (2022) 2250103:1-13.

¹antonio.andrade@unesp.br. Agradecimentos a Fapesp, Proc. 2022/02303-0

O problema do isomorfismo de reticulados para módulos e suas conexões com a criptografia pós-quântica

Robson Ricardo de Araujo ¹

Instituto Federal de São Paulo, Catanduva - SP

Desde os trabalhos de Peter Shor na década de 1990, sabe-se que a maioria dos criptosistemas atualmente em uso se tornarão obsoletos quando os computadores quânticos se tornarem viáveis. Por isso, nas últimas décadas, a comunidade científica tem buscado alternativas ao RSA e à criptografia baseada em curvas elípticas - é a chamada criptografia pós-quântica. Entre as diversas categorias de propostas para criptografia supostamente resistentes a ataques quânticos, destacam-se os protocolos criptográficos baseados em polinômios multivariados, isogenias super-singulares, códigos corretores de erros, função Hash e, principalmente, reticulados [1].

Um dos objetivos da criptografia é a assinatura digital, que consiste na busca por mecanismos que garantam a autenticidade de mensagens recebidas por um usuário. Já há alguns protocolos para assinatura digital bem aceitos pela comunidade, tais como o *Falcon* e o *Dilithium* [6]. Recentemente, um novo esquema de assinatura digital baseado em reticulados, chamado *Hawk*, tem demonstrado eficiência e segurança quando comparado a estes dois últimos [3]. O esquema *Hawk* é considerado seguro por que sua demonstração de segurança baseia-se na solução do Problema do Isomorfismo de Reticulados, ou mais especificamente, na versão algébrica de tal problema conhecida como *Module-LIP* (do inglês, *Module-Lattice Isomorphism Problem*) [4].

Desde a proposta do esquema *Hawk* para assinatura digital, diversos esforços têm sido feitos para fins de criptoanálise desse esquema, ou seja, para encontrar bons algoritmos que resolvam o problema *Module-LIP* (de posto 2) sob certas instâncias. Entre elas, destacam-se o artigo de Mureau et al. [5], onde os autores descrevem cuidadosamente o problema *Module-LIP* e propõem um algoritmo eficiente para resolvê-lo sob corpos totalmente reais. Recentemente, em [2], Chevignard et al. apresentam uma redução de segurança não-uniforme do problema *Module-LIP* sob CM-corpos para o Problema do Ideal Principal sobre a álgebra dos quatérnios.

Nesta comunicação, faremos uma apresentação sobre o problema *Module-LIP* e uma exposição sobre diversos avanços recentes feitos na criptoanálise do esquema *Hawk*, incluindo uma discussão sobre problemas matemáticos em Teoria dos Números Algébricos relacionados a esses assuntos.

Dois reticulados L e L' são ditos isomorfos se existe uma transformação linear O tal que $L' = O \cdot L$ [4]. O Problema do Isomorfismo de Reticulados (LIP) consiste em revelar tal transformação O , sabendo que o isomorfismo está estabelecido. A segurança do esquema *Hawk* reduz-se à busca pela solução da versão algébrica do LIP conhecida como *module-LIP*, que descrevemos brevemente a seguir no caso particular de interesse do *Hawk*.

Seja C uma base do reticulado $\mathcal{O}_{\mathbb{K}}^2$ (considerado sob o mergulho canônico), em que $\mathcal{O}_{\mathbb{K}}$ denota o anel de inteiros de um corpo de números $\mathbb{K}$. A chave pública do *Hawk* é a matriz $G = C^*C$. Neste contexto, a solução do *module-LIP* consiste em determinar C dado que G é conhecida.

Em [5], um algoritmo eficiente para solucionar o problema *module-LIP* é apresentado para corpos totalmente reais. De fato, neste caso, o referido problema pode ser tratado pela busca da solução de equações do tipo $x^2 + y^2 = a$ sobre um corpo de números totalmente real e pela busca de geradores de ideais principais nesse contexto. Por sua vez, quando $\mathbb{K}$ é um CM-corpo (em particular, quando $\mathbb{K}$ é um corpo ciclotômico), em [2] mostrou-se que o *module-LIP* reduz-se ao problema de determinar geradores

¹robson.ricardo@ifsp.edu.br. Agradecimentos à Fapesp, Proc. 2022/12667-9, e ao CNPq - Universal 405842/2023-6.

curtos de ideais principais em ordens maximais da álgebra dos quatérnios (problema *nrd-PIP*), o que vem da associação desse problema com a busca por soluções para a equação $x^2 + y^2 + z^2 + w^2 = a$ sobre $\mathbb{K}$.

