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. 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. Novamente, em 2024, estamos empenhados em organizar um minissimpósio intitulado *Códigos e reticulados algébricos* dentro do XLIII CNMAC, que será realizado no período de 16 à 20 de setembro, que será realizado em Porto de Galinhas - PE, 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 binários e aplicações.
   Filiação: Departamento de Matemática, Ibilce - Unesp, São José do Rio Preto - SP.

2. Prof. Dr. Robson Ricardo de Araujo

Título: Reticulados algébricos em dimensões primas ímpares advindos de famílias de $\mathbb{Z}$-módulos em corpos de números cíclicos.
Filiação: Instituto Federal de Educação de São Paulo (IFSP), Catanduva - SP.

3. Profa. Dra. Carina Alves.
   Título: Alguns resultados sobre reticulados cíclicos e bem arredondados.
   Filiação: Departamento de Matemática, Igce - Unesp, Rio Claro - SP.

4. Profa. Dra. Grasiele Cristiane Jorge.
   Título: Reticulados bem-arredondados via o composto de corpos quadráticos.
   Filiação: Instituto de Ciência e Tecnologia - Unifesp, São José dos Campos - SP.

5. Profa. Dra. Cintya Wink de Oliveira Benedito.
   Título: Códigos Matriciais MDS para Aplicação em Sistemas de Armazenamento Distribuído.
   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: Conjunto de sinais geometricamente uniformes casados a métricas de grupo.
   Filiação: Departamento de Matemática, Feis - Unesp, Ilha Solteira - SP.

7. Prof. Dr. João Eloir Strapasson.
   Título: Códigos t-imperfeitos em reticulados.
   Filiação: Faculdade de Ciências Agronômicas, Unicamp, Limeria - SP.

8. Prof. Dr. Danilo Antonio Caprio.
   Título: Uma classe de conjuntos de Julia em $\mathbb{Q}_p$.
   Filiação: Departamento de Matemática, Feis - Unesp, Ilha Solteira - SP.

3 Resumos das palestras

Corpos de números binários e aplicações

Antonio Aparecido de Andrade [1]
Deparatmento 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 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.

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

Neste trabalho, determinamos uma base para o anel de inteiros de $\mathbb{Q}[\sqrt[2^k]{d}]$, onde $d \equiv 2, 3 (\text{mod } 4)$ e d livre de quadrados. Note que só não estarão incluídos nessa prova o caso $d \equiv 1 (\text{mod } 4)$, pois se $d \equiv 0 (\text{mod } 4)$, então d não é livre de quadrados.

Para determinar essa base, faremos uso do conceito de índice de um inteiro algébrico e alguns resultados que serão enunciados a seguir. Se α inteiro algébrico de grau n e $\mathbb{L} = \mathbb{Q}(\alpha)$, então $\text{Ind}(\alpha) = [\mathcal{O}_{\mathbb{L}} : \mathbb{Z}[\alpha]]$ e que $D(\alpha) = Ind(\alpha) d_L$, onde $D(\alpha)$ é o discriminante do inteiro algébrico α e d_L o discriminante do corpo $\mathbb{L}$. Além dessas definições, os dois lemas enunciados a seguir serão cruciais.

Lemma 2.1. *$\mathbb{L} = \mathbb{Q}(\theta)$ um corpo de números de grau n e $\theta \in \mathcal{O}_{\mathbb{L}}$. Então $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ é uma base integral de $\mathbb{L}$ se, e somente se, Ind(θ) $= 1$.*

Lemma 2.2. *Seja θ um inteiro algébrico e $\mathbb{L} = \mathbb{Q}(\theta)$. Se o polinômio minimal de θ sobre $\mathbb{Q}$ é Eisenstein com respeito ao primo p, ou sja, ele é da forma $x^n + a_{n-1}x^{n-1} + a \cdots + a_0$ onde $a_0, a_1, \ldots a_{n-1}$ são divisíveis por p e a_0 não é divisível por p^2, então Ind(θ) não é divisível por p.*

Com esse lema, para demonstrar que $\mathbb{L}$ é monogênico, basta mostrar que para $x^{2^k} - d$ é p-Eisenstein para todo primo p dividindo d, com $d \equiv 2, 3 (\text{mod } 4)$.

Theorem 2.1. *Seja $\mathbb{L} = \mathbb{Q}(\theta)$, onde θ é uma raiz do polinômio $f(x) = x^{2^k} - d$, com $d \neq \pm 1$ inteiro e livre de quadrados e $d \equiv 2, 3 (mod\ 4)$. Então $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$, ou seja, $\mathbb{L}$ é monogênico.*

Theorem 2.2. *Seja o corpo de números $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[n]{d}$, com d livre de quadrados e $n = 2^k$, onde $k > 1$. Se $d \equiv 2, 3 (mod\ 4)$, então o discriminante do anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por $-n^n d^{n-1}$.*

Referências

[1] J. H. Conway and N. J. A Sloane. *Sphere packings, lattices and group*. Springer-Verlag, New York, 1998.

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

[3] 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.

[4] 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.

