Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 11, n. 1, 2025.

Trabalho apresentado no XLIII CNMAC, Centro de Convenções do Armação Resort - Porto de Galinhas - PE, 2024

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Mapas Tangente-Chebyshev do Terceiro Tipo sobre Corpos Finitos

Ravi B. D. Figueiredo[1], Juliano B. Lima[2]
Departamento de Eletrônica e Sistemas / UFPE, Recife, PE

Desde o século XIX, os polinômios de Chebyshev têm sido extensivamente estudados e empregados em diversas aplicações [6]. Geralmente, esses polinômios são avaliados sobre os reais, mas também podem ser definidos sobre estruturas algébricas finitas [7]. Neste caso, suas propriedades de semigrupo e de permutação são particularmente importantes, sendo aplicáveis ao embaralhamento de símbolos em criptossistemas de chave secreta [1] e ao projeto de algoritmos criptográficos de chave pública [3], respectivamente.

Num artigo recente [5], Lima e Campello de Souza introduziram um novo mapa racional do tipo Chebyshev sobre corpos finitos. Tal mapa, que é identificado como mapa tangente-Chebyshev (ou t-Chebyshev), é definido basicamente pela substituição das funções cosseno e cosseno inverso sobre corpos finitos, na definição do polinômio de Chebyshev de primeiro tipo [4], pelas funções tangente e tangente inversa sobre corpos finitos, respectivamente, as quais o referido trabalho também definiu. Precisamente, denotando por $\mathbb{F}_q$ o corpo finito com $q = p^r$ elementos, em que p é um primo ímpar, tem-se:

Definição 1. *[5] O n-ésimo mapa tangente-Chebyshev sobre $\mathbb{F}_q$, com $n \in \mathbb{N}$, é definido como*

$$C_n(x) = \tan_\zeta \left(n \arctan_\zeta(x)\right), \tag{1}$$

em que $\zeta \in \mathbb{I}_q$ (o conjunto de inteiros Gaussianos sobre $\mathbb{F}_q$ com elementos da forma $a+bi$, $a, b \in \mathbb{F}_q$ e i^2 é um não-resíduo quadrático sobre $\mathbb{F}_q$), $x \in \mathbb{T}_\zeta$ (o conjunto de todos os possíveis valores para tangentes sobre $\mathbb{F}_q$ calculados com relação a ζ),

$$\tan_\zeta(y) = \frac{1}{i}\frac{\zeta^y - \zeta^{-y}}{\zeta^y + \zeta^{-y}} \tag{2}$$

e $\arctan_\zeta(\cdot)$ denota a tangente inversa sobre $\mathbb{F}_q$ calculada com relação a ζ.

O mapa em questão teve suas propriedades de semigrupo, permutação e involução estabelecidas e seus zeros e pólos determinados em [5]. Outras propriedades de C_n e grafos funcionais induzidos por este mapa foram investigados em [2].

No presente trabalho, é introduzido um novo tipo de mapa tangente-Chebyshev sobre corpos finitos. Ele se origina da substituição, na expressão trigonométrica dos polinômios de Chebyshev do terceiro tipo sobre corpos finitos [4], das funções cosseno e cosseno inverso sobre corpos finitos pelas funções tangente e tangente inversa sobre corpos finitos, respectivamente. Assim, o novo mapa é identificado como tangente-Chebyshev do terceiro tipo sobre corpos finitos. Sua definição é a seguinte:

[1] ravi.bdf@gmail.com
[2] juliano.lima@ufpe.br

Definição 2. *Sejam $\zeta \in \mathbb{I}_q$ e $n \in \mathbb{N}$. O n-ésimo mapa tangente-Chebyshev do terceiro tipo sobre $\mathbb{F}_q$ é definido como*

$$E_n(x) = \frac{\tan_\zeta\left(\left(n+\frac{1}{2}\right)\arctan_\zeta(x)\right)}{\tan_\zeta\left(\frac{1}{2}\arctan_\zeta(x)\right)}, \quad \zeta \in \mathbb{I}_q \quad e \quad x \in \mathbb{T}_\zeta. \tag{3}$$

Tem-se $E_0(x) = 1$, para todo $x \in \mathbb{F}_q$. Para outros valores de n, $E_n(x)$ pode ser obtido por meio da relação de recorrência estabelecida a seguir.