Para fins práticos, o esquema *Hawk* tem sido aplicado através de corpos ciclotômicos de índice 2^n . Neste caso, o problema *nrd-PIP* ainda não pode ser resolvido por algoritmos quânticos eficientes, o que garante a sua segurança atualmente. No entanto, a busca por solucionar este último problema justifica-se na perspectiva de reforçar essa segurança ou de quebrar o *Hawk*.

Referências

- [1] Bernstein, D., Lange, T. *Post-quantum cryptography*. Nature 549, 188?194 (2017).
- [2] Chevignard, C., Fouque, P.-A., Mureau, G., Pellet-Mary, A., Wallet, A. *A reduction from Hawk to the principal ideal problem in a quaternion algebra*. Cryptology ePrint Archive, Paper 2024/1147, 2024.
- [3] Ducas, L., Postlethwaite, E. W., Pulles, L. N., van Woerden, W. P. J. *Hawk: Module LIP makes lattice signatures fast, compact and simple*. In: Shweta Agrawal and Dongdai Lin, editors, Advances in Cryptology - ASIACRYPT 2022 - Proceedings, Part IV, volume 13794 of Lecture Notes in Computer Science, pages 65?94. Springer, 2022.
- [4] Ducas, L., van Woerden, W. P. J. *On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography*. In: Orr Dunkelman and Stefan Dziembowski, editors, Advances in Cryptology - EUROCRYPT 2022 - Proceedings, Part III, volume 13277 of Lecture Notes in Computer Science, pages 643?673. Springer, 2022.
- [5] Mureau, G., Pellet-Mary, A., Pliatsok, G., Wallet, A. *Cryptanalysis of rank-2 module-lip in totally real number fields*. In: Advances in Cryptology - EUROCRYPT 2024 - Proceedings, Part VI, volume 14656 of Lecture Notes in Computer Science, pages 226?255. Springer, 2024.
- [6] National Institute of Standards and Technology. *Post-Quantum Cryptography - Selected Algorithms 2022*. Available online: <https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>. Acesso em 24/10/2024.

Alguns resultados sobre reticulados torcidos bem arredondados via corpos quadráticos imaginários

Carina Alves ¹

Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de Rio Claro, São Paulo - SP

Reticulados têm várias aplicações em matemática, incluindo teoria dos números, criptografia e teoria de códigos. Em particular, reticulados algébricos, ou seja, construídos via o homomorfismo canônico [5] e derivados de corpos quadráticos, são estruturas de interesse devido às suas propriedades geométricas e algébricas, que os tornam adequados para diversos problemas de telecomunicações [5]. Uma característica desejável em reticulados algébricos é que sejam bem arredondados, ou do inglês “well-rounded”, o que significa que os vetores mínimos do reticulado, ou seja, aqueles com menor norma, geram todo o espaço, permitindo uma distribuição mais eficiente dos pontos do reticulado [2]. Nesse contexto, os reticulados bem arredondados torcidos, ou do inglês “well-rounded twists”, surgem como uma estratégia para ajustar um reticulado algébrico, transformando-o em uma forma bem arredondada. Um reticulado bem arredondado torcido consiste em uma transformação específica que preserva certas propriedades, mas modifica a distribuição geométrica dos vetores, visando obter uma configuração ideal para aplicações práticas e teóricas [3]. Este trabalho investiga reticulados bem arredondados torcidos provenientes de reticulados algébricos obtidos a partir de corpos quadráticos imaginários.