Reticulados algébricos em dimensões primas ímpares advindos de famílias de $\mathbb{Z}$-módulos em corpos de números cíclicos

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

1 Introdução

Nas últimas décadas têm sido frequente o uso de reticulados, que são grupos abelianos discretos em espaços euclidianos n-dimensionais, para fins de transmissão de sinais em canais de comunicação [3, 4]. Recentemente, os reticulados têm ainda se mostrado muito importantes na formulação de novos sistemas criptográficos possivelmente resistentes a computadores quânticos. Reticulados podem ser obtidos de várias formas, mas uma das mais vantajosas é como imagens de $\mathbb{Z}$-módulos em anéis de inteiros de corpos de números via o mergulho canônico ou mergulhos torcidos. Neste caso, chamamos tais estruturas de *reticulados algébricos* [5].

Seja $\mathbb{K}$ um corpo de números cíclico de grau $p > 2$ primo. Neste caso, o Teorema de Kronecker-Weber garante que $\mathbb{K}$ está contido em um corpo ciclotômico de índice n, o qual podemos assumir ser o menor com esta propriedade - chamamos n de *condutor* de $\mathbb{K}$. É fato que $n = \prod_{i=1}^{r} p_i$ ou $n = p^2 \prod_{i=1}^{r} p_i$, sendo cada p_i um número primo distinto de p tal que $p_i \equiv 1 \ (mod\ p)$ e tal que $p_i \neq p_j$ se $i \neq j$. No primeiro caso, dizemos que n é *não-ramificado* e, no segundo, que n é *ramificado*.

No caso não ramificado, em [7] foi proposta uma família de $\mathbb{Z}$-módulos $\mathcal{M}_m$, para cada $m > 0$ inteiro, para obter reticulados algébricos. Tal família inclui todos os ideais primos ramificados em $\mathbb{K}$. Os reticulados algébricos obtidos por meio dessa família já foram bem estudados do ponto de vista do seu empacotamento esférico e da propriedade do bom-arredondamento [2, 6].

Em paralelo ao caso descrito acima, neste trabalho apresentamos alguns resultados e perspectivas sobre os reticulados algébricos produzidos através de uma família de $\mathbb{Z}$-módulos $\mathcal{M}_{m,c}$ que inclui os ideais primos ramificados em $\mathbb{K}$ no caso em que o condutor deste corpo é ramificado.

2 Resultados

Seja $\mathbb{K}$ um corpo de números cíclico de grau primo $p > 2$ com condutor $n = p^2 \prod_{i=1}^{r} p_i$, sendo $r \geq 0$ e cada p_i um número primo distinto de p tal que $p_i \equiv 1 \ (mod\ p)$ e tal que $p_i \neq p_j$ sempre que $i \neq j$. Neste caso, o anel de inteiros de $\mathbb{K}$ tem uma $\mathbb{Z}$-base $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$, em que θ é o gerador do grupo de Galois de $\mathbb{K}$ sobre $\mathbb{Q}$ e $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$ [1]. Para cada $m > 1$ e

[1] robson.ricardo@ifsp.edu.br. Agradecimentos a Fapesp, Proc. 2022/12667-9 e 2013/25977-7. Trabalho em conjunto com os professores Antonio Aparecido de Andrade, Trajano Pires da Nóbrega Neto e Jefferson Luiz Rocha Bastos, todos do Departamento de Matemática do Ibilce/Unesp.

c inteiros tais que $0 \leq c < m$, definimos o $\mathbb{Z}$-módulo

$$\mathcal{M}_{m,c} = \left\{ \alpha \in \mathcal{O}_{\mathbb{K}} \ : \ Tr_{\mathbb{K}/\mathbb{Q}}\left(\frac{\alpha}{p}\right) = Tr_{\mathbb{K}/\mathbb{Q}}\left(\frac{pc\alpha t}{n}\right) \right\},$$

o qual tem posto máximo no anel de inteiros e índice m. Essa família de $\mathbb{Z}$-módulos é interessante porque inclui todos os ideais primos ramificados em $\mathbb{K}$. É possível verificar que a forma traço associada a esses módulos é calculada pela seguinte fórmula:

$$Tr_{\mathbb{K}}(\alpha^2) = p\left(\left(a_0 m + c\sum_{i=1}^{p-1} a_i\right)^2 + u\left(p\sum_{i=1}^{p-1} a_i^2 - \left(\sum_{i=1}^{p-1} a_i\right)^2\right)\right)$$

para cada $\alpha \in \mathcal{M}_{m,c}$. Neste trabalho vamos apresentar resultados relacionados à minimização desta forma, parâmetro este que está associado à norma mínima do reticulado algébrico obtido pela família dos módulos $\mathcal{M}_{m,c}$ e analisamos situações em que esses reticulados podem ser classificados como bem-arredondados. Veremos que, no caso em que $c \neq 0$, a minimização depende de uma função inteira que é quadrática por partes, a qual ainda merece um estudo mais aprofundado e abre margem para novas pesquisas.