Proposição 1. *Sejam $\zeta \in \mathbb{I}_q$, i^2 um não-resíduo quadrático sobre $\mathbb{F}_q$ e $n \in \mathbb{N}$. Os mapas tangente-Chebyshev do terceiro tipo sobre $\mathbb{F}_q$ satisfazem à relação de recorrência*

$$E_{n+1}(x) = \frac{E_n(x) + x[c(x)]^{-1}}{1 + i^2 x c(x) E_n(x)}, \quad c(x) = \tan_\zeta\left(\frac{1}{2}\arctan_\zeta(x)\right). \tag{4}$$

Empregando a Definição 2, a Proposição 1 e outros resultados relativos à manipulação da função tangente sobre corpos finitos e de sua inversa, é possível prover expressões fechadas para os mapas tangente-Chebyshev do terceiro tipo sobre corpos finitos. Além disso, derivam-se relações entre os mapas em questão e aqueles dados na Definição 1. Mais especificamente, tem-se:

Proposição 2. *Sejam $\zeta \in \mathbb{I}_q$, i^2 um não-resíduo quadrático sobre $\mathbb{F}_q$ e $n \in \mathbb{N}$. Então,*

$$E_n(x) = [c(x)]^{-1}\frac{1 \pm \sqrt{1 - i^2 C_{2n+1}^2(x)}}{i^2 C_{2n+1}(x)} = \frac{C_{2n+1}\left(\frac{1\pm\sqrt{1-i^2x^2}}{i^2 x}\right)}{\frac{1\pm\sqrt{1-i^2x^2}}{i^2x}} = \frac{C_{2n+1}(c(x))}{c(x)}. \tag{5}$$

Por fim, vale mencionar que os pólos e zeros de $E_n(x)$ também já foram especificados. Atualmente, têm sido estudadas outras propriedades desses mapas e caracterizados os seus grafos funcionais. A expectativa é que, com isso, possa ser investigada a sua potencial aplicabilidade em cenários práticos da Criptografia e da codificação de canal. Espera-se, ainda, definir outros tipos de mapas tangente-Chebyshev, como os do segundo e do quarto tipos e estabelecer as suas propriedades.

Referências

[1] P. Charpin, S. Mesnager e S. Sarkar. "Involutions Over the Galois Field $\mathbb{F}_{2^n}$". Em: **IEEE Transactions on Information Theory** 62.4 (2016), pp. 2266–2275.

[2] R. B. D. Figueiredo e J. B. Lima. "Tangent-Chebyshev maps over finite fields: New properties and functional graphs". Em: **Cryptography and Communications** 14 (2022), pp. 897–908.

[3] X. Liao, F. Chen e K.-W. Wong. "On the Security of Public-Key Algorithms Based on Chebyshev Polynomials over the Finite Field Z_N". Em: **IEEE Trans. Comput.** 59.10 (2010), pp. 1392–1401.

[4] J. B. Lima, D. Panario e R. M. C. Campello de Souza. "A trigonometric approach for Chebyshev polynomials over finite fields". Em: **Applied Algebra and Number Theory**. Ed. por Gerhard Larcher, Friedrich Pillichshammer, Arne Winterhof e Chaoping Xing. Cambridge: Cambridge University Press, 2014, pp. 255–279.

[5] J. B. Lima e R. M. Campello de Souza. "Tangent Function and Chebyshev-like Rational Maps over Finite Fields". Em: **IEEE Trans. Circuits Syst. II, Exp. Briefs** 67.4 (2020), pp. 775–779.

[6] J. C. Mason e D. C. Handscomb. **Chebyshev Polynomials**. Boca Raton: Chapman & Hall/CRC, 2003.

[7] G. L. Mullen e D. Panario. **Handbook of Finite Fields**. Chapman & Hall/CRC, 2013.