Seja Λ um reticulado em $\mathbb{R}^2$. O conjunto dos vetores mínimos de Λ é $S(\Lambda) = \{x \in \Lambda : \|x\| = \lambda_1(\Lambda)\}$, onde $\lambda_1(\Lambda) = \min_{0 \neq x \in \Lambda} \|x\|$. O reticulado Λ é chamado *bem arredondado* se o conjunto $S(\Lambda)$ gera $\mathbb{R}^2$. Se Λ é bem arredondado e $\{x_1, x_2\}$ é sua base tal que $x_1, x_2 \in S(\Lambda)$, então $\{x_1, x_2\}$ é chamada de *base mínima* de Λ . Uma base $\{x_1, x_2\}$ é *torcível* se existe uma matriz T_α tal que $\|T_\alpha x\| = \|T_\alpha y\|$. Note que, se $S(\Lambda)$ contiver dois vetores independentes, então esses vetores formam uma base mínima para Λ . Este fato não é verdadeiro para reticulados de dimensão superior [4]. Para cada número real $\alpha > 0$, definimos a matriz $T_\alpha = \begin{bmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{bmatrix}$. O reticulado $T_\alpha \Lambda$ é chamado de *reticulado torcido* de Λ em relação a α . Seja d um inteiro livre de quadrados tal que $K = \mathbb{Q}(\sqrt{-d})$. Veremos que se $-d \not\equiv 1 \pmod{4}$ então é possível obter um único reticulado torcido bem arredondado, que é semelhante a um reticulado ortogonal, e que se $-d \equiv 1 \pmod{4}$ então é possível obter um único reticulado torcido bem arredondado, que é semelhante ao reticulado hexagonal. Além disso, para todo ideal do anel dos inteiros de um corpo quadrático imaginário K é possível obter pelo menos um reticulado torcido bem arredondado.

Referências

- [1] M. T. Damir and D. Karpuk, Well-rounded twists of ideal lattices from real quadratic fields, *J. Number Theory* v.196, p.168-196, 2019.
- [2] L. Fukshansky and K. Petersen. On well-rounded ideal lattices. *Int. J. Number Theory*, v.8, n. 1, p. 189-206, 2012.
- [3] N. H. Le , D. T. Tran, and H. T. N. Tran, Well-rounded twists of ideal lattices from imaginary quadratic fields, *Journal of Algebra and Its Applications*, v. 21, n. 7, p. 2250133, 2022.

¹Esta pesquisa é financiada pela FAPESP Proc. 2023/15735-8 e CNPq 405842/2023-6. E-mail: carina.alves@unesp.br

- [4] P. Q. Nguyen, Hermite's Constant and Lattice Algorithms, in *The LLL Algorithm :Survey and Application*, Springer, p. 19-69, 2009.
- [5] F.E. Oggier, Algebraic methods for channel coding, *Ph.D. Thesis, école Polytechnique Fédérale de Laussane*, Laussane, 2005.

Algumas construções do reticulado de Leech via subcorpos de corpos ciclotômicos

Grasiele Cristiane Jorge ¹

Departamento de Ciência e Tecnologia, Universidade Federal de São Paulo - São José dos Campos - SP

João Eloir Strapasson²

Universidade Estadual de Campinas - Limeira - SP

Agnaldo José Ferrari ³

Universidade Estadual Paulista - Bauru - SP

Um reticulado é um subgrupo aditivo e discreto de $\mathbb{R}^n$. Pode ser demonstrado que, dado um reticulado $\Lambda \subset \mathbb{R}^n$, existem m vetores linearmente independentes sobre $\mathbb{R}$, com $m \leq n$, de forma que Λ pode ser descrito como combinação linear desses m vetores com coeficientes inteiros. Reticulados são definidos como subgrupos aditivos discretos de $\mathbb{R}^n$ e, desde a década de 1970, têm desempenhado papéis fundamentais na confiabilidade e segurança da informação [2]. Um dos problemas clássicos associados aos reticulados é o empacotamento de esferas. Um empacotamento, na métrica euclidiana, consiste em uma distribuição de esferas de mesmo raio, de modo que quaisquer duas esferas ou não se intersectam ou se intersectam apenas em seus bordos. Foi demonstrado que, nas dimensões 2, 3, 8 e 24, o empacotamento mais denso possível de esferas pode ser obtido por meio de reticulados. A prova para $n = 3$ (conhecida como a Conjectura de Kepler, de 1612) foi resolvida por Thomas C. Hales em 2005. Nas dimensões $n = 8$ e $n = 24$, as soluções foram alcançadas por Maryna Viazovska e colaboradores em 2017 [1,4]. Este trabalho notável resultou na concessão da Medalha Fields a Maryna Viazovska em 2022. Um reticulado em $\mathbb{R}^n$ é dito algébrico se ele pode ser obtido como a imagem de um homomorfismo aplicado a um $\mathbb{Z}$ -módulo livre de posto n contido em um corpo de números de grau n . Construções de reticulados algébricos podem ser utilizadas para calcular alguns parâmetros dos reticulados que são difíceis de determinar em reticulados gerais em $\mathbb{R}^n$.