Em particular, como ilustração das possibilidades oferecidas por tal família de módulos, mostramos que é possível construir os reticulados mais densos possíveis nas dimensões 3 e 5 a partir de alguns deles em certos subcorpos ciclotômicos reais: por meio do corpo $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ obtém-se uma versão equivalente ao reticulado D_3 através de $\mathcal{M}_{6,2}$; por sua vez, o $\mathbb{Z}$-módulo $\mathcal{M}_{10,4}$ em um corpo cíclico de grau cinco e condutor 25 realiza um reticulado com a melhor densidade na quinta dimensão.

Referências

[1] Araujo, R.R., Chagas, A.C.M.M., Andrade, A.A., Nóbrega Neto, T.P. *Trace form associated to cyclic number fields of ramified odd prime degree.* Journal of Algebra and Its Applications 19(04), 2020.

[2] Araujo, R.R., Costa, S.I.R. *Well-rounded algebraic lattices in odd prime dimension.* Archiv der Mathematik 112(2), 139-148, 2019.

[3] Conway, J.H., Sloane, N.J.A. *Sphere packings, lattices and group.* Springer-Verlag, New York, 1998.

[4] Costa, S.I.R., Oggier, F., Campello, A., Belfiore, J.-C., Viterbo, E. *Lattices Applied to Coding for Reliable and Secure Communications.* Springer, 2017.

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

[6] Nunes, J.V.L., Interlando, J.C., Nóbrega Neto, T.P., Lopes, J.O.D. *New p-dimensional lattices from cyclic extensions.* Journal of Algebra and Its Applications 16(10), 2017.

[7] Oliveira, E.L., Interlando, J.C., Nóbrega Neto, T.P., Lopes, J.O.D. *The integral trace form of cyclic extensions of odd prime degree.* Rocky Mountain Journal of Mathematics 47(4), 1075-1088, 2017.

Alguns resultados sobre reticulados cíclicos e bem arredondados

Carina Alves [1]
Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de Rio Claro, Rio Claro - SP

1 Introdução

Existem problemas nos quais o uso de reticulados é adequado. O problema do empacotamento esférico é um deles, em que o objetivo é colocar esferas idênticas em $\mathbb{R}^n$ que se tangenciem em apenas um ponto. Outro problema é o do número de contato (do inglês, *kissing number*), em que procura-se pelo número de esferas que podem tocar uma esfera central sem sobreposição. No entanto, para esses problemas não se sabe se reticulados fornecem solução em todas as dimensões. Apesar disso, sabe-se quais propriedades um reticulado deve ter para potencialmente fornecer uma solução para qualquer um desses problemas. Uma delas é que o reticulado seja bem arredondado (do inglês, *well-rounded*). Neste trabalho será abordada duas classes importantes de reticulados, os reticulados bem arredondados e os reticulados cíclicos. Um dos objetivos é mostrar que todo reticulado bem arredondado no plano é semelhante a um reticulado cíclico.

2 Resultados

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 $||\cdot||$ 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 *bem arredondado* se o conjunto $S(\Lambda)$ gera $\mathbb{R}^n$.

Dois reticulados Λ_1 e Λ_2 são *semelhantes,* se existe um número real $\alpha > 0$ e uma matriz invertível U tal que $\Lambda_2 = \alpha U \Lambda_1$.

Finalmente, um reticulado $\Lambda \subset \mathbb{R}^n$, não necessariamente de posto completo, é chamado *cíclico* se ele é fechado com relação ao operador $rot : \mathbb{R}^n \to \mathbb{R}^n$ definido por

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

isto é, $rot(\Lambda) = \Lambda$. Reticulados cíclicos tem sido especialmente estudados no contexto de reticulados baseados em criptografia em [3, 4].

Veremos que todo reticulado bem arredondado $\Lambda \subset \mathbb{R}^2$ é semelhante a um único reticulado cíclico. No entanto, nem todo reticulado cíclico no plano é bem arredondando. Veremos também que reticulados bem arredondados de posto ≥ 3 não são necessariamente semelhantes a um reticulado cíclico [1, 2].

[1] e-mail: carina.alves@unesp.br

Referências

[1] L. Fukshansky and D. Kogan. Cyclic and well-rounded lattices. *Mosc. J. Comb. Number Theory*, v. 11, n. 1, p. 79–96, 2022.

[2] L. Fukshansky and K. Peterson. On well-rounded ideal lattices. *Int. J. Number Theory*, v.8, n. 1, p. 189–206, 2012.

[3] D. Micciancio. Generalized compact knapsacks, cyclic lattices and efficient one-way functions. *Comput. Complexity*, 16(4):365–411, 2007.

[4] C. Peikert and A. Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. Theory of cryptography. *Lecture Notes in Comput. Sci.*, 3876, Springer, Berlin, pp. 145–166, 2006.

Reticulados bem-arredondados via o composto de corpos quadráticos

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

1 Introdução

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.