Neste trabalho, apresentamos versões rotacionadas do reticulado de Leech Λ_{24} , que é o empacotamento de esferas mais denso na dimensão 24, via corpos numéricos totalmente reais, assegurando diversidade máxima e calculando a distância do produto mínima. Esses reticulados têm potencial de aplicação tanto em canais gaussianos quanto com desvanecimento do tipo Rayleigh.

Referências

- [1] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko e M. Viazovska. The sphere packing problem in dimension 8. *Annals of Mathematics*, 185(3): 1017-1033, 2017.
- [2] S. I. R. Costa, F. Oggier, A. Campello, J.-C. Belfiore e E. Viterbo, *Lattices applied to coding for reliable and secure communications*, 1st ed., Springer Cham, 2017.

¹grasiele.jorge@unifesp.br. Este trabalho foi apoiado pela Fapesp 2023/05215-7, 2013/25977-7 e pelo CNPq 405842/2023-6.

²strapass@unicamp.br

³agnaldo.ferrari@unesp.br

- [3] J. E. Strapasson, A. J. Ferrari, G. C. Jorge e 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), 2150029, (2021).
- [4] M. Viazovska. The sphere packing problem in dimension 24. *Annals of Mathematics*, 185(3):991-1015, 2017.

Códigos de bloco espaço-tempo via álgebra dos quatérnios associativas e não associativas

Cintya Wink de Oliveira Benedito ¹

Faculdade de Engenharia, FESJ - Unesp, São João da Boa Vista - SP

Sistemas MIMO (*Multiple-Input Multiple-Output*), com múltiplas antenas de transmissão e múltiplas antenas de recepção, surgiram como uma técnica promissora para melhorar o desempenho de dispositivos digitais em sistemas de transmissão. Visando maximizar o ganho de diversidade nestes sistemas, os Códigos de Bloco Espaço-Tempo (*Space-Time Block Code - STBC*) são projetados e utilizados. Considere $\mathbb{L} = \mathbb{Q}(\theta)$ uma extensão quadrática de $\mathbb{K} = \mathbb{Q}(i)$. Um STBC infinito $\mathcal{C}$ pode ser definido como o conjunto de matrizes da forma

$$\mathcal{C} = \left\{ \mathbf{X} = \begin{pmatrix} x_0 + x_1\theta & x_2 + x_3\theta \\ \gamma(x_2 - x_3\bar{\theta}) & x_0 + x_1\bar{\theta} \end{pmatrix}; x_0, x_1, x_2, x_3 \in \mathbb{Z}[i] \right\}, \quad (1)$$

em que γ é um elemento que não é uma norma em $\mathbb{L}$. Temos inicialmente que $\mathcal{C}$ é um código linear se $\mathbf{X}_1, \mathbf{X}_2 \in \mathcal{C}$ então $\mathbf{X}_1 + \mathbf{X}_2 \in \mathcal{C}$. O código finito $\mathcal{C}$ é obtido limitando os símbolos de informação $x_0, x_1, x_2, x_3 \in S$, assumindo a constelação de sinal S sendo M -QAM (*Quadrature Amplitude Modulation*), logo temos um código linear de taxa máxima.

A diversidade máxima é obtida se o código possuir a propriedade do determinante diferente de zero (NVD - *Non-Vanishing Determinant*). O determinante da diferença entre duas palavras-código é diferente de zero se

$$|\det(\mathbf{X}_i - \mathbf{X}_j)|^2 \neq 0, \quad \text{para } \mathbf{X}_i \neq \mathbf{X}_j \in \mathcal{C}. \quad (2)$$

Pela linearidade, essa expressão é simplificada para $|\det(\mathbf{X})|^2 \neq 0$, para toda palavra-código $\mathbf{X} \in \mathcal{C}$ diferente de zero. Como uma álgebra cíclica de divisão herda um conjunto estruturado de matrizes invertíveis, a diversidade máxima do STBC $\mathcal{C}$ é alcançada. De forma geral, se $\mathcal{A} = (a, b)_{\mathbb{K}}$ é uma álgebra dos quatérnios sobre um corpo de números $\mathbb{K}$, pode-se construir códigos espaço-tempo 2×2 .

Usualmente, STBCs com diversidade máxima são construídos a partir de álgebras de divisão associativas, como as álgebras cíclicas ou os quatérnios clássicos. Por exemplo, em [1], o código de ouro foi obtido a partir da álgebra $\mathcal{A} = (5, i)_{\mathbb{Q}(i)}$, com $\mathbb{L} = \mathbb{Q}(i, \sqrt{5})$ e, em [2] o código de prata foi obtido a partir da álgebra $\mathcal{A} = (7, i)_{\mathbb{Q}(i)}$, em que $\mathbb{L} = \mathbb{Q}(i, \sqrt{7})$. Em [3] são apresentadas condições para que os STBCs sejam considerados perfeitos. Já em [4], foram propostas construções de STBCs fazendo uso de álgebras de divisão não associativas a partir do processo de duplicação de Cayley-Dickson, [5], ampliando assim o conjunto de ferramentas disponíveis para obter STBCs com diversidade máxima e, oferecendo vantagens em termos de desempenho e flexibilidade. Neste trabalho, iremos apresentar construções de STBCs com diversidade máxima a partir de álgebras dos quatérnios associativas e não associativas. Iremos utilizar corpos de números do

¹cintya.benedito@unesp.br. Agradecimentos a Fapesp, Proc. 2024/05051-7 e 2013/25977-7

tipo $\mathbb{L} = \mathbb{Q}(i)(\sqrt{d})$, em que d é livre de quadrados e $d \notin \mathbb{Q}(i)$. Tais construções podem projetar famílias de STBCs para serem utilizados em canais MIMO para 2×2 , 2×4 (multibloco) e 4×4 antenas. Esses códigos são projetados para maximizar a diversidade em sistemas MIMO.

Referências

- [1] Belfiore J.-C.; Rekaya, G.; Viterbo, E. The Golden Code: A 2×2 full-rate space-time code with non-vanishing determinants. *IEEE Transactions on Information Theory*, v. 51, n. 4, p. 1432-1436, 2005.
- [2] Hollanti, C. et al. On the algebraic structure of the silver code: A 2×2 perfect space-time block code. In: 2008 IEEE Information Theory Workshop. [S.l.: s.n.], 2008. p. 91-94.
- [3] Oggier, F. et al. Perfect Space Time Block Codes. *IEEE Transactions on Information Theory*, IEEE Press, v. 52, n. 9, 09 2006.
- [4] Pumplun, S. and Unger, T. Space-time block codes from nonassociative division algebras. *Advances in Mathematics of Communications*, 2011, 5(3): 449-471.
- [5] Waterhouse, W.C. Nonassociative quaternion algebras, *Algebras Groups Geom.* 4 (1987), no. 3, 365-378.

Algoritmo para obtenção de elemento totalmente positivo em corpos totalmente reais, via SVP-Problem.