Denominamos um reticulado $\Lambda \subset \mathbb{R}^n$ como bem arredondado se possuir um subconjunto de n vetores linearmente independentes sobre $\mathbb{R}$ cujo tamanho de cada um deles é igual à norma mínima do reticulado. A norma mínima de um reticulado Λ é definida como o tamanho do menor vetor não nulo em Λ. Reticulados bem arredondados têm sido empregados para abordar questões abrangentes relacionadas a reticulados, principalmente na Teoria de Códigos Corretores de Erros, visando a construção de códigos eficazes para canais gaussianos com escuta.

Um reticulado em $\mathbb{R}^n$ é dito algébrico se ele pode ser obtido como a imagem de um homomorfismo canônico ou torcido 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 serem calculados em reticulados gerais em $\mathbb{R}^n$.

2 Resultados

Nos últimos anos, várias publicações têm abordado a questão de quais reticulados bem arredondados podem ser obtidos por meio de corpos de números, buscando também aplicações práticas [1, 2].

No trabalho de referência [3], foi estabelecido que os únicos reticulados bem arredondados provenientes de ideais principais do anel de inteiros de um corpo quadrático, utilizando o homomorfismo de Minkowski, são obtidos através de $\mathbb{Q}(\sqrt{-1})$ e $\mathbb{Q}(\sqrt{-3})$. Além disso, o estudo revela a existência de infinitos corpos quadráticos nos quais é possível obter reticulados bem arredondados por meio de ideais não principais de seus anéis de inteiros e o homomorfismo de Minkowski. Vale ressaltar que o anel de inteiros de um corpo de números $\mathbb{K}$ é composto por todos os elementos de $\mathbb{K}$ que são inteiros algébricos, ou seja, raízes de polinômios mônicos com coeficientes inteiros.

Nesta palestra, apresentaremos algumas construções novas de reticulados bem-arredondados via o composto de corpos quadráticos.

[1] grasiele.jorge@unifesp.br. Agradecimentos à Fapesp, Proc. 2023/05215-7

Referências

[1] M. T. Damir, A. Karrila, L. Amorós, O. W. Gnilke, D. Karpuk, and C. Hollanti. Well-rounded lattices: Towards optimal coset codes for Gaussian and fading wiretap channels. IEEE Transactions on Information Theory, 67(6), pp. 3645-3663, 2021.

[2] R. R. de Araujo and S. I. R. Costa. Well-rounded algebraic lattices in odd prime dimension. IEEE Transactions on Information Theory, 112(2), pp. 139-148, 2019.

[3] L. Fukshansky and K. Petersen. On well-rounded ideal lattices, International Journal of Number Theory, 08, pp. 189-206, 2012.

Códigos Matriciais MDS para Aplicação em Sistemas de Armazenamento Distribuído

Cintya Wink de Oliveira Benedito, Débora Beatriz Claro Zanitti, Isabella Silva Teixeira [1]
Faculdade de Engenharia, FESJ - Unesp, SÃ£o JoÃ£o da Boa Vista - SP

Códigos corretores de erros sÃ£o utilizados para transmitir ou armazenar informações de modo confiável e seguro, uma vez que a mensagem transmitida pode ter seu conteúdo comprometido devido a interferências no canal. A ideia básica de um código corretor de erros é de codificar uma informação acrescentando a esta, de maneira organizada, bits de redundâncias permitindo assim, ao receber tal informação, detectar e corrigir erros. Os códigos corretores de erros em formato matricial fazem parte de uma categoria de códigos lineares bidimensionais que se destacam pela sua capacidade de corrigir erros em formato de rajada (*burst of errors*), ou seja, erros que ocorrem em bits consecutivos [1]. Os códigos matriciais podem ser gerados a partir de diversos métodos e sÃ£o conhecidos por sua flexibilidade e facilidade tanto na codificação quanto na decodificação. Um método para obter códigos corretores de erros de alta qualidade é buscar códigos que possuam a máxima distância mínima possível. Os códigos que apresentam a propriedade de máxima distância de separação sÃ£o conhecidos como códigos MDS (*Maximum Distance Separable*), os quais proporcionam uma proteção máxima contra falhas de um dispositivo, utilizando uma quantidade específica de redundância para tal propósito [5].

Códigos Matriciais MDS tem se apresentado como uma estratégia de grande interesse em aplicações recentes de sistemas de armazenamento distribuído [3] . Um exemplo desta aplicação sÃ£o nos sistemas denominados como *Redundant Array of Independent Disks*, popularmente conhecidos como RAIDs. A tecnologia do RAID 6 utiliza a estrutura de corpos de Galois para codificar dados nas unidades para proteger dados de erros ou apagamento [4].

Nesta palestra iremos apresentar a codificação de códigos matriciais MDS utilizando matrizes superregulares, algoritmos de decodificação para correção de erros em rajadas baseados em [2] e [4], e aplicações destes códigos em sistemas de armazenamento distribuído, em especial, como uma alterativa para a tecnologia utilizada no RAID 6.

Referências

[1] M. Blaum, P.G. Farrell, H.C.A. Van Tilborg, *Array codes*. Chapter 22 in Handbook of Coding Theory, V.S. Pless and W.C. Huffman (Eds.), Elsevier Science B.V, 1998.