João Eloir Strapasson ¹

Faculdade de Ciências Aplicadas, FCA - Unicamp, Limeira - SP

Seja M um número natural da forma $M = 2^r q$, em que q é um número ímpar, considere o corpo real maximal $\mathbb{K} = \mathbb{Q}(\zeta_M + \zeta_M^{-1})$, 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, [1,2]: $\langle x, y \rangle = \text{Tr}_{\mathbb{K}/\mathbb{Q}}(xy\alpha)$ em que, α é um elemento totalmente positivo (positivo para cada mergulho canônico). Quando $\alpha = 1$, teremos o mergulho canônico. Para encontrar elemento totalmente positivo, precisamos concluir duas etapas fundamentais:

- A obtenção de um elemento β que possua uma norma previamente desejada;
- A obtenção de uma unidade u tal que $\alpha = u\beta$ seja um elemento totalmente positivo.

A primeira etapa é determinada em tempo polinomial, basta encontrar os geradores da decomposição ideais da forma $p_i \mathcal{O}_{\mathbb{K}}$ com p_i primo. A segunda etapa é a mais complexa (de ordem exponencial), pois as unidades formam um grupo multiplicativo gerado por $n - 1$ unidades fundamentais (u_i). Ou seja, $u = u_1^{d_1} \cdots u_{n-1}^{d_{n-1}}$, em que as potências d_i podem ser restringidas para $d_i = 0$ ou $d_i = 1$. Portando termos 2^{n-1} possibilidades.

A variedade formada pelos elementos da $\alpha = u\beta = u_1^{d_1} \cdots u_{n-1}^{d_{n-1}}\beta$ com $d_i \in \mathbb{Z}$ é um conjunto discreto infinito. Assim como o reticulado logarítmico é usado para obtenção das unidades fundamentais, nosso objetivo é usar mecanismos de busca como SVP ([3]) e SVP-Ideal ([4]) para encontrar o elemento, α , de menor norma euclidiana e que seja totalmente positivo. Para este fim, é necessário estabelecer o menor raio de busca, que é limitado superiormente em função da densidade de centro máxima da dimensão. Em suma, em dimensão baixa é possível determinar quais são os elementos totalmente positivos com norma produto fixada e quais são os reticulados associados a estes mergulhos.

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] G. Hanrot, X. Pujol, D. Stehlé, Algorithms for the shortest and closest lattice vector problems. In International Conference on Coding and Cryptology pp. 159-190. Springer (2011).
- [4] J. Felderhoff, A. Pellet-Mary, D. Stehlé, B. Wesolowski, Ideal-svp is hard for small-norm uniform prime ideals. In: Theory of Cryptography Conference. pp. 63-92. Springer (2023).

¹strapass@unicamp.br. Agradecimentos a Fapesp, Proc. 2020/09838-0

Codificação baseada na teoria das Q -matrizes de Fibonacci

Edson Donizete de Carvalho ¹

Departamento de Matemática - FEIS-UNESP.

Danilo Antonio Caprio ²

Departamento de Matemática - FEIS-UNESP.

Recorrências baseadas nos números de Fibonacci é tema ativo de pesquisa com aplicações em diferentes áreas do conhecimento. Nestas últimas décadas esta temática também tem despertado interesse nos pesquisadores da Teoria de Códigos e Criptografia . Um destes tópicos de interesse são os p números de Fibonacci e as Q_p -matrizes de Fibonacci.

Seja p um inteiro. Em [1], Stakhov introduziu os p números de Fibonacci por meio da relação de recorrência:

$$F_p(n) = F_p(n - 1) + F_p(n - p - 1) \quad (1)$$

onde $n > p + 1$ e com os termos iniciais dados por $F_p(1) = F_p(2) = \dots = F_p(p) = F_p(n) = F_p(p + 1) = 1$. Tomando $p = 1$, a relação de recorrência (7) gera os clássicos números de Fibonacci, dados por:

$$1, 1, 2, 3, 5, 8, 13, \dots \quad (2)$$

As matrizes de Fibonacci generalizadas Q_p^n são descritas da forma:

$$Q_p^n = \begin{pmatrix} F_p(n+1) & F_p(n) & \dots & F_p(n-p+2) & F_p(n-p+1) \\ F_p(n-p+1) & F_p(n-p) & \dots & F_p(n-2p+2) & F_p(n-2p+1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ F_p(n-1) & F_p(n-2) & \dots & F_p(n-p) & F_p(n-p-1) \\ F_p(n) & F_p(n-1) & \dots & F_p(n-p+1) & F_p(n-p) \end{pmatrix}, \quad (3)$$

onde $F_p(n)$ é um número de p - Fibonacci, $n = 0, \pm 1, \pm 2, \pm 3, \dots$

Fixando $n = 1$, e para $p = 0, 1, 2, 3$, temos, respectivamente, as seguintes matrizes:

$$Q_0 = (1), \quad Q_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad Q_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad Q_3 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