[2] S. D. Cardell, J.J. Climent and V. Requena, "A Construction Of MDS Array Codes", in *WIT Transactions on Information and Communication Technologies*, v.45, pp. 47 - 58, May 2013. Doi:10.2495/DATA130051.

[1] cintya.benedito@unesp.br. Agradecimentos a Fapesp, Proc. 2017/17948-8, 2019/02720-7 e 2013/25977-7

[3] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright and K. Ramchandran, "Network Coding for Distributed Storage Systems," in *IEEE Transactions on Information Theory*, v. 56, no. 9, pp. 4539-4551, Sept. 2010. Doi:10.1109/TIT.2010.2054295.

[4] M. Moussa and M. Rychlik, "Beyond raid 6 - an efficient systematic code protecting against multiple errors, erasures, and silent data corruption," ArXiv, vol. abs/1806.08266, 2018. Available: https://api.semanticscholar.org/CorpusID:49336065 6

[5] S. Roman, *Coding and Information Theory*, Springer-Verlag, 1992.

Conjunto de sinais geometricamente uniformes casados a métricas de grupo

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

1 Introdução

Códigos e conjunto de sinais geometricamente uniformes são caracterizadas pela existência de simetrias internas, as regiões de Voronoi são congruentes, o que leva a uma redução na complexidade de decodificação como consequência da distribuição uniforme dos sinais.

Do ponto de visto algébrico, os sinais de um conjunto de sinais S que é geometricamente uniforme podem seren obtidos por meio da ação transitiva de um grupo H em S, onde H é um subgrupo de $\Gamma(S)$ (grupo de simetrias de S) em S.

Dizemos que um conjunto de sinais S está casado a um grupo G se existe uma aplicação sobrejetora m de G em S tal que, para todo g e h em G, vale $d(m(g), m(h)) = d(m(g^{-1}h), m(e))$ onde e denota o elemento neutro de G. Além disso, se m também for uma aplicação injetiva, então m^{-1} é chamado de rotulamento casado.

Se existe um rotulamento casado entre um conjunto de sinais S e um grupo G, então S também é geometricamente uniforme.

Dado G um grupo, se existe uma função $d : G \times G \to \mathbb{R}$ que seja compatível com a operação do grupo G e satisfaça as condições de que $d_G(g, h) = d_G(gh^{-1}, e)$ e que d_G seja uma métrica em G, então d_G é chamado de métrica de grupo.

Exemplo 1.1. *1. Seja $G = \mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ (o grupo aditivo dos inteiros módulo m). Tomando em $\mathbb{Z}_m$ a aplicação dada por $d_{\mathbb{Z}_m}(g, h) = min\{(g-h) \ mod \ m, (h-g) \ mod \ m)\}$, fácilmente prova-se que $d_{\mathbb{Z}_m}$ define uma métrica em $\mathbb{Z}_m$.*

2. Seja $G = \mathbb{Z}_m$. Dado $l \in G$, desde que $mdc(l, m) = 1$, e temos que $G = \langle l \rangle$ e podemos escrever os elementos de G na forma $G = \{a + bl \ \ (mod \ \ m) \ \ com \ \ a, b \in \mathbb{Z}\}$. Tomando em G a aplicação dada por $d_G(a + bl, a' + b'l) = |a - a'| \ \ (mod \ \ m) + |b - b'| \ \ (mod \ \ m)\}$, fácilmente prova-se que d_G define uma métrica em G .

Dado um grupo G e uma métrica d_G em G, então d_G é invariante a esquerda se $d_G(fg, fh) = d_G(g, h)$ para todo $f, g, h \in G$. Em particular as métricas de grupos dos itens (1) e (2) do Exemplo 1.1 são invariantes a esquerda.

[1] edson.donizete@unesp.br.

2 Resultados

Seja, G um grupo e S um conjunto de sinais sobre o espaço métrico M. Dizemos que S é G-isométrico se existe uma isometria $m : (G, d_G) \to (S, d_S)$, onde d_G é uma métrica em G e d_S é uma métrica em $S \subset M$, e d_G é invariante a esquerda.

Theorem 2.1. *[1] Seja $m : (G, d_G) \to (S, d)$ uma isometria. Se d_G é invariante a esquerda, então a aplicação m^{-1} é um rotulamento casado.*

Theorem 2.2. *1. Seja S um conjunto de sinais m-PSK formado pelos vértices de um polígono de m lados inscrito em um círculo unitário. A aplicação $m : \mathbb{Z}_m \to S$ dada por $m(k) = e^{i2k\pi/m}$ define uma isometria entre elementos de $\mathbb{Z}_m$ e os sinais do conjunto de sinais S caracterizados pelos rótulos $m(k)$ (vértices do pololígono) ao considerarmos a métrica $d_{\mathbb{Z}_m}$ em $\mathbb{Z}_m$ definida no item (1) do Exemplo 1.1 e a métrica de Lee em S dada por $d_{Lee}(a, b) = min\{|a - b|, m - |a - b|\}$.*