As seguintes propriedades aritméticas são verificadas para as Q_p^n -matrizes generalizadas de Fibonacci:

$$Q_p^n \times Q_p^m = Q_p^m \times Q_p^n = Q_p^{m+n}. \quad (4)$$

$$Q_p^n = Q_p^{n-1} + Q_p^{n-p-1}. \quad (5)$$

¹edson.donizete@unesp.br

²danilo.caprio@unesp.br.

$$\det Q_p^n = (-1)^{pn}. \quad (6)$$

No caso $p = 1$, as Q_p^n -matrizes generalizadas de Fibonacci se reduzem a

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \quad (7)$$

com $\det Q^n = F_{n+1}F_{n-1} - F_n^2 = (-1)^n$, onde $n = 0, \pm 1, \pm 2, \pm 3, \dots$ e F_{n-1}, F_n, F_{n+1} são números de Fibonacci que obedecem a relação de recorrência:

$$F_{n+1} = F_n + F_{n-1} \quad (8)$$

A transmissão de informação envolvendo múltiplas antenas, por exemplo, de N antenas para N antenas é realizada via codificação de canal. As matrizes códigos tem ordem N . A introdução das Q_p^n matrizes Generalizadas de Fibonacci em [1, 2] Q_p^n permite a aplicação em problemas envolvendo codificação de canal, como da transmissão de informação de N antenas para N antenas. Basta tomarmos $N = p+1$, um mensagem inicial será representada na forma de matriz de ordem $(p+1) \times (p+1)$ onde $p = 0, 1, 2, 3, \dots$. Pela escolha da matriz generalizada de Fibonacci Q_p^n de ordem $(p+1) \times (p+1)$. Então, a sua matriz codificação e a matriz inversa Q_p^{-n} tem a mesma ordem da matriz de decodificação. Consideramos a codificação generalizada de Fibonacci dada por $E = M \times Q_p^n$, onde M é matriz mensagem. Já decodificação generalizada de Fibonacci é dada por $M = E \times Q_p^{-n}$, onde M é matriz Q_p^{-n} é a matriz inversa da matriz Q_p^n .

Referências

- [1] A. P. Stakhov;, *Introduction into algorithmic mesurement theory, Moscow: Soviet Radio, 1977* [in Russian]
- [2] A. P. Stakhov;, *Fibonacci matrices, a generalization of the "Cassini formula", and a new coding theory, Chaos Solutions e Fractais* (30), 2006, 56-66.

Um estudo sobre a teoria das Q -matrizes e aplicações.

Danilo Antonio Caprio ¹

Departamento de Matemática - FEIS-UNESP.

Edson Donizete de Carvalho ²

Departamento de Matemática - FEIS-UNESP.

Desde o seu surgimento, os números de Fibonacci despertam curiosidade e fascínio por modelar diversos fenômenos na natureza. Nesta últimas décadas surgiram diversos conceitos matemáticos que generalizam os números de Fibonacci. Dentre elas a teoria das Q -matrizes de Fibonacci [1] que aparecem em aplicações envolvendo a teoria de codificação e criptografia, as matrizes desta classe de matrizes de ordem 2 são geradas pelas n ésimas potências da matriz Q , onde

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}. \quad (1)$$

As n ésimas potências da matriz Q descritas pela Equação (1) são caracterizadas na forma :