2. Seja S um conjunto de sinais 25-$QAM \subset \mathbb{Z}[\theta]$, onde $\theta = i/\omega$, onde $\omega = \frac{1}{2} + i\frac{\sqrt{3}}{2}$. A aplicação $m : \mathbb{Z}_{25} \to S$ dada por $m(a+bl \mod 25) = a+b\theta \ (mod \ (q_1+q_2\theta))$ ($l = 3, q_1 = 3$ e $q_2 = 4$, se $\theta = i$ e com $l = 4, q_1 = 5$ e $q_2 = 5$, se $\theta = \omega$) define uma isometria entre elementos de $\mathbb{Z}_{25}$ e os elementos de S ao considerarmos a métrica de grupo $d_{\mathbb{Z}_{25}}$ em $\mathbb{Z}_{25}$ como definida no item (2) do Exemplo 1 e a métrica de Mannheim em S dada por $d_{Mannheim}(a, b) = (a + b\theta, a' + b'\theta) = |a - a'| + |b - b'|$.

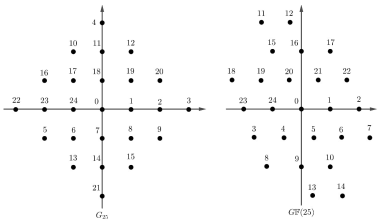

Figura 1:

Como consequência do Teorema 2.1 e 2.2, concluímos existe um rotulamento casado entre os grupos G e os conjuntos sinais S dos itens (1) e (2) do Teorema 2.2. A figura 1, ilustra o rotulamento casado dos conjuntos de sinais S e os grupos aditivos de cardinalidade 25 do item (2) do Teorema 2.2 .

Agradecimentos

FAPESP: 2023/10981-0.

Referências

[1] E. M. V. Gomes, E. D. Carvalho, C. A. R. Martins, W. S. Soares, Jr. and E. B. Silva, E. M. Brizola and E. B. Silva, *A general framework for geometrically uniform codes and signals sets matched to groups*, Symmetry. vol. 14 (6), 1214, 2022.

Códigos t-imperfeitos em reticulados [1]

João Eloir Strapasson [2]
FCA - Unicamp, Limeira - SP

1 Introdução

Vários escritores investigaram a presença e ausência de Códigos Perfeitos em $\mathbb{Z}^n$. Isso é evidenciado em diversos artigos, como no trabalho de Golomb e Welch [1], que formularam a hipótese de que Códigos Perfeitos existem em dimensões reduzidas e raios pequenos na métrica ℓ_1, também conhecida como métrica do táxi. Desde então, inúmeros autores têm contribuído para reforçar essa conjectura. Devido à escassez de Códigos Perfeitos no contexto de $\mathbb{Z}^n$, levando em consideração as métricas do táxi e a métrica euclideana, alguns pesquisadores passaram a explorar as métricas ℓ_p. Além disso, eles também direcionaram sua atenção para o estudo de Códigos Quase-Perfeitos. No entanto, a quantidade de Códigos Perfeitos, embora mais significativa nessas métricas alternativas, ainda é limitada e se concentra principalmente em dimensões reduzidas.

Existem também pesquisas dedicadas aos Códigos Perfeitos em reticulados raiz A_n [4, 5]. Inspirados por esses estudos, conseguimos estabelecer condições essenciais para a presença desses Códigos Perfeitos em reticulados mais abrangentes, que agora chamamos de "reticulados ambiente"como mencionado em [6]. A quantidade de Códigos Perfeitos está fortemente ligada ao raio de cobertura do reticulado ambiente. Isso significa que reticulados ambiente com um raio de cobertura mais amplo têm uma maior probabilidade de conter Códigos Perfeitos e em maior quantidade.

Neste trabalho, apresentaremos as condições necessárias para a existência desses códigos perfeitos e quase-perfeitos, na métrica ℓ_p, forneceremos um algoritmo de busca e exibiremos exemplos de Códigos Perfeitos em reticulados 2D e 3D, bem como alguma estratégia para em dimensões mais elevadas.

2 Resultados

Considerem Λ e Λ_a reticulados no $\mathbb{R}^n$ tal que $\Lambda \subset \Lambda_a$. Nós diremos que Λ é um **código linear** no espaço ambiente Λ_a. Seja $\mathcal{T}$ um subconjunto finito de Λ_a. Diremos que $\mathcal{T}$ é um Λ-**ladrilho** para Λ_a se as seguintes condições são satisfeitas: i) $\mathcal{T} \cap (\mathcal{T} + \mathbf{x}) = \emptyset, \forall \mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}$ e ii) $\bigcup_{\mathbf{x}\in\Lambda}(\mathcal{T} + \mathbf{x}) = \Lambda_a$. Dado um reticulado Λ_a, a **bola discreta** centrada em $\mathbf{z} \in \Lambda_a$ e raio r, é o conjunto: $\tilde{B}_p(\mathbf{z}, r) = \{\mathbf{x} \in \Lambda_a : \|\mathbf{z} - \mathbf{x}\|_p \leq r\}$. Os raios possíveis para as bolas discretas são dadas pelo conjunto:

$$\mathcal{D}_{p,n} = \mathcal{D}_{p,n}(\Lambda_a) = \{\|\mathbf{x}\|_p : x \in \Lambda_a\}. \tag{1}$$

[1] Processo nº 2020/09838-0, Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP).
[2] strapass@unicamp.br

O raio de **empacotamento discreto**, denotado por $\tilde{r}(\Lambda)$, é definido como o maior $r \in \mathcal{D}_{p,n}$ tal que:

$$(\tilde{B}_r + \mathbf{x}) \cap \tilde{B}_r) \cap \Lambda_a = \emptyset, \forall \mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}. \quad (2)$$

O raio de **cobertura discreto**, denotado por $\tilde{R}_\Lambda$, é o menor $r \in \mathcal{D}_{p,n}$ tal que $\bigcup_{\mathbf{z}\in\Lambda} \tilde{B}(\mathbf{z}, r) = \Lambda_a$. A distância entre dois elementos $r, s \in \mathcal{D}_{p,n}$ é definida como sendo $d(r, s) = \#\mathcal{D}_{p,n} \cap [r, s)$. Diremos que um reticulado $\Lambda \subset \Lambda_a$ tem **grau de imperfeição** t se $d(\tilde{r}(\Lambda), \tilde{R}(\Lambda)) = t$. Em particular, se $t = 0$ diremos que é perfeito e se $t = 1$ diremos que é quase-perfeito.

Seja $d_{n,p,i}$ o i-ésimo elemento de $\mathcal{D}_{p,n}$. Um reticulado é t-impertifeito se, e só se, existem um inteiro positivo i, um grupo abeliano G de ordem M $(\#\tilde{B}_{p,n}(\mathbf{0}, d_{p,n,i}) \leq M \leq \#\tilde{B}_{p,n}(\mathbf{0}, d_{p,n,i+t}))$ e um homomorfismo $\Phi : \Lambda_a \longrightarrow G$ tal que Φ restrita a bola $\tilde{B}_{p,n}(\mathbf{0}, d_{p,n,i})$ é injetora e Φ restrita a bola $\tilde{B}_{p,n}(\mathbf{0}, d_{p,n,i+t})$ é sobrejetora.

Por fim, concluímos que o número de reticulados t-imperfeitos depende do raio de cobertura do reticulado ambiente e da métrica p, i.e., quanto maior for o raio de cobertura do reticualdo ambiente, provavelmente teremos mais códigos t-imperfeitos teremos, analogamente se aumentarmos o valor de p. Também mais provável que existam mais códigos $t + 1$-imperfeitos do que t-imperfeitos.

Referências

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

[2] A. Campello and G. C. Jorge and J. E. Strapasson and S. I. R. Costa, "Perfect Codes in the ℓ_p metric", *European Journal of Combinatorics*, v. 53, pp. 72-85, 2016.

[3] J. E. Strapasson and G. C. Jorge and A. Campello and S. I. R. Costa, "Quasi-perfect Codes in the ℓ_p metric", *Computational and Applied Mathematics*, v. 37, pp. 852-866, 2018.

[4] S. I. R. Costa and M. Muniz and E. Agustini and R. Palazzo, "Graphs, Tessellations, and Perfect Codes on Flat Tori", *IEEE Transactions on Information Theory*, v. 50, pp. 2363-2377, 2004.

[5] M. Kovacevic, "Codes in A_n Lattices: Geometry of B_h Sets and Difference Sets", *Arxiv*, 2019.

[6] G. Strey and A. Campello and J. E. Strapasson and S. I. R. Costa, "Perfect Codes in Euclidean Lattices: Bounds and Case Studies", *IEEE International Symposium on Information Theory (ISIT)*, pp. 1607-1611, Paris, 2019.

Uma classe de conjuntos de Julia em $\mathbb{Q}_p$

Danilo Antonio Caprio [1]
Departamento de Matemática, Feis - Unesp, Ilha Solteira - SP

1 Introdução

Seja $f : \mathbb{C} \longrightarrow \mathbb{C}$ uma função holomorfa. O conjunto de Julia cheio de f é, por definição, o conjunto $\mathcal{K}^+(f) = \{z \in \mathbb{C} : (f^n(z))_{n\geq 0}$ é limitado$\}$, onde f^n é a $n-$ésima iterada de f. Essa definição pode ser estendida para funções polinomiais definidas em $\mathbb{C}^d$, para $d \geq 2$.

Conjuntos de Julia cheio e sua fronteira (chamada simplesmente de conjunto de Julia) possuem muitas propriedades topológicas e dinâmicas. Esses conjuntos foram definidos de forma independente por Fatou e Julia (ver [6] e [7]) e estão associados a váras áreas da matemática, como por exemplo sistemas dinâmicos, teoria dos números, topologia e análise funcional (see [5]).