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \quad (2)$$

com $\det Q^n = F_{n+1}F_{n-1} - F_n^2 = (-1)^n$, onde $n = 0, \pm 1, \pm 2, \pm 3, \dots$ e F_{n-1}, F_n, F_{n+1} são números de Fibonacci e obedecem a relação de recorrência :

$$F_{n+1} = F_n + F_{n-1} \quad (3)$$

que tem como termos iniciais $F_1 = F_2 = 1$ e satisfazem as seguintes propriedades aritméticas :

$$Q^n = Q^{n-1} + Q^{n-2}. \quad (4)$$

$$Q^n Q^m = Q^m Q^n = Q^{m+n}. \quad (5)$$

As formas explícitas para a matriz Q_0 (matriz identidade) e as matrizes Q^n ($n = \pm 1, \pm 2, \pm 3, \dots$) são obtidas de forma recursiva como consequência das relações dadas pelas Equações (4) e (5). Também como consequência da Propriedade descrita pela Equação (5), temos que :

$$Q^{-2k} = \begin{pmatrix} F_{2k-1} & -F_{2k} \\ -F_{2k} & F_{2k+1} \end{pmatrix}, \quad Q^{-(2k+1)} = \begin{pmatrix} -F_{2k} & F_{2k+1} \\ F_{2k+1} & -F_{2k+2} \end{pmatrix} \quad (6)$$

são as matrizes inversas das matrizes Q^n para $n = 2k$ e $2k + 1$, respectivamente.

As propriedades aritméticas provenientes das Q matrizes de Fibonacci introduzidas em [1] permite obter bons parâmetros para aplicações envolvendo codificação de canal. Seja M a matriz mensagem dada por:

$$M = \begin{pmatrix} m_1 & m_2 \\ m_2 & m_4 \end{pmatrix}$$

uma matrix mensagem . Assumiremos que todas as entradas da matriz M sejam inteiros positivos. A codificação de Fibonacci dada na forma $M \times Q^n = E$, ou seja,

¹danilo.caprio@unesp.br.

²edson.donizete@unesp.br

$$E = M \times Q^n = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \times Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} e_1 & e_2 \\ e_3 & e_4 \end{pmatrix} \quad (7)$$

A matriz E é chamada de matriz código E . As entradas inteiras de E , e_1, e_2, e_3 e e_4 são transmitidos através do canal comunicação. A decodificação de Fibonacci é realizada da seguinte forma:

$$M = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} = E \times Q^{-n} = \begin{pmatrix} e_1 & e_2 \\ e_3 & e_4 \end{pmatrix} \times Q^{-n} \quad (8)$$

Para $n = 2k + 1$, podemos usara matrix inversa dada pela matrix da Equação (6 e a matriz decodificação dada pela fórmula 8:

$$\begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} = \begin{pmatrix} e_1 & e_2 \\ e_3 & e_4 \end{pmatrix} \times \begin{pmatrix} -F_{n-1} & F_n \\ F_n & -F_{n+1} \end{pmatrix} \quad (9)$$

Desenvolvendo, obtemos:

$$-F_n e_1 + F_n e_2 > 0 \text{ e } F_n e_1 - F_{n-1} e_2 > 0. \quad (10)$$

$$-F_{n-1} e_3 + F_n e_4 > 0, \text{ e } F_n e_3 - F_{n+1} e_4 > 0. \quad (11)$$

Das condições de $m_1, m_2, m_3, m_4 > 0$, obtemos as desigualdades:

$$\frac{F_{n+1}}{F_n} < \frac{e_1}{e_2} < \frac{F_n}{F_{n-1}}, \text{ e } \frac{F_{n+1}}{F_n} < \frac{e_3}{e_4} < \frac{F_n}{F_{n-1}} \quad (12)$$

A medida que a razão entre números de Fibonacci adjacentes tende ao número áureo $\tau = \frac{1+\sqrt{5}}{2}$, temos que $e_1 \simeq \tau e_2$ e $e_3 \simeq \tau e_4$. Se tomarmos $n = 2k$, e tomarmos a matrix inversa dada pela matrix da Equação (6 e a matriz decodificação dada pela fórmula 8, obtemos o mesmo resultado obtido para $n = 2k + 1$.

Referências

- [1] A. P. Stakhov, *Fibonacci matrices, a generalization of the "Cassini formula", and a new coding theory*, Chaos Solutions e Fractais (30), 2006, 56-66.