Seja $\mathbb{N}$ o conjunto dos números inteiros não negativos. O grupo aditivo dos inteiros p-ádicos é o conjunto $\mathbb{Z}_p$ das sequências $(x_i)_{i\in\mathbb{N}}$ onde x_i é um inteiro $mod\ p^{i+1}$. Cada elemento de $\mathbb{Z}_p$ pode ser escrito como uma série

$$\sum_{i=0}^{+\infty} a_i p^i \text{ onde } a_i \in A = \{0, \ldots, p-1\}.$$

Em $\mathbb{Z}_p$, definimos a norma p-ádica $\|\cdot\|_p$ por

$$\|x\|_p = \begin{cases} p^{-v_p(x)} & \text{se } x \neq 0 \\ 0 & \text{se } x = 0 \end{cases},$$

onde $v_p(x) = \min\{i \in \mathbb{N}, a_i \neq 0\}$ para todo $x = \sum_{i=0}^{+\infty} a_i p^i \neq 0$. Tal define uma métrica d em $\mathbb{Z}_p$ dada por $d(x, y) = |x - y|$ para todo $x, y \in \mathbb{Z}_p$. Além disso, temos que

$$|x - y| \leq \max\{|x|, |y|\}, \text{ para todo } x, y \in \mathbb{Z}_p.$$

Seja $\mathbb{Q}_p$ o corpo das frações de $\mathbb{Z}_p$. Assim, $x \in \mathbb{Q}_p \setminus \{0\}$ pode ser escrito como

$$x = \sum_{i=l}^{+\infty} a_i p^i \text{ onde } a_i \in A = \{0, \ldots, p-1\},\ l \in \mathbb{Z} \text{ e } a_l \neq 0.$$

Considere em $\mathbb{Q}_p$ a norma $\|\cdot\|_p = |\cdot|$ definida por $|x| = p^{-l}$ e a métrica p-ádica d definida $d(x, y) = |x - y|$ para todo $x, y \in \mathbb{Q}_p$.

Vale mencionar que o estudo de sistemas dinâmicos no conjunto dos números p-ádicos possui aplicações na física, ciência cognitiva e criptografia (por exemplo, ver [2] e [8]).

Recentemente, Allen, DeMark, e Petsche (ver [1]) consideraram o estudo dos conjuntos de Julia de aplicações de Hénon definidas no conjuntos dos números p-ádicos $\mathbb{Q}_p$.

[1] danilo.caprio@unesp.br.

2 Resultados

Considere a classe de polinômios $f_c = f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ definida por $f(x, y) = (xy + c, x)$, onde $c \in \mathbb{R}$. Os conjuntos de Julia cheio $\mathcal{K}^+$ e $\mathcal{K}^-$ de f, onde

$$\mathcal{K}^- = \{z \in \mathbb{C} : f^{-n}(z) \text{ existe para todo } n \text{ e } (f^{-n}(z))_{n\geq 0} \text{ é limitado}\}$$

foram estudados por Sylvain Bonnot, André Salles de Carvalho e Ali Messaoudi (para $0 \leq c < 1/4$) em [3] e por Danilo Caprio (para $-1 < |c| < 0$) em [4] e eles provaram que o $\mathcal{K}^+$ é a união das variedades estáveis do ponto fixos fixos e $3-$periódicos de f. Eles também provaram resultados semelhantes para o conjunto de Julia cheio $\mathcal{K}^-$.

Nesse trabalho, consideramos a classe de funções polinomiais $f_c = f : \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ definidas por $f(x, y) = (xy+c, x)$, onde $c \in \mathbb{Q}_p$, e provamos algumas propriedades dinâmicas e topológicas sobre os conjuntos de Julia cheios $\mathcal{K}^+$ e $\mathcal{K}^-$ de f. Em particular, provamos resultados análogos feitos em [3] e [4], porém definidos nos conjuntos dos números p-ádicos.

Este trabalho é em colaboração com Jefferson Bastos e Oyran Raizzaro.

Referências

[1] K. Allen, D. DeMark, and C. Petsche, Non-Archimedean Hénon maps, attractors, and horseshoes, Number Theory, (2018), Art. 5, 30 pp.

[2] V. Anashin, *Uniformly distributed sequences in computer algebra or how to constructprogram generators of random numbers*, Computing mathematics and cybernetics, 2,J. Math. Sci.89 (1998) no. 4, 1355-1390.

[3] S. Bonnot, A. De Carvalho and A. Messaoudi, Julia sets for Fibonacci endomorphisms of $\mathbb{R}^2$, *Dynamical Systems*, **33(4)** (2018), 622–645.

[4] D. Caprio, Filled Julia set of some class of Hénon-like maps, Dynamical Systems, (2019) 35:1, 156-183.

[5] R. Devaney, An Introduction to Chaotic Dynamical Systems, 2nd ed. (1989), Addison-Wesley.

[6] P. Fatou, Sur les équations fonctionnelles, *Bull. Soc. Mat. France*, **47** (1919) 161–271; **48** (1920), 33–94, 208–314.

[7] G. Julia, Mémoire sur l'itération des fonctions rationnelles, *J. Math. Pure Appl.*, **8** (1918), 47–245.

[8] A. Y. Khrennikov, M. Nilsson, *P-adic deterministic and random dynamics*, Math-ematics and Its Applications 574, Kluwer Academic Publishers, 2